CCIE Self-Study

CCIE Security Exam Certification Guide Second Edition

Henry Benjamin, CCIE No. 4695

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

CCIE Self-Study: CCIE Security Exam Certification Guide, Second Edition

Henry Benjamin, CCIE No. 4695

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

First Printing May 2005

Library of Congress Cataloging-in-Publication Number: 2004109069

ISBN: 1-58720-135-6

Warning and Disclaimer

This book is designed to provide information about the CCIE Security written exam. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The author, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Corporate and Government Sales

Cisco Press offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales.

For more information please contact: U.S. Corporate and Government Sales 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the U.S. please contact: International Sales international@pearsoned.com

Publisher: John Wait

Editor-in-Chief: John Kane

Executive Editor: Brett Bartow

Cisco Representative: Anthony Wolfenden

Cisco Press Program Manager: Jeff Brady

Production Manager: Patrick Kanouse

Development Editor: Andrew Cupp

Project Editor: Sheila Schroeder

Copy Editor: Bill McManus

Technical Editors: Yusuf Bhaiji, Randy Ivener, Stephen Kalman

Team Coordinator: Tammi Barnett

Book and Cover Designer: Louisa Adair

Composition: Mark Shirar

Indexer: Tim Wright

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA

About the Author

Henry Benjamin, CCIE No. 4695, is a triple CCIE, having been certified in Routing and Switching in May 1999, ISP Dial in June 2001, and Communications and Services in May 2002. He has more than 15 years experience in Cisco networks including planning, designing, and implementing large IP networks running IGRP, EIGRP, BGP, OSPF, and voice over IP (VoIP). Recently Henry has worked for a large IT organization based in Sydney, Australia as a key network designer, securing, designing, and implementing data and VoIP networks all over Australia.

Henry has been a key member of the CCIE global team and internal Cisco IT team based in Sydney. As a senior and core member of the team his tasks included writing questions for the coveted CCIE Routing and Switching, CCIE Security, and CCIE Communications and Services tracks as well as the CCIE written recertification examinations, and proctoring new laboratory examinations. Henry has authored two other titles, CCNP Practical Studies: Routing (Cisco Press) and CCIE Routing and Switching Exam Cram (Exam: 350-001) (Coriolis Group Books). Henry currently is a senior technical consultant for the premier Cisco Gold Partner in Australia.

Henry holds a bachelor of aeronautical engineering degree from Sydney University (1991).

About the Technical Reviewers

Yusuf Bhaiji, CCIE No. 9305, has been with Cisco Systems, Inc., for four years and is currently the content manager, CCIE security, and proctor in the Cisco Systems Sydney, Australia Lab. Prior to this, he was technical lead for the Sydney TAC Security and VPN team. Yusuf's passion for security- and VPN-related technologies has played a dominant role in his 14 years of industry experience, from as far back as his initial master's degree in computer science, and since is reflected in his numerous certifications. Yusuf authored the Cisco Press publication *CCIE Security Practice Labs* (ISBN 1-58705-134-6) released early 2004. He has also been a technical reviewer for several Cisco Press publications and has written articles for various publications and magazines. His recent article "Cracking the Code" was published in *Packet* magazine (Vol. 16, No. 3, Third Quarter 2004).

Randy Ivener, CCIE No. 10722, is a security specialist with Cisco Systems Product Security Incident Response Team. He is a CISSP and ASQ CSQE. Randy has spent many years as a network security consultant helping companies understand and secure their networks. Before becoming immersed in information security, he spent time in software development and as a training instructor. Randy graduated from the U.S. Naval Academy and holds a master's degree in business administration.

Stephen Kalman is a data security trainer. He is the author or tech editor of more than 20 books, courses, and CBT titles. His most recent book is *Web Security Field Guide* (ISBN 1-58705-092-7) from Cisco Press. In addition to those responsibilities, he runs a consulting company, Esquire Micro Consultants, that specializes in network security assessments and forensics. Mr. Kalman holds CISSP, CEH, CHFI, CCNA, CCDA, A+, Network+, and Security+ certifications and is a member of the New York State Bar.

Dedications

I dedicate this book to Our Lady, Mary, the Mother of the Eucharist.

“I am the Mother of the Eucharist. Know Jesus’ word. Love Jesus, the Eucharist.”

—Our Lady, Mary, Mother of the Eucharist

Dedica (Italiano)

Dedico questo libro alla Madonna, Maria, Madre dell’Eucaristia.

“Io sono la Madre dell’Eucaristia. Conoscete Gesù Parola. Amate Gesù Eucaristia.”

—La Madonna, Maria, Madre dell’Eucaristia

Acknowledgments

First I would like to thank the folks at Cisco Press for helping me and introducing me to this challenging project.

Without Brett Bartow this book would never have been started. Thank you Brett for liaising with the CCIE team on my behalf and believing that I could complete this book.

Andrew Cupp, who was expecting his first baby at the time of completion, I really appreciate your expert advice and guidance. Without you both this book would only be a dream. Michelle, I will never forget you. Also I want to mention Sheila Schroeder, Chris Cleveland, John Kane, and Bill McManus for being part of the best virtual team I have ever had the pleasure to be part of.

I would like to especially thank Gert De Laet for his valuable input and direction of this guide. Gert was a contributing author to Chapter 8, "CCIE Security Self-Study Lab." Thank you, my dear friend.

I must also mention the enormous effort of the technical reviewers, especially Randy for your eye for the smallest and most technical aspects of every word I write, Steve for sharing with me and the readers real-life scenarios, and of course Yusuf who made sure I did not break any rules. I look forward to reviewing your next books with great anticipation.

I would also like to thank my family, including two beautiful sons, Simon (the Xbox and PC guru) and Daniel, and my wife Sharon, who was expecting during the writing of this guide. I was always grateful for my family's understanding when I needed time to complete this project. I treasure my time with my family and my growing boys who make me proud to be their Dad. Simon I love you to the sun and keep going around forever. Daniel I cannot wait to hold you in my arms each day that goes by. I also thank my Dad and Mum (1948-2001) for bringing me up with such great examples. Massimo Piccinini, my physicist friend in the most beautiful City of the World, Roma, thank you for friendship and love over the past 5 years; thank you for sharing your life with me even though we live so far apart, thank you for your Italian translation and many more beautiful things you do for me and my family. It was an inspiration to know you. I would also like to mention these wonderful friends who support me from far with much love: Vescovo Claudio (Vescovo Ordinato da Dio Vescovo dell'Eucaristia), my favorite priest in all the world, I will never forget the warm embrace you gave me, who also helped me realize what is important in life, Saint Marisa Rossi (thank you for your prayers), Massimo (yes twice), Giorgio, Antonella, Domenico, Federica, Fabrizio, Giulia, Alessandro, Paola, Fabio, Riccardo, Alessandra, Elisa, Selenia, Angelo, Mariasole, Giacomo, Laura, Jacopo, Samuele, Yari, Laura, Emanuele, and Sara.

I would like to specially mention Claudine Campbell for ensuring my musical hardware arrived also on time and saved me loads of money. Thank you cousin.

I want to thank my wonderful aunties who gave me wonderful encouragement over all the years they have known me; thank you Oto, Lyda, and Alice.

May God bless us all.

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:

- Go to http://www.ciscopress.com/safarienabled
- Complete the brief registration form
- Enter the coupon code Y6M1-BYDL-7W20-85MU-DU7Z

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

Contents at a Glance

Contents

Foreword

Cisco Systems launched the CCIE Program in November 1993; it was the first certification program from Cisco. CCIE certification is widely considered the industry's highest-level IT certification program, and it is commonly referred as the doctorate of networking. It equips candidates with excellent internetworking skills that are simply the best in the industry. The program identifies leaders with a proven commitment to their career, the industry, and the process of ongoing learning.

Internet Security

As Dr. Vinton G. Cerf has said, "The wonderful thing about the Internet is that all these computers are connected. However, the challenge of the Internet also is that all these computers are connected."

The luxury of access to this wealth of information comes with its risks, and anyone on the Internet is a potential stakeholder. The risks vary from information loss or corruption to information theft to lost revenue and productivity. The number of security incidents is also growing dramatically. On the other hand, organizations cannot simply cut off communications with the outside world and hope to survive. The risks inherent in modern networked communications drive the need for network security implementations to improve the security posture within every organization worldwide. Today's most complex networks require a comprehensive and integrated security solution.

Need for Security Certification

Security is one of the fastest-growing areas in the industry. Information security is on top of the agenda at all organizations. Companies have a need, and many times a legal requirement, to keep information secure. As a result, there is an ever-growing demand for IT professionals with the skills to implement effective, end-to-end security solutions to guard against all manner of threats. Cisco Systems helps to meet this demand by offering CCIE Security certification, setting the professional benchmark in internetworking expertise.

This book

Every chapter of this book holds facts on one of the objectives from the CCIE Security 2.0 written exam. This book will be a valuable asset for potential CCIE Security candidates. I am positive individuals will inevitably gain extensive security network knowledge during their preparation for the CCIE Security written exam by using this book.

Best wishes and Good Luck!

Yusuf Hussain Bhaiji

Program Manager, CCIE Security

Cisco Systems, Inc.

Command Syntax Conventions

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

- **Boldface** indicates commands and keywords that are entered literally as shown.
- *Italics* indicate arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets, [ ], indicate optional elements.
- Braces, { }, indicate a required choice.
- Braces within brackets, [{ }], indicate a required choice within an optional element.

Introduction

The Cisco Certified Internetwork Expert (CCIE) Security Certification is an increasingly popular internetworking certification and one of the most popular security certifications in the world. Although CCIE certification builds on the foundation you may have established from CCNA certification, CCNP certification, and other certifications, there is no prerequisite to attempt to gain CCIE certification. However, attaining CCNA and CCNP certifications will help you understand the Cisco subjects and testing strategies that are necessary to be successful when you attempt the CCIE written and lab exams.

This book is designed to help you prepare for the CCIE Security written exam. This second edition builds on the successful first edition by incorporating full coverage of the latest exam topics. This book will also help you prepare for the CCIE Security recertification exam.

The CCIE Security certification was recognized in December 2003 as being the second hottest certification in the IT industry.

NOTE Cisco recently announced a revision of the CCIE Security certification exam with a number of new topics added and a small amount of old and unused technologies removed.

For more details on the new CCIE Security 2.0 written exam, visit http://www.cisco.com/en/US/learning/le3/ccie/security/index.html.

This new edition has been updated to consider all of these new changes.

The CCIE Security track was released in 2001 by Cisco and since security technologies have been evolving so much, Cisco is constantly working towards improving the track and ensuring the content is up-to-date.

To achieve CCIE Security certification you must first pass a written qualification exam (a computer-based exam of 100 multiple-choice questions) and a one-day lab exam. To qualify for the CCIE Security lab exam, you must first successfully pass the written exam.

Both exams are difficult, and this book is primarily aimed at helping you prepare for the written exam by covering all of the stated written exam blueprint topics. However, Chapter 8, "CCIE Security Self-Study Lab," includes a CCIE Security self-study lab that helps you with comprehensive preparation for the lab exam by giving you an idea of the challenges you will face in the lab exam. Appendix C, "Sample CCIE Routing and Switching Lab I" and Appendix D, "Sample CCIE Routing and Switching Lab II," also contain bonus Routing and Switching lab topics to help you prepare for that exam as well. This is an added bonus because the lab portion of the CCIE Security certification contains approximately 50 percent of topics from Routing and Switching content. Recent Cisco announcements regarding the lab exam mean that simple assignments such as basic Frame Relay configurations, VLAN configuration, and routing protocols are now preconfigured for you. This ensures that the CCIE Security track is focused more on testing an individual's security skills.

Achieving CCIE Security certification is made intentionally difficult by Cisco. You should have extensive practical experience and you should consult many resources to be prepared to pass a CCIE exam. Cisco advises that you have 3 to 5 years of prior experience before attempting any CCIE track. What this book will do for you is give you a comprehensive look at all of the topics covered on the CCIE Security written exam. Use this book and the CD-ROM to confidently assess your level of preparedness for all of the topics covered on the written exam.

The CCIE Security written exam is a 2-hour multiple-choice exam with a surprising amount of Cisco IOS configurations and scenario-type questions. Some questions require only one answer while other questions require two or more.

Passing the written exam means that you have mastered networking concepts and fundamental security topics necessary to build a complex, secure, and routable IP network using Cisco routers and security equipment and software. This is a great skill and demonstrates to any employer you are ready for any challenges that may be asked of you.

NOTE The CCIE Security written exam is a computer-based exam with multiple-choice questions. The exam can be taken at any Thomson Prometric testing center (http://www.prometric.com/Default.htm) or Pearson VUE testing site (http://www.vue.com/). The exam is 2 hours long and has 100 questions. You should check with Prometric or VUE for the exact length of the exam. The exam is constantly under review, so be sure to check the latest updates from Cisco at http://www.cisco.com/en/US/learning/le3/ccie/security/index.html.

Goals of This Book

The primary goal of this book is to ensure that a CCIE Security candidate has all the technical skills and knowledge required to pass the written exam. Most Cisco certifications require practical skills, and the only way to hone those skills is in a working environment using common Cisco-defined techniques.

This book provides you with comprehensive coverage of CCIE Security exam topics. Ultimately, the goal of this book is to get you from where you are today to the point that you can confidently pass the CCIE Security written exam. Therefore, this book's features are all geared toward helping you discover the IP routing challenges and security scenarios that are on the exam, helping you discover where you have a knowledge deficiency in these topics, and helping you discover what you need to know to master those topics.

Organization of this Book

Each chapter starts by testing your current knowledge on the chapter's topics with a "Do I Know This Already?" quiz. This quiz is aimed at helping you decide whether you need to cover the whole chapter, read only parts of the chapter, or just skip the chapter altogether. See the introduction to each "Do I Know This Already?" quiz for more details.

Each chapter then contains a "Foundation Topics" section with extensive coverage of the CCIE Security exam topics covered in that chapter. This is followed by a "Foundation Summary" section that provides more-condensed coverage of the topics and is ideal for review and study later. Each chapter ends with "Q & A" and "Scenarios" sections to help you assess how well you mastered the topics covered in the chapter. Finally, the book includes a CD-ROM with sample exam questions and other preparation resources. All of these tools are designed to help you assess your preparedness level and then teach you. Once you identify deficiencies, you should concentrate your studies on those areas until you feel comfortable with them.

The following list summarizes the individual elements of this book:

- **Chapter 1, "General Networking Topics"**—This chapter covers general networking technologies, including an overview of the OSI model, switching concepts, and routing protocols. The TCP/IP model is presented and explained with common applications used in today's IP networks. Routing protocols and sample configurations are presented to ensure that you have a good understanding of how Cisco IOS routes IP datagrams. Concluding this chapter is a discussion of some of today's most widely used WAN protocols, namely PPP, ISDN, and Frame Relay. Keep in mind that the CCIE Security exam covers Routing and Switching topics as well as Security topics. Telephony and wireless best practices round off this chapter.
- **Chapter 2, "Application Protocols"**—This chapter covers the principles of Domain Name System and TFTP file transfers. The most widely used applications such as FTP and HTTP are covered along with some of the more secure methods used to download information from the web, such as Secure Shell and the Secure Sockets Layer protocol. SSH and Remote Data Exchange Protocol (RDEP) are new topics covered for the latest exam. A challenging scenario is included to ensure that you have the IOS skill set to configure DNS, TFTP, NTP, and SNMP.
- **Chapter 3, "Cisco IOS Specifics and Security"**—This chapter covers the more advanced topics available to Cisco IOS routers. It covers in detail the hardware components of a Cisco router and how to manage Cisco routers. Common Cisco device operational commands are described, and examples

show how to manage Cisco IOS in today's large IP networks. Cisco password recovery techniques and basic password security are detailed to ensure that you have a solid grasp of Cisco device operation. Coverage of standard and extended access lists and examples conclude this chapter. Chapter 3 contains a wealth of new material covering the new exam objectives, such as new routing and switching features, access layer controls, port security, DHCP snoop, and security policy best practices.

- **Chapter 4, "Security Protocols"**—This chapter focuses on security protocols developed and supported by Cisco Systems and refined in RFCs, namely TACACS+ and RADIUS. Following sample configurations, the chapter covers encryption technologies and their use in today's vulnerable IP networks. Additionally, to ensure that you have all the bases covered, Advanced Encryption Standard (AES) and securing wireless networks are covered.
- **Chapter 5, "Cisco Security Applications"**—This chapter required a large overhaul from the first edition. It covers new topics such as Cisco IDS, the VPN 3000 Concentrator, VPN Client software, and new Catalyst security modules. Cisco Secure ACS and Security Information Monitoring System round off this chapter.
- **Chapter 6, "Security Technologies"**—This chapter describes the basic security methods and evolution of new secure networks including packet filtering and proxies. The IP address depletion rates with IPv4 have led to NAT/PAT becoming increasingly popular; this chapter covers these topics along with sample IOS configurations. The Cisco PIX Firewall is Cisco's trademark security device, and this chapter teaches you the architecture and configuration of these unique security devices. The Cisco IOS Firewall feature set and VPN are covered. Network-based IDS, host-based IDS, and Cisco Threat Response are covered in detail as well.
- **Chapter 7, "Network Security Policies, Vulnerabilities, and Protection"**—This chapter reviews today's most common Cisco security policies and mechanisms available to the Internet community used to combat cyber attacks. The security standards body CERT/CC is covered along with descriptions of Cisco IOS–based security methods used to ensure that all attacks are reported and acted upon. Cisco security applications such as Intrusion Detections System are covered to lay the foundation you will need to master the topics covered on the CCIE Security written exam.
- **Chapter 8, "CCIE Security Self-Study Lab"**—This chapter is designed to assist you in your final preparation for CCIE Security certification. This rare sample lab was put together by one former (Sydney CCIE lab) and one current (Brussels CCIE lab) CCIE proctor from the CCIE team. It is a sample CCIE Security lab with working solutions to ensure that you are fully prepared for the final hurdle, the CCIE Security lab exam. In my view and experience (including writing numerous CCIE lab exams) this sample exam is more challenging than most Cisco exams. Please enjoy and study this sample CCIE Security lab. Many readers have e-mailed me in the past to ask what is their next step after passing the written exam. An excellent start is Chapter 8 of this book. When the CCIE program first started, there were no sample lab questions. Now in your hands you have a sample Security lab exam and bonus sample Routing and Switching lab exams (Appendixes C and D).

- **Appendix A, "Answers to Quiz Questions"**—Appendix A provides the answers to the "Do I Know This Already?" and "Q & A" quiz questions in each chapter. Explanations are included where appropriate.
- **Appendix B, "Study Tips for CCIE Security Examinations"**—Appendix B describes some of the study tips and preparation steps you should consider before embarking on the long hard road to CCIE Security certification. There are also answers to frequently asked question about the written exam and CCIE Security certification.
- **Appendix C, "Sample CCIE Routing and Switching Lab I"**—Appendix C is a bonus appendix designed to assist you in your final preparation for the CCIE Routing and Switching lab exam and help you appreciate the level of difficulty found in any CCIE lab exam.
- **Appendix D, "Sample CCIE Routing and Switching Lab II"**—Appendix D is a second bonus appendix designed to assist you in your final preparation for the CCIE Routing and Switching lab exam and help you appreciate the level of difficulty found in any CCIE lab exam. This second bonus version of the R&S lab exam contains only four routers, for those readers who do not have access to a large number of routers.
- **CD-ROM**—The CD-ROM provides you with a testing engine that simulates the written exam with a database of over 500 questions. Take several sample CD-ROM exams and ensure that you review all the answers and results so that you can fully prepare for the exam by identifying areas where you need extra preparation.

CCIE Security Written Exam Blueprint

Table I-1 lists the CCIE Security written exam blueprint topics and the corresponding chapters where you can find the material covered in this book. As you can see, the blueprint places the objectives into eight categories. The book covers all of these topics. This blueprint is a guideline for the type of content that is likely to appear on the exam. You can also find it at http://www.cisco.com/en/US/learning/le3/ccie/security/wr_exam_blueprint.html.

Table 8-1 *CCIE Security Written Exam Blueprint**

ID	Topic Area	Chapter Covering the Topic
I. Security Protocols		
A.	Remote Authentication Dial-In User Service (RADIUS)	Chapter 4
B.	Terminal Access Controller Access Control System Plus (TACACS+)	Chapter 4
C.	AES	Chapter 4
D.	EAP, PEAP, TKIP, TLS	Chapter 4
E.	Data Encryption Standard (DES)	Chapter 4
F.	Triple DES (DES3)	Chapter 4
G.	IP Secure (IPSec)	Chapter 4
H.	Internet Key Exchange (IKE)	Chapter 4
I.	Certificate Enrollment Protocol (CEP)	Chapter 4
ID	**Topic Area**	**Chapter Covering the Topic**
J.	Point-to-Point Tunneling Protocol (PPTP)	Chapter 4
K.	Layer 2 Tunneling Protocol (L2TP)	Chapter 4
II. Application Protocols		
A.	Domain Name System (DNS)	Chapter 2
B.	Trivial File Transfer Protocol (TFTP)	Chapter 2
C.	File Transfer Protocol (FTP)	Chapter 2
D.	Hypertext Transfer Protocol (HTTP)	Chapter 2
E.	Secure Sockets Layer (SSL)	Chapter 2
F.	Simple Mail Transfer Protocol (SMTP)	Chapter 2
G.	Network Time Protocol (NTP)	Chapter 2
H.	IOS SSH	Chapter 2
I.	Lightweight Directory Access Protocol (LDAP)	Chapter 2
J.	Active Directory	Chapter 2
K.	Remote Data Exchange Protocol (RDEP)	Chapter 2
III. General Networking		
A.	Networking Basics	Chapter 1
B.	TCP/IP	Chapter 1
C.	Switching and Bridging (including: VLANs, Spanning Tree, etc.)	Chapter 1

Table 8-1 *CCIE Security Written Exam Blueprint* (Continued)*

ID	Topic Area	Chapter Covering the Topic
D.	Routed Protocols	Chapter 1
E.	Routing Protocols (including: RIP, EIGRP, OSPF, BGP)	Chapter 1
F.	Point-to-Point Protocol (PPP)	Chapter 1
G.	IP Multicast	Chapter 1
H.	Integrated Services Digital Network (ISDN)	Chapter 1
I.	Async	Chapter 1
J.	Access Devices (for example, Cisco AS 5300 series)	Chapter 1
K.	Telephony Best Practices	Chapter 1
L.	Wireless Best Practices	Chapter 1
IV. Security Technologies		
A.	Concepts – Security Best Practices	Chapter 6
B.	Packet Filtering	Chapter 6
C.	PIX and IOS Authentication Proxies	Chapter 6
D.	Port Address Translation (PAT)	Chapter 6
E.	Network Address Translation (NAT)	Chapter 6
F.	Firewalls	Chapter 6
G.	Content Filters	Chapter 6
H.	Public Key Infrastructure (PKI)	Chapter 6
I.	Authentication Technologies	Chapter 6
J.	Authorization Technologies	Chapter 6
K.	Virtual Private Networks (VPNs)	Chapter 6
L.	Network IDS: Anomaly, Signature, Passive, Inline	Chapter 6
M.	Host Intrusion Prevention	Chapter 6
N.	Cisco Threat Response	Chapter 6
V. Cisco Security Applications		
A.	Cisco Secure NT	Chapter 5
B.	Cisco Secure PIX Firewall	Chapter 6
C.	VMS	Chapter 5
D.	Cisco Secure Intrusion Detection System (formerly NetRanger)	Chapter 5

Table 8-1 *CCIE Security Written Exam Blueprint* (Continued)*

ID	Topic Area	Chapter Covering the Topic
E.	IOS Firewall Feature Set	Chapter 6
F.	VPN 3000	Chapter 5
G.	Client-Side VPN	Chapter 5
H.	CAT Service Modules	Chapter 5
I.	IOS IDS (in line)	Chapter 5
J.	Cisco Secure ACS	Chapter 5
K.	Security Information Monitoring System (event correlation, basic forensics)	Chapter 5
VI. Security General		
A.	Policies – Security Policy Best Practices	Chapter 7
B.	Standards Bodies – IETF	Chapter 7
C.	Vulnerability Discussions	Chapter 7
D.	Attacks and Common Exploits – recon, priv escalation, penetration, cleanup, backdoor	Chapter 7
VII. Cisco General		
A.	IOS specifics	Chapter 3
B.	Routing and Switching Security Features: IE MAC Address Controls, Port Security, DHCP Snoop	Chapter 3
C.	Security Policy Best Practices	Chapter 3

*Note from Cisco.com: The Security written exam (350-018) went into production in all testing locations on June 1, 2004. The exam has 100 multiple-choice questions and is two hours in duration. The topic areas listed are general guidelines for the type of content that is likely to appear on the exam. Please note, however, that other relevant or related topic areas may also appear. Italicized bold type indicates topic areas changed from the previous Security exam (prior to June 1, 2004) and strengthens coverage of highly-secure enterprise networks.

How to Prepare for the CCIE Security Written Exam Using This Book and CD-ROM

The chapters open by identifying the exam blueprint topics covered in that chapter. You can begin by taking the "Do I Know This Already?" quiz to immediately evaluate how familiar you are with the chapter's subjects. Use the quiz instructions in each chapter to decide how to proceed. If you feel unfamiliar with the material and you need to learn a lot about the topics, start by reading the "Foundation Topics" section, which goes into detail about the objectives covered in that chapter. If your quiz results demonstrate that you already have a strong grasp of the subjects, you can skim certain topics in the chapter and then move

on to the "Foundation Summary," "Q & A," and "Scenarios" sections at the end of the chapter. If you feel comfortable with your results after working through these sections, move on to the next chapter or use the CD-ROM to practice the topics. If you are consistently identifying areas that you have trouble with, study those topics more and then assess yourself again.

This book covers all the objectives in the CCIE Security written exam blueprint, but no one book can teach you everything you need to know for a CCIE exam. Although you can use this book to identify and fill in knowledge gaps, you might encounter areas where you feel less prepared than others. Consider supplementing your learning in these areas with practical experience, specific books on the subject, or by searching the topic at Cisco.com.

In addition to the chapters in this book, the accompanying CD-ROM provides tools that can help you prepare for the exam. The CD-ROM includes over 500 sample questions that you can explore in different modes. You can work through the questions in practice mode so that you can learn as you go or you can assess your preparedness in test mode. Practice mode allows you to link to an electronic version of the book when you want more information on the particular topic covered in the question. In practice mode, you can choose the topics and number of questions you want to work through. Test mode simulates the exact conditions in the CCIE Security certification exam, where you are presented with 100 difficult questions and asked to attain a pass score of 80 percent within 2 hours.

At the end of a CD-ROM practice exam, you receive a score and a categorical breakdown of your performance. Use these results to identify areas of strengths and weaknesses, so you can use this book and other resources to fill in any knowledge gaps.

Using this book is one of the best steps you can take toward achieving one of the most sought-after certifications in the IT industry. You need to rely on your extensive experience to pass the exam, but this book can make your preparation focused and efficient. Do not give up, and keep studying until you become certified.

Final Thoughts

Having many Cisco certifications myself, the joy and success they can help bring has significantly changed my life and that of my family. There are always challenges facing network engineers, and no doubt once you are a CCIE, meeting those challenges will drive you to acquire skills you never knew you could master.

I sincerely hope you enjoy your time spent with this book; it took over 6 months of long exhausting nights to complete to ensure that you have the perfect companion through your journey to becoming a Security CCIE.

When you succeed in attaining your certification, feel free to e-mail me at henry.benjamin@optusnet.com so I too can enjoy your success and joy. Please feel free to send me your feedback as well, as many readers of the first edition did to my wonderful surprise. I wish you the best in your endeavors and good luck!

Exam Topics in This Chapter

- Networking Basics
- TCP/IP
- Switching and Bridging (including VLANs, Spanning Tree, and more)
- Routed Protocols
- Routing Protocols (including RIP, EIGRP, OSPF, and BGP)
- Point-to-Point Protocol (PPP)
- IP Multicast
- Integrated Services Digital Network (ISDN)
- Async
- Access Devices (for example, Cisco AS5300 series)
- Telephony Best Practices
- Wireless Best Practices

You can find in this book's introduction a list of all of the exam topics. For the latest updates on exam topics, visit Cisco.com.

CHAPTER 1

General Networking Topics

This chapter covers general networking concepts listed in the CCIE Security blueprint for the written exam. The CCIE Security blueprint lists some example topics that define general networking, including switching, TCP/IP, routed and routing protocols, PPP, ISDN, asynchronous communications, and telephony and wireless best practices.

The CCIE Security written exam contains approximately 50 percent security questions and approximately 50 percent general networking questions. This chapter prepares you for the general networking questions. Although the CCIE Security written exam blueprint lists some specific networking topics, it does not, for example, mention Frame Relay, which might appear on the exam. This chapter covers many of the listed, and a few of the unlisted, general networking topics.

Although these topics are not extensively defined in the blueprint, the CCIE Security written exam might include topics taken from the CCIE Routing and Switching written exam blueprint. This chapter endeavors to cover all bases and provide quality test examples to ensure that you are well prepared to tackle the general networking questions you encounter in the examination.

This chapter covers the following topics:

- **Networking Basics**—Discusses the OSI model, concepts, and functions. Topics include the seven layers of the OSI model and common TCP/IP networking examples.
- **Switching and Bridging**—Covers the process that today's networks use to switch packets and describes traditional bridging methods. Virtual LANs, spanning tree protocol (STP), and Fast Ethernet Channel are discussed.
- **Routing IP**—Covers the most widely-used routed protocol in today's Internet, IP, and the routing protocols available on Cisco routers, such as RIP, EIGRP, OSPF, and BGP. Cisco IOS commands and configuration examples demonstrate the power of routing IP on Cisco routers.
- **PPP, ISDN, Frame Relay, IP Multicast, and Async**—Two of the most widely used dialup protocols are PPP and ISDN. Frame Relay is covered briefly to ensure that you have a good understanding of the common terminology used in today's networks. IP multicast and async protocols are also covered.

- **Telephony Best Practices**—IP Telephony is one of the largest investments that Cisco has made in its 20-year history. This section covers the best practices used in today's Cisco Voice over IP (VoIP) implementation.
- **Wireless Best Practices**—Wireless, another emerging technology, contains a complex array of standards and bodies that have left the IT market rather insecure about wireless. This section helps alleviate some of those concerns by covering the best practices for Cisco wireless networks.

"Do I Know This Already?" Quiz

The purpose of this assessment quiz is to help you determine how to spend your limited study time.

If you can answer most or all of these questions, you might want to skim the "Foundation Topics" section and return to it later, as necessary. Review the "Foundation Summary" section and answer the questions at the end of the chapter to ensure that you have a strong grasp of the material covered.

If you already intend to read the entire chapter, you do not necessarily need to answer these questions now. If you find these assessment questions difficult, read through the entire "Foundation Topics" section and review it until you feel comfortable with your ability to answer all of these questions and the "Q & A" questions at the end of the chapter.

Answers to these questions can be found in Appendix A, "Answers to Quiz Questions."

1. Which layer of the OSI model is responsible for converting frames into bits and bits into frames?
   a. Physical
   b. Network
   c. Transport
   d. LLC sublayer
   e. Data link
2. Routing occurs at what layer of the OSI model?
   a. Physical
   b. Network
   c. Transport
   d. LLC sublayer
   e. Data link

3. Bridging occurs at what layer of the OSI model?
   a. Physical
   b. Network
   c. Transport
   d. Data link
4. Which of the following is *not* part of the OSI model?
   a. Network layer
   b. Physical layer
   c. Operational layer
   d. Application layer
5. IP operates at what layer of the OSI model?
   a. Layer 1
   b. Layer 2
   c. Layer 3
   d. Layer 4
   e. Layer 5
   f. Layer 6
   g. Layer 7
6. On which layer of the OSI model is data commonly referred to as segments?
   a. Layer 4
   b. Layer 3
   c. Layer 2
   d. Layer 1
7. On which layer of the OSI model is data commonly referred to as packets?
   a. Layer 1
   b. Layer 2
   c. Layer 4
   d. Layer 3

8. Which layer of the OSI model transmits raw bits?
   a. Layer 1
   b. Layer 2
   c. Layer 3
   d. Layer 4
9. Which of the following protocols is *not* routable?
   a. IP
   b. IPX
   c. NetBEUI
   d. NetBIOS
10. Which of the following is *not* a required step to enable Fast EtherChannel (FEC)?
   a. Ensure that all ports share the same speed at 10 Mbps.
   b. Ensure that all ports share the same parameter such as speed.
   c. Ensure that all ports operate at 100 Mbps.
   d. Ensure eight ports are selected to be bundled into a logical link or trunk.
11. How is Fast EtherChannel best defined?
   a. A bundle of 10-Mbps ports on a switch
   b. Another name for half-duplex 100 Mbps
   c. Not available on Cisco Catalyst switches
   d. The ability to bundle 100-Mbps ports into a logical link
   e. Only supported with Gigabit ports
12. On what OSI layer does bridging occur?
   a. Layer 1
   b. Layer 2
   c. Layer 3
   d. Both Layer 1 and 2
13. In the spanning tree protocol, what is a BPDU?
   a. A break protocol data unit
   b. A routable frame
   c. A bridge protocol data unit
   d. A frame sent out by end stations

14. An incoming frame on a Layer 2 switch is received on port 10/1 on a Catalyst 5000. If the destination address is known through port 10/2, what happens?

- **a.** The frame is discarded.
- **b.** The frame is sent via port 10/2.
- **c.** The frame is broadcast to all ports on the switch.
- **d.** The frame is sent back via 10/1.
- **e.** None of these.

15. Which of the following are the four possible states of spanning tree?

- **a.** Listening, learning, blocking, broadcasting
- **b.** Listening, learning, blocking, connecting
- **c.** Discovering, learning, blocking, connecting
- **d.** Listening, learning, blocking, forwarding

16. How many bits make up an IP address?

- **a.** 64 bits
- **b.** 48 bits
- **c.** 32 bits
- **d.** 24 bits
- **e.** 8 bits

17. Identify the broadcast address for the subnet 131.108.1.0/24.

- **a.** 131.108.1.1
- **b.** 131.108.1.254
- **c.** 131.108.1.255
- **d.** 131.108.1.2
- **e.** More data required

18. Convert the address 131.1.1.1/24 to binary:

- **a.** 10000011.1.1.1
- **b.** 10000011.00000010.1.1
- **c.** 10000011.1.1.01010101
- **d.** 10000011.1.1.11111111

19. How many subnets are possible in VLSM if the Class C address 131.108.255.0 is used with the subnet mask 255.255.255.252 in the fourth octet field? (Allow for subnet zero.)

- **a.** None
- **b.** 100
- **c.** 255
- **d.** 254
- **e.** 253
- **f.** 252
- **g.** 66
- **h.** 64

20. How many hosts are available when a /26 subnet mask is used?

- **a.** 254
- **b.** 62
- **c.** 64
- **d.** 126

21. How many hosts are available in a Class C or /24 network?

- **a.** 255
- **b.** 254
- **c.** 253
- **d.** 0
- **e.** More data required

22. You require an IP network to support, at most, 62 hosts. What subnet mask will accomplish this requirement?

- **a.** 255.255.255.255
- **b.** 255.255.255.252
- **c.** 255.255.255.224
- **d.** 255.255.255.192
- **e.** 255.255.255.240

23. Which of the following are multicast addresses? (Choose all that apply.)

- **a.** 224.0.0.5
- **b.** 2240.0.6
- **c.** 221.0.0.5
- **d.** 192.1.1.1
- **e.** 131.108.1.1

24. Which of the following routing protocols does *not* support VLSM?

- **a.** RIPv1
- **b.** RIPv2
- **c.** OSPF
- **d.** EIGRP
- **e.** BGP

25. What is the source TCP port number when a Telnet session is created by a PC to a Cisco router?

- **a.** 23
- **b.** A value higher than 1024
- **c.** 21
- **d.** 20
- **e.** 69

26. What best describes the ARP process?

- **a.** DNS resolution
- **b.** Mapping an IP address to a MAC address
- **c.** Mapping a next-hop address to the outbound interface on a Cisco router
- **d.** Both a and b

27. If two Cisco routers are configured for HSRP and one router has a default priority of 100 and the other 99, which router assumes the role of active router?

- **a.** The default priority cannot be 100.
- **b.** The router with a higher priority.
- **c.** The router with the lowest priority.
- **d.** Neither router because Cisco routers do not support HSRP; only clients do.

28. A Cisco router has the following route table:

```
R1#show ip route
     131.108.0.0/16 is variably subnetted, 17 subnets, 2 masks
C       131.108.255.0/24 is directly connected, Serial0/0
C       131.108.250.0/24 is directly connected, Serial0/1
O       131.108.254.0/24 [110/391] via 131.108.255.6, 03:33:03, Serial0/1
                         [110/391] via 131.108.255.2, 03:33:03, Serial0/0
R       131.108.254.0/24 [120/1] via 131.108.255.6, 03:33:03, Serial1/0
                         [120/1] via 131.108.255.2, 03:33:03, Serial1/1
```

What is the preferred path to 131.108.254.0/24? (Choose the best two answers.)

a. Via Serial0/0

b. Via Serial0/1

c. None

d. To null0

29. IP RIP runs over what TCP port number?

a. 23

b. 21

c. 69

d. 520

e. None of these

30. IP RIP runs over what UDP port number?

a. 23

b. 21

c. 69

d. 520

31. An OSPF virtual link should _____.

a. never be used

b. allow nonpartitioned areas access to the backbone

c. allow partitioned areas access to the backbone

d. not be used in OSPF, but rather in ISDN

32. What is the BGP version most widely used today?

- **a.** 1
- **b.** 2
- **c.** 3
- **d.** 4
- **e.** 5
- **f.** 6

33. What is the destination port number used in a Telnet session?

- **a.** 23
- **b.** 69
- **c.** 21
- **d.** 161

34. In what field, or fields, does the IP checksum calculate the checksum value?

- **a.** Data only
- **b.** Header and data
- **c.** Header only
- **d.** Not used in an IP packet

35. The TCP header checksum ensures integrity of what data in the TCP segment?

- **a.** The data only.
- **b.** The header only.
- **c.** The data and header.
- **d.** There are no TCP header checksums; IP covers the calculation.

36. ISDN BRI channels are made up of what?

- **a.** 1×64-kbps channel and one D channel at 64 kbps
- **b.** 2×64-kbps channels and one D channel at 64 kbps
- **c.** 2×64-kbps channels and one D channel at 16 kbps
- **d.** 32×64-kbps channels and one D channel at 16 kbps

37. What services can ISDN carry?

- **a.** Data only
- **b.** Data and voice only
- **c.** Voice and video
- **d.** Data, voice, and video

38. Place the following steps in the correct order for PPP callback, as specified in RFC 1570.

1. A PC user (client) connects to the Cisco access server.
2. The Cisco IOS Software validates callback rules for this user/line and disconnects the caller for callback.
3. PPP authentication is performed.
4. Callback process is negotiated in the PPP Link Control Protocol (LCP) phase.
5. The Cisco access server dials the client.

a. 1, 2, 3, 4, 5

b. 1, 3, 2, 5, 4

c. 1, 4, 5, 3, 2

d. 1, 5, 4, 3, 2

39. What hardware port is typically designed to connect a Cisco router for modem access?

a. The console port

b. The vty lines

c. The auxiliary port

d. The power switch

e. The Ethernet interface

40. The AS5300 series router can support which of the following incoming connections?

a. Voice

b. Dialup users via PSTN

c. ISDN

d. All of these

41. Which of the following routing protocols are protected by an authentication mechanism?

a. OSPF

b. RIPv2

c. RIPv1

d. EIGRP

e. IGRP

f. EBGP

g. IBGP

h. BGP

42. What UDP port range is used between Cisco IP Phones when a call is in progress?

- **a.** 67–68
- **b.** 80–80
- **c.** 2748–3748
- **d.** 16384–32766
- **e.** 16384–32767
- **f.** None; TCP is used

43. What two methods are commonly used to secure Voice over IP? (Choose two answers.)

- **a.** Access lists
- **b.** IDSs
- **c.** Enable passwords
- **d.** Deny HTTP access to the CCM

44. Which of the following can be used by attackers to gain access to WLANs? (Select three answers.)

- **a.** Call the TAC
- **b.** Audit the MAC address
- **c.** Detect the SSID
- **d.** Exploit flaws in the operating system
- **e.** Use a sniffer tool with a wireless adapter

45. Which of the following is *not* a method used to secure a wireless network? (Select the best three answers.)

- **a.** Deploy WEP with a static key only
- **b.** Deploy mutual client-to-server authentication, such as RADIUS?
- **c.** Use dynamic key management
- **d.** Disable MAC authentication
- **e.** Nothing, wireless is inherently secure

Foundation Topics

Networking Basics—The OSI Reference Model

This section covers the Open System Interconnection (OSI) seven-layer reference model and common examples of each Individual OSI layer. CCIE candidates must fully understand and appreciate the OSI model, because almost every routed protocol in use today is based on its architecture. The OSI model was developed by a standards body called the International Organization for Standardization (ISO) to provide software developers with a standard architecture to develop protocols (such as IP). For example, the OSI model allows a PC to communicate with a UNIX device.

NOTE ISO developed the OSI reference model in 1984. Layers 1 and 2 are implemented in hardware and Layers 3 through 7 are typically implemented in software. Layer 2 is broken up into two smaller sublayers: the software-based LLC sublayer and the hardware-based MAC sublayer.

Table 1-1 displays the seven layers of the OSI model.

Table 1-1 *OSI Seven-Layer Model*

Layer Name	Layer Number
Application	Layer 7
Presentation	Layer 6
Session	Layer 5
Transport	Layer 4
Network	Layer 3
Data link	Layer 2
Physical	Layer 1

The following sections cover each layer and provide protocol examples for each.

Layer 1: The Physical Layer

The physical layer consists of standards that describe bit ordering, bit transmission rates, connector types, and electrical and other specifications. Information at Layer 1 is transmitted in

binary (1s and 0s). For example, the letter *A* is transmitted (in hex) as 00001010. Examples of physical layer standards include the following:

- RS-232
- V.24
- V.35
- RJ-45
- RJ-12

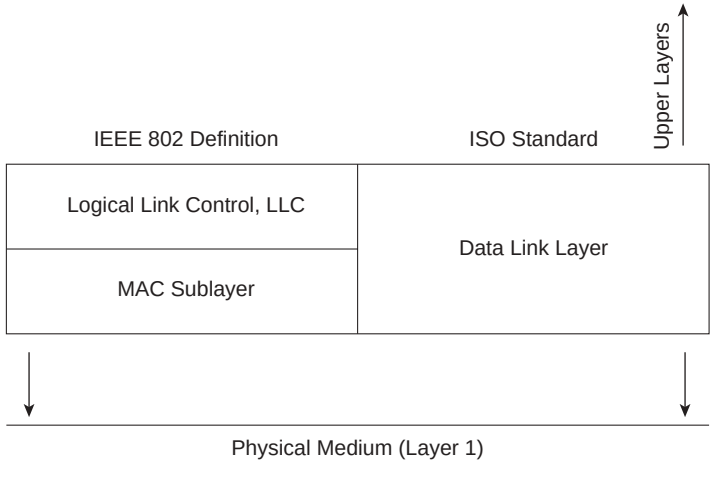
Layer 2: The Data Link Layer

The data link layer focuses on reliably getting data across any particular kind of link. Flow control and error notifications are also functions of the data link layer. The data link layer applies to all access methods, whether they are LAN or WAN methods. Information processed at this layer is commonly known as frames.

The IEEE further complicated matters by subdividing the data link layer into two sublayers: the Logical Link Control (LLC) sublayer and the MAC sublayer.

Figure 1-1 displays the IEEE definition compared to the ISO definition.

Figure 1-1 *IEEE Sublayers Versus ISO Definitions*



The LLC sublayer manages and ensures communication between end devices, and the MAC sublayer manages protocol access to the physical layer.

Examples of data link layer frame types include the following:

- Integrated Services Digital Network (ISDN)
- Synchronous Data Link Control (SDLC)
- High-Level Data Link Control (HDLC)
- Point-to-Point Protocol (PPP)
- Frame Relay
- Ethernet version 2
- Bridge protocol data units (BPDUs) in the Spanning Tree Protocol (STP)

Layer 3: The Network Layer

The network layer determines the best path to a destination. Device addressing, packet fragmentation, and routing all occur at the network layer. Information at this layer is processed in what are commonly known as packets. Examples of network layer protocols include the following:

- Internet Protocol (IP)
- Internetwork Packet Exchange (IPX)

Routing protocols, such as Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), and Border Gateway Protocol (BGP), provide the information required to determine the topology of the internetwork and the best path to a remote destination. A routed protocol is one that is transported by a routing protocol (such as Routing Information Protocol [RIP]). For example, IP is a routed protocol that can be advertised by a number of routing algorithms, such as RIP, OSPF, and BGP. The Layer-3 field format of protocol type defines to the higher layers what protocol is being carried inside the IP packet. For example, OSPF has an IP protocol number of 89; EIGRP has an IP protocol number of 88. Technically, OSPF and EIGRP are not Layer-3 mechanisms.

NOTE Layer 3 protocols, such as IP, are commonly referred to as connectionless protocols, whereas Layer 4 protocols, such as TCP, are commonly referred to as connection-oriented protocols.

A connection-oriented protocol, such as TCP, ensures delivery of all information, whereas a connectionless protocol, such as IP, packages the data but sends it without guaranteeing delivery. Connection-oriented protocols exchange control information (also called Handshake) before transmitting data. A telephone call can be considered a connection-oriented service because the call is established before conversation can take place, much the same way that TCP sets up a data connection before data is sent. FTP is another example of a connection-oriented protocol.

Layer 4: The Transport Layer

The transport layer is responsible for segmenting upper-layer applications and establishing end-to-end connections between devices. Other transport layer functions include providing data reliability and error-free delivery mechanisms. Information at this layer is processed in what are commonly known as segments. Examples of transport layer protocols include the following:

- Transmission Control Protocol (TCP)
- Real-Time transport protocol (RTP)
- User Datagram Protocol (UDP)

RTP has some important properties of a transport Layer-4 protocol; however, it also runs on end systems. RTP differs from transport protocols like TCP in that it (currently) does not offer any form of reliability or a protocol-defined flow/congestion control. IP voice is an example of RTP operating at Layer 4 of the OSI model.

Layer 5: The Session Layer

The session layer performs several major functions, including managing sessions between devices and establishing and maintaining sessions. Examples of session layer protocols include the following:

- Database SQL
- NetBIOS Name Queries
- H.323 (supports video as well; it is the packet-switched voice standard)
- Real-Time Control Protocol (RTCP)

Layer 6: The Presentation Layer

The presentation layer handles data formats and code formatting. The layer's functions are normally transparent to the end user because this layer takes care of code formats and presents them to the application layer (Layer 7), where the end user can examine the data. Examples of presentation layer protocols include the following:

- Graphics Interchange Format (GIF)
- Joint Photographic Experts Group (JPEG)
- American Standard Code for Information Interchange (ASCII)
- Moving Picture Experts Group (MPEG)

- Tagged Image File Format (TIFF)
- Musical Instrument Digital Interface (MIDI)
- Hypertext Markup Language (HTML)

Layer 7: The Application Layer

The application layer is closest to the end user, which means that the application will be accessed by the end user. This layer's major function is to provide services to end users. Examples of application layer services include the following:

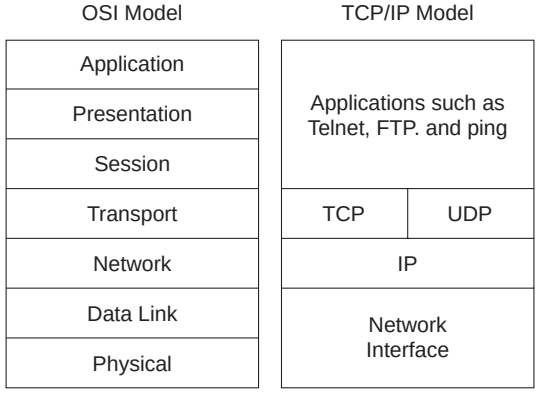
- File Transfer Protocol (FTP)
- Telnet
- Ping
- Trace route
- Simple Mail Transfer Protocol (SMTP)
- Mail clients

TCP/IP and OSI Model Comparison

TCP/IP is the most widely used networking protocol and is often compared to the industry-defined OSI model.

Figure 1-2 displays the TCP/IP model in relation to the OSI model and shows where the protocol suite of TCP/IP lines up with the ISO standard. This comparison is provided to demonstrate that TCP/IP does not conform exactly to the OSI model. For example, the TCP/IP model has no Layer 5 or 6.

Figure 1-2 *OSI and TCP/IP Models*

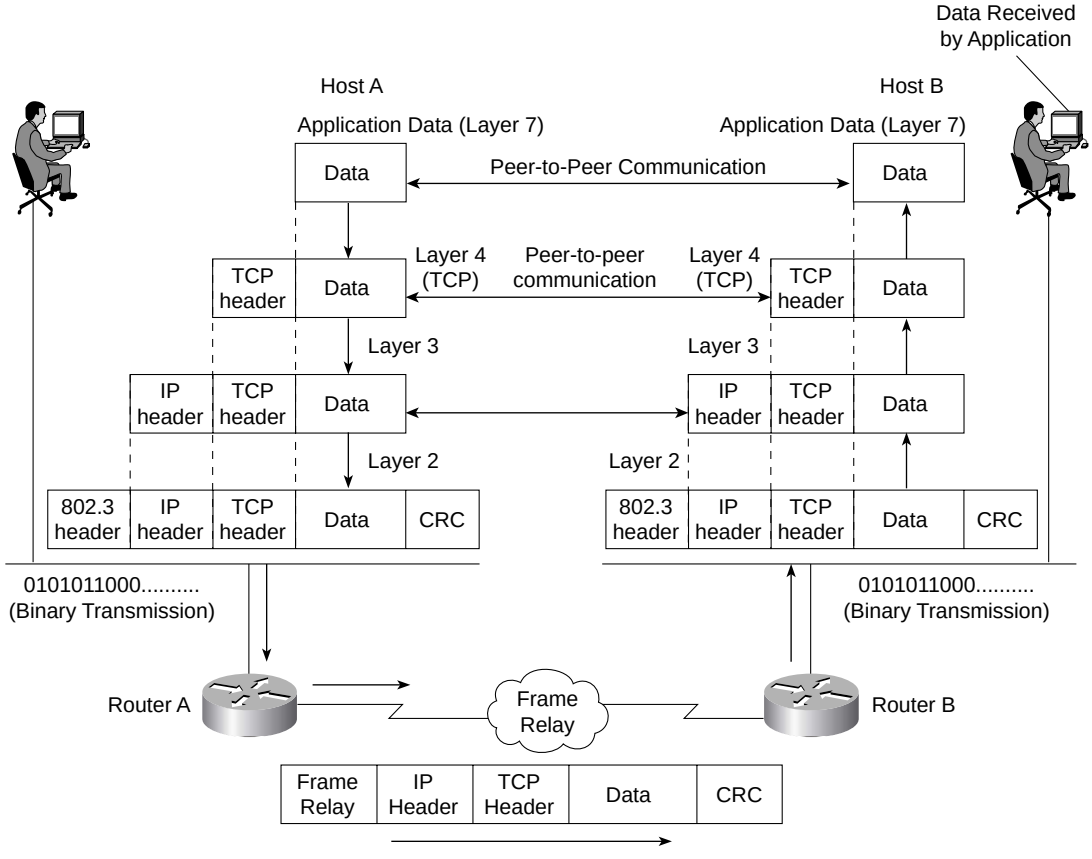


Example of Peer-to-Peer Communication

Each layer of the OSI or TCP model has its own functions and interacts with the layer above it and layer below it. Furthermore, the communication between each layer's end devices also establishes peer-to-peer communication; this means that each layer of the OSI model communicates with the corresponding peer. For example, Layer 3 of Host A in Figure 1-3 will communicate with the corresponding Layer 3 (IP) device host B.

Consider the normal communication that occurs between two IP hosts over a WAN running Frame Relay, as displayed in Figure 1-3.

Figure 1-3 *Peer-to-Peer Communication Example*



The data from Host A is encapsulated inside a TCP header and passed down to Layer 3 (the IP layer) for address configuration, where an IP header is also added. Information included here is the source IP address and destination address. Layer 3 (the network layer) passes the data to the local router acting as the gateway via the Ethernet connection in raw binary.

Router A strips the 802.3 header and encapsulates the IP, TCP, and data in a Frame Relay packet for delivery over the WAN. A CRC is added here to ensure the packet is not corrupted over the WAN. Because Frame Relay is connectionless, if an error occurs, it's up to the upper layers to retransmit; Frame Relay will not retransmit the packet. Similarly, HDLC (Layer 2 protocol) is connectionless and depends on upper layers to resubmit damaged data packets. PPP (connection-oriented), on the other hand, resubmits packets damaged in transmission over the WAN.

Router B receives the Layer 2 frames, strips the Frame Relay header/CRC, and encapsulates the IP, TCP, and data frame back into an 802.3 header (with its own CRC, Ethernet checks only for errors and cannot repair them; once more, upper layers, such as TCP, ensure data delivery) for binary transmission across the Ethernet to Host B. The data is passed up the layers through IP, TCP, and finally to the application, where the application layer reads and acts upon the data.

The good news for security candidates is that Token Ring and legacy technologies are not covered in the written exam, so this chapter concentrates only on Ethernet switching. Before covering switching, the next section summarizes the evolution of Ethernet so that you are aware of the standards that have developed since Xerox Corporation first introduced Ethernet.

Ethernet Overview

Ethernet networks are based on a development made by Xerox, Digital Equipment Corporation, and Intel Corporation. The two versions of Ethernet are commonly referred to as Ethernet I and Ethernet II (or version 2).

Ethernet uses carrier sense multiple access collision detection (CSMA/CD) to transmit frames on the wire. In an Ethernet environment, all hosts can transmit as long as no other devices are transmitting. CSMA/CD is used to detect and warn other devices of any collisions, and colliding stations use a backoff algorithm and wait a random amount of time before trying again. Colliding devices send a jam signal to advise all stations that a collision has occurred. When a jam signal is sent (a jam signal is detected by all devices, because the voltage is that of the combined colliding devices), all stations also stop transmitting. A device attempts to transmit up to 16 times before a user is notified of the collisions; typically, an application error informs the user that data could not be delivered. Microsoft's famous words are "Network is busy."

NOTE The only situation in which CSMA/CD is not used is in a full-duplex connection, because collisions are not possible when one pair of unshielded twisted-pair cable (UTP, the physical cable connection) is used to transmit data (one pair of twisted-pair cable) and receive data (a second pair of twisted-pair cable). In other words, devices connected in full-duplex mode can send and receive data at the same time without the possibility of collision.

Table 1-2 lists some of the common Ethernet media specifications and the characteristics of each.

Table 1-2 *Ethernet Media Formats*

Media Type	Characteristics
10BASE5*	Maximum length: 500 m Maximum stations: 1024 Speed: 10 Mbps Minimum distance between devices: 2.5 m
10BASE2	Maximum length: 185 m, using RG58 cable types and T connectors on all end stations Minimum distance between devices: 0.5 m Maximum devices per 185-m segment: 30 stations Speed: 10 Mbps
10BASE-T	Based on UTP cabling Up to 100 m; better-category cables longer One device per cable; typically, only one device per segment with hubs or switches connecting all devices together Speed: 10 Mbps Physical topology: star Logical topology: bus
100BASE-T	Same characteristics as 10BASE-T but operates faster, at 100 Mbps Can be fiber, as well (100BASE-FX); defined in IEEE 802.3U Physical topology: star Logical topology: bus
1000 GE	Gigabit Ethernet operating at 1000 Mbps Can run over fiber or UTP; frame formats and CSMA/CD identical to Ethernet standards Physical topology: star Logical topology: bus

*The word BASE refers to baseband signaling, which uses a single channel, as opposed to broadband, which uses multiple frequency channels.

Switching and Bridging

This section covers Layer 2 devices that are used to bridge, or switch, frames using common techniques to improve network utilization, such as VLANs. The terms *switch* and *bridge* are used to refer to the same technology.

Switching, or bridging, is defined as a process of taking an incoming frame from one interface and delivering it through another interface. Source stations are discovered and placed in a switch address table (called a content-addressable memory [CAM] table in Cisco terms). Routers use Layer 3 switching to route packets, and Layer 2 switches use Layer 2 switching to forward frames.

Switches build CAM tables when activity is noted on switch ports. Example 1-1 displays a sample CAM table on a Cisco Catalyst 5000 switch.

Example 1-1 *CAM Table or Bridge Table*

```
CAT5513 (enable) show cam ?
Usage: show cam [count] <dynamic|static|permanent|system> [vlan]
       show cam <dynamic|static|permanent|system> <mod_num/port_num>
       show cam <mac_addr> [vlan]
       show cam agingtime
       show cam mlsrp <ip_addr> [vlan]
CAT5513 (enable) show cam dynamic
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry. X = P
ort Security Entry

VLAN  Dest MAC/Route Des  Destination Ports or VCs / [Protocol Type]
----  ------------------  -----------------------------------------------------
36    00-10-7b-54-37-c6   8/13 [ALL]
35    00-09-43-3b-ac-20   8/5 [ALL]
101   00-01-02-00-4a-ff   1/1 [ALL]
1     00-01-02-00-4a-ff   1/1 [ALL]
102   00-03-e3-5e-ac-81   1/1 [ALL]
101   00-00-0c-92-0c-af   1/1 [ALL]
102   00-03-e3-53-7f-81   1/1 [ALL]
102   00-03-e3-5e-ae-c1   1/1 [ALL]
37    00-03-e3-63-55-80   8/9 [ALL]
102   00-03-e3-5e-a9-01   1/1 [ALL]
```

Example 1-1 displays a CAM table on a Catalyst switch with the CatOS command **show cam dynamic**. You can use other CatOS commands to view specific ports (**show cam dynamic 8/13** would show only devices discovered on port 8/13). Example 1-1 displays that the MAC address 01-10-7b-54-37-c6 is located via the port 8/13.

NOTE The examples in this chapter display the traditional Cisco CatOS operating system. The CCIE Security exams test on both Cisco CatOS and Cisco IOS. Chapter 8, "CCIE Security Self-Study Lab," displays CAM tables of the newest form of Cisco IOS–based switches so that you have exposure to both operating systems.

A Cisco switch populates the CAM tables as new devices send frames, so a switch bases all bridging decisions on the source MAC address. When a device first sends a frame to a connected port on a switch, the switch adds the incoming source address to the CAM table. Any broadcasts (packets sent by a host that are destined for all hosts in the same broadcast domain) received because the switch has no CAM entry are sent out all ports except the port the frame was received on. The switch then adds the source MAC address on the source port. Frames that are received as broadcasts are sent out all ports active in spanning tree.

NOTE Transparent bridges can operate in two traditional modes. *Cut-through switching* occurs when, after the destination MAC address is received, the switch immediately forwards the frame to the outgoing port. If a switch in cut-through mode encounters a large number of frames with CRCs, it drops down to store-and-forward mode. This technique is known as *adaptive cut-through*. *Store-and-forward switching* occurs when the entire frame is received before forwarding the frame. The CRC is checked to ensure that frames containing errors or CRCs are not forwarded. Although cut-through switching is faster, the switch could potentially forward frames with errors, because the CRC is not checked. The default mode is typically store-and-forward on Cisco switches. Routers can also be configured to bridge packets. The most common form of switching is adaptive cut-through.

Spanning tree is a Layer 2 protocol used to ensure a loop-free topology. A Layer 2 loop is devastating to a network, because a frame circulates (meaning frames are not dropped by intelligent Layer 2 devices) the entire broadcast domain until all the switches eventually run out of memory because of the intensive broadcast storm that occurs. Broadcasts must be forwarded to all ports except the source port.

NOTE A *broadcast domain* is defined as a group of all devices that receive broadcast frames originating from any device within the group. Broadcast domains are typically bound by routers, because routers do not forward broadcast frames. Switches, on the other hand, must forward all broadcasts out all ports except the port the frame was received from.

Spanning tree is used when there are multiple LAN segments or VLANs. A VLAN is a defined group of devices on one or more LANs that are configured (using management software, such as Catalyst switch code or CatOS) to communicate as if they were attached to the same wire when,

in fact, they are located on a number of different LAN segments. VLANs are based on logical instead of physical connections and must be connected to a Layer 3 device, such as a router, to allow communication between all segments or VLANs.

To create a VLAN on a Catalyst switch, the CatOS command is **set vlan** *vlan-id* (where *vlan-id* is a number between 2 and 1005). By default, Cisco switches have VLAN 1 already configured. Previously, VLAN 1 could not be removed for management purposes, but in the newest versions of operating system software, you can disable it for security reasons. Cisco IOS–based switches now extend VLAN coverage from 1-1005 to the extended ranges of 1025-4094. You can disable Cisco Discovery Protocol (CDP) and spanning tree (not recommended in large switches networks).

Spanning tree is on by default on all Catalyst switches, and before data can be received or sent on any given port, STP goes through a root bridge election phase. A root bridge election takes into account the bridge priority (value between 0 and 65535, default is 32768), and a lower priority is better. If the bridge priority is equal in a segment with multiple bridges, the lowest MAC address associated with the bridge is elected as the root bridge.

Bridges communicate using frames called bridge protocol data units (BPDUs). BPDUs are sent out all ports that are not in a blocking state. A root bridge has all ports in a forwarding state. To ensure a loop-free topology, nonroot bridges block any paths to the root that are not required. BPDUs use the destination MAC address 01-08-C2-00-00-00 in Ethernet environments.

Bridge Port States

Every bridge and associated port is in one of the following spanning tree states:

- **Disabled**—The port is not participating in spanning tree and is not active.
- **Listening**—The port has received data from the interface and will listen for frames. The bridge only receives data; it does not forward any frames to the interface or to other ports.
- **Learning**—The bridge still discards incoming frames. The source address associated with the port is added to the CAM table. BPDUs are sent and received.
- **Forwarding**—The port is fully operational; frames are sent and received.
- **Blocking**—The port has been through the learning and listening states, and because this particular port is a dual path to the root bridge, the port is blocked to maintain a loop-free topology.

In some situations, you do not want spanning tree to go through the preceding steps (listening, learning, and forward/blocking, which can take up to 45 seconds) but rather to immediately enter a forwarding state. For example, a PC with a fast processor connected to a switch does not need

to test for any BPDUs (PCs do not run spanning tree), and the port on the Ethernet switch should enter a forwarding state to allow the PC immediate connectivity. This feature is known as *portfast* on Cisco switches. To enable portfast, use the Catalyst command **set spantree** *spantree-number* **portfast** *interface* **enable**.

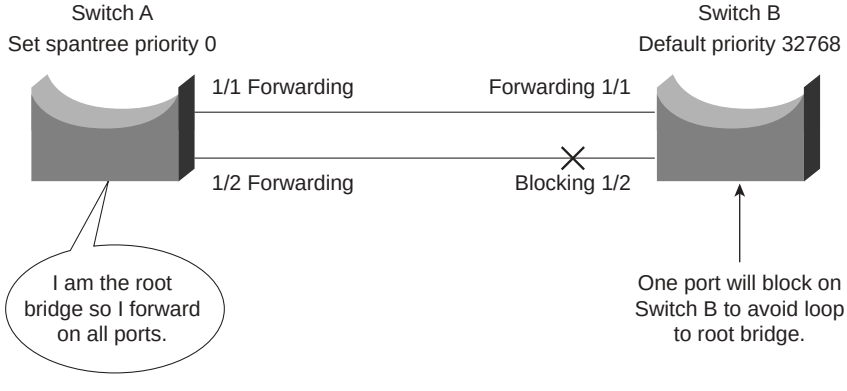
NOTE Concurrent routing and bridging/integrated routing and bridging, routing information fields, source-route bridging, and source-route translational bridging are not covered in the CCIE Security written exam, and they are not part of the blueprint.

Fast EtherChannel

Fast EtherChannel (FEC) is a Cisco method that bundles 100-Mbps Fast Ethernet ports into a logical link. The existence of any redundant paths between two switches results in some ports being in a blocking state, thus reducing available bandwidth.

Figure 1-4 displays a switched network with two 100-Mbps connections between them. Because of STP, one of the links (Switch A, in this case) will be in a blocking state after the election of a root bridge. Switch B will block one of the paths to ensure that only one path exists to the root bridge (Switch A). To purchase and enable a Fast Ethernet port is expensive, and to have it sitting in an idle position means wasted resources, so Cisco developed a method that enables Fast Ethernet ports to be bundled together and used concurrently (in other words, cheating spanning tree into believing that the two ports are one to send data from Switch A to Switch B with two 100-Mbps links instead of one).

Figure 1-4 *Spanning Tree Loop Avoidance*



To enable Fast EtherChannel, follow these steps:

Step 1 Set to the same speed all ports that are part of FEC.

Step 2 Configure all ports so that they belong to the same VLAN.

Step 3 Set duplex to be the same, either half or full, not a mixture.

Step 4 Bundle up to eight ports together.

Step 5 To set Fast EtherChannel on a switch, use the CatOS syntax **set port channel**.

Step 6 To set Fast EtherChannel on a router, use the Cisco IOS syntax **channel-group** under the Fast Ethernet interface.

Step 7 Configure up to four FEC groups per switch. This limit could change with future Catalyst releases.

For Cisco IOS–based switches, fewer steps are required.

Step 1 Create the port-channel interface. The number can be from 1 to 64 (256 with Release 12.1(2)E and earlier).

```
Router(config)# interface port-channel port_channel_number
```

Step 2 Assign an IP address and subnet mask to the EtherChannel.

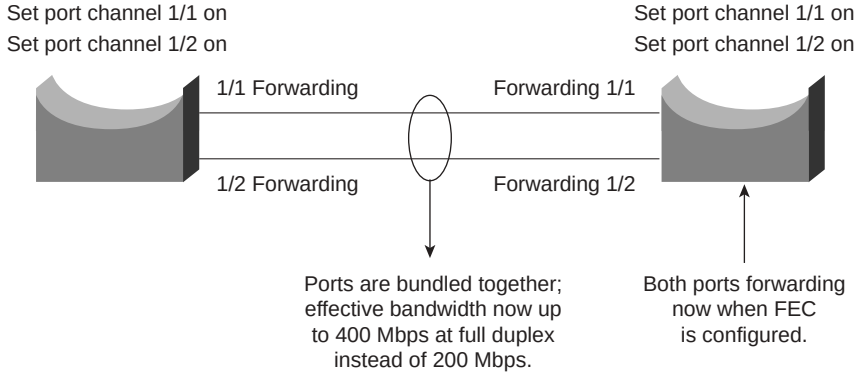
```
Router(config-if)# ip address ip_address mask
```

NOTE A group of bundled ports running FEC is commonly known as a *trunk*. In switching terms, a trunk is a physical and logical connection between two switches. A trunk, for example, can carry multiple VLANs.

Inter-Switch Link (ISL) is a Cisco proprietary protocol that maintains VLAN information as traffic flows between switches and routers. ISL allows members of one VLAN to be located on any given switch. 802.1Q is an IEEE standard for trunking. You can use IEEE 802.1q in a multivendor environment. Be aware that not all Cisco switches support ISL encapsulation. For example, the 2850 only supports 802.1q.

Figure 1-5 displays the logical link when FEC is enabled between Switch A and Switch B.

Figure 1-5 *FEC: Logical Link or Trunk-Enabled*



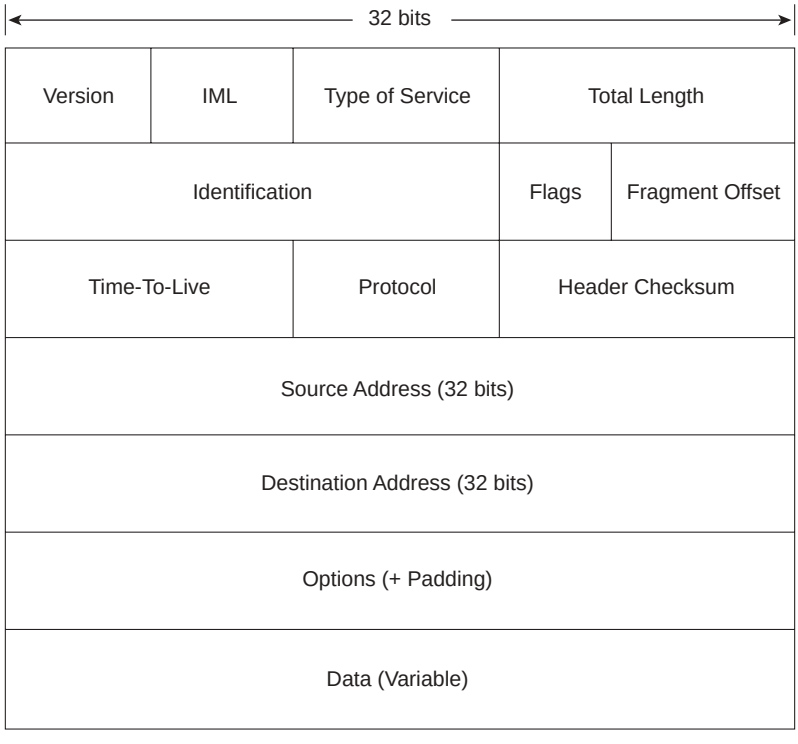
Internet Protocol

Internet Protocol (IP) is a widely used networking term that describes a network layer protocol that logically defines a distinct host or end system, such as a PC or router, with an IP address.

An IP address is configured on end systems to allow communication between hosts over wide geographic locations. An IP address is 32 bits in length, with the network mask or subnet mask (also 32 bits in length) defining the host and subnet portion.

Figure 1-6 displays the IP packet header frame format in detail.

Figure 1-6 *IP Frame Format*



The following describes the IP packet fields illustrated in Figure 1-6:

- **Version**—Indicates the version of IP currently used. IPv4 is the most widely used version. IPv6 is also available. This version is not tested in the CCIE Security written exam yet, but will most likely be included in the future.
- **IP Header Length (IHL)**—Indicates the datagram header length in 32-bit words.

- **Type-of-Service (ToS)**—Specifies how an upper-layer protocol wants current datagrams to be handled and assigns to datagrams various levels of importance. The ToS field (8 bits) defines the first 3 bits for precedence, of which there are eight possible values:
  - 000—Routine delivery
  - 001—Priority
  - 010—Immediate
  - 011—Flash
  - 100—Flash override
  - 101—Critical
  - 110—Internetwork control
  - 111—Network control

  Typically, IP packets are set with the value 000. The remaining 5 bits in the ToS are defined as follows:
  - Bit 3—D bit defines normal or low delay.
  - Bit 4—T bit defines normal or high throughput.
  - Bit 5—R bit defines normal or high reliability.
  - Bits 6 and 7—Not in current use.
- **Total Length**—Specifies the entire packet's length in bytes, including the data and header. The mathematically defined limit is calculated as 65,535 bytes (2^{16}–1).
- **Identification**—Contains an integer that identifies the current datagram. This field helps piece together datagram fragments (16 bits in length).
- **Flags**—Consists of a 3-bit field of which the two low-order (least-significant) bits control fragmentation. The low-order bit specifies whether the packet can be fragmented. The middle bit specifies whether the packet is the last fragment in a series of fragmented packets. The third, or high-order, bit is not used.
- **Fragment Offset**—Indicates the position of the fragment's data relative to the beginning of the data in the original datagram, which allows the destination IP process to properly reconstruct the original datagram.
- **Time-to-Live**—Maintains a counter that gradually decrements to 0, at which point the datagram is discarded. This keeps packets from looping endlessly.

- **Protocol**—Indicates which upper-layer protocol receives incoming packets after IP processing is complete. For TCP, this value is 6; for GRE, it is 47; for ICMP, it is 1; for OSPF, it is 89; for UDP, it is 17; for ESP, it is 50; and for AH, it is 51. These are common uses in today's networks. Visit http://www.iana.org/assignments/protocol-numbers for a comprehensive list.
- **Header Checksum**—Helps ensure only IP header integrity and not the data field.
- **Source Address**—Specifies the sending node (32 bits).
- **Destination Address**—Specifies the receiving node (32 bits).
- **Options**—Allows IP to support various options, such as security. The Options field varies in length. Some options are Security, Loose Source Routing, Strict Source Routing, Record Route, and Timestamp.
- **Data**—Contains upper-layer information.

NOTE A subnet is a network that is segmented by network administrators, allowing a hierarchical routing topology. Subnetting allows great use of IP address space using binary bits from the subnet mask. Examples of subnets appear later in this chapter.

Routing allows communication between these subnets. The host address is a logical, unique address that resides on a subnet.

The Internet Engineering Task Force (IETF) standards body, which consists of more than 80 working groups responsible for developing Internet standards, has defined five address classes and the appropriate address ranges. Table 1-3 displays the five ranges.

Table 1-3 *Class A, B, C, D, and E Ranges**

Class of Address	Starting Bit Pattern	Range	Default Subnet Mask
Class A	0xxxxxxx	1–126, 127**	255.0.0.0
Class B	10xxxxxx	128–191	255.255.0.0
Class C	110xxxxx	192–223	255.255.255.0
Class D	1110xxxx	224–239	Not officially defined
Class E	1111xxxx	240–255	Reserved

*Only Classes A, B, and C have predefined default subnet masks.

**127.0.0.0 is reserved for loopback purposes. Other reserved addresses for private use as defined by RFC 1918 are as follows:

10.0.0.0–10.255.255.255

172.16.0.0–172.31.255.255

192.168.0.0–192.168.255.255

Soon after these ranges were defined and the Internet's popularity extended beyond the Department of Defense in the United States, it became clear that to ensure that a larger community could connect to the World Wide Web, there had to be a way to extend IP address space using subnetting. Subnetting allows an administrator to extend the boundary for any given subnet.

To understand an IP address and subnet portion, determine how many hosts are available on a particular subnet, and learn how to best use an IP address space, consider the following example.

Suppose you are given the IP address 131.108.1.56 and the subnet mask is 255.255.255.0.

You can deduce the subnet for any IP address by performing a logical AND operation for the IP address along with the subnet mask. A logical AND operation follows two basic rules: positive and positive equal positive, and negative and either positive or negative equal negative. In binary (positive is 1 and negative is 0), 0 AND 0 is 0, 0 AND 1 is 0, 1 AND 1 is 1, and 1 AND 0 is 0.

Figure 1-7 displays the logical AND operation used to determine the subnet address.

Figure 1-7 *Logical AND Operation*

IP Address (131.108.1.56)	10000011	11001100	00000001	00111000
IP Subnet Mask (255.255.255.0)	11111111	11111111	11111111	00000000
Logical AND	10000011	11001100	00000001	00000000
In Decimal	131	108	1	0

The result of the logical AND operation reveals that the subnet address is 131.108.1.0. The subnet address is reserved and cannot be assigned to end devices.

To determine the number of hosts available in any given subnet, simply apply the formula $2^n - 2$, where n is the number of borrowed bits. This is best explained with examples. To determine the number of borrowed bits, you must examine the subnet mask in binary. For a default Class C network mask of 11111111.11111111.11111111.00000000 or, in decimal, 255.255.255.0, the last 8 bits represent the borrowed bits. For a Class C network, the number of hosts that can reside is $2^8 - 2 = 256 - 2 = 254$ hosts. You subtract two host addresses because host devices are not permitted to use the subnet address or the broadcast address. In IP, a broadcast address consists of all binary 1s. So, for this example, the broadcast address for the subnet 131.108.1.0 is 131.108.1.255 (255 in binary is 11111111).

Consider another example. Given the host address 171.224.10.67 and the subnet mask of 255.255.255.224, this example shows you how to determine the subnet and the number of hosts that can reside on this network.

To determine the subnet, perform a logical AND. Figure 1-8 displays the operation.

Figure 1-8 *Logical AND Operation*

IP Address (171.224.10.67)	10101011.	11100000.	00001010.	01000011
IP Subnet Mask (255.255.255.224)	11111111.	11111111.	11111111.	11100000
Logical AND	10101011.	11100000.	00001010.	01000000
In Decimal	171	224	10	64

The subnet is 171.224.10.64. The number of hosts that can reside on this network with a subnet mask of 255.255.255.224 (or 11100000) is $2^5 - 2 = 32 - 2 = 30$ hosts. You can apply this simple example to any Class A, B, or C address, and applying a subnet mask that is not the default or classful kind allows network administrators to extend IP address space and allows a larger number of devices to connect to the IP network.

Table 1-4 displays some common network subnets and the number of hosts available on those subnets.

Table 1-4 *Common Subnets in Today's Networks*

Decimal	Subnets	Hosts
252 (1111 1100)	64 subnets	2 hosts*
248 (1111 1000)	32 subnets	6 hosts
240 (1111 0000)	16 subnets	14 hosts
224 (1110 0000)	8 subnets	30 hosts
192 (1100 0000)	4 subnets	62 hosts
128 (1000 0000)	2 subnets	126 hosts

*Used commonly for point-to-point WAN circuits when no more than two hosts or routers reside. Point-to-point networks typically connect a remote router to a central router.

Variable-Length Subnet Masks

A variable-length subnet mask (VLSM) is designed to allow greater use of IP address space by borrowing bits from the subnet mask and allocating them to host devices. To allow a greater number of devices to connect to the Internet and intranets, the standards bodies of various routing protocols designed an IP routing algorithm to cater to IP networks with a different subnet mask than the default used in classful networks.

NOTE Routing algorithms that support VLSM are as follows:

- RIPv2
- OSPF
- Intermediate System-to-Intermediate System (IS-IS)
- EIGRP
- BGP version 4 (BGP4)

Additionally, Cisco IOS allows the use of any 0 subnets (for example, subnet 131.108.0.0/24) with the global Cisco IOS command, **ip subnet-zero**. This can be very useful for networks that are running out of IP address space.

To effectively use any IP address space, use the least number of subnet bits and the least number of host bits. You could use a Class C mask or a mask that allows for 254 hosts. For a WAN link that will never use more than two hosts, this is a vast amount of wasted space. Applying different masks to cater to the exact requirement means that IP address space is not wasted unnecessarily.

Apply the formula to determine the best subnet to use to cater to two hosts on any given subnet and class of address. Remember that you must subtract two host addresses for the subnet address and broadcast address.

Applying the formula, you get $2^n - 2 = 2$, or $2^n = 4$, or $n = 2$. You need to borrow only 2 bits from the subnet mask to allow for two host addresses. The subnet mask is 30 bits in length, or 255.255.255.252 in binary. This is represented as 11111111.11111111.11111111.111111100. The last 2 bits (00) are available for host addresses. The subnet is 00, the first host address is 01, the second is 10, and the broadcast address is 11.

TIP Loopback interfaces configured on Cisco routers are typically configured with a host address using a 32-bit subnet mask. This allows, for example, a Class C network with 256 (from 0–255) hosts among 256 different routers and conserves valuable IP address space.

Classless Interdomain Routing

Classless interdomain routing (CIDR) is a technique supported by BGP4 and based on route aggregation. CIDR allows routers to group routes together to reduce the quantity of routing information carried by the core Internet routers. With CIDR, several IP networks appear to networks outside the group as a single, larger entity. With CIDR, IP addresses and their subnet masks are written as four octets, separated by periods, and followed by a forward slash and a two-digit number that represents the subnet mask. CIDR representation can be either a forward slash with a one-digit number or a forward slash with a two-digit number (for example, 131.108.1/24 or 131.0.0.0/8).

In the past few years, the expansion of the Internet has been phenomenal. Currently, the Internet uses more than 100,000 routes. From 1994 through 1996, the routing table increased from approximately 20,000 entries to more than 42,000. Currently, there are over 120,000 IP routing entries. How can network administrators reduce the large routing table size? Each routing entry requires memory and a table lookup by the router each time a packet is required to reach a destination. Reducing memory requirements and the time it takes to send a packet to the destination provides faster response times for packets to travel around the Internet.

CIDR helps to reduce the number of routing table entries and memory requirements. CIDR helps conserve resources because it removes the limitation of using the default mask (which wastes IP address space) and leaves the addressing up to the IP designer. Routers use CIDR to group networks together to reduce routing table size and memory requirements. CIDR is typically represented with the network number/bits used in the mask, such as 131.108.1.0/24, or the equivalent of 131.108.1.0 255.255.255.0. BGP and classless routing protocols use CIDR to reduce routing table entries, allowing faster lookup and requiring less memory on Cisco routers, for example.

Classful and Classless Routing Protocols

Routing protocols can also be classed, or described, as classful and classless.

Classful addressing, namely Classes A, B, and C (Class D is reserved for multicasts and Class E is reserved for future use), defines a set number of binary bits for the subnet portion. For example, a Class A network ranges from 1 to 127 and uses a subnet mask of 255.0.0.0. A Class B network uses the mask 255.255.0.0, and a Class C network uses 255.255.255.0. Classful routing protocols apply the same rules. If a router is configured with a Class A address of 10.1.1.0, the default mask of 255.0.0.0 is applied, and so forth. This routing method does not scale well, so to design networks to better utilize address space, you can use classless routing, which enables the network designer to apply different masks to Class A, B, and C networks to better utilize address space. For example, you can use a Class B network, such as 131.108.0.0, and apply a Class C mask (255.255.255.0 or /24 mask).

Classful routing protocol examples include RIP and IGRP. Examples of classless routing protocols are OSPF, IS-IS, EIGRP, and BGP. With classless routing, the ability to apply summarization techniques allows for a reduction in routing table size. Over 100,000 IP routing table entries exist on the Internet. Reducing the IP route table size allows for faster delivery of IP packets and lower memory requirements. BGP is commonly referred to as a path vector protocol. To accomplish CIDR, you must allocate subnets at the common bit boundary, ensuring that your networks are continuous. For example, allocating 131.108.0.0/22 to one location and 131.108.1.0/24 to another results in a discontinuous allocation and does not allow CIDR to work properly.

Transmission Control Protocol

TCP is the most widely used protocol today, and all Cisco certification exams test your understanding of TCP/IP. This section covers TCP and how this connection-oriented protocol ensures efficient delivery of data across an IP network.

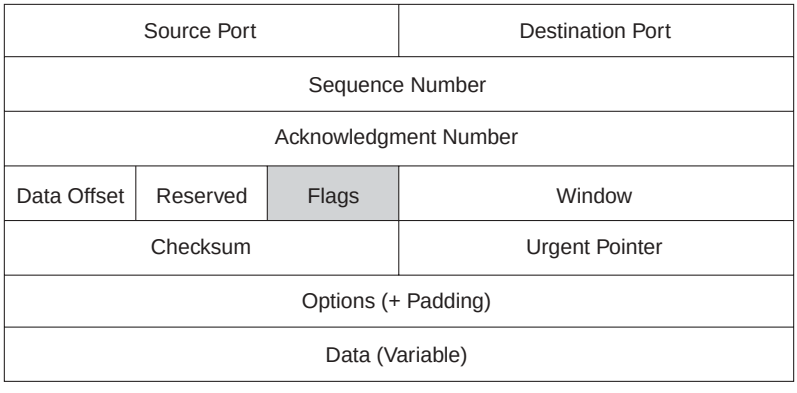
The TCP/IP model actually does not fully conform to the OSI model because IP was developed by the Department of Defense in the 1980s.

IP provides each host device with a 32-bit host address that is used to route across the IP network. TCP is a Layer 4 protocol that ensures that data is delivered across any IP cloud by using mechanisms such as connection startup, flow control, slow start (a congestion-avoidance scheme in TCP in which a host can increase the window size upon arrival of an acknowledgment), and acknowledgments. UDP is the connectionless protocol for applications such as a TFTP transfer.

TCP Mechanisms

Figure 1-9 displays the TCP header format.

Figure 1-9 *TCP Header Format*



The following descriptions summarize the TCP packet fields illustrated in Figure 1-9:

- **Source Port and Destination Port**—Identifies points at which upper-layer source and destination processes receive TCP services (16 bits in length). Common destination ports include 23 for Telnet, 21 for FTP, and 20 for FTP data.
- **Sequence Number**—Usually specifies the number assigned to the first byte of data in the current message. In the connection-establishment phase, this field can also identify an initial sequence number to be used in an upcoming transmission.

- **Acknowledgment Number**—Contains the sequence number of the next byte of data that the sender of the packet expects to receive.
- **Data Offset**—Indicates the number of 32-bit words in the TCP header.
- **Reserved**—Remains reserved for future use.
- **Flags**—Carries a variety of control information, including the SYN and ACK bits used for connection establishment and the FIN bit used for connection termination.
- **Window**—Specifies the size of the sender's receive window (that is, the buffer space available for incoming data).
- **Checksum**—Indicates whether the header was damaged in transit.
- **Urgent Pointer**—Points to the first urgent data byte in the packet.
- **Options**—Specifies various TCP options.
- **Data**—Contains upper-layer information.

A number of mechanisms are used by TCP to ensure the reliable delivery of data, including the following:

- Flags
- Acknowledgments
- Sequences numbering
- Checksum
- Windowing

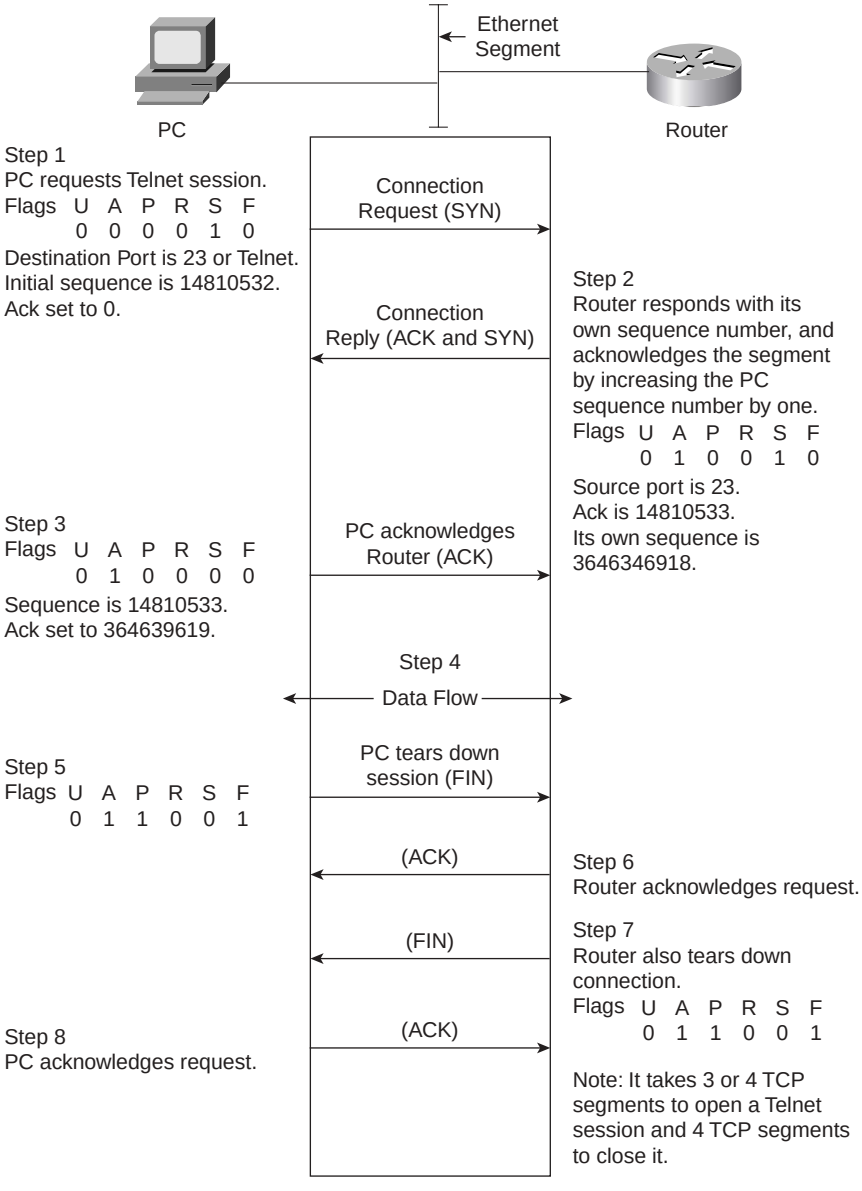
NOTE The Flags field is critical in a TCP segment. The field's various options include the following:

- **URG (U) (Urgent)**—Informs the other station that urgent data is being carried. The receiver will decide what to do with the data.
- **ACK (A) (Acknowledge)**—Indicates that the packet is an acknowledgment of received data, and the acknowledgment number is valid.
- **PSH (P) (Push)**—Informs the end station to send data to the application layer immediately.
- **RST (R) (Reset)**—Resets an existing connection.
- **SYN (S) (Synchronize)**—Initiates a connection. An acknowledgment or SYN-ACK is returned by the receiving station. Once this second segment is received, the initiating station can open the TCP session.
- **FIN (Finished)**—Indicates that the sender is finished sending data and terminates the session.

To best describe how TCP is set up and established, consider a Telnet request from a PC to a Cisco router and follow the flags, acknowledgments, sequence, and windowing options.

Figure 1-10 displays a typical Telnet session between a PC and a Cisco router. The PC initializes a Telnet request using destination port 23 and an initial sequence number.

Figure 1-10 *Telnet (TCP) Packet Flow*



The following steps are then taken by TCP:

Step 1 A user on the PC initiates a Telnet session to the router.

The PC sends a request with the SYN bit sent to 1.

The destination port number is 23 (Telnet). The PC also places an initial sequence number (in this case, random number 14810532) in the segment.

Step 2 The router responds with its own sequence number (such as 3646349618) and acknowledges (ACK) the segment sent by the PC. The ACK will be the next expected sequence number generated by the PC; in this example, the ACK is numbered 14810533.

Step 3 The PC sends a segment that acknowledges (ACK) the router's reply. The first three steps are commonly known as the *TCP three-way handshake*. It is possible for four packets to start a session if a parameter must be negotiated.

Step 4 Data is transferred. The window size can be adjusted according to the PC or the router. The window size, for example, might be four packets before an acknowledgment is required. The sender waits for an acknowledgment before sending the next four segments. The window size can change during a data transfer; this is commonly known as the *sliding window*. If, for example, a lot of bandwidth is available, the sender might resize the window to eight segments. Or the sender might resize the window to two segments during periods of high congestion. The ACK sent by the receiver is the next expected segment. This indicates that all previous segments have been received and reassembled. If any segment is lost during this phase, TCP can renegotiate the time waited before receiving the ACK and resend any lost segments.

Step 5 After the PC completes the data transfer, the Telnet session closes by sending a TCP segment with the FIN flag set to 1.

Step 6 The router acknowledges (ACK) the request.

Step 7 At this stage, the session is still open and the router could send data (this is known as *TCP half close*), but the router has no data to send and usually sends a segment with the FIN bit set to 1.

Step 8 The PC acknowledges the router's FIN request, and the Telnet session is closed. At any stage, the session can be terminated if either host sends a reset (RST flags in the TCP header); in this case, the session must be reestablished from scratch.

You need to know the TCP process and how packets are sequenced and acknowledged. TCP acknowledgments specify the next expected segment from a sender. A TCP session requires three or four segments to start (known as three-way handshake) and four segments to shut down.

TCP/IP Services

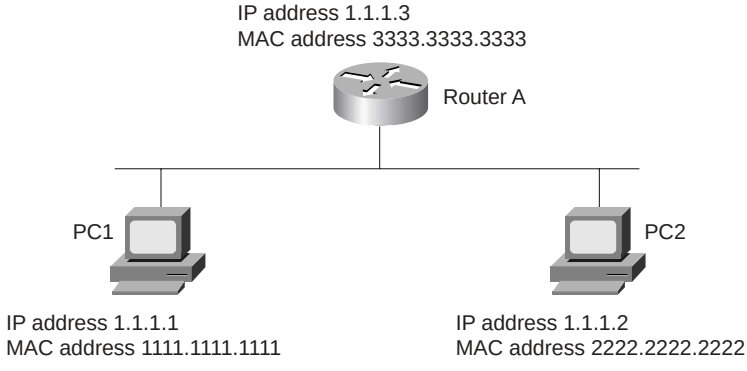
This section covers common TCP/IP services or applications used in today's large IP networks:

- Address Resolution Protocol (ARP)
- Reverse Address Resolution Protocol (RARP)
- Dynamic Host Configuration Protocol (DHCP)
- Hot Standby Router Protocol (HSRP)
- Internet Control Message Protocol (ICMP)
- Telnet (TCP based)
- File Transfer Protocol (FTP, TCP based)
- Trivial File Transfer Protocol (TFTP, UDP based)

Address Resolution Protocol

ARP determines a host's MAC address when the IP address is known. For example, to ping one device from another, the Layer 2 MAC fields require a destination MAC address. Because this is the first such request, a broadcast packet is sent across the wire to discover the remote host's MAC address. Figure 1-11 displays a scenario where PC1 wants to ping Host PC2.

Figure 1-11 *ARP Request*



When PC1 sends a ping request to PC2 using the known IP address 1.1.1.2 (Layer 3), a broadcast Layer 2 frame must first be sent by PC1; without a Layer 2 MAC address, PC1 cannot communicate with PC2. PC1 will then send a Layer 2 frame to the destination address FF-FF-FF-FF-FF-FF, and ARP (the ARP frame contains the source MAC address, destination MAC address, the source IP address, and the destination address) is sent to all devices requesting the Layer 2

MAC address of the device configured with the IP address 1.1.1.2 (by sending a Layer 2 broadcast frame). PC2 responds to the ARP request with its source MAC address, 2222.2222.2222. PC1 now has PC2's MAC address and sends a packet to the destination address, 2222.2222.2222, and Layer 3 destination address, 1.1.1.2.

NOTE A less common ARP term used in ARP terminology is *gratuitous ARP*. A gratuitous ARP is an ARP request with its own IP address as the target address. It refreshes a device's ARP table entries and also looks up duplicate IP addresses. Routers are devices that can send a gratuitous ARP.

To view the IP ARP table on a Cisco router, the command is **show ip arp**. The IP ARP table from Figure 1-11 is displayed in Example 1-2.

Example 1-2 **show ip arp** *Command on Router A*

```
RouterA#show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  1.1.1.3                -   3333.3333.3333  ARPA   Ethernet0
Internet  1.1.1.1              170   1111.1111.1111  ARPA   Ethernet0
Internet  1.1.1.2               94   2222.2222.2222  ARPA   Ethernet0
```

NOTE If you have ever wondered why the first ping request on a Cisco router fails, it is because an ARP request is sent first when an entry is not present in the ARP table. Subsequent pings will have 100 percent success.

Reverse ARP

RARP is the protocol that is used when a device boots up without an IP address and requests an IP address. RARP is typically not used in today's networks, and is replaced by DHCP.

Inverse Address Resolution Protocol (InARP) is an addition to ARP which addresses ARP in a Frame Relay environment. InARP discovers the remote end's data-link connection identifier (DLCI).

A gratuitous ARP is when the MAC address in a system is changed. That is, the MAC address for a given Hosts IP address mapping is changed for any valid reason, such as network card replacement or router failure. In this case, when the host or router is rebooted or replaced, the device sends a gratuitous ARP packet advising all hosts of the new MAC address. Because this is a broadcast packet, all the hosts in the network receive and process this packet. They update their old mapping in the ARP cache with this new mapping. This ensures that devices can communicate immediately.

Dynamic Host Configuration Protocol

DHCP is defined in RFC 1531 (the latest is RFC 2131) and provides a comprehensive method of allocating IP addresses, subnet mask, gateway address, DNS server, WINS servers, and many more parameters for IP devices.

DHCP clients send messages to the server on UDP 67, and servers send messages to the client on UDP 68. Cisco routers can also be configured for DHCP.

Example 1-3 configures a Cisco IOS router to allocate the entire range 131.108.1.0/24, with a gateway address 131.108.1.1, subnet mask 255.255.255.0, DNS servers 141.108.1.1 and 141.108.1.2, domain name cisco.com, and WINS (for Windows clients) server addresses 64.104.1.1 and 141.108.2.1. The lease should last forever, so the final command is **lease infinite**. You can exclude IP addresses from the pool with the following command:

```
ip dhcp excluded-address low-ip-address high-ip-address
```

Example 1-3 *DHCP Configuration on Cisco IOS Router*

```
R1#show running-config | begin dhcp
ip dhcp excluded-address 131.108.1.1
!Exclude the address 131.108.1.1 to the end address 13.1.108.1.10
ip dhcp excluded-address 131.108.1.1 131.108.1.10
Interface Ethernet 0
ip address 131.108.1.1 255.255.255.0
!
ip dhcp pool DHCPpool
   network 131.108.1.0 255.255.255.0
   dns-server 141.108.1.1 141.108.1.2
   domain-name cisco.com
   default-router 148.16.36.6 148.16.36.3
   netbios-name-server 64.104.1.1 141.108.2.1
   lease infinite
```

To view the DHCP leases, use the Cisco IOS command **show ip dhcp server**. Example 1-4 displays the output taken from a router configured for DHCP (note that Cisco IOS 12.2 and higher output is shown in Example 1-4).

Example 1-4 **show ip dhcp server statistics** *Sample Display*

```
Router> show ip dhcp server statistics
Memory usage          40392
Address pools         1
Database agents       1
Automatic bindings    180
```

Example 1-4 **show ip dhcp server statistics** *Sample Display (Continued)*

```
Manual bindings         1
Expired bindings        3
Malformed messages      0
Secure arp entries      1

Message                 Received
BOOTREQUEST             12
DHCPDISCOVER            200
DHCPREQUEST             178
DHCPDECLINE             0
DHCPRELEASE             0
DHCPINFORM              0

Message                 Sent
BOOTREPLY               12
DHCPOFFER               180
DHCPACK                 172
DHCPNAK                 6
```

Example 1-4 shows that 180 devices are currently allocated IP addresses, and 178 requests were made.

Hot Standby Router Protocol

HSRP allows networks with more than one gateway to provide redundancy in case of interface or router failure on any given router.

HSRP allows router redundancy in a network. It is a Cisco proprietary solution that existed before the IETF defined the Virtual Router Redundancy Protocol (VRRP). To illustrate HSRP, Figure 1-12 displays a six-router network with clients on segments on Ethernet networks, Sydney and San Jose.

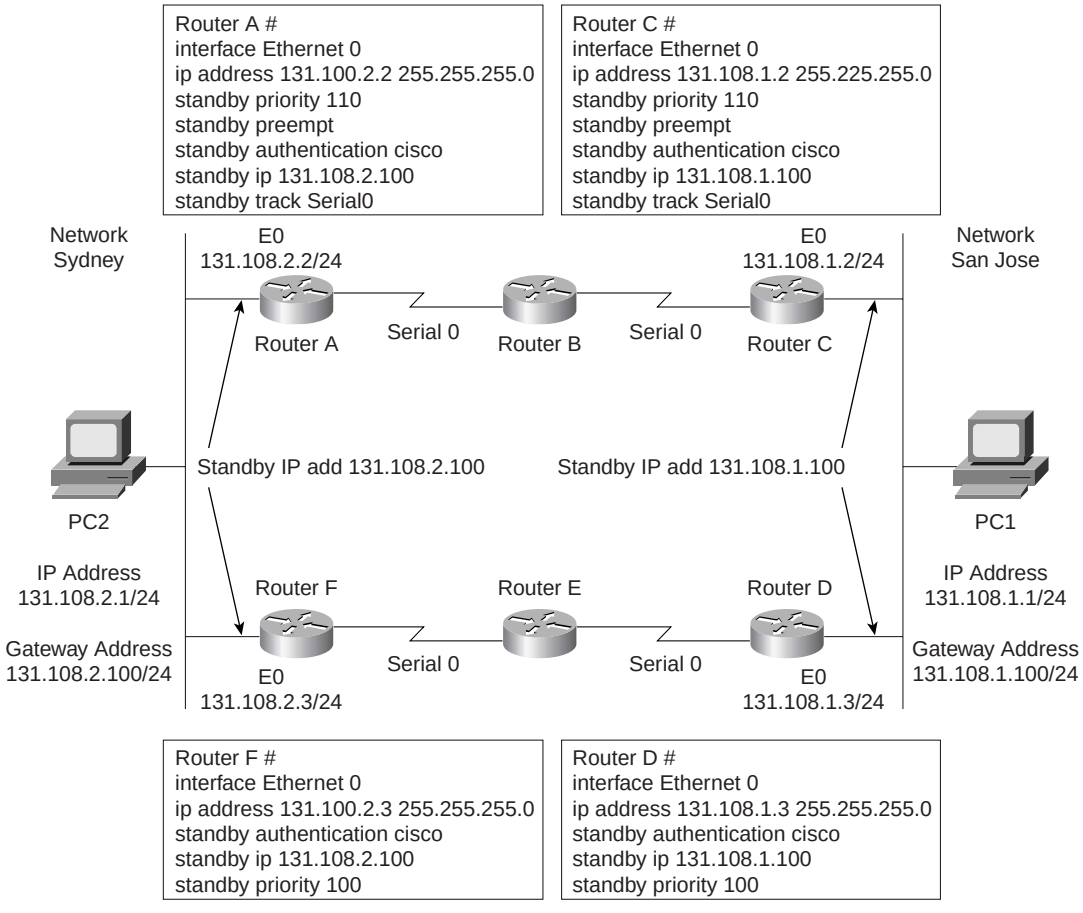
Cisco exams typically test Cisco proprietary protocols more heavily than industry-standard protocols, such as VRRP. At the time of this writing, Cisco.com does not list VRRP as an objective that will be tested.

HSRP failover can be applied to VPN routers (Cisco IOS 12.2 and later) through the use of HSRP. Remote VPN gateways connect to the local VPN router through the standby address that belongs to the active device in the HSRP group. This ensures that statically configured VPN tunnels have some form of redundancy if a router or interfaces fails.

Cisco.com provides more details on IPSec VPN failure and HSRP at the following URL:

http://cisco.com/en/US/products/sw/iosswrel/ps5012/
products_feature_guide09186a0080116d4c.html

Figure 1-12 *HSRP Example*



PCs are typically configured with only one gateway address. (Windows 2000/XP clients can take more than one, but this still leaves a problem in that all devices must be configured for multiple gateways; the most scalable solution is to configure a single gateway on all devices and allow an intelligent network to provide redundancy where only a few devices require configuration.) Assume that PC1 is configured with a gateway address of 131.108.1.100. Two routers on the Ethernet share the segment labeled San Jose network. To take advantage of the two routers, HSRP allows only Routers C and D to bid for a virtual IP address, and if any one router (Router C or D, in this example) fails, the operational router assumes the HSRP gateway address. Host devices typically have only a brief 100- to 200-ms interruption when a network failure occurs.

To illustrate how HSRP provides default gateway support, refer to Figure 1-12, which shows a network with two local routers configured with an Ethernet interface address of 131.108.1.2/24 for

Router C and 131.108.1.3/24 for Router D. Notice that both routers share a common Ethernet network. Assume that PC1 has been configured with a default gateway pointing to Router C. If Router C goes down or the Ethernet interface becomes faulty, all the devices must be manually reconfigured to use the second default gateway (Router D, 131.108.1.3/24). HSRP enables the network administrator to elect one of the two routers to act as the default gateway. If the elected router goes down, the second router assumes the IP default gateway. The Cisco IOS command **standby track** *interface-of-wan* under the Ethernet interface allows the router to monitor the WAN link. If the WAN link continuously fails past a threshold, the HSRP default router decreases its priority to allow a more reliable WAN connection to provide a gateway. For example, in Figure 1-12, if the link between Routers C and B fails past a threshold, Router D can be configured to assume the HSRP address to provide a faster connection to the IP backbone network.

The steps to enable HSRP are as follows:

1. Enable HSRP (required).
2. Configure HSRP group attributes (optional).
3. Change the HSRP MAC refresh interval (optional).

Table 1-5 illustrates the various required and optional commands to enable HSRP.

Table 1-5 *HSRP Commands*

Cisco IOS Command	Purpose
standby [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime*	These required commands configure the time between Hello packets and the hold time before other routers declare the active router to be down.
standby [*group-number*] **ip** [*ip-address* [**secondary**] or **standby** [*group-number*] **preempt** [**delay** {**minimum** *delay* | **reload** *delay* | **sync** *delay*}]	The **standby ip** command activates HSRP on the configured interface. If an IP address is specified, that address is used as the designated address for the Hot Standby group. If no IP address is specified, the designated address is learned through the standby function. For HSRP to elect a designated router, at least one router on the cable must have been configured with, or have learned, the designated address. Configuring the designated address on the active router always overrides a designated address that is currently in use. Also note if **preempt** is not enabled, a router with a higher priority will not become the HSRP active router.
standby [*group-number*] **track** *type number* [*interface-priority*]	This optional command configures the interface to track other interfaces so that if one of the other interfaces goes down, the device's Hot Standby priority is lowered.

continues

Table 1-5 *HSRP Commands (Continued)*

Cisco IOS Command	Purpose
standby [*group-number*] **authentication** *string*	Selects an authentication string to be carried in all HSRP messages. An optional authenticator field allows only authenticated routers to offer HSRP.
standby use-bia [**scope interface**]	Configures HSRP to use the burned-in address of an interface as its virtual MAC address instead of the preassigned MAC address (on Ethernet and FDDI) or the functional address (on Token Ring).

Now configure Routers C and D in Figure 1-12 for HSRP, and ensure that Router C is the primary gateway address and that the PC is configured with a gateway address of 131.108.1.100. Router C is configured with a higher priority (**standby priority 110 preempt**) than the default 100 to ensure that Router C becomes the default gateway for the hosts on the San Jose network; authentication is also enabled between the two gateway routers.

Example 1-5 displays the sample Cisco IOS configuration for Router C.

Example 1-5 *HSRP Configuration on Router C*

```
interface Ethernet0
 ip address 131.108.1.2 255.255.255.0
 standby priority 110
 standby preempt
 standby authentication cisco
 standby ip 131.108.1.100
 standby track Serial0
```

Example 1-5 displays Router C configured with a virtual IP address of 131.108.1.100 and **preempt**, which allows Router C to assume the role if a failure occurs. The **track** command ensures that Serial0, or the WAN link to Router B, is monitored to make sure that a flapping link does not cause bandwidth delays for users, such as PC1. For every tracked interface failure, the priority is reduced by 10 by default. The Cisco IOS default priority is set to 100. In this configuration, two failures must occur for Router D to assume the HSRP address (110 – 10 – 10 = 90 < 100).

Example 1-6 displays the sample Cisco IOS configuration for Router D. Configure Router D with an HSRP priority of 105 so that any two (not one) failures on Router C will mean that Router D priority is higher than Router C. (Router C is set to 110; one failure and then it is set to 110 – 20 = 90 < 100.) Router D is not configured for **preempt** because Router C is designed to be the active HSRP address when both C and D are operational.

Example 1-6 *HSRP Configuration on Router D*

```
interface Ethernet0
 ip address 131.108.1.3 255.255.255.0
 standby authentication cisco
 standby ip 131.108.1.100
```

To view the status of HSRP, the Cisco IOS command is **show standby**. Example 1-7 displays the sample output when this command is entered in Router C.

Example 1-7 **show standby** *on Router C*

```
Router-C#show standby
Ethernet0 - Group 0
Local state is Active, priority 110, may preempt
Hellotime 3 sec, holdtime 10 sec
Next hello sent in 1.458
Virtual IP address is 131.108.1.100 configured
Active router is local
Standby router is 131.108.1.3 expires in 8.428
Virtual mac address is 0000.0c07.ac01
2 state changes, last state change 02:09:49
IP redundancy name is "hsrp-Et0-1" (default)
Priority tracking 1 interface, 1 up:
Interface    Decrement  State
Serial0         10      Up
```

Router C is currently the configured gateway and is tracking Serial 0 for failures; every WAN failure decrements the priority value by 10. If a single failure occurs, the priority on Router C drops to 100 (110 – 10 = 100), the same as Router D. Because Router C still has the **preempt** option, Router C remains active when it returns. However, if a second failure occurs on Router C, its priority drops another 10 to 90, below the priority of D, so Router D remains as the default gateway until the interface on Router C has fully recovered. After the priority on Router C increments back to 110, Router C assumes the gateway function because **preempt** is enabled, as displayed in Example 1-7.

Example 1-8 displays the output of the **show standby** command on Router D when in standby mode.

Example 1-8 **show standby** *on Router D*

```
Router-D#show standby
Ethernet - Group 0
  Local state is Standby, priority 100,
  Hellotime 3 holdtime 10
  Next hello sent in 00:00:01.967
  Hot standby IP address is 131.108.1.100 configured
  Active router is local
  Standby router is unknown expired
  Standby virtual mac address is 0000.0c07.ac00
  2 state changes, last state change 00:03:59
```

Internet Control Message Protocol

ICMP is a network layer (Layer 3) Internet protocol that reports errors and provides other information relevant to IP packet processing. ICMP is fully documented in RFC 792. ICMP's purpose is to report error and control messages.

ICMP provides a number of useful services supported by the TCP/IP protocol, including ping requests and replies. ICMP Echo requests and replies enable an administrator to test connectivity with a remote device.

Be aware that ICMP runs over IP, which means that there is no guarantee of delivery (because IP is a connectionless protocol). Example 1-9 provides a sample **ping** command in which an administrator wants to see if a remote device is reachable by sending the remote device a ping request from a Cisco router. By default, a Cisco router sends out a series of five ICMP requests whenever the **ping** command is issued. Example 1-9 displays a sample ping request to the remote IP address 131.108.1.1 on Router R2.

Example 1-9 *The* **ping 131.108.1.1** *Command*

```
R2>ping 131.108.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 131.108.1.1,
!!!!!
Success rate is 100 percent (5/5),
R2>
```

The **ping** command has a number of reporting mechanisms that run over ICMP. The exclamation point (!) indicates a successful reply. The **ping** command can also advise you, using a special code character, that the end device is not reachable, as depicted in Table 1-6.

Table 1-6 *Possible Test Characters When Using the* **ping** *Command*

Code	Indicates
!	The receipt of a reply
.	The network server timed out while waiting for a reply
U	Destination unreachable
N	Network unreachable
P	Protocol unreachable
Q	Source quench
M	Could not fragment
?	Unknown packet type

Cisco IOS provides a detailed version of the ping tool, which you can evoke by typing **ping** in the enabled mode. This command is known as the *extended ping command*.

Telnet

Telnet is an application layer protocol and part of the TCP/IP protocol suite. The TCP destination port number is 23 and commonly manages routers and switches, for example. Telnet is an insecure protocol, because data flows in plain text and the Telnet passwords can be sniffed. SSH is more secure for remote logins.

File Transfer Protocol and Trivial File Transfer Protocol

FTP and TFTP are application layer protocols (part of the TCP/IP protocol suite of applications). FTP is a connection-oriented protocol running over TCP. FTP uses two connections to maintain connectivity between two IP hosts: port 20 is used for the data port and port 21 is used for control.

TFTP runs over UDP port 69 and is a connectionless protocol. TFTP commonly uploads Cisco IOS and configurations to a TFTP server. TFTP is regarded as the simple version of FTP. TFTP does not require any username/password combination to transfer data, as opposed to FTP, which requires a username and password before data can be transferred. Note, however, that FTP sends the username and password in clear text, whereas TFTP transfers data between two high UDP port values.

NOTE Domain Name System (DNS) is another common application that uses both TCP and UDP port 53.

Now that you fully appreciate the TCP/IP model, the next section covers routing protocols used to ensure that TCP/IP data can be moved, or routed, from one location to another.

Routing Protocols

This section covers four main routing protocols:

- Routing Information Protocol (RIP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Open Shortest Path First (OSPF)
- Border Gateway Protocol (BGP)

Before discussing the characteristic of each protocol, this section covers how routers (Cisco routers, in particular) generally route IP packets.

Routing is a process whereby a path to a destination host is selected by either a dynamic or static routing protocol. A routing protocol is an algorithm that routes data across the network. Each router makes routing decisions from host to destination based on specific metrics used by the operating routing protocol. For example, RIP uses hop count (commonly known as the network diameter) to decide which router interface the data is sent over. A lower hop count is always preferred. OSPF, on the other hand, uses a cost metric; the lower a path's cost, the more preferred it is as a path to the destination.

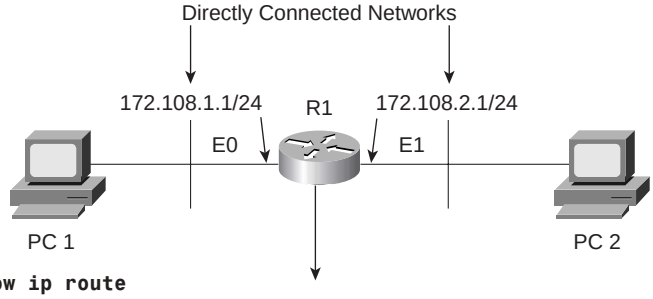
Routing IP across a network of Cisco routers requires IP address allocation to interfaces and then a static or dynamic routing protocol to advertise these networks to local or remote routers. After these networks are advertised, IP data can flow across the network. Routing occurs at Layer 3 (the network layer) of the OSI model.

By default, IP routing is enabled on Cisco routers. The command used to start or disable IP routing is [**no**] **ip routing**. By default, IP routing is enabled on all routers, so you do not see this command by viewing the configuration. On the Catalyst switches, you have to enable IP routing to make it a Layer 3 device. Consider a one-router network with two directly connected Ethernet interfaces as an introductory example. Figure 1-13 displays a two-port Ethernet router configured with two subnets.

PC1 can communicate with PC2, as shown in Figure 1-13, because Cisco routers route to directly connected interfaces.

The Cisco IOS command **show ip route** is used to view the IP routing table, and a number of symbols define how remote or local networks have been discovered. Table 1-7 defines the various symbols and their meanings. The Cisco Documentation CD-ROM defines the routing fields or codes as follows.

Figure 1-13 *Connected Routes*




```
R1# show ip route
Codes C- connected, S- static, I- IGRP, R- RIP, M- mobile, B- BGP
D- EIGRP, EX- EIGRP external, Q- QSPF, 1A- OSPF inter area
N1- OSPF NSSA external type 1, N2- OSPF NSSA external type 2
E1- OSPF external type 1, E2- OSPF external type 2, E- EGP
i- IS-IS, L1- IS-IS level-1, L2- IS-IS level-2.*-candidate default
U- per-user static route, o- ODR
-
Gateway of last resort is not set
-
 172.108.0.0/24 is subnetted, 2 subnets
C  172.108.1.0 is directly connected, Ethernet0
C  172.108.2.0 is directly connected, Ethernet1
R1#
```

Table 1-7 **show ip route** *Defined**

Field Value	Description
O	Indicates the protocol that derived the route. Possible values include the following: I—IGRP derived R—RIP derived O—OSPF derived C—Connected S—Static E—EGP derived B—BGP derived D—EIGRP EX—EIGRP external I—IS-IS derived Ia—IS-IS M—Mobile P—Periodic downloaded static route U—Per-user static route O—On-demand routing

continues

Table 1-7 **show ip route** *Defined* (Continued)*

Field Value	Description
E2	Indicates the type of route. Possible values include the following: *—The last path used when a packet was forwarded. It pertains only to the non-fast-switched packets. However, it does not indicate what path will be used next when forwarding a non-fast-switched packet, except when the paths are equal cost. IA—OSPF interarea route. E1—OSPF external type 1 route. E2—OSPF external type 2 route. L1—IS-IS Level 1 route. L2—IS-IS Level 2 route. N1—OSPF NSSA external type 1 route. N2—OSPF NSSA external type 2 route.
O 10.110.0.0 [90/5] via 10.119.254.6, 0:01:00, Ethernet2 E 10.67.10.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2	Indicates the address of the remote network.
[90/5]	The first number in the brackets is the information source's administrative distance; the second number is the metric for the route.
via	Specifies the address of the next router to the remote network.
0:01:00 (O 10.110.0.0 [90/5] via 10.119.254.6)	Specifies the last time the route was updated, in hours:minutes:seconds.
Ethernet2	Specifies the interface through which the specified network can be reached.

*Part of this table taken from http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fiprrp_r/ind_r/1rfindp2.htm#102251, all rights are reserved to Cisco.

By default, Cisco IOS assigns to each routing protocol an administrative distance (AD) that indicates the trustworthiness of a routing entry if more than one path exists to a remote network running two or more routing algorithms. You can configure the AD value from the default with the **distance** *administrative-distance* Cisco IOS command if you want to manually choose RIP over OSPF, for example. The value for *administrative-distance* can be 1 to 255.

IP routing protocols support multipath destinations. In other words, if more than one path exists to a remote network, then metrics are used to determine whether load balancing will occur. If load

balancing occurs and more than one routing protocol has learned this remote path, then the distinguisher becomes the AD—the lower its value, the more trusted it is. Remember that AD is first considered the delineator, followed by the metric.

Table 1-8 displays the administrative distances enabled by default on Cisco routers.

Table 1-8 *Default Administrative Distances*

Route Source	Default Administrative Distance
Connected interface	0
Static route	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
EIGRP external route	170
Internal BGP	200
Unknown	255

For example, Table 1-8 demonstrates that an EIGRP (AD 90) route is preferred over a network entry discovered by RIP (AD 120) because the AD is lower, or more trustworthy.

NOTE The IP address source and destination in an IP datagram do not alter, but the Layer 2 MAC source and destination do, for example, when PC1 sends a packet to PC2 in Figure 1-13. The TCP/IP software on PC1 identifies that the remote destination (172.108.2.0/24) is not locally connected and sends the Layer 3 frame to the local gateway address, 171.108.1.1/24. For the Layer 2 frame to traverse the local Ethernet, the destination Layer 2 MAC address must be that of the local router or gateway. PC2 resides on a different subnet, so the destination MAC address will be that of Router R1 (E0 burnt-in address) or the default gateway address of 172.108.1.1. Router R1 then strips the Layer 2 header and installs its own Layer 2 header when the packet enters the network where PC2 resides. The Layer 2 header contains the source address (Layer 2) of R1 E1 and destination address of PC2's MAC address. The Layer 3 IP source and destination addresses do not change during the routing of the IP packet. The exception to changes in Layer 3 addressing is when Network Address Translation (NAT) is used.

Routing Information Protocol

RIP is one the oldest routing protocols in use today.

RIP is a distance vector protocol. Table 1-9 defines the characteristics of a distance vector protocol.

Table 1-9 *Distance Vector Protocol Characteristics*

Characteristic	Description
Periodic updates	Periodic updates are sent at a set interval; for IP RIP, this interval is 30 seconds.
Broadcast updates	Updates are sent to the broadcast address 255.255.255.255. Only devices running routing algorithms listen to these updates.
Full table updates	When an update is sent, the entire routing table is sent.
Triggered updates	Also known as Flash updates, these are sent when a change occurs outside the update interval.
Split horizon	This method stops routing loops. Updates are not sent out an outgoing interface from which the source network was received. This saves bandwidth, as well.
Count to infinity	Maximum hop count. For RIP, it is 15, and for IGRP, it is 255.
Algorithm	Example: Bellman-Ford for RIP.
Examples	RIP and IGRP.

RIP comes in two versions: RIPv1 (does not support VLSM) and RIPv2. Both versions of RIP automatically summarize at the network boundary (you can configure the classful routing protocol, RIPv2, to support VLSM).

The following list summarizes RIPv1 characteristics:

- Distance vector protocol
- Runs over UDP port 520
- Metric is hop count (maximum is 15; 16 is unreachable)
- Periodic updates every 30 seconds
- Up to 25 networks per RIP update
- Implements split horizon
- Implements triggered updates

- No support for VLSM or authentication
- Administrative distance is 120
- Updates are sent to the broadcast address 255.255.255.255

NOTE Split horizon is a routing technique in which information about routes is prevented from exiting the router interface through which that information was received. Split horizon updates are useful in preventing routing loops. To enable split horizon, the Cisco IOS command is **ip split-horizon** (an interface command). Split horizon on Frame Relay subinterfaces is enabled by default. Always use the Cisco IOS command **show ip interface** to determine if split horizon is enabled or displayed.

A triggered update is a method by which a routing protocol sends an instant message as soon as a network failure is detected. If a triggered update were not used, the only way the update would be sent would be via the normal update every 30 seconds, causing a delay in network convergence times. Split horizon is a favorite topic in CCIE lab exams.

Poison Reverse updates explicitly indicate that a network is unreachable rather than implying that a remote network is unreachable by not sending that network in an update. Poison Reverse updates are intended to defeat routing loops in large IP networks.

Split horizon, Poison Reverse, and triggered updates are methods used by distance vector protocols to avoid routing loops

RIPv2 was developed to enable RIPv1 to support VLSM, so it is a classless routing protocol that also supports authentication. RIPv1 and RIPv2 use the same hop count as the metric.

The following list summarizes RIPv2 characteristics:

- Distance vector protocol
- Runs over UDP port 520
- Metric is hop count (maximum is 15; 16 is unreachable)
- Periodic updates every 30 seconds
- Up to 25 networks per RIP update
- Implements split horizon
- Implements triggered updates
- Supports VLSM (subnet mask carried in updates)

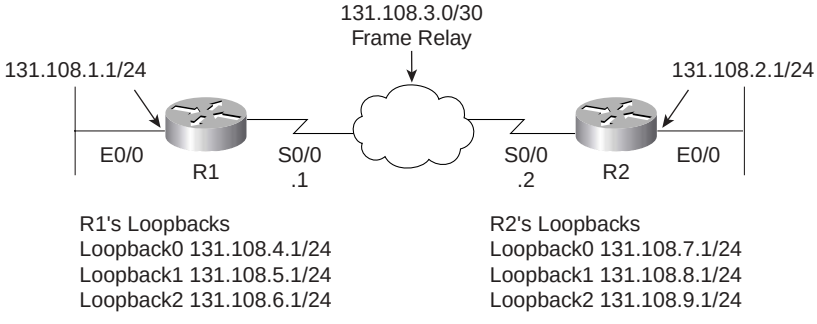
- Supports authentication
- Administrative distance is 120
- Updates sent to multicast address 224.0.0.9
- Can set up neighbors to reduce broadcast traffic (send unicast updates)

To enable RIPv1 or RIPv2 on a Cisco router, the command required is **router rip**. By default, after you enable this command and install the network statements, RIPv1 sends and receives updates and RIPv2 only listens for updates.

Consider a two-router topology running VLSM and RIP. Figure 1-14 displays two routers, named R1 and R2, with a 30-bit network used across the WAN. Loopbacks are used to populate the IP routing tables.

To start, enable RIP on both routers with the commands in Example 1-10. Version 2 must be enabled because you are implementing VLSM across the WAN links between R1 and R2.

Figure 1-14 *Practical Example of Routing RIP*



Example 1-10 displays the RIP configuration on R1. The same configuration commands are applied to R2.

Example 1-10 *IP RIP Configuration on R1*

```
router rip
 version 2
 network 131.108.0.0
```

You can view the RIP forward database with the command **show ip rip database**. Example 1-11 displays the output when **show ip rip database** is executed on R1.

Example 1-11 **show ip rip database** *Command on R1*

```
R1#show ip rip database
131.108.0.0/16    auto-summary
131.108.1.0/24    directly connected, Ethernet0/0
131.108.2.0/24
    [1] via 131.108.3.2, 00:00:12, Serial0/0
131.108.3.0/30    directly connected, Serial0/0
131.108.4.0/24    directly connected, Loopback0
131.108.5.0/24    directly connected, Loopback1
131.108.6.0/24    directly connected, Loopback2
131.108.7.0/24
    [1] via 131.108.3.2, 00:00:12, Serial0/0
131.108.8.0/24
    [1] via 131.108.3.2, 00:00:12, Serial0/0
131.108.9.0/24
    [1] via 131.108.3.2, 00:00:12, Serial0/0
```

Example 1-11 displays the directly connected routes and the four dynamically discovered routes via Serial0/0 to R2. To confirm that the entries are reachable, display the IP routing table on R1 and perform a few ping requests across the Frame Relay cloud.

Example 1-12 displays the IP routing table and the successful ping requests to the four remote networks.

Example 1-12 **show ip route** *and* **ping** *to R2*

```
R1#show ip route
Codes: C - connected, R - RIP,
     131.108.0.0/16 is variably subnetted, 9 subnets, 2 masks
R       131.108.9.0/24 [120/1] via 131.108.3.2, 00:00:00, Serial0/0
R       131.108.8.0/24 [120/1] via 131.108.3.2, 00:00:00, Serial0/0
R       131.108.7.0/24 [120/1] via 131.108.3.2, 00:00:00, Serial0/0
C       131.108.6.0/24 is directly connected, Loopback2
C       131.108.5.0/24 is directly connected, Loopback1
C       131.108.4.0/24 is directly connected, Loopback0
C       131.108.3.0/30 is directly connected, Serial0/0
R       131.108.2.0/24 [120/1] via 131.108.3.2, 00:00:01, Serial0/0
C       131.108.1.0/24 is directly connected, Ethernet0/0
R1#ping 131.108.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 131.108.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
R1#ping 131.108.7.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 131.108.7.1, timeout is 2 seconds:
!!!!!
```

continues

Example 1-12 **show ip route** *and* **ping** *to R2 (Continued)*

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
R1#ping 131.108.8.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 131.108.8.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
R1#ping 131.108.9.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 131.108.9.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
R1#
```

Example 1-12 displays the four remote networks reachable by the Serial 0/0 and four successful ping requests (five replies from each remote network) to those interfaces on R2.

Stop R2 from sending R1 any updates via the Frame Relay cloud to demonstrate the **passive-interface** command, **passive-interface serial0/0**. New Cisco IOS revision levels also permit the administrator to set a default state (routing or just listening-passive) for all interfaces. The Cisco IOS command **passive-interface default** ensures that all interfaces, unless specified otherwise, are passive. To take an interface from passive into active, for example, you would use the command **no passive-interface serial0/0** in conjunction with the **passive-interface default** command**.** This new command can be helpful in large IP networks.

Example 1-13 displays the passive interface configuration on R2 Serial0/0.

Example 1-13 *Passive Interface Configuration on R2*

```
R2(config)#router rip
R2(config-router)#passive-interface serial 0/0
```

R1's routing table now contains no remote entries from R2, which will still receive updates because the command affects only outbound updates. Example 1-14 confirms the missing routing RIP entries in R1's IP routing table.

Example 1-14 **show ip route** *on R1*

```
R1#show ip route
Codes: C - connected,
     131.108.0.0/16 is variably subnetted, 5 subnets, 2 masks
C       131.108.6.0/24 is directly connected, Loopback2
C       131.108.5.0/24 is directly connected, Loopback1
C       131.108.4.0/24 is directly connected, Loopback0
C       131.108.3.0/30 is directly connected, Serial0/0
C       131.108.1.0/24 is directly connected, Ethernet0/0
```

NOTE RIPv2 also offers MD5 authentication as an optional authentication mode added by Cisco to the original RFC 1723-defined plain-text authentication. The configuration is identical to that for plain-text authentication, except for the use of the additional command **ip rip authentication mode md5**. You must configure router interfaces on both sides of the link for the MD5 authentication method, making sure the key number and key string match on both sides.

Enhanced Interior Gateway Routing Protocol

EIGRP is a Cisco-developed routing protocol that uses the same metric defined by IGRP multiplied by 256. The routing metric in EIGRP is based on bandwidth, delay, load, and reliability. The CCIE Security written exam does not test your understanding of EIGRP too greatly, so this section includes only the relevant topics for the exam.

EIGRP is a Cisco proprietary routing protocol that can be used to route a number of Layer 3 protocols, including IP, IPX, and AppleTalk. This section is concerned only with routing IP.

To ensure EIGRP is as efficient as possible, the following features were built into EIGRP:

- **Rapid convergence**—EIGRP uses the Diffusing Update Algorithm (DUAL) to achieve rapid convergence. A Cisco IOS router that runs EIGRP will ensure that any redundant paths are stored and used in case of a network failure.
- **Reduced bandwidth usage**—By default, EIGRP uses up to 50 percent of available bandwidth, and this option can be changed with the Cisco IOS command **ip bandwidth-percent eigrp** *as-number percent.* By default, EIGRP uses up to 50 percent of the bandwidth defined by the interface bandwidth command. The interface command **ip bandwidth-percent eigrp** *as-number percent* can be used to change this value (a good method to use for the CCIE lab).

EIGRP is considered a hybrid routing protocol, meaning that EIGRP uses characteristics of both distance vector and link-state routing protocols to maintain routing tables.

A distance vector protocol counts the number of devices data must flow through to reach a destination—this is called the hop count.

A link-state protocol such as OSPF, discussed later in this book, permits routers to exchange information with one another about the reachability of other networks.

EIGRP Terminology

You need to understand several EIGRP-related terms for the CCIE Security written exam. Table 1-10 defines some of the common terminology used in EIGRP.

Table 1-10 *EIGRP Terms*

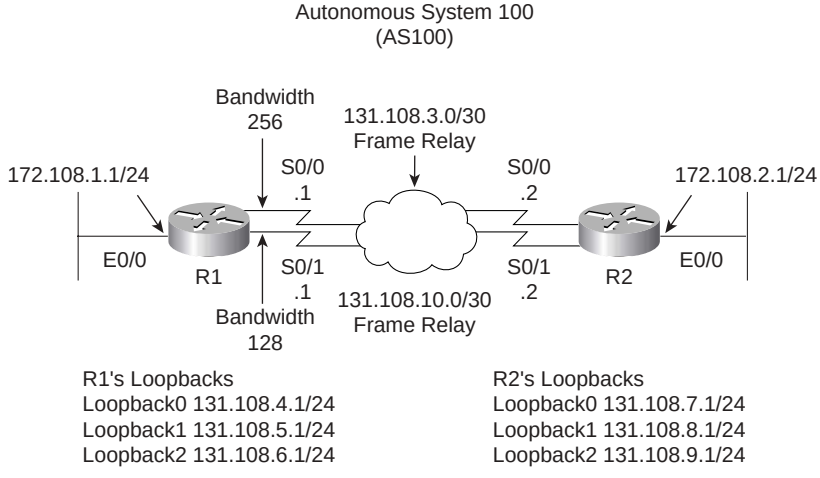
Term	Meaning
Neighbor	A router in the same autonomous system running EIGRP.
Neighbor table	EIGRP maintains a table with all adjacent routers. To view the EIGRP neighbors, use the Cisco IOS command **show ip eigrp neighbors**.
Topology table	EIGRP maintains a topology table for all remote destinations discovered by neighboring routers. To view the topology table, the Cisco IOS command is **show ip eigrp topology**.
Hello	A packet used to monitor and maintain EIGRP neighbor relationships; it is multicast.
Query	A query packet that is sent to neighboring routers when a network path is lost; can be multicast or unicast.
Reply	A reply packet to a query packet; it is unicast.
ACK	Acknowledgment of an update packet, typically a Hello packet with no data; it is unicast.
Holdtime	How long a router waits for a Hello packet before tearing down a neighbor adjacency.
Smooth Round Trip Time (SRTT)	Time taken to send a packet reliably to an acknowledgment. SRTT is the average delta between the time a packet is sent and the arrival of the neighbor's acknowledgment.
Retransmission Timeout (RTO)	The time a router waits for the arrival of the neighbor's acknowledgment.
Feasible distance	Lowest metric to remote network.
Feasibility condition (FC)	A condition under which the sum of a neighbor's cost to a destination and the cost to this neighbor is less than the current successor's cost. If the EIGRP neighbor's reported distance (the metric after the slash) is less than the feasible distance, the feasibility condition is met and that path is a feasible successor.
Feasible successor	A neighboring router with a path whose reported distance is less than the feasible successor.
Successor	A neighboring router that meets the feasibility condition and also contains the best path.
Stuck in Active (SIA)	An EIGRP router waiting for all acknowledgments from neighboring routers for all the queries sent.
Active	When a router is querying neighboring routers about a network path.
Passive	Normal route operation to a remote destination. This means there are no outstanding queries to reply to. This is normal network operation.

EIGRP Configuration Example

This examples describes how to configure a two-router EIGRP network with two Frame Relay links between the two routers, to demonstrate the redundancy mechanism with the EIGRP DUAL algorithm.

Figure 1-15 displays a two-router topology using the same addressing as the RIP example in Figure 1-14.

Figure 1-15 *EIGRP Configuration Example*



Routers R1 and R2 reside in AS 100, and to enable EIGRP on both routers, you need to start by configuring EIGRP. Example 1-15 displays the EIGRP configuration required on R1 and R2.

Example 1-15 *Enabling EIGRP in AS 100*

```
router eigrp 100
 network 131.108.0.0
```

The **network** command in Example 1-15 enables EIGRP to send and receive updates for interfaces configured with the Class B address, 131.108.0.0. EIGRP will automatically summarize Class A, B, or C addresses.

Example 1-16 displays the IP routing table on R1.

Example 1-16 **show ip route** *on R1*

```
R1#show ip route
Codes: C - connected, D - EIGRP, EX - EIGRP external,
     131.108.0.0/16 is variably subnetted, 10 subnets, 2 masks
C       131.108.10.0/30 is directly connected, Serial0/1
```

continues

Example 1-16 **show ip route** *on R1 (Continued)*

```
D       131.108.9.0/24 [90/10639872] via 131.108.3.2, 00:04:27, Serial0/0
D       131.108.8.0/24 [90/10639872] via 131.108.3.2, 00:04:27, Serial0/0
D       131.108.7.0/24 [90/10639872] via 131.108.3.2, 00:04:27, Serial0/0
C       131.108.6.0/24 is directly connected, Loopback2
C       131.108.5.0/24 is directly connected, Loopback1
C       131.108.4.0/24 is directly connected, Loopback0
C       131.108.3.0/30 is directly connected, Serial0/0
D       131.108.2.0/24 [90/10537472] via 131.108.3.2, 00:04:28, Serial0/0
C       131.108.1.0/24 is directly connected, Ethernet0/0
```

Example 1-16 displays four remote EIGRP entries (designated by D in the routing table) via the serial interface Serial0/0. EIGRP has discovered these networks as the preferred path because the WAN bandwidth is 256 kbps, as opposed to 128 kbps via Serial 0/1. To view the alternate paths, use the **show ip eigrp topology** Cisco IOS command to display backup paths.

Example 1-17 displays the output of the **show ip eigrp topology** command on R1.

Example 1-17 **show ip eigrp topology** *on R1*

```
R1#show ip eigrp topology
IP-EIGRP Topology Table for AS(100)/ID(131.108.6.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 131.108.10.0/30, 1 successors, FD is 2169856
         via Connected, Serial0/1
         via 131.108.3.2 (11023872/1761792), Serial0/0
P 131.108.9.0/24, 1 successors, FD is 2297856
         via 131.108.3.2 (10639872/128256), Serial0/0
         via 131.108.10.2 (20640000/128256), Serial0/1
P 131.108.8.0/24, 1 successors, FD is 2297856
         via 131.108.3.2 (10639872/128256), Serial0/0
         via 131.108.10.2 (20640000/128256), Serial0/1
P 131.108.7.0/24, 1 successors, FD is 2297856
         via 131.108.3.2 (10639872/128256), Serial0/0
         via 131.108.10.2 (20640000/128256), Serial0/1
P 131.108.6.0/24, 1 successors, FD is 128256
         via Connected, Loopback2
P 131.108.5.0/24, 1 successors, FD is 128256
         via Connected, Loopback1
P 131.108.4.0/24, 1 successors, FD is 128256
         via Connected, Loopback0
P 131.108.3.0/30, 1 successors, FD is 2169856
         via Connected, Serial0/0
         via 131.108.10.2 (21024000/1761792), Serial0/1
P 131.108.2.0/24, 1 successors, FD is 2195456
         via 131.108.3.2 (10537472/281600), Serial0/0
```

Example 1-17 **show ip eigrp topology** *on R1 (Continued)*

```
          via 131.108.10.2 (20537600/281600), Serial0/1
P 131.108.1.0/24, 1 successors, FD is 281600
          via Connected, Ethernet0/0
```

Example 1-17 shows that the remote network 131.108.2.0 is reachable via two paths, and because the feasible distance is lower through Serial 0/0, that path is injected into the routing table. If, for some reason, the link with Serial 0/0 on R1 fails, the alternate path will be chosen and inserted into the routing table, decreasing convergence times.

When EIGRP loses a path to a remote network, it sends requests to neighboring routers for alternative ways to reach the failed network. The neighboring router that returns the most favorable routes is called the feasible successor; in Figure 1-15, that router is R2.

NOTE The Cisco CD Documentation defines the state (active, passive, and more) of a given network with the following:

- **P (Passive)**—Indicates that no EIGRP computations are being performed for this destination.
- **A (Active)**—Indicates that EIGRP computations are being performed for this destination.
- **U (Update)**—Indicates that an update packet was sent to this destination.
- **Q (Query)**—Indicates that a query packet was sent to this destination.
- **R (Reply)**—Indicates that a reply packet was sent to this destination.
- **r (Reply status)**—A flag that is set after the software has sent a query and is waiting for a reply.

Cisco.com was the source for this material, http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fiprrp_r/1rfeigrp.htm#wp1018743.

EIGRP also supports an authentication mechanism. To enable authentication of EIGRP packets, use the **ip authentication key-chain eigrp** command in interface configuration mode. Chapter 8, "CCIE Security Self-Study Lab," contains an example of this command and its proper use.

Open Shortest Path First

OSPF is a link-state routing protocol. Link-state protocols use Dijkstra's shortest path first (SPF) algorithm to populate the routing table. OSPF shares information with every router in the network. OSPF is a classless protocol and supports VLSM.

OSPF in a Single Area

When configuring any OSPF router, you must establish for which area assignment the interface will be enabled. OSPF has some basic rules when it comes to area assignment. OSPF must be configured with areas. The backbone area 0, or 0.0.0.0, must be configured if you use more than one area assignment. If your OSPF design has only one area, it may have any number. Table 1-11 defines common OSPF terminology.

Table 1-11 *Common OSPF Terms*

Term	Description
Hello packet	Exchanged by the routers for neighbor discovery and forming adjacencies, neighbor keepalives, and designated router (DR)/backup DR (BDR) election.
Link state	Information is shared between directly connected routers. This information propagates unchanged throughout the network and is also used to create an SPF tree.
Area	A group of routers and links that share the same area ID. All OSPF routers require area assignments. All routers within an area have the same database. Link-state flooding is limited to an area.
Autonomous system	A network under a common network administration domain running common routing protocols.
Cost (OSPF metric)	The routing metric used by OSPF. Lower costs are always preferred. You can manually configure the cost of an interface with the **ip ospf cost** command. By default, the cost is calculated by using the formula, cost = 10^8 ÷ bandwidth.
Router ID	Each OSPF router requires a unique router ID, which is the highest IP address configured on a Cisco router or the highest-numbered loopback address. You can manually assign the router ID.
Adjacency	When two OSPF routers have exchanged information between each other and have the same topology table. Adjacency can have a number of states or exchange states: **Init state**—When Hello packets have been sent and are awaiting a reply to establish two-way communication. **Establish bidirectional (two-way) communication**—Accomplished by the discovery of the Hello protocol routers and the election of a DR. **Exstart**—Two neighbor routers form a master/slave relationship and agree upon a starting sequence that will be incremented to ensure that LSAs are acknowledged. **Exchange state**—Database Description (DD) packets continue to flow as the slave router acknowledges the master's packets. OSPF is operational because the routers can send and receive LSAs between each other. DD packets contain information such as the router ID, area ID, checksum, if authentication is used, link-state type, and the advertising router. LSA packets also contain information such as router ID, and additionally include MTU sizes, DD sequence numbering, and any options. **Loading state**—Link-state requests are sent to neighbors, asking for recent advertisements that have been discovered in Exchange state but not received. **Full state**—Neighbor routers are fully adjacent because their link-state databases are fully synchronized within the area. Routing tables begin to be populated.

Table 1-11 *Common OSPF Terms (Continued)*

Term	Description
Topology table	Also called the link-state table, contains every link in the entire network.
Designated router (DR)	Ensures adjacencies between all neighbors on a multiaccess network (such as Ethernet). This ensures that not all routers need to maintain full adjacencies with each other. The DR is selected based on the priority. In a tie, the router with the highest router ID is selected.
Backup DR	Designed to perform the same functions in case the DR fails.
Link-state advertisement (LSA)	A packet that contains all relevant information regarding a router's links and the state of those links.
Priority	Sets the router's priority so a DR or BDR can be correctly elected.
Router links	Describe the state and cost of the router's interfaces to the area. Router links use LSA type 1.
Summary links	Originated by Area Border Routers, these links describe networks in the AS. Summary links use LSA type 3 and 4.
Network links	Originated by DRs. Network links use LSA type 2.
External links	Originated by Autonomous System Boundary Routers; they advertise destinations external to the AS or the default route external to the AS.
Area Border Router (ABR)	Router located on the border of one or more OSPF areas to connect those areas to the backbone network.
Autonomous System Boundary Router (ASBR)	An ABR located between an OSPF autonomous system and a non-OSPF network.

The configuration steps to enable OSPF in a single area are as follows:

Step 1 Start OSPF with the command **router ospf** *process ID*. The process ID is locally significant to the router.

Step 2 Enable the interfaces with the **network** command. For example, to place the network 131.108.1.0 in area 1, the Cisco IOS command is **network 131.108.1.0 0.0.0.255 area 1**.

Step 3 Identify area assignments.

Step 4 (Optional) Assign the router ID with the **router-id** *router-id* Cisco IOS command under the OSPF process.

NOTE The following is a list of reasons OSPF (link-state) is considered a better routing protocol than RIPv1 (distance vector):

- OSPF has no hop count limitation. (RIP has a limit of 15 hops only.)
- OSPF understands VLSM and allows for summarization.
- OSPF uses multicasts (not broadcasts) to send updates.
- OSPF converges much faster than RIP because OSPF propagates changes immediately. OSPF is faster because it sends the link update and then calculates the local routing table. RIP calculates the local routing table and then sends an update.
- OSPF allows for load balancing with up to six equal-cost paths.
- OSPF has authentication available (RIPv2 does also, but RIPv1 does not).
- OSPF allows sophisticated tagging of external routes injected by other autonomous systems.
- OSPF configuration, monitoring, and troubleshooting have a far greater Cisco IOS tool base than RIP.

Multiple OSPF Areas

An OSPF area is a logical grouping of routers and links by a network administrator. OSPF routers in any area share the same topological view (also known as the OSPF or database) of the network. OSPF is configured in multiple areas to reduce routing table sizes, which in return reduces the topological database and CPU/memory requirements on a router.

Routing tables become very large even with just 50 routers. Cisco does not recommend the number of routers per area. Recommended networking design, however, typically recommends no more than 50 routers per area. The OSPF database is exchanged in full every 30 minutes, and if this database is too large, every time this occurs, the amount of bandwidth used over the network increases and can cause severe delays in sending user-based traffic because convergence times are increased.

Area assignments allow OSPF designers to limit and confine changes. Additionally, a number of predefined area types, outlined in Table 1-12, help to reduce the demand on routers.

Table 1-12 *Additional Area Types*

Area Type	Function
Stubby area	Does not accept LSA types 4 and 5, which are summary links and external link advertisements, respectively. The only way to achieve a route to unknown destinations is a default route injected by the ABR.
Totally stubby area	Blocks LSA types 3, 4, and 5. Only a single type 3 LSA advertising the default route is allowed. This solution is Cisco proprietary and is used to further reduce a topological database.
Not-so-stubby area (NSSA)	Used primarily for connections to an ISP. This area is designed to allow type 7 LSAs only. All advertised routes can be flooded through the NSSA and an ABR translates it into a type 5 LSA. Basically, a type 7 LSA (if the P bit is set to 1) is converted to a type 5 LSA and flooded through the rest of the network. The bit P is used to tell the NSSA ABR whether to translate type 7 into type 5. If the P bit is set to 0, no translation takes place. Type 4 or 5 LSAs are not permitted. This advertisement is not propagated to the rest of the network. NSSAs typically provide a default route.

Table 1-13 defines the challenges across various media types, such as Frame Relay and broadcast media.

Table 1-13 *SPF over Various Media Types Using Cisco IOS Software*

Method	Description
Point-to-point nonbroadcast	Used typically for Frame Relay interfaces.
Point-to-point	The default mode for subinterfaces.
Point-to-multipoint	Used for multiple destinations.
Nonbroadcast	Nonbroadcast multiaccess (NBMA) mode.
Broadcast	Used in Ethernet and broadcast environments where the election of DR/BDR takes place. To define the DR, use the Cisco IOS command **ip ospf priority** *priority-number*. The *priority-number* is 1 to 255. The highest priority will be to elect the DR.

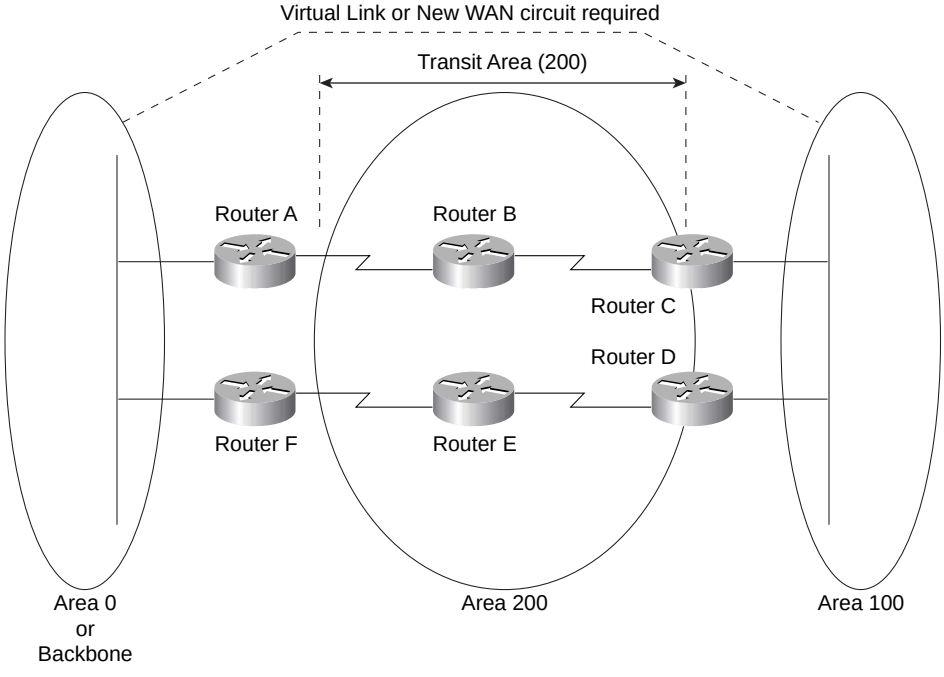
Ethernet is an example of a broadcast medium for which OSPF will elect a DR to minimize the number of OSPF updates. Each multiaccess OSPF network that has at least two attached routers has a designated router elected by the OSPF Hello protocol. The DR reduces the number of adjacencies required on a multiaccess network, which reduces the amount of routing protocol traffic and the size of the topological database, especially when more than two routers are deployed on this network segment. In a nonbroadcast multi-access (or NBMA) network, OSPF elects both a DR and a BDR. NBMA simulates a broadcast model by electing a DR and a BDR. There are two ways to simulate a broadcast model on an NBMA network: define the network type

as broadcast with the **ip ospf network broadcast** interface subcommand or configure the neighbor statements by using the **router ospf** command.

Virtual Links

All OSPF areas must be connected to the backbone area (Area 0). Figure 1-16 demonstrates a topology where an area (Area 100) is not directly connected to the backbone.

Figure 1-16 *OSPF Area Assignment*

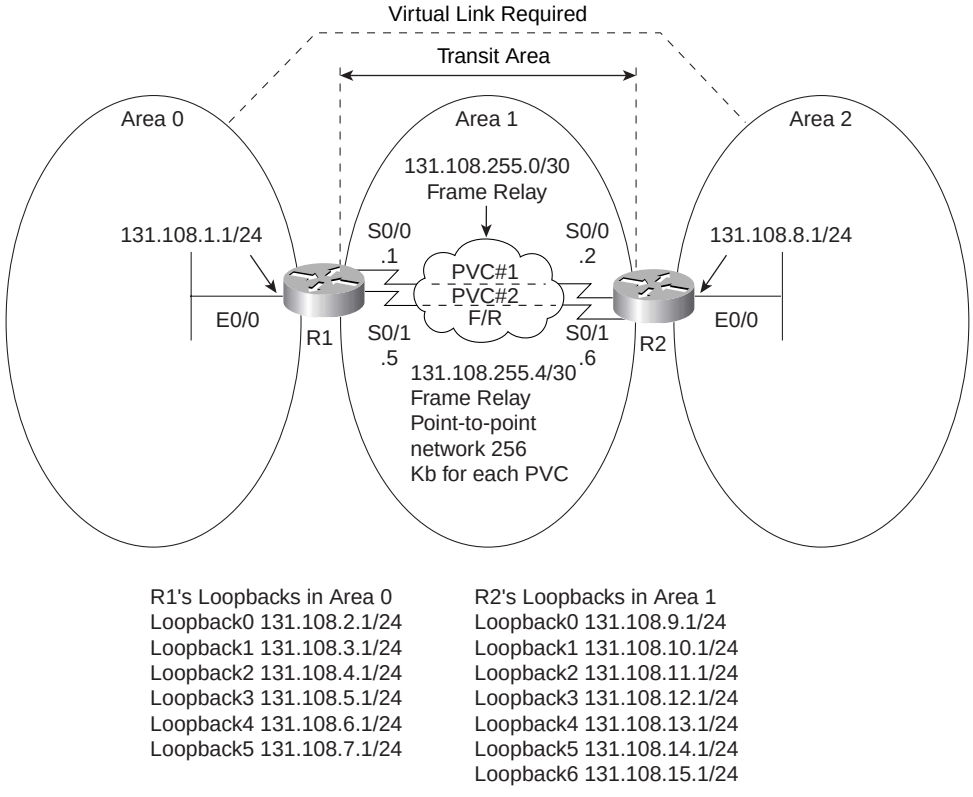


To ensure that Area 100 is reachable by the backbone, a virtual link can be configured over the transit area (200), and IP connectivity will be maintained. Virtual links are typically used in a transition phase (for example, when one company buys another and both companies use OSPF). Another solution to the problem depicted in Figure 1-16 is to install a physical link between Router C or Router D and the backbone core network.

OSPF Configuration Example

Figure 1-17 demonstrates a two-router topology and displays three OSPF areas, with Area 2 partitioned from the backbone, necessitating a virtual link.

Figure 1-17 *Typical Cisco IOS OSPF topology*



Example 1-18 displays the full working configuration of R1.

Example 1-18 *R1's OSPF Configuration*

```
!
hostname R1
enable password cisco
interface Loopback0
 ip address 131.108.2.1 255.255.255.0
 ip ospf network point-to-point
!
interface Loopback1
ip address 131.108.3.1 255.255.255.0
 ip ospf network point-to-point
!
interface Loopback2
 ip address 131.108.4.1 255.255.255.0
 ip ospf network point-to-point
!
```

continues

Example 1-18 *R1's OSPF Configuration (Continued)*

```
interface Loopback3
 ip address 131.108.5.1 255.255.255.0
 ip ospf network point-to-point
!
interface Loopback4
 ip address 131.108.6.1 255.255.255.0
 ip ospf network point-to-point
!
interface Loopback5
 ip address 131.108.7.1 255.255.255.0
 ip ospf network point-to-point
!
interface Ethernet0/0
 ip address 131.108.1.1 255.255.255.0
!
interface Serial0/0
 bandwidth 256
 ip address 131.108.255.1 255.255.255.252
 encapsulation frame-relay
 ip ospf network point-to-point
!
interface Serial0/1
 bandwidth 256
 ip address 131.108.255.5 255.255.255.252
 encapsulation frame-relay
 ip ospf network point-to-point
!
router ospf 1
 router-id 131.108.7.1
area 1 virtual-link 131.108.15.1
 network 131.108.0.0 0.0.7.255 area 0
 network 131.108.255.0 0.0.0.3 area 1
 network 131.108.255.4 0.0.0.3 area 1
!
end
```

By default, loopback interfaces are stub hosts in OSPF and are advertised as 32-bit hosts. The Cisco IOS command **ip ospf network point-to-point** advertises the loopback networks as /24 networks (in this case, you use the /24 subnet mask). The Frame Relay connection is configured as point-to-point to ensure that no manual OSPF neighbor configuration is required to form OSPF neighbors. The virtual link is configured across the transit area, 1, to the R2 router ID of 131.108.15.1.

Example 1-19 displays R2's full working configuration.

Example 1-19 *R2's OSPF Configuration*

```
hostname R2
enable password cisco
interface Loopback0
 ip address 131.108.9.1 255.255.255.0
 ip ospf network point-to-point
!
interface Loopback1
ip address 131.108.10.1 255.255.255.0
 ip ospf network point-to-point
!
interface Loopback2
 ip address 131.108.11.1 255.255.255.0
 ip ospf network point-to-point
!
interface Loopback3
 ip address 131.108.12.1 255.255.255.0
 ip ospf network point-to-point
!
interface Loopback4
 ip address 131.108.13.1 255.255.255.0
 ip ospf network point-to-point
!
interface Loopback5
 ip address 131.108.14.1 255.255.255.0
 ip ospf network point-to-point
!
interface Loopback6
 ip address 131.108.15.1 255.255.255.0
 ip ospf network point-to-point
!
interface Ethernet0/0
 ip address 131.108.8.1 255.255.255.0
 half-duplex
!
interface Serial0/0
 ip address 131.108.255.2 255.255.255.252
 encapsulation frame-relay
 ip ospf network point-to-point

interface Serial0/1
 ip address 131.108.255.6 255.255.255.252
 encapsulation frame-relay
 ip ospf network point-to-point
!
router ospf 1
```

continues

Example 1-19 *R2's OSPF Configuration (Continued)*

```
 router-id 131.108.15.1
 area 1 virtual-link 131.108.7.1
 network 131.108.8.0 0.0.0.255 area 2
 network 131.108.9.0 0.0.0.255 area 1
 network 131.108.10.0 0.0.0.255 area 1
 network 131.108.11.0 0.0.0.255 area 1
 network 131.108.12.0 0.0.0.255 area 1
 network 131.108.13.0 0.0.0.255 area 1
 network 131.108.14.0 0.0.0.255 area 1
 network 131.108.15.0 0.0.0.255 area 1
 network 131.108.255.0 0.0.0.3 area 1
 network 131.108.255.4 0.0.0.3 area 1
end
```

Example 1-20 displays the IP OSPF routing table on R1.

Example 1-20 **show ip route ospf** *on R1*

```
R1#show ip route ospf
     131.108.0.0/16 is variably subnetted, 17 subnets, 2 masks
O       131.108.15.0/24 [110/391] via 131.108.255.6, 00:00:41, Serial0/1
                        [110/391] via 131.108.255.2, 00:00:41, Serial0/0
O       131.108.14.0/24 [110/391] via 131.108.255.6, 00:00:41, Serial0/1
                        [110/391] via 131.108.255.2, 00:00:41, Serial0/0
O       131.108.13.0/24 [110/391] via 131.108.255.6, 00:00:41, Serial0/1
                        [110/391] via 131.108.255.2, 00:00:41, Serial0/0
O       131.108.12.0/24 [110/391] via 131.108.255.6, 00:00:41, Serial0/1
                        [110/391] via 131.108.255.2, 00:00:41, Serial0/0
O       131.108.11.0/24 [110/391] via 131.108.255.6, 00:00:41, Serial0/1
                        [110/391] via 131.108.255.2, 00:00:41, Serial0/0
O       131.108.10.0/24 [110/391] via 131.108.255.6, 00:00:41, Serial0/1
                        [110/391] via 131.108.255.2, 00:00:41, Serial0/0
O       131.108.9.0/24  [110/391] via 131.108.255.6, 00:00:41, Serial0/1
                        [110/391] via 131.108.255.2, 00:00:42, Serial0/0
O IA    131.108.8.0/24  [110/400] via 131.108.255.6, 00:00:42, Serial0/1
                        [110/400] via 131.108.255.2, 00:00:42, Serial0/0
```

R1's routing table has the remote OSPF networks labeled as O IA because the network 131.108.8.0/24 is part of an area not directly attached to R1. Also, R1 is automatically load balancing across the two paths because the cost metric is the same (391). The administrative distance is 110 (the default).

NOTE The election of the designated router in networks such as Frame Relay is important, and you must ensure that the hub or core network router is the elected DR so that the hub router disseminates information to all spoke routers. To ensure that the hub is the DR, you can disable the DR election process on edge routers with the Cisco IOS command **ip ospf priority 0**.

Border Gateway Protocol

BGP is an exterior routing protocol used widely on the Internet. It is commonly referred to as BGP4 (version 4).

BGP4, defined in RFC 1771, allows you to create an IP network free of routing loops between different autonomous systems. (As defined in Table 11-1, an autonomous system is a set of routers under the same administrative control.)

BGP is called a path vector protocol because it carries a sequence of autonomous system numbers that indicates the path taken to a remote network. This information is stored so that routing loops can be avoided.

BGP uses TCP as its Layer 4 protocol (TCP port 179). No other routing protocol in use today relies on TCP. This allows BGP to make sure that updates are sent reliably, leaving the routing protocol to concentrate on gathering information about remote networks and ensuring a loop-free topology.

Routers configured for BGP are typically called *BGP speakers*, and any two BGP routers that form a BGP TCP session are called *BGP peers* or *BGP neighbors*.

BGP peers initially exchange full BGP routing tables. After the exchange, only BGP updates are sent between peers, ensuring that only useful data is sent unless a change occurs.

Four message types are used in BGP4 to ensure that peers are active and updates are sent:

- **Open messages**—Used when establishing BGP peers
- **Keepalives**—Sent periodically to ensure connections are still active or established
- **Update messages**—Sent as a result of any changes that occur, such as a loss of network availability
- **Notification**—Used only to notify BGP peers of any receiving errors

Key BGP characteristics include the following:

- BGP is a path vector protocol.
- BGP uses TCP as the transport layer protocol.
- A full routing table is exchanged only during the initial BGP session.
- Updates are sent over TCP port 179.
- BGP sessions are maintained by keepalive messages.

- Any network changes result in update messages.
- BGP has its own BGP table. Any network entry must reside in the BGP table first.
- BGP has a complex array of metrics, such as next-hop address and origin, which are called attributes.
- BGP supports VLSM and summarization (sometimes called classless interdomain routing [CIDR]).

BGP4's ability to guarantee routing delivery (and the complexity of the routing decision process) is the reason that BGP is widely used in large IP routing environments, such as the Internet. The Internet consists of over 100,000 BGP network entries, and BGP is the only routing protocol available today that can handle and manage such a large routing table. The Internet (120,000+ routes) would not be functional today if BGP were not the routing protocol in use.

Before covering some simple examples, the next section describes BGP attributes.

OSPF also provides an authentication mechanism, a clear-text form, and an MD5 authentication type. MD5 authentication provides higher security than plain-text authentication. Like plain-text authentication, passwords don't have to be the same throughout an area, but they do need to be the same between neighbors. MD5 authentication uses a key ID that allows the router to reference multiple passwords, making password migration easier and more secure. For more details, search the keywords "OSPF authentication" at Cisco.com.

BGP Attributes

BGP has a number of complex attributes that determine a path to a remote network. The BGP attributes allow a greater flexibility and complex routing decision process that ensures the path to a remote network is taken , which is turn can be manipulated by the BGP designer.

The network designer can also manipulate these attributes. BGP, when supplied with multiple paths to a remote network, always chooses a single path to a specific destination. (Load balancing is possible with static routes.) BGP always propagates the best path to any peer.

BGP attributes are carried in update packets.

Table 1-14 describes the well-known and optional attributes used in BGP4.

Table 1-14 *Well-Known and Optional Attributes*

Attribute	Description
Origin	Mandatory attribute that defines the source of the path, and can be any of three different values: **IGP**—Originating from interior of the AS. **EGP**—Learned through an External Gateway Protocol. **Incomplete**—The BGP route was discovered using redistribution or static routers.
AS_Path	Describes the sequences of AS that the route has traversed to the destination IP network.
Next Hop	Describes the next-hop address taken to a remote path, typically the EBGP peer.
Local Preference	Indicates the preferred path to exit the AS. A higher Local Preference is always preferred. This is local to the AS and exchanged between IBGP peers only.
Multi-Exit Discriminator (MED)	Informs BGP peers in other autonomous systems about which path to take into the AS when multiple autonomous systems are connected. A lower MED is always preferred.
Weight	Cisco-defined attribute that is used in local router selection. Weight is not sent to other BGP peers, and a higher Weight value is always preferred. Weight is locally significant to the router and specifies a preferred path when more than one path exists. Cisco-only attribute.
Atomic Aggregate	Advises BGP routers that route aggregation has taken place. Not used in route selection process.
Aggregator	The router ID responsible for aggregation; not used in the route selection process.
Community	A transitive, optional attribute in the range 0 to 4,294,967,200 that provides a way to group destinations in a certain community and apply routing decisions (accept, prefer, redistribute, etc.) according to those communities.
Originator ID	Prevents routing loops. This information is not used for route selection. The Originator ID is generated by a route reflector, and the route reflector must never send routing information back to the router specified in the Originator ID.
Cluster-List	Used in a route-reflector's environment. This information is not used for route selection.

There are two types of BGP sessions: internal BGP (IBGP) and external BGP (EBGP). IBGP is a connection between two BGP speakers in the same autonomous system. EBGP is a connection between two BGP speakers in different autonomous systems.

IBGP peers also make sure that routing loops cannot occur, by ensuring that any routes sent to another autonomous system must be known via an interior routing protocol, such as OSPF, before sending that information. That is, the routers must be synchronized. The benefit of this added rule in IBGP TCP sessions is that information is not sent unless it is reachable, which reduces any unnecessary traffic and saves bandwidth. Route reflectors in IBGP ensure that large, internal BGP networks do not require a fully meshed topology. Route reflectors are not used in EBGP connections. A BGP route reflector disseminates routing information to all route-reflector clients, and ensures that BGP tables are sent and that a fully meshed IBGP need not be configured.

The BGP routing decision is quite complex and takes several attributes into account. The attributes and process taken by a Cisco router running BGP4 are as follows:

1. If the next-hop address is reachable, consider it; if it is unreachable, ignore it.
2. Prefer the route with the highest weight (Cisco IOS routers only).
3. If the weight is the same, prefer the largest Local Preference attribute.
4. If the local preference is the same, prefer the route originated by this local router (routes generated by **network** or **redistribute** commands).
5. Then, prefer the route with the shortest AS_Path.
6. If the AS_Path length is the same, prefer the route with the lowest origin type.
7. If the origin codes are the same, prefer the route with the lowest MED.
8. If the MED is the same, prefer EBGP over IBGP.
9. Then, prefer the path with the lowest IGP metric.
10. Finally, if all else is equal, prefer the path with the lowest BGP router ID.

Configuring BGP

To start the BGP process on a Cisco router requires the following command:

```
router bgp autonomous-system-number
```

To define networks to be advertised, apply the following command:

```
network network-number mask network-mask
```

You must be aware that the **network** commands is not used in the same way that you apply **network** commands in OSPF or EIGRP. With BGP, the **network** command advertises networks

that are originated from the router and should be advertised via BGP. For more Cisco IOS examples of BGP, see Chapter 8, "CCIE Security Self-Study Lab." The BGP **network** command does not affect for which interfaces BGP is enabled. Also, BGP routes that originate from a BGP-enabled device can include connected routes, static routes, and routes learned from a dynamic routing protocol.

To identify peer routers, apply the following command:

```
neighbor {ip-address | peer-group name} remote-as autonomous-system-number
```

NOTE Route redistribution allows routing information discovered through one routing protocol to be distributed in the update messages of another routing protocol. Whenever redistribution is configured on Cisco routers, the routing metric must also be converted. For example, with redistribution from a RIP domain into OSPF, the RIP network inserted into OSPF requires an OSPF cost metric.

BGP neighbor authentication can be configured whenever routing updates are exchanged between neighbor routers. This authentication ensures that a router receives reliable routing information from a trusted source. BGP supports MD5 authentication only. If a firewall exists between two neighboring BGP routers, the firewall cannot NAT the BGP router addresses because it breaks the MD5 hash. It is important to remember that BGP runs over TCP, with the well-known TCP port number 179.

Integrated Services Digital Network

ISDN is a digital service that enables network users to send and receive data, voice, and video transmissions over a network. ISDN offers a variety of link speeds, ranging from 64 kbps to 2.048 Mbps (including a signaling channel of 64 kbps). With the advent of DSL and cable, ISDN may not be a viable network solution for anything other than a backup link, because of the expense involved.

Basic Rate and Primary Rate Interfaces

ISDN can be supplied by a carrier in two main forms: Basic Rate Interface (BRI) and Primary Rate Interface (PRI). An ISDN BRI consists of two 64-kbps services (B channels) and one 16-kbps signaling channel (D channel). An ISDN PRI consists of 23 B or 30 B channels, depending on the country. In North America and Japan, a PRI service consists of 23 B channels. In Europe and Australia, a PRI service consists of 30 B channels. A signaling channel (or D channel) is used in a PRI service and is a dedicated 64-kbps channel. The B channel sends data and the D channel primarily controls signaling.

NOTE The effective throughput of a PRI service with 23 channels is 1.472 Mbps (23 × 64 kbps). With 30 B channels, the effective throughput is 1.920 Mbps (30 × 64 kbps). The International Telecommunications Union (ITU) defines the standards for ISDN. The specified standard is ITU-T Q.921.

ISDN Framing and Frame Format

The ISDN physical layer provides the ability to send outbound traffic and receive inbound traffic by transmitting binary bits over the physical media. The ISDN data link layer provides signaling, which ensures that data is sent and received correctly. The signaling protocol used in ISDN is called the Link Access Procedure on the D channel (LAPD).

ISDN Layer 2 Protocols

ISDN can use a number of Layer 2 encapsulation types. Point-to-Point Protocol (PPP) and High-Level Data Link Control (HDLC) are the only methods tested in the qualification exam.

NOTE X.25 is not tested in the CCIE Security written exam.

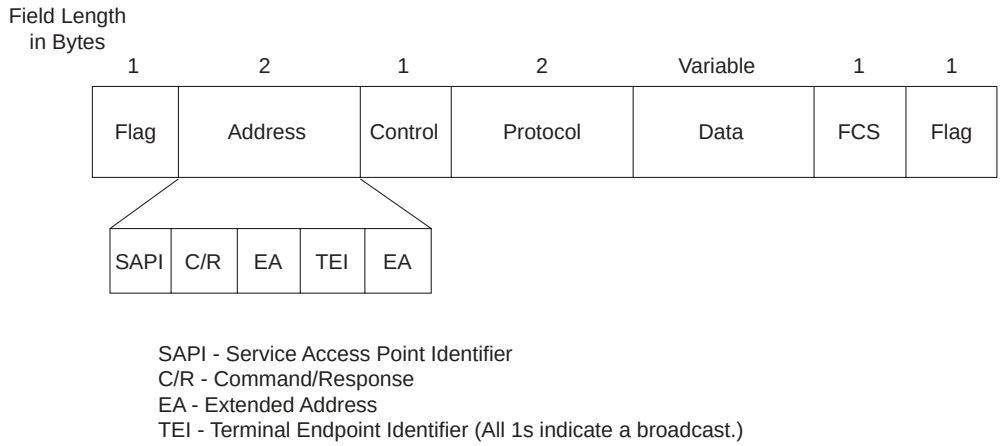
High-Level Data Link Control

HDLC is a WAN protocol encapsulation method that allows point-to-point connections between two remote sites. Typically, HDLC is used in a leased-line setup. HDLC is a connectionless protocol that relies on upper layers to recover any frames that have encountered errors across a WAN link. HDLC is the default encapsulation on Cisco serial interfaces.

Cisco routers use HDLC encapsulation, which is proprietary. Cisco added an address field in the HDLC frame, which is not present in the HDLC standard. This field is used by Cisco devices to indicate the type of payload (protocol). Cisco routers use the address field in an HDLC frame to indicate a payload type, but other routers or manufacturers that implement the HDLC standard do not use the Address Field. Hence, HDLC support between vendors is not supported. HDLC cannot be used to connect a Cisco router with another vendor.

Figure 1-18 displays the HDLC frame format, which shares a common format with the PPP frame format discussed in the next section. HDLC has no authentication mechanism.

Figure 1-18 *HDLC Frame Format*



Point-to-Point Protocol

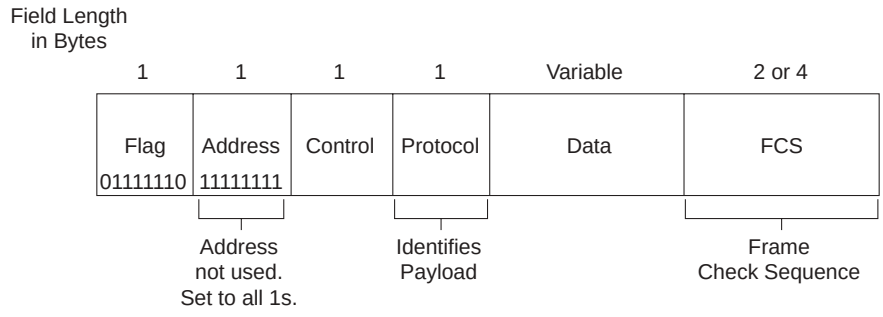
PPP was designed to transport user information between two WAN devices (also referred to as point-to-point links). PPP was designed as an improvement over the Serial Line Internet Protocol (SLIP). When PPP encapsulation is configured on a Cisco WAN interface, the network administrator can carry protocols such as IP and IPX, as well as many others. Cisco routers support PPP over asynchronous lines, High-Speed Serial Interfaces (HSSIs), ISDN lines, and synchronous serial ports. PPP has the added function of allowing authentication to take place before any end-user data is sent across the link.

The following three phases occur in any PPP session:

- **Link establishment**—Link Control Protocol (LCP) packets are sent to configure and test the link.
- **Authentication (optional)**—After the link is established, authentication can ensure that link security is maintained.
- **Network layers**—In this phase, Network Control Protocol (NCP) packets determine which protocols are used across the PPP link. An interesting aspect of PPP is that each protocol (IP, IPX, and so on) supported in this phase is documented in a separate RFC that discusses how it operates over PPP.

Figure 1-19 displays the PPP frame format, which is similar to the HDLC frame format in Figure 1-18.

Figure 1-19 *PPP Frame Format*



Link Control Protocol

LCP is used to establish, configure, and test the link between two devices, such as Cisco routers. LCP provides the necessary negotiations between end devices to activate the link. After the link is activated, but before data is flowing, the next phase of the PPP session, authentication (if configured), can take place.

Authentication

PPP supports authentication through the Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP), with CHAP providing a more secure method of authentication. CHAP passwords are encrypted and safe from intruders because they are never actually transmitted on the wire. This technique, known as shared secrets, means that both devices know the secret (password), but they never talk about it directly. PAP passwords are sent in clear text; they are clearly visible on the wire.

Network Control Protocol

PPP uses NCP packets to allow multiple network layer protocol types to transfer across WANs from point to point. IP Control Protocol (IPCP) allows IP connectivity, and IPXCP allows IPX connectivity. NCP establishes and configures the network layer protocol, such as IP.

Cisco IOS ISDN Commands

Cisco routers support ISDN. The commands most often used to enable data and voice communications over ISDN are listed in Table 1-15.

Table 1-15 *ISDN Commands*

Cisco IOS Command	Description
isdn caller *phone-number*	The number called by the router. The *phone-number* is the remote router's ISDN number.
Cisco IOS Command	**Description**
isdn calling-number *calling-number*	The number of the device making the outgoing call; only one entry is allowed.
isdn switch-type	ISDN service provider switch type.
isdn spid1 *number number*	Some service providers use service profile identifiers (SPIDs) to define the services subscribed to by the ISDN device that is accessing the ISDN service provider. This is an optional command.

NOTE Frame Relay is a Layer 2 protocol that provides connectionless delivery between devices.

Frame Relay, although not listed in the official blueprint for the CCIE Security written exam, has a few terms you should be aware of for the exam:

- **Forward explicit congestion notification (FECN)**—A bit set by a Frame Relay network to inform DTE receiving the frame that congestion was experienced in the path from source to destination. DTE receiving frames with the FECN bit set can request that higher-level protocols take flow-control action, as appropriate.
- **Backward explicit congestion notification (BECN)**—A bit set by a Frame Relay network in frames traveling in the opposite direction of frames encountering a congested path. DTE receiving frames with the BECN bit set can request that higher-level protocols take flow-control action, as appropriate. The ISP or WAN switches typically set FECN/BECN.
- **Data-link connection identifier (DLCI)**—A value that specifies a PVC or SVC in a Frame Relay network. DLCIs are locally significant. Globally significant DLCIs are used for LMI (Local Management Interface) communication between Frame Relay switches.

IP Multicast

This section briefly covers the IP multicast areas of interest for the CCIE written test.

The multicasting protocol was designed to reduce the high bandwidth requirements of technologies, such as video on demand, to a single stream of information to more than one device. Applications include electronic learning, company share meetings (video on demand), and software distribution.

Multicasting transmits IP packets from a single source to multiple destinations. The network device transmitting the multicast source copies single packets, which are sent to a subset of

network devices. In IPv4, the Class D addresses ranging from 224.0.0.0 to 239.255.255.255 are reserved for multicast. Routing protocols, for example, use multicasting to send Hello packets and establish neighbor adjacencies.

Table 1-16 displays some common multicast addresses and their uses.

Table 1-16 *Class D Multicast Address Examples*

Multicast Address	Use
224.0.0.1	All hosts on subnets
224.0.0.2	All multicast routers
224.0.0.5	All OSPF-enabled routers
224.0.0.6	All OSPF DR routers
224.0.0.9	All RIPv2-enabled routers
224.0.0.10	All EIGRP-enabled routers

TIP The Class D addresses used in multicast traffic range from 224.0.0.0 to 239.255.255.255.

Asynchronous Communications and Access Devices

An asynchronous (async) communication is a digital signal that is transmitted without precise clocking. The RS-232 session between a router and PC through the console connection is an example of async communications. Such signals generally have different frequencies and phase relationships. Asynchronous transmissions usually encapsulate individual characters in control bits (called start and stop bits) that designate the beginning and the end of each character.

For example, the auxiliary port on Cisco routers can be used to connect a modem and allow out-of-band (not via the network) management.

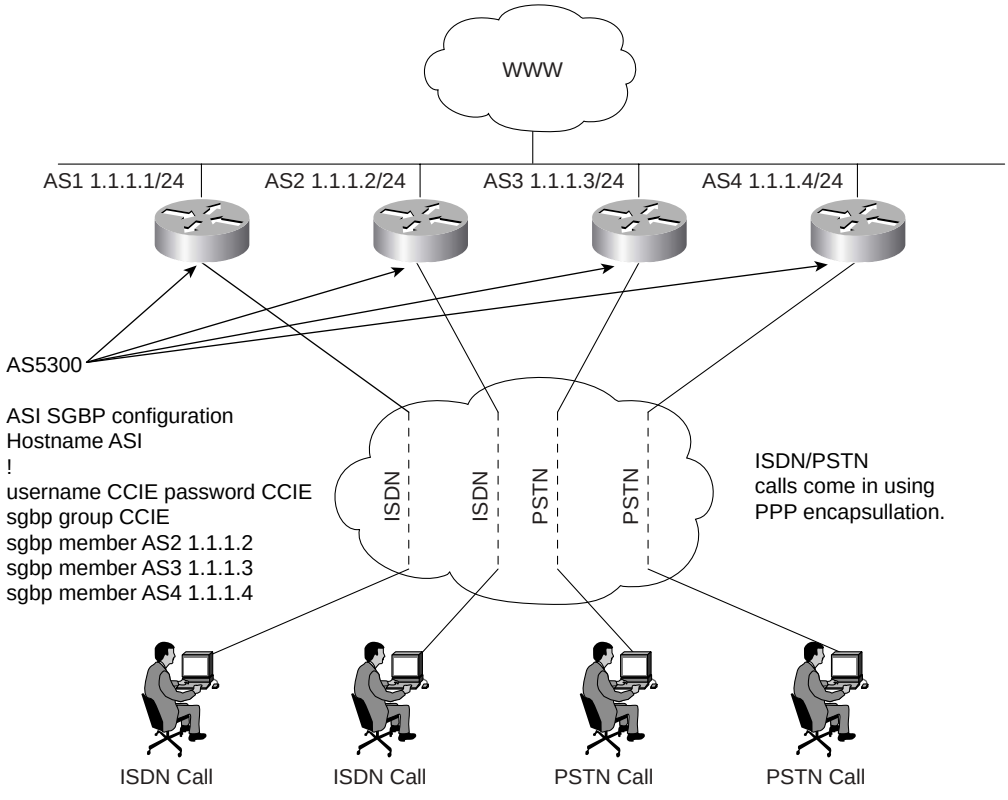
The Cisco AS5300 is an example of a device that supports both synchronous and async communication, such as voice, digital, and modem-based traffic (via a Public Switched Telephone Network [PSTN]).

The AS5300, or universal access server, is a versatile data communications platform that provides the functions of an access server, router, and digital modem in a single modular chassis. The access server is intended for ISPs, telecommunications carriers, and other service providers that offer managed Internet connections. The AS5300 provides both digital (for example, ISDN) and analog (dialup users using PSTN) access to users on a network.

Figure 1-20 displays a typical scenario where clients, such as Internet dialup users with ISDN and analog phone lines (PSTN), can connect to the Internet using PPP.

Clients are supplied one number to call, and the AS5300 makes intelligent decisions based on the incoming call type, whether it be digital (ISDN) or analog (PSTN).

Figure 1-20 *AS5300 Typical Design Scenario*



Users, such as clients with ISDN, call the dedicated number supplied by the ISP. The four AS5300s in Figure 1-20 can also share the load of incoming calls using the Stack Group Bidding Protocol (SGBP), which is used when multiple PPP, or multilink PPP (MPPP), sessions are in use. When SGBP is configured on each Cisco AS5300, each access server sends a query to each stack group member. A stack group member is a router running SGBP.

Each router participating in SGBP then bids for the right to terminate the call. The router with an existing PPP session, for example, will win the bid; this allows the best bandwidth allocation to the end client, as both PPP sessions are terminated on the same router. If the PPP call is the first session to be terminated on the AS5300, the AS5300 with the lowest CPU usage will have a higher probability of terminating the call. Example 1-21 displays a typical Cisco IOS configuration when SGBP is enabled on the four AS5300 routers in Figure 1-20.

Example 1-21 *SGBP Configuration Example*

```
Hostname AS1
!
username CCIE password CCIE
sgbp group CCIE
sgbp member AS2 1.1.1.2
sgbp member AS3 1.1.1.3
sgbp member AS4 1.1.1.4
```

The following list explains the Cisco IOS commands used in Example 1-21.

- **username CCIE password CCIE**—Defines the username and password used to authenticate SGBP members. If the password is wrong, an error such as the following is presented on the console:

  ```
  %SGBP-1-AUTHFAILED: Member [chars] failed authentication
  ```

- **sgbp group CCIE**—Defines a named stack group and makes this router a member of that stack group. Use the **sgbp group** command in global configuration mode. To remove the definition, use the **no** form of this command.

- **sgbp member** *ip-address*—Specifies the host name and IP address of a router or access server that is a peer member of a stack group. Use the **sgbp member** command in global configuration mode.

Telephony Best Practices

IP networks are a prime target for intruders and hackers. Traditionally, voice networks were secure because the PBXs in place did not have any IP connectivity. In today's Voice over IP (VoIP) telephony-based networks, every IP phone contains a routable IP address and thus is a prime target. For example, a hacker could program the Cisco Call Manager (CCM) to make every IP phone call the number 911 (or 000, depending on what part of the world you are in). If you do not secure the voice networks from attacks like these, then not only is your IP data network a potential target, but so is your VoIP network. It must also be stressed that legacy phone networks are subjected to toll fraud very easily. Having said that, VoIP also is subject to loss of privacy, loss of integrity, impersonation, and denial of service. Latest hardware releases by Cisco and the Integrated Services Routers (ISR) platforms have addressed these issues somewhat with new Cisco IOS Software.

This section covers some of the core recommendations made by the "SAFE: IP Telephony Security in Depth" white paper, which can be viewed at http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a00801b7a50.shtml. The CCIE Security written exam covers this subject only very lightly; in fact, the lab portion of the exam does not even test VoIP best practices as of this writing. This section ensures that you

understand the details that are required for the written exam, knowledge of which will also help you in the real world.

Establishing the identity of every IP phone is the key to VoIP security. The handset identifies itself with the CCM via the MAC address. If auto registration is enabled on the CCM, then any rogue IP phone can be installed and operated. Thus, you should disable auto registration or place the phone in a partition whereby only local internal calls can be made, for instance. You should also disable the switched port to the PC until the phone is correctly identified and reregistered with the correct access rights, such as a calling search space (CSS).

A CSS comprises an ordered list of route partitions (logical groupings of directory numbers and route patterns, not to be confused with IP routing) that is typically assigned to devices such as IP phones. CSSs determine the partitions where calling devices search when they are attempting to complete a call. If an intruder places a rogue device in an incorrect partition, then that intruder could potentially call any number around the globe and discover the IP subnet the phone is allocated, the CCM, the DHCP server, the TFTP server, and so forth. The intruder can simply press the Settings button on the phone and select Network Configuration to view the IP address of these core devices, such as the CCM's IP address. This information can then be used to attach to the main component of a VoIP network—the CCM(s).

A common best practice is to disable all unused network ports in a switched Layer 2 environment; this prevents deployment of any rogue IP phones. You could also consider statically defining IP addresses so that DHCP does not allocate a valid routable IP address in your network to rogue IP phones. You can secure the network by placing phones in a voice VLAN (isolated, that is) and permitting only that particular VLAN access to the CCM and associated servers and ports. In this way, you can enable DHCP for IP phones.

This leads to the best practice of all—securing the network where the CCMs reside. The call processing of VoIP networks means that the RTP stream is vital and can be hijacked by potential intruders. Call gateways and CCMs are the most vulnerable devices in your network. Hence, Cisco advises that you use network intrusion detection systems, along with well-defined access lists, to ensure that the core devices in your VoIP are secure.

The "SAFE: IP Telephony Security in Depth" white paper recommends the following for all VoIP installations:

- Use host-based virus checking. This is common antivirus software.
- Use a host-based IDS (HIDS). Cisco Security Agent network shimmy needs to be installed.
- Use network-based intrusion detection systems (NIDSs).

- Prevent toll fraud by not allowing unregistered phones to register. Typically, implementations leave auto registration in place although unregistered phones are placed in a partition. This partition can be configured to permit only internal calls, for example, thus preventing toll fraud.
- Prevent denial of service (DoS) attacks by using separate voice and data networks.
- Use access lists to prevent unauthorized access.

Table 1-17 defines the common TCP and UDP ports used in an IP telephony environment when deploying access list security.

Table 1-17 *Common TCP/UDP Ports in VoIP*

Application	Protocol	Port(s)
DHCP	UDP	67/68
HTTP	TCP	80
RTP	UDP	16384–32767
TAPI/JTAPI (Softphone if present)	TCP	2748
Cisco Softphone Directory Lookup	TCP	389/8404
Cisco skinny	TCP	2000
HIDS management	TCP	5000
Directory access (DCD)	TCP	8404

IDSs can be easily deployed in chassis-based switches, making their integration fairly easy, as discussed in Chapter 5, "Operating Systems and Cisco Security Applications."

Other common best practices include securing Internet Information Server (IIS) on the CCMs, disabling Windows services, locking down SQL, and using IPS and virus protection on CCMs.

Cisco has recently released IP wireless phones. Any network that has VoIP installed must secure the wireless networks as well, as the following section discusses.

Wireless Best Practices

Cisco Architecture for Voice, Video and Integrated Data (AVVID) also contains details on best practices for wireless networks. As wireless networks grow around the globe, Cisco intends to ensure that you can connect wherever you are, 24 hours a day, thereby boosting your connectivity to the workplace. This means, of course, that connectivity is required in areas where there are no cables, such as cafés, airplanes, street corners, and hotel lobbies.

Wireless networks have become one of the most interesting targets for hackers. Wireless technology deployment is growing at a rapid rate, and sometimes without consideration of all security aspects. This rapid deployment is due, in part, to the low cost of the devices, ease of deployment, and the large productivity gains. Because WLAN devices ship with all security features disabled, increasingly, WLAN deployments have attracted the attention of the hacker community. Several websites document freely available wireless connections throughout the United States.

Although most hackers are using these connections as a means to get free Internet access, a smaller group, using more sophisticated tools to capture data, modify data, capture passwords, or to hide their identity, sees this situation as an opportunity to break into networks that otherwise might have been difficult to attack from the Internet. Unlike a wired network (Ethernet for example), a WLAN sends data over the air and may be accessible outside the physical boundary of an organization. Power settings should be used, for example, to ensure that only the secure building floors have coverage and not café shops on the ground level.

When WLAN data is not encrypted, the packets can be viewed by anyone within radio frequency range. For example, a person with a Linux laptop, a WLAN adapter, and a program such as TCPDUMP can receive, view, and store all packets circulating on a given WLAN.

Vendors are constantly updating and providing new mechanisms to thwart hackers, such as with protocols like the following:

- **Extensible Authentication Protocol (EAP)**—Provides enhanced functionality by allowing wireless client adapters, which may support different authentication types, to communicate with different back-end servers such as RADIUS
- **Lightweight Extensible Authentication Protocol (LEAP)**—The Cisco implementation of EAP, based on the IEEE 802.1x authentication framework

To support all popular operating systems, Cisco designed and implemented LEAP on Cisco Aironet WLAN products and solutions. Microsoft's latest operating system, Windows XP, provides support for 802.1x (specifically EAP-TLS and EAP MD5). Thus, a variety of EAP authentication protocols can be used to authenticate users in today's WLAN networks.

The Cisco AVVID WLAN solution is a fundamental element of the Cisco AVVID network infrastructure. This means that there are few or no cables. What is still required, of course, is network security. This section covers the main methods used to ensure that wireless networks are secure when they are implemented and designed and that common best practices are used in today's wireless LANs. The need for security must also be balanced with users' need for maximum flexibility when accessing a corporate or public network.

This section also ensures that you have all the information that you need to answer the questions that may appear on the CCIE Security written exam.

The IEEE has defined a number of wireless standards, the most important of which are the following:

- **802.11a**—Standard for the 5.0-GHz UNI band (22 Mbps)
- **802.11b**—Standard for the 2.4-GHz UNI band (11 Mbps)
- **802.11g**—Standard for higher speeds (54 Mbps)

Cisco has implemented the following wireless LAN security features in its access points and bridges:

- Dynamic or static Wired Equivalent Privacy (WEP) key management.
- 802.1x user authentication, which is covered in Chapter 4, "Security Protocols."
- Enhancement beyond the IEEE recommendations, such as dynamic WEP keys to prevent WEP spoofing. Other enhancements include Message Integrity Check (MIC) and the Temporal Key Integrity Protocol (TKIP), also covered in Chapter 4.
- Wi-Fi Protected Access (WPA) support.

NOTE For more details on Cisco wireless enhancements, visit http://www.cisco.com/en/US/products/hw/wireless/ps5279/prod_bulletin09186a00802134a9.html.

WEP is an 802.11 standard that describes the communication that occurs in wireless LANs. The WEP algorithm is used to protect wireless communications from eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network; this function is not an explicit goal in the 802.11 standard, but it is frequently considered to be a feature of WEP. WEP uses the RC4 encryption algorithm, which is known as a stream cipher.

There are some very common best practices that you should consider when deploying wireless networks:

- Use dynamic, per-user, per-session key enhancements to mitigate a variety of passive attacks. Enhancements detect and drop packets that have been (maliciously) modified in transit.
- Deploy authentication between the client and user. This may connect to a RADIUS server or, for example, may need to authenticate through a firewall. The authentication is still only between the client and the access point.

- Use rekeying policies that can be centrally configured by external servers such as an AAA server. This allows the secret key rotation to occur transparently to end users. Customers can also configure broadcast key rotation policies at the access points.
- Keep accounting records. Every time a wireless client associates with an access point or disassociates from an access point, a record should be kept for auditing purposes.
- Use TKIP to defend against an attack on WEP in which the intruder uses an unencrypted segment called the initialization vector (IV) in encrypted packets to calculate the WEP key. TKIP removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs. TKIP protects both unicast and broadcast WEP keys. TKIP still requires the WEP key to be changed every 16.7 million packets.
- Use MIC to prevent attacks on encrypted packets, called *bit-flip attacks.* During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. MIC, implemented on both the access point and all associated client devices, adds a few bytes to each packet to make the packets tamper proof.
- Use EAP authentication, which provides dynamic unicast WEP keys for client devices but uses static broadcast keys. With broadcast WEP key rotation enabled, the bridge provides a dynamic broadcast WEP key and changes it at the interval you select. Broadcast key rotation should be used with TKIP. If the wireless clients do not support TKIP, using broadcast key rotation just means that the client keys get hacked first.

Intruders typically use a number of tools, freely available on the Internet, to sniff out the airwaves for access points. Thus, it is vital that you make sure every wireless access point in your network has the most secure features enabled. Some common tools include:

- **MAC address auditing**—A device is placed on the network and pings a number of local devices and caches the MAC. The intruder can then, for example, configure their NIC to receive packets for devices acting as the gateway and thereby redirect them to the wrong location.
- **Sniffers**—By using a simple network monitor, of which many are available on the Internet, such as Ethereal, an intruder can sniff packets over the airwaves by using any wireless adapter.
- **Operating system imperfections**—By using the fingerprint of Windows and Cisco IOS, intruders can discover weaknesses in the code to develop tools to bypass internal security. Recent reports of code thefts from Cisco and Microsoft have further heightened this flaw. Examples of tools freely available on the Internet include Airsnort, Asleap, and Network Stumbler.

- **Disable SSID broadcast**—Not allowing the SSID to broadcast protects against someone gaining unauthorized association. Although the SSID is not for security, it is a simple means of access control.

This section discussed in brief some of the main points you should consider when designing a wireless network. Simple practices such as dynamic key management, deploying authentication between a client and access point, and enabling 802.1X authentication encompass the crucial wireless best practices.

There are more wireless security features available to administrators:

- Using access control between wired and wireless networks
- Suppressing broadcast SSIDs
- Deploying multiple VLANs across various wireless networks
- Providing firewall protection between wired and wireless networks

802.11 networks are insecure, and only careful design and monitoring will ensure that your IP network is not compromised. Prevention and detection are the keys to a safe wireless network.

Prevention is best designed with these points in mind:

- Corporate policy
- Physical security
- Supported WLAN infrastructure
- 802.1x port-based security on edge switches

Detection is best designed with these practices in mind:

- Using wireless analyzers or sniffers
- Using scripted tools on the wired infrastructure
- Physically observing WLAN access point placement and usage
- Implementing various levels of VLAN support for various levels of wireless access—for example, ensuring that users who are permitted only Internet access are not placed on corporate LAN-based networks

For more details on common best practices in wireless technologies, refer to the "SAFE: Wireless LAN Security in Depth – version 2" white paper:

http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008009c8b3.shtml

Foundation Summary

The "Foundation Summary" is a condensed collection of material for a convenient review of this chapter's key concepts. If you are already comfortable with the topics in this chapter and decided to skip most of the "Foundation Topics" material, the "Foundation Summary" will help you recall a few details. If you just read the "Foundation Topics" section, this review should help further solidify some key facts. If you are doing your final preparation before the exam, the "Foundation Summary" offers a convenient and quick final review.

Table 1-18 *OSI Model*

OSI Name and Layer Number	Description
Application layer (Layer 7)	The application layer is closest to the end user, which means that the application is being accessed by the end user. This layer's major function is to provide services to end users. Examples of application layer services include the following: • File Transfer Protocol • Telnet • Ping • Trace route • SMTP • Mail clients
Presentation layer (Layer 6)	The presentation layer handles data formats and code formatting. This layer's functions are normally transparent to the end user because it takes care of code formats and presents them to the application layer, where the end user can examine the data. Examples of presentation layer protocols include the following: • GIF • JPEG • ASCII • MPEG • TIFF • MIDI • HTML

continues

Table 1-18 *OSI Model (Continued)*

OSI Name and Layer Number	Description
Session layer (Layer 5)	The session layer performs several major functions, including managing sessions between devices and establishing and maintaining sessions. Examples of session layer protocols include the following: • Database SQL • NetBIOS Name Queries • H.323
Transport layer (Layer 4)	The transport layer is responsible for segmenting upper-layer applications and establishing end-to-end connections between devices. Other transport layer functions include providing data reliability and error-free delivery mechanisms. Information being processed at this layer is processed in what are commonly known as segments. Examples of transport layer protocols include Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Voice RTP resides here also.
Network layer (Layer 3)	The network layer determines the best path to a destination. Device addressing, packet fragmentation, and routing all occur at the network layer. Information at this layer is processed in what are commonly known as packets. Examples of network layer protocols include the following: • Internet Protocol (IP) • Open Shortest Path First (OSPF) • Cisco Enhanced Interior Gateway Routing Protocol (EIGRP)
Data link layer (Layer 2)	The data link layer focuses on getting data reliably across any particular kind of link. Flow control and error notifications are other data link layer functions. The data link layer applies to all access methods, whether they are LAN or WAN methods. Information being processed at this layer is processed in what are commonly known as frames. Examples of correct frame types include the following: • ISDN • SDLC • HDLC • PPP • Frame Relay • Bridge protocol data units (spanning tree)

Table 1-18 *OSI Model (Continued)*

OSI Name and Layer Number	Description
Physical layer (Layer 1)	The physical layer consists of standards that describe bit ordering, bit transmission rates, connector types, and electrical and other specifications. Information at Layer 1 is transmitted in binary (1s and 0s; for example, the letter *A* is transmitted as 00001010). Examples of physical layer standards include the following: • RS-232 • V.24 • V.35 • RJ-45 • RJ-12 • 10BASE-T • 100BASE-T • 1000BASE-T • Gigabit Ethernet

Table 1-19 *Ethernet Media Formats*

Media Type	Characteristics
10BASE5*	• Maximum length: 500 m • Maximum stations: 1024 • Speed: 10 Mbps • Minimum distance between devices: 2.5 m
10BASE2	• Maximum length: 185 m, using RG58 cable types and T connectors on all end stations • Minimum distance between devices: 0.5 m • Maximum devices per 185 m segment: 30 stations • Speed: 10 Mbps
10BASE-T	• Based on UTP cabling • Up to 100 m; better-category cables longer • One device per cable; typically, only one device per segment with hubs or switches connecting all devices together • Speed: 10 Mbps • Physical topology: star • Logical topology: bus

continues

Table 1-19 *Ethernet Media Formats (Continued)*

Media Type	Characteristics
100BASE-T	• Same characteristics as 10BASE-T but operates faster, at 100 Mbps • Can be fiber, as well (100BASE-FX); defined in IEEE 802.3U • Physical topology: star • Logical topology: bus
1000 GE	• Gigabit Ethernet operating at 1000 Mbps • Can run over fiber or UTP; frame formats and CSMA/CD identical to Ethernet standards • Physical topology: star • Logical topology: bus

*The word BASE refers to baseband signaling, which uses a single channel, as opposed to broadband, which uses multiple frequency channels.

- All ports part of FEC must be set to the same speed.
- All ports must belong to the same VLAN.
- Duplex must be the same (half or full), not a mixture.
- Up to eight ports can be bundled together.
- To set FEC on a switch, the CatOS syntax is **set port channel**.
- To set Fast EtherChannel on a router, the Cisco IOS syntax is **channel-group** under the Fast Ethernet interface.

Table 1-20 *The States of Spanning Tree*

Bridge Port State	Description
Disabled	The port is not participating in spanning tree and is not active.
Listening	The port has received data from the interface and will listen for frames. In this state, the bridge only receives data; it does not forward any frames to the interface or to other ports.
Learning	The bridge still discards incoming frames. The source address associated with the port is added to the CAM table. BPDU are sent and received.
Forwarding	The port is fully operational; frames are sent and received.
Blocking	The port has been through the learning and listening states, and because this particular port is a dual path to the root bridge, the port is blocked to maintain a loop-free topology.

Table 1-21 *Class A, B, C, D, and E Ranges**

Class of Address	Starting Bit Pattern	Range	Default Subnet Mask
Class A	0xxxxxxx	1–126, 127**	255.0.0.0
Class B	10xxxxxx	128–191	255.255.0.0
Class C	110xxxxx	192–223	255.255.255.0
Class D	1110xxxx	224–239	Not officially defined
Class E	1111xxxx	240–255	Reserved

*Only Class A, B, and C have predefined default subnet masks.

**127.0.0.0 is reserved for loopback purposes. Other reserved addresses for private use as defined by RFC 1918 are as follows:

10.0.0.0–10.255.255.255

172.16.0.0–172.31.255.255

192.168.0.0–192.168.255.255

Table 1-22 *Routing Protocol Classifications*

Routing Protocol	Class
IGRP	Distance vector (classful)
EIGRP	Hybrid (classless)
OSPF	Link-state (classless)
RIPv1	Distance vector (classful)
RIPv2	Distance vector (classless)
BGP	Path vector (classless)

Table 1-23 *TCP Flags Summary*

Flag	Description
URG (U)	Urgent—Informs the other station that urgent data is being carried. The receiver will decide what to do with the data.
ACK (A)	Acknowledge—Indicates that the packet is an acknowledgment of received data, and the acknowledgment number is valid.
PSH (P)	Push—Informs the end station to send data to the application layer immediately.
RST (R)	Reset—Resets an existing connection.
SYN (S)	Synchronize—Initiates a connection.
FIN	Finished—Indicates that the sender is finished sending data and terminates the session.

Table 1-24 *TCP/IP Common Applications*

Application	Description
Address Resolution Protocol (ARP)	Maps an IP address to a MAC address.
Reverse Address Resolution Protocol (RARP)	Determines a host's IP address when the MAC address is known.
Dynamic Host Configuration Protocol (DHCP)	Dynamically provides IP addresses to TCP/IP hosts, subnet masks, and gateway addressing. Many other IP options can be assigned, as well.
Hot Standby Router Protocol (HSRP)	Redundancy gateway protocol, Cisco proprietary.
Internet Control Message Protocol (ICMP)	A network layer (Layer 3) Internet protocol that reports errors and provides other information relevant to IP packet processing. ICMP is fully documented in RFC 792.
Telnet	TCP/IP application layer protocol that enables remote management of TCP/IP hosts, such as routers or switches.
File Transfer Protocol (FTP)	TCP/IP application layer protocol that enables file transfer between TCP/IP hosts using a TCP, connection-orientated protocol.
Trivial File Transfer Protocol (TFTP)	TCP/IP application layer protocol that enables file transfers between TCP/IP hosts using a UDP, connectionless protocol.

Table 1-25 *Default Administrative Distances*

Route Source	Default Administrative Distance
Connected interface	0
Static route	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
EIGRP external route	170
Internal BGP	200
Unknown	255

Table 1-26 *Common TCP/UDP Ports in VoIP*

Application	Protocol	Port(s)
DHCP	UDP	67/68
HTTP	TCP	80
RTP	UDP	16384–32767
TAPI/JTAPI (Softphone if present)	TCP	2748
Cisco Softphone Directory Lookup	TCP	389/8404
Cisco skinny	TCP	2000
HIDS management	TCP	5000
Directory access (DCD)	TCP	8404

Wireless Best Practices

- Deploy authentication between the client and access point.
- Keep accounting records.
- Secret key rotation to occur transparently to end users.

Q & A

The Q & A questions are designed to help you assess your readiness for the topics covered on the CCIE Security written exam and those topics presented in this chapter. This format should help you assess your retention of the material. A strong understanding of the answers to these questions will help you on the CCIE Security written exam. You can also look over the questions at the beginning of the chapter again for further review. As an additional study aid, use the CD-ROM provided with this book to take simulated exams, which draw from a database of over 500 multiple-choice questions.

Answers to these questions can be found in Appendix A, "Answers to Quiz Questions."

1. What are the seven layers of the OSI model?
2. What layer of the OSI model is responsible for ensuring that IP packets are routed from one location to another?
3. What mechanism is used in Ethernet to guarantee packet delivery over the wire?
4. Name two physical characteristics of 10BASE-T?
5. What Catalyst command displays the bridging or CAM table on a Cisco 3550 series switch?
6. What are the possible states of spanning tree?
7. Fast EtherChannel (FEC) allows what to occur between Cisco Catalyst switches?
8. Does an IP packet include a known and common field that guarantees data delivery? If so, what is this field.
9. Name some examples of connection-orientated protocols used in TCP/IP networks.
10. Given the address 131.108.1.56/24, what are the subnet and broadcast addresses? How many hosts can reside on this network?
11. How many hosts can reside when the subnet mask applied to the network 131.108.1.0 is 255.255.255.128 (or 131.108.1.0/25)?
12. Name five routing protocols that support VLSM.
13. What is the destination port number used in a Telnet session?
14. What TCP/IP services are common in today's large IP networks?
15. What Cisco IOS command displays the IP ARP table on a Cisco IOS router?

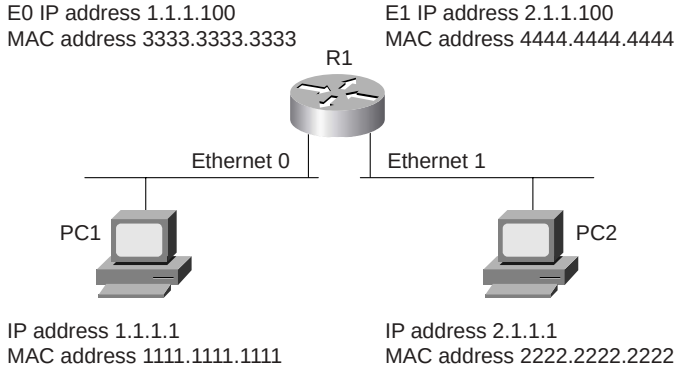
16. Cisco IOS routers use what mechanism to determine the routing selection policy for remote networks if more than one routing protocol is running?
17. What is the administrative distance for OSPF, RIP, and external EIGRP?
18. Name five characteristics of distance vector routing protocols and provide two examples of routing protocols classified as distance vector.
19. IP RIP runs over what protocol and port number when sending packets to neighboring routers?
20. How many networks can be contained in an IP RIP update?
21. Specify three main differences between RIPv1 and RIPv2.
22. What is an EIGRP feasible successor?
23. What is the metric used by OSPF?
24. If OSPF is configured for one area, what area assignment should be used?
25. What LSA types are not sent in a total stubby area?
26. What Cisco IOS command disables an interface from participating in the election of an OSPF DR/BDR router?
27. On an Ethernet broadcast network, a DR suddenly reboots. When the router recovers and discovers neighboring OSPF routers, will it be the designated router once more?
28. What Layer 4 protocol does BGP use to guarantee routing updates, and what destination port number is used?
29. What are ISDN BRI and PRI?
30. What are the three phases that occur in any PPP session?
31. Define what BECN and FECN mean in a Frame Relay network?
32. Frame Relay DLCI values are used for what purpose?
33. What is the IP address range used in IP multicast networks?
34. What type of network environment typically uses an AS5300?
35. What is the best method you can easily deploy to protect CCMs from unauthorized access?
36. What is WEP? Is WEP inherently secure or insecure?

Scenario

Scenario: Routing IP on Cisco Routers

Figure 1-21 displays a network with one Cisco router and two directly attached Ethernet interfaces. Use Figure 1-21 to answer the following questions.

Figure 1-21 *Scenario Diagram*



1. In Figure 1-21, PC1 cannot communicate with PC2. What is the likely cause of the problem, assuming that the router is configured correctly?
   - **a.** Router R1 requires a routing protocol to route packets from Ethernet0 to Ethernet1.
   - **b.** There is a problem with the IP address configuration on Router R1.
   - **c.** The gateway address on PC1 is wrong.
   - **d.** The gateway address on the router is wrong.
2. In Figure 1-21, what will be the ping response display when an exec user on Router R1 pings PC1's IP address for the first time? Assume that all configurations are correct.
   - **a.** !!!!!
   - **b.** !!!!.
   - **c.** .....
   - **d.** .!!!!
   - **e.** .!!!!!

3. What Cisco IOS command was used to display the following output taken from Router R1?

```
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  1.1.1.100              -   333.3333.3333   ARPA   Ethernet0
Internet  2.1.1.100              -   4444.4444.4444  ARPA   Ethernet1
Internet  1.1.1.1               10   1111.1111.1111  ARPA   Ethernet0
Internet  2.1.1.1               10   2222.2222.2222  ARPA   Ethernet1
```

a. show ip arpa

b. show ip arp

c. show interface ethernet0

d. show interface ethernet1

Scenario Answers

Scenario Solutions

1. c. Cisco IOS routers will route between directly connected interfaces and, because PC1 cannot ping PC2 on another subnet, the PC1 gateway address must not be configured correctly.
2. d. The first request will fail because of the ARP broadcast. The four subsequent pings will reply successfully. (There are five in total: one for an ARP request and four successful replies.)
3. b. **show ip arp** displays the correct ARP address table for the devices in Figure 1-21.

Exam Topics in This Chapter

- Domain Name System (DNS)
- Trivial File Transfer Protocol (TFTP)
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Secure Sockets Layer (SSL)
- Simple Mail Transfer Protocol (SMTP)
- Network Time Protocol (NTP)
- Secure Shell (SSH) and Cisco IOS SSH
- Lightweight Directory Access Protocol (LDAP)
- Active Directory
- Remote Data Exchange Protocol (RDEP)

You can find a list of all of the exam topics in the introduction to this book. For the latest updates on exam topics, visit Cisco.com.

CHAPTER 2

Application Protocols

This chapter covers some of today's most widely used application protocols.

This chapter covers the following topics:

- **Domain Name System (DNS)**—Topics in this section include how DNS is configured on Cisco routers and what port numbers are used when delivered across an IP network.
- **Trivial File Transfer Protocol (TFTP)**—This section covers the common uses of TFTP, particularly on Cisco IOS–enabled routers. The process used to copy files to and from a TFTP server is described.
- **File Transfer Protocol (FTP)**—This section covers FTP and the advanced mechanisms used in this connection-orientated protocol to ensure data delivery.
- **Other application topics**—Sections are included for Hypertext Transfer Protocol (HTTP), Secure Sockets Layer (SSL), Simple Network Management Protocol (SNMP), Simple Mail Transfer Protocol (SMTP), Network Time Protocol (NTP), Secure Shell (SSH), Lightweight Directory Access Protocol, and Active Directory. These sections cover some common configurations and Cisco IOS commands on Cisco routers that enable these applications. Cisco implementation of SSH in IOS and RDEP will also be covered.

NOTE SNMP, although not listed officially as an exam topic on Cisco.com, is a possible topic in the written examination.

"Do I Know This Already?" Quiz

The purpose of this assessment quiz is to help you determine how to spend your limited study time.

If you can answer most or all of these questions, you might want to skim the "Foundation Topics" section and return to it later, as necessary. Review the "Foundation Summary" section and answer the questions at the end of the chapter to ensure that you have a strong grasp of the material covered.

If you already intend to read the entire chapter, you do not necessarily need to answer these questions now. If you find these assessment questions difficult, read through the entire "Foundation Topics" section and review it until you feel comfortable with your ability to answer all of these questions and the "Q & A" questions at the end of the chapter.

Answers to these questions can be found in Appendix A, "Answers to Quiz Questions."

1. RFC 1700 defines what well-known ports for DNS?
   a. TCP port 21
   b. TCP port 23
   c. UDP port 21
   d. UDP port 53
   e. TCP/UDP port 53
2. What supplies DNS security?
   a. A default username/password pairing
   b. A TFTP directory
   c. A filename
   d. A domain name
   e. None of these
3. What Cisco IOS command will stop a Cisco router from querying a DNS server when an invalid Cisco IOS command is entered at the EXEC or PRIV prompt?
   a. no ip domain-lookup
   b. no ip dns-lookup
   c. no ip dns-queries
   d. no exec
4. What does the following Cisco IOS global configuration mode line accomplish?

```
ip host SimonisaCCIE 131.108.1.1 131.108.1.2
```

   a. Defines the router name as SimonisaCCIE
   b. Defines a local host name, SimonisaCCIE, mapped to IP addresses 131.108.1.1 and 131.108.1.2
   c. Configures the Cisco IOS router for remote routing entries 131.108.1.1 and 131.108.1.2
   d. Nothing, because it is not a valid Cisco IOS command
   e. Configures the local routers with the IP address 131.108.1.1 and 131.108.1.2 on bootup

5. TFTP uses what predefined UDP port number?

   a. 21

   b. 22

   c. 23

   d. 53

   e. 69

6. What Cisco IOS command will copy a Cisco IOS image from the current system flash to a TFTP server?

   a. copy tftp image:

   b. copy flash tftp

   c. copy tftp flash

   d. copy tftp tftp

7. Suppose a client calls and advises you that an FTP data transaction is not allowing the client to view the host's directory structure. What are the most likely causes of the problem? (Choose all that apply.)

   a. The client's username/password combination is wrong.

   b. The client's FTP data port is not connected.

   c. The host machine has denied the client access because the password is wrong.

   d. A serious network outage has occurred, which requires that you reload the router closest to the client.

   e. An access list is stopping port 20 from detailing the directory list.

8. FTP runs over what Layer 4 protocol?

   a. IP

   b. TCP

   c. TFTP

   d. DNS

   e. UDP

9. HTTPs traffic uses what TCP port number?

   a. 21

   b. 443

   c. 334

   d. 333

   e. 343

10. SNMP is restricted on Cisco routers by what Cisco IOS command?
    a. snmp-server enable
    b. snmp-server community string
    c. snmp-server ip-address
    d. snmp-server no access permitted
11. TFTP uses which of the following?
    a. Username/password pairs to authorize transfers
    b. TCP port 169
    c. UDP port 169
    d. Can use UDP/TCP and port 69
    e. None of these is correct
12. Which of the following statements is true regarding SSL?
    a. Every packet sent between host and client is authenticated.
    b. Encryption is used after a simple handshake is completed; that is, after the client is authenticated.
    c. SSL uses port 2246.
    d. SSL is not a predefined standard.
    e. SSL does not perform any data integrity checks.
13. What is the **HELO** SMTP command used for?
    a. To authenticate SMTP clients.
    b. To identify SMTP clients.
    c. This is an unknown standard.
    d. The **HELO** command is used in SNMP (not SMTP).
14. POP3 clients can do what?
    a. Receive SNMP queries.
    b. Retrieve mail.
    c. Send SNMP queries.
    d. The POP3 protocol is a routing algorithm.

15. NTP uses what well-known TCP port as defined by RFC 1700?

    a. 23

    b. 551

    c. 21

    d. 20

    e. 123

    f. 321

16. Secure Shell (SSH) is used to do what?

    a. Disable spanning tree on Catalyst 5000 switches.

    b. Protect the data link layer only from attacks.

    c. Protect the TCP/IP host with an encrypted channel.

    d. Allow TCP/IP access to all networks without any security.

    e. SSH is used only in the data link layer.

17. Which of the following protocols can be authenticated? (Select the best four answers.)

    a. Telnet

    b. HTTP

    c. HTTPs

    d. Spanning tree protocol (STP)

    e. TFTP

    f. FTP

18. What is the community string value when the following Cisco IOS commands are entered in global configuration mode?

```
snmp-server community publiC RO
snmp-server enable traps config
snmp-server host 131.108.255.254 isdn
```

    a. ISDN

    b. Config

    c. publiC

    d. public

    e. Public

    f. More data required

19. Which of the following best describes an SNMP inform request?

    a. Requires no acknowledgment.

    b. Requires an acknowledgment from the SNMP agent.

    c. Requires an acknowledgment from the SNMP manager.

    d. Only SNMP traps can be implemented on Cisco IOS routers.

20. What UDP port number will SNMP traps be sent from?

    a. 21

    b. 22

    c. 161

    d. 162

21. What TCP port number will an SNMP inform acknowledgment packet be sent to?

    a. 21

    b. 22

    c. 23

    d. 161

    e. 162

    f. None of these

22. To restrict SNMP managers from the source network 131.108.1.0/30, what Cisco IOS command is required?

    a. `ip http enable 131.108.1.1 131.108.1.2`

    b. `snmp community  131.108.1.1 131.108.1.2`

    c. `snmp-server community SimonisCool ro 4`
       `access-list 4 permit 131.108.1.0 0.0.0.3`

    d. `snmp-server community SimonisCool ro 4`

    e. `snmp-server community SimonisCool ro 1`
       `access-list 11 permit 131.108.1.0 0.0.0.252`

23. Cisco IOS SSH supports what version of SSH?

    a. SSH version 1 only

    b. SSH version 2 only

    c. Both versions 1 and 2

    d. SSH version 3

24. When enabling Cisco IOS SSH on a Cisco IOS router, which of the following is not a required step?

    a. Configure the **hostname** command.

    b. Configure the DNS domain.

    c. Generate a secret and enable password.

    d. Type the command **transport input** [**ssh**].

25. What Cisco IOS command will enable an SSH client session with the username cisco, encryption 3DES, and target IP address 10.1.1.1/24?

    a. Simon#**ssh –c 3des –l cisco 10.1.1.1**

    b. Simon(config-term)#**ssh –c 3des –l Cisco 10.1.1.1**

    c. Simon>**ssh –c des –l des cisco 10.1.1.1**

    d. None of these

26. SSH provides a security mechanism but lacks one certain feature. What feature is that?

    a. Provides a secure private channel for all messages.

    b. Endpoints are authenticated.

    c. Each transmission requires authentication.

    d. A message integrity check.

27. What protocol allows network administrators to monitor IDS sensors and what two protocols can be used?

    a. RDEP and HTTP/SSL

    b. RDEP and HTTP/SSL

    c. RIP and HTTP/SSL

    d. LDAP and HTTP/SSL

Foundation Topics

Domain Name System

This section covers the Domain Name System (DNS) and sample DNS configurations used on Cisco IOS routers.

The primary use of DNS is to manage Internet names across the World Wide Web. To enable users or clients to use names instead of 32-bit IP addresses, the TCP/IP model designers developed DNS to translate names into IP addresses.

DNS uses TCP and UDP port number 53. TCP port 53 is also used for DNS zone transfers. UDP 53 is used for DNS lookups and browsing.

In a large IP environment, network users need a way to connect to hosts without having to remember 32-bit IP addresses—that is where DNS comes into play. DNS provides a service that allows users to use a host's name in place of an IP address to connect to the host. When DNS services are running, the host's name is used to request its IP address from a DNS server. A DNS server is a host that is running the DNS service, and it is configured to do the translation for the user transparently. In other words, the user never sees the DNS request and host name-to-IP address translation. The client simply connects to a host name, and the DNS server does the translation. For example, the website www.cisco.com is translated to the IP address 198.133.219.25.

DNS is a distributed database where organizations can use a predefined name or extension for all their devices. Nations can use extensions to define hosts residing in their country. For example, the extension for Australia is defined as .au. To reach the Cisco website in Australia, a user would type www.cisco.com.au in a web browser.

A regulatory body called the Internet Policy Registration Authority manages domain names. Internet Corporation for Assigned Names and Numbers (ICANN), a certificate authority, also manages domain names.

Similar to DNS, Cisco routers can be configured to locally look up names so that network administrators can simply type a name rather than an IP address. Local names can also be configured for devices.

To illustrate a local name lookup on a Cisco IOS router, look at the following Cisco router command that provides a host lookup. (Note: a router will not provide DNS server responses to client devices such as PCs or UNIX hosts.)

```
ip host name [tcp-port-number] ip-address1 [ip-address2...ip-address8]
```

You can assign more than one IP address to any given name.

Example 2-1 displays three hosts and their corresponding IP addresses.

Example 2-1 *Local IP Host Configuration on a Cisco Router*

```
ip host Router1 131.108.1.1
ip host Router2 131.108.1.2
ip host Router3 131.108.1.3
```

The three locally defined hosts (remember, these are available only to the local router; they are not DNS entries and thus are not available to other devices) named Router1, Router2, and Router3 are translated into IP addresses 131.108.1.1, 131.108.1.2, and 131.108.1.3.

When a network administrator types in the local host name defined in the global configuration, the router translates the name to an IP address. Example 2-2 displays a network administrator Telneting from Router R1 to the remote host, Router2.

Example 2-2 *Local DNS Translation*

```
R1#router2
Translating "router2"
Trying Router2 (131.108.1.2)... Open
User Access Verification

Password: *****
Router2>
```

When the network administrator types the local name router2 (defined local names are not case sensitive) at the exec prompt, the Cisco IOS router does a local host lookup for the name router2 and translates the address to 131.108.1.2.

What would happen if you were to type a name that is not configured locally? Example 2-3 displays the sample output from a Cisco router when an unknown name (ccie, in this case) is typed at the exec prompt.

Example 2-3 *Name Translation for ccie*

```
R1#ccie
Translating "ccie"...domain server (255.255.255.255)
Translating "ccie"...domain server (255.255.255.255)
 (255.255.255.255)% Unknown command or computer name,
    or unable to find computer address

R1#
```

From the privileged exec prompt on Router R1 in Example 2-3, R1 performs a DNS entry lookup via a broadcast packet to 255.255.255.255. After no response (assuming no DNS server responds), R1 then does a local DNS lookup, discovers there is no DNS translation, and provides the following error message:

```
% Unknown command or computer name, or unable to find computer address
```

Scalability issues with local host configuration can become a nightmare in a large network. Thankfully, DNS servers can be placed around the network (typically in the core infrastructure) to ensure that only a few devices in the network require the full table of names and IP address translations. The World Wide Web has DNS servers that provide DNS mappings for websites.

DNS has become so important that one DNS server typically is not enough for an organization, because of the need for redundancy in case the primary DNS server fails. For example, typically an organization provides an internal protected DNS server for internal DNS requests and an external DNS server for external DNS resolutions.

NOTE By default, Cisco routers search for a DNS server. To disable this feature, use the Cisco IOS global configuration command **no ip domain-lookup**. This stops the router from querying a DNS server whenever a name translation is required. This command is a definite time saver for the CCIE Security lab exam.

To enable a Cisco IOS router to perform DNS lookup to a remote DNS server, the following steps are required:

Step 1 For local name entries (available to the router only; not the same as a DNS entry), you must specify any local host mapping with the following Cisco IOS command (note that *tcp-port-number* is used for connections on a TCP port number other than the default, 23):

ip host *name* [*tcp-port-number*] *ip-address1* [*ip-address2...ip-address8*]

Step 2 Specify the domain name or a domain list (Cisco routers can be configured with multiple domain names) with the following Cisco IOS commands:

- **ip domain-name** *name*—Defines a default domain name that the Cisco IOS software uses to complete unqualified host names
- **ip domain-list** *name*—Defines a list of default domain names to complete unqualified host names

Step 3 Specify the DNS server or servers with the following Cisco IOS command:

ip name-server *server-address1* [*server-address2...server-address6*]

Devices such as PCs can also be configured for DNS servers and domain names. Example 2-4 configures a router named R1 with the domain name cisco.com. The domain name servers are 131.108.255.1 and 131.108.255.2.

Example 2-4 *DNS Configuration*

```
R1(config)#ip domain-name cisco.com
R1(config)#ip name-server 131.108.255.1
R1(config)#ip name-server 131.108.255.2
```

When a network administrator types a name (not a valid Cisco IOS command, of course), the Cisco router attempts to translate the name into an IP address—first from any defined local names, second from the DNS server with the IP address 131.108.255.1, and third from the DNS server 131.108.255.2.

Example 2-5 displays a successful DNS query and translation to the host named ccie (another Cisco router) from the DNS server 131.108.255.1.

Example 2-5 *DNS Query from the Exec Prompt*

```
R1#ccie
! Administrator types ccie
Translating "ccie"
! Query is sent to first configured DNS server
Trying CCIE (131.108.255.1)... Open
User Access Verification
Password: ****
CCIE>
```

NOTE In Example 2-5, a Telnet connection requires a password authentication phase (a requirement for all Telnet-based connections, for that matter). You can disable the Telnet login password on Cisco routers with the command **no login** under the **line vty 0 4** line configuration, as follows:

```
line vty 0 4
no login
```

Trivial File Transfer Protocol

TFTP is a protocol that allows data files to be transferred from one device to another using the connectionless protocol, UDP. TFTP uses UDP port number 69.

TFTP is typically used in environments where bandwidth is not a major concern and IP packets that are lost can be re-sent by the higher layers (typically the application layer). TFTP has little security. In fact, the only way to provide security to TFTP transfer is by defining (on the TFRTP server) the directory on the host TFTP device and the filenames that will be transferred. The following numbered list outlines the main components of TFTP:

1. TFTP has no method to authenticate a username or password; the TFTP packet has no field enabling the exchange of a username or password between two TCP/IP hosts. TFTP communication or data transfer is actually transferred between two UDP port values, a source and destination UDP port number.
2. TFTP directory security (configurable on UNIX and Windows platforms) on the TFTP server is accomplished by allowing a predefined file on the server access to the file to be copied across. This allows the remote hosts to TFTP the file from the remote TFTP client. For example, to copy a configuration file from a Cisco router to a UNIX or Windows host, the file must be predefined on the TFTP server with the appropriate access rights defined. Security is reliant on the application and not the operating system. For example, the TFTP server daemon does not ship on Windows-based platforms and hence you need a third-party application.

Upgrading Cisco IOS images is a great example of a situation in which TFTP is useful; Cisco IOS images can be downloaded from a TFTP server to the Cisco router's system flash.

Cisco no longer offers a free TFTP application protocol, but the following URL provides some alternatives:

http://www.cisco.com/en/US/products/hw/routers/ps133/
products_tech_note09186a00801f7735.shtml#locate

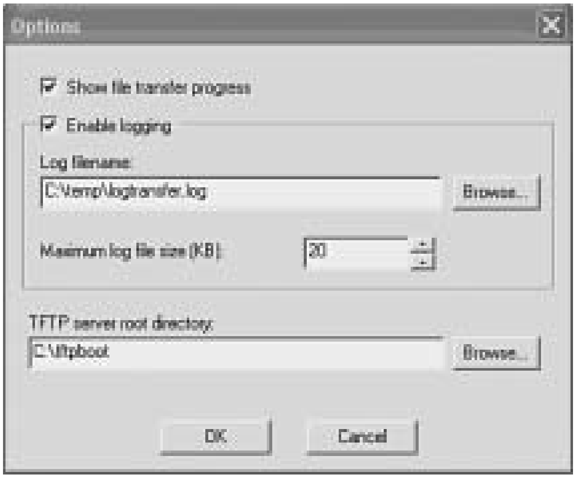
The Cisco TFTP Client Software no longer is available to the public. It was used to transfer software image files from a PC to your device, such as a router or switch. The favorite TFTP software of this author can be downloaded for free from 3Com's website:

http://infodeli.3com.com/software/utilities_for_windows_32_bit.htm

Now, configure the Cisco application software, Cisco TFTP, to enable a Cisco router to download a version of Cisco IOS code.

Figure 2-1 displays the available options when configuring the TFTP application software.

Figure 2-1 *Cisco TFTP Application Software Options*



The TFTP directory in Figure 2-1 is defined as c:\tftpboot. On the host TFTP server (in this case, a Windows 2000 PC), the Cisco IOS images reside in the tftpboot directory at c:\tftpboot. This download directory option is a configurable option, and you can select any valid directory on the host TFTP server.

The file is located in the tftpboot directory. In this example, the Cisco IOS image is named c2600-js-mz.121-5.T10.bin.

To copy a Cisco IOS image from a TFTP server, the Cisco IOS command is **copy tftp flash**. Example 2-6 displays a TFTP request for the file c2600-js-mz.121-5.T10.bin from a TFTP server with an IP address of 150.100.1.253.

Example 2-6 *TFTP File Transfer*

```
R1#copy tftp flash
Address or name of remote host []?150.100.1.253
Source filename []?c2600-js-mz.121-5.T10.bin
Destination filename [c2600-js-mz.121-5.T10.bin]? c2600-js-mz.121-5.T10.bin
Erase flash: before copying? [confirm]Y
Erasing the flash filesystem will remove all files! Continue? [confirm]Y
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
    eeeeee ...erased
Erase of flash: complete
Loading c2600-js-mz.121-5.T10.bin from 150.100.1.253 (via Ethernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

continues

Example 2-6 *TFTP File Transfer (Continued)*

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 11432808/22864896 bytes]
Verifying checksum...  OK (0xBC59)
11432808 bytes copied in 106.126 secs (107856 bytes/sec)
R1#
```

The file (c2600-js-mz.121-5.T10.bin) is successfully copied and placed on the flash system on Router R1. The only two mechanisms for security permitted with TFTP are predefining the filename and directory on the TFTP server. TFTP has no mechanism for checking the username and password. On a UNIX server that has the TFTP server daemon installed, the file to be copied must have the appropriate access rights. In UNIX, the **touch** command is used to allow a TFTP request by setting access rights appropriately. For a Windows-based platform, the software must be configured to permit file creation on the Windows-based file system.

For Windows TFTP applications such as Cisco TFTP (retired) and the 3Com TFTP server, the software does not have this option of access rights and hence can be less secure because any files can be loaded and downloaded.

FTP, on the other hand, is a connection-based protocol, where username and password combinations (in clear text) are used to authorize file transfers.

File Transfer Protocol

FTP, an application layer protocol of the TCP/IP protocol suite of applications, allows users to transfer files from one host to another. Two ports are required for FTP—one port is used to open the connection (port 21), and the other port is used to transfer data (20). FTP runs over TCP and is a connection-oriented protocol. To provide some level of security, FTP allows usernames and passwords to be exchanged before any data can be transferred, adding some form of security authentication mechanism to ensure that only valid users access FTP servers. FTP exchanges usernames and passwords in clear text.

The advantages of FTP are the ability to list a remote FTP server's full list of directories and to ensure that only valid users are connected. The file transfer progress can be displayed to the FTP client, as well. Many FTP applications are available, and the range of options is endless. For example, on the CCIE Security lab exam, the application WRQ Reflection 2000 can be used for Telnet and FTP. For more details on this application, visit http://www.wrq.com/products/reflection/.

NOTE FTP connection issues are typically communicated by end users (FTP clients) as poor network performance, but the problem might actually be a result of filtering the FTP data on port 20. For example, when a client successfully logs into an FTP server remotely but fails to list the remote FTP server's directory or to transfer files, this can indicate a problem with the FTP data port (via TCP port 20) or with an access list on the remote network.

FTP clients can be configured for two modes of operation (note that the names in parentheses are the names used in this guide):

- PORT mode (sometimes referred to as active mode)
- PASV mode (sometimes referred to as passive mode)

Active FTP

FTP active mode is defined as one connection initiated by the client to the server for the FTP control connection. Remember that FTP requires two port connections through TCP ports 20 (data) and 21 (control). The second connection is made for the FTP data connection (where data is transferred), which is initiated from the server back to the client.

Active FTP is less secure than passive mode because the FTP server, which, in theory, could be any host, initiates the data channel. Also, port 20 must be opened up to the outside world, which is inherently less secure than using just port 21.

Figure 2-2 displays the active FTP mode of operation between an FTP client and FTP server.

Figure 2-2 *FTP Active Mode*

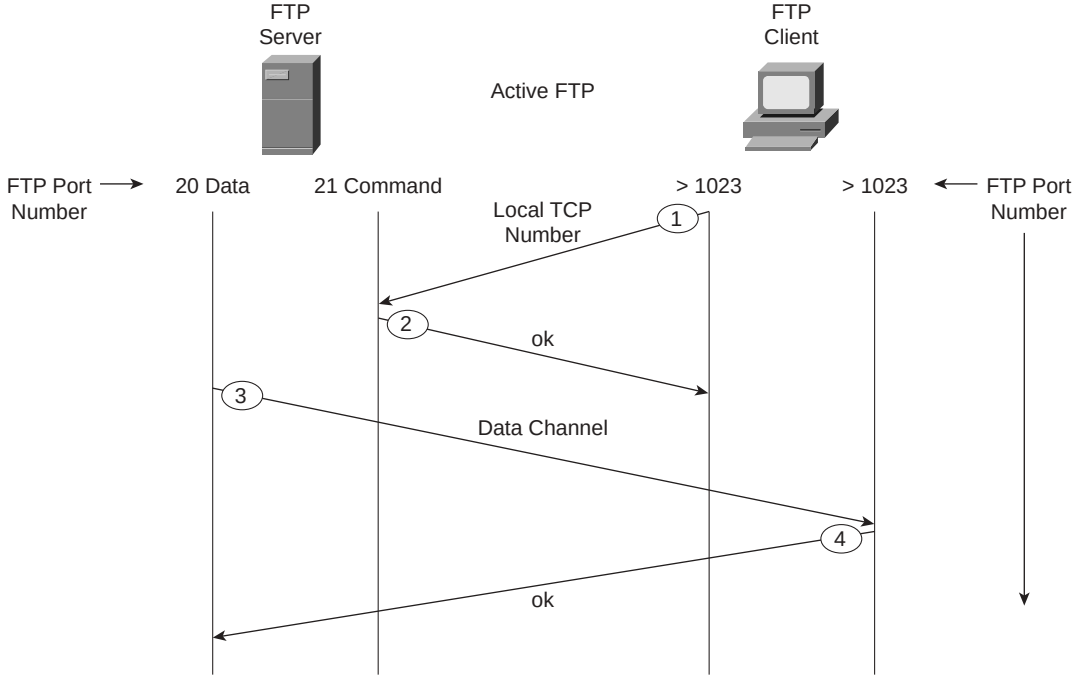


Figure 2-2 displays a typical FTP mode of operation between a client PC and an FTP server in active mode. The following steps are completed before FTP data can be transferred:

1. The FTP client opens a control channel on TCP port 21 to the FTP server. The source TCP port number on the FTP client is any number randomly generated above 1023.
2. The FTP server receives the request and sends an acknowledgment. FTP commands are exchanged between client and server.
3. When the FTP client requests a directory list or initiates a file transfer, the client sends a command (FTP **port** command). The FTP server then opens (initiates) a data connection on the FTP data port, TCP port 20.
4. The FTP client generates a new ephemeral (a decimal number above 1023) and sends the information to the server using the **port** command. The FTP server responds on the data port on the port number requested by the client.

Passive FTP

Passive FTP still requires a connection for the initial FTP control connection, which is initiated from the FTP client to the server. However, the second connection for the FTP data connection is also initiated from the client to the server (the reverse of active FTP).

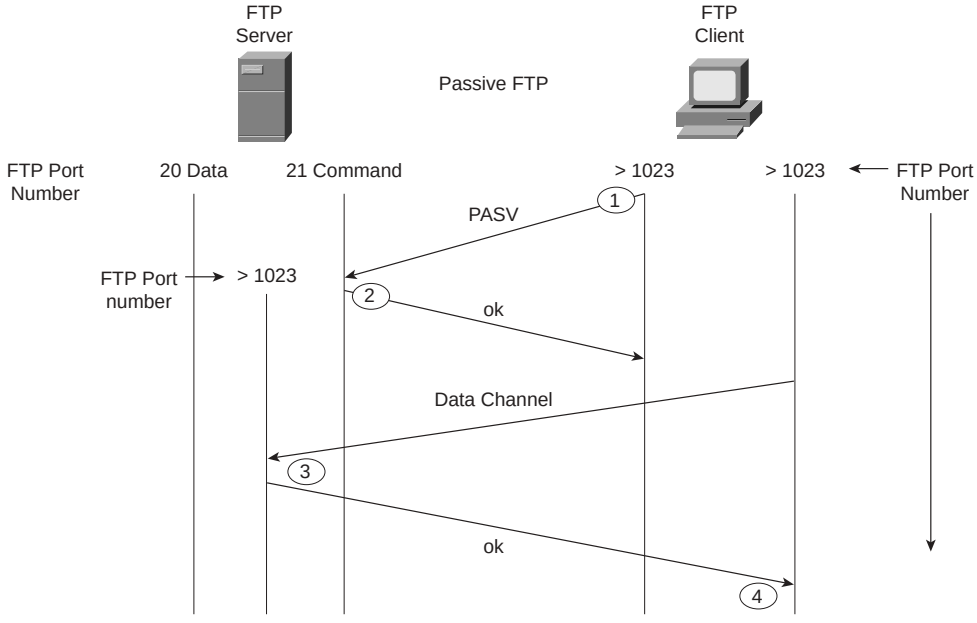
Figure 2-3 displays a typical FTP mode of operation between a client PC and FTP server in passive mode.

The following steps are completed before data can be transferred:

1. The FTP client opens a control channel on TCP port 21 to the FTP server and requests passive mode with the FTP command **pasv**, or **passive**. The source TCP port number for the control connection is any number randomly generated above 1023.
2. The server sends the port number to the client and waits for the client to initiate a data connection on that port. The FTP server receives the request and agrees to the connections using a randomly generated, local TCP port number greater than 1023.
3. The FTP client receives the information, selects a local TCP number randomly generated and greater than 1023, and opens a data channel to the FTP server (using the destination TCP port number selected by the server, a number greater than 1023).
4. The FTP server receives the FTP client's request and agrees to the connection by beginning to transfer data.

In passive FTP, the client initiates both the control connection and the data connection. In active mode, the FTP server initiates the FTP data channel. When using passive FTP, the probability of compromising data is lower because the FTP client initiates both connections.

Figure 2-3 *FTP Passive Mode*



Hypertext Transfer Protocol

HTTP, used by web browsers and web servers, transfers files, such as text and graphic files. HTTP can also authenticate users with username and password verification between clients and web servers.

Cisco IOS routers can be configured from a browser client. By default, Cisco routers are disabled for HTTP servers (HTTP is enabled by default on a few Cisco 1000 models, namely the Cisco 1003, 1004, and 1005 model routers), and there have been issues with users entering certain hash pairs to gain access to configuration commands when HTTP has been enabled. Fortunately, the latest versions of Cisco IOS code have been strengthened, and users must now enter valid username and password pairings (which means a hashed pair can be checked; only a valid username/password pair can produce the required hash) to gain access to the configuration options. HTTP authentication is not very secure, so Secure Sockets Layer (SSL) was developed to provide a stronger method to authenticate HTTP users.

NOTE For more details on the HTTP security vulnerability with Cisco IOS software, visit http://www.cisco.com/en/US/products/products_security_advisory09186a00800b1393.shtml.

To view the router's home page, use a web browser pointed to http://*a.b.c.d*, where *a.b.c.d* is the IP address of your router or access server. If a name has been set via a DNS server, use http://*router-name*.

Figure 2-4 displays a sample HTTP request to a remote router with the IP address 10.66.32.5 displaying the request for a valid username and password. The default username is the Cisco router's local host name, and the password is set to the enable or secret password.

Figure 2-4 *HTTP Authentication on a Cisco Router*

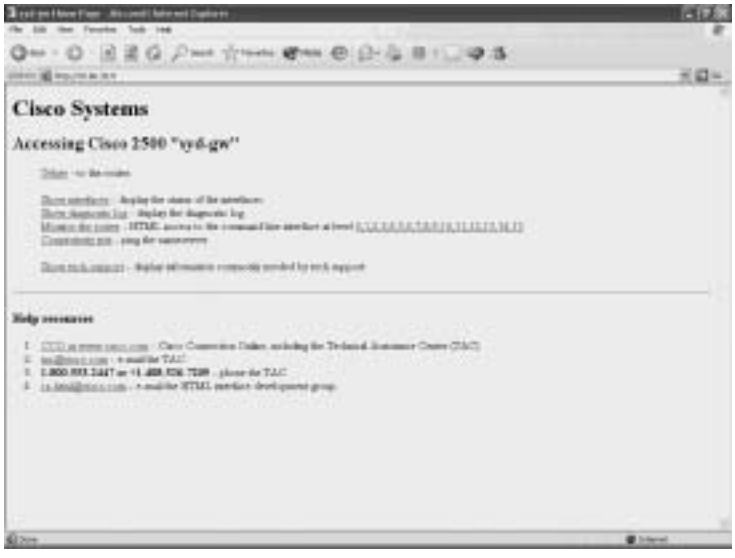
After the user is authenticated, the user enters the remote IP address or DNS name.

Varying forms of authentication for login can be set using the **ip http authentication** command. However, the default login method is to enter the host name as the username and the enable or secret password as the password, as displayed in Figure 2-4.

After the user is authenticated with the correct username and password pairing, the user is permitted HTTP access. Figure 2-5 displays the options available after authentication. Note that the HTML options may be different, depending on the Cisco IOS revision of your router.

After HTTP is authenticated, the available options are identical to the command-line interface (CLI) prompt. Depending on the configurable username and password pairing on the router, you will have certain privilege levels. For example, if you type the username as the local host name of the Cisco IOS router and the enable or secret password as completed in Figure 2-5, you will have privilege level 15, which is the same as the PRIV level on the CLI permitting all Cisco IOS commands. If the username/password pairing has a lower privilege level (via the **ip http authentication** command), the corresponding Cisco IOS command set will be available via HTTP. For example, a user with privilege level 5 will not have the option to reload the router. The user can also click the option (via the HTTP GUI interface) labeled **Monitor the router**, as shown in Figure 2-5, to access the CLI.

Figure 2-5 *HTTP Web Page on a Cisco Router*



NOTE The command to disable an HTTP server on a Cisco router is **no ip http server**. To set username/password pairs, use the following Cisco IOS command:

```
username username privilege [0-15] password password
```

You can also define the HTTP port number with the following command:

```
ip http [0-65535]
```

The default is 80. You can restrict access to the router by using an access list that defines networks and/or hosts permitted to access the router via HTTP.

Secure Sockets Layer

SSL is an encryption technology for web host devices used to process secure transactions. For example, a secure transaction is required when a client enters their credit card number for e-commerce via their browser. When the end user enters a web address via an Internet browser, such as Internet Explorer, instead of entering HTTP://*web address* in the address window, the end user enters HTTPs://*web address*.

NOTE Secure Hypertext Transfer Protocol (S-HTTP) transports HTTP-based traffic over an SSL connection and provides a stronger authentication mechanism than HTTP.

S-HTTP is not the same as SSL or HTTPs. S-HTTP is covered in RFC 2660 and is significantly different from SSL. More details on S-HTTP and how it differs from SSL are provided at http://www.ucs.mun.ca/~dgoudie/B8205/SSL.html.

HTTPs runs over TCP port 443. SSL is defined in RFC 2246.

The SSL Handshake Protocol was first developed by Netscape Communications Corporation to provide security and privacy over the World Wide Web. The SSL protocol supports server and client authentication. The SSL protocol is application-independent, allowing protocols like HTTP, FTP, and Telnet to be layered on top of it transparently. In other words, it is a session layer–based protocol. Cisco has developed a number of content-based switches to accelerate this communication, such as the Cisco SCA 11000 Series Secure Content Accelerator, an appliance-based solution that increases the number of secure connections supported by a website by offloading the processor-intensive tasks related to securing traffic with SSL. After an SSL session is established, no further authentication is required. Chapter 4, "Security Protocols," broadens this discussion on public security by discussing topics such as private and public keys, and how keys are exchanged through the Certificate Authority (CA) to ensure that SSL is secure.

Simple Network Management Protocol

SNMP is an application layer protocol used to manage IP devices. SNMP is part of the TCP/IP application layer suite. SNMP enables network administrators to view and change network parameters and monitor connections locally and remotely. Managing network performance over a period of time is one of the major functions that SNMP provides.

There are three versions of SNMP:

- SNMP Version 1 (SNMPv1)
- SNMP Version 2 (SNMPv2)
- SNMP Version 3 (SNMPv3)

Both SNMPv1 and SNMPv2 use a community-based form of security. The community string allows access to the SNMP agent and can also be defined by an IP address access control list and password.

SNMPv2c is the newer version of SNMP, and SNMPv2c (the *c* stands for community) is an experimental Internet protocol defined in RFC 1901, RFC 1905, and RFC 1906. SNMPv2c is an update of the protocol operations and data types of SNMPv2p (SNMPv2 classic), and uses the community-based security model of SNMPv1.

To set up the community access strings to permit access to SNMP on a Cisco IOS router, use the **snmp-server community** global configuration command:

```
snmp-server community string [view view-name] [ro | rw] [number]
```

Table 2-1 describes this syntax.

Table 2-1 **snmp-server community** *Command Syntax Description*

Syntax	Description
string	Case-sensitive community string that acts like a password and permits access to the SNMP protocol.
view *view-name*	(Optional) Name of a previously defined view. The view defines the objects available to the community.
ro	(Optional) Specifies read-only access. Authorized management stations are able to retrieve only MIB objects. There is no defined default value.
rw	(Optional) Specifies read-write access. Authorized management stations are able to retrieve and modify MIB objects. There is no defined default value.
number	(Optional) Integer from 1 to 99 that specifies an access list of IP addresses that are allowed to use the community string to gain access to the SNMP agent.

SNMP servers collect information from remote devices known as SNMP agents. SNMP packets are sent and received by devices on UDP ports 161 (SNMP servers-receivers) and 162 (SNMP agents-senders).

The Management Information Base (MIB) is a virtual information storage area for network management information consisting of collections of managed objects. Within the MIB are collections of related objects, defined in MIB modules. MIB modules are written in the SNMP MIB module language, as defined in STD 58, RFC 2578, RFC 2579, and RFC 2580. SNMP port 161 is used to query SNMP devices, and SNMP port 162 is used to send SNMP traps. SNMP runs over UDP and is secured by a well-known, case-sensitive community string. A well-known community string is one that is commonly known to all devices such as the default community string named “Public”.

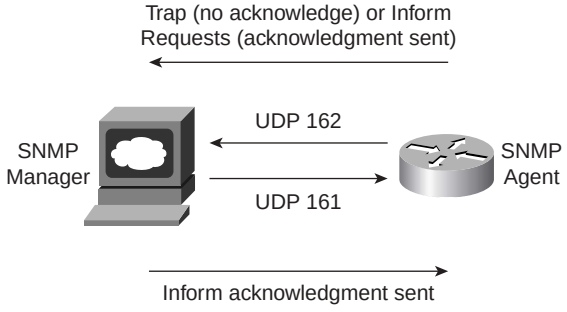
SNMP Notifications

SNMP’s key feature is that it enables you to generate notifications from SNMP agents.

Cisco routers can be configured to send SNMP traps or informed requests to a network management system (NMS), where a network administrator can view the data.

Figure 2-6 displays the typical communication between an SNMP manager and the SNMP agent (for example, a Cisco-enabled SNMP router).

Figure 2-6 *Communication Between SNMP Manager and SNMP Agent*



Unsolicited notifications can be generated as *traps* or *inform requests*. Traps are messages that alert the SNMP manager about a condition on the network (sent by the SNMP agent). Inform requests (informs) are traps that include a request for confirmation of receipt from the SNMP manager. SNMP notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to a neighbor router, or other significant events.

The major difference between a trap and an inform packet is that an SNMP agent has no way of knowing if an SNMP trap was received by the SNMP manager. An inform request will be sent continually until an acknowledgment is received by the sending SNMP agent.

Table 2-2 defines some of the common terminology used in SNMP.

Table 2-2 *SNMP Terminology*

Term	Description
Managed device	A network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and make this information available to NMSs using SNMP.
Agent	A network management software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP.
Network management system (NMS)	Executes applications that monitor and control managed devices.
SNMP manager	Management station that collects SNMP information from agents such as routers or switches.

NOTE Managed devices are monitored and controlled using three common SNMP commands:

- **read**—Used by an NMS to monitor managed devices. The NMS examines different variables that are maintained by managed devices.
- **write**—Used by an NMS to control managed devices. The NMS changes the values of variables stored within managed devices.
- **trap**—Used by managed devices to asynchronously report events to the NMS. For example, Cisco IOS routers can be configured to report errors, such as emergencies alerts, to the NMS for urgent action, such as low memory resources or unauthorized access. When certain types of events occur, a managed device sends a trap to the NMS.

The value of an MIB object can be changed or retrieved using SNMP commands, usually through a GUI network management system. Cisco supports a number of defined and proprietary MIB commands.

NOTE Be aware that newer and more functional Cisco IOS releases have new features and new added options. For this book, we are using the common features found in version 12.2. The CCIE Security candidate sitting for the written exam is not expected to remember the entire range of options available. Just be aware when you sit for the lab exam that you may have additional options.

Refer to http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_r/ffrprt3/frf014.htm#wp1056809 for more details. For example, in 12.0.3(T) there are additional options with the **snmp community host** command defined as:

```
version 3 [auth | noauth | priv]
hsrp
```

Example 2-7 configures a Cisco IOS (12.2 mainline) router for SNMP support.

Example 2-7 *Sample SNMP Configuration*

```
snmp-server community public RO
snmp-server enable traps config
snmp-server host 131.108.255.254 isdn
```

The Cisco IOS command **snmp-server community public RO** enables SNMP on a Cisco router. This command is also used to restrict access via SNMP. The community string is defined as public and acts as a password protection mechanism against unauthorized users. The community string is sent in every SNMP packet, so an incorrect community string results in no authorized access to the SNMP agent. The read-only attribute means that no configuration changes will be permitted

via an SNMP management station. Security administrators should never use the well-known community string "public". SNMPv1 and SNMPv2 (easily spoofed) send information in clear text. SNMPv3 is the most secure model, because it allows packet encryption.

The Cisco IOS command **snmp-server enable traps config** advises the NMS of any configuration changes. The Cisco IOS command **snmp-server host 131.108.255.254 isdn** alerts the host 131.108.254.254 of any ISDN traps which can include link flapping or high link usage, for example.

To specify the recipient of an SNMP notification operation, use the **snmp-server host** global configuration command. To remove the specified host, use the **no** form of this command.

```
snmp-server host host-addr [traps | informs] [version {1 | 2c | 3
[auth | noauth | priv]}] community-string
[udp-port port] [notification-type]
```

Table 2-3 expands the **snmp-server host** Cisco IOS command and presents the full range of options, including MD5 authentication.

Table 2-3 **snmp-server host** *Command**

Syntax Description	Meaning
host-addr	Name or Internet address of the host (the targeted recipient).
traps	(Optional) Sends trap messages to this host. This is the default.
informs	(Optional) Sends inform messages to this host.
version	(Optional) Version of the SNMP used to send the traps. Version 3 is the most secure model because it allows packet encryption with the **priv** keyword. If you use the **version** keyword, one of the following must be specified: **1**—SNMPv1 (not available with informs) **2c**—SNMPv2C **3**—SNMPv3 The following three optional keywords can follow the **3** keywords: **auth**—(Optional) Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. This is known as authNoPriv. **noauth**—(Default) The noAuthNoPriv security level. This is the default if the [**auth** | **noauth** | **priv**] keyword choice is not specified. **priv**—(Optional) Enables Data Encryption Standard (DES) packet encryption (also called privacy). This is known as authPriv.
community-string	Password-like community string sent with the notification operation. Although you can set this string using the **snmp-server host** command by itself, it is recommended that you define this string using the **snmp-server community** command prior to using the **snmp-server host** command.
udp-port *port*	(Optional) UDP port of the host to use. The default is 162.

Table 2-3 **snmp-server host** *Command* (Continued)*

Syntax Description	Meaning
notification-type	(Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the following keywords: **bgp**—Sends Border Gateway Protocol (BGP) state change notifications. **calltracker**—Sends Call Tracker call-start/call-end notifications. **config**—Sends configuration notifications. **dspu**—Sends downstream physical unit (DSPU) notifications. **entity**—Sends Entity MIB modification notifications. **envmon**—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded. **frame-relay**—Sends Frame Relay notifications. **hsrp**—Sends Hot Standby Routing Protocol (HSRP) notifications. **isdn**—Sends Integrated Services Digital Network (ISDN) notifications. **llc2**—Sends Logical Link Control, type 2 (LLC2) notifications. **repeater**—Sends standard repeater (hub) notifications. **rsrb**—Sends remote source-route bridging (RSRB) notifications. **rsvp**—Sends Resource Reservation Protocol (RSVP) notifications. **rtr**—Sends SA Agent (RTR) notifications. **sdlc**—Sends Synchronous Data Link Control (SDLC) Protocol notifications. **sdllc**—Sends Synchronous Data Logical Link Control (SDLLC) notifications. **snmp**—Sends any enabled RFC 1157 SNMP linkUp, linkDown, authenticationFailure, warmStart, and coldStart notifications. **stun**—Sends serial tunnel (STUN) notifications. **syslog**—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the **logging history level** command. **tty**—Sends Cisco enterprise-specific notifications when a TCP connection closes. **voice**—Sends SNMP poor quality of voice traps when used with the **snmp enable peer-trap poor qov** command. **x25**—Sends X.25 event notifications. Note in version 12.2T and higher the options have been extended to include such protocols as BGP, HSRP, and more. Refer to Cisco.com for details.

Author Query:

is this correct?

*From http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_r/frprt3/frd3001.htm#xtocid655917.

SNMP is disabled by default on Cisco IOS routers.

SNMP Examples

The following example assigns the SimonisCool string to SNMP, allowing read-only access, and specifies that IP access list 4 can use the community string:

```
R1(config)# snmp-server community SimonisCool ro 4
R1(config)# access-list 4 permit 131.108.1.0 0.0.0.255
```

The hosts on network 131.108.1.0/24 are permitted SNMP access if the read-only string is set to SimonisCool. This enables an added feature which ensures that devices that source SNMP information are from a trusted or internal network.

The following example assigns the string SnR to SNMP, allowing read-write access to the objects in the restricted view (read-write):

```
R1(config)# snmp-server community SnR view restricted rw
```

The following example disables all versions of SNMP:

```
R1(config)# no snmp-server
```

The following example enables the router to send all traps to the host, host.cisco.com, using the community string "publiC":

```
R1(config)# snmp-server enable traps
R1(config)# snmp-server host host.cisco.com public
```

In the following example, the BGP traps are enabled for all hosts, but only the ISDN traps are enabled to be sent to an actual host named simon:

```
R1(config)# snmp-server enable traps bgp
R1(config)# snmp-server host simon public isdn
```

The following example enables the router to send all inform requests to the host test.cisco.com using the community string publiC:

```
R1(config)# snmp-server enable traps
R1(config)# snmp-server host test.cisco.com informs publiC
```

Simple Mail Transfer Protocol

SMTP, defined in RFC 821, is used to provide e-mail services to IP devices over the Internet. Typically, two mail servers “talk” SMTP to exchange e-mail. After the e-mail is exchanged, the users can retrieve their mail from the mail server and read it. This can be done using any mail client, such as Pine, Eudora, Outlook, and so on, which use different protocols, such as Post Office Protocol 3 (POP3), to connect to the server. SMTP uses well-known ports TCP port 25 and UDP port 25. Typically, though, SMTP applications use only TCP port 25.

A process or daemon running on a server uses SMTP to send mail to clients. A program called Sendmail is a common tool used for SMTP mail transfer. Recently, a new release of SMTP, called Enhanced SMTP (ESMTP), was developed. You are not required to know this protocol for the written exam.

The client and SMTP server send various commands when communicating. The most common command is **HELO**, which introduces the calling machine to the receiving machine; the client machine advertises its host name to the mail server. There are numerous other commands, some of which are described in the following list. If you are interested in further details on the Sendmail application, a great resource is *Sendmail*, by Bryan Costales and Eric Allman (O'Reilly and Associates, ISBN 1-56592-839-3). For more details on SMTP, refer to the RFC 821 documentation at http://www.faqs.org/rfcs/rfc821.html.

To test whether a remote host's SNMP mail is operational and active, use Telnet with the defined **HELO** command. The following is a summary of other useful SMTP commands, in case you are questioned on these commands during the exam:

MAIL (**MAIL**)—Initiates a mail transaction in which the mail data is delivered to mailboxes.

RECIPIENT (**RCPT**)—Identifies an individual recipient of the mail data; multiple use of the command is needed for multiple users.

DATA (**DATA**)—Identifies the lines following the command (such as the MAIL command) as the mail data in ASCII character codes.

SEND (**SEND**)—Initiates a mail transaction in which the mail data is delivered to one or more terminals.

SEND OR MAIL (**SOML**)—Initiates a mail transaction in which the mail data is delivered to one or more terminals or mailboxes.

SEND AND MAIL (**SAML**)—Initiates a mail transaction in which the mail data is delivered to one or more terminals and mailboxes.

RESET (**RSET**)—Aborts the current mail transaction. Any stored sender, recipients, and mail data must be discarded, and all buffers and state tables must be cleared. The receiver must send an OK reply.

VERIFY (**VRFY**)—Verifies if a user exists; a fully specified mailbox and name are returned.

NOOP (**NOOP**)—Specifies no action other than that the receiver sent an OK reply.

QUIT (**QUIT**)—Closes the transmission channel; the receiver must send an OK reply.

Network Time Protocol

NTP is used for accurate time-keeping and can, for example, reference atomic clocks that are present on the Internet. NTP is capable of synchronizing clocks within milliseconds and is a useful protocol when reporting error logs (for instance, from Cisco routers). NTP is useful for security/incident event correlation across multiple security devices and helps to determine the exact time of the event.

For NTP, the defined ports are UDP port 123 and TCP port 123. NTP can support a connection-orientated server (TCP guarantees delivery) or a connectionless server (UDP for noncritical applications). NTP applications typically use only UDP port 123.

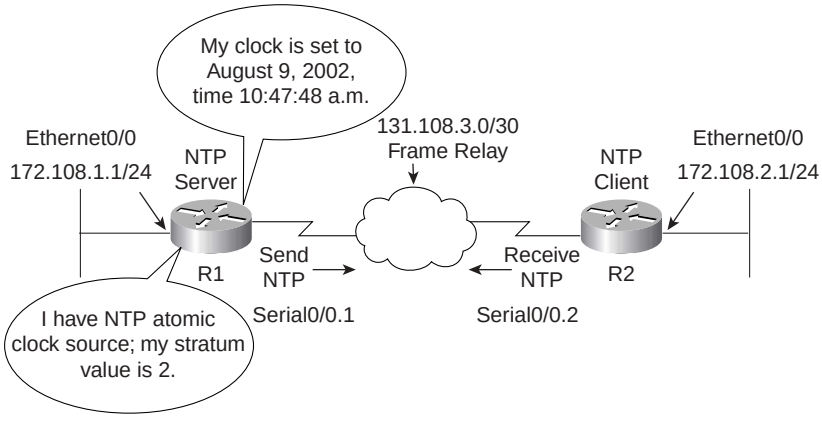
An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within a millisecond of one another.

NOTE NTP uses the concept of a *stratum* to describe how many NTP hops away a machine is from an authoritative time source. A stratum 1 time server has a radio or atomic clock directly attached; a stratum 2 time server receives its time via NTP from a stratum 1 time server, and so on. Cisco routers cannot support stratum 1 (you cannot connect a Cisco router to an atomic clock source) and need to derive an atomic clock source from the Internet. NTP can also authenticate sessions.

A Cisco 7200 series router, however, does support attachment of a GPS clock to the aux port, which would make the router a stratum 1 time source.

Figure 2-7 displays a simple two-router network where Router R1 will be configured to supply a clock source to Router R2. In this example, you will configure authentication and ensure that the NTP peering between the two routers is secure.

Figure 2-7 *NTP Sample Configuration*



The following steps are required to enable NTP on a Cisco router:

Step 1 Define the time zone with the following command:

```
clock timezone zone hours [minutes]
```

Step 2 Configure the master NTP router (which will supply a clock to other routers) with the following command:

```
ntp master [stratum-value]
```

stratum-value is 1 to 15, with 1 representing the best clock source.

Step 3 To configure a remote NTP peer to a Cisco router with a better stratum value, use the following Cisco IOS command:

```
ntp peer ip-address [version number] [key keyid]
[source interface] [prefer]
```

Table 2-4 displays the required parameters for the **ntp peer** command.

Step 4 To define NTP to authenticate the NTP session, use the following Cisco IOS commands:

```
ntp trusted-key key-number
```

key-number is the authentication key to be trusted.

```
ntp authentication-key number md5 value
```

Table 2-4 **ntp peer** *Command Defined*

Syntax	Description
Ip-address	IP address of the peer providing, or being provided, the clock
version	(Optional) Defines the NTP version number
number	(Optional) NTP version number (1 to 3)
key	(Optional) Defines the authentication key
keyid	(Optional) Authentication key to use when sending packets to this peer
source	(Optional) Names the interface
interface	(Optional) Name of the interface from which to pick the IP source address
prefer	(Optional) Makes this peer the preferred peer to provide synchronization

To ensure that R1 sends a clock source to R2 via NTP, R1 must be configured to send NTP traffic over the Frame Relay cloud, by using the command **ntp broadcast**. To specify that a specific interface should send NTP broadcast packets, use the **ntp broadcast** interface configuration command. Similarly, R2 must receive NTP traffic and is considered an NTP client, which is accomplished by using the Cisco IOS command **ntp broadcast client**.

R2's Serial0/0 interface is configured with the command **ntp broadcast client**.

Example 2-8 configures Router R1 in Figure 2-7 to supply a clock source to Router R2.

Example 2-8 *NTP Configuration on R1*

```
clock set 10:20:00 9 August 2002
clock timezone UTC 10
!Interface configuration
interface serial0/0
ntp broadcast
!Global configuration
ntp authentication-key 1 md5 121A061E17 7
ntp authenticate

ntp trusted-key 1
ntp master 2
ntp peer 131.108.2.1 key 1
```

Notice that the router is set to the correct time with the Cisco IOS command **clock set**.

The router is configured for the UTC time zone and 10 hours behind UTC time. (This particular router resides in Sydney, Australia, 10 hours behind UTC.) The authentication key is set to 1.

Example 2-9 configures R2 to get the clock from R1 using the same MD5 password (set to ccie) from Example 2-8.

Example 2-9 *NTP Configuration on R2*

```
interface serial0/0
ntp broadcast client
!Global configuration
ntp authentication-key 1 md5 ccie
ntp authenticate
ntp trusted-key 1
ntp peer 131.108.1.1 key 1
```

Example 2-10 displays the two clocks on Routers R1 and R2, confirming that R1 is sending the correct time to R2 via NTP. The Cisco IOS command **ntp authenticate** ensures that the NTP peers are authenticated. Optionally, you can define where a device will source the NTP clock from with the command **ntp server** *ip-address*.

Example 2-10 **show clock** *on R1 and R2*

```
R1#show clock
10:47:48.508 UTC Fri Aug 9 2002
R2#show clock
10:47:48.508 UTC Fri Aug 9 2002
```

Example 2-11 confirms that NTP is authenticated (the remote stratum value is 2) by displaying the output of the Cisco IOS command **show ntp associations detail**.

Example 2-11 **show ntp associations detail** *Command on R2*

```
R2# show ntp associations detail
131.108.1.1 configured, authenticated, selected, sane, valid, stratum 2
ref ID .LOCL., time C0FD8D45.0B1C72E0 (10:37:25.043 UTC Fri Aug 9 2002)
our mode active, peer mode passive, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.03, reach 1, sync dist 15878.372
delay 6.67 msec, offset 297909193935.7106 msec, dispersion 15875.02
precision 2**16, version 3
org time C0FD8D45.BA55E231 (10:37:25.727 UTC Fri Aug 9 2002)
rcv time AF3BD17B.CBA5DDF0 (10:04:11.795 UTC Mon Mar 1 1993)
xmt time AF3BD17B.C9CB2BA2 (10:04:11.788 UTC Mon Mar 1 1993)
filtdelay =     6.67    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset = 2979091    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =     0.02 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0
131.108.255.1 dynamic, authenticated, our_master, sane, valid, stratum 2
ref ID .LOCL., time C0FD8D05.0AE0774C (10:36:21.042 UTC Fri Aug 9 2002)
our mode passive, peer mode active, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.03, reach 2, sync dist 1.007
delay 0.00 msec, offset 0.0000 msec, dispersion 16000.00
precision 2**16, version 3
org time C0FD8D43.0B54AAFA (10:37:23.044 UTC Fri Aug 9 2002)
rcv time AF3BD179.1C9F231D (10:04:09.111 UTC Mon Mar 1 1993)
xmt time AF3BD186.C9CB3361 (10:04:22.788 UTC Mon Mar 1 1993)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =  16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0
```

Example 2-11 displays that R2 is dynamically peered to R1 and is authenticated. The IP address of the NTP peer server, a configured peer, is 131.108.255.1, as highlighted midway down in Example 2-11.

Secure Shell and Cisco IOS SSH

Secure Shell (*SSH*) is a protocol that provides a secure connection to a router. Cisco IOS supports version 1 and 2 of SSH, which enables clients to make a secure and encrypted connection to a Cisco router. Cisco refers to this SSH support as Cisco IOS SSH. Before SSH was implemented, the only form of security available when accessing devices such as routers was Telnet username/password authentication, which is clearly visible with a network sniffer. Telnet is insecure because a protocol analyzer can view the information in clear-text form. Figure 2-8 displays a simple protocol analyzer viewing information between a source address, 10.66.32.5, and the destination address, 192.168.1.13, after a Telnet session is initiated by the address (PC) 1066.32.1/24.

SSH support has been available in Cisco IOS since 12.1(1)T and 12.0(5)S.

NOTE Secure Shell and Cisco IOS SSH are not two different protocols; rather, Cisco IOS SSH is the Cisco terminology for the fact that Cisco IOS supports SSH. Do not confuse them as different protocols.

Figure 2-8 *Sniffer Capture of a Telnet Connection*

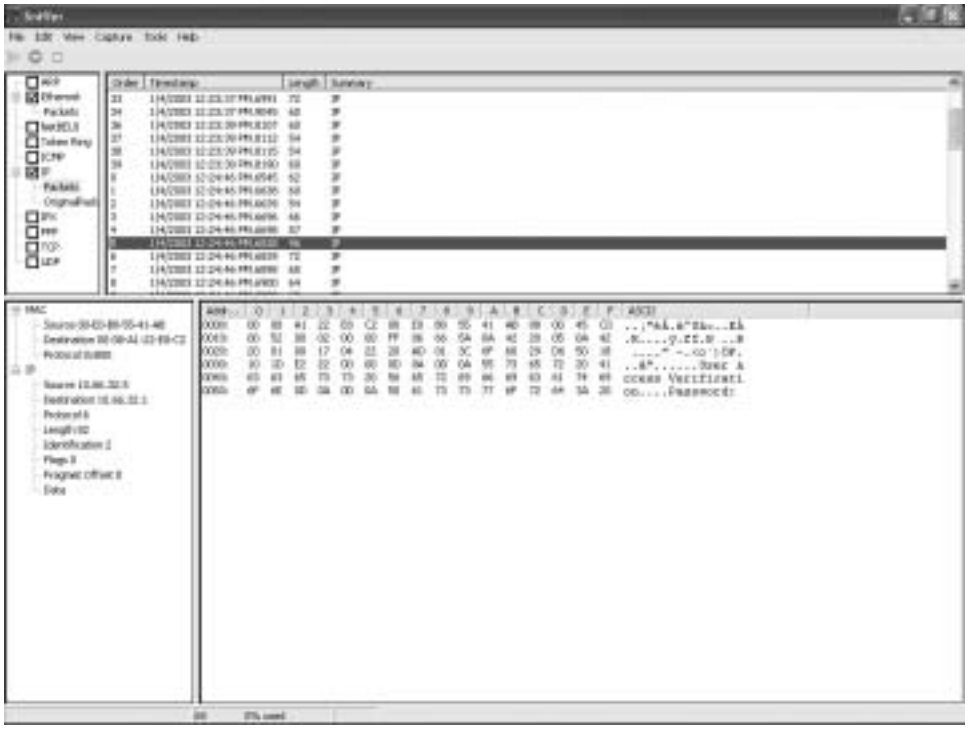


Figure 2-8 displays a simple Telnet connection between a PC and a remote router. Figure 2-8 is a packet trace from a client PC Telnet connection to a Cisco IOS router with the IP address 10.32.66.5. The packet trace clearly captures the password prompt sent by the router. Therefore, the prompt is viewable in clear text. If you scrolled down the next few frames (frames numbered 98 to 103 in Figure 2-8), the password would be clearly visible. An intruder or hacker could piece together the password and gain unauthorized access. For security reasons, these frames are not shown, but it is clear that the Telnet application protocol is not a secure protocol; all data is sent as clear text (including the password exchanged).

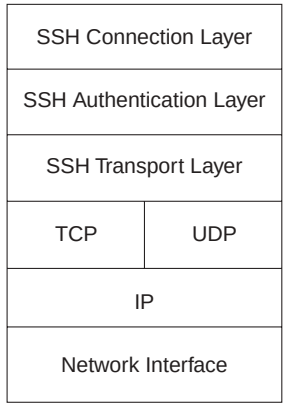
SSH is implemented with TCP port 22 and UDP port 22 and ensures that data is encrypted by a network sniffer. SSH can be configured on both Cisco IOS routers and Catalyst switches. Typically, however, SSH software supplied by vendors supports TCP port 22.

Figure 2-9 displays the SSH protocol layers.

NOTE *Lightweight Directory Access Protocol* (*LDAP*) is an Internet protocol that e-mail programs use to look up contact information from a server. For more details on LDAP, visit http://www.gracion.com/server/whatldap.html.

Active Directory is a Windows-defined application that stores and manages network services, resources, and information about where computers and printers are located. Active Directory enables network administrators of Windows 2000 and 2003 servers to allocate and control how network resources are accessed by clients' PCs. LDAP can be used for much more than just e-mail. For more information on Active Directory, visit http://www.microsoft.com.

Figure 2-9 *SSH Protocol Layers*



SSH sits on top of the TCP/IP layers, protecting the hosts from unknown devices. The SSH transport layer is responsible for securing the data, by using encryption authentication. Also, because SSH encrypts the username and password, SSH protects vulnerable devices from unknown users masquerading as trusted users. There are currently two versions of SSH: SSHv1 and SSHv2. Cisco IOS supports SSHv1 and SSHv2.

Cisco IOS SSH

The Cisco IOS implementation of SSH (which has been available for several years now), called Cisco IOS SSH (available in S, E, and T trains of Cisco IOS software), is a service feature that is available in the service provider Cisco IOS revision levels. Cisco IOS SSH is used to ensure that remote devices are managed securely; Telnet is a very insecure protocol, because all segments are sent in clear text. Cisco IOS SSH allows an administrator to remotely manage a Cisco IOS device, such as a router or Catalyst operating system (CatOS), securely. Cisco IOS SSH provides a secure link between a client and server.

SSH uses the Rivest, Shamir, and Adelman (RSA) public key cryptography, therefore allowing a secure communication channel between a client and router.

SSH was introduced into Cisco IOS platforms/images as follows:.

- SSHv1 server support was introduced in some Cisco IOS platforms/images starting in 12.0.5.S.
- SSH client support was introduced in some Cisco IOS platforms/images starting in 12.1.(5)T9.
- SSH terminal-line access (also known as reverse-Telnet) was introduced in some Cisco IOS platforms/images starting in 12.2.2.T. It can be used to secure reverse-telnet connections from terminal servers.
- SSHv2 support was introduced in some Cisco IOS platforms/images starting in 12.1(19)E6.

The following is an example of configuring a Cisco router as an SSH server and a client connection from another Cisco IOS router.

There are four steps required to enable SSH support on a Cisco IOS router:

1. Configure the **hostname** command.
2. Configure the DNS domain.
3. Generate the public (RSA) key to be used.
4. Enable SSH transport support for the vtys (optional step).

Example 2-12 displays a sample Cisco IOS SSH configuration. The exclamation points (!) identify comments that have been added to make the configuration more reader-friendly.

Example 2-12 *Cisco IOS SSH Server*

```
!Configure the hostname if not previously done so.
hostname Massimo
! configure a local username and password to authenticate
! the remote SSH user, AAA can
! also be used
username cisco password 0 cisco
!Configure the router's DNS domain.
ip domain-name cisco.com
Interface Ethernet0
ip address 10.1.1.1 255.255.255.0
! Generate RSA key, completed from the configuration mode in IOS.
crypto key generate rsa
! Following are optional SSH commands that control parameters on your route
ip ssh time-out 120
ip ssh authentication-retries 2
!
!
!By default the vtys' transport is all available such as Telnet.
! In this case, only SSH will be used.

line vty 0 4
login local
transport input SSH
end
```

Example 2-12 configures a router named Massimo for Cisco IOS SSH. In particular, the command **crypto key generate rsa** generates the RSA public key, the **ip ssh time-out 120** command sets the default idle time to 120, and the **ip ssh authentication-retries 2** command sets a maximum retry limit of 2. The **crypto key generate** command builds both halves of the key pair. There is an optional **write** keyword that saves the key pair to NVRAM; otherwise, it is lost on reboot or a reload as the volatile RAM is refreshed.

To start an encrypted session with a remote networking device, use the **ssh** user EXEC command:

```
ssh [-l userid] [-c {des | 3des}] [-o numberofpasswordprompts n] [-p portnum]
    {ipaddr | hostname} [command]
```

Table 2-5 displays the options available with the **ssh** EXEC command.

Table 2-5 ssh Command Summary*

-l *userid*	(Optional) Specifies the user ID to use when logging into the remote networking device running the SSH server. If no user ID is specified, one needs to be defined. Otherwise, the following error appears on the router's CLI: % No user specified nor available for SSH client
-c {**des** | **3des**}	(Optional) Specifies the crypto algorithm, DES or 3DES, to use for encrypting data. To use SSH, you must have an encryption image running on the router. Cisco software images that include encryption have the designators "k8" (DES) or "k9" (3DES).
-o numberofpasswdprompts *n*	(Optional) Specifies the number of password prompts that the software generates before ending the session. The SSH server may also apply a limit to the number of attempts. If the limit set by the server is less than the value specified by the **-o numberofpasswdprompts** keyword, the limit set by the server takes precedence. The default is 3 attempts, which is also the Cisco IOS SSH server default. The range of values is from 1 to 5.
-p *portnum*	(Optional) Indicates the desired port number for the remote host. The default port number is 22.
ipaddr | *hostname*	Specifies the IP address or host name of the remote networking device.
command	(Optional) Specifies the Cisco IOS command that you want to run on the remote networking device. If the remote host is not running Cisco IOS software, this may be any command recognized by the remote host. If the command includes spaces, you must enclose the command in quotation marks.

*From http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_r/fothercr/srfssh.htm#wp1024082.

The following is sample output from the **show ip ssh** command:

```
Router# show ip ssh
Connection Version Encryption State Username
0          2.0    3DES       4     guest
```

The connection is labeled 0 (vty number), is running version 2.0, is using 3DES encryption, and the username is guest.

Example 2-13 displays a session connection from a router named Simon to the SSH server–enabled router named Massimo.

Example 2-13 *SSH Connection Example*

```
Simon#ssh -c 3des -l cisco 10.1.1.1
Trying 10.1.1.1…Open
Password:cisco
Massimo>
```

The username is defined with the **–l** option; in Example 2-13, it is set to cisco.

To display the version and configuration data for SSH, use the **show ip ssh** privileged EXEC command.

For more detailed information on SSH and on the Cisco IOS functional matrix, visit http://www.ssh.com/products/tectia/ and http://www.cisco.com/warp/public/707/ssh.shtml, respectively.

Remote Data Exchange Protocol

The Cisco Intrusion Detection System (IDS) provides an in-depth, self-healing mechanism to provide network administrators a defense against attacks from inside and outside the network. The Cisco definition of a self-healing network is a network that is intelligent enough to stop unwanted traffic and correct any security vulnerabilities before they occur.

Beginning with Cisco IDS 4.0, the network IDS sensors use the Remote Data Exchange Protocol (RDEP) for communication. With RDEP, the network operator can subscribe to specific IDS event types and better control which events are received or ignored.

The sensor software was re-architected in Cisco IDS 4.0. All of the pre-4.0 software applications, such as nr.postoffice, nrConfigure, nr.packetd, and nr.managed, have been replaced with 4.0 software applications. Postoffice protocol has been replaced with RDEP, which uses the HTTP/HTTPs protocol to communicate with XML documents between the sensor and external systems.

Sensor configuration, control, log, and event information are communicated and stored in XML documents. Version 4.0 provides an open interface that is accessible by clients that can communicate over HTTP/HTTPs and process XML documents.

So, in summary, RDEP allows IDS sensors to communicate with external systems. RDEP uses HTTP and SSL to pass XML documents over an encrypted session, between the sensor and the external system. XML files located on the IDS sensors can control the configuration and operation of the sensor.

NOTE Although RDEP is listed as a blueprint item, RDEP is a propriety protocol, and you can expect the exam to test you only lightly on this protocol. RDEP is a subset of the HTTP/1.1 protocol and uses a client request/server response model; it replaces the old IDS Postoffice protocol. The IDS sensor is the RDEP server, and management stations are the clients.

Foundation Summary

The "Foundation Summary" is a condensed collection of material for a convenient review of this chapter's key concepts. If you are already comfortable with the topics in this chapter and decided to skip most of the "Foundation Topics" material, the "Foundation Summary" will help you recall a few details. If you just read the "Foundation Topics" section, this review should help further solidify some key facts. If you are doing your final preparation before the exam, the "Foundation Summary" offers a convenient and quick final review.

Table 2-6 *DNS Concepts*

Concept	Description
Well-known port numbers	UDP port 53, TCP port 53
ip host *name* [*tcp-port-number*] *ip-address1* [*ip-address2...ip-address8*]	Configured locally to assign a host name with up to eight IP addresses
no ip domain-lookup	Disables the IP DNS-based host name-to-address translation
ip domain-name *name*	Defines a default domain name that the Cisco IOS Software uses to complete unqualified host names; also part of the fully qualified DNS name
ip domain-list *name*	Defines a list of default domain names to complete unqualified host names
ip name-server *ip-address*	Specifies the address of one or more name servers to use for name and address resolution; up to six name servers permitted

Table 2-7 *TFTP Concepts*

Concept	Description
Well-known port numbers	UDP port 69 (UDP is typically the only supported protocol for TFTP produced by vendors) and TCP port 69
copy tftp flash	Cisco IOS command to copy images from a TFTP server
Security	Only filename and directory names created on the server provide the only method used to secure transfers

Table 2-8 *HTTPs and SSL Concepts*

Concept	Description
Well-known port number	TCP port 443-SSL.
HTTPs	HTTP traffic runs over a secure connection.
Service/client authentication	SSL uses a client/server model where clients request secure connections to a host device, such as with a credit card transaction over the World Wide Web.

Table 2-9 *SNMP Concepts*

Concept	Description
Well-known port numbers	UDP 161 (SNMP servers) and UDP 162 (SNMP clients).
SNMP managed device	A network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and make this information available to the network management system using SNMP.
SNMP agent	A network management software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP.

Table 2-10 *SMTP Concepts*

Concept	Description
Well-known port numbers	TCP 25 (commonly used) and UDP 25
HELO command	Used in communications between host and client

Table 2-11 *NTP Concepts*

Concept	Description
Well-known port numbers	TCP 123 and UDP 123 (commonly used).
ntp master *1-15*	Defines stratum value between 1 and 15.
clock set *hh*:*mm*:*ss day month year*	Manually sets clock on a Cisco router.
ntp peer *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**]	Defines NTP peers.
ntp server *ip-address*	Defines where the device will source the clock from.
ntp authenticate	Enables authentication.
ntp authentication-key *number* **md5** *value*	Defines NTP authentication key and password.
ntp trusted-key *key-number*	Defines NTP to authenticate NTP session; *key-number* is the authentication key to be trusted.

Table 2-12 *Cisco IOS SSH Configurations Steps**

Step	Description
1	Configure the **hostname** command.
2	Configure the DNS domain.
3	Generate the public RSA key to be used.
4	Enable SSH transport support for the vtys. SSH transport is enabled by default. Also, the final step (not documented at Cisco.com) is to create a local username/password pair or enable AAA authentication.

*For an example of this configuration, visit http://cisco.com/en/US/tech/tk583/tk617/technologies_tech_note09186a00800949e2.shtml.

Q & A

The Q & A questions are designed to help you assess your readiness for the topics covered on the CCIE Security written exam and those topics presented in this chapter. This format should help you assess your retention of the material. A strong understanding of the answers to these questions will help you on the CCIE Security written exam. You can also look over the questions at the beginning of the chapter again for further review. As an additional study aid, use the CD-ROM provided with this book to take simulated exams, which draw from a database of over 500 multiple-choice questions.

Answers to these questions can be found in Appendix A, "Answers to Quiz Questions."

1. According to RFC 1700, what is the well-known TCP/UDP port used by DNS?
2. What does the Cisco IOS command **no ip domain-lookup** accomplish?
3. What is the correct Cisco IOS syntax to specify local host mapping on a Cisco router?
4. TFTP uses what well-known, defined TCP/UDP port?
5. Define the two modes of FTP.
6. FTP uses what TCP port numbers?
7. What well-known port do Secure Sockets Layer (SSL) and Secure Shell (SSH) use?
8. Define SNMP and give an example of how SNMP traps can be used to identify problems with Cisco IOS routers.
9. What well-known UDP ports are used by SNMP?
10. What Cisco IOS command enables SNMP on a Cisco IOS router?
11. Which TCP/UDP port numbers are defined for use by the Network Time Protocol (NTP)?
12. When defining a stratum value on a Cisco router, what is the range and what value is closest to an atomic clock?
13. Secure Shell (SSH) allows what to be accomplished when in use?
14. What is the difference between an SNMP inform request and an SNMP trap?
15. What does the SNMP MIB refer to?
16. What is the SNMP read-write community string for the following router configuration?

```
snmp-server community simon ro
snmp-server community Simon rw
```

17. Before you can TFTP a file from a Cisco router to a UNIX- or Windows-based system, what is the first step you must take after enabling the TFTP server daemon on either platform?
18. What Cisco IOS command can be implemented to restrict SNMP access to certain networks by applying access-lists? Can you apply standard, extended, or both to these access lists?
19. Does TFTP have a mechanism for username and password authentication?
20. Can you use your Internet browser to configure a Cisco router? If so, how?
21. Suppose that a network administrator defines a Cisco router to allow HTTP requests but forgets to add the authentication commands. What is the default username and password pairing that allows HTTP requests on the default TCP port 80? Can you predefine another TCP port for HTTP access other than port 80?
22. What are the four steps to enable Cisco IOS SSH for a SSH server?

Scenario

Scenario: Configuring DNS, TFTP, NTP, and SNMP

This scenario uses a configuration taken from a working Cisco IOS router and tests your skills with DNS, TFTP, NTP, and SNMP. Example 2-14 displays the configuration of a Cisco router named R1.

Example 2-14 *R1 Running Configuration*

```
version 12.1
hostname R1
clock timezone UTC 10
!
no ip domain-lookup
ip domain-name cisco.com
ip host CCIE 131.108.1.1
ip host Router3 131.108.1.3
ip host Router2 131.108.1.2
ip host Router1 131.108.1.1
ip name-server 131.108.255.1
ip name-server 131.108.255.2
interface Ethernet0/0
 ip address 131.108.1.1 255.255.255.0
!
interface Serial0/0
 ip address 131.108.255.1 255.255.255.252
 ntp broadcast
!
no ip http server
snmp-server community public RO
snmp-server community publiC RW
snmp-server host 131.108.255.254 isdn
line con 0
!
ntp authentication-key 1 md5 121A061E17 7
ntp authenticate
ntp trusted-key 1
ntp master 1
ntp peer 131.108.2.1 key 1
end
```

1. What happens when a network administrator types the host name Router1 at the router prompt? (Select the best two answers.)

   a. DNS queries are disabled; nothing will be translated.

   b. The name Router1 is mapped to the IP address 131.108.1.1.

   c. The administrator could also type CCIE to reach the same IP address (131.108.1.1).

   d. Because DNS is disabled with the command **no ip domain-lookup**, the router assumes that this is an invalid Cisco IOS command and returns the error "% Unknown command or computer name, or unable to find computer address."

   e. Local DNSs are case-sensitive so you can only type Router1 to map to 131.108.1.1.

2. The following commands are entered on the router named R1. What are the TFTP server address and TFTP filename stored on the router on board flash?

```
R1#copy tftp flash
Address or name of remote host []? 150.100.1.253
Source filename []? c2600-jo3s56i-mz.121-5.T10.bin
Destination filename [c2600-jo3s56i-mz.121-5.T10.bin]? c2600-c1
```

3. R1 supplies an NTP clock source to a remote router. What is the NTP peer IP address, and what is the MD5 password used to ensure that NTP sessions are authenticated?

4. What is the SNMP read-write access community string for the following configuration?

```
snmp-server community public RO
snmp-server community publiC RW
```

Scenario Answers

Scenario Solutions

1. b and c. The host name Router1 (not case sensitive) is mapped to 131.108.1.1 with the command **ip host Router1 131.108.1.1**. Also, the Cisco IOS command **CCIE** is mapped to the same name with the Cisco IOS command **ip host CCIE 131.108.1.1**. If you look at the IP address assigned to Ethernet 0/0, it is the local IP address. Therefore, if a user types **Router1** or **CCIE**, they will be returned to the same router. The following sample display demonstrates this fact:

```
R1#router1
Translating "router1"
Trying Router1 (131.108.1.1)... Open
User Access Verification
Password:
R1>quit
! quit commands exit Telnet session and you return
! to the first Telnet connection on R1
[Connection to router1 closed by foreign host]
R1#ccie
Translating "ccie"
Trying CCIE (131.108.1.1)... Open
User Access Verification
Password:
R1>
```

   Both DNS names, CCIE and Router1, are translated to the same IP address, 131.108.1.1.

2. The TFTP server address is 150.100.1.253 and the filename requested is c2600-jo3s56i-mz.121-5.T10.bin. However, the last command entered is the destination filename, which defines the names stored locally on the system flash. In this case, the network administrator types the filename c2600-c1.

3. R1 is configured statically to peer to the remote NTP IP address, 131.108.2.1 (**ntp peer 131.108.2.1 key 1**). The MD5 password is configured but, unfortunately, the configuration will not display the MD5 password (encrypted), so it cannot be derived.

4. The read-only (**RO**) community string is named "public", and the read-write (**RW**) community string is set to "public". Community strings are case sensitive.

Exam Topics in This Chapter

- Cisco IOS specifics
- Routing and switching security features: IE MAC address controls, port security, DHCP snoop
- Security policy best practices

You can find a list of all of the exam topics in the introduction to this book. For the latest updates on exam topics, visit Cisco.com.

CHAPTER 3

Cisco IOS Specifics and Security

This chapter covers the CCIE Cisco IOS specifics topic area. Unfortunately, the blueprint does not detail the exact requirements, and "Cisco IOS" in general could mean the entire range of topics. Thus, this chapter covers topics that are actually possible topics on the written exam and that are common to the routing and switching blueprint. This chapter covers routing and switching blueprint objectives together with the security blueprint objectives. The CCIE technical teams generally gather the test questions from a common pool available to any CCIE track.

This chapter covers the following topics:

- **Cisco Hardware**—Covers the hardware components on a Cisco router, namely the System Flash, nonvolatile RAM (NVRAM), and how files are saved to and from a TFTP server.
- **show and debug Commands**—Presents the most common **show** and **debug** commands used on Cisco routers to manage an IP network.
- **Password Recovery**—Describes how password recovery is completed on Cisco IOS routers.
- **Basic Security on Cisco Routers**—Reviews some commands used to ensure that Cisco routers are secured with basic passwords.
- **IP Access Lists**—Covers both standard and extended IP access lists and their formats.
- **Layer 2 Switching Security**—Introduces MAC address controls, port security on Cisco switches, and Dynamic Host Configuration Protocol (DHCP) security options.
- **Security Policy Best Practices: A Cisco View**—Takes a brief look at Cisco-recommended best practices for developing a security policy.

"Do I Know This Already?" Quiz

The purpose of this assessment quiz is to help you determine how to spend your limited study time.

If you can answer most or all of these questions, you might want to skim the "Foundation Topics" section and return to it later, as necessary. Review the "Foundation Summary" section and answer the questions at the end of the chapter to ensure that you have a strong grasp of the material covered.

If you already intend to read the entire chapter, you do not necessarily need to answer these questions now. If you find these assessment questions difficult, read through the entire "Foundation Topics" section and review it until you feel comfortable with your ability to answer all of these and the "Q & A" questions at the end of the chapter.

Answers to these questions can be found in Appendix A, "Answers to Quiz Questions."

1. What IOS command will display the System Flash?
   a. show flash
   b. show system flash
   c. show memory
   d. show process flash
2. The network administrator has forgotten the enable password, and all passwords are encrypted. What should the network administrator do to recover the password without losing the current configuration?
   a. Call the TAC and ask for a special backdoor password.
   b. Call the TAC and raise a case to supply the engineering password.
   c. Reboot the router, press the Break key after the reload, and enter ROM mode and change the configuration register.
   d. Reboot the router, press the Break key during the reload, enter ROM mode and change the configuration register, and when the router reloads, remove the old configuration.
3. What is the enable password for the following router?

```
enable password Simon
```

   a. More data is required.
   b. Simon.
   c. simon or Simon.
   d. You cannot set the password to a word; it must also contain digits.
4. If the configuration register is set to 0x2101, where is the IOS image booted from?
   a. slot0:
   b. slot1:
   c. Flash
   d. ROM
   e. TFTP server

5. What IOS command will copy the running configuration to a TFTP server?

   a. **copy running-config to tftp**

   b. **write network**

   c. **copy running-config tftp**

   d. **write erase**

6. What **debug** command allows an administrator to debug only packets from the network 131.108.0.0/16?

   a. `debug ip packet`

   b. `terminal monitor`

   c. `debug ip packet 1`
      `access-list 1 permit 131.108.0.0`

   d. `debug ip packet 1`
      `access-list 1 permit 131.108.0.0 0.0.255.255`

   e. `debug ip packet 1`
      `access-list 1 permit 131.108.0.0 255.255.0.0`

7. After entering **debug ip packet**, no messages appear on your Telnet session. What is the likely cause?

   a. OSPF routing is required.

   b. The console port does not support debug output.

   c. The **terminal monitor** command is required.

   d. IP packets are not supported with the **debug** command.

8. To change the configuration register to 0x2141, what is the correct IOS command?

   a. **copy running-config register**

   b. **configuration 0x2141**

   c. **config 0x2141 register**

   d. **config-register 0x2142**

   e. **config-register 0x2141**

9. Where is the startup configuration stored on a Cisco router?

   a. In the CAM table

   b. NVRAM

   c. RAM

   d. Flash

   e. slot0:

10. Which of the following statements is true?

    a. The **enable secret** command overrides the **enable password** command.

    b. The **enable** command overrides the **enable secret** *password* command.

    c. Enable passwords cannot be used when the secret password is used.

    d. Both a and c are true.

11. A Cisco router has the following configuration:

```
line vty 0 4
login
```

    What will happen when you telnet to the router?

    a. You will be prompted for the login password.

    b. You will enter EXEC mode immediately.

    c. You will not be able to access the router without the password set.

    d. More configuration is required.

12. A Cisco router has the following configuration:

```
line vty 0 4
no login
password cIscO
```

    When a Telnet user tries to establish a remote Telnet session to this router, what will happen?

    a. The Telnet user will be prompted for the login password, which is set to cIscO.

    b. The Telnet user will enter EXEC mode immediately.

    c. The Telnet user will not be able to access the router without the password set.

    d. More configuration is required.

    e. The Telnet user will be prompted for the login password; password case does not matter.

13. A Cisco router has the following configuration:

```
line vty 0 1
no login
password cisco
line vty 2 4
login
password ciSco
```

When a third Telnet session is established to a remote router with the preceding configuration, what will happen?

a. You will be prompted for the login password, which is set to cisco.

b. You will be prompted for the login password, which is set to ciSco.

c. You will enter EXEC mode immediately.

d. You will not be able to access the router without the password set.

e. More configuration is required.

14. Which of the following access lists will deny any IP packets sourced from network 131.108.1.0/24 and destined for network 131.108.2.0/24 and permit all other IP-based traffic?

a.
```
access-list 1 deny 131.108.1.0
```

b.
```
access-list 1 deny 131.108.1.0 0.0.0.255
```

c.
```
access-list 100 permit/deny ip 131.108.1.0 0.0.0.255 131.108.2.0 0.0.0.255
```

d.
```
access-list 100 deny ip 131.108.1.0 0.0.0.255 131.108.2.0 0.0.0.255
access-list 100 permit ip any any
```

15. Which of the following *secure* protocols are available to manage Cisco IOS software? (Choose the best three answers.)

a. Telnet

b. SSH

c. HTTPS

d. HTTP

e. IPSec-ESP

f. IPSec-AH

16. What types of attacks can intruders use to enable them to attack VLANs on a Layer 2 switched network?

a. CAM table overflow

b. VLAN manipulation or hopping

c. BPDU manipulation

d. MAC address spoofing

e. DHCP starvation

f. All of these

17. What information is stored in the CAM table?
    a. IP-to-MAC address information
    b. BPDU details
    c. The CAM table is only used on routers
    d. MAC information mapped to port interfaces
18. How can the CAM table be exploited by intruders?
    a. It cannot be exploited.
    b. CAM tables can be used to forward all packets to certain interfaces by flooding the switch with the MAC address's source by one or more interfaces.
    c. It can be used to gain Telnet access.
    d. It can be used to cause a memory leak attack.
19. What is VLAN hopping?
    a. Using a trunk port to access all VLANs, thus bypassing an access control device
    b. Modifying the 802.1p field to an IP packet, causing the switch to put the attacker's port in a different VLAN
    c. Sniffing a Layer 2 port to determine the DSCP fields
    d. None of these
20. How is a DHCP starvation attack achieved?
    a. Freeing IP packets so that they can traverse the network endlessly
    b. Broadcasting DHCP requests with spoofed MAC addresses
    c. Intercepting DHCP offer packets and performing a DOS attack on the DHCP server
    d. None of these
21. When preparing a security policy, what are the three core requirements?
    a. Define a password list.
    b. Create acceptable-usage policy statements.
    c. Conduct a risk analysis.
    d. Establish a security team structure.
    e. None of these.

22. An administrator notices a router's CPU utilization has jumped from 2 percent to 100 percent, and that a CCIE engineer was debugging. What IOS command can the network administrator enter to stop all debugging output to the console and vty lines without affecting users on the connected router?

a. **no logging console debugging**

b. **undebug all**

c. **line vty 0 4**

d. **no terminal monitor (term no monitor)**

e. **reload the router**

Foundation Topics

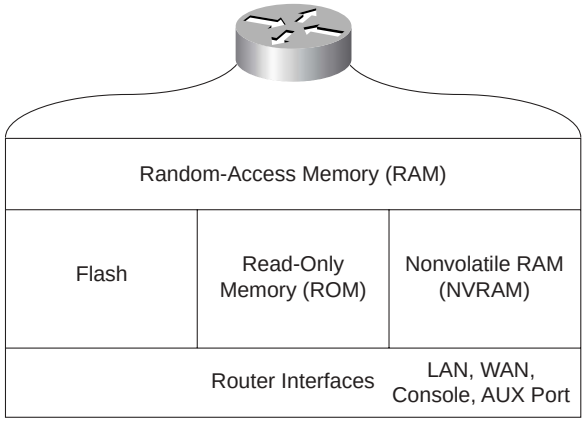
Cisco Hardware

Cisco routers consist of many hardware components. The main components of a Cisco router include the following:

- RAM
- NVRAM
- Flash
- CPU
- ROM
- Configuration registers
- Interfaces

Figure 3-1 illustrates the hardware components on Cisco routers.

Figure 3-1 *Components of a Cisco Router*



Each hardware component is vital for Cisco routers to operate properly. To help you prepare for the CCIE Security written exam, the next few sections present the main concepts you need to know about Cisco hardware components.

Random-Access Memory

Routers use RAM to store the current configuration file and other important data collected by the router (such as Cisco Express Forwarding [CEF] tables and Address Resolution Protocol [ARP] entries, to name a few). This data includes the IP routing table and buffer information. Buffers temporarily store packets before they are processed. All Cisco IOS processes, such as routing algorithms (Open Shortest Path First [OSPF] and Border Gateway Protocol [BGP], for example), also run in RAM.

RAM information is lost if the router power cycles (when a router loses and regains power) or is restarted by an administrator. To view a router's current configuration, use the **show running-config** IOS command. Before Cisco IOS version 10.3, administrators used the **write terminal** command to show a router's configuration. The **write terminal** command is still valid in today's Cisco IOS releases, although Cisco IOS releases 12.2T and above now provide a warning to use the new commands only.

Cisco IOS software is hardware-specific, and the image loaded on various router platforms varies from platform to platform. For example, the image on a Cisco 4500 (end of sale in 2004) will not run on a Cisco 3600, nor will an image designed for an 1800 run on the 3800. Also, IOS images contain certain features, such as Internetwork Packet Exchange (IPX) or Data Encryption Standard (DES) encryption. For example, you can load only Cisco IOS software that supports IP or IP plus DES encryption, and so forth.

Visit the following Cisco website for more details on Cisco IOS images and platform requirements: http://www.cisco.com/public/sw-center/sw-ios.shtml.

Nonvolatile RAM

NVRAM stores a copy of the router's configuration file. The NVRAM storage area is retained by the router in the event of a power cycle. When the router powers up from a power cycle or a reboot (**reload** command), the Cisco IOS software copies the stored configuration file from the NVRAM to RAM. To view the configuration file stored in NVRAM, issue the **show startup-config** command. In earlier versions of Cisco IOS software (before version 10.3), the **show config** command was used to view the configuration file stored in NVRAM. In Cisco IOS versions 11.0 and above, both the **show config** and **show startup-config** commands will work. The crypto keys are also stored in NVRAM.

System Flash

The System Flash is erasable and programmable memory used to store the router's IOS image. Although Flash memory is always limited in size, it can contain multiple versions of Cisco IOS software. Therefore, you can delete, retrieve, and store new versions of Cisco IOS software in the

Flash memory system. To view the Flash memory on a Cisco router, use the **show flash** IOS command. Example 3-1 displays the Flash filename on a router named R1.

> **NOTE** On a high-performance router, such as Cisco 3800 series or 7500 series routers, you can make the Flash system look like a file system and store many versions of Cisco IOS software. The IOS command to partition the System Flash is **partition flash** *number-of-partition size-of-each-partition*. Even on a low-end router, such as the 2500, the Flash can be partitioned.

Example 3-1 **show flash** *Command*

```
R1>show flash
System flash directory:
File  Length   Name/status
  1   9558976  c2500-ajs40-l.12-17.bin
[9559040 bytes used, 7218176 available, 16777216 total]
16384K bytes of processor board System flash
```

Example 3-1 shows that the IOS image, c2500-ajs40-l.12-17.bin, is currently stored on the router's on-board System Flash.

The Cisco IOS series routers, such as the 7500 or 3800 series, provide the option of installing additional PCMCIA Flash memory. If this additional memory is installed, the **dir slot0**: IOS command displays the IOS image stored in slot0.

> **NOTE** Cisco recently renamed all of its IOS images to permit a total of only eight possible trains. Visit http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml for more details. This link requires a Cisco CCO account.

Central Processing Unit

The CPU is the heart of a router, and every Cisco router has a CPU. A CPU manages all the router's processes, such as IP routing, and new routing entries, such as remote IP networks learned through a dynamic routing protocol.

To view a CPU's status, use the **show process** IOS command.

Example 3-2 shows a sample display taken from a Cisco IOS router.

Example 3-2 *(Truncated)* **show process** *Command*

```
R1>show process
CPU utilization for five seconds: 9%/7%; one minute: 9%;
five minutes: 10%
PID QTy   PC      Runtime (ms)  Invoked  uSecs   Stacks TTY Proc
  1 Csp  318F396  24456   1043   234     732/1000  0    Load Meter
  2 M*         0     28     28  1000     3268/4000 0    EXEC
  3 Lst  317D1FC   1304    175  5257     1724/2000 0    Check heap
...
```

The **show process** command displays the router utilization within the past 5 seconds, the past 1 minute, as well as the average over the last 5 minutes. Details about specific processes follow the CPU utilization statistics.

Read-Only Memory

ROM stores a scaled-down version of a router's IOS image in the event that the Flash system becomes corrupted or no current IOS image is stored in Flash. ROM also contains the bootstrap program (sometimes referred to as the rxboot image in Cisco documentation) and a device's power-up diagnostics. You can perform a software upgrade (that is, perform a software image upgrade on ROM) only by replacing ROM chips, because ROM is not programmable.

The bootstrap program enables you to isolate or rule out hardware issues. For example, suppose that you have a faulty Flash memory card and, subsequently, the router cannot boot the IOS image. The power diagnostics program tests all the hardware interfaces on the router. ROM mode contains a limited number of IOS commands, which enable the administrator or the Technical Assistance Center (TAC) to help troubleshoot and ascertain any hardware or configuration issues on a Cisco router. Cisco TAC is available 24 hours a day, 7 days a week. You must pay Cisco for this service and have a valid contract number to open any cases.

Unfortunately, not all Cisco routers have the same ROM code, so the commands might vary, but the principle remains the same. You can always issue the **?** command in ROM mode to identify the available commands used to troubleshoot a Cisco IOS–based router. Newer Cisco hardware models now contain a new boot program stored in boot Flash rather than in ROM. The program is a little more user-friendly. Menu-driven options are available to change the configuration register, for example.

Example 3-3 provides all the available options on a Cisco 3800 router when the **?** command is used in ROM mode.

Example 3-3 **?** *Command Used When in ROM Mode*

```
System Bootstrap, Version 12.0(3)T, RELEASE SOFTWARE (fc1)
Copyright  1999 by cisco Systems, Inc.
C1700 platform with 49152 Kbytes of main memory
rommon 1 > ?
alias               set and display aliases command
boot                boot up an external process
break               set/show/clear the breakpoint
confreg             configuration register utility
cont                continue executing a downloaded image
context             display the context of a loaded image
cookie              display contents of cookie PROM in hex
I                   Initialize
dev                 list the device table
unalias             unset an alias
unset               unset a monitor variable
xmodem              x/ymodem image download
```

The options in Example 3-3 include the ability to initialize a router with the **i** command after you have finished ROM mode. ROM mode enables you to recover lost passwords by altering the configuration registers (covered in the "Password Recovery" section, later in this chapter).

Configuration Registers

The configuration register is a 16-bit number that defines how a router operates on a power cycle. These options include whether the IOS image will be loaded from Flash or ROM. Configuration registers advise the CPU to load the configuration file from the NVRAM or to ignore the configuration file stored in memory, for example. The default configuration register is displayed as 0x2102. Table 3-1 lists the binary conversion from 0x2102.

Table 3-1 *x2102 Binary Conversion*

Bit Number	Value
15	0
14	0
13	1
12	0
11	0
10	0

Table 3-1 *x2102 Binary Conversion (Continued)*

Bit Number	Value
9	0
8	1
7	0
6	0
5	0
4	0
3	0
2	0
1	1
0	0

Visit http://www.cisco.com/en/US/products/hw/routers/ps282/products_installation_guide_chapter09186a008007dfd0.html#wp1010336 for more details on the Configuration Register Settings.

The bits are numbered from right to left. In the preceding example, the value is displayed as 0x2102 (0010.0001.0000.0010). The function of the configuration register bits is determined by their position, as follows:

- **Bits 0 through 3**—Determines whether the router loads the IOS from the Flash. Possible values are 00 - stays at the ROM monitor on a reload or power cycle, 01 - boots the first image in CompactFlash memory as a system image, or 02 - F enables default booting from CompactFlash memory. In Hexadecimal the range is 0x0000-0x000F.
- **Bit 4**—Reserved.
- **Bit 5**—Reserved.
- **Bit 6**—Tells the router to load the configuration from NVRAM if set to 1 and to ignore the NVRAM if set to 0.
- **Bit 7**—Referred to as the original equipment manufacturer (OEM) bit in Cisco documentation and is not used.
- **Bit 8**—Specifies whether to enter ROM mode without power cycling the router. If bit 8 is set to 1 and the Break key is issued while the router is up and running normally, the router will go into ROM mode. This is a dangerous scenario, because if this occurs, your router immediately stops functioning.

- **Bit 9**—Causes the system to use the secondary bootstrap. This bit is typically not used and is set to 0.
- **Bit 10**—Specifies the broadcast address to use, where 1 equals the use of all 0s for broadcast at boot (in conjunction with bit 14). Bit 10 interacts with bit 14.
- **Bits 11 and 12**—Set the console port's baud rate. For example, if bits 11 and 12 are set to 00, the baud rate is 9600 bps. A baud rate of 4800 bps can be set when these bits are set to 01. 10 sets the baud rate to 2400 bps, and 11 sets the baud rate to 1200 bps.
- **Bit 13**—Tells the router to boot from ROM if the Flash cannot boot from a network, such as a TFTP server. If bit 13 is set to 0 and no IOS image is found, the router will hang. If bit 13 is set to 1 and no IOS image is found, the router boots from ROM.
- **Bit 14**—Interacts with bit 10 to define the broadcast address.
- **Bit 15**—Specifies whether to enable diagnostics display on startup and ignore the NVRAM.

To view the current configuration register, use the **show version** IOS command.

Example 3-4 displays the configuration register of a router, R1 (taken from a 7500 series router).

Example 3-4 *(Truncated)* **show version Command**

```
Router1> show version
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-J-M), Experimental Version 11.3(19970915:164752) [
hampton-nitro-baseline 249]
Copyright  1986-1997 by cisco Systems, Inc.
Compiled Wed 08-Oct-97 06:39 by hampton
Image text-base: 0x60008900, data-base: 0x60B98000

ROM: System Bootstrap, Version 11.1(11855) [beta 2], INTERIM SOFTWARE
BOOTFLASH: 7200 Software (C7200-BOOT-M), Version 11.1(472), RELEASE SOFTWARE (fc1)

Router1 uptime is 23 hours, 33 minutes
System restarted by abort at PC 0x6022322C at 10:50:55 PDT Tue Oct 21 1997
System image file is "tftp://171.69.1.129/hampton/nitro/c7200-j-mz"

cisco 7206 (NPE150) processor with 57344K/8192K bytes of memory.
R4700 processor, Implementation 33, Revision 1.0 (512KB Level 2 Cache)
Last reset from power-on
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
8 Ethernet/IEEE 802.3 interface(s)
2 FastEthernet/IEEE 802.3 interface(s)
```

Example 3-4 *(Truncated)* **show version Command**

```
4 Token Ring/IEEE 802.5 interface(s)
4 Serial network interface(s)
1 FDDI network interface(s)
125K bytes of non-volatile configuration memory.
1024K bytes of packet SRAM memory.

20480K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
20480K bytes of Flash PCMCIA card at slot 1 (Sector size 128K).
4096K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x2102
```

The output from Example 3-4 displays the configuration register as 0x2102. The **show version** command also displays other useful router information, such as the router's uptime, the IOS image in use, and the hardware configuration. To change the configuration register, use the global configuration command, **configure-register** *register-value*. When a configuration register is changed, use the **show version** command to ensure that the register has been changed to the new value.

Table 3-2 displays common configuration register values you can use in day-to-day troubleshooting of Cisco IOS routers.

Table 3-2 *Common Registers*

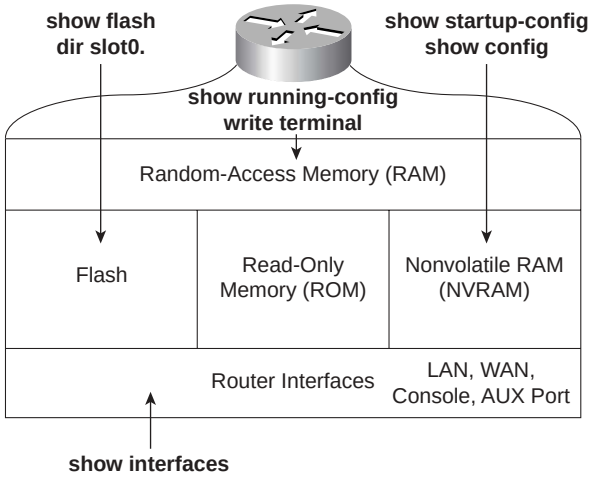
Register Value	Description
0x2100	Boots the router using the system bootstrap found in ROM.
0x2102	Boots the router using Flash and NVRAM. This is the default setting.
0x2142	Boots the router using Flash and ignores NVRAM. This value is used to recover passwords or modify configuration parameters.

Cisco Interfaces

Interfaces provide connections to a network. Interfaces include LANs, WANs, and management ports (that is, console and auxiliary ports).

To view the current LAN or WAN interfaces, issue the **show interface** command, which displays all LAN and WAN interfaces. To display information regarding console or auxiliary ports, use the **show line** command. Figure 3-2 summarizes the available IOS commands that administrators can use to view a router's current configuration.

Figure 3-2 *Interface IOS Commands*



Now that you have reviewed Cisco router hardware basics, it is time to review how routers operate. In addition to router operation, this chapter covers how administrators can manage Cisco routers by saving and loading files to and from a TFTP server.

NOTE Cisco routers can operate in a number of modes. Cisco defines them as follows:

- **ROM boot mode**—When the router is in boot mode and loaded with a subset of the IOS image, only a limited number of commands are available.
- **Configuration mode**—Where you make configuration changes. An example prompt is Router1(config)#.
- **Interface configuration mode**—Where you make configuration changes to interfaces such as the Ethernet or Serial connections. An example prompt is Router1(config-if)#.
- **Initial configuration mode**—When a router first boots up out of the box with no initial configuration, you are prompted for basic system configuration details, such as name and IP address assignment. The prompt looks like this:

```
Would you like to answer the initial configuration dialog? [yes/no]
```

- **User EXEC mode**—Basic IOS commands are permitted from the command-line interface (CLI). An example prompt is R1>.
- **Privileged EXEC mode (also referred to as enabled mode)**—Advance IOS commands are permitted when the enable password or secret password is entered from the CLI. An example prompt is R1#.

Saving and Loading Files

The configuration file can reside on the router's NVRAM or RAM, or on a TFTP server. When a router boots with the default configuration register (0x2102), the configuration file is copied from NVRAM to RAM.

Network administrators typically save the configuration files to a TFTP server as a backup, in case of a router failure.

To save a configuration file from RAM to NVRAM (after configuration changes are made), the IOS command is **copy running-config startup-config**. The **write memory** (legacy IOS command, removed in 12.2T versions) command will also copy the running configuration to startup configuration. The **write** command is a legacy command from earlier releases of IOS that is still valid in today's versions of Cisco IOS software.

Example 3-5 displays a successful configuration change on Ethernet 0/0, followed by a network administrator in PRIV EXEC (privileged EXEC mode) mode saving the new configuration file to NVRAM.

Example 3-5 *Saving Cisco IOS Configuration Files*

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface ethernet 0/0
R1(config-if)#ip address 131.108.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#exit

R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Table 3-3 summarizes the configuration file manipulation that can be performed on Cisco IOS routers.

Table 3-3 *Cisco IOS File Manipulations*

Cisco IOS Command	Meaning
copy running-config startup-config	Copies the configuration file from RAM to NVRAM.
write memory	Copies the running configuration to NVRAM. (Superseded by the new command, **copy running-config startup-config**.)
copy startup-config running-config	Copies the configuration file from NVRAM to RAM.

continues

Table 3-3 *Cisco IOS File Manipulations (Continued)*

Cisco IOS Command	Meaning
write terminal	Displays the current configuration file in RAM. (Superseded by the new command, **show running-config**.)
show config	Displays the current configuration file in NVRAM. (Superseded by the new command, **show startup-config**.)
copy running-config tftp	Copies the configuration file stored in RAM to a TFTP server. Can also be copied to an FTP or Remote Copy (RCP) server.
copy tftp running-config	Copies a configuration file from a TFTP server to the running configuration.
write memory	Copies the running configuration to NVRAM.
write erase	Clears the NVRAM.

show and debug Commands

Cisco IOS CLI has an enormous number of **show** and **debug** commands available to the privileged EXEC user. This section covers the **show** and **debug** commands most often used to manage Cisco IOS devices.

Router CLI

Cisco IOS routers give network administrators access to a wide range of **show** and **debug** commands. The **show** command displays various information about the router's state of play, such as the Ethernet collisions on a particular interface or a router's configuration file. Only a subset of **show** commands is available when in user EXEC mode. The full range is available when in PRIV EXEC mode.

The **debug** command is a more advanced IOS command that allows the administrator to view the router's analyses of packets or buffering mechanisms and is used only to troubleshoot a device or a complete network. The **debug** command is very CPU-intensive.

show Commands

The best method to appreciate the use of **show** commands is to display sample output from a Cisco IOS router.

Example 3-6 displays a list of truncated **show** commands available from the CLI on a Cisco router in PRIV EXEC mode. (Version 12.2 was used to supply this output.)

Example 3-6 **show** *Commands*

```
R1#show ?
  access-expression        List access expression
  access-lists             List access lists
  accounting               Accounting data for active sessions
  adjacency                Adjacent nodes
  aliases                  Display alias commands
  arp                      ARP table
  async                    Information on terminal lines used as router
                           interfaces
  backup                   Backup status
  bgp                      BGP information
  bridge                   Bridge Forwarding/Filtering Database [verbose]
  buffers                  Buffer pool statistics
  caller                   Display information about dialup connections
  cef                      Cisco Express Forwarding
  class-map                Show QoS Class Map
  clock                    Display the system clock
  configuration            Contents of Non-Volatile memory
  connection               Show Connection
  context                  Show context information
  controllers              Interface controller status
  cops                     COPS information
  crypto                   Encryption module
  debugging                State of each debugging option
  derived-config           Derived operating configuration
  dhcp                     Dynamic Host Configuration Protocol status
  diag                     Show diagnostic information for port
                           adapters/modules
  dial-peer                Dial Plan Mapping Table for, e.g. VoIP Peers
  dialer                   Dialer parameters and statistics
  dialplan                 Voice telephony dial plan
  diffserv                 Differentiated services
  dlsw                     Data Link Switching information
  dnsix                    Shows Dnsix/DMDP information
  docsis                   Show DOCSIS
  drip                     DRiP DB
  dspu                     Display DSPU information
  dxi                      atm-dxi information
  entry                    Queued terminal entries
  environment              Environmental monitor statistics
  exception                exception informations
  file                     Show filesystem information
  flash:                   display information about flash: file system
  frame-relay              Frame-Relay information
  fras                     FRAS Information
  fras-host                FRAS Host Information
  gateway                  Show status of gateway
  history                  Display the session command history
```

continues

Example 3-6 **show** *Commands (Continued)*

```
  hosts                    IP domain-name, lookup style, nameservers, and host
                           table
  html                     HTML helper commands
  idb                      List of Hardware Interface Descriptor Blocks
  interfaces               Interface status and configuration
  ip                       IP information (show ip route follows)
  ipv6                     IPv6 information
  key                      Key information
  line                     TTY line information
  llc2                     IBM LLC2 circuit information
  lnm                      IBM LAN manager
  local-ack                Local Acknowledgement virtual circuits
  location                 Display the system location
  logging                  Show the contents of logging buffers
  memory                   Memory statistics
  mgcp                     Display Media Gateway Control Protocol information
  microcode                show configured microcode for downloadable hardware
  modemcap                 Show Modem Capabilities database
  mpoa                     MPOA show commands
  ncia                     Native Client Interface Architecture
  netbios-cache            NetBIOS name cache contents
  ntp                      Network time protocol
  num-exp                  Number Expansion (Speed Dial) information
  parser                   Display parser information
  pas                      Port Adaptor Information
  pci                      PCI Information
  policy-map               Show QoS Policy Map
  ppp                      PPP parameters and statistics
  printers                 Show LPD printer information
  privilege                Show current privilege level
  processes                Active process statistics
  protocols                Active network routing protocols
  registry                 Function registry information
  reload                   Scheduled reload information
  rmon                     rmon statistics
  route-map                route-map information
  running-config           Current operating configuration
  sessions                 Information about Telnet connections
  sgbp                     SGBP group information
  snmp                     snmp statistics
  spanning-tree            Spanning tree topology
  srcp                     Display SRCP Protocol information
  ssh                      Status of SSH server connections
  ssl                      Show SSL command
  stacks                   Process stack utilization
  standby                  Hot standby protocol information
  startup-config           Contents of startup configuration
  tcp                      Status of TCP connections
```

Example 3-6 **show** *Commands (Continued)*

```
  tech-support              Show system information for Tech-Support
  terminal                  Display terminal configuration parameters
  traffic-shape             traffic rate shaping configuration
  users                     Display information about terminal lines
  version                   System hardware and software status
  vlans                     Virtual LANs Information
  vtemplate                 Virtual Template interface information
  whoami                    Info on current tty line
```

This section briefly covers the shaded commands in Example 3-6.

Example 3-7 displays sample output from the most widely used IOS command, **show ip route**.

Example 3-7 **show ip route** *Command*

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
     131.108.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       131.108.255.0/30 is directly connected, Serial0/0
O       131.108.2.0/24 [110/400] via 131.108.255.2, 00:00:03, Serial0/0
C       131.108.1.0/24 is directly connected, Ethernet0/0
R1#show ip route ?
  Hostname or A.B.C.D  Network to display information about or hostname
  bgp                  Border Gateway Protocol (BGP)
  connected            Connected
  egp                  Exterior Gateway Protocol (EGP)
  eigrp                Enhanced Interior Gateway Routing Protocol (EIGRP)
  dhcp                 Show routes added by DHCP Server or Relay
  igrp                 Interior Gateway Routing Protocol (IGRP)
  isis                 ISO IS-IS
  list                 IP Access list
  mobile               Mobile routes
  odr                  On Demand stub Routes
  ospf                 Open Shortest Path First (OSPF)
  profile              IP routing table profile
  rip                  Routing Information Protocol (RIP)
  static               Static routes
  summary              Summary of all routes
  supernets-only       Show supernet entries only
```

continues

Example 3-7 **show ip route** *Command (Continued)*

```
  vrf                  Display routes from a VPN Routing/Forwarding instance
  |                    Output modifiers
  <cr>

R1#show ip route ospf
     131.108.0.0/16 is variably subnetted, 3 subnets, 2 masks
O       131.108.2.0/24 [110/400] via 131.108.255.2, 00:00:30, Serial0/0
R1#
```

Example 3-7 displays three IP routing entries. The more specific command, **show ip route ospf**, displays only remote OSPF entries. Every IOS command can be used with the **?** character to display more options. In this case, the network administrator used it to identify the **ospf** option and then typed **show ip route ospf** to view only remote OSPF entries.

Example 3-8 displays the output from the **show ip access-lists** IOS command**.**

Example 3-8 **show ip access-lists** *Command*

```
R1#show ip access-lists ?
  <1-199>      Access list number
  <1300-2699>  Access list number (expanded range)
  WORD         Access list name
  |            Output modifiers
  <cr>
R1#show ip access-lists
Standard IP access list 1
    permit 131.108.0.0, wildcard bits 0.0.255.255
Extended IP access list 100
    permit tcp any host 131.108.1.1 eq telnet
```

Example 3-8 enables the network administrator to quickly verify any defined access lists. Example 3-8 includes two access lists, numbered 1 and 100.

Use the **show debugging** command to display any **debug** commands in use. This verifies whether any debugging is currently enabled.

Example 3-9 displays the sample output when **debug ip routing** is enabled.

Example 3-9 **show debugging** *Command*

```
R1#show debugging
IP routing:
  IP routing debugging is on
R1#undebug all
All possible debugging has been turned off
```

Currently, the router in Example 3-9 is enabled for debugging IP routing. To turn off the debugging, apply the **undebug all** command, as shown in Example 3-9. This command ensures that all debug options are disabled. You can specify the exact debug option you want to disable with the **no** option; for example, to disable the IP packet option, the IOS command is **no debug ip packet**.

To display the hardware interfaces on the router, use the **show interfaces** command to explore the physical and statistical state.

Example 3-10 displays the **show interfaces** command on a router named R1.

Example 3-10 **show interfaces** *Command*

```
R1#show interfaces
Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is 0002.b9ad.5ae0 (bia 0002.b9ad.5ae0)
  Internet address is 131.108.1.1/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:01, output hang never
  Last clearing of "show interface" counters 00:00:05
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1 packets input, 366 bytes, 0 no buffer
     Received 1 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     3 packets output, 202 bytes, 0 underruns(0/0/0)
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Serial0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 131.108.255.1/30
  MTU 1500 bytes, BW 256 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set
  Keepalive set (10 sec)
  LMI enq sent  0, LMI stat recvd 0, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 0  LMI type is ANSI Annex D  frame relay DTE
  Broadcast queue 0/64, broadcasts sent/dropped 1/0, interface broadcasts 1
```

continues

Example 3-10 **show interfaces** *Command (Continued)*

```
  Last input 00:00:02, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:00:07
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 192 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     2 packets input, 86 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     2 packets output, 86 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up

Ethernet0/1 is administratively down, line protocol is down
  Hardware is AmdP2, address is 0002.b9ad.5ae1 (bia 0002.b9ad.5ae1)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 00:00:10
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns(0/0/0)
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Example 3-10 displays a router with two Ethernet interfaces and one serial interface. Interface Ethernet 0/0 is enabled and is currently running packets over the wire, while Ethernet 0/1 is not

enabled. Interface Serial 0/0 is configured for Frame Relay and the physical layer (Layer 1) details are displayed. Other possible physical states are as follows:

- **Ethernet0/1 is up, line protocol is up**—The Ethernet interface is active, sending and receiving Ethernet frames.
- **Ethernet0/1 is up, line protocol is down**—The Ethernet interface is cabled but no keepalives are received, and no Ethernet frames are sent or received (possible cable fault).
- **Ethernet0/1 is administratively down, line protocol is down**—The Ethernet interface is not enabled administratively; typically an interface is not enabled for connectivity as yet.
- **Ethernet 0/1 is down, line protocol is up**—A physical condition is not possible. The protocol is up only if the physical state of the line is up. The IOS image will never report this condition because it is not a possible state of any IOS interface.

To display the system log (syslog), use the **show logging** command. Example 3-11 displays sample output taken from a router named R1.

Example 3-11 **show logging** *Command*

```
R1#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited, 0 flushes,
 0 overruns)
    Console logging: level debugging, 27 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 1 messages logged
    Logging Exception size (4096 bytes)
    Trap logging: level debugging, 31 message lines logged
        Log Buffer (60000 bytes):
2d20h: %SYS-5-CONFIG_I: Configured from console by console
2d20h: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console
```

Example 3-11 shows that 27 messages have been logged and that the logging level is debugging, which entails the following log message types:

- **Emergencies**—System is unusable (severity = 0)
- **Alerts**—Immediate action needed (severity = 1)
- **Critical**—Critical conditions (severity = 2)
- **Errors**—Error conditions (severity = 3)
- **Warnings**—Warning conditions (severity = 4)
- **Notifications**—Normal but significant conditions (severity = 5)

- **Informational**—Informational messages (severity = 6)
- **Debugging**—Debugging messages (severity = 7)

Two messages have also been displayed on the terminal: the first message is a configuration change, and the second appears when a PRIV EXEC user has cleared the counters on all the interfaces.

The **show route-map** command displays any policy route maps configured. Policy route maps override routing decisions on Cisco routers. Route maps basically allow an administrator to change or modify a router to override the current IP routing table entries. The only caveat of this is that the **show ip route** command does not show the administrator routes following a route map. The **show route-map** command can be used instead.

The **show version** command displays the system's hardware configuration, the software version, the names and sources of configuration files, and the boot images. Issue the **show version** EXEC command to accomplish this. Example 3-12 displays sample output.

Example 3-12 **show version** *Command on R1*

```
R1#show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IK8O3S-M), Version 12.2(2)T,  RELEASE SOFTWARE (f
c1)
TAC Support: http://www.cisco.com/cgi-bin/ibld/view.pl?i=support
Copyright  1986-2001 by cisco Systems, Inc.
Compiled Sat 02-Jun-01 15:47 by ccai
Image text-base: 0x80008088, data-base: 0x813455F8
ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)
ROM: C2600 Software (C2600-IK8O3S-M), Version 12.2(2)T,  RELEASE SOFTWARE (fc1)
R1 uptime is 2 days, 20 hours, 15 minutes
System returned to ROM by reload at 14:57:18 UTC Mon Mar 1 1993
System restarted at 10:00:02 UTC Mon Mar 1 1993
System image file is "flash:c2600-ik8o3s-mz.122-2.T.bin"
cisco 2611 (MPC860) processor (revision 0x203) with 61440K/4096K bytes of memory
Processor board ID JAD043000VK (1947766474)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
2 Ethernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102
```

Example 3-12 displays a number of key components and identifies the hardware installed on the router. For example, the Cisco IOS software version is 12.2T, the router's uptime is 2 days, 20

hours, 15 minutes, and the memory installed on the router is 64 MB. There is 16 MB of System Flash, and the current configuration register is 0x2102.

NOTE The **alias** command allows you to create a custom shortcut to an IOS command so that the EXEC user does not have to type the complete IOS command. In addition to these custom commands that you might define, there are some predefined shortcut commands already. For example, **show ip route** is already defined in IOS with the shortcut **sh ip ro**. You can define your own alias with the following global IOS command:

```
alias EXEC alias-name IOS-command
```

View the predefined aliases with the following command:

```
Router#show aliases
EXEC mode aliases:
  h                    help
  lo                   logout
  p                    ping
  r                    resume
  s                    show
  u                    undebug
  w                    where
```

For example, you could make the command **ospf** display only OSPF routes by issuing the following command:

```
alias EXEC ospf show ip route ospf
```

Debugging Cisco Routers

The **debug** command is one of the best sets of tools you will encounter on Cisco routers. The **debug** command is available only from PRIV EXEC mode.

Cisco IOS routers' debugging includes hardware and software to aid in troubleshooting internal problems and problems with other hosts on the network. The **debug** privileged EXEC mode commands start the console display of several classes of network events.

For debug output to display on a console port, you must ensure that debugging to the console has not been disabled or sent to the logging buffer with the **logging console debug** command**.** The logging messages from the IOS image can be sent to the buffer (use **show logging** to view) and the console**.**

If you enable any **debug** commands through a console and no debug output is displayed, logging may have been disabled. Check the running configuration for the line **no logging debugging console** and, if present, remove it (by typing **logging debugging console**) to enable debug messages to be viewed by the console port. If the console setting is set to a level lower than debugging, the command **logging debugging console** will also override any current settings**.**

Remember to turn off console logging when you are done troubleshooting the problem. The router will continue to send to the console even if no one is there, tying up valuable CPU resources.

On virtual lines (vty lines), you must enable the **terminal monitor** command to view the debug output. You use vty lines when you telnet to a remote Cisco router.

NOTE Refer to the *Cisco IOS Debug Command Reference* at the following URL for the most recently updated **debug** command information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122sup/122debug/index.htm

When debugging data, you must also be aware of the switching method used by the router (for example, fast or process switches) because the CPU will use the same method when sending debug output to the console or vty line.

The **ip route-cache** IOS command with no additional keywords enables fast switching. When **debug ip packet** is enabled, make sure you disable fast switching (**no ip route-cache**) so that you can view packet-by-packet flow through the router. Search Cisco.com for the keywords "process" and "fast switching" for more details on switching methods. The following URL provides quality information on switching methods available on Cisco 7200 routers:

http://www.cisco.com/en/US/customer/products/sw/iosswrel/ps1831/products_configuration_guide_ chapter09186a00800ca6c7.html#xtocid6 . Please note you must have a valid CCO login for this link.

Also make sure you check out the Cisco Express Forwarding overview for a discussion on CEF at the same link.

Table 3-4 displays the **debug** commands and the system debug message feature.

Table 3-4 **debug** *Command Summary*

Cisco IOS Command	Purpose
show debugging	Displays the state of each debugging option
debug ?	Displays a list and brief description of all the **debug** command options
debug *command*	Begins message logging for the specified **debug** command
no debug *command* (or **undebug all**)	Turns message logging off for the specified **debug** command or turns off all debug messages with the **undebug all** command

Example 3-13 displays the list of **debug** command options covered in this section.

Example 3-13 **debug** *Command Options*

```
R1#debug ?
  all                      Enable all debugging
  ip                       IP information
  list                     Set interface or/and access list for the next debug
                           command
R1#debug ip ?
  audit                  IDS audit events
  auth-proxy             Authentication proxy debug
  bgp                    BGP information
  cache                  IP cache operations
  cef                    IP CEF operations
  cgmp                   CGMP protocol activity
  dhcp                   Dynamic Host Configuration Protocol
  drp                    Director response protocol
  dvmrp                  DVMRP protocol activity
  egp                    EGP information
  eigrp                  IP-EIGRP information
  error                  IP error debugging
  flow                   IP Flow switching operations
  ftp                    FTP dialogue
  html                   HTML connections
  http                   HTTP connections
  icmp                   ICMP transactions
  igmp                   IGMP protocol activity
  igrp                   IGRP information
  inspect                Stateful inspection events
  interface              IP interface configuration changes
  mbgp                   MBGP information
  mcache                 IP multicast cache operations
  mhbeat                 IP multicast heartbeat monitoring
  mobile                 IP Mobility
  mpacket                IP multicast packet debugging
  mrm                    IP Multicast Routing Monitor
  mrouting               IP multicast routing table activity
  msdp                   Multicast Source Discovery Protocol (MSDP)
  mtag                   IP multicast tagswitching activity
  nat                    NAT events
  nbar                   StILE - traffic classification Engine
  ospf                   OSPF information
  packet                 General IP debugging and IPSO security transactions
  peer                   IP peer address activity
  pim                    PIM protocol activity
  policy                 Policy routing
  postoffice             PostOffice audit events
  rgmp                   RGMP protocol activity
```

continues

Example 3-13 **debug** *Command Options (Continued)*

```
rip                        RIP protocol transactions
routing                    Routing table events
rsvp                       RSVP protocol activity
rtp                        RTP information
scp                        Secure Copy
sd                         Session Directory (SD)
security                   IP security options
socket                     Socket event
ssh                        Incoming ssh connections
tcp                        TCP information
tempacl                    IP temporary ACL
trigger-authentication     Trigger authentication
udp                        UDP based transactions
urd                        URL RenDezvous (URD)
wccp                       WCCP information
```

The rest of this section covers the **debug** commands shaded in Example 3-13.

CAUTION The CPU system on Cisco routers gives the highest priority to debugging output. For this reason, debugging commands should be turned on only for troubleshooting specific problems or during troubleshooting sessions with technical support personnel. Excessive debugging output can render the system inoperable.

Try to use the most specific **debug** command possible to reduce the load on the CPU. For example, the **debug all** command will surely disable a router. You should use the **debug all** command only in a lab environment.

Typically, the console port is used for debugging major faults because the CPU places debugging messages to the console port as the highest priority. Sometimes, debugging messages can overwhelm a network administrator's ability to monitor the router, and the IOS command **logging synchronous** can limit the messages to the console.

When synchronous logging of unsolicited messages and debug output is turned on (the line console is configured with the **logging synchronous** IOS command), unsolicited Cisco IOS software output is displayed on the console or printed after solicited Cisco IOS software output is displayed or printed. Unsolicited messages and debug output are displayed on the console after the prompt for user input is returned. This keeps unsolicited messages and debug output from being interspersed with solicited software output and prompts. After the unsolicited messages are displayed, the console displays the user prompt again. The IOS command's logging trap can be used to limit the logging of error messages sent to syslog servers to only those messages at the specified level (levels range from 0 to 7). The highest level is 7; level 7 encompasses all possible levels from 0 to 7. The lowest level is 0, or emergencies (system is unusable).

The **debug all** command turns on all possible debug options available to a Cisco router. This will crash any router in a busy IP network, so we strongly recommended that you never apply this command in a working network environment.

Example 3-14 displays the options when enabling IP debugging through a Cisco router.

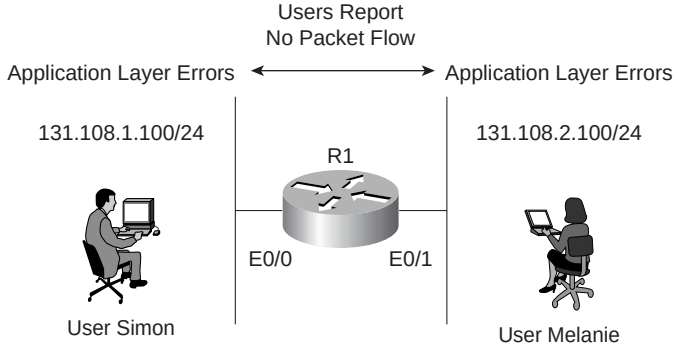
Example 3-14 **debug ip packet ?** *Command*

```
R1#debug ip packet ?
  <1-199>      Access list
  <1300-2699>  Access list (expanded range)
  detail       Print more debugging detail
  <cr>
```

You can define an access list so that only packets that satisfy the access list are sent through to the console or vty line.

Figure 3-3 displays a typical example in which a user (Simon) on one Ethernet (Ethernet 0/0) is advising you that packets from users on Ethernet 0/1 (Melanie's PC) are not reaching each other. To view the routing packet flow through Router R1, you can debug the IP packets and use a standard access list or an extended one (access lists are covered later in this chapter).

Figure 3-3 *IP Data Flow from One Segment to Another*



To view the IP packet flow and ensure that you view only packets from Melanie's PC to Simon's PC, you can define an extended access list matching the source address, 131.108.2.100 (Melanie's PC), to the destination address, 131.108.1.100 (Simon's PC).

Example 3-15 displays the **debug** command configuration on Router R1.

Example 3-15 *Enabling* **debug ip packet** *with Access List 100*

```
R1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 100 permit ip host 131.108.2.100 host 131.108.1.100
R1#debug ip packet ?
  <1-199>      Access list
  <1300-2699>  Access list (expanded range)
  detail       Print more debugging detail
  <cr>
R1#debug ip packet 100 ?
  detail  Print more debugging detail
  <cr>
R1#debug ip packet 100 detail
IP packet debugging is on (detailed) for access list 100
```

Applying the exact **debug** command for only traffic generated from one device to another ensures that the router is not using too many CPU cycles to generate the debug output to the console. When a ping request is sent from Melanie's PC to Simon's PC, debug output displays a successful ping request.

Example 3-16 displays the sample output matching access list 100 when five ping packets are sent.

Example 3-16 *Ping Request*

```
R1#ping 131.108.1.100
2d22h: IP: s=131.108.2.100 (local), d=131.108.1.100 (Ethernet0/0), len 100,
    sending
2d22h:     ICMP type=8, code=0
2d22h: IP: s=131.108.2.100 (Ethernet0/0), d=131.108.1.100 (Ethernet0/0),
    len 100, rcvd 3
2d22h:     ICMP type=8, code=0
2d22h: IP: s=131.108.2.100 (local), d=131.108.1.100 (Ethernet0/0), len 100,
    sending
2d22h:     ICMP type=8, code=0
2d22h: IP: s=131.108.2.100 (Ethernet0/0), d=131.108.1.100 (Ethernet0/0),
    len 100, rcvd 3
2d22h:     ICMP type=8, code=0
2d22h: IP: s=131.108.2.100 (local), d=131.108.1.100 (Ethernet0/0), len 100,
    sending
2d22h:     ICMP type=8, code=0
2d22h: IP: s=131.108.2.100 (Ethernet0/0), d=131.108.1.100 (Ethernet0/0),
    len 100, rcvd 3
2d22h:     ICMP type=8, code=0
2d22h: IP: s=131.108.2.100 (local), d=131.108.1.100 (Ethernet0/0), len 100,
    sending
```

Example 3-16 *Ping Request (Continued)*

```
2d22h:     ICMP type=8, code=0
2d22h: IP: s=131.108.2.100 (Ethernet0/0), d=131.108.1.100 (Ethernet0/0),
    len 100, rcvd 3
2d22h:     ICMP type=8, code=0
2d22h: IP: s=131.108.2.100 (local), d=131.108.1.1 (Ethernet0/0), len 100,
    sending
2d22h:     ICMP type=8, code=0
2d22h: IP: s=131.108.2.100 (Ethernet0/0), d=131.108.1.100 (Ethernet0/0),
    len 100, rcvd 3
2d22h:     ICMP type=8, code=0
```

When debugging with a specific IP access list, be sure to stop all debugging options with the **undebug all** IOS command before removing IP access lists; Cisco IOS routers are prone to failure if the access list is removed before the debugging options are disabled. For example, no debug output will be captured and sent to the console if no access list is defined, but one is referenced by a **debug** command (for example, **debug ip packet 100**, when access list 100 is not defined). Also, remember that the default behavior for Cisco IOS access lists is to deny traffic that is not specifically permitted. Make sure you permit only traffic for which you are interested in viewing debug messages like the example shown in Figure 3-3.

The debug output demonstrates that five packets were successfully routed from Ethernet 0/1 to Ethernet 0/0. (Note there are 10 entries in Example 3-16—the ICMP echo and ICMP reply packets.) Therefore, the network fault reported by the users points to an application error rather than a network error.

Table 3-5 displays the meaning of the codes in Example 3-16.

Table 3-5 **ping 131.108.1.100** *Explanation*

Field	Meaning
IP:	Indicates an IP packet
s=131.108.2.100 (Melanie's PC)	Indicates the packet's source address
d=131.108.1.100 (Simon's PC)	Indicates the packet's destination address
ICMP type 8 code 0	Ping request
Len 100	The length of the IP packet (100 bytes)

NOTE The **detail** option allows for further detail in the debug output.

Using the route cache is often called *fast switching*. The route cache allows outgoing packets to be load-balanced on a *per-destination* basis rather than on a per-packet basis.

NOTE The output modifier | (pipe) is a great time saver. For example, the command **show running-config | begin router ospf 100** shows only the running configuration starting from the **router ospf 100** part instead of showing the entire output.

Password Recovery

Sometimes, the Cisco enable or secret password is unknown and thus you must use password recovery to attain or change the enable or secret password.

Password recovery allows the network administrator to recover a lost or unknown password on a Cisco router. For password recovery, an administrator must have physical access to the router through the console or auxiliary port. When an EXEC user enters an incorrect enable password, the user receives an error message similar to the message shown in Example 3-17; the password entered is Cisco, which is displayed as *****.

Example 3-17 *Incorrect-Password Error Message*

```
R1>enable
Password: ******
Password: *****
Password: *****
% Bad passwords
R1>
```

When a user receives a % Bad passwords message, they can neither access the advanced command set (in this case, enabled mode) nor make any configuration changes. Fortunately, Cisco provides the following method to recover a lost password without losing configuration files:

Step 1 Power cycle the router.

Step 2 Press the **Break** key (for Windows 2000, press **Control-Break**) to enter into boot ROM mode. The Control-Break key sequence must be entered within 60 seconds of the router restarting after a power cycle. Other terminal applications will have their own sequence, so make sure that you consult the help files.

Step 3 After you are in ROM mode, change the configuration register value to ignore the startup configuration file that is stored in NVRAM. Use the **o/r 0x2142** command (2500 series routers). For Cisco IOS 12.2T (2600 models and higher) or later the command is **confreg 0x2142**.

Step 4 Allow the router to reboot by entering the **i** command.

Step 5 After the router has finished booting up (you will be prompted to enter the setup dialog—answer **no** or press **Control-c** to abort the setup dialog) without its startup configuration, look at the **show startup-config** command output. If the password is encrypted, move to Step 6, which requires you to enter enabled mode (type **enable** and you will not be required to enter any password) and copy the startup configuration to the running configuration with the **copy startup-config running-config** command. Then, change the password. If the password is not encrypted and the **enable secret** command is not used, simply document the plain-text password and go to Step 8.

Step 6 Because the router currently has no configuration in RAM, you can enter enabled mode by simply typing **enable** (no password is required). Copy the startup configuration to RAM with the IOS command **copy startup-config running-config.**

Step 7 Enable all active interfaces.

Step 8 Change the configuration register to 0x2102 (default) with the global IOS command **config-register 0x2102**. Note that this IOS command is automatically saved and there is no need to write changes to NVRAM when modifying the configuration register even though the IOS image will prompt you to save when you do perform a reload.

Step 9 After saving the configuration, you can optionally reload the router.

Step 10 Check the new password if it is not encrypted. If the password is encrypted, simply enter enabled mode and verify your password.

These are the generic steps for password recovery on a Cisco router. Some commands and steps might be slightly different depending on the hardware platform. Refer to the "Password Recovery Procedures" index (http://www.cisco.com/warp/public/474/) for more information on each platform.

To review, look at an example. Assume that you are directly connected to Router R1 and you do not know the enable password. You power cycle the router and press the Control-Break key combination (the Esc key) to enter boot mode.

Example 3-18 shows the dialog displayed by the router after a break is issued.

Example 3-18 *Password Recovery Dialog on a Cisco Router*

```
System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE
Copyright  1986-1995 by cisco Systems

Abort at 0x10EA882 (PC)
!control break issued followed by ? to view help options
>>?
------------>control break issued followed by ? to view help options
$            Toggle cache state
```

continues

Example 3-18 *Password Recovery Dialog on a Cisco Router (Continued)*

```
B [filename] [TFTP Server IP address | TFTP Server Name]
             Load and EXECute system image from ROM
             or from TFTP server
C [address]  Continue EXECution [optional address]
D /S M L V   Deposit value V of size S into location L with
             modifier M
E /S M L     Examine location L with size S with modifier M
G [address]  Begin EXECution
H            Help for commands
I            Initialize
K            Stack trace
L [filename] [TFTP Server IP address | TFTP Server Name]
             Load system image from ROM or from TFTP server,
             but do not begin EXECution
O            Show configuration register option settings
P            Set the break point
S            Single step next instruction
T function   Test device (? for help)
```

As you can see in Example 3-18, the **?** symbol can display all the available options. To view the current configuration register, issue the **e/s 2000002** command, which displays the value of the configuration register. Example 3-19 displays the current configuration register.

Example 3-19 **e/s 2000002** *Command in Boot ROM Mode*

```
>e/s 2000002
! This command will display the current configuration register
2000002: 2102
! Type q to quit
>
```

The default value for the configuration register on Cisco IOS routers is 2102. For illustrative purposes, change the register to **0x2142**, which tells the IOS image to ignore the configuration in NVRAM.

The command to change the configuration register in Boot ROM mode is **o/r 0x2142** followed by the **initialize** (**i**) command, which reloads the router. Example 3-20 displays the configuration change and the initialization of the router from boot ROM mode. New ROMMON versions require a different command to set the confirmation register, namely **confreg 0x2142** (or follow the menu system by typing **confreg**).

Example 3-20 *Changing the Configuration Register to 0x2142*

```
>o/r 0x2142
>i
```

The **i** command reboots the router and ignores your startup configuration because the configuration register has been set to 0x2142. The aim here is to change the password without losing your original configuration. Example 3-21 shows a truncated display by the Cisco IOS image after the router is reloaded.

Example 3-21 *Dialog After Reload*

```
System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE
Copyright  1986-1995 by Cisco Systems
2500 processor with 6144 Kbytes of main memory
F3: 9407656+151288+514640 at 0x3000060

              Restricted Rights Legend
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-AJS40-L), Version 11.2(17)
Copyright  1986-1999 by cisco Systems, Inc.
Compiled Tue 05-Jan-99 13:27 by ashah
Image text-base: 0x030481E0, data-base: 0x00001000
Basic Rate ISDN software, Version 1.0.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
2 Low-speed serial(sync/async) network interface(s)
1 ISDN Basic Rate interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read ONLY)
         --- System Configuration Dialog ---
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Would you like to enter the initial configuration dialog? [yes]:No
Press RETURN to get started!
......
Router>ena  !(no password required or entered)
Router#
```

Notice that the router reverts to the default configuration. Enter the **enable** command to enter PRIV EXEC mode. In this example, you are not prompted for the enable password because there is not one; by default, no enable password is configured when a Cisco IOS router boots from the default configuration (no passwords are configured in this default state).

You can view the startup configuration by using the **show startup-config** command (or **show config** in Cisco IOS versions predating version 10.3), as shown in Example 3-22.

Example 3-22 **show startup-config** *Command*

```
Router#show startup-config
Using 1968 out of 32762 bytes
! Last configuration change at 16:35:50 UTC Tue May 18 2002
! NVRAM config last updated at 16:35:51 UTC Tue May 18 2002
version 2.2
service password-encryption
hostname R1
! Note there is no secret password either
enable password 7 05080F1C2243
...
```

As you can see in Example 3-22, the enable password is encrypted. In instances where the password is not encrypted, you could view the password by using the **show startup-config** command. When a password is encrypted, you must copy the startup configuration to the running configuration and change the password manually by using the following IOS command:

```
copy startup-config running-config
```

Follow this by changing the enable or secret password, as follows:

```
enable pass new-password
enable secret new password
```

At this point, you are still in privileged mode, so you can now enter global configuration mode to change the password back to its original setting (cisco, in this instance).

Example 3-23 displays the password change in global configuration mode set to the new password of cisco.

Example 3-23 *Changing a Password and Setting the Configuration Registry Commands*

```
hostname#copy startup-config running-config
Destination filename [running-config]?
2818 bytes copied in 1.475 secs (2818 bytes/sec)
R1#config terminal
R1(config)#enable password cisco
R1(config)#config-register 0x2102
R1(config)#exit
R1#reload
```

You complete password recovery by changing the configuration register back to the default value (0x2102). The **configuration register** command is the only IOS command that you can type without the need to save the configuration, because IOS image automatically changes the setting regardless.

NOTE If a secret password is also configured, you must use the **enable secret** *password* IOS command because the secret password overrides the enable password. Example 3-23 includes no secret password, so you can use the **enable password** command.

When the Cisco IOS router reloads, it loads the new configuration file with the password set to cisco. To ensure that you can view the new password when the router reloads, optionally turn off encryption with the command **no service password-recovery.** When the router reloads and is running, you must administratively activate all interfaces because by default the interface is shut down.

Basic Security on Cisco Routers

You can access a Cisco router in a number of ways. You can physically access a router through the console port, or you can access a router remotely through a modem via the auxiliary port. You can also access a router through a network or virtual terminal ports (vty lines), which allow remote Telnet access.

If you do not have physical access to a router—either through a console port or through an auxiliary port via dialup—you can access a router through the software interface, called the virtual terminal (also referred to as a vty port). When you telnet to a router, you might be required to enter the vty password set by the network administrator. For example, on Router R1, the administrator types R2's remote address and tries to telnet to one of the vty lines.

Example 3-24 provides the session dialog when a user telnets to the router with the IP address 131.108.1.2.

Example 3-24 *Using a Vty Port to Establish a Telnet Connection*

```
R1#Telnet 131.108.1.2
Trying 131.108.1.2 ... Open
User Access Verification
Password: xxxxx
R2>
```

Cisco routers can have passwords set on all operation modes, including the console port, privilege mode, and virtual terminal access. To set a console password to prevent unauthorized console access to the router, issue the commands shown in Example 3-25.

NOTE All passwords are case sensitive.

Example 3-25 *Setting a Console Password*

```
R1(config)#line con 0
R1(config-line)#password cisco
!You can also set a password on the auxiliary port
R1(config)#line aux 0
R1(config-line)#password cisco
```

To set the privilege mode password, you have two options: the enable password and the secret password. To set these passwords, use the respective commands listed in Example 3-26.

Example 3-26 *Setting the Enable Password and Secret Password*

```
R1(config)#enable password cisco
R1(config)#enable secret ccie
```

The command to set an enable password is **enable password** *password*. You can also set a more secure password, called a secret password, which is encrypted when viewing the configuration with the **enable secret** *password* command.

The **enable secret** *password* IOS command overrides the **enable password** *password* command. Cisco IOS does permit you to configure the same password if you apply both commands but warns you that you should apply different passwords. It is a good security practice to use only the secret password.

In Example 3-26, the secret password will always be used. Now, issue the **show running-config** command to display the configuration after entering the enable and secret passwords in Example 3-26.

Example 3-27 displays the output from the **show running-config** IOS command after entering enable and secret passwords.

Example 3-27 **show running-config** *Command on R1*

```
R1#show running-config
Building configuration
Current configuration:
!
version 12.2
!
hostname R1
!
enable secret 5 $1$Aiy2$GGSCYdG57PdRiNg/.D.XI.
enable password cisco
```

Example 3-27 shows that the secret password is encrypted (using a Cisco proprietary algorithm), while the enable password is readable. This setup enables you to hide secret passwords when the configuration is viewed.

If you want, you can also encrypt the enable password by issuing the **service password-encryption** command, as displayed in Example 3-28. Cisco uses the MD5 algorithm to hash the secret password. You can easily reverse-engineer the hashed password (for example, 1Aiy2$GGSCYd G57PdRiNg/.D.XI.) with a number of open-source tools that can brute-force or apply dictionary attacks to the secret hash and attain the password. For the simple user, though, MD5 might be just enough to stop an intruder from gaining access and going to the next router.

Example 3-28 **service password-encryption** *Command*

```
R1(config)#service password-encryption
```

The **service password-encryption** command encrypts all passwords issued to the router by using a simple Vigenere cipher, which can be easily reversed. Example 3-29 shows an example of how these passwords appear when the configuration is viewed after all passwords have been encrypted.

Example 3-29 **show running-config** *Command on R1 After Encrypting All Passwords*

```
R1#show running-config
Building configuration...
Current configuration:
!
service password-encryption
version 12.2
hostname R1
!
enable secret 5 $1$Aiy2$GGSCYdG57PdRiNg/.D.XI.
enable password 7 0822455D0A16
```

NOTE Note the digits, 5 and 7, before the encrypted passwords. The number 5 signifies that the MD5 hash algorithm is used for encryption, whereas the number 7 signifies a weaker algorithm. You are not expected to know this for the written exam, but it is valuable knowledge for troubleshooting complex networks. In fact, a great network engineer is measured by his well-defined troubleshooting techniques, and not by how many CCIE lab exams he has passed.

Notice in Example 3-29 that both the secret and enable passwords are encrypted. If you enable the **service password-encryption** command in global configuration mode, all passwords will be encrypted and will not be viewable when displaying the configuration on the Cisco router.

The final Cisco password you can set is the virtual terminal password. This password verifies remote Telnet sessions to a router. Example 3-30 displays the commands necessary to set the virtual terminal password on a Cisco router.

Example 3-30 **password** *Command to Set a Virtual Terminal Password to ccie*

```
R4(config)#line vty 0 4
R4(config-line)#password ccie
```

If you issue the **no login** command below the virtual terminal command (**line vty 0 4**), remote Telnet users are not asked to supply a password and automatically enter EXEC mode. Example 3-31 displays the Telnet session dialog when the **no login** command is entered.

Example 3-31 *Dialog Display When* ***no Login*** *Is Enabled*

```
R1#telnet 1.1.1.1
Trying 1.1.1.1 ... Open
R2>
```

Keep in mind that the preceding setup is not a secure access method for a router network.

IP Access Lists

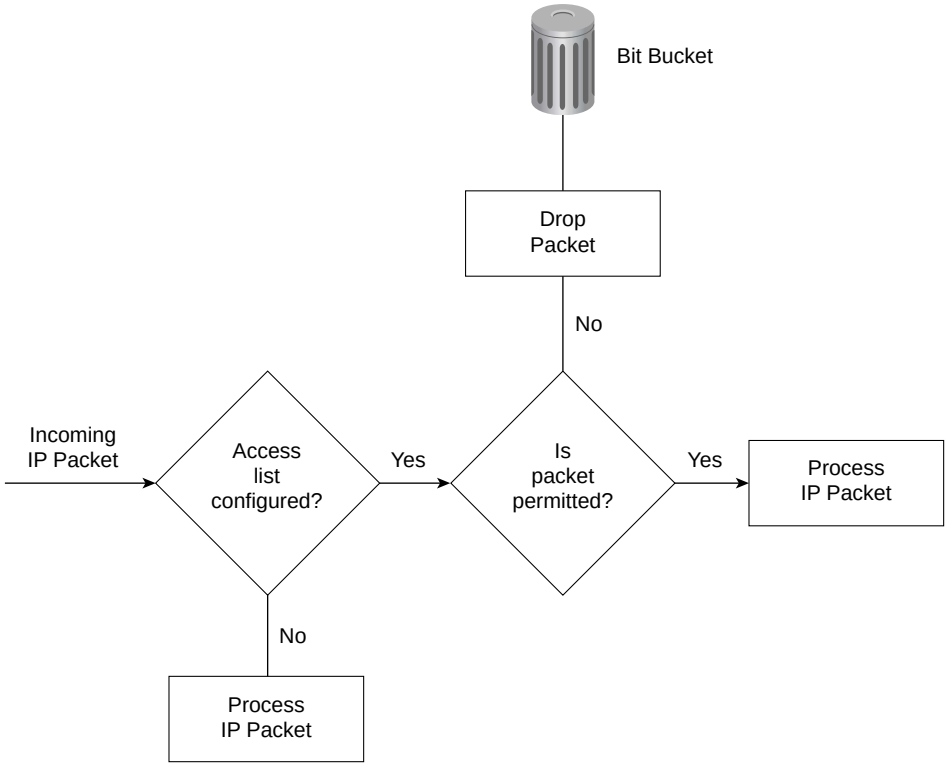
Standard and extended access lists filter IP traffic. An access list is basically a set of **permit** or **deny** statements. *Standard access lists* control IP traffic based on the source address only. *Extended access lists* can filter on source and destination addresses. Extended access lists can also filter on specific protocols and port numbers. This section covers how a Cisco router handles access lists.

Access Lists on Cisco Routers

By default, a Cisco router permits all IP and TCP traffic unless an access list is defined and applied to the appropriate interface. Figure 3-4 illustrates the steps taken if an access list is configured on a Cisco router.

If an incoming IP packet is received on a router and no access list is defined, the packet is forwarded to the IP routing software. If an access list is defined and applied, the packet is checked against the access list, and the appropriate permit or deny action is taken. The default action taken by any access list is to permit any explicitly defined statements and explicitly deny everything else. You will not see the explicit deny statement when you issue the **show ip access-lists** command because that is the default behavior.

Figure 3-4 *Access List Decision Taken by a Cisco Router*



NOTE If you do not apply the keyword **out** or **in** when defining an IP filter on an interface, the default action is to apply the filter on the outbound traffic. When applying an access list to an interface on a router running Cisco IOS 12.2T, you must define whether it is applied to outbound or inbound to the interface.

Standard IP access lists range from 1 through 99 and 1300 through 1999.

Extended IP access lists range from 100 through 199 and 2000 through 2699. When configuring access lists on a router, you must identify each access list uniquely within a protocol by assigning either a name or a number to the protocol's access list.

Standard IP access lists filter on the source address only.

Cisco IOS software also permits remarks so that administrators can easily manage large code blocks of access list lines. The following IOS output displays the available options:

```
R3-1720a(config)#access-list 8 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
  remark  Access list entry comment
```

The Cisco IOS syntax is as follows:

```
access-list access-list-number {deny | permit} [source-address]
    [source-wildcard]
```

Table 3-6 describes the purpose of each field.

Table 3-6 *Standard IP* **access-list** *Command Syntax Description*

Command Field	Description
access-list-number	A number from 1 through 99 that defines a standard access list number. Versions of Cisco IOS 12.0 or later also have standard access lists ranging from 1300 through 1999.
deny	IP packet is denied if a match is found.
permit	IP packet is permitted if it matches the criteria, as defined by the administrator.
source-address	Source IP address or network. Any source address can be applied by using the keyword **any**.
source-wildcard (optional)	Wildcard mask that is to be applied to the source address. This is an inverse mask, which is further explained with a few examples later in this section. The default is 0.0.0.0, which specifies an exact match.

After creating the access list as described in Table 3-6, you must apply the access list to the required interface by using the following command:

```
ip access-group {access-list-number | name} {in | out}
```

Table 3-7 describes the purpose of each field.

Table 3-7 **ip access-group** *Command Syntax Description*

Command Field	Description
access-list-number	A number in the range from 1 through 99 and 1300 through 1999 that defines a standard access list number.
name	If you are using named access lists, that name will be referenced here.
in	Keyword that designates the access list as an inbound packet filter.
out	Keyword that designates the access list as an outbound packet filter. This is the default action. For IOS images versions below 12.2T, the **in** or **out** keyword must be defined, there is no longer a default option.

The wildcard mask previously mentioned in the **access-list** command matches the source address. When the wildcard mask is set to binary 0, the corresponding bit field must match; if it is set to binary 1, the router does not care to match any bit or it is an insignificant bit. For example, the mask 0.0.255.255 means that the first two octets must match, but the last two octets do not need to match—hence, the commonly used phrases *care bits* (0s) and *don't care bits* (1s).

For further clarification, look at some examples of using access lists.

Suppose you have found a faulty NIC with the address 141.108.1.99/24. You have been asked to stop packets from being sent out Serial 0 on your router but to permit everyone else (**access-list 1 permit any**). In this situation, you need to deny the host address 141.108.1.99 and permit all other host devices. Example 3-32 displays the access list that fulfills this requirement.

Example 3-32 *Access List Configuration*

```
access-list 1 deny 141.108.1.99 0.0.0.0
access-list 1 permit 141.108.1.0 0.0.0.255
access-list 1 permit any
```

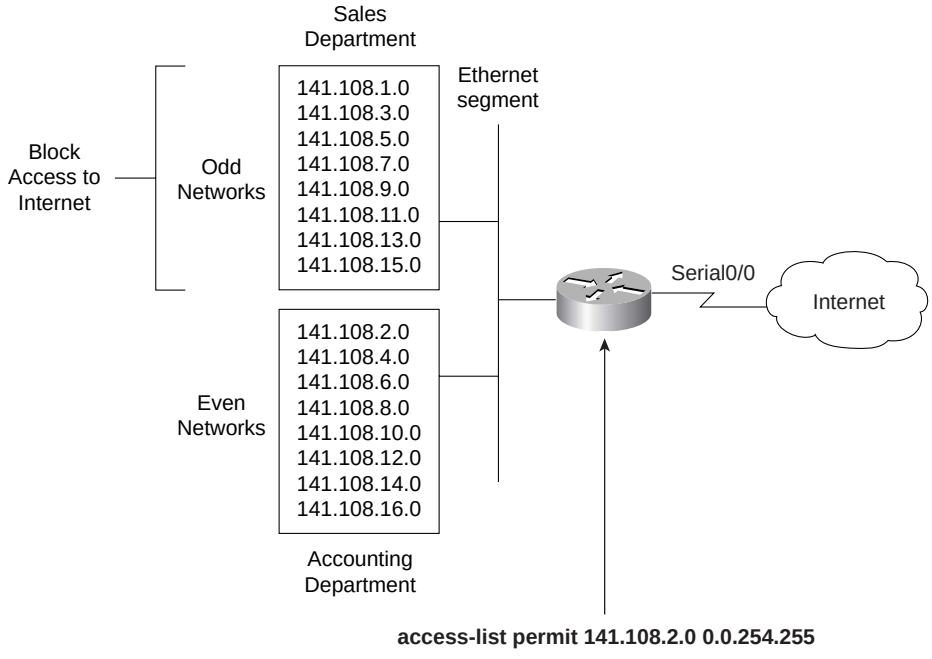
Next, you would apply the access list to filter outbound (the keyword **out** is supplied) IP packets on the Serial 0 interface. Example 3-33 applies the access list number 1 to the serial interface (outbound packets). You can be a little wiser and filter the incoming packets on the Ethernet interface. This ensures that the packet is immediately dropped before it is processed by the CPU for delivery over the serial interface. Both examples are displayed in Example 3-33.

Example 3-33 *Applying the Access List*

```
Interface Ethernet0
ip access-group 1 in
interface Serial 0
ip access-group 1 out
```

Now look at a more complex example of using a standard access list. Suppose you have 16 networks ranging from 141.108.1.0 to 141.108.16.0, as shown in Figure 3-5.

Figure 3-5 *Standard Access List Example*



You have assigned even subnets (2, 4, 6, 8, 10, 12, 14, and 16) to the Accounting department and odd subnets (1, 3, 5, 7, 9, 11, 13, and 15) to the Sales department. You do not want the Sales department to access the Internet, as shown in Figure 3-5. To solve this issue, you configure a standard access list. Figure 3-5 displays a simple requirement to block all odd networks from accessing the Internet.

You could configure the router to deny all the odd networks, but that would require many configuration lines.

NOTE Access lists are CPU-process-intensive because the router has to go through every entry in the access list for each packet until a match is made. If you want to determine the actual effect an access list has on your router, compare the CPU processes before and after activating an access list. Remember to check on a regular basis to see the big picture.

Instead, permit only even networks (2, 4, 6, and so forth) with one IOS configuration line. To accomplish this, convert all networks to binary to see if there is any pattern that you can use in the wildcard mask.

Table 3-8 displays numbers 1 through 16 in both decimal and binary format.

Table 3-8 *Example Calculation of Numbers in Binary*

Decimal	Binary
1	00000001
2	00000010
3	00000011
4	00000100
5	00000101
6	00000110
7	00000111
8	00001000
9	00001001
10	00001010
11	00001011
12	00001100
13	00001101
14	00001110
15	00001111
16	00010000

Notice that odd networks always end in the binary value of 1, and even networks end with 0. Therefore, you can apply your access lists to match on the even network and implicitly deny everything else. Even numbers will always end in binary 0. You do not care about the first 7 bits, but you must have the last bit set to 0. The wildcard mask that applies this condition is 111111110 (1 is don't care and 0 is must match; the first 7 bits are set to 1, and the last bit is set to 0).

This converts to a decimal value of 254. The following access list will permit only even networks (from 2, 4, 6,..to 254):

```
access-list 1 permit 141.108.2.0 0.0.254.255
```

The preceding access list will match networks 2, 4, 6, 8, 10, 12, 14, and 16 in the third octet. The default action is to deny everything else, so only even networks will be allowed, and odd networks are blocked by default. Next, you would apply the access list to the inbound interface. Example 3-34 describes the full configuration.

Example 3-34 *Applying the Access List*

```
Hostname R1
interface Serial0/0
ip access-group 1 in
access-list 1 permit 141.108.2.0 0.0.254.255
```

You can be a little wiser and filter the incoming packets on the Ethernet interface. This ensures that the packet is immediately dropped before it is processed by the CPU for delivery over the serial interface. This conserves critical CPU cycles.

Extended Access Lists

Extended access lists range from 100 through 199 and 2000 through 2699. Alternatively, you can use a named access list with Cisco IOS release 12.0 or later. As mentioned earlier in this chapter, extended access lists can be applied to both source and destination addresses, as well as to filter protocol types and port numbers. Following are some examples of extended access lists that allow you to filter several different types of traffic.

For Internet Control Message Protocol (ICMP) traffic, use the syntax shown in Example 3-35.

Example 3-35 *Access List Syntax for ICMP Traffic*

```
access-list access-list-number [dynamic dynamic-name
[timeout minutes]] {deny | permit} icmp source source-wildcard
destination destination-wildcard [icmp-type [icmp-code]
[icmp-message] [precedence precedence] [tos tos] [log]
```

For Internet Group Management Protocol (IGMP) traffic, use the syntax shown in Example 3-36.

Example 3-36 *Access List Syntax for IGMP Traffic*

```
access-list access-list-number [dynamic dynamic-name
[timeout minutes]] {deny | permit} igmp source source-wildcard
destination destination-wildcard [igmp-type]
[precedence precedence] [tos tos] [log]
```

For TCP traffic, use the syntax shown in Example 3-37.

Example 3-37 *Access List Syntax for TCP Traffic*

```
access-list access-list-number [dynamic dynamic-name
[timeout minutes]] {deny | permit} tcp source source-wildcard
[operator port [port]] destination destination-wildcard
[operator port [port]] [established] [precedence precedence]
[tos tos] [log]
```

For User Datagram Protocol (UDP) traffic, use the syntax shown in Example 3-38.

Example 3-38 *Access List Syntax for UDP Traffic*

```
access-list access-list-number [dynamic dynamic-name
[timeout minutes]] {deny | permit} udp source source-wildcard
[operator port [port]] destination destination-wildcard
[operator port [port]] [precedence precedence] [tos tos] [log]
```

As you can see, extended access lists have a range of options to suit any requirement. The most often used extended access list options are as follows:

- *access-list-number*—Provides a number ranging from 100 through 199 that defines an extended access list. Extended Access Lists also range from 2000 through 2699.
- **deny**—Denies access if the conditions are matched.
- **permit**—Permits access if the conditions are matched.
- *protocol*—Specifies the protocol you are filtering. Some common options include **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ospf**, **tcp**, and **udp**. You can also define the protocol number with a valid protocol value.
- *source*—Specifies the source address.
- *source-wildcard*—Specifies the source wildcard mask.
- *destination*—Identifies the destination network.
- *destination-wildcard*—Identifies the destination wildcard mask.

You are expected to demonstrate your understanding of standard and extended access lists. You are not expected to memorize the available options in an extended access list. The options are provided in this chapter for your reference only. When constructing access lists, the built-in help feature (**?**) is extremely useful.

Here are a few more complex examples of access lists.

Example 3-39 *Extended Access List Example*

```
access-list 100 permit tcp any any  eq smtp
! Permits Simple Mail Transfer Protocols
access-list 100 permit udp any any eq domain
! Permits DNS queries
access-list 100 permit icmp any any echo
! Permits ICMP ping requests
access-list 100 permit icmp any any echo-reply
! Permits ICMP replies
```

continues

Example 3-39 *Extended Access List Example (Continued)*

```
access-list 100 permit ospf any any
! Permits OSPF packets
access-list 100 permit tcp any any eq bgp
! Permits BGP to any device
```

In Example 3-39, the access list numbered 100 is not concerned with specific host addresses or networks, but rather ranges of networks.

The **any** keyword is shorthand for 0.0.0.0 255.255.255.255, which means that the device's address is irrelevant. This address can be entered in shorthand as **any**. If any IP packet arrives to the router and does not match the specified criteria, the packet is dropped.

The Cisco CD-ROM documentation provides additional quality examples of access lists. You should take some time to study the Cisco examples available on the CD-ROM and at Cisco.com under the Technical Documentation quick link.

Access lists are difficult to manage because you cannot explicitly delete a specific line; you must first remove the entire access list and re-enter the new access list with the correct order for numbered access lists. For a large access list that might contain over 1000 lines of code, any variations are completed on a TFTP server and copied to the startup configuration. I have worked with some access lists that were 2500 lines in length and took over 5 minutes to load on Cisco routers. On the other hand, named access lists allow you to determine where in the access list the new line will be placed. In a named access list, you must first delete the lines up to where you want to add the new lines and then re-add the lines you deleted. Simply search for the keywords "IP named access lists" for more configuration details on named access lists at Cisco.com.

IP Named Access Lists might be a likely scenario for the CCIE security lab exam, so ensure that you are fully comfortable with named and numbered access lists for the laboratory exam.

Now that you are familiar with some of the best practices used in securing Cisco IOS routers, the next section presents the best practices used in Layer 2 switched networks, in particular Cisco Catalyst switches.

NOTE As you may have noticed, the CCIE Security blueprint at times is a little difficult to understand. Having taken the CCIE Security examination a number of times has made me aware of exactly how the blueprint topics actually match up to examination content. It is the aim of the next few sections to ensure that you have the information you need to answer possible questions about security on switches. Having covered routing security, it is imperative to concentrate on the new content, namely securing Layer 2 devices in a Cisco-powered network.

Layer 2 Switching Security

Switches operating at Layer 2 of the OSI model are designed to be able to control the flow of data between their ports or interfaces. They do this by creating almost instant networks that contain only the two end devices communicating with each other so that information flow is increased to the optimal level. Devices not involved in this two-way communication are not involved at that moment in time.

At the data link layer (Layer 2 of the OSI model), the only mechanism permitted to allow communication is via the Media Access Control (MAC) address—a 48-bit (HEX) bit address.

Cisco switches build Content-Addressable Memory (CAM) tables to store the MAC addresses available on physical ports, along with their associated VLAN parameters. They are the Layer 2 equivalent of routing tables. If a device sends a frame to an unknown MAC address, the switch first receives the frame and then floods it out all ports or interfaces except where the originating frame was sourced from. Switches thereby provide a switching path between end users' devices.

Then why is the CAM table widely regarded as the weakest link in Cisco security? The next few sections describe some of today's most widely used mechanisms used to exploit the CAM table on Cisco switches, along with some other common exploits.

Switches are subjected to the following common attacks:

- CAM table overflow
- VLAN hopping
- Spanning Tree Protocol manipulation
- MAC address spoofing
- DHCP starvation attacks

CAM Table Overflow

This section first reviews exactly how the CAM table operates, so that you appreciate how easily it can be comprised.

Figure 3-6 displays a typical Layer 2 switch network with one switch and three PCs labeled with MAC addresses A, B, and C to simplify the figure.

Figure 3-6 *CAM Table Operation*

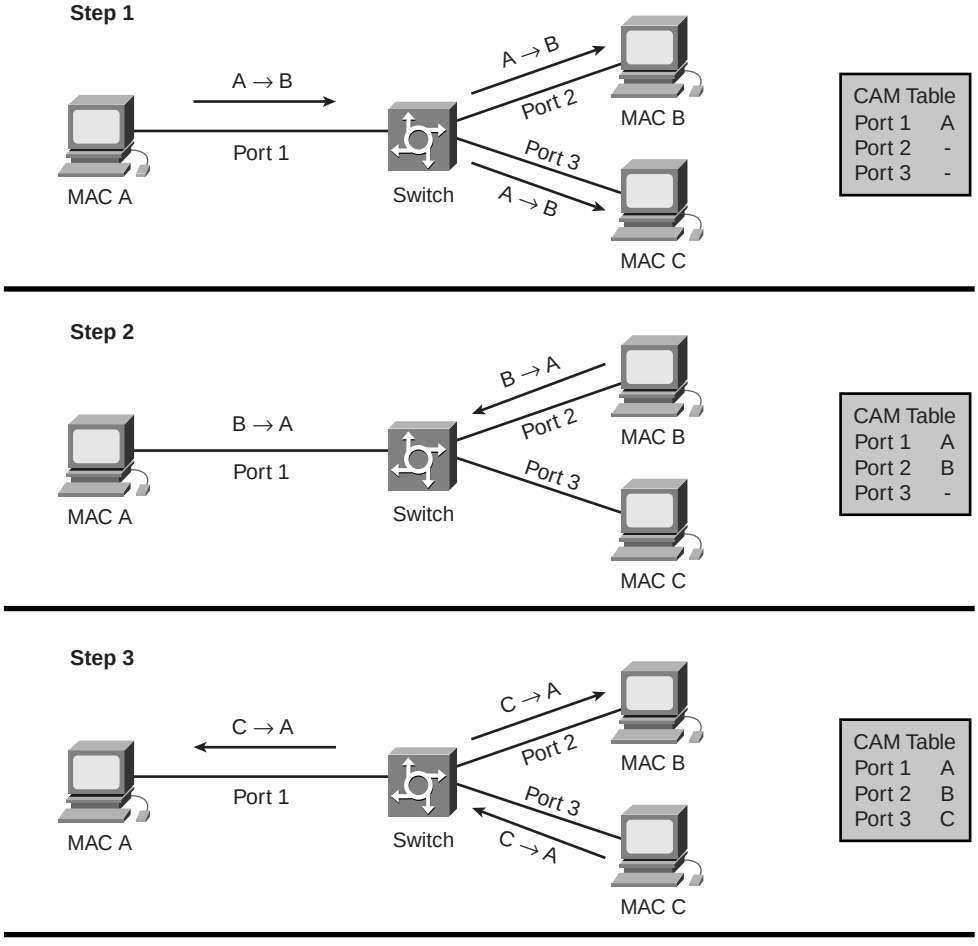


Figure 3-6 displays the typical CAM table population by a Cisco switch. When Device A, with MAC address A, sends a frame destined for Device B, with MAC address B, the switch looks at the source MAC address from Port 1 and installs MAC address A into the CAM table immediately. Because this is the first frame, the switch does not know where Device B is, so the frame is copied to all other ports (2 and 3 in Figure 3-6) and awaits a response.

Device B responds to the frame from Device A and the switch installs Device B's MAC address into the CAM table. Eventually, when Device C sends a frame, the CAM table will contain all three devices.

Most CAM tables are limited in size, depending on the switch hardware, based on memory available. It is not difficult to fill a CAM table on a Cisco switch. If enough entries are entered into

the CAM table before other entries are expired (based on an idle timer), the CAM table fills up to the point that no new entries can be accepted. This is how an intruder typically attacks a switch—by sending multiple frames with different source addresses attempting to overflow the CAM table so that authorized devices can no longer reside in the CAM table, which causes the switch to continuously send frames out all ports as the default until the CAM table discovers which devices reside on what interfaces.

Typically a network intruder will flood the switch with a large number of invalid-source MAC addresses until the CAM table fills up. This renders your powerful Layer 2 switch as a hub where all frames are repeated out all ports or interfaces.

Figure 3-7 displays the invalid-source MAC addresses populating the CAM table.

Figure 3-7 *CAM Overflow Attack*

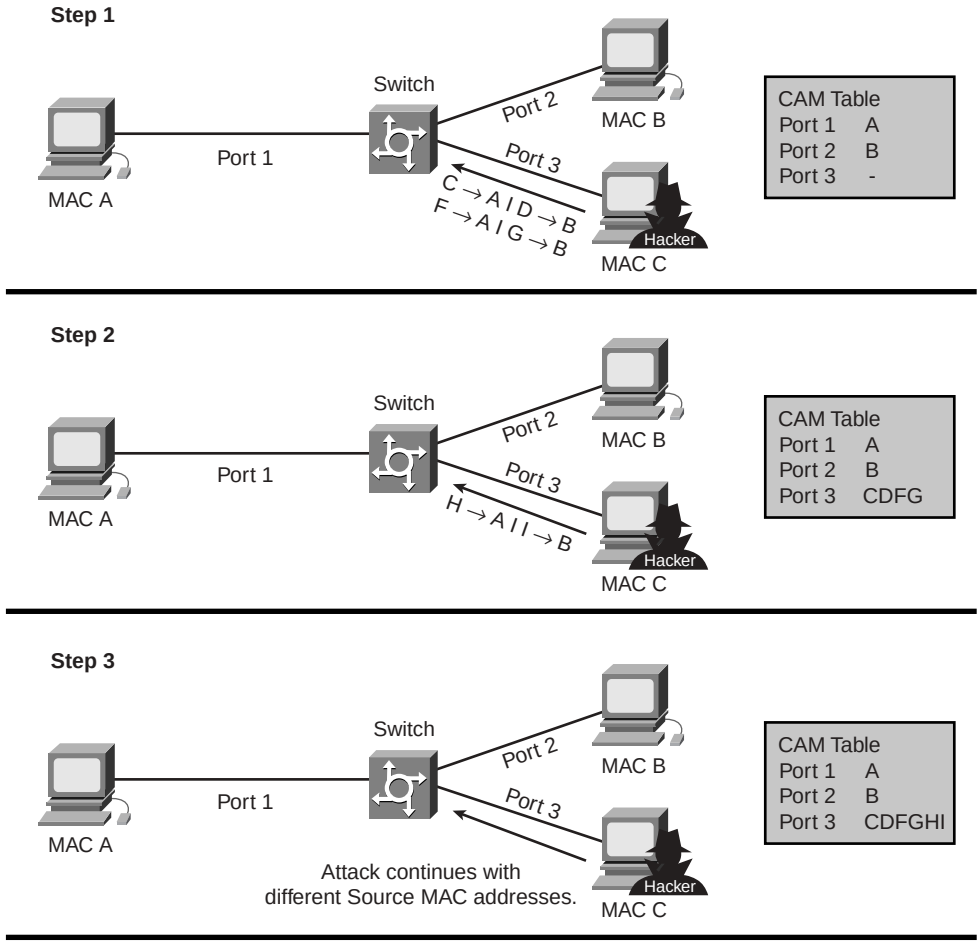


Figure 3-7 displays an intruder device labeled with the PC Device C, sending multiple packets with various source addresses labeled C, D, E, F, G, H, and I.

By continuously sending packets, the CAM table for Port 3 will continue to grow. A simple tool, freely available on the Internet, named Macof floods a switch with packets containing randomly generated source and destination MAC and IP addresses. The switch will keep building the CAM table until its memory runs out, rendering the switch to certain failure.

The only method to mitigate this style of attack is to enable MAC port security by configuring your switch ports with port security. For a large network, it is advisable to configure dynamic port security, whereby you allow dynamic security to take over any static-based configuration and allow only one MAC address to connect to the port. In an IP telephony environment (like Cisco AVVID), you would need to allow at least two MAC addresses per port, one for the IP phone and one for the PC attached to the phone.

Example 3-40 displays the command syntax to enable port security on a Catalyst-based operating system.

Example 3-40 **set port security** *Command on CatOS Systems*

```
set port security mod/port enable [MAC_addr]
set port security mod/port MAC_addr
set port security mod/port maximum num_of_MAC
set port security mod/port violation
set port security mod/port age
set port security mod/port shutdown shutdown-time
```

Example 3-41 displays the equivalent commands for Cisco IOS–based switches.

Example 3-41 *Cisco IOS Port Security Configuration Commands*

```
Router(config-if)# switchport port-security
Router(config-if)# switchport port-security maximum value
Router(config-if)# switchport port-security violation {protect ¦ restrict ¦ shutdown}
Router(config-if)# switchport port-security MAC-address MAC-address
Router(config-if)# switchport port-security aging
```

VLAN Hopping

VLAN hopping is a network attack whereby an end system sends out packets destined for a system on a different VLAN that cannot normally be reached by the end system. Typically, for a device to reach another device in a different VLAN, a Layer 3 device such as a router or Layer 3–aware switch is required. The attacker manipulates the frame and sends the traffic based on a different VLAN ID. The attacker may even attempt to be a trunk port and send 802.1q frames with data inside those frames.

Switch spoofing is a common technique whereby the attacker emulates a trunk port by using Inter-Switch Link (ISL) or 802.1q frames. By using this method, the attacker can become a member of any VLAN configured in the VLAN Trunking Protocol (VTP) domain.

To mitigate this form of attack, it is highly recommended to turn off trunking on all ports that will not be enabled for Cisco ISL or the IEEE 802.1q trunking methods.

Attackers may even use a double tagging mechanism whereby the initial frame is tagged with two 802.1q frames so that when the first switch removes the header, the end device is still presented with a frame with an 802.1q header, as Figure 3-8 demonstrates.

Figure 3-8 *Double Tagging 802.1q Method*

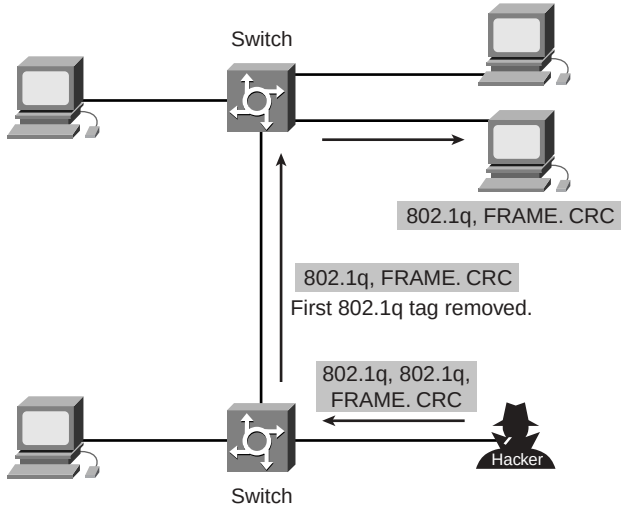


Figure 3-8 shows the method of double tagging whereby the transmitted frames have two 802.1q (or ISL) headers in order to forward the frames to the wrong VLAN. The first switch to encounter the double-tagged frame (1) strips the first tag off the frame and forwards the frame. The result is that the frame is forwarded with the inner 802.1q tag out all the switch ports (2) including trunk ports configured with the native VLAN of the network attacker. The second switch then forwards the packet to the destination based on the VLAN identifier in the second 802.1q header. This enables a device in one VLAN to communicate with a device in a separate VLAN. This is an extremely vulnerable situation for your network, because now your frames do not communicate to the legitimate Layer 3 device but rather to a rouge device where all sorts of sensitive data could be compromised.

To mitigate this potential issue, all non-trunking ports should be disabled (that is, trunking is disabled) and configured as access ports or interfaces that only permit devices such as PCs or Voice over IP (VoIP) phones.

Another common technique is to disable all ports not in use on the particular switch in question.

Example 3-42 displays the Catalyst OS and IOS configurations that disable trunking.

Example 3-42 *Disable Trunk Ports on Catalyst OS and IOS Switches*

```
! Catalyst OS
CatOS>(enable) set trunk mod_num/port_num off
! IOS Based switches
IOS#(config-if)switchport mode access
```

Spanning Tree Protocol Manipulation

Another common attack against switches is to manipulate the STP configuration by sending valid bridge protocol data units (BPDUs) and changing the topology of the network so as to create a spanning-tree loop.

A Layer 2 loop in any network will bring down the entire broadcast domain and render all services unusable. Sometimes, in fact, spanning-tree loops occur naturally, so do not always assume that a Layer 2 loop is the result of an attacker's involvement without first properly investigating.

By attacking STP, the network attacker hopes to spoof his or her system as the root bridge in the topology. To become the root bridge in a Layer 2 environment, all you need to accomplish is to send a valid BPDU frame telling all other devices that your root priority is the lowest in the network and should install it as the root bridge. By accomplishing a spanning-tree event (through the use of sending what appears to be a valid BPDU frame), the intruder's PC can accomplish a spanning-tree topology change that results in ports forwarding incorrectly and can result in a potential Layer 2 loop. Layer 2 loops in any switched network will bring the network to a standstill.

To mitigate this form of attack, you simply configure all switch ports not connected to other switches with BPDU guard. This feature allows the switches to immediately disable the port if a BPDU frame is received, thus rendering this attack immediately ineffectual and disabling the intruder.

Example 3-43 displays the Catalyst OS and IOS commands to enable BPDU guard.

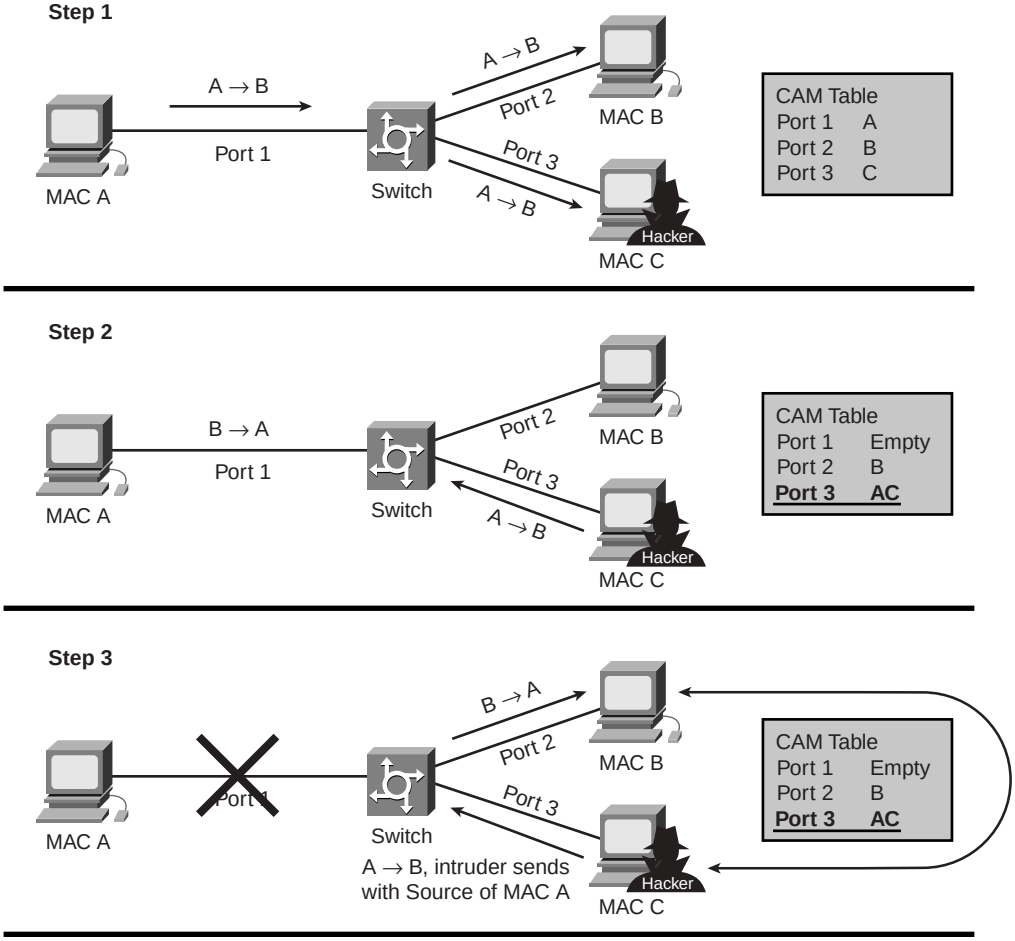
Example 3-43 *Enable BPDU Guard*

```
! Catalyst OS
CatOS> (enable)set spantree portfast mod/num bpdu-guard enable
! IOS enabled Switch
CatSwitch-IOS(config)#spanning-tree portfast bpduguard enable
```

MAC Spoofing Attack

A MAC spoofing attack is where the intruder sniffs the network for valid MAC addresses and attempts to act as one of the valid MAC addresses. The intruder then presents itself as the default gateway and copies all of the data forwarded to the default gateway without being detected. This provides the intruder valuable details about applications in use and destination host IP addresses. This enables the spoofed CAM entry on the switch to be overwritten as well. This is best illustrated in Figure 3-9.

Figure 3-9 *MAC Spoof Attack*



Step 1 in Figure 3-9 demonstrates the three discovered devices (Devices A, B, and C) in the CAM table. Device C is an intruder. After spoofing the MAC address of Device A (remember, the initial frame when a CAM table is empty is sent to all ports except the source port), Device C sends out a frame with the source address of MAC A, with a new spoofed IP address. The switch relearns the MAC address and changes the CAM table entries in Step 2 of the attack. Now when Device B wishes to communicate to the legitimate Device A, the switch sends the packet according to the CAM table, which is now Port 3 or the attacking PC. Until Device A resends packets, the data flow will remain and the attacker will receive and view active data. By ensuring that any ARP requests are replied to, the intruder can maintain the connection until manual intervention occurs from the network administrator.

Mitigating this form of attack takes a little more design because the attacker is far more intelligent. To start with, you must enable port security. Example 3-41, earlier in the chapter, displays how this can be achieved.

However, as with the CAM table overflow attack mitigation, specifying a MAC address on every port is an unmanageable solution. Another solution would be to use private VLANs to help mitigate these network attacks.

Using private VLANs is a common mechanism to restrict communications between systems on the same logical IP subnet. This is not a fool-proof mechanism. Private VLANs work by limiting the ports within a VLAN that can communicate with other ports in the same VLAN. To configure a private VLAN on switch-based Cisco IOS or Catalyst OS, follow these steps:

Step 1 Create the primary private VLAN.

```
Switch_CatOS> (enable) set vlan primary_vlan_id pvlan-type primary name
primary_vlan
Switch_IOS(config)#vlan primary_vlan_id
```

Step 2 Create the isolated VLAN(s).

```
Switch_CatOS> (enable) set vlan secondary_vlan_id pvlan-type
    isolated name isolated_pvlan
Switch_CatOS> (enable) set pvlan primary_vlan_id secondary_vlan_id
```

Step 3 Bind the isolated VLAN(s) to the primary VLAN.

```
Switch_CatOS> (enable) set pvlan primary_vlan_id secondary_vlan_id
Switch_IOS(config)#vlan primary_vlan_id
Switch_IOS(config-vlan)#private-vlan association secondary_vlan_id
Switch_IOS(config-vlan)#exit
```

The best method, in conjunction with port security, is to use DHCP snooping mechanisms to ensure that only valid DHCP servers are enabled across your network. One DHCP snooping mechanism is to permit only trusted DHCP messages to flow between client PC and authorized DHCP servers. The ideal solution to mitigate various ARP-based network exploits is the use of DHCP snooping along with Dynamic ARP Inspection (DAI).

When a client sends out a broadcast message for an IP address, the intruder's PC also sees the request, of course, because broadcasts are sent out to all interfaces or ports except the source port. So, in effect, the network must not allow DHCP offers, acknowledgements, or negative acknowledgements (DHCPOffer, DHCPAck, or DHCPNak) to be sent from untrusted sources.

Illegal DHCP messages are messages received from outside the network or firewall. The DHCP snooping binding table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information corresponding to the local untrusted interfaces of a switch; it does not, however, contain information regarding hosts interconnected with a trusted interface. By configuring trusted and untrusted DHCP sources, the switch can be configured to drop illegal frames immediately. DHCP snooping will still not stop an intruder sniffing for MAC addresses.

DAI determines the validity of an ARP packet based on the valid MAC address—to—IP address bindings stored in a DHCP snooping database. This means that only valid MAC addresses are permitted to reply to authorized devices on the network. Some really crafty attackers are out there waiting to pounce on networks, and for a majority of them these features are not enabled, so it is a gold mine in many parts of the world even in today's climate.

To enable DHCP snooping, the following commands are required. Example 3-44 enables DHCP snooping. Notice that the only supported platforms are switches with Cisco IOS–based software.

Example 3-44 *Enabling MAC Spoofing on Cisco IOS Switches*

```
!Catalyst IOS switches
CatIOS(config)# ip dhcp snooping
CatIOS (config)# ip dhcp snooping vlan number [number]
CatIOS (config)# ip dhcp snooping information option
! Enable trusted ports on the DHCP server interface
CatIOS (config-if)# ip dhcp snooping trust
```

DHCP Starvation Attacks

As the name implies, a DHCP starvation attack is where a DHCP server is sent so many DHCP requests that eventually there are no more IP addresses available to allocate to legitimate devices, hence rendering the network unusable.

A DHCP starvation attack works by broadcasting DHCP requests with spoofed MAC addresses. As you have seen, there are many tools available on the Internet to send out these sorts of frames. The end result may involve the attacker installing their own DHCP server and responding to a client request for an IP address, which will result in data being sent to the wrong destination, thus compromising company data. Because DHCP responses typically include default gateway and DNS server information, the network attacker can supply their own system as the default gateway and DNS server, resulting in a man-in-the-middle-style attack.

Additional features in Cisco IOS–enabled switches can mitigate this attack by enabling DHCP snooping. In additon to the defense shown in Example 3-44, IP source guard can provide additional defense against attacks such as DHCP starvation and IP spoofing. Like DHCP snooping, IP source guard is enabled on untrusted Layer 2 ports. All IP traffic is initially blocked *except* for DHCP packets captured by the DHCP snooping process. Once a client receives a valid IP address from the DHCP server, a per-port and VLAN access control list (PACL) is applied to the port. This restricts the client IP traffic to those source IP addresses configured in the binding. Any other IP traffic with a source address other than the addresses in the binding will be filtered and thrown away by the switch. Example 3-45 displays a sample configuration to help alleviate a DHCP starvation attack.

Example 3-45 *DHCP Starvation Attack Mitigation*

```
CatIOS(config)# ip dhcp snooping
CatIOS (config)# ip dhcp snooping vlan number [number]
CatIOS (config)# ip verify source vlan dhcp-snooping port-security
CatIOS (config)# switchport port-security limit rate invalid-source-MAC rate
CatIOS (config)# ip source binding ip-address MAC-address vlan vlan-id
    interface interface
!Finally trust the interfaces with the following command
CatIOS (config-if)# ip dhcp snooping trust
```

Example 3-45 enables DHCP snooping and ensures that any other IP traffic with a source address other than the addresses in the binding will be filtered and dropped immediately.

There are, of course, many other techniques used by attackers. Other examples include using Cisco Discovery Protocol (CDP), trying to manipulate VTP messages without password authentication, and searching for vulnerabilities over wireless and telephony-based networks, as already discussed in Chapter 1, "General Networking Topics." Once you pass the written examination, make sure you do not limit your knowledge to just those mechanisms presented here, because Cisco releases new features almost daily to overcome new and even smarter techniques used by attackers.

The next section briefly covers some of the overall security policy best practices that Cisco recommends be designed and implemented in networks.

Security Policy Best Practices—A Cisco View

Cisco released a number of excellent SAFE blueprints containing security design guideless. The material at http://www.cisco.com/safe is a must read for any IP engineer or designer.

Too many organizations have not followed the fundamental crucial step of developing a security policy upon which to base all security strategies. Any network without a security policy is liable to be compromised, because when an event does occur, there are no processes in place to mitigate the event efficiently and thoroughly. Hence, an important step for any organization serious about

network security is to perform a risk assessment of the current network and then build a security policy that considers that risk assessment. This risk assessment should be carried out on a regular basis and improved when new vulnerabilities are discovered.

NOTE This section presents some of the SAFE recommendations in brief. The examination is very light on this material.

Prior to implementing a security policy, you must do the following:

- **Create usage policy statements**—Involves outlining users' roles and functions within an organization. The main purpose of these statements is to ensure that the user communities understand the security policy. The next step is to define a usage policy for partners involved within an organization. Finally, the administrators within the organization must have defined procedures for user account management, policy enforcement, and a regular status review of privileged users.
- **Conduct a risk analysis**—Identifies the risks to your current network, resources, and data devices. This involves identifying resources within your network and assigning each critical device an appropriate level of security—low, medium, and high.
- **Establish a security team structure**—Involves assembling a cross-functional security team—typically a virtual team (a team of experts that communicates over the phone, Internet, and e-mail) for global companies such as Cisco—lead by a security manager. Each team member is responsible for the technical aspects of the security policy and must be fully aware of the current and future polices that are in place.

The security team in any organization has the fundamental responsibility of ensuring network integrity. In fact, in some parts of the world, the chief information officer can be jailed for not ensuring that the network is secure. The three primary areas of concern for security administrators are the following:

- Policy development
- Practice
- Response

In addition to the three key areas of policy development, ensure the security policy remains at the forefront to protect data integrity by ensuring there is adequate preparation, prevention, and response.

The following URL provides more details on a security team's core responsibilities and areas of focus (please note requires a CCO login):

http://www.cisco.com/en/US/partner/tech/tk869/tk769/technologies_white_paper09186a008014f945.shtml#t3

Foundation Summary

The "Foundation Summary" is a condensed collection of material for a convenient review of this chapter's key concepts. If you are already comfortable with the topics in this chapter and decided to skip most of the "Foundation Topics" material, the "Foundation Summary" will help you recall a few details. If you just read the "Foundation Topics" section, this review should help further solidify some key facts. If you are doing your final preparation before the exam, the "Foundation Summary" offers a convenient and quick final review.

Table 3-9 *Cisco Device Commands and Information*

Command/Subject	Description
show flash	Displays the content of the System Flash.
Standard IP access list range	1–99, 1300–1999.
Extended access list range	100–199, 2000–2699.
copy running-config startup-config	IOS command to save running configuration from RAM to NVRAM.
copy running-config startup-config	IOS command to save running configuration from NVRAM to RAM.
0x2102 IOS syntax: **config-register** *value*	0x2102 is the standard default configuration register, which is a 16-bit number defining how the router loads. To ignore the startup configuration, use 0x2142.
show version	Displays detailed information about Cisco IOS and hardware configuration on a Cisco router.

Table 3-10 *Advanced Cisco Device Operation*

Cisco IOS Command	Description
show debugging	Displays the current **debug** commands processed by the CPU
debug ?	Displays a list of available **debug** options
undebug all	Turns off all possible debugging commands
debug ip packet *access-list*	Allows debugging of specific network addresses without burdening the router with every IP packet processed by the CPU

Table 3-11 *Password Recovery Steps*

Step	Description
1	Power cycle the router.
2	Press the **Break** key (for Windows 2000, press **Control-Break**) to enter into boot ROM mode. The Control-Break key sequence must be entered within 60 seconds of the router restarting after a power cycle. Other terminal applications will have their own sequence, so make sure that you consult the help files.
3	After you are in ROM mode, change the configuration register value to ignore the startup configuration file that is stored in NVRAM. Use the **o/r 0x2142** command (2500 series routers). For Cisco IOS 12.2T (2600 models and higher) or later, the command is **confreg 0x2142**.
4	Allow the router to reboot by entering the **i** command.
5	After the router has finished booting up (you will be prompted to enter the setup dialog—answer **no** or press **Control-c** to abort the setup dialog) without its startup configuration, look at the **show startup-config** command output. If the password is encrypted, move to Step 6, which requires you to enter enabled mode (type **enable** and you will not be required to enter any password) and copy the startup configuration to the running configuration with the **copy startup-config running-config** command. Then, change the password. If the password is not encrypted and the **enable secret** command is not used, simply document the plain-text password and go to Step 8.
6	Because the router currently has no configuration in RAM, you can enter enabled mode by simply typing **enable** (no password is required). Copy the startup configuration to RAM with the IOS command **copy startup-config running-config.**
7	Enable all active interfaces.
8	Change the configuration register to 0x2102 (default) with the global IOS command **config-register 0x2102**. Note that this IOS command is automatically saved and there is no need to write changes to NVRAM when modifying the configuration register even though the IOS will prompt you to save when you do perform a reload.
9	After saving the configuration, you can optionally reload the router.
10	Check the new password if it is not encrypted. If the password is encrypted, simply enter enabled mode and verify your password.

Table 3-12 *Basic Password Security*

Cisco IOS Command	Description
enable password *password*	Defines the enable password (case sensitive) to allow the EXEC user to enter privileged mode, where they can make configuration changes. Typically not encrypted, and it is viewable when the configuration is displayed.
enable secret *password*	Sets the secret password to enable EXEC user to Privilege mode where configuration changes can be made. Overrides an enable password and is encrypted by default.
service password-encryption	Encrypts all passwords on Cisco routers with a weak encryption algorithm.

Table 3-13 *Five Common Switch Exploits*

Exploit	Description
CAM table overflow	Manipulating CAM tables
VLAN hopping	Sending data across VLANs by manipulating VLAN tag information
Spanning Tree Protocol manipulation	Sending rogue BPDU frames
MAC address spoofing	Spoofing Layer 2 MAC addressing for improper use
DHCP starvation	Sending limitless DHCP requests to drain a DHCP pool

Table 3-14 *Three Steps to Securing a Network*

Step	Description
1. Create usage policy statements	Outline user roles and functions within an organization. The main purpose of usage policy statements is to ensure that the user communities understand the security policy.
2. Conduct a risk analysis	Determine the risks to your current network, resources, and data devices.
3. Establish a security team structure	Assemble a cross-functional security team.

Q & A

The Q & A questions are designed to help you assess your readiness for the topics covered on the CCIE Security written exam and those topics presented in this chapter. This format should help you assess your retention of the material. A strong understanding of the answers to these questions will help you on the CCIE Security written exam. You can also look over the questions at the beginning of the chapter again for further review. As an additional study aid, use the CD-ROM provided with this book to take simulated exams, which draw from a database of over 500 multiple-choice questions.

Answers to these questions can be found in Appendix A, "Answers to Quiz Questions."

1. Where is the running configuration stored on a Cisco router?
2. What IOS command displays the startup configuration?
3. What IOS command provides the following output?

```
System flash directory:
File  Length   Name/status
  1   9558976  c2500-ajs40-l.12-17.bin
[9559040 bytes used, 7218176 available, 16777216 total]
16384K bytes of processor board System flash
```

4. What configuration register enables a Cisco router to ignore the startup configuration?
5. To copy the startup configuration to the running configuration, what IOS command or commands are used?
6. What is the range for standard access lists and for extended IP access lists on Cisco IOS routers?
7. What command displays the IP access lists configured on a Cisco router?
8. How do you disable all **debug** commands currently enabled on a Cisco router, assuming you are not sure what debug commands are enabled?
9. What must you be very careful of when enabling any form of debugging on a Cisco router?
10. What are the required steps when performing password recovery on a Cisco router?
11. What is the enable password for the following configuration?

```
enable password CiscO
```

12. What is the CAM table?
13. What are five methods used by intruders to compromise Cisco-based switches?

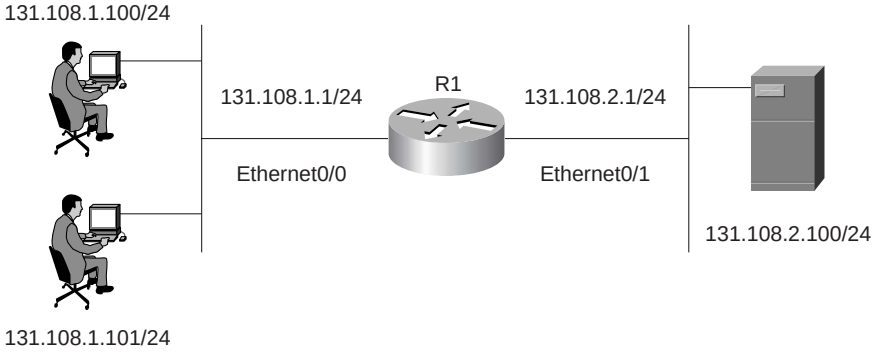
14. What IOS command enables port security for the interface FastEthernet0/1? The MAC address of the end station is 00-DE-AD-CC-EE-00. Ensure that the port is shut down if a violation occurs for more than one MAC address.
15. How does a DHCP starvation attack work?
16. Prior to implementing a security policy, what three common steps should you accomplish?

Scenario

Scenario: Configuring Cisco Routers for Passwords and Access Lists

Figure 3-10 displays a simple one-router network with two Ethernet LAN interfaces connecting users on subnet 131.108.1.0/24 to the server IP network, 131.108.2.0/24.

Figure 3-10 *Scenario Physical Topology*



Example 3-46 displays the working configuration file on Router R1, numbered from line 1 to 25.

Example 3-46 *R1's Full Configuration*

```
1.  version 12.2
2.  no service password-encryption
3.  hostname R1
4.  no logging console debugging
5.  enable secret 5 $1$TBUV$od27CrEfa4UVICBtwvqol/
6.  enable password ciscO
7.  interface Ethernet0/0
8.  ip address 131.108.1.1 255.255.255.0
9.  interface Ethernet0/1
10. ip address 131.108.2.1 255.255.255.0
11. no ip http server
12. access-list 1 permit 131.108.0.0 0.0.255.255
13. access-list 100 permit tcp any host 131.108.1.1 eq telnet
14. access-list 100 permit ip host 131.108.2.100 host 131.108.1.1
15. alias EXEC test show ip route ospf
16. alias EXEC eth0 show interface ethernet0/0
17. alias EXEC eth1 show interface ethernet0/1
```

continues

Example 3-46 *R1's Full Configuration (Continued)*

```
18. line con 0
19. exec-timeout 0 0
20. login
21. line aux 0
22. line vty 0 4
23. exec-timeout 0 0
24. no login
25. end
```

1. The network administrator enables the **debug ip packet** command on Router R1, but no output is seen when connected to the console. IP traffic is following correctly from Ethernet0/0 to Ethernet0/1. What is the likely problem? What IOS configuration change is required to rectify the fault?
2. There are a number of configured aliases. What alias will display the Ethernet interface statistics for the Ethernet interface labeled Ethernet0/1?
3. When the following command is entered at the privileged EXEC prompt, what will the output be?

```
R1#eth0
```

4. What is the password of Router 1 that enables a network administrator to make configuration changes?
5. What Cisco IOS **debug** command can be used to debug the IP packets' source IP address from the address 131.108.2.100 to the PC with the IP address 131.108.1.1?
6. A user telnets to Router R1 and runs the command **debug ip packet**.

   IP data travels from the PC to the server but no output is displayed on the router.

   What is the likely problem?

```
R2#R1
Trying 131.108.255.1 ... Open


R1>debug ip packet
    ^
% Invalid input detected at '^' marker.

R1>
```

7. What is the configuration register of the router in Figure 3-10?
8. What is the vty password required for Telnet clients logging into R1?
9. What does access list 1 accomplish in line 12?
10. What global IOS command would encrypt all passwords configured on R1 in Figure 3-10?

Scenario Answers

Scenario Solutions

1. Line 4 in Example 3-46 has disabled the debug output from being visible. To enable debug messages to be sent to the console port, the command **logging console debugging** must be configured in global configuration mode. Alternatively, telneting to the router and enabling the **terminal monitor** command via the vty line enables the network administrator to view the debug output. (You must also ensure that the command **logging monitor debugging** is configured for Telnet users.)

2. Line 17 displays the alias, **eth1**, which is the command **show interface ethernet0/1**.

3. Line 16 defines an alias, **eth0**, which will be used as a shortcut to the **show interface ethernet0/0** command. This IOS command displays the statistics of interface Ethernet0/0.

4. Line 6 (**enable password ciscO**) defines the enable password as ciscO. However, because a secret password exists on line 5, that is the password required to enter enabled mode, and because the secret password is encrypted, you cannot decipher the password.

5. Access list 100 defines an **access-list** with the source address 131.108.2.100 to the destination IP address 131.108.1.1. You can apply the command **debug ip packet 100** with the optional keyword **detail** to view IP packets sent from the server to the IP address 131.108.1.1.

6. The Telnet user must be in privileged EXEC mode and must enable the **terminal monitor** command to ensure that debug output is sent to the vty line. Use the command **logging monitor debugging** to enable Telnet users to access console messages. See Example 3-47 for IOS help commands.

Example 3-47 **logging ?** *Output*

```
Randy1(config)#logging ?
  Hostname or A.B.C.D  IP address of the logging host
  buffered             Set buffered logging parameters
  cns-events           Set CNS Event logging level
  console              Set console logging level
  exception            Limit size of exception flush output
  facility             Facility parameter for syslog messages
  history              Configure syslog history table
  monitor              Set terminal line (monitor) logging level
  on                   Enable logging to all supported destinations
  rate-limit           Set messages per second limit
  source-interface     Specify interface for source address in logging
                       transactions
  trap                 Set syslog server logging level
```

7. The configuration in Example 3-46 does not include a configuration register, so the default register (0x2102) can be assumed as the correct setting. To correctly identify the configuration register, the **show version** (or **show hardware**) command is required.

8. Line 24 configures the router for no vty login, so there is no password; any Telnet users will be directed to the router at the EXEC prompt level.

9. Access list 1 is not defined on any interface and can be used when **debug ip packet** is turned on. Because it is a standard access list, it can be used to debug packets sourced from IP addresses 131.108.0.0 to 131.108.255.255.

10. The global IOS command **service password-encryption** encrypts all passwords, including the enable and vty password, if any.

Exam Topics in This Chapter

- Remote Authentication Dial-In User Service (RADIUS)
- Terminal Access Controller Access Control System Plus (TACACS+)
- Advanced Encryption Standard (AES)
- EAP, PEAP, TKIP, TLS
- Data Encryption Standard (DES)
- Triple DES (3DES)
- IP Security (IPSec)
- Internet Key Exchange (IKE)
- Certificate Enrollment Protocol (CEP)
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)

You can find a list of all of the exam topics in the introduction to this book. For the latest updates on exam topics, visit Cisco.com.

CHAPTER 4

Security Protocols

This chapter covers some of today's most widely used technologies that enable network administrators to ensure that sensitive data is secure from unauthorized sources.

Standards such as IP Security (IPSec) and encryption standards are covered, as are all the fundamental foundation topics you need to understand to master the topics covered in the CCIE Security written exam.

The chapter ends with a discussion of some of the security features used in wireless networking to improve security. Protocols such as Extensible Authentication Protocol (EAP), Protected Extensible Authentication Protocol (PEAP), Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC), and Transport Layer Security (TLS) are discussed, all of which are newly defined protocols used to help secure vulnerable wireless networks.

This chapter covers the following topics:

- **Security protocol topics**—Sections are included for authentication, authorization, and accounting (AAA), RADIUS, and TACACS+.
- **Encryption Technology Overview**—Covers encrypting IP using standard encryption such as 3DES, AES, and IPSec. The mechanism used to authenticate encryption tunnels is also covered.
- **Certificate Enrollment Protocol**—Describes the Cisco-defined certificate management protocol, CEP, and how a device communicates with a Certificate Authority (CA).
- **EAP, PEAP, and TKIP**—Shows common new mechanisms used in the fight to keep intruders and hackers away from wireless networks.

"Do I Know This Already?" Quiz

The purpose of this assessment quiz is to help you determine how to spend your limited study time.

If you can answer most or all of these questions, you might want to skim the "Foundation Topics" section and return to it later, as necessary. Review the "Foundation Summary" section and answer the questions at the end of the chapter to ensure that you have a strong grasp of the material covered.

If you already intend to read the entire chapter, you do not necessarily need to answer these questions now. If you find these assessment questions difficult, read through the entire "Foundation Topics" section and review it until you feel comfortable with your ability to answer all of these questions and the "Q & A" questions at the end of the chapter.

Answers to these questions can be found in Appendix A, "Answers to Quiz Questions."

1. What are the three components of AAA? (Choose the three best answers.)
   a. Accounting
   b. Authorization
   c. Adapting
   d. Authentication
2. What Cisco IOS command must be issued to start AAA on a Cisco router?
   a. aaa old-model
   b. aaa model
   c. aaa new model
   d. aaa new-model
   e. aaa new_model
3. What mathematical algorithm initiates an encrypted session between two routers by exchanging public keys over an insecure medium such as the Internet?
   a. Routing algorithm
   b. Diffie-Hellman algorithm
   c. The switching engine
   d. The stac compression algorithm
4. Can you configure RADIUS and TACACS+ to be used on the same router?
   a. No.
   b. Yes, provided you have the same lists names applied to the same interfaces.
   c. Yes, provided you have the different lists names applied to the same interfaces.
   d. Yes, provided you have the different list names applied to different interfaces.

5. How do you remotely launch ACS to a Windows 2000 device? (The remote IP address is 10.1.1.1 and the client is Internet Explorer.)

   a. Type launch.
   b. Type 10.1.1.1.
   c. Type 10.1.1.1:2002.
   d. Type 10.1.1.1:8080.

6. What RADIUS attribute is used by vendors and not predefined by RFC 2138?

   a. 1
   b. 2
   c. 3
   d. 4
   e. 13
   f. 26
   g. 333
   h. 33

7. RADIUS can support which of the following protocols?

   a. PPP
   b. OSPF
   c. AppleTalk
   d. IPX
   e. NLSP

8. When a RADIUS server identifies the wrong password entered by the remote user, what packet type is sent?

   a. ACCEPT-USER
   b. REJECT-USERS
   c. REJECT-DENY
   d. REJECT-ACCEPT
   e. REJECT-ERROR
   f. ACCESS-REJECT

9. Identify the false statement about RADIUS.

   a. RADIUS is a defined standard in RFC 2138/2139.
   b. RADIUS runs over TCP port 1812.
   c. RADIUS runs over UDP port 1812.
   d. RADIUS accounting information runs over port 1646.

10. What is the RADIUS key for the following configuration? If this configuration is not valid, why isn't it? (Assume that this configuration is pasted into Notepad and not on an active router.)

```
aaa authentication login use-radius group radius local
aaa authentication ppp user-radius if-needed group radius
aaa authorization exec default group radius
aaa authorization network default group radius
radius-server 3.3.3.3
radius-server key IlovemyMum
```

    a. The RADIUS key is IlovemyMum, and it is a valid configuration.

    b. The RADIUS key is Ilovemymum, and it is a valid configuration.

    c. This configuration will not work because the command **aaa new-model** is missing**.**

    d. The RADIUS key is 3.3.3.3, and it is a valid configuration.

11. What is the RADIUS key for the following configuration?

```
aaa new-model
aaa authentication login use-radius group radius local
aaa authentication ppp user-radius if-needed group radius
aaa authorization exec default group radius
aaa authorization network default group radius
radius-server 3.3.3.3
radius-server key IlovemyMum
```

    a. The RADIUS key is IlovemyMum.

    b. The RADIUS key is Ilovemymum.

    c. No RADIUS key exists.

    d. The RADIUS key is 3.3.3.3.

12. What versions of TACACS does Cisco IOS support? (Select the best three answers.)

    a. TACACS+

    b. TACACS

    c. Extended TACACS

    d. Extended TACACS+

13. TACACS+ is transported over which TCP port number?

    a. 520

    b. 23

    c. 21

    d. 20

    e. 49

14. What is the predefined RADIUS server key for the following configuration?

```
radius-server host 3.3.3.3
radius-server key CCIEsrock
```

a. 3.3.3.3

b. Not enough data

c. CCIESROCK

d. CCIEsRock

e. CCIEsrock

15. What does the following command accomplish?

```
tacacs_server host 3.3.3.3
```

a. Defines the remote TACACS+ server as 3.3.3.3

b. Defines the remote RADIUS server as 3.3.3.3

c. Nothing, because it is not a valid IOS command

d. Configures a Radius server 3.3.3.3

e. An Invalid IOS command

16. Which of the following protocols does TACACS+ support?

a. PPP

b. AppleTalk

c. NetBIOS

d. All of these

17. Which of the following key lengths are *not* supported by AES?

a. 64

b. 128

c. 192

d. 256

e. 512

18. What is the number of bits used with a standard DES encryption key?

a. 56 bits

b. 32 bits; same as IP address

c. 128 bits

d. 256 bits

e. 65,535 bits

f. 168 bits

19. What is the number of bits used with a 3DES encryption key?
    a. 56 bits
    b. 32 bits; same as IP address
    c. 128 bits
    d. 256 bits
    e. 65,535 bits
    f. 168 bits
20. In IPSec, what encapsulation protocol encrypts only the data and not the IP header?
    a. ESP
    b. AH
    c. MD5
    d. HASH
21. In IPSec, what encapsulation protocol encrypts the entire IP packet?
    a. ESH
    b. ESP
    c. AH
    d. MD5
    e. HASH
22. Which of the following is AH's IP number?
    a. 23
    b. 21
    c. 50
    d. 51
    e. 500
    f. 444
23. Which of the following is ESP's IP number?
    a. 23
    b. 21
    c. 50
    d. 51
    e. 500
    f. 444

24. Which of the following is *not* part of IKE phase I negotiations?

- **a.** Authenticating IPSec peers
- **b.** Exchanging keys
- **c.** Establishing IKE security
- **d.** Negotiating SA parameters

25. Which of the following is *not* part of IKE phase II?

- **a.** Negotiating IPSec SA parameters
- **b.** Periodically updating IPSec SAs
- **c.** Occasionally updating SAs (at most, once a day)
- **d.** Establishing IPSec security parameters

26. Which is the fastest mode in IPSec?

- **a.** Main mode
- **b.** Fast mode
- **c.** Aggressive mode
- **d.** Quick mode

27. Certificate Enrollment Protocol (CEP) runs over what TCP port number? (Choose the best two answers.)

- **a.** Same as HTTP
- **b.** Port 80
- **c.** Port 50
- **d.** Port 51
- **e.** Port 333
- **f.** Port 444

28. Which of the following are new features aimed at increasing wireless security? (Choose the best four answers.)

- **a.** TKIP
- **b.** AES
- **c.** EAP
- **d.** PEAP
- **e.** MIC
- **f.** 802.1D
- **g.** ESP
- **h.** AH

Foundation Topics

Authentication, Authorization, and Accounting

Authentication, authorization, and accounting (AAA, pronounced triple A) provides security to Cisco IOS routers and network devices beyond the simple user authentication available on IOS devices.

AAA provides a method to identify which users are logged into a router and each user's authority level. AAA also provides the capability to monitor user activity and provide accounting information.

In today's IP networks, access to network data is available in a variety of methods, including the following:

- PSTN dialup modems
- ISDN dialup
- Internet access through virtual private networks (VPNs)

The AAA model is defined as follows:

- **Authentication**—Who are you?
- **Authorization**—What resources are you permitted to use?
- **Accounting**—What resources were accessed, at what time, by whom, and what commands were issued?

The three phases ensure that legitimate users are permitted access. A remote user must be authenticated before being permitted access to network resources.

Authentication allows the user to submit a username and password and permits challenges and responses. After the user is authenticated, authorization defines what services or resources in the network users are permitted access to. The operations permitted here can include IOS-privileged EXEC commands. For example, a user might type commands but be permitted to use only certain **show** and **debug** commands for which the user is authorized.

Accounting allows the network administrator to log and view what was actually performed (for example, if a Cisco router was reloaded or the configuration was changed). Accounting ensures

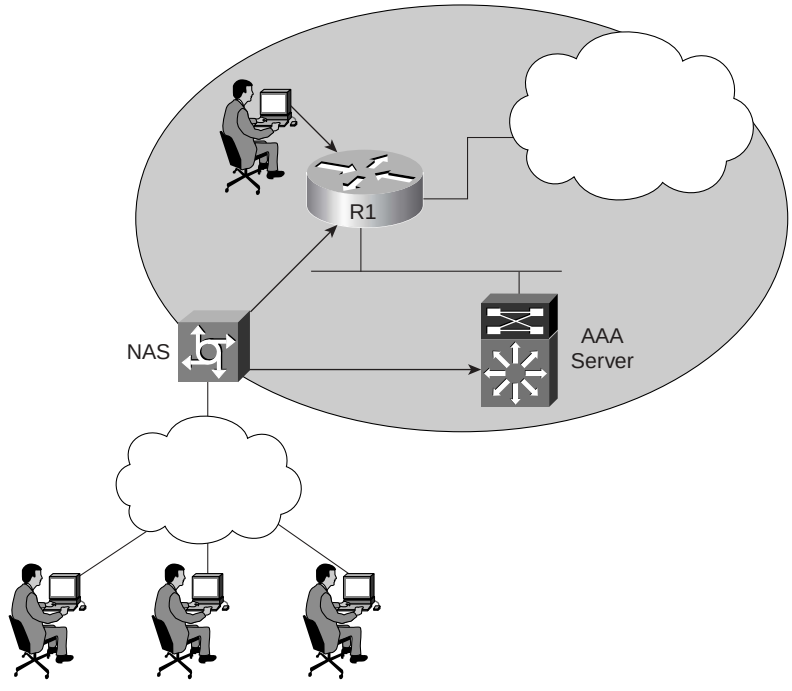
that an audit will enable network administrators to view what was performed and at what time it was performed. Accounting keeps track of the information needed to audit and report network resource usage. This typically includes the username, the start and stop time of login, and the commands typed by the user.

NOTE To start AAA on a Cisco router, issue the following IOS command:

```
aaa new-model
```

Figure 4-1 displays a typical secure network scenario.

Figure 4-1 *Secure Network Access*



The users could be dialup users running async (in this case, PSTN) or using ISDN with Point-to-Point Protocol (PPP). The network access server (NAS) ensures that only authenticated users have access to the secure network; it maintains resources and accounting information.

Authorization tells which resources, or host devices, are authorized to be accessed (such as FTP servers). The NAS implements the AAA protocols and also collects data regarding what network resources were accessed. The NAS can also ensure that devices in the secured network require authentication. For example, the users in Figure 4-1 who are accessing Router R1 require a valid username/password pairing to enter any IOS commands.

The following sections further define what authentication, authorization, and accounting are by discussing a common Cisco IOS router example.

Authentication

Authentication allows administrators to identify who can connect to a router by including the user's username and password. Normally, when a user connects to a router remotely by Telnet, the user must supply only a password, and the administrator has no way of knowing the user's username. You can, however, configure local usernames and passwords on a Cisco IOS router, but this does not scale well and it is not very secure. Configuring a small set of routers with individual usernames and passwords (IOS syntax **username** *username* **password** *password*) is fine, but doing so for large networks would be a difficult exercise to manage. Centrally locating the usernames and passwords is a better solution because only a few devices need to be updated and maintained. Also, users are not logged, and their configuration changes are not monitored without further configuration changes made on each individual router.

Example 4-1 displays a sample code snippet of a remote user accessing a AAA-configured Cisco router by Telnet.

Example 4-1 *Username/Password Pair Entry*

```
Sydney>telnet San-Fran
Trying san-fran (10.99.1.1)... Open User Access Verification
Username: drewrocks
Password: xxxxxxxx
San-Fran>
```

As you can see in Example 4-1, the user must enter a valid username and password to gain access to the router. Typically, a database containing the valid usernames resides locally on the router or on a remote security server.

Authorization

Authorization comes into play after authentication. Authorization allows administrators to control the level of access users have after they successfully gain access to the router. Cisco IOS allows certain access levels (called *privilege levels*) that control which IOS commands the user can issue. For example, a user with a privilege level of 0 cannot issue many IOS commands. There are five commands at privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. A user with a privilege level of 15 can perform all valid IOS commands. The local database or remote security server can grant the required privilege levels.

Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights with the appropriate user. AAA

authorization assembles a set of attributes that describes what the user is authorized to perform. These attributes are compared with the information contained in a database for a given user, and the result is returned to AAA to determine the user's actual permissions and restrictions.

NOTE You can display the user's privilege level on a Cisco router with the **show privilege** command. The following code displays the privilege level when the enable password has already been entered:

```
R1#show privilege
Current privilege level is 15
```

The higher the privilege, the more capabilities a user has with the IOS command set.

Accounting

Accounting occurs after authentication and authorization have been completed. Accounting allows administrators to collect information about users. Specifically, administrators can track which user logged into which router, which IOS commands a user issued, and how many bytes were transferred during a user's session. For example, accounting enables administrators to monitor which routers have had their configurations changed. Accounting information can be collected by a remote security server.

To display local account information on a Cisco router collecting accounting information, issue the **show accounting** IOS command. Example 4-2 displays sample output when the command is issued on Router R1. (Note that for Cisco IOS 12.2T and higher, the command has changed to **show aaa user all**.)

Example 4-2 show accounting Command

```
R1#show accounting
Active Accounted actions on Interface Serial0:1, User jdoe Priv 1
 Task ID 15, Network Accounting record, 00:00:18 Elapsed
 task_id=15 timezone=PDT service=ppp mlp-links-max=4 mlp-links-current=4
protocol=ip addr=119.0.0.2 mlp-sess-id=1
      Overall Accounting Traffic
          Starts   Stops  Updates  Active  Drops
Exec           0       0        0       0       0
Network        8       4        0       4       0
Connect        0       0        0       0       0
Command        0       0        0       0       0
Rsrc-mgmt      1       0        0       1       0
System         0       0        0       0       0
 User creates:21, frees:9, Acctinfo mallocs:15, frees:6
Users freed with accounting unaccounted for:0
Queue length:0
```

Table 4-1 describes the fields contained in Example 4-2.

Table 4-1 **show accounting** *Fields*

Field	Description
User	The user's ID
Priv	The user's privilege level (0–15)
Task ID	Each accounting session's unique identifier
Accounting Record	Type of accounting session
Elapsed	Length of time (hh:mm:ss) for this session type

Rather than maintain a separate database with usernames, passwords, and privilege levels, you can use external security servers to run external security protocols—namely RADIUS and TACACS.

These security server protocols stop unauthorized access to your network. The following sections review these two security protocols.

Security Server Protocols

In many circumstances, AAA uses security protocols to administer its security functions. If your router or access server is acting as an NAS, AAA is the means through which you establish communication between your NAS and your RADIUS, TACACS+, or Kerberos security server.

Remote Authentication Dial-In User Service

RADIUS is a client/server-based system that secures a Cisco network against intruders. Implemented in Cisco IOS, RADIUS sends authentication requests to a RADIUS server. RADIUS was created by Livingston Enterprises and is now defined in RFCs 2865/2866 (RFCs 2138/2139 are now obsolete).

A RADIUS server is a device that has the RADIUS daemon or application installed. RADIUS must be used with AAA to enable the authentication, authorization, and accounting of remote users when using Cisco IOS routers.

When a RADIUS server authenticates a user, the following events occur:

1. The user is prompted for and enters a username and password.
2. The username and encrypted password are sent over the network to the RADIUS server. These events are sent via the packet format known as Access-Request.

3. The user receives one of the following responses from the RADIUS server:

   ACCESS-ACCEPT—The user is authenticated.

   ACCESS-REJECT—The user is not authenticated and is prompted to re-enter the username and password, or access is denied. The RADIUS server sends this response when the user enters an invalid username/password pairing.

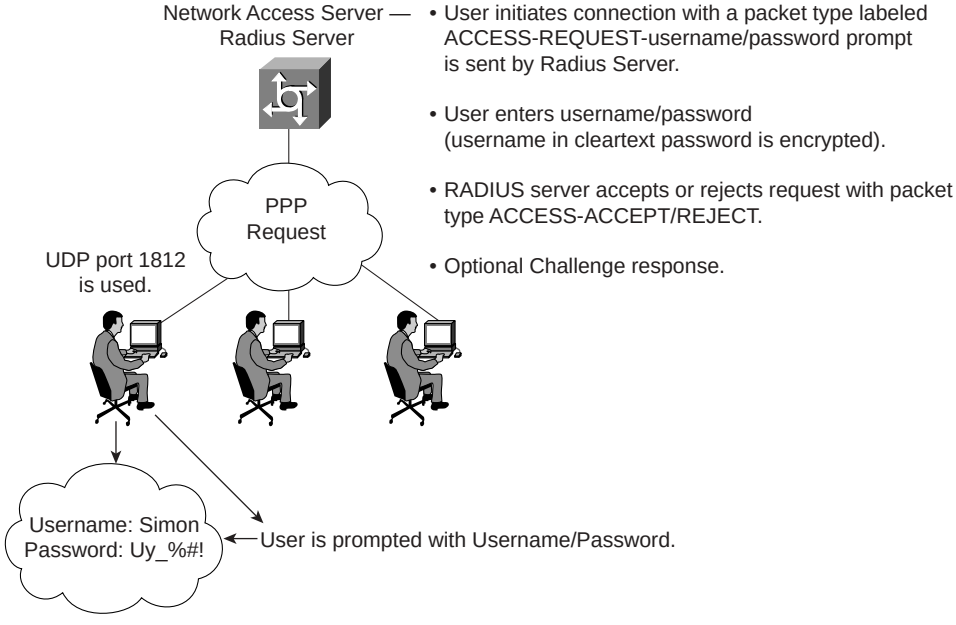
   ACCESS-CHALLENGE—A challenge is issued by the RADIUS server. The challenge collects additional data from the user.

   CHANGE PASSWORD—The RADIUS server issues a request asking the user to select a new password.

An ACCESS-ACCEPT or ACCESS-REJECT response may contain additional information for services that the user can access, including Telnet, rlogin, or local-area transport (LAT) connections, and PPP, Serial Line Internet Protocol (SLIP), or EXEC services.

RADIUS is commonly used when PPP is used. Figure 4-2 displays a typical PPP connection request to a RADIUS server.

Figure 4-2 *RADIUS Sequence Example*



The RADIUS server accepts or rejects a username and password pair. In some instances, a user might be asked to enter more information (this is called a challenge response). For example, if a user's password has expired, a RADIUS server prompts the user for a new password.

Transactions between the client (end user) and the RADIUS server are authenticated through a shared secret. The username is sent as clear text. RADIUS supports both Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). PAP and CHAP are security protocols that allow users to gain access to remote devices with PPP. A RADIUS server will never send the user's password over the network in any circumstance. If the username/password pairing is entered incorrectly, the RADIUS server sends an ACCESS-REJECT response. The end user must re-enter the pairings or the connection will be rejected. Note that PAP sends the end user's password in the clear to the NAS, but from the NAS to the RADIUS server (the NAS and the RADIUS communicate using the shared secret), the end user's password is encrypted.

RADIUS supports a number of predefined attributes that can be exchanged between client and server, such as the client's IP address. RADIUS attributes carry specific details about authentication.

RFC 2138 defines a number of attributes. The following list provides details for the most common attributes:

- **Attribute type 1**—Username (defines usernames, such as numeric, simple ASCII characters, or a Simple Mail Transfer Protocol [SMTP] address).
- **Attribute type 2**—User Password (defines the password, which is encrypted using Message Digest 5 [MD5]).
- **Attribute type 3**—CHAP Password (used only in access-request packets).
- **Attribute type 4**—NAS IP Address (defines the NAS's IP address; used only in access-request packets).
- **Attribute type 5**—NAS Port (this is not the User Datagram Protocol [UDP] port number; it indicates the NAS's physical port number, ranging from 0 to 65,535).
- **Attribute type 6**—Service-Type of service requested or type of service to be provided. Now supported in Cisco IOS. See (requires CCO login) http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1839/products_feature_guide09186a0080110bed.html#1024276.
- **Attribute type 7**—Framed-Protocol defines required framing; for example, PPP is defined when this attribute is set to 1 and SLIP is set to 2.
- **Attribute type 8**—Framed-IP-Address defines the IP address to be used by the remote user.
- **Attribute type 9**—Framed-IP-Netmask defines the subnet mask to be used by the remote user.
- **Attribute type 10**—Framed-Routing.

- **Attribute type 13**—Framed-Compression.
- **Attribute type 19**—Callback-Number.
- **Attribute type 26**—Vendor-Specific. Cisco (vendor-ID 9) uses one defined option: vendor type 1 named cisco-avpair; this attribute transmits TACACS+ A/V pairs.
- **Attribute type 61**—NAS-Port-Type

Table 4-2 summarizes the RADIUS protocol's main features.

Table 4-2 *Summary of RADIUS Protocol Features*

Feature	Description
UDP	Packets sent between the client and server are UDP, primarily because TCP's overhead does not allow for significant advantages. Typically, the user can wait for a username/password prompt.
UDP destination port	1812 and 1813. Defined in RFC 2865, which supersedes RFC 2138. Early deployments RADIUS used UDP ports 1645 and 1646.
Attributes	Attributes are used to exchange information between the NAS and client.
Model	Client/server-based model in which packets are exchanged in a unidirectional manner.
Encryption method	The password is encrypted using MD5; the username is not encrypted. RADIUS encrypts only the password in the access-request packet, sent from the client to the server. The remainder of the packet is transmitted in clear text. A third party could capture other information, such as the username, authorized services, and accounting information.
Multiprotocol support	Does not support protocols such as AppleTalk, NetBIOS, or IPX. IP is the only protocol supported.

Now, examine the RADIUS configuration tasks required on a Cisco router.

IETF Attribute 26 (Vendor-Specific) encapsulates vendor-specific attributes, thereby allowing vendors to support their own extended attributes. Attribute 26 contains the following three elements:

- Type
- Length
- String (also known as data)

RADIUS Configuration Task List

A RADIUS server is usually software that runs on a variety of platforms, including Microsoft Windows 2000 Server and various UNIX hosts. RADIUS can authenticate router users and even validate IP routes.

To configure RADIUS on your Cisco router or NAS, perform the following tasks:

Step 1 Enable AAA with the **aaa new-model** global configuration command. AAA must be configured if you plan to use RADIUS.

Step 2 Use the **aaa authentication** global configuration command to define method lists for RADIUS authentication.

Step 3 Use **line** and **interface** commands to enable the defined method lists to be used.

Step 4 Define the RADIUS server and secret key with the following IOS commands:

```
radius-server ip-address
radius-server key secret-key
```

NOTE There are two optional RADIUS commands:

Use the **aaa authorization** global command to authorize specific user functions.

Use the **aaa accounting** command to enable accounting for RADIUS connections.

Examples are the best method to show the enormous IOS command set that is available for use when configuring RADIUS support with AAA.

Example 4-3 configures a Cisco IOS router with AAA and RADIUS support.

Example 4-3 *AAA and RADIUS IOS Configuration*

```
aaa new-model
aaa authentication login use-radius group radius local
aaa authentication ppp user-radius if-needed group radius
aaa authorization exec default group radius
aaa authorization network default group radius
radius-server 3.3.3.3
radius-server key ccie2005
! Ensure you apply the named access list on the VTY line
line vty 0 4
aaa authentication login
```

The command lines in this RADIUS authentication and authorization configuration are defined as follows:

- The **aaa authentication login use-radius group radius local** command configures the router to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database. In this example, **use-radius** is the name of the method list, which specifies RADIUS and then local authentication. If the RADIUS server returns the ACCESS-REJECT response, the user is denied access and the router will not check its local database.
- The **aaa authentication ppp user-radius if-needed group radius** command configures the Cisco IOS software to use RADIUS authentication for lines using PPP with CHAP or PAP, if the user is not already authorized. If the EXEC facility has authenticated the user, RADIUS authentication is not performed. In this example, **user-radius** is the name of the method list defining RADIUS as the if-needed authentication method.
- The **aaa authorization exec default group radius** command sets the RADIUS information used for EXEC authorization, autocommands, and access lists.
- The **aaa authorization network default group radius** command sets RADIUS for network authorization, address assignment, and access lists.
- The **radius-server** commands define the NAS.
- The **radius-server key** commands define the shared secret text string between the NAS and the RADIUS server host.

Example 4-4 displays an example in which AAA is enabled on a Cisco IOS router.

Example 4-4 *AAA and RADIUS Example*

```
Hostname R1
username simon password SimonisisAgreatdrummeR
aaa new-model
aaa authentication ppp dialins group radius local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
aaa authentication login simon local
aaa authorization exec default local
radius-server host 3.3.3.3
radius-server key CCIEsrock
line vty 0 4
login authentication radius-login
```

The Example 4-4 line configurations are defined as follows:

- The **radius-server host** command defines the RADIUS server host's IP address.
- The **radius-server key** command defines the shared secret text string between the NAS and the RADIUS server host.
- The **aaa authentication ppp dialins group radius local** command defines the authentication method list, dialins, which specifies that RADIUS authentication and then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP.
- The **aaa authorization network default group radius local** command sets RADIUS for network authorization, address assignment, and access lists.
- The **aaa accounting network default start-stop group radius** command tracks PPP usage. This command is used for all network services. It can be PPP, but also SLIP or ARAP.
- The **aaa authentication login simon local** command defines the method list, simon, for local authentication.
- The **aaa authentication login simon** command applies the simon method list for login authentication.

NOTE A method list simply defines the authentication methods to be used, in sequence, to authenticate a user. Method lists enable you to designate one or more security protocols to be used for authentication, ensuring a backup system for authentication in case the initial method fails. Cisco IOS software uses the first method listed to authenticate users; if that method does not respond, the Cisco IOS software selects the next authentication method listed. This process continues until there is successful communication with a listed authentication method or the authentication method list is exhausted, in which case authentication fails.

TIP Cisco.com provides a long list of configuration examples. To view more detailed configurations, visit the following web address and follow the link to Security Management:

http://www.cisco.com/pcgi-bin/Support/browse/index.pl?i=Products&f=753&viewall=true

Terminal Access Controller Access Control System Plus

Cisco IOS supports three versions of TACACS—TACACS, extended TACACS, and TACACS+. All three methods authenticate users and deny access to users who do not have a valid username/password pairing. TACACS+ is Cisco proprietary, whereas RADIUS is an open standard originally created by Livingston Enterprises.

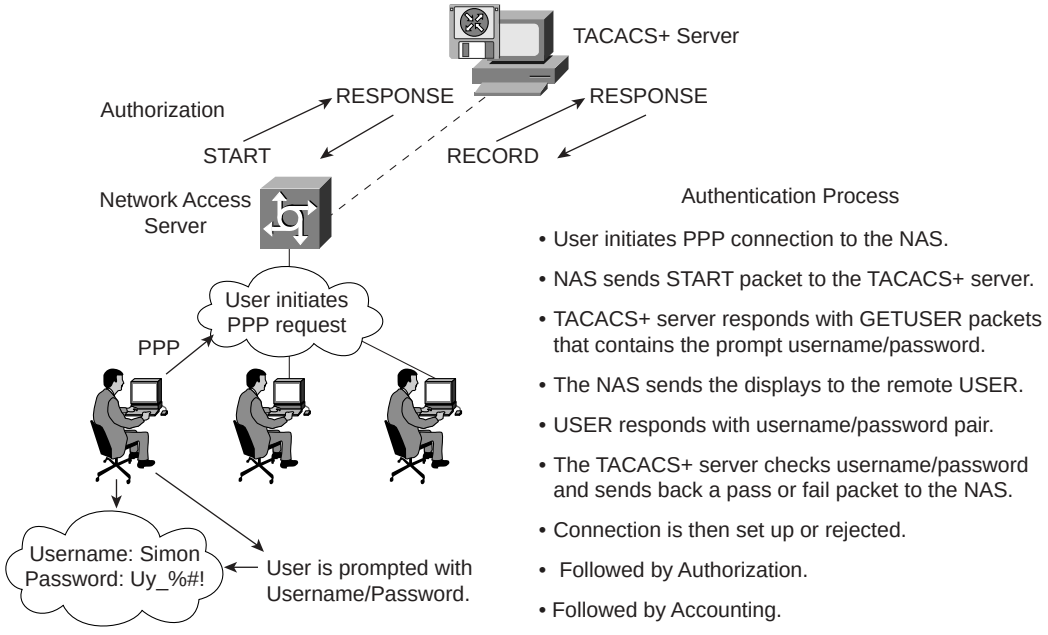
Cisco has also developed Cisco Secure Access Control Server (ACS), a flexible family of security servers that supports both RADIUS and TACACS+. You can even run debugging commands on the Cisco Secure ACS software. In UNIX, you can modify files, such as syslog.conf and csu.cfg, to change the output to your screen. For more details on how to debug on a UNIX server, see http://www.cisco.com/warp/public/480/cssample2x.html#debug.

TACACS+ has the following features:

- TCP packets (port 49) ensure that data is sent reliably across the IP network.
- Supports AAA architectures and, in fact, separates each of the three AAA mechanisms.
- The data between the NAS and server is encrypted.
- Supports both PAP/CHAP and multiprotocols such as IPX and X.25.
- Access control lists (ACL) can be defined on a per-user basis. (RADIUS can also define ACLs on a per-user basis.)

Figure 4-3 displays a typical TACACS+ connection request (authentication).

Figure 4-3 *TACACS+ Authentication Example Sequence*



When a TACACS+ server authenticates a remote user, the following events occur:

1. When the connection is established, the NAS contacts the TACACS+ daemon to obtain a username prompt, which is then displayed to the user. The user enters a username and the NAS and communicates to the TACACS+ server to obtain a password prompt. The NAS displays the password prompt to the user, the user enters a password, and the password is sent to the TACACS+ daemon.
2. The NAS eventually receives one of the following responses from the TACACS+ daemon:
   - **ACCEPT**—The user is authenticated and service can begin. If the NAS is configured to require authorization, authorization begins at this time.
   - **REJECT**—The user has failed to authenticate. The user may be denied further access or may be prompted to retry the login sequence, depending on the TACACS+ daemon.
   - **ERROR**—An error occurred at some time during authentication. This can be either at the daemon or in the network connection between the daemon and the NAS. If an ERROR response is received, the NAS typically tries to use an alternative method for authenticating the user.
   - **CONTINUE**—The user is prompted for additional authentication information.
3. A PAP login is similar to an ASCII login, except that the username and password arrive at the NAS in a PAP protocol packet instead of being typed in by the user, so the user is not prompted. PPP CHAP logins are also similar, in principle.
4. Following authentication, the user is required to undergo an additional authorization phase, if authorization has been enabled on the NAS. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.
5. If TACACS+ authorization is required, the TACACS+ daemon is again contacted and it returns an ACCEPT or REJECT authorization response. If an ACCEPT response is returned, the response contains data in the form of attributes used to direct the EXEC or NETWORK session for that user, determining services that the user can access.

   Services include the following:

   - Telnet, rlogin, PPP, SLIP, or EXEC services
   - Connection parameters, including the host or client IP address, ACL, and user timeouts

The TACACS+ authorization process is defined as the packet flow between the NAS and the TACACS+ server. The packets exchanged between the NAS and server contain AV pairs. The NAS sends Start packets and the TACACS+ server responds with Response packets. The server can permit, deny, or modify commands requested by the end user. The data (that contains the full list of all username/password pairs) is stored on a local file defining what commands are permitted by the end user, for example.

TACACS+ accounting provides an audit record of what commands were completed. The NAS sends a record of any commands, and the TACACS+ server sends a response acknowledging the accounting record.

Table 4-3 summarizes the main features of TACACS+.

Table 4-3 *Summary of TACACS+ Protocol*

	Feature
TCP	Packets sent between client and server are TCP.
TCP destination port	Port 49.
Attributes	Packet types are defined in TACACS+ frame format as follows: Authentication 0x01 Authorization 0x02 Accounting 0x03
Seq_no	The sequence number of the current packet flow for the current session. The Seq_no starts with 1, and each subsequent packet increments by one. The client sends only odd numbers. The TACACS+ server sends only even numbers.
Encryption method	The entire packet is encrypted. Data is encrypted using MD5 and a secret key that matches both on the NAS (for example, a Cisco IOS router) and the TACACS+ server.
Multiprotocol support	Multiprotocol Support indicates the following are fully supported in non IP networks, multiprotocols such as AppleTalk, NetBIOS, or IPX, along with IP.

Now, examine the TACACS+ configuration tasks required when enabling TACACS+ on a Cisco IOS router.

TACACS+ Configuration Task List

To configure your router to support TACACS+, you must perform the following tasks:

Step 1 Use the **aaa new-model** global configuration command to enable AAA, which must be configured if you plan to use TACACS+. For more information about using the **aaa new-model** command, refer to http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt1/scdaaa.htm.

Step 2 Use the **tacacs-server host** command to specify the IP address of one or more TACACS+ daemons:

```
tacacs-server host hostname [single-connection] [port integer] [timeout
integer] [key string]
```

Step 3 Use the **tacacs-server key** command to specify an encryption key to encrypt all exchanges between the NAS and the TACACS+ daemon. This same key must also be configured on the TACACS+ daemon. The actual command is as follows:

```
tacacs-server key key
```

The key should match the one used on the TACACS+ daemon.

Step 4 Use the **aaa authentication** global configuration command to define method lists that use TACACS+ for authentication.

Step 5 Use **line** and **interface** commands to apply the defined method lists to various interfaces.

Step 6 To enable authorization, use the **aaa authorization** global command to configure authorization for the NAS. Unlike authentication, which can be configured per line or per interface, authorization is configured globally for the entire NAS.

Step 7 To enable accounting for TACACS+ connections, use the **aaa accounting** command. Optional commands include the following:

- Configuring AAA server groups (Optional)
- Configuring AAA server group selection based on Dialed Number Identification Service (DNIS) (Optional)
- Specifying TACACS+ authentication (Required)
- Specifying TACACS+ authorization (Optional)
- Specifying TACACS+ accounting (Optional)

Example 4-5 displays a sample configuration of a Cisco router with TACACS+ authentication for PPP.

Example 4-5 *TACACS+ Authentication for PPP Example*

```
aaa new-model
aaa authentication ppp CCIE group tacacs+ local
tacacs-server host 10.1.2.3
tacacs-server key cciesarecool
interface serial 0
 ppp authentication chap pap CCIE
```

The configuration lines in Example 4-5 are defined as follows:

- The **aaa new-model** command enables the AAA security services.
- The **aaa authentication** command defines a method list, CCIE, to be used on serial interfaces running PPP. The keyword **group tacacs+** means that authentication is done through TACACS+. If TACACS+ returns an ERROR during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the NAS. Note that the local database is not used if a REJECT response is received from the security server.

- The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 10.1.2.3. The **tacacs-server key** command defines the shared encryption key as cciesarecool.
- The **interface** command selects the line, and the **ppp authentication** command applies the CCIE method list to this line.

Example 4-6 shows how to configure TACACS+ as the security protocol for PPP authentication using the default method list; it also shows how to configure network authorization through TACACS+.

Example 4-6 *Authorization and TACACS+ Example*

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
aaa authorization network default group tacacs+
tacacs-server host 3.3.3.3
tacacs-server key simoniscool
interface serial 0
ppp authentication default
```

The lines in the preceding sample configuration are defined as follows:

- The **aaa new-model** command enables the AAA security services.
- The **aaa authentication** command defines a method list, default, to be used on serial interfaces running PPP. The keyword **default** means that PPP authentication is applied by default to all interfaces. The **if-needed** keyword means that if the user has already authenticated by going through the ASCII login procedure, PPP authentication is not necessary and can be skipped. If authentication is needed, the keyword **group tacacs+** means that authentication is done through TACACS+. If TACACS+ returns an ERROR during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the NAS.
- The **aaa authorization** command configures network authorization via TACACS+.
- The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 3.3.3.3.
- The **tacacs-server key** command defines the shared encryption key as simoniscool.
- The **interface** command selects the line, and the **ppp authentication** command applies the default method list to this line.

The source interface used by TACACS+ or RADIUS can be defined when required as follows:

```
ip tacacs source-interface subinterface-name
ip radius source-interface subinterface-name
```

The **source-interface** commands force the security protocol to use a specific interface as the source IP address. For example, it may be a loopback address (remember, it is always active, unlike a physical interface, which may fail or be down) for redundancy purposes in case of a physical interface failure.

Example 4-7 displays a sample configuration where accounting is also enabled.

Example 4-7 *Accounting Example*

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
aaa accounting network default stop-only group tacacs+
tacacs-server host 3.3.3.3
tacacs-server key andrewiscool
interface serial 0
ppp authentication default
```

The lines in the Example 4-7 configuration are defined as follows:

- The **aaa new-model** command enables the AAA security services.
- The **aaa authentication** command defines a method list, default, to be used on serial interfaces running PPP. The keyword **default** means that PPP authentication is applied by default to all interfaces. The **if-needed** keyword means that if the user has already authenticated through the ASCII login procedure, PPP authentication is not necessary. If authentication is needed, the keyword **group tacacs+** means that authentication is done through TACACS+. If TACACS+ returns an ERROR during authentication, the keyword local indicates that authentication will be attempted using the **local** database on the NAS.
- The **aaa accounting** command configures network accounting through TACACS+. In this example, accounting records stop-only, meaning that the session that just terminated will be sent to the TACACS+ daemon whenever a network connection terminates.
- The **interface** command selects the line, and the **ppp authentication** command applies the default method list to this line.

NOTE You can define a group of TACACS+ servers by defining the servers with the IOS commands **tacacs-server host** *ip-address-of-server* and **tacacs-server key** *secret-key*. For example, to define six servers, you would use the following IOS configuration:

```
tacacs-server host 1.1.1.1
tacacs-server host 2.2.2.2
tacacs-server host 3.3.3.3
tacacs-server host 4.4.4.4
tacacs-server host 5.5.5.5
tacacs-server host 6.6.6.6
tacacs-server key ccie
```

If the first server does not respond within a timeout period (the default is 5 seconds), the next server is queried, and so forth.

Typically, the console port is not configured for authorization.

TACACS+ Versus RADIUS

Table 4-4 compares the main differences between TACACS+ and RADIUS.

Table 4-4 *TACACS+/RADIUS Comparison*

	RADIUS	TACACS+
Packet delivery	UDP.	TCP.
Packet encryption	Encrypts only the password in the access-request packet from the client to the server.	Encrypts the entire body of the packet but leaves a standard TCP header.
AAA support	Combines authentication and authorization.	Uses the AAA architecture, separating authentication, authorization, and accounting.
Multiprotocol support	None.	Supports other protocols, such as AppleTalk, NetBIOS, and IPX.
Router management	Can pass a privilege level down to the router, which can then be used locally for command authorization.	Enables network administrators to control which commands can be executed on a router.
Responses	Uses single-challenge response. Combines authentication and authorization.	Uses multiple-challenge response for each of the AAA processes. Uses the AAA architecture and separates each process.

NOTE You can configure both RADIUS and TACACS+ concurrently on a Cisco router provided that you have defined different list names and applied the list to different interfaces.

NOTE You can download and install a trial copy of Cisco Secure ACS for Windows NT/2000 or UNIX. This comes with a built-in RADIUS and TACACS+ server. You also need a Cisco router with Cisco IOS 12.X with one working Ethernet port. This will reinforce your understanding of the AAA concept. For more information, visit the Cisco Secure Software Center at Cisco.com.

The AAA configuration options are numerous, and those presented in this guide are only a small subset of a larger set that you can view online at Cisco.com. Visit the following URL for more quality examples of how AAA, along with RADIUS or TACACS, can be implemented on Cisco IOS routers:

http://www.cisco.com/pcgi-bin/Support/browse/index.pl?i=Technologies&f=774

The IOS **debug** command set for RADIUS and TACACS is extensive. Presented here are some common RADIUS and TACACS debug outputs found in real networks.

Example 4-8 displays a sample output from the **debug aaa authentication** command for a RADIUS login attempt that failed. The information indicates that TACACS is the authentication method used.

Example 4-8 **debug aaa authentication** *Command*

```
R1# debug aaa authentication
14:02:55: AAA/AUTHEN (164826761): Method=RADIUS
14:02:55: AAA/AUTHEN (164826761): status = GETPASS
14:03:01: AAA/AUTHEN/CONT (164826761): continue_login
14:03:01: AAA/AUTHEN (164826761): status = GETPASS
14:03:04: AAA/AUTHEN (164826761): status = FAIL
```

Example 4-9 displays a sample output from the **debug radius** command that shows a successful login attempt (note that newer versions of IOS code may display some differences), as indicated by an Access-Accept message.

Example 4-9 **debug radius** *Command*

```
R1# debug radius
 13:59:02: Radius: IPC Send 0.0.0.0:1645, Access-Request, id 0xB, len 56
13:59:02:         Attribute 4 6 AC150E5A
13:59:02:         Attribute 5 6 0000000A
13:59:02:         Attribute 1 6 62696C6C
13:59:02:         Attribute 2 18 0531FEA3
13:59:04: Radius: Received from 131.108.1.1:1645, Access-Accept, id 0xB, len 26
13:59:04:         Attribute 6 6 00000001
```

Example 4-10 displays a sample output from the **debug radius** command that shows an unsuccessful login attempt, as indicated by an Access-Reject message.

Example 4-10 **debug radius** *Command*

```
R1# debug radius
13:57:56: Radius: IPC Send 0.0.0.0:1645, Access-Request, id 0xA, len 57
13:57:56:         Attribute 4 6 AC150E5A
13:57:56:         Attribute 5 6 0000000A
13:57:56:         Attribute 1 7 62696C6C
13:57:56:         Attribute 2 18 49C28F6C
13:57:59: Radius: Received from 171.69.1.152:1645, Access-Reject, id 0xA, len 20
```

Encryption Technology Overview

When prominent Internet sites, such as http://www.cnn.com, are exposed to security threats, the news reaches all parts of the globe. Ensuring that data crossing any IP network is secure and not vulnerable to threats is one of today's most challenging tasks in the IP storage arena (so much so that Cisco released an entirely new CCIE for the storage networking certification track).

Major problems for network administrators include the following:

- **Packet snooping (eavesdropping)**—When intruders capture and decode traffic, obtaining usernames, passwords, and sensitive data such as salary increases for the year.
- **Theft of data**—When intruders use sniffers, for example, to capture data over the network and steal that information for later use.
- **Impersonation**—When an intruder assumes the role of a legitimate device but, in fact, is not legitimate. The intruder efficiently assumes the role of an authorized user.

The solution to these and numerous other problems is to provide encryption technology to the IP community and enable network administrators to ensure that data is not vulnerable to any form of attack or intrusion. This ensures that data is confidential, authenticated, and has not lost any integrity during the routing of packets through an IP network.

Encryption (user data that is encrypted will require decryption also) is defined as the process by which plain data is converted into ciphered data (a system in which plain-text data is arbitrarily substituted according to a predefined algorithm known as cipertext) so that only the intended recipient(s) can observe the data. Encryption ensures data privacy, integrity, and authentication.

Figure 4-4 displays the basic methodologies behind data encryption.

Figure 4-4 *Encryption Methodologies*

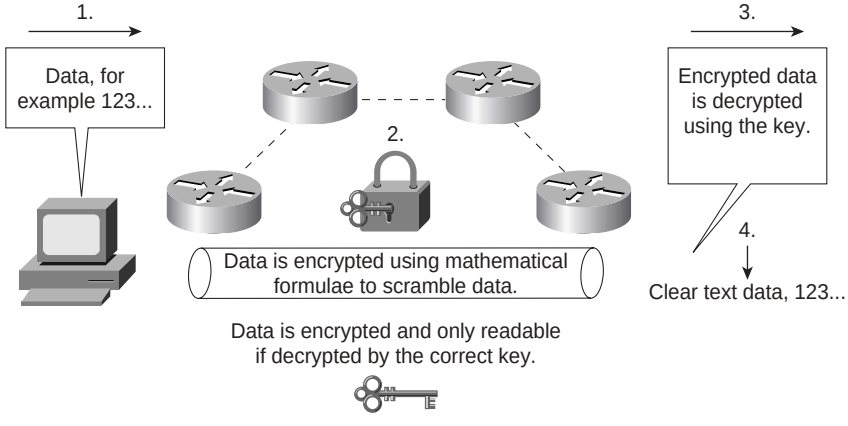


Figure 4-4 demonstrates the basic principles of data encryption, including the following:

1. User data is forwarded over the network.

2. Data (clear text) is modified according to a key. The key is a sequence of digits that decrypts and encrypts messages. Each device has three keys:
   - A private key used to sign messages that is kept secret and never shared.
   - A public key that is shared (used by others to verify a signature).
   - A shared secret key that is used to encrypt data using a symmetric encryption algorithm, such as DES. Typically, however, a device has two keys, a symmetric key and an asymmetric key. The symmetric key is a shared secret that is used to both encrypt and decrypt the data. The asymmetric key is broken into two parts, a private key and a public key.
3. A mathematical formula is applied to scramble the data. In Figure 4-4, the mathematical formula is applied during Step 2.
4. The data flows throughout the network and can be decrypted only if the correct key and algorithm are applied.

Encryption can take place at the application layer, the network layer, or the data link layer. Be aware of the following encryption technologies for the CCIE Security written exam:

- Data Encryption Standard (DES)
- Triple DES (3DES)
- Advanced Encryption Standard (AES)
- IP Security (IPSec)

Cisco IOS routers support the following industry standards to accomplish network layer encryption:

- DES/3DES
- AES
- MD5
- Diffie-Hellman exchange
- IPSec

DES and 3DES

DES is one of the most widely used encryption methods. DES turns clear-text data into cipher text with an encryption algorithm. The receiving station will decrypt the data from cipher text into clear text. The shared secret key is used to derive the session key, which is then used to encrypt and decrypt the traffic.

Figure 4-5 demonstrates DES encryption.

Figure 4-5 *DES Encryption Methodologies*

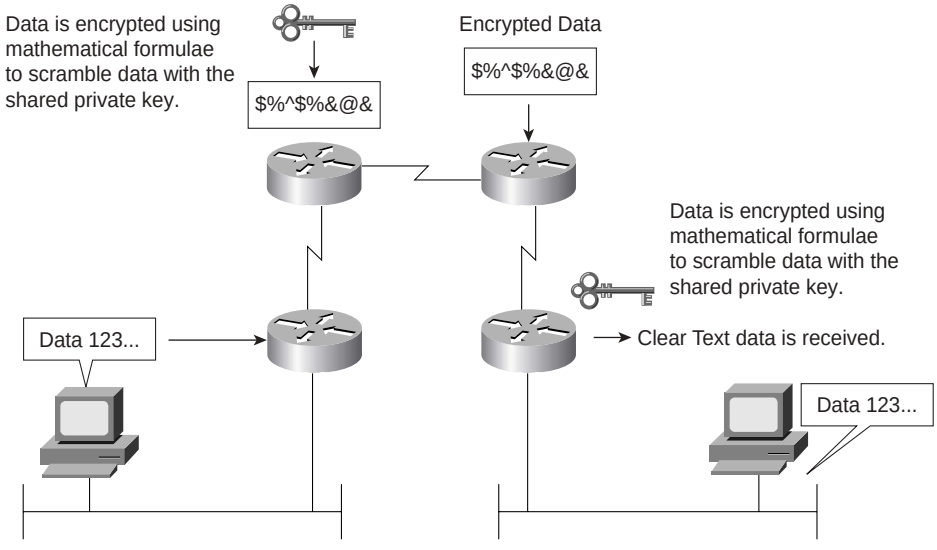


Figure 4-5 demonstrates the PC's clear-text generation. The data is sent to the Cisco IOS router, where it is encrypted with a shared key (remember, the shared secret key is used to derive the session key, which is then used to encrypt and decrypt the traffic) and sent over the IP network in unreadable format until the receiving router decrypts the message and forwards it in clear-text form.

DES is a block cipher algorithm, which means that DES performs operations on fixed-length data streams. DES uses a 56-bit key to encrypt 64-bit datagrams.

DES is a published, U.S. government–standardized encryption method; however, it is no longer a U.S. government–approved encryption algorithm.

3DES is the DES algorithm that performs three times (3 x 3 x encryption and 3 x decryption) sequentially (although there are some variations as well). Three keys are used to encrypt data, resulting in a 168-bit encryption key.

3DES is an improved encryption algorithm standard and is summarized as follows:

1. The sending device encrypts the data with the first 56-bit key.
2. The sending device decrypts the data with the second key, also 56 bits in length.
3. The sending device encrypts for a final time with another 56-bit key.

4. The receiving device decrypts the data with the first key.
5. The receiving device then encrypts the data with the second key.
6. Finally, the receiving device decrypts the data with the third key.

A typical hacker uses a Pentium III computer workstation and takes approximately 22 hours to break a DES key. In the case of 3DES, the documented key-breaking times are approximately 10 billion years when 1 million PC III computers are used. Encryption ensures that information theft is difficult.

TIP It is possible to increase the number of bits in the key, but brute-force cracking of a 1024-bit key is not feasible using current or reasonably foreseeable technology. Even if, based on future innovations, this becomes a weak key length, the value of the data it protects will have very likely diminished to zero. In the event that you have need for more protection, you can increase the key size. However, you should be aware that this will take a processing toll on every secure transaction.

NOTE Unbeknownst to the author of the previous tip, a mathematician named D. J. Bernstein delivered a paper entitled "How To Find Small Factors Of Integers" (http://cr.yp.to/papers.html#nfscircuit) earlier in the year. At the Financial Cryptography conference held in late March, 2002, it was discovered that, using his formulas, 512-bit keys can be broken in less than 10 minutes using Pentium IV–based computers and that an array of them (cost estimate, $1 billion) could break a 1024-bit key in the same time. That price tag is well within the reach of the world's major security agencies; an NSA satellite's price tag is double that, and it has several of them.

The lessons here are two-fold. First, if your data is attractive enough to those able to afford those rapidly declining but still very large price tags, go for the biggest key your software supports. Second, authors who write tips like the previous one do so at great risk.

Encryption can be used to enable secure connections over the LAN, WAN, and World Wide Web.

The end goal of DES/3DES is to ensure that data is confidential by keeping data secure and hidden. The data must have integrity to ensure that it has not been modified in any form, and be authenticated by ensuring that the source or destination is indeed the proper host device. Another encryption standard in common use today is widely regarded as the new industry standard, namely AES.

Advanced Encryption Standard

AES, developed by Joan Daemen and Vincent Rijmen, is a new encryption standard and is considered a replacement for DES. The U.S. government made AES a standard in May 2002, and

the National Institute of Standards and Technology (NIST) has adopted AES. AES provides key lengths for 128, 192, and 256 bits.

AES supports Cipher Blocks Chaining (CBC), which circumvents one of the problems with block algorithms in that two equal plain-text blocks will generate the same two equal ciphertext blocks. With CBC, the key is applied to Plain(1) to get Cipher(1). Then, Cipher(1) is used *as the key* against Plain(2) to get Cipher(2), which is used as the key against Plain(3) to get Cipher(3), continuing on until the end.

AES is designed to be more secure than DES through the following enhancements:

- A larger key size.
- Ensures that the only known approach to decrypt a message is for an intruder to try every possible key.
- Has a variable key length; the algorithm can specify a 128-bit key (the default), a 192-bit key, or a 256-bit key.

NOTE AES is supported in Cisco IOS 12.2.13(T) and later. To enable AES, your router must support IPSec. AES cannot encrypt IPSec and IKE traffic if an acceleration card is present. This restriction will be lifted in a future release of Cisco IOS.

For more details on Cisco IOS support for AES, visit http://cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080110bb6.html.

Message Digest 5 and Secure Hash Algorithm

Several hashing algorithms are available. The two discussed here are MD5 and SHA. There is a slight, unknown difference between SHA and SHA-1. NSA released SHA and then later discovered a flaw (undisclosed). NSA fixed it, and called the new version SHA-1. In this guide, SHA refers to SHA-1 also.

Message hashing is an encryption technique that ensures that a message or data has not been tampered with or modified. MD5 message hashing is supported on Cisco IOS routers. A variable-length message is taken, the MD5 algorithm is performed (for example, the **enable secret** *password* command), and a final fixed-length hashed output message called a message digest is produced. MD5 is defined in RFC 1321.

Figure 4-6 displays the MD5 message operation.

Figure 4-6 *MD5 Operation*

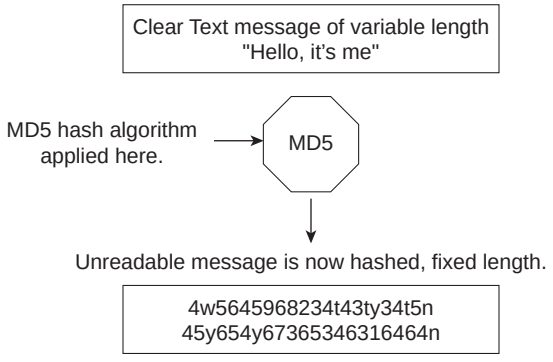


Figure 4-6 displays the simple clear-text message, "Hello, it's me," which can be of any variable length. This message is sent to the MD5 process, where the clear-text message is hashed and a fixed-length, unreadable message is produced. The data can include routing updates or username/password pairings, for example. MD5 produces a 128-bit hash output.

SHA is the newer, more secure version of MD5, and Hash-based Message Authentication (HMAC) provides further security with the inclusion of a key exchange. SHA produces a 160-bit hash output, making it even more difficult to decipher. SHA follows the same principles as MD5 and is considered more CPU-intensive.

For more details on Cisco IOS encryption capabilities, visit the following website:

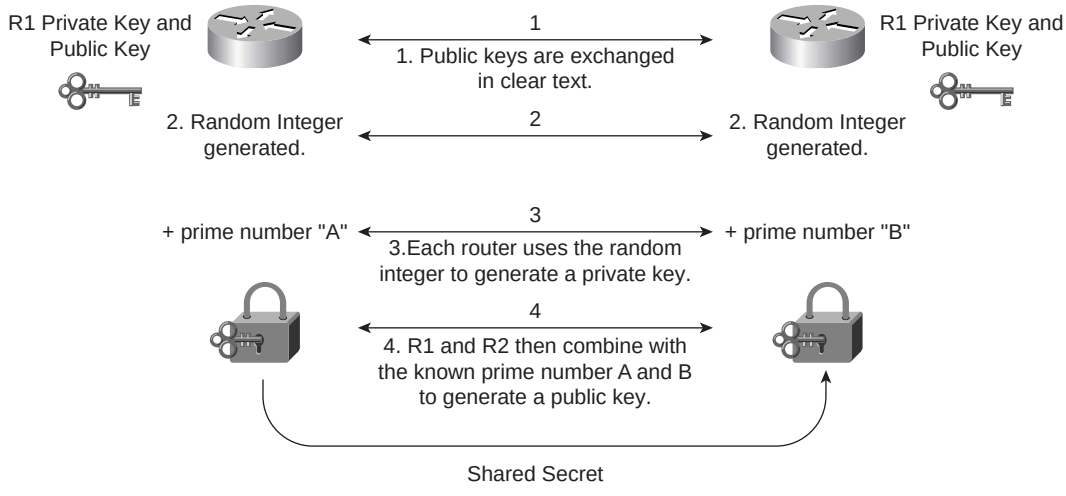
http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html

Diffie-Hellman

The Diffie-Hellman protocol allows two parties to establish a shared secret over insecure channels, such as the Internet. This protocol allows a secure shared key interchange over the public network, such as the World Wide Web, before any secure session and data transfer is initiated. Diffie-Hellman ensures that, by exchanging just the public portions of the key, both devices can generate a session and ensure that data is encrypted and decrypted by valid sources only. Only public keys (clear text) are exchanged over the public network. Using each device's public key and running the key through the Diffie-Hellmann algorithm generates a common session key. Only public keys will ever be exchanged.

Figure 4-7 displays the Diffie-Hellman exchange between Cisco routers, R1 and R2.

Figure 4-7 *Diffie-Hellman Key Exchange*



The Diffie-Hellman key exchange takes place over a public domain. With the private key kept secret, it is very difficult for an outside intruder to generate the same key, and the private key is never exchanged over the public domain, making the process very secure.

The shared prime numbers (mathematically, a prime number is any positive integer greater than 1 and divisible without a remainder only by 1 and itself) have a special relationship that makes agreeing on a shared secret possible. An analogy would be to have two milkshake blenders making a chocolate milkshake, but with one blender supplied with apples and the other with oranges. The Diffie-Hellman algorithm is the secret ingredient that, when mixed in with both blenders, produces the chocolate milkshake. Remember, it really is a superb algorithm.

NOTE RSA is another public key cryptographic algorithm (named after its inventors, Rivest, Shamir, and Adleman) with a variable key length. RSA's main weakness is that it is significantly slow to compute compared to popular secret-key algorithms, such as DES or 3DES. The Cisco IKE implementation uses a Diffie-Hellman exchange to get the secret keys. This exchange can be authenticated with RSA (or preshared keys). With the Diffie-Hellman exchange, the DES key never crosses the network, which is not the case with the RSA encryption and signing techniques. RSA is public domain like DES/3DES, and to apply RSA, you must be licensed from RSA Data Security. RSA is also approved by the U.S. government. An RSA signature is defined as the host (for example, PC or routers) public and private key, which is bound with a digital certificate. With RSA, only the public key is ever transmitted—the private key is never shared.

IP Security

IPSec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services.

–RFC 2401, "Security Architecture for the Internet Protocol"

IPSec is a defined encryption standard that encrypts the upper layers of the OSI model by adding a new predefined set of headers. IPSec is not just an encryption standard; IPSec provides a variety of other services, as discussed in this section. A number of RFCs defined IPSec.

IPSec is a mandatory requirement for IP version 6 (IPv6 is not covered in the examination). IPSec ensures that the network layer of the OSI model is secured. In TCP/IP's case, this would be the IP network layer. The two IPSec frame formats available, Authentication Header (AH) and Encapsulating Security Payload (ESP), both have protocol numbers assigned to them. They are shimmed in between IP and transport. (The protocol number says to give the datagram to AH or ESP, each of which has a next protocol number that eventually delivers the datagram to TCP or UDP or whatever else might be at the higher layer, such as OSPF.) Therefore, IPSec ensures that the data and headers above the network layer are secured.

IPSec can be configured in two protection modes, which are commonly referred to as security associations (SA). These modes provide security to a given IP connection. The modes are as follows (you have to use IPSec in tunnel mode if you want to obscure the network layer):

- **Transport mode**—Protects payload of the original IP datagram; typically used for end-to-end sessions
- **Tunnel mode**—Protects the entire IP datagram by encapsulating the entire IP datagram in a new IP datagram

An SA is required for inbound and outbound connections. In other words, IPSec is unidirectional. IKE, discussed in this chapter, allows for bidirectional SAs.

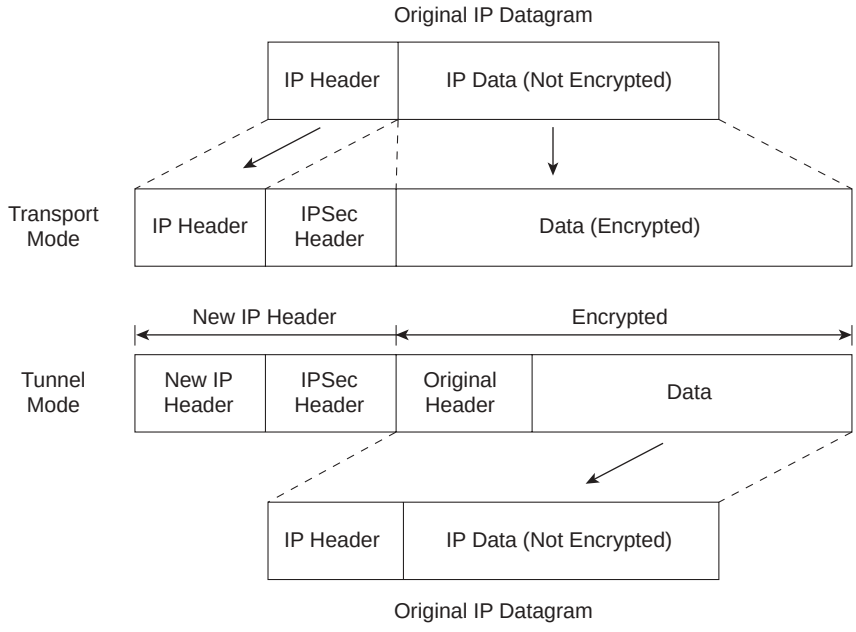
Figure 4-8 displays the extension to the current IP packet frame format for both transport and tunnel modes.

The Encapsulating Security Payload (labeled IPSec header in Figure 4-8) can be of [the] form:

- ESP
- AH

Each of these is discussed in the following sections.

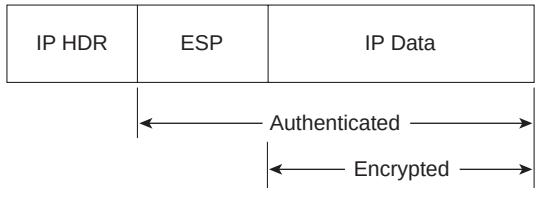
Figure 4-8 *IPSec Protection Modes*



Encapsulating Security Payload

The ESP security service is defined in RFC 2406. ESP provides a service to the IP data (payload), including upper-layer protocols such as TCP. The destination IP number is 50. The ESP header is located between the user data and original IP header, as displayed in Figure 4-9.

Figure 4-9 *ESP Header*



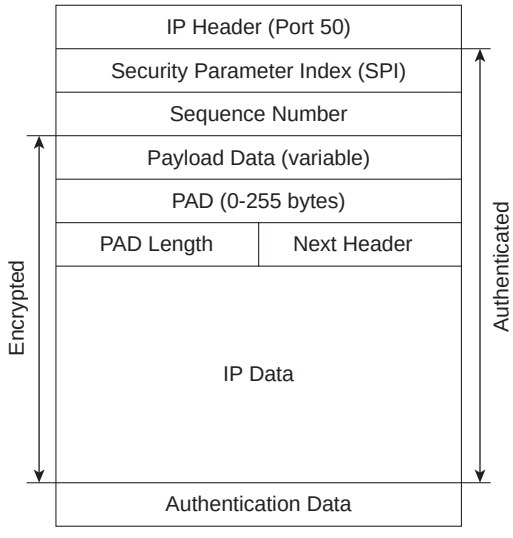
ESP does not encrypt the original IP header (when in transport mode), and encrypts only the IP data by placing a header in between the original IP header and data. ESP provides data confidentiality, data integrity, and data origin authentication. ESP also prevents replay attacks. Replay attacks can include intruders capturing a valid packet and replaying it over the network in an attempt to get a packet conversation between an illegal and legal host.

In tunnel mode ESP, the original IP datagram is placed in the encrypted portion of the Encapsulating Security Payload and that entire ESP frame is placed within a datagram that has unencrypted IP headers. The information in the unencrypted IP headers is used to route the secure datagram from origin to destination. An unencrypted IP routing header might be included between the IP header and the Encapsulating Security Payload.

ESP does not protect the IP header and cannot detect any alternations during packet delivery.

Figure 4-10 displays the frame formats when ESP is applied.

Figure 4-10 *ESP Frame Format*



The Security Parameters Index (SPI) is an arbitrary 32-bit value that, in combination with the destination IP address and security protocol (ESP), uniquely identifies the SA for this datagram.

The Sequence Number, an unsigned 32-bit field, contains a monotonically increasing counter value. It is mandatory and is always present, even if the receiver does not elect to enable the antireplay service for a specific SA. PAD or padding is used when the frame needs to meet the minimum frame size formats. The PAD Length defines the length of padding used. Padding is used for a number of reasons. For example, padding can ensure that the minimum frame size is set so that packets are not discarded because they are too small. Padding is typically all binary ones (1111. . .) or zeros (0000. . .). The sequence number ensures that no intruder or intruders can replay data transactions by using any form of attack mechanisms.

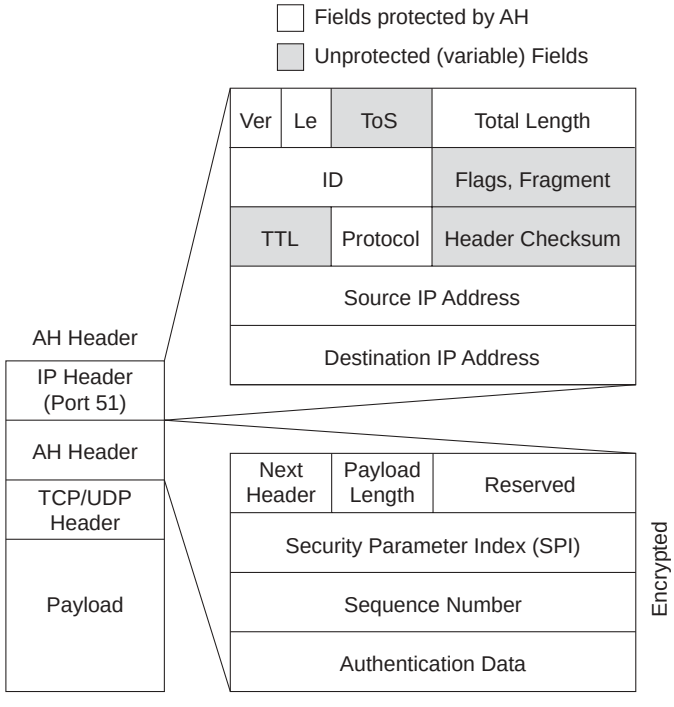
The Next Header is an 8-bit field that identifies the type of data contained in the Payload Data field. The IP Data field contains the data to be sent. The Authentication Data field is a variable-length field containing an Integrity Check Value (ICV) computed over the ESP packet minus the Authentication Data.

Authentication Header

AH is described in RFC 2402. The IP destination protocol is 51. Figure 4-11 highlights the fields in the IP datagram that are encrypted (data is not encrypted) and authenticated. Note that not all fields, such as the Time to Live fields, are encrypted.

NOTE AH provides data origin authentication and optional replay-detection services. AH doesn't provide data confidentiality (or encryption). Authentication is done by applying a one-way hash to create a message digest of the packet. Replay detection can be implemented by using the sequence number in the AH packet header.

Figure 4-11 *AH Header (Tunnel Mode)*



Following is a description of an AH packet:

- Next Header, an 8-bit field, identifies the type of the next payload after the Authentication Header.
- The Payload Length field is an 8-bit field specifying AH's length in 32-bit words (4-byte units), minus 2.
- The Reserved field is a 16-bit field reserved for future use. It *must* be set to 0.

- The SPI is an arbitrary 32-bit value that, in combination with the destination IP address and security protocol (AH), uniquely identifies the SA for this datagram.

AH can operate in transport or tunnel mode; however, unlike ESP, AH also protects fields in the outer IP header (in transport mode, this is the original IP header; in tunnel mode, this is the newly added IP header), which are normally considered nonvariable. AH ensures that if the original IP header has been altered, the packet is rejected. The protection mechanism thereby with AH is authentication only.

Before you take a look at how IPSec is enabled on Cisco routers, you need to understand how keys are exchanged between secure devices to ensure that data is not compromised. IPSec ensures that once an IPSec tunnel is created, the keys are modified so that intruders cannot replicate the keys and create IPSec tunnels to insecure locations. A recent study showed that a network of computer hackers was able to decipher a DES-encrypted message in just a day. (For details on this study please download ants.dif.um.es/~humberto/ asignaturas/v30/docs/CryptographyFAQ.pdf.)

In IPSec, key exchange is provided by Internet Key Exchange (IKE).

Internet Key Exchange

In IPSec, an SA between any two devices will contain all relevant information, such as the cryptographic algorithm in use. A cryptographic algorithm is the product of the science of cryptography. This field of science includes the exact details of encryption algorithms, digital signatures, and key agreement algorithms.

A simple two-router network requires two SAs, one for each router. (IPSec requires one SA on each router for two-way communication.)

Clearly, for a large network, this would not scale. IKE offers a scalable solution to configuration, and key exchange management.

IKE was designed to negotiate and provide authenticated keys in a secure manner. IKE has two phases. In phase I, the cryptographic operation involves the exchange of a master secret where no security is currently in place. IKE phase I is primarily concerned with establishing the protection suite for IKE messages. Phase I operations are required infrequently and can be configured in two modes of operation—aggressive mode and main mode.

Aggressive mode eliminates several steps during IKE authentication negotiation phase I between two IPSec peers. Aggressive mode is faster than main mode but not as secure. Aggressive mode is a three-way packet exchange, while main mode is a six-way packet exchange.

IKE can be configured in aggressive mode or main mode (not both). Aggressive mode is a less-intensive process that requires only three messages to establish a tunnel, versus the six messages required in main mode. Aggressive mode is typically used in remote-access VPN environments.

NOTE Cisco devices use main mode but can respond to peers using aggressive mode. Cisco IOS 12.2T and 12.3 now support configurable options as well.

IKE Phase I Message Types 1–6

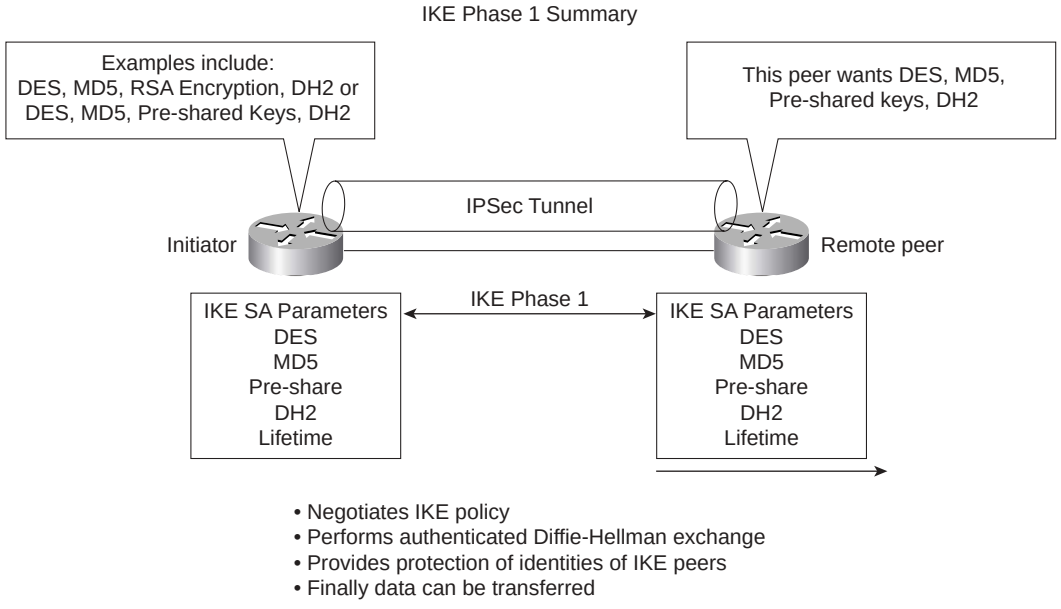
IKE phase I completes the following tasks:

- Main mode negotiates IKE policy (message types 1 and 2). Information exchanges in these message types include IP addresses. Proposals, such as Diffie-Hellman group number and encryption algorithm, are also exchanged here. All messages are carried in UDP packets with a destination UDP port number of 500. The UDP payload comprises a header, an SA payload, and one or more proposals. Message type 1 offers many proposals, and message type 2 contains a single proposal. For message type 2, it is the single proposal and transform that the responder wishes to accept.
- Performs authenticated Diffie-Hellman (DH) exchange. Message types 3 and 4 carry out the DH exchange. Message types 3 and 4 contain the key exchange payload, which is the DH public value and a random number (called a *nonce*). Message types 3 and 4 also contain the remote peer's public key hash and the hashing algorithm. A common session key created on both ends, and the remaining IKE messages exchanged from here are encrypted. If perfect forward secrecy (PFS) is enabled, another DH exchange will be completed. The public key hash and hashing algorithm are sent only if the authentication mechanism is public key encryption.
- Protects IKE peers' identities—identities are encrypted. Message types 5 and 6 are the last stage before traffic is sent over the IPSec tunnel. Message type 5 allows the responder to authenticate the initiating device. Message type 6 allows the initiator to authenticate the responder. These message types are not sent as clear text. Message types 5 and 6 will now be encrypted using the agreed-upon encryption methods established in message types 1 and 2.

After IKE phase I is completed, each peer or router has authenticated itself to the remote peer, and both have agreed on the characteristics of all the SA parameters (IKE parameters).

Figure 4-12 summarizes the key components of IKE phase I and some of the possible permutations available on Cisco IOS routers.

Figure 4-12 *IKE Phase I Summary*



The first message exchanged offers the remote router a choice of IPSec parameters, such as encryption algorithm, 3DES, MD5, and DH group number, for example. The first message's aim is to negotiate all SA policies.

In the second message (type 2), the responding device indicates which of the IPSec parameters it wants to use in the tunnel between the two devices, including the information required to generate the shared secret and provide authentication details. The final message (type 3; until now no encryption is enabled) authenticates the initiator.

After IKE phase I is complete, IKE phase II is initiated. As discussed in the following section, IKE phase II negotiation has three message types.

IKE Phase II Message Types 1–3

IKE phase II negotiates the SA and the keys that will be used to protect the user data. IKE phase II messages occur more frequently, typically every few minutes, whereas IKE phase I messages might occur once a day. On most Cisco IOS devices, the timeout is 1 hour.

IP datagrams that exchange IKE messages use UDP (connectionless) destination port 500.

Phase II negotiations occur in a mode called Oakley quick mode and have three different message exchanges. Quick mode can be the following:

- **Without key exchange**—No PFS is enabled.
- **With key exchange**—When PFS is enabled, the DH algorithm is run once more to generate the shared secret.

Message type 1 allows the initiator to authenticate itself, and selects a random (nonce) number and proposes an SA to the remote peer. Additionally, a public key is provided (can be different than a key exchanged in IKE phase I). IKE phase II message type 2 allows the responding peer to generate the hash. Message type 2 allows the responder to authenticate itself, and selects a random number and accepts the SA offered by the initiating IPSec peer. A hash is intended as a collision-resistant function, as required for the hashing of information prior to application of a signature function.

IKE message type 3 acknowledges information sent from quick mode message type 2 so that the phase II tunnel can be established.

NOTE Perfect forward secrecy can be requested as part of the IKE SA. PFS ensures that a given IPSec SA key was not derived from any other secret. In other words, if someone were to break a key or get the key used between two peers, PFS ensures that the attacker would not be able to derive any other key. If PFS was not enabled, someone could hypothetically break the IKE SA secret key, copy all the IPSec-protected data, and use knowledge of the IKE SA secret to compromise the IPSec SA's setup by this IKE SA. With PFS, breaking IKE would not give an attacker immediate access to IPSec. The attacker would have to break each IPSec SA individually.

Changing the secret key being used for encryption after some period of time (or after a specified number of bytes have been encrypted) is a good idea. Changing keys makes it more difficult for an attacker to derive the key or the newly created key.

Now that all the required data has been exchanged, the initiating IPSec router, or peer, sends a final phase I message with the hash of the two random numbers generated and the message ID. The responder needs to verify the hash before data can be protected.

Figure 4-13 summarizes the key components of IKE phase II.

Figure 4-13 *IKE Phase II Summary*

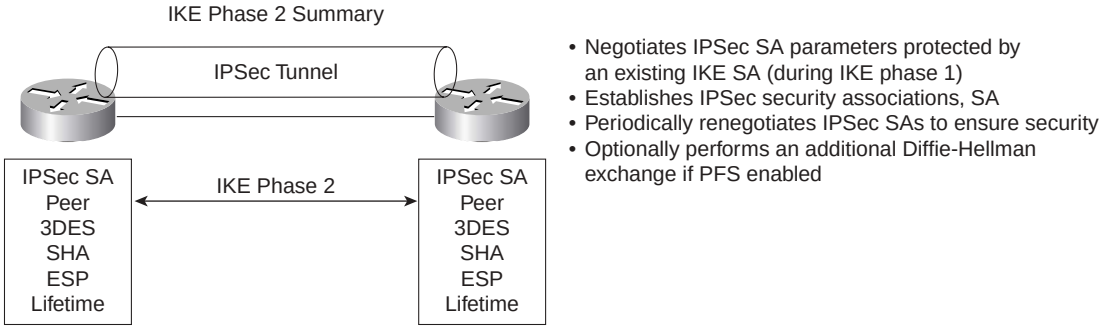


Figure 4-14 displays a typical IKE phase I/II completion.

Figure 4-14 *IKE Phase I/II*

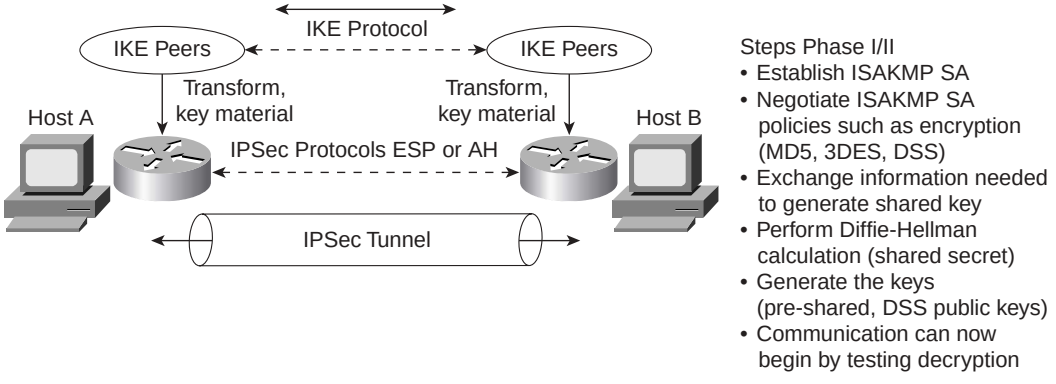


Table 4-5 summarizes the key components of IKE phases I and II.

Table 4-5 *IKE Phases I and II*

Phase	Tasks
IKE phase I	Authenticates IPSec peers Negotiates matching policy to protect IKE exchange Exchanges keys via Diffie-Hellman Establishes the IKE SA
IKE phase II	Negotiates IPSec SA parameters by using an existing IKE SA Establishes IPSec security parameters Periodically renegotiates IPSec SAs to ensure security and that no intruders have discovered sensitive data Can also perform optional additional Diffie-Hellman exchange

IKE requires that all information exchanges be encrypted and authenticated. In addition, IKE is designed to prevent the following attacks:

- **Denial of service**—When messages are constructed with unique cookies that can be used to identify and reject invalid messages.
- **Man in the middle**—Prevents the intruder from modifying messages and reflecting them back to the source or replaying old messages.

NOTE Access control lists determine what traffic to encrypt. For example, you can specify that certain networks are to be encrypted and other networks are not. The **permit** statement encrypts data, and the **deny** statement (implicit) in an ACL does not send traffic encrypted. An ACL applied to IPSec configuration parameters does not stop IP routing on a Cisco IOS router.

Table 4-6 summarizes the key terms and concepts used in IPSec terminology.

Table 4-6 *Summary of IPSec Terms and Concepts*

Term	Meaning
Internet Key Exchange (IKE)	Provides utility services for IPSec, such as authentication of peers, negotiation of IPSec SAs, and encryption algorithms. IKE operates over the assigned UDP port 500.
Security associations (SAs)	Connections between IPSec peers. Each IPSec peer maintains an SA database containing parameters, such as peer addresses, security protocols, and a Security Parameter Index (SPI). An SA is unidirectional, and two SAs are required to form a complete tunnel.
Data Encryption Standard (DES)	Encrypts and decrypts data. It is not considered a strong algorithm and was replaced by 3DES. DES supports only a 56-bit key. 3DES supports three 56-bit keys, or a 168-bit key.
Triple DES (3DES)	A variant of DES that is a much stronger encryption method and uses a 168-bit key.
Advanced Encryption Standard (AES)	A new standard that supports 128-, 192-, and 256-bit key lengths; considered a replacement for DES.
Message Digest version 5 (MD5)	A hash algorithm (128 bit) that takes an input message (of variable length) and produces a fixed-length output message. IKE uses MD5 for authentication purposes.
Secure Hash Algorithm (SHA-1)	A hash algorithm (160 bit) that signs and authenticates data. It is stronger than MD5 but more CPU-intensive and, therefore, slower.
RSA signatures	RSA is a public-key encryption system used for authentication. Users are assigned both private and public keys. The private key is not available to the public and decrypts messages created with the public key. To obtain a legitimate signature, you need to have a Certificate Authority sign your public key, making it a certificate.

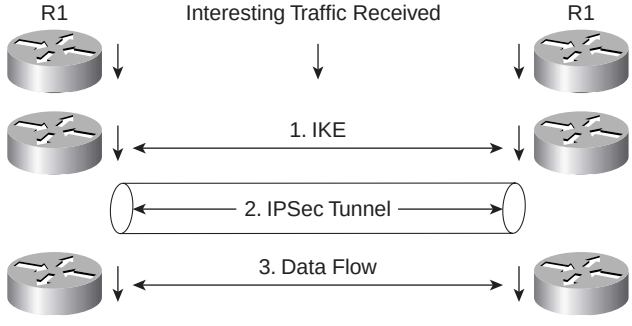
continues

Table 4-6 *Summary of IPSec Terms and Concepts (Continued)*

Term	Meaning
Certificate Authority (CA)	A trusted third party whose purpose is to sign certificates for network entities that it has authenticated.
Diffie-Hellman (DH)	Algorithm that is used to initiate and secure the session between two hosts, such as routers.
Encapsulating Security Payload (ESP)	ESP (transport mode) does not encrypt the original IP header, and only encrypts the IP data by placing a header in between the original IP header and data. ESP (tunnel and transport modes) provides data confidentiality, data integrity, and data origin authentication.

Figure 4-15 displays the flow chart before any data can be transferred between two IPSec peers.

Figure 4-15 *IPSec Flow*



In Figure 4-15, interesting traffic (or traffic from an end user, for example, defined in the ACLs) triggers IKE phases I and II followed by the establishment of the IPSec tunnel. After the IPSec tunnel is established, the data can be transferred. After the data is transferred, the IPSec tunnel is closed. You can tunnel any form of data across the IPSec tunnel, such as IP, Novel IPX, or AppleTalk.

Cisco IOS IPSec Configuration

To enable IPSec between Cisco IOS routers, the following steps are required:

Step 1 Enable Internet Security Association Key Management Protocol (ISAKMP) with the IOS command **crypto isakmp enable**.

This step globally enables or disables ISAKMP at your peer router.

ISAKMP is enabled by default (ACLs define what interesting traffic will be encrypted using defined ACLs).

Step 2 Define an ISAKMP policy, a set of parameters used during ISAKMP negotiation:

crypto isakmp policy *priority*

You will enter **config-isakmp** command mode.

Options available include the following:

```
Router(config-isakmp)#?
authentication {rsa-sig | rsa-encr | pre-share}
  default
  encryption {des} {3des} {aes}
  exit
  group 1 2 5
  hash {md5 | sha}
  lifetime seconds
  no
```

This command invokes the ISAKMP policy configuration (**config-isakmp**) command mode. While in ISAKMP policy configuration command mode, the following commands are available to specify the parameters in the policy:

- **encryption** (IKE policy)—The default is 56-bit DES-CBC. To specify the encryption algorithm within an IKE policy, options are **des, 3des**, or **aes**.
- **hash** (IKE policy)—The default is SHA-1. To specify the hash algorithm within an IKE policy, options are **sha**, which specifies SHA-1 (HMAC variant) as the hash algorithm, or **md5**, which specifies MD5 (HMAC variant) as the hash algorithm. Hashed Message Authentication Code (HMAC) uses keyed message digest functions to authenticate a message. The technique used in IPSec is defined in RFC 2104.
- **authentication** (IKE policy)—The default is RSA signatures. To specify the authentication method within an IKE policy, options are **rsa-sig**, which specifies RSA signatures as the authentication method; **rsa-encr**, which specifies RSA encryption as the authentication method; or **pre-share**, which specifies preshared keys as the authentication method.
- **group** {**1** | **2**}—The default is 768-bit Diffie-Hellman. To specify the DH group identifier within an IKE policy, options are **1**, which specifies the 768-bit DH group, or **2**, which specifies the 1024-bit DH group. DH group 5 is also available (1536-bit).
- **lifetime** (IKE policy)—The default is 86,400 seconds (once a day). To specify the lifetime of an IKE SA, use the ISAKMP lifetime policy configuration command. If two IPSec peers share different lifetime values, the chosen value is the shortest lifetime.

Step 3 Set the ISAKMP identity (can be IP address or host name based):

```
crypto isakmp identity {address | hostname}
```

Step 4 Define transform sets (Phase II).

A transform set represents a combination of security protocols and algorithms. During the IPSec SA negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

To define a transform set, use the following commands, starting in global configuration mode:

```
crypto ipsec transform-set
    transform-set-name transform1 [transform2 [transform3]]
```

This command puts you into the crypto transform configuration mode. Then, define the mode associated with the transform set:

```
Router(cfg-crypto-tran)# mode [tunnel | transport]
```

The default is **tunnel**.

Step 5 Define crypto maps, which tie the IPSec policies and SAs together:

```
crypto map name seq method [dynamic dynamic-map-name]
```

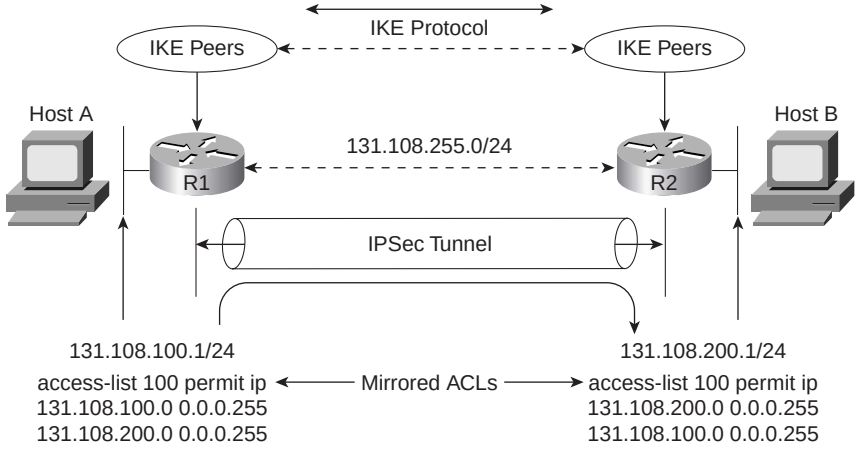
NOTE Crypto map entries created for IPSec pull together the various parts used to set up IPSec SAs, including the following:

- Which traffic should be protected by IPSec (per a crypto ACL).
- The granularity of the flow to be protected by a set of SAs.
- Where IPSec-protected traffic should be sent (who the remote IPSec peer is).
- The local address to be used for the IPSec traffic.
- What IPSec security should be applied to this traffic.
- Whether SAs are manually established or are established through IKE.
- Other parameters that might be necessary to define an IPSec SA.

A dynamic crypto map entry is essentially a crypto map entry without all the parameters configured. It acts as a policy template where the missing parameters are later dynamically configured (as the result of an IPSec negotiation) to match a remote peer's requirements. This allows remote peers to exchange IPSec traffic with the router even if the router does not have a crypto map entry specifically configured to meet all the remote peer's requirements. Dynamic crypto maps are typically used to ensure security between a remote access IPSec client and Cisco IOS router, for example.

The following typical configuration scenario illustrates the IPSec configuration tasks with a two-router network. Figure 4-16 displays two routers configured with the networks 131.108.100.0/24 and 131.108.200.0/24, respectively. Suppose that the Frame Relay cloud is an unsecured network and you want to enable IPSec between the two routers, R1 and R2.

Figure 4-16 *Typical IPSec Topology Between Two Remote Routers*



The network administrator has decided to define the following ISAKMP parameters:

- MD5.
- Authentication will be via preshared keys.
- The shared key phrase is CCIE.
- IPSec mode is transport mode.

To start, configure IKE on Router R1. Example 4-11 displays the IKE configuration on R1. Remember that IKE policies define a set of parameters to be used during IKE negotiation. (Note that in Cisco IOS 12.2T and later, the commands have different options.)

Example 4-11 *R1 IKE Configuration*

```
crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key CCIE address 131.108.255.2
```

R1 is configured to use the MD5 algorithm, and the authentication method is defined as preshared. The preshared key value (password) is CCIE, and the remote IPSec peer's address is 131.108.255.2 (R2 serial link to R1 in Figure 4-16).

Preshared Keys Versus Manual Keys

The example shown here is an example of preshared keys whereby IKE is used to negotiate all SA parameters. You can also define IPSec not to use IKE, and this is referred to as *manual IPSec* or *manual keys.* Cisco strongly recommends that you use IKE with preshared keys or RSA signatures, because it is very difficult to ensure that all SA parameters are matching between remote peers. The Diffie-Hellman algorithm is a more secure method when generating secret keys between peers. Manual keys are vulnerable to intruders and unauthorized sources that gain entry to Cisco configuration files. Another major disadvantage of manual keys is that the IOS **crypto map** command used to establish SAs does not expire.

Following the IKE configuration, you can configure IPSec parameters. Example 4-12 enables the IPSec configuration parameters.

Example 4-12 *IPSec Configuration*

```
crypto ipsec transform-set anyname esp-des esp-sha-hmac  mode transport
!
crypto map anyname1 1 ipsec-isakmp
 set peer 131.108.255.2
 set security-association lifetime seconds 900
 set transform-set anyname
 match address 100
!
access-list 100 permit ip 131.108.100.0 0.0.0.255 131.108.200.0 0.0.0.255
```

The transform-set command defines an acceptable combination of security protocols and algorithms. This example applies ESP-DES (ESP with the 56-bit DES encryption algorithm) and ESP with the SHA (HMAC variant) authentication algorithm. (Note that you can also apply 3DES or AES to provide even stronger encryption methods.) The next-hop peer address is defined, and access-list 100 defines what traffic will be encrypted. In Figure 4-16, only IP traffic sourced from 131.108.100.0 destined for 131.108.200.0/24 is sent across the IPSec tunnel.

Example 4-13 displays the configuration on R2.

Example 4-13 *R2 IKE and IPSec Configuration*

```
! IKE configuration
crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key CCIE address 131.108.255.1
!
crypto ipsec transform-set anyname esp-des esp-sha-hmac
 mode transport
```

Example 4-13 *R2 IKE and IPSec Configuration (Continued)*

```
!IPSec configuration
crypto map anyname1 1 ipsec-isakmp
 set peer 131.108.255.1
 set security-association lifetime seconds  900
 set transform-set anyname
 match address 100
!Access list defines traffic to be encrypted or interesting traffic
access-list 100 permit ip 131.108.200.0 0.0.0.255 131.108.100.0 0.0.0.255
```

Notice that the routers have mirrored ACLs. This ensures that when encrypted data is received from a source, such as R1, the corresponding IPSec peer router, R2, enables encryption in the reverse direction. For example, when traffic from the network 131.108.100.0/24 residing on Router R1 is sent across, destined for R2's Ethernet network, the IP subnet 131.108.200.0/24, R2 must have a corresponding ACL permitting traffic from the locally connected Ethernet segment, 131.108.200.0/24, to the remote network, the IP subnet on R1, 131.108.100.0/24. This is referred to as mirrored ACLs.

Example 4-13 configures R2 to peer to R1 and only encrypt traffic sourced from 131.108.200.0/24 destined for R1's Ethernet network, 131.108.100.0/24. The crypto predefined map name is anyname1.

Finally, you must apply a previously defined crypto map in Example 4-12. The defined crypto map name is anyname1 in this example, so apply that configuration to the interface. The IOS command that applies the crypto map to an interface is as follows (in config-interface mode):

```
crypto map anyname1
```

Example 4-14 assigns the serial links on R1 and R2 to the crypto map name anyname1 and assigns the crypto map to interface Serial 0/0 on R1/R2.

Example 4-14 *Serial Links and* **crypto map** *on R1/R2*

```
Hostname R1
!
interface Serial0/0
 ip address 131.108.255.1 255.255.255.252
 crypto map anyname1
!
Hostname R2
!
interface Serial0/0
 ip address 131.108.255.2 255.255.255.252
 crypto map anyname1
```

To display the status of all crypto engine active connections, use the IOS command **show crypto engine connections active**.

Example 4-15 displays the current active crypto engines on R1.

Example 4-15 **show crypto engine connections active** *on R1*

```
R1#show crypto engine connections active
 ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
 1 Serial0/0       131.108.255.1   set    HMAC_MD5+DES_56_CB        5        5
```

R1 has an IPSec peer connection to R2, through the Serial0/0 interface (131.108.255.1). The algorithm in use is defined and displayed, as well.

To view the crypto map configuration from the PRIV EXEC, use the IOS command **show crypto map**.

Example 4-16 displays the configuration present on R1.

Example 4-16 **show crypto map** *on R1*

```
R1#show crypto map
Crypto Map "anyname1" 1 ipsec-isakmp
 Peer = 131.108.255.2
 Extended IP access list 100
access-list 100 permit ip 131.108.100.0 0.0.0.255 131.108.200.0 0.0.0.255
 Current peer: 131.108.255.2
 Security association lifetime: 4608000 kilobytes/180 seconds
 PFS (Y/N): N
 Transform sets={ anyname, }
 Interfaces using crypto map anyname1:
 Serial0/0
```

Example 4-16 displays the fact that the crypto map named "anyname1" is peered to a remote router, 131.108.255.2, and the access-list 100 defines what traffic will be encrypted across the tunnel.

IPSec is a large field, and to define every possible scenario would require a book in itself. What is presented in this guide is a conceptual overview of IPSec and a common configuration example. For more extensive details, visit:

> http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fipsenc/index.htm

For the CCIE Security written exam, expect to see scenarios of the variant presented in Figure 4-16 and questions on terminology and the main characteristics of IPSec.

NOTE IPSec can also be supported over the Cisco software tunnel interface. Typically, the tunnel (IP tunnel; GRE, for example) can be configured to carry non-IP traffic by defining a crypto map to the tunnel interface and a crypto control list.

Table 4-7 defines some key IPSec configuration **show** and **debug** commands available on Cisco IOS routers.

Table 4-7 *IOS IPSec Configuration, Show, and Debug Commands*

Command	Description
crypto map *map-name seq-num* **ipsec-isakmp** [**dynamic** *dynamic-map-name*] [**discover**]	Creates a crypto map entry.
crypto ipsec transform-set *transform-set-name transform1* [*transform2* [*transform3*]]	Defines a transform set, an acceptable combination of security protocols and algorithms. This is IKE phase II.
match address [*access-list-id* | *name*]	This command is required for all static crypto map entries. Defines interesting traffic.
crypto dynamic-map *dynamic-map-name dynamic-seq-num*	Use dynamic crypto maps to create policy templates that can be used when processing negotiation requests for new SAs from a remote IPSec peer, even if you do not know all the crypto map parameters.
crypto ca authenticate *name*	This command is required when you initially configure CA support at your router.
crypto ca identity *name*	Use this command to declare a CA.
crypto isakmp enable	Globally enables IKE at your local router.
Show crypto engine connection active	Displays phase I and II SA and traffic sent.
authentication {**rsa-sig** | **rsa-encr** | **pre-share**}	Specifies the authentication method within an IKE policy.
show crypto ipsec sa	Displays the settings used by current SAs to declare a CA.
show crypto map	Displays the crypto map configuration.
show crypto isakmp sa	Displays all current IKE SAs at a peer.
debug crypto engine	Displays debug messages about crypto engines, which perform encryption and decryption.
debug crypto ipsec	Displays IPSec events.
debug crypto pki messages	Displays debug messages for the details of the interaction (message dump) between the CA and the router.
debug crypto isakmp	Enables global IKE debugging.

NOTE A number of PC-based applications are available to the public that allow application layer encryptions.

An excellent e-mail encryption application is a product called Pretty Good Privacy (PGP). Designed and freely available on the Internet (http://www.pgp.com), PGP allows users to authenticate files and e-mail text, allowing only the intended recipient to decrypt the message. Users who send and receive encrypted data exchange keys. With encrypted data, the remote user's key is used to encrypt clear-text data or files. This ensures that the data is authenticated and not forged. Also check out http://www.gnupg.org for a free version of PGP.

Microsoft Outlook 2000 supports PGP and allows the client to encrypt and decrypt data using the preshared public keys.

Certificate Enrollment Protocol

CEP is a protocol jointly developed by Cisco and VeriSign, Inc. CEP is an early implementation of Certificate Request Syntax (CRS), a proposed standard to the IETF. CEP specifies how a device communicates with the CA, how to retrieve the CA's public key, and how to enroll a device with the CA. CEP uses Public Key Cryptography Standards (PKCS).

CEP uses HTTP as a transport mechanism and uses the same TCP port (80) used by HTTP.

NOTE You can find more details on CEP at http://www.cisco.com/warp/public/cc/pd/sqsw/tech/scep_wp.htm. For the CCIE Security lab, the candidate is expected to be able to use common IOS commands such as **crypto ca trustpoint** and know how to enroll certificates**.**

To declare the CA that a Cisco IOS router should use, use the **crypto ca identity** *name* command in global configuration mode. The CA might require a particular name, such as the domain name.

Finally, to cover the exam blueprint, this chapter closes with a short explanation of some of the security protocols used in today's networks to ensure security over wireless connections.

Extensible Authentication Protocol, Protected EAP, and Temporal Key Integrity Protocol

Extensible Authentication Protocol (EAP) enables the dynamic selection of the authentication mechanism at authentication time based on information transmitted in the Access-Request (that is, via RADIUS). PPP also supports EAP during the link establishment phase.

EAP allows the authenticator to request more information before determining the specific authentication mechanism.

A proposal jointly submitted to the IEEE by Cisco Systems, Microsoft, and various other organizations introduced Protected EAP (PEAP), an EAP to provide enhanced functionality and security features to wireless networks. PEAP is today's preferred authentication mechanism in wireless networks.

PEAP provides the following security benefits:

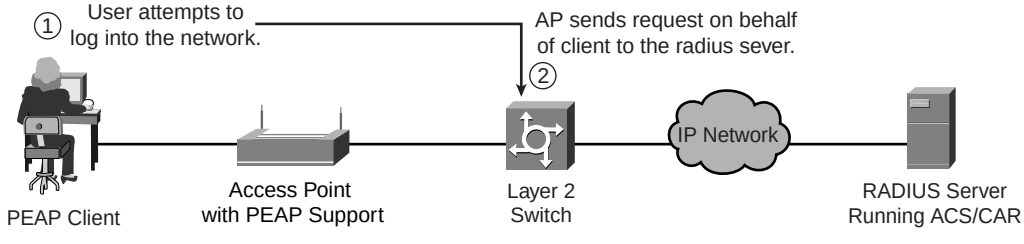
- Relies on Transport Layer Security (TLS) to allow nonencrypted authentication types such as EAP-Generic Token Card (GTC) and One Time Password (OTP) support.
- Uses server-side PKI-based digital certification authentication.
- Allows authentication to an extended suite of directories, including Lightweight Directory Access Protocol (LDAP), Novell NDS, and OTP databases.
- Uses TLS to encrypt all user-sensitive authentication information.
- Supports password change at expiration.
- Does not expose the logon username in the EAP identity response.
- Is not vulnerable to dictionary attacks.

That functionality is provided to wireless client adapters, which may support different authentication types, to communicate with different back-end servers such as RADIUS servers. EAP can be used with wired networks as well.

Microsoft Windows XP supports an extension to EAP, namely Extensible Authentication Protocol Transport Layer Security (EAP-TLS). Hence, a number of options are available to end users so that authentication may be completed securely over a wireless network. Recently Microsoft has added support for EAP-TLS and PEAP to several of its operating systems.

Figure 4-17 displays a typical wireless network in which a user labeled PEAP Client is required to authenticate to either a Cisco Secure ACS or the Cisco Access Registrar. The Cisco Access Registrar is based on a client/server model, which supports AAA. The client passes user information on to the RADIUS server and acts on the response it receives. The server, on the other hand, is responsible for receiving user access requests, authenticating and authorizing users, and returning all of the necessary configuration information the client can then pass on to the user.

Figure 4-17 *PEAP Sample Deployment*



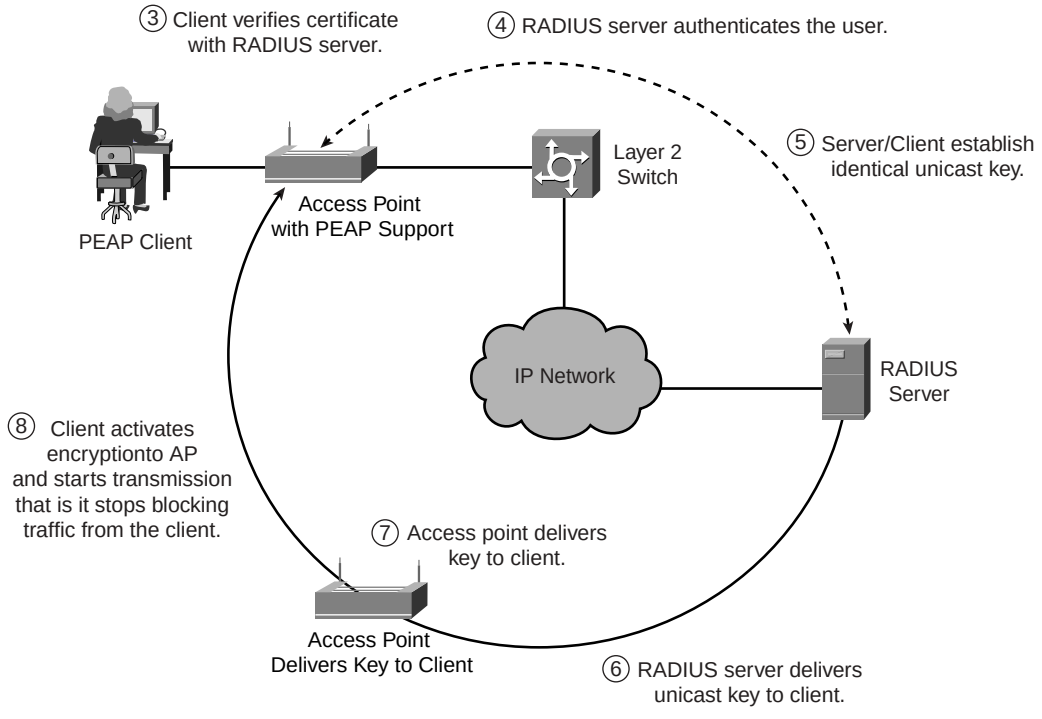
NOTE There have been some additions to EAP to help alleviate some of the weaknesses in other technologies, such as wireless networks.

PEAP is an EAP authentication type that provides mutual authentication of the client and RADIUS server via the access point. PEAP mutual authentication has two parts. In the first part, the server certificate is verified by the client; in the second part, the user is authenticated using the information protected in the TLS tunnel. Additionally, EAP-TLS provides mutual authentication using digital certificates on both the client and the server.

Figure 4-17 displays a Windows XP client trying to associate with a wireless access point—the first step the client performs. The second step is that the access point in Figure 4-17 blocks the request because the client has not been verified by the RADIUS server.

Figure 4-18 displays the next six steps in the PEAP authentication process.

Figure 4-18 *PEAP Authentication Process*



The eight-step process in Figure 4-17 and Figure 4-18 starts with the clients' attempt to authenticate with the RADIUS server. Once a valid username and password are exchanged, the RADIUS server and client establish a common key used to send and receive data over a secured wireless connection.

NOTE Cisco Secure ACS or the Cisco Access Registrar can be used for a combined LEAP and EAP-TLS protocol deployment in an enterprise network. Cisco LEAP is an 802.1X authentication type for wireless LANs that supports mutual authentication between the client and a RADIUS server.

EAP allows the administrator access to a number of password authentication mechanisms, including one-time passwords, public key authentication using smart cards, certificates, and others.

EAP is discussed in RFC 2284, "PPP Extensible Authentication Protocol" (March 1998).

RFC 2284 can be found at http://www.ietf.org/rfc/rfc2284.txt

The Cisco Wireless Security Suite supports IEEE 802.1X authentication and numerous EAP types, including EAP Cisco Wireless (LEAP); EAP-Transport Layer Security (EAP-TLS), and types that operate over EAP-TLS, such as PEAP, EAP-Tunneled TLS (EAP-TTLS), and EAP-Subscriber Identity Module (EAP-SIM). The suite also supports a pre-standard version of Temporal Key Integrity Protocol (TKIP).

TKIP defends against an attack on Wired Equivalent Privacy (WEP) in which the intruder uses an unencrypted segment called the initialization vector (IV) in encrypted packets to calculate the WEP key. TKIP removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs. TKIP protects both unicast and broadcast WEP keys.

TKIP provides enhancements to 128-bit encryption. One such enhancement is *per-packet key hashing*, where the encryption key is changed on each packet. This feature helps combat a common WLAN hacking tool called AirSnort, freely available at http://airsnort.shmoo.com/, which takes advantage of a weakness in WEP encryption when static WEP keys are not changed during a session. It must be pointed out, however, that even with TKIP, the session key needs to be changed before the IV space recycles at 16.7 million packets.

Another important new security advance with TKIP is Message Integrity Check (MIC). With MIC, a digital signature is included with every frame sent, neutralizing the man-in-the-middle attack by hackers who can capture a wireless packet, modify it, and resend it.

TKIP and MIC are easily deployed on an access point. The following list details the simple three-step IOS configuration process:

Step 1 Enter global configuration mode:

```
configuration terminal
```

Step 2 Enter interface configuration mode for the radio interface:

```
interface dot11radio 0
```

Step 3 Enable WEP, MIC, and TKIP:

```
encryption [vlan vlan-id] mode wep {optional [key-hash] ¦ mandatory [mic]
    [key-hash]}
```

Virtual Private Dial-Up Networks (VPDN)

A VPDN is a network that extends remote access dialup clients to a private network. VPDN tunnels use either Layer 2 forwarding (L2F) or Layer 2 Tunnel Protocol (L2TP).

Cisco introduced L2F in RFC 2341. It is also used to forward PPP sessions for Multichassis Multilink PPP.

L2TP, introduced in RFC 2661, combines the best of the Cisco L2F protocol and Microsoft Point-to-Point Tunneling Protocol (PPTP). Moreover, L2F supports only dial-in VPDN, while L2TP supports both dial-in and dial-out VPDN.

Both protocols use UDP port 1701 to build a tunnel through an IP network to forward link-layer frames.

For L2F, the setup for tunneling a PPP session consists of two steps:

Step 1 Establish a tunnel between the NAS and the home gateway (HWY). The HWY is a Cisco router or access server (for example, an AS5300) that terminates VPDN tunnels and PPP sessions. This phase takes place only when no active tunnel exists between both devices.

Step 2 Establish a session between the NAS and the home gateway.

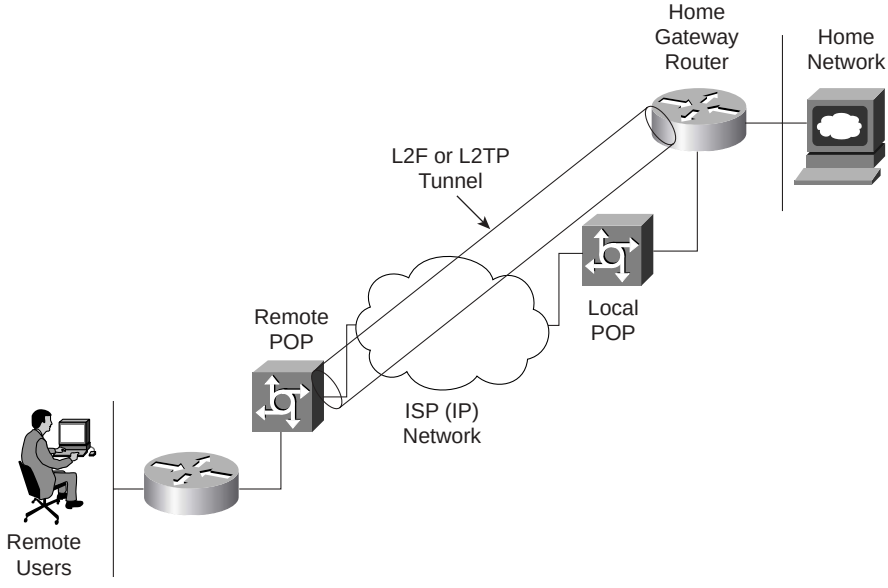
For L2TP, the setup for tunneling a PPP session consists of two steps:

Step 1 Establish a tunnel between the L2TP access concentrator (LAC) and the L2TP network server (LNS). The LAC acts as one side of the L2TP tunnel endpoint and has a peer to the LNS. This phase takes place only when no active tunnel exists between both devices.

Step 2 Establish a session between the LAC and the LNS.

Figure 4-19 displays the tunnel termination points between a remote point of presence (POP) (typically an ISP router) and the home gateway router.

Figure 4-19 *L2F or L2TP Tunnel Termination*



The remote POP accepts frames encapsulated in L2F or L2TP and forwarded over the tunnel.

The LAC and LNS are hardware devices, such as Cisco's AS 5300 series router platform. The LAC's function is to sit between the LNS and the remote system and forward packets to and from each device. The LNS logically terminates the PPP connection.

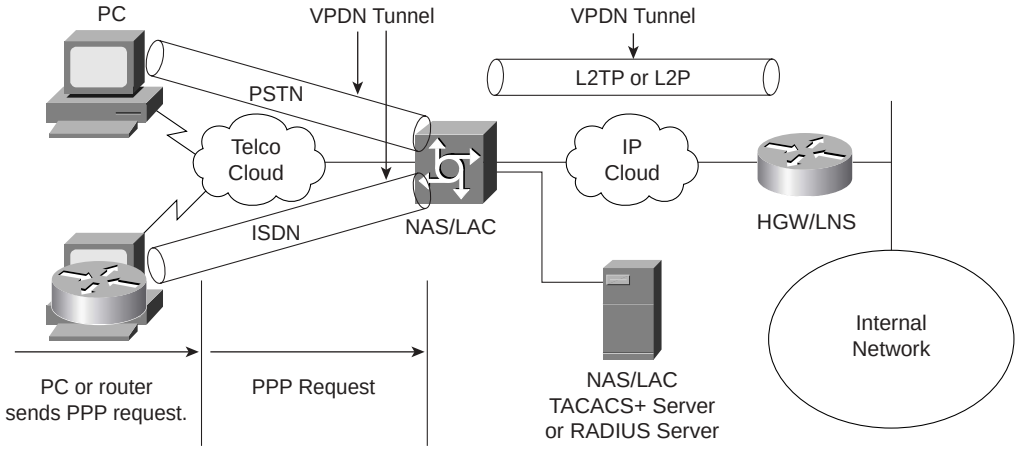
VPDNs are implemented so that users connected through ISPs in any part of the world can take advantage of the connection to the ISP and tunnel the company's remote access traffic through the ISP network.

VPDNs include the following benefits:

- Access to the corporate network from a remote location.
- Offload remote access services to the ISP, which already has the infrastructure place.
- End system transparency because the remote user does not require any hardware or software to use VPDN. Cisco IOS routers performs all the requirements.
- Allows for accounting, which is sent from the home gateway router.

Figure 4-20 displays a typical VPDN scenario where a PC or router dials the NAS/LAC to request a VPDN connection to the private network.

Figure 4-20 *VPDN Network Scenario*



To implement the VPDN configuration, you need the following:

- A Cisco router or access server for client access (NAS/LAC) and a Cisco router for network access (HGW/LNS) with IP connectivity between them.
- Host names of the routers or local names to use on the VPDN groups.
- A tunneling protocol, either the L2TP or L2F Protocol. L2TP is an industry standard, and L2F is a Cisco-proprietary protocol.
- A password for the routers to authenticate the tunnel.
- A tunneling criteria, either domain name or Dialed Number Identification Service (DNIS).
- Username and password for the user (client dialing in).
- IP addresses and keys for your TACACS+ servers.

A VPDN connection between a remote user (router or through PSTN) and the corporate LAN is accomplished in the following steps:

Step 1 The remote user initiates a PPP connection to the ISP using the analog telephone system or ISDN.

Step 2 The ISP's NAS accepts the connection.

Step 3 The ISP NAS authenticates the end user with CHAP or PAP. The username determines whether the user is a VPDN client. If the user is not a VPDN client, the client accesses the Internet or other contacted service.

Step 4 The tunnel endpoints—the NAS and the home gateway—authenticate each other before any sessions are attempted within a tunnel.

Step 5 If no L2F tunnel exists between the NAS and the remote users' home gateway, a tunnel is created. Then, an unused slot within the tunnel is allocated.

Step 6 The home gateway accepts or rejects the connection. Initial setup can include authentication information required to allow the home gateway to authenticate the user.

Step 7 The home gateway sets up a virtual interface. Link-level frames can now pass through this virtual interface through the L2F tunnel.

VPDN Configuration Task List

To configure VPDNs on the home gateway router, complete the following steps:

Step 1 Create a virtual template interface, and enter the interface configuration mode:

```
interface virtual-template number
```

Step 2 Identify the virtual template interface type and number on the LAN:

```
ip unnumbered interface number
```

Step 3 Enable PPP encapsulation on the virtual template interface:

```
encapsulation ppp
```

Step 4 Enable PPP authentication on the virtual template interface:

```
ppp authentication {chap | ppp}
```

Step 5 Enable the global configuration command to allow virtual private networking on the NAS and home gateway routers:

```
vpdn enable
```

Step 6 Specify the remote host (the NAS), the local name (the home gateway) to use for authenticating, and the virtual template to use:

Home gateway router:

```
vpdn incoming nas-name hgw-name virtual-template number
```

NAS configuration:

```
vpdn outgoing domain-name NAS-nameip ip ip-address
```

NOTE You can also enable the NAS to authenticate users via TACACS+ or RADIUS using AAA commands.

A typical configuration file on a UNIX server has a configuration similar to the following configuration:

```
LAC Radius Configuration - Sample
Sanjose.cisco.com   Password = "cisco"
Service-Type = Outbound-User,
cisco-avpair = "vpdn:tunnel-id=DEFGH",
cisco-avpair = "vpdn:tunnel-type=l2tp",
cisco-avpair = "vpdn:ip-addresses=10.31.1.9",
cisco-avpair = "vpdn:l2tp-tunnel-password=ABCDE"
```

The configuration on the LAC defines the specific av-pairs, namely the tunnel-id, tunnel-type, ip-address, and l2tp password.

Example 4-17 displays a typical NAS/LAC configuration using TACACS+.

Example 4-17 *Sample NAS/LAC Configuration*

```
hostname NAS-LAC
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authentication ppp default if-needed group tacacs+
aaa authorization network default group tacacs+
enable password cciesarecool
!
username Melanie password 0 verysecretpassword
!
vpdn enable
!
interface Ethernet0
ip address 131.108.1.1 255.255.255.0
interface Dialer1
Description USER dials in and is assigned this interface
 ip unnumbered Ethernet0
 encapsulation ppp
 dialer-group 1
 peer d\efault ip address pool IPaddressPool
 ppp authentication chap
!
ip local pool IPaddressPool 10.10.10.1 10.10.10.254
!
tacacs-server host 3.3.3.3
tacacs-server key extremelysecrtetpassword
dialer-list 1 protocol ip permit
line con 0
 login authentication CONSOLE
 transport input none
line 1 96
```

Example 4-17 *Sample NAS/LAC Configuration (Continued)*

```
 autoselect during-login
 autoselect ppp
 modem Dialin
line aux 0
line vty 0 4
```

Example 4-17 displays the ISP router that typically supplies the tunnel-id to the HGW and IP address to the dial users.

Example 4-18 displays a typical configuration the home gateway router.

Example 4-18 *Sample HGY/LNS Configuration*

```
hostname HGY-LNS
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authentication ppp default if-needed group tacacs+
aaa authorization network default group tacacs+
enable password cciesarecool
vpdn enable
!
vpdn-group DEFAULTcanbeanyname
! Default L2TP VPDN group
 accept-dialin
  protocol any
  virtual-template 1
 local name LNS
 lcp renegotiation always
 l2tp tunnel password 0 secretpwd
interface Virtual-Template1
 ip unnumbered FastEthernet0/0
 peer default ip address pool IPaddressPool
 ppp authentication chap
ip local pool IPaddressPool 11.11.11.1 11.11.11.254
!
tacacs-server host 3.3.3.3
tacacs-server key easypwd
!
end
```

Foundation Summary

The "Foundation Summary" is a condensed collection of material for a convenient review of this chapter's key concepts. If you are already comfortable with the topics in this chapter and decided to skip most of the "Foundation Topics" material, the "Foundation Summary" will help you recall a few details. If you just read the "Foundation Topics" section, this review should help further solidify some key facts. If you are doing your final preparation before the exam, the "Foundation Summary" offers a convenient and quick final review.

Table 4-8 *AAA Terminology*

Attribute	Meaning
Authentication	Who are you? A remote user must be authenticated before being permitted access to network resources. Authentication allows users to submit their usernames and passwords, and permits challenges and responses. Username/password pairs are a common form of authentication.
Authorization	What resources are you permitted to use? Once the user is authenticated, authorization defines what services in the network the user is permitted access to. The operations permitted here can include IOS privileged EXEC commands.
Accounting	What resources were accessed, at what time, and by whom, and what commands were issued to access them? Accounting allows the network administrator to log and view what was actually performed; for example, if a Cisco router was reloaded or the configuration was changed. Accounting ensures that an audit will enable network administrators to view what was performed and at what time.

Table 4-9 *RADIUS Summary*

Feature	Meaning
UDP	Packets sent between clients and servers are UDP primarily because TCP's overhead does not allow for significant advantages. Typically, the user can wait for a username/password prompt.
UDP destination port	Early deployments of RADIUS used UDP ports 1645 and 1646. The officially assigned port numbers are 1812 and 1813.
Attributes	Attributes are used to exchange information between the NAS and client.
Model	Client/server-based model in which packets are exchanged in a unidirectional manner.
Encryption method	The password is encrypted using MD5; the username is not encrypted. RADIUS encrypts only the password in the access-request packet, sent from the client to the server. The remainder of the packet is in clear text. A third party could capture other information, such as the username, authorized services, and accounting information.
Multiprotocol support	Does not support protocols such as AppleTalk, NetBIOS, or IPX. IP is the only protocol supported.

Table 4-10 *TACACS+ Summary*

Feature	Meaning
TCP	Packets sent between client and server are TCP.
TCP destination port	Port 49.
Attributes	Packet types are defined in TACACS+ frame format as follows: Authentication 0x01 Authorization 0x02 Accounting 0x03
Seq_no	The sequence number of the current packet flow for the current session. The Seq_no starts with 1, and each subsequent packet increments by one. The client sends only odd numbers. TACACS+ servers send only even numbers.
Encryption method	The entire packet is encrypted. Data is encrypted using MD5 and a secret key that matches both on the NAS (for example, a Cisco IOS router) and the TACACS+ server.
Multiprotocol support	Supports protocols such as AppleTalk, NetBIOS, or IPX. IP-supported only.

Table 4-11 *RADIUS Versus TACACS+*

	RADIUS	TACACS+
Packet delivery	UDP	TCP
Packet encryption	Encrypts only the password in the access-request packet from the client to the server.	Encrypts the entire body of the packet, but leaves a standard TCP header.
AAA support	Combines authentication and authorization.	Uses the AAA architecture, separating authentication, authorization, and accounting.
Multiprotocol support	None.	Supports other protocols, such as AppleTalk, NetBIOS, and IPX.
Router management	Can pass a privilege level down to the router, which can then be used locally for command authorization.	Enables network administrators to control which commands can be executed on a router.

Table 4-12 *Encryption Methods*

Encryption Method	Description
Data Encryption Standard (DES)	A block cipher algorithm, which means that it performs operations on fixed-length data streams. Uses a 56-bit key to encrypt 64-bit datagrams. DES is a published, U.S. government–approved encryption algorithm.

continues

Table 4-12 *Encryption Methods (Continued)*

Encryption Method	Description
Triple DES (3DES)	A variant of DES that iterates three times with three separate keys (encrypts with one 56-bit key, decrypts with another 56-bit key, and then encrypts with another 56-bit key). Three keys are used to encrypt data, resulting in a 168-bit encryption key.
Advanced Encryption Standard (AES)	A new standard that replaces DES. Encryption key lengths are 128, 192, and 256 bits.

Table 4-13 *IKE Phase I/II*

Phase	Tasks
IKE phase I	Authenticates IPSec peers Negotiates matching policy to protect IKE exchange Exchanges keys using Diffie-Hellman Establishes the IKE security association
IKE phase II	Negotiates IPSec SA parameters by using an existing IKE SA Establishes IPSec security parameters Periodically renegotiates IPSec SAs to ensure security and that no intruders have discovered sensitive data Can also perform optional additional Diffie-Hellman exchange

Table 4-14 *IPSec Terminology*

Term	Meaning
Internet Key Exchange (IKE)	A protocol that provides utility services for IPSec, such as authentication of peers, negotiation of IPSec SAs, and encryption algorithms.
Security association (SA)	A connection between IPSec peers. An SA is unidirectional, and two SAs are required to form a complete tunnel.
Message Digest 5 (MD5)	A hash algorithm (128 bit) that takes an input message (of variable length) and produces a fixed-length output message. IKE uses MD5 or SHA-1 for authentication purposes.
Secure Hash Algorithm (SHA-1)	A hash algorithm (160 bit) that signs and authenticates data.

Table 4-14 *IPSec Terminology (Continued)*

Term	Meaning
RSA signatures	RSA is a public-key encryption system used for authentication. Users are assigned both private and public keys. The private key is not available to the public and is used to decrypt messages created with the public key. To have a signature validated you need to have a CA sign the public key, making it a certificate.
Certificate Authority (CA)	A trusted third party whose purpose is to sign certificates for network entities it has authenticated.
Authentication Header (AH)	Used to authenticate data. AH provides data origin authentication and optional replay-detection services.
Encapsulating Security Payload (ESP)	ESP (transport mode) does not encrypt the original IP header, and only encrypts the IP data by placing a header in between the original IP header and data. ESP (tunnel and transport modes) provides data confidentiality, data integrity, and data origin authentication.
Diffie-Hellman (DH)	Algorithm that is used to initiate and secure the session between two hosts, such as routers.
Advanced Encryption Standard (AES)	A new encryption standard that is considered a replacement for DES. The U.S. government made AES a standard in May 2002. AES provides key lengths for 128, 192, and 256 bits.

Table 4-15 *Enabling TKIP on an Access Point*

Step 1	Enter global configuration mode: **configuration terminal**
Step 2	Enter interface configuration mode for the radio interface: **interface dot11radio 0**
Step 3	Enable WEP, MIC, and TKIP: **encryption** [**vlan** *vlan-id*] **mode wep** {**optional** [**key-hash**] | **mandatory** [**mic**] [**key-hash**]}

Q & A

The Q & A questions are designed to help you assess your readiness for the topics covered on the CCIE Security written exam and those topics presented in this chapter. This format should help you assess your retention of the material. A strong understanding of the answers to these questions will help you on the CCIE Security written exam. You can also look over the questions at the beginning of the chapter again for further review. As an additional study aid, use the CD-ROM provided with this book to take simulated exams, which draw from a database of over 500 multiple-choice questions.

Answers to these questions can be found in Appendix A, "Answers to Quiz Questions."

1. Define the AAA model and a typical application on a Cisco IOS router.
2. Can you allow a remote user authorization before the user is authenticated with AAA?
3. What IOS command is required when enabling AAA for the first time?
4. What is the privilege level of the following user? Assume AAA is not configured.

   ```
   R2>
   ```

5. Define four possible RADIUS responses when authenticating the user through a RADIUS server.
6. What are RADIUS attributes? Supply five common examples.
7. What protocols does RADIUS use when sending messages between the server and client?
8. What predefined destination UDP port number is RADIUS accounting information sent to?
9. What does the following Cisco IOS software command accomplish on a Cisco IOS router?

   ```
   aaa authentication ppp user-radius if-needed group radius
   ```

10. What is the RADIUS server IP address and key for the following configuration?

    ```
    radius-server host 3.3.3.3
    radius-server key GuitarsrocKthisplaneT
    ```

11. TACACS+ is transported over what TCP server port number?
12. What information is encrypted between a Cisco router and a TACACS+ server?
13. What are the four possible packet types from a TACACS+ server when a user attempts to authenticate a Telnet session to a Cisco router configured for AAA, for example?

14. What is the significance of the sequence number in the TACACS+ frame format?

15. What does the following IOS command accomplish?

```
aaa authentication ppp default if-needed group tacacs+ local
```

16. What IOS command defines the remote TACACS+ server?

17. What are the major difference between TACACS+ and RADIUS?

	RADIUS	TACACS+
Packet delivery	UDP	TCP
Packet encryption	Encrypts only the password in the access-request packet from the client to the server.	Encrypts the entire body of the packet but leaves a standard TCP header.
AAA support	Combines authentication and authorization. Accounting is handled differently.	Uses the AAA architecture, separating authentication, authorization, and accounting.
Multiprotocol support	None.	Supports other protocols, such as AppleTalk, NetBIOS, and IPX.
Router management	Does allow users to control which commands can be executed on a router. Can pass a privilege level down to the router, which can then be used locally for command authorization.	Enables network administrators to control which commands can be executed on a router.

18. What are the three most common threats from intruders that network administrators face?

19. What is a hash in encryption terminology?

20. Name the two modes of operation in IPSec and their characteristics.

21. What does IKE accomplish?

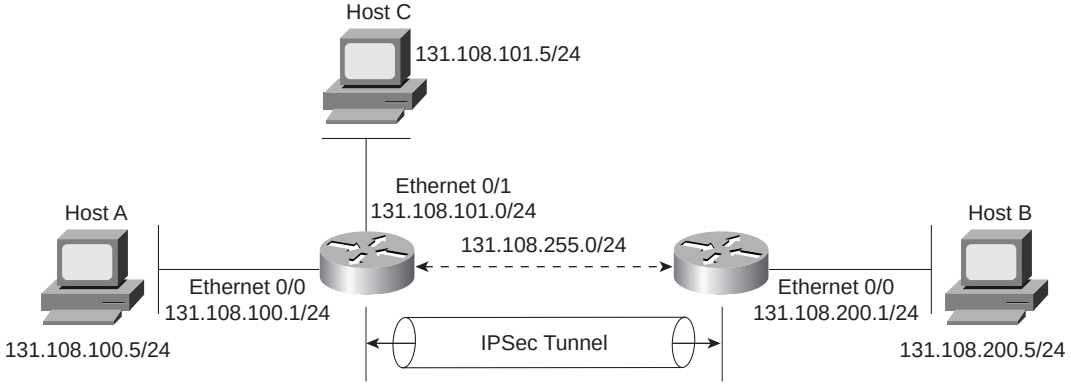
22. Certificate Enrollment Protocol is transported over what TCP port?

Scenario

Scenario: Configuring Cisco Routers for IPSec

Figure 4-21 displays a simple two-router topology where traffic from network 131.108.100.0/24 is encrypted when it is sent to the remote network 131.108.200.0/24.

Figure 4-21 *Scenario Topology*



Example 4-19 displays the working configuration of R1, with lines numbered from 1 to 31.

Example 4-19 *R1's Full Configuration*

```
1.  version 12.2
2.  hostname R1
3.  enable password cisco
4.  crypto isakmp policy 1
5.   hash md5
6.   authentication pre-share
7.  crypto isakmp key CCIE address 131.108.255.2
8.  crypto ipsec transform-set anyname esp-des esp-sha-hmac
9.  mode tunnel
10. crypto map anyname1 1 ipsec-isakmp
11.  set peer 131.108.255.2
12.  set security-association lifetime seconds 180
13.  set transform-set anyname
14.  match address 100
15. interface Ethernet0/0
16.  ip address 131.108.100.1 255.255.255.0
17. interface Serial0/0
18. ip address 131.108.255.1 255.255.255.252
```

Example 4-19 *R1's Full Configuration (Continued)*

```
 encapsulation frame-relay
 ip split-horizon
 ip ospf network point-to-point
 frame-relay map ip 131.108.255.2 102 broadcast
 frame-relay interface-dlci 102
 frame-relay lmi-type ansi
 crypto map anyname1
interface Ethernet0/1
 ip address 131.108.101.1 255.255.255.0
router ospf 1
 network 131.108.0.0 0.0.255.255 area 0
 access-list 100 permit ip 131.108.100.0 0.0.0.255 131.108.200.0 0.0.0.255
end
```

Example 4-20 displays the working configuration of R2, with lines numbered from 1 through 29.

Example 4-20 *R2's Full Configuration*

```
Version 12.2
hostname R2
enable password cisco
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key CCIe address 131.108.255.1
crypto ipsec transform-set anyname esp-des esp-sha-hmac
mode tunnel
crypto map anyname1 1 ipsec-isakmp
set peer 131.108.255.1
set security-association lifetime seconds 180
set transform-set anyname
match address 100
interface Ethernet0/0
ip address 131.108.200.1 255.255.255.0
interface Serial0/0
 ip address 131.108.255.2 255.255.255.252
 encapsulation frame-relay
 ip split-horizon
 ip ospf network point-to-point
 frame-relay map ip 131.108.255.1 201 broadcast
 frame-relay interface-dlci 201
 frame-relay lmi-type ansi
 crypto map anyname1
 router ospf 1
 network 131.108.0.0 0.0.255.255 area 0
 access-list 100 permit ip 131.108.200.0 0.0.0.255 131.108.100.0 0.0.0.255
end
```

The following debug output is seen on R1 after the network administrator pings remote network 131.108.100.1 from Router R2's console port.

1. Why will the IPSec tunnel not negotiate properly?

```
R2#debug crypto engine
Crypto Engine debugging is on
R2#ping
Protocol [ip]:
Target IP address: 131.108.100.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 131.108.200.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 131.108.100.1, timeout is 2 seconds:
22:58:55: CryptoEngine0: generate alg parameter
22:58:55: CRYPTO_ENGINE: Dh phase 1 status: 0
22:58:55: CRYPTO_ENGINE: Dh phase 1 status: 0
22:58:55: CryptoEngine0: generate alg parameter
22:58:55: CryptoEngine0: create ISAKMP SKEYID for conn id 1
22:58:55: CryptoEngine0: generate hmac context for conn id 1.
22:58:55: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 131.108.255.1   failed it
s sanity check or is malformed....
Success rate is 0 percent (0/5)
R2#
```

2. What subnets will be encrypted between Routers R1 and R2?

3. What IOS command produced the following display and from which router?

```
Crypto Map "anyname1" 1 ipsec-isakmp
        Peer = 131.108.255.2
        Extended IP access list 100
    access-list 100 permit ip 131.108.100.0 0.0.0.255 131.108.200.0 0.0.0.255
        Current peer: 131.108.255.2
        Security association lifetime: 4608000 kilobytes/180 seconds
        PFS (Y/N): N
        Transform sets={ anyname, }
        Interfaces using crypto map anyname1:
                Serial0/0
```

4. Will Host A be able to communicate with Host B or Host C? The following displays are the IP routing tables on R1 and R2. (Assume the gateway configurations on the PCs are correct.)

   R1's IP routing table:

```
R1>show ip route
Codes: C - connected, , O - OSPF,
     131.108.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       131.108.255.0/30 is directly connected, Serial0/0
O       131.108.200.0/24 [110/400] via 131.108.255.2, 00:52:00, Serial0/0
C       131.108.101.0/24 is directly connected, Ethernet0/1
C       131.108.100.0/24 is directly connected, Ethernet0/0
```

   R2's IP routing table:

```
R2>show ip route
Codes: C - connected, , O - OSPF
     131.108.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       131.108.255.0/30 is directly connected, Serial0/0
C       131.108.200.0/24 is directly connected, Ethernet0/0
O       131.108.101.0/24 [110/58] via 131.108.255.1, 00:52:09, Serial0/0
131.108.100.0/24 [110/58] via 131.108.255.1, 00:52:09, Serial0/0
```

5. To allow the IP subnet 131.108.101.0/24 attached to the R1 Ethernet 0/1 interface to be encrypted over the IPSec tunnel and to communicate with the remote PC IP address 131.108.200.5, what configuration changes are required on which router?

Scenario Answers

Scenario Solutions

1. The following debug output advises the network administrator of the problem:

```
22:58:55: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 131.108.255.1   failed it
s sanity check or is malformed....
```

During the IKE negotiation, the router reports a message that identifies the fault as the share password. R2 is configured with the password, CCIe (should match R1's preshared password set to CCIE). See Example 4-17, and code line 7.

Changing the IKE password to CCIE with the IOS command **crypto isakmp key CCIE address 131.108.255.1**, the following debug output confirms the IPSec connections by pinging from R2 Ethernet 0/0 IP address to R1 Ethernet 0/0 IP address:

```
R2#ping
Protocol [ip]:
Target IP address: 131.108.100.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 131.108.200.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 131.108.100.1, timeout is 2 seconds:
23:12:21: CryptoEngine0: generate alg parameter
23:12:21: CRYPTO_ENGINE: Dh phase 1 status: 0
23:12:21: CRYPTO_ENGINE: Dh phase 1 status: 0
23:12:21: CryptoEngine0: generate alg parameter
23:12:21: CryptoEngine0: create ISAKMP SKEYID for conn id 1
23:12:21: CryptoEngine0: generate hmac context for conn id 1
23:12:21: CryptoEngine0: generate hmac context for conn id 1
23:12:21: CryptoEngine0: generate hmac context for conn id 1
23:12:21: CryptoEngine0: clear dh number for conn id 1
23:12:22: CryptoEngine0: generate hmac context for conn id 1
23:12:22: validate proposal 0
23:12:22: validate proposal request 0
23:12:22: CryptoEngine0: generate hmac context for conn id 1.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 12/13/16 ms
R2#
```

The first ping packet fails because the IPSec tunnel has not yet been created. Then, the IPSec tunnel is successfully brought up between R1 and R2.

2. Access-list 100 on both routers defines the IP subnets that need to be encrypted between R1 and R2. Packets flowing between subnets 131.108.100.0/24 and 131.108.200.0/24 will be encrypted.

   R1's ACL is as follows:

   ```
   access-list 100 permit ip 131.108.100.0 0.0.0.255 131.108.200.0 0.0.0.255
   ```

   R2's ACL is as follows:

   ```
   access-list 100 permit ip 131.108.200.0 0.0.0.255 131.108.100.0 0.0.0.255
   ```

3. The **show crypto map** IOS command displays the remote peer address and the transform set. The previous displays are taken from R1 because the remote peer address is displayed as 131.108.255.2 (R2's serial 0/0 IP address).

4. Yes, because IPSec has nothing to do with routing IP data, IPSec will encrypt only data as configured. R1 has a remote entry to the network residing on R2, and R2 has a remote entry to the network residing on R1. Traffic between A and C and B and C will not be encrypted; only traffic between A and B will be encrypted.

   Here is a sample ping request from R2 to R1 and Host A and Host C:

   ```
   R2>ping 131.108.100.1
   Type escape sequence to abort.
   Sending 5, 100-byte ICMP Echos to 131.108.100.1, timeout is 2 seconds:
   !!!!!
   Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
   R2>
   R2>ping 131.108.101.1
   Type escape sequence to abort.
   Sending 5, 100-byte ICMP Echos to 131.108.101.1, timeout is 2 seconds:
   !!!!!
   Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
   R2>
   R2>ping 131.108.100.5
   Type escape sequence to abort.
   Sending 5, 100-byte ICMP Echos to 131.108.100.5, timeout is 2 seconds:
   !!!!!
   Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
   R2>
   R2>ping 131.108.101.5
   Type escape sequence to abort.
   Sending 5, 100-byte ICMP Echos to 131.108.105.1, timeout is 2 seconds:
   !!!!!
   Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
   ```

5. Because the source network is located on R1, access-list 100 on R1 needs to be modified, remembering that, by default, an implicit deny is defined on ACL 100. Network 131.108.101.0/24 is only permitted to encrypt traffic to the static IP address 131.108.200.5, hence the ACL line required on R1 becomes the following:

```
access-list 100 permit ip 131.108.100.5 0.0.0.0 131.108.200.0 0.0.0.255
access-list 100 permit ip 131.108.101.0 0.0.0.255 131.108.200.5 0.0.0.0
```

or:

```
access-list 100 permit ip 131.108.100.5 0.0.0.0 131.108.200.0 0.0.0.255
access-list 100 permit ip 131.108.101.0 0.0.0.255 host 131.108.200.5
```

On R2 the access list becomes:

```
access-list 100 permit ip 131.108.200.0 0.0.0.255 131.108.101.0 0.0.0.255
access-list 100 permit ip 131.108.200.5 0.0.0.0 131.108.100.0 0.0.0.255
```

IP routing is already configured and working. IPSec will ensure only that IP data is encrypted.

Exam Topics in This Chapter

- Cisco Secure NT
- CiscoWorks VPN/Security Management Solution (VMS)
- Cisco Secure Intrusion Detection System (formerly NetRanger)
- VPN 3000
- Client-side VPN
- CAT Service Modules
- Cisco IOS IDS (inline)
- Cisco Secure ACS
- Security Information Monitoring System (event correlation, basic forensics)

You can find a list of all of the exam topics in the introduction to this book. For the latest updates on exam topics, visit Cisco.com.

CHAPTER 5

Cisco Security Applications

This chapter reviews a number of Cisco-defined CCIE Security written exam blueprint objectives covering security applications and the Cisco Secure product suites.

This chapter covers the following topics:

- **Cisco Secure for Windows (NT) and Cisco Secure ACS**—Introduces Cisco Secure, the Cisco security application that is available on Windows platforms, and Cisco Secure Access Control Server (ACS), which provides additional network security when managing IP networks designed with Cisco devices.
- **IDS Fundamentals**—Covers intrusion detection systems (IDSs), which allow administrators to monitor their networks for protocol anomalies and much more. A solid understanding of IDS fundamentals and different IDS technologies is required before analysis and deployment discussions can be covered.
- **Cisco Secure Intrusion Detection System and Catalyst Services Modules**—Describes Cisco Secure IDS, which ensures that networks are secured. Coverage also includes inline IDS and the Catalyst Services Module.
- **CiscoWorks VMS**—Describes how CiscoWorks VPN/Security Management Solution (VMS), an integral element of the SAFE Blueprint for enterprise network security from Cisco, can be used to help secure networks.
- **Cisco VPN 3000 Concentrator and Cisco Secure VPN Client**—Includes information on the VPN Concentrator and the Cisco Secure VPN Client required to ensure that connections over public networks are secured.
- **Cisco Router and Security Device Manager (SDM)**—Details SDM, a web-based embedded device manager of Cisco IOS–enabled devices.
- **Security Information Monitoring System**—Explains how Cisco IDS can monitor and identify intruder-based attacks and enable security information to be monitored and acted upon.

"Do I Know This Already?" Quiz

The purpose of this assessment quiz is to help you determine how to spend your limited study time.

If you can answer most or all of these questions, you might want to skim the "Foundation Topics" section and return to it later, as necessary. Review the "Foundation Summary" section and answer the questions at the end of the chapter to ensure that you have a strong grasp of the material covered.

If you already intend to read the entire chapter, you do not necessarily need to answer these questions now. If you find these assessment questions difficult, read through the entire "Foundation Topics" section and review it until you feel comfortable with your ability to answer all of these questions and the "Q & A" questions at the end of the chapter.

Answers to these questions can be found in Appendix A, "Answers to Quiz Questions."

1. In a secured network architecture, which of the following components are to be considered security devices? (Choose all that apply.)
   a. Switches
   b. Routers
   c. Firewalls
   d. Intrusion detection systems
   e. VPN 3000 Concentrator
   f. All of these
2. Cisco Secure ACS supports what two security protocols? (Choose the best two answers.)
   a. RADIUS
   b. TCP
   c. TACACS+
   d. TFTP
   e. ICMP
3. The Cisco IDSM-2 has which of the following interfaces?
   a. Console port.
   b. Console and auxiliary ports.
   c. Only an auxiliary port.
   d. IDSM-2 has no interfaces available.

4. In a secured network architecture, which of the following components is typically *not* considered a security appliance?
   a. Router
   b. Switch
   c. Firewall
   d. Intrusion detection appliance
   e. VPN Concentrator
   f. Windows XP PC
   g. All of these
5. A VPN 3000 Concentrator is typically located in what part of a security network?
   a. The inside interface of a PIX Firewall
   b. The outside interface of a PIX Firewall
   c. The inside interface of the DMZ
   d. The outside interface of the DMZ
   e. None of these
6. All but which of the following is a Cisco VPN model currently supported by Cisco?
   a. 3001
   b. 3002
   c. 3005
   d. 3015
   e. 3020
   f. 3030
   g. 3060
   h. 3080
7. All but which of the following is part of the Cisco SAFE Blueprint for IDS tuning?
   a. Identify potential locations for sensors.
   b. Apply an initial configuration.
   c. Monitor the sensor while tuning.
   d. Analyze alarms, tune out false positives, and implement signature tuning (if needed).
   e. Selectively implement response actions.
   f. Update sensors with new signatures.
   g. Remove the PIX Firewall.

8. What application layer protocol does a security manager use when using the Cisco Security Device Manager (SDM) application?
   a. ICMP
   b. SSC
   c. SSCP
   d. SSL
   e. CCH
   f. AES
   g. ESP
   h. 3DES
9. What is the default username and password combination for a Catalyst 6500 ISDM-2 module (not the IDS 4.0)?
   a. Cisco/cisco
   b. cisc/cisc
   c. ciscoids/attacks
   d. cisco/cisco
   e. attack/attack
   f. None of these
10. What is the default username and password combination for a VPN 3000 Concentrator?
   a. Admin/admin
   b. admin/admin
   c. cisco/cisco
   d. 3000/3000
   e. attack/attack
   f. None of these

Foundation Topics

Cisco Secure for Windows (NT) and Cisco Secure ACS

Cisco Systems has developed a number of scalable security software products to help protect and ensure a secured network in relation to Cisco products.

Cisco Secure provides additional network security when managing IP networks designed with Cisco devices.

Cisco Secure can run on Windows NT/2000 and UNIX platforms. The latest CCIE Security examination no longer requires a candidate to be proficient in the UNIX version. Some details are left in this guide for completeness so that in the real world you may have the full story from Cisco.

Cisco Secure for ACS is supported in three main flavors, for small, medium, and large ISP-based networks. Three versions of Cisco Secure are listed here:

- **Cisco Secure ACS for NT**—This powerful ACS application for NT servers runs both TACACS+ and RADIUS. It can use an NT username/password database or Cisco Secure ACS database.
- **Cisco Secure ACS for UNIX**—This powerful ACS application for UNIX includes support for TACACS+ and RADIUS. It supports SQL applications such as Oracle and Sybase.
- **Cisco Secure Global Roaming Server**—This server performs TACACS+ and RADIUS proxy functions. It is a standalone server for large ISP networks. Cisco Secure Global Roaming Server recently has been replaced by Cisco CNR Access Register to take advantage of multiprocessor systems and provide the highest AAA performance.

NOTE Cisco Secure topics are tested in the CCIE Security lab exam (particularly Cisco Secure for Windows 2000 Server). The written exam does not require you to have a detailed understanding of this application. Chapter 8, "CCIE Security Self-Study Lab," contains an excellent example of how to configure Cisco Secure ACS for Windows NT in a real lab scenario and hence it is not covered in depth in this chapter.

Chapter 8 also contains a detailed example of how a VPN 3000 Concentrator is configured.

The main features of Cisco Secure include the following:

- Supports centralization of AAA access for all users, including routers and firewalls
- Can manage Telnet access to routers and switches

- Can support a limited number of network access servers of between 5000 and 20,000 AAA clients
- Supports many different Cisco platforms, including PIX access servers and routers

Figure 5-1 displays typical centralized Cisco Secure Server performing functions such as user authentication, authorization, and accounting.

Figure 5-1 *Cisco Secure Example*

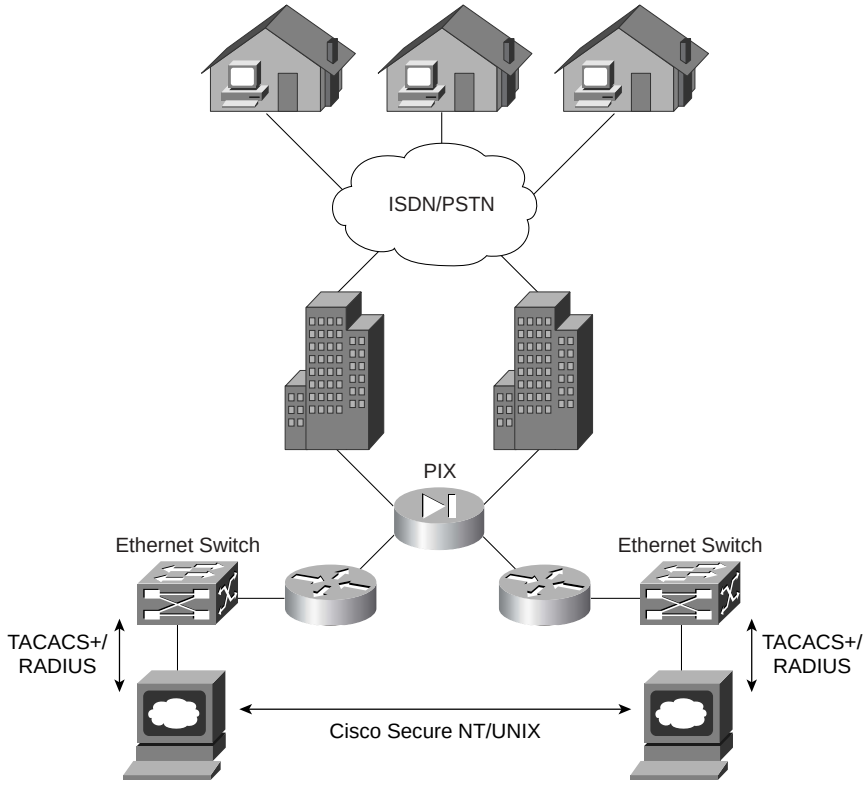


Figure 5-1 displays a typical application where ISDN/PSTN users are authenticated by RADIUS or TACACS+ via Cisco Secure.

In addition to simultaneous support for RADIUS/TACACS+, Cisco Secure also supports the following AAA features:

- TACACS+ support for the following:
  - Access lists
  - Privilege level support

  - Time restrictions where access to the network is controlled during the day and night

- RADIUS support for the following:
  - Cisco RADIUS AV pairs
  - IETF support (RADIUS is a defined standard)
- Other features include the following:
  - Support for virtual private networking
  - The ability to disable accounts after a set number of failed attempts

Cisco Secure ACS

Cisco Secure Access Control Server (ACS) is a network security software application that provides a number of security features such as logging, debugging, authorization, and authentication of users.

Cisco ACS supports both RADIUS and TACACS+. You can download a trial version of the software that is supported on a Windows-based platform at http://cisco.com/public/sw-center/. Click the link to "Cisco Secure Software."

Although the CCIE Security written exam does not heavily test this application, it is tested in the lab portion, so you are highly encouraged to study Chapter 8, which has a detailed Cisco Secure ACS example and discusses how features such as user-based access are enabled.

If you want more details on Cisco Secure ACS, go to http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs33/user/o.htm.

IDS Fundamentals

A solid understanding of IDS fundamentals and different IDS technologies is required before analysis and deployment discussions can be covered—not only for the written and lab exams but also for real-life scenarios. Out of all the CCIE tracks available, the Security exam is one of the most sought-after certifications because it relates to everyday real-life scenarios.

Notification Alarms

The overall purpose of intrusion detection systems is to trigger alarms when a given packet or sequence of packets seems to represent suspicious activity that violates the defined network security policy. Although alarms are essential, it is critical for network security personnel to configure the IDS to minimize the occurrence of false negative and false positive alarms. There are a number of terms you should be familiar with when discussing host- or network-based IDSs:

- **False positive alarm**—False positives (benign triggers) occur when the IDS reports certain benign activity as malicious, requiring human intervention to diagnose the event.
- **False negative alarm**—A false negative alarm can occur when the IDS sensor does not detect and report a malicious activity, but the system allows it to pass as nonintrusive behavior. Because this can be catastrophic for network operation, minimizing false negatives is the highest priority.
- **True positive alarm**—This is the opposite of a false negative. In this case an alarm has been correctly sent in response to malicious activity. These alarms cause the most concern for a network administrator.
- **True negative alarm**—A true negative is not an actual alarm but rather a situation in which the IDS in place does not trigger an alarm for activity permitted within a network.

Signature-Based IDS

The signature-based IDS monitors the network traffic or observes the system and sends alarms if a known malicious event is happening. It does this by comparing the data flow against a database of known attack conditions. These signatures explicitly define what traffic or activity should be considered malicious. Various types of signature-based IDSs exist, including the following:

- Simple and stateful pattern matching
- Protocol decode-based analysis
- Heuristic-based analysis
- Anomaly detection

The pattern-matching systems look for a fixed sequence of bytes in a single packet, which has three advantages:

- It is simple.
- It generates reliable alerts.
- It is applicable to all protocols.

The weakness of a pattern-matching system is that any slightly modified attack leads to false negatives. Multiple signatures may be required to deal with a single vulnerability in stateful pattern-matching systems, as matches are made in context within the state of the stream.

Anomaly-Based IDS

The anomaly-based IDS looks for traffic that deviates from what is seen normally. The definition of the normal and abnormal network traffic patterns forms the identity of the culprit. Once the definition is in place, the anomaly-based IDS can monitor the system or network and send an alarm if an event outside known normal behavior is detected. An example of suspicious behavior is the detection of specific data packets (routing updates) that originate from a user device rather than from a network router.

Network-Based IDS Versus Host-Based IDS

Host-based IDS (HIDS) and network-based IDS (NIDS) should be seen as complimentary, because the systems fill in for each other's weaknesses. Therefore, they should be deployed together rather than only one or the other. Table 5-1 lists the most important advantages and disadvantages of deploying NIDS or HIDS.

Table 5-1 *Comparison of Host-Based IDS and Network-Based IDS**

IDS	Pros	Cons
Host-based	Verification of success or failure of an attack possible. Has a good knowledge of the host's context, and as a result is more focused on a specific system.	OS/platform-dependent. Not available for all operating systems. Impact on the available resources of the host system. Expensive to deploy one agent per host. Expensive to train staff to support and implement on a large basis.
Network-based	Protects all hosts on the monitored network cost effectively. Independent of the OS and has no impact on the host (runs invisibly). Especially useful for low-level attacks (network probes and denial of service attacks).	Deployment is very challenging in switched environment. Network traffic may overload the NIDS (CPU intensive). Not effective for single-packet attacks and hidden attacks in encrypted packets.

*Cisco NIDS is covered in more detail in Chapter 6 of this guide.

IDS Placement

The HIDS is typically placed in a number of locations, such as the DMZ, behind a firewall, inline inside a Catalyst 6500, or on the inside network.

Figure 5-2 displays a typical IDS placement and shows how this technology can be used to prevent attacks from within and from outside an organization.

Figure 5-2 *IDS Placement*

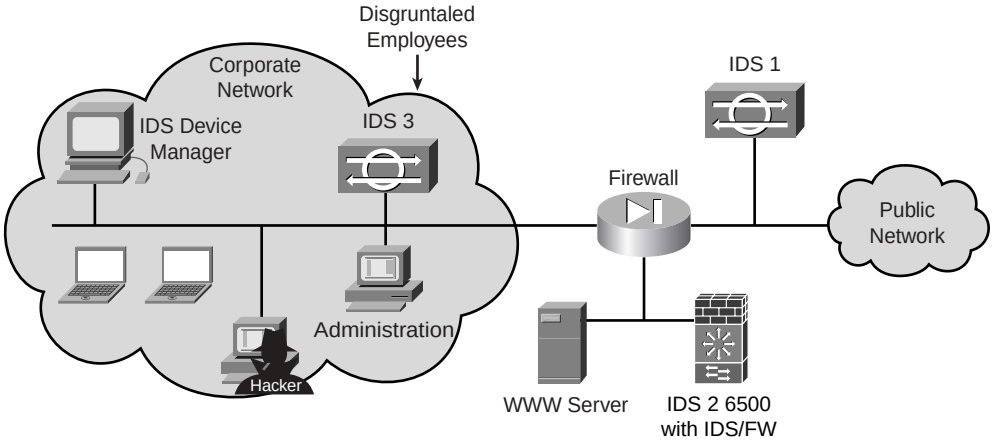


Figure 5-2 displays a network with three NIDSs in place communicating back to an IDS Device Manager (IDM).

IDS 1 in Figure 5-2 is the frontline defense against all the noise from the Internet and will typically stop attacks such as port scans, Network Mapper (Nmap) for example. Nmap is a free, open-source utility for network exploration or security auditing, downloadable from http://www.insecure.org/nmap/index.html.

NOTE The NIDS appliance (IDS 1) in Figure 5-2 at the public side of the firewall is monitoring for attacks based on Layer 4 through Layer 7 analysis and on comparisons against known signatures. Still, this NIDS should have alarms set to a lower level than appliances on the inside of the firewall. Alarms seen here do not represent actual breaches, but merely attempts to reduce the number of false positives and to decrease the amount of time it takes to discover any successful attacks against devices within the corporate network.

However, IDS 2 in Figure 5-2 is a 6500 series switch with an IDS blade and a Cisco Firewall Services Module (FWSM). The Cisco FWSM is a high-speed, integrated firewall module for Cisco Catalyst 6500 switches and Cisco 7600 Series routers and is based on Cisco PIX Firewall technology. It includes advanced features like multiple security contexts both at the routed levels and in bridging mode, helping to reduce cost and operational complexity while managing multiple firewalls from the same management platform. IDS 2 in Figure 5-2 can prevent much more sophisticated forms of attack, such as manipulated Internet Information Server (IIS) services in

Windows-based platforms. Recent reports mention a number of vulnerabilities in the IIS services, such as device manager traversal, Unicode device manager traversal, and the ability to decode command execution via a webpage.

Cisco IDS Sensors are network devices that perform real-time monitoring of network traffic for suspicious activities and active network attacks. When an event does occur, the Cisco IDS sends an alarm to the Cisco IDS Device Manager (IDM), a software package installed on an HP OpenView, HPUX, or Solaris workstation.

Typically, when an alarm is raised, the IDS can send e-mail messages at a particular alarm level via the daemon named eventd. IDS sensors can also set an alarm that is user configurable. IDS sensors cannot perform a trace route function to the intruding system; this is not often effective, because hackers use other IP addresses by spoofing valid network addresses. Recent developments in Cisco security also mean that sensors can modify and add new access lists, for example, when an event does occur, and block the source IP address from instigating any more attacks. This is called *shunning* in Cisco terminology.

IDS 3 in Figure 5-2 will prevent intruders from within an organization.

It is vital that any organization that is serious about defending against new styles of attacks constantly tune the IDS signatures so that the number of false positives is minimized.

IDS Tuning

Tuning IDS sensors is critical to a successful network implementation. IDS sensors generate alerts in response to all traffic matching established criteria; without tuning, this will not be as reliable as possible. This could result in a large number of false positives, which could easily overwhelm security personnel and reduce the value of the information the IDS provides, resulting in a relaxed attitude by security support and administration staff until a real event occurs. But that could be too late.

The Cisco SAFE Blueprint recommends a number of key guidelines when tuning an IDS sensor (as described by Cisco at http://cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a00801bc111.shtml):

Step 1 **Identify Potential Locations for Sensors**—To properly tune IDS sensors, the first step is to identify network locations where the sensors can be placed for maximum efficiency.

Step 2 **Apply an Initial Configuration**—The objective of this step is to take a first pass at configuring the network IDS sensors. First, sensors are classified and grouped according to active signatures and are then configured by group with a common signature profile. The sensors in a group are managed collectively, which simplifies the management of large numbers of sensors.

Step 3 **Monitor the Sensor While Tuning**—The objective of steps 3 and 4 is to monitor IDS sensor alarms and tune out any alarms caused by normal background traffic rather than malicious activity. This results in a decrease in the number of false alarms.

Step 4 **Analyze Alarms, Tune Out False Positives, and Implement Signature Tuning (If Needed)**—During the initial tuning period, you will need to determine the cause of every alarm in order to identify false positives. This task could be tedious, but it is necessary for your network IDS deployment to be of any use in detecting malicious activity.

Step 5 **Selectively Implement Response Actions**—Once the false positives are tuned out and logging due to IDS tuning changes is sufficiently reduced, response actions such as TCP resets, shunning, and IP logging can be implemented.

Step 6 **Update Sensors with New Signatures**—Automatic signature updates should be implemented for deployments with large numbers of sensors.

Network managers or security users can define user blade signatures with string matches using the signature in the 8000 range. Each signature is defined by a signature ID or number.

Network IDSs imbedded in Cisco IOS, in hardware-based models, or in PIX Firewalls can respond to attacks with a number of predefined actions to help network security managers:

- **Blocking**—Blocking (also known as shunning) may also be implemented within the network to protect corporate servers that are not customer facing.
- **Resetting TCP connections**—TCP Reset is a blocking method whereby an IDS sensor responds to an attack by sending the source and destination address of the attack a TCP RST packet to terminate the connection.
- **IP logging**—Network IDS sensors can be configured to log IP packet data after an attack signature is seen.
- **Logging/reporting**—Extensive logging and reporting can be performed on Cisco IDS sensors to report and log an event, indicate the attack signature seen, notify the management stations, report deviations from a particular attack signature, and look at new signatures not seen before.

As you can see, IDS technology offers many advantages to protect today's growing networks. The need to be connected to the public Internet has meant IP networks are always vulnerable if not protected.

Cisco Secure Intrusion Detection System and Catalyst Services Modules

This section covers tools that are useful for managing network security. Cisco Secure IDS, formerly known as NetRanger, is designed to efficiently and effectively protect your network against intruders from inside and outside of your networking domain.

NOTE The CCIE Security written exam still refers to the term NetRanger. The new CCIE Security exam no longer tests the NetSonar application. NetRanger is now commonly known as Cisco Secure Intrusion Detection System or Cisco Secure IDS. This guide refers to the terms Cisco Secure IDS to match the marketing and terminology used on the Cisco website.

Cisco Secure IDS

Cisco Secure IDS is an enterprise intrusion detection system designed to detect, report, and, in the event of unauthorized access, terminate data sessions between users and host devices.

Users are not aware that Cisco Secure IDS is watching data across the network; it is transparent to all systems.

Cisco Secure IDS has three components:

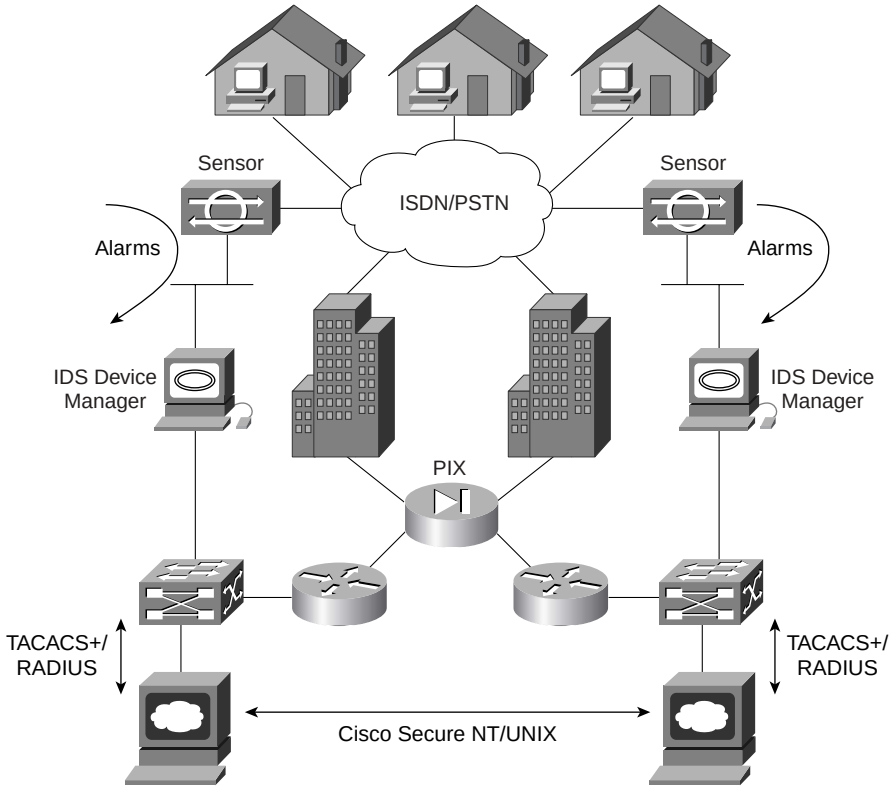
- **Cisco Secure IDS Sensor**—High-speed device that analyzes the contents of data being transported across a network and determines whether that traffic is authorized or unauthorized. Unauthorized traffic includes ping requests from intruders. Traffic detected from unauthorized sources is sent directly to the IDM and the intruder is removed from the network.
- **Cisco IDS Device Manager (IDM)**—Enables IDS security administrators to easily manage the IDS solution in place by allowing secure communication between local and remote IDS systems.
- **Cisco IDS Management Center (MC)**—Communicates with the Cisco Secure ACS server. It dictates to Cisco Secure ACS the creation of a command authorization set type, which appears in the Shared Profile Components section of the Cisco Secure ACS HTML interface.

Figure 5-3 displays the typical network placement of Cisco Secure IDS products. Cisco Secure IDS sensors are typically placed on the DMZ network, because that region contains hosts that are publicly reachable via the Internet.

Cisco Secure IDS Sensors can be located anywhere in the network. They are typically located close to hosts or entry points to a network, such as dial-in users or Internet connections. Alarms are logged on the Sensor and IDM. The alarms are displayed or viewed on the IDM. Optional configuration settings include killing an active TCP session or reconfiguring access lists (termed shunning).

The sensor can detect the intruder's IP address and destination ports, and buffer up to 256 characters entered by the illegal devices. Cisco Secure IDS 4.1 supports Ethernet (10/100/1000) only. Cisco Secure IDS Sensors can modify predefined access lists on Cisco IOS routers and change the definitions of permitted networks in response to an attack. Cisco Secure IDS Sensors cannot modify the IP routing table nor reload or shut down interfaces. When illegal activity is discovered, an alarm is sent directly to configured IDMs.

Figure 5-3 *Typical Cisco Secure IDS Design*



The software used on the sensors can be loaded from a central IDM, allowing easier software upgrades. The GUI on the IDM also allows network monitoring from one central location, ensuring that one central group within an organization can be directly responsible for monitoring and acting on alarms. GUIs and colored alarms indicate possible vulnerabilities.

The section "Security Information Monitoring System," later in this chapter, covers some sample events.

NOTE For more details on software and hardware requirements for Cisco IDS Device Manager, go to http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids10/idmiev/swchap1.htm#wp50470.

IDS Device Manager can send out an alarm when certain configuration changes are made on Cisco routers, can send e-mail messages when particular alarm levels are reached, and can ensure a TCP attack is thwarted by sending TCP reset segments to unauthorized sources. When a Cisco Secure IDS Sensor communicates with the IDM, if the network is down, up to 255 alternate route paths can be attempted. Packets can be buffered and sent when the network is restored and communications occur (there are no keepalive communications; rather, one device sends and the other waits and listens) to ensure that alarms are sent.

NOTE Cisco Secure IDS 4.1 examines the entire packet. Intruders usually use an attack based on large ICMP traffic, typically fragmented, to discover the behavior of routers in a network. Cisco IDS 4.1 can mitigate this form of attack because packets can be reassembled and alerts sent if required, but this feature is available only in the most recent releases of IDS. Previously, this form of attack could cause networking issues and loss of packets.

Intruders typically also use context-based attacks by scanning TCP or UDP ports in use.

For more details on Cisco Secure IDS, search with the keywords "Cisco Secure IDS" at Cisco.com. For example, information on the latest Cisco Secure IDS (version 4.1) can be found at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/index.htm.

Cisco Inline IDS (Intrusion Prevention System)

Recently Cisco marketing released security concept, Intrusion Prevention System (IPS), along with the new router platforms, namely the 1800, 2800, and 3800. IPS is designed to leverage Cisco PIX software and Cisco IDS sensor technologies, combined with IOS software features. Cisco IOS IPS is an inline, deep-packet, inspection-based solution that helps enable Cisco IOS software to effectively mitigate network attacks.

Cisco inline IDS (or IPS) allows for traffic to be dropped, can send an alarm, or can reset a connection, enabling the router to respond immediately to security threats and protect the network. Cisco IOS IPS relies on inline IDS to provide features such as the following:

- The ability to dynamically load and enable selected IPS signatures in real time
- An increase in the number of supported signatures to more than 740 of the signatures supported by Cisco IDS sensor platforms
- The ability for a user to modify an existing signature or create a new signature to address newly discovered threats; each signature can be enabled to send an alarm, drop the packet, or reset the connection

Typical types of attacks from hackers and, most importantly, internal intruders and disgruntled employees are of the following forms:

- Reconnaissance attacks
- Access attacks
- Denial of service (DoS) attacks

Most large organizations install a number of firewall technologies such as PIX Firewall, CyberGuard, or Netscreens, but fail to adequately prevent attacks that initiate from the inside. Chapter 6, "Security Technologies," discusses in detail some of the most common attacks that employees (or an attacker who has plugged into a network by tailgating their way into an office area) can instigate within organizations. Some large organizations, which will remain nameless, have experienced this very problem.

You will now cover the details about the different forms of inline IDS before we take a look at some example scenarios.

IDS sensors are software and/or hardware used to collect and analyze network traffic. These sensors are available in two flavors, network IDS and host IDS.

The CiscoWorks Management Center for IDS Sensors is a component of the CiscoWorks VMS and acts as the collection point for alerts and performs configuration and deployment services for the IDS sensors in the network.

Cisco recently announced a new series of architectures based on IPS. IDS and IPS are used in tandem to provide a secure and reliable IP network. You are encouraged to maximize your security knowledge of IDS and IPS not just for the written exam but for your own career development. More details on IDS and IPS can be found at http://www.cisco.com/security/.

Catalyst Services Module

The Cisco Catalyst 6500 Series Switch is the Cisco frontline router and switch. Although not yet used in the CCIE Security lab exam, the Catalyst 6500 is covered in the written exam. The Catalyst 6500 security features are very enhanced and widely deployed across the globe.

Cisco supports IDS in the Catalyst 6500 Series Switch with the Cisco Catalyst 6500 Series IDS Services Module (IDSM-2), shown in Figure 5-4. The original version of the same card was IDSM.

The IDSM-2 module works in concert with the other components to efficiently protect your data and voice infrastructure. With the increased complexity of security threats and smarter intruders, network administrators are constantly trying to stay ahead of the pace by maintaining their IP networks with high-quality network intrusion security solutions. The IDSM-2 module certainly provides this, but at a very high cost.

NOTE In today's age, though, almost any security cost is a good investment, because business continuity and keeping host systems operating is paramount to the success of most organizations. If Cisco.com were to go down and stay down due to a DoS attack, for example, Cisco would lose up to an estimated $10 million an hour in lost or delayed purchase orders.

Figure 5-4 *IDSM-2 Module*

The IDSM-2 does not have a console port. To manage and configure the IDSM-2, you issue the following command from the Cisco Catalyst 6500 Series Supervisor Engine:

```
session module-number
```

For example:

```
session 8
```

The default password for the administrator account is *cisco*. The username is *cisco*. The default password should be changed as soon as possible.

The Cisco IDSM-2 offers many Security features and benefits, for further details please visit

http://cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09186a00801e55dd.html

CiscoWorks VMS

CiscoWorks VPN/Security Management Solution (VMS) is core management software that provides a centralized means of defining and distributing security policies, providing patches and software updates, and ensuring communication with all agents. A Cisco Security Agent is defined as an endpoint software device that resides on servers or desktops/laptops and autonomously enforces local policies that prevent attacks.

CiscoWorks VMS is an integral part of the SAFE Blueprint. The following are some of the devices it maintains:

Virtual private networks (VPNs)

- Firewalls
- Network-based IDS (NIDS)
- Host-based IDS (HIDS)
- Monitoring

CiscoWorks VMS addresses the needs of both small- and large-scale VPN and security deployments, and enables organizations to protect productivity gains and reduce operating costs.

CiscoWorks VMS provides the following tools for management of IDS appliances:

- Firewall management
- CiscoWorks Auto Update Server
- Network IDS management
- Host IPS management
- VPN router management
- Security monitoring
- VPN monitoring
- Operational management

NOTE The written exam does not currently test the candidate's knowledge of this product. For more details on VMS, go to http://www.cisco.com/go/vms and http://cisco.com/en/US/products/sw/cscowork/ps2330/products_data_sheet09186a0080092536.html.

The Agent Manager is an integral part of the CiscoWorks VMS. The CiscoWorks Management Center for Cisco Security Agents is a featured component within the VMS.

There are some excellent articles on the Management Center for Cisco Security Agents at http://cisco.com/en/US/products/sw/cscowork/ps5212/index.html.

Cisco VPN 3000 Concentrator

The Cisco VPN 3000 Series Concentrators are purpose-built, remote access virtual private network (VPN) platforms that incorporate high availability, high performance, and scalability with the most advanced encryption and authentication techniques available today. The VPN 3000 supports a number of secure protocols:

- IP Security (IPSec)
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP) over IPSec
- Cisco WebVPN (SSL)

The Cisco VPN 3000 Series Concentrator supports the widest range of connectivity options, including WebVPN (clientless using a web browser), the Cisco Secure VPN Client, Microsoft L2TP/IPSec, and Microsoft PPTP.

Figure 5-5 displays a VPN 3000 Concentrator, front view.

Figure 5-5 *VPN 3000 Concentrator, Front View*

The VPN Concentrator is designed to terminate IPSec connections over a public domain such as the Internet. The placement of the VPN Concentrator is crucial for any network security engineer. Cisco makes a number of recommendations in its SAFE Blueprint, but in general requires that the VPN Concentrator be located behind a Cisco PIX Firewall on the inside interface where the DMZ is located. The Cisco SAFE Blueprint has a number of recommendations based on network size and appliances, though. See http://www.cisco.com/safe for the latest details.

There are currently six different VPN Concentrator models that you can purchase from Cisco. The following list details the hardware specifications of the models (reprinted from http://cisco.com/en/US/partner/products/hw/vpndevc/ps2284/products_data_sheet09186a00801d3b56.html):

- **Cisco VPN 3005 Concentrator**—The Cisco VPN 3005 Concentrator is a VPN platform designed for small- to medium-sized organizations with bandwidth requirements up to full-duplex T1/E1 (4 Mbps maximum performance) with support for up to 200 simultaneous IPSec sessions or 50 simultaneous clientless sessions. Encryption processing is performed in software. The Cisco VPN 3005 does not have built-in upgrade capability.

- **Cisco VPN 3015 Concentrator**—The Cisco VPN 3015 Concentrator is a VPN platform designed for small- to medium-sized organizations with bandwidth requirements up to full-duplex T1/E1 (4 Mbps maximum performance) and up to 100 simultaneous IPSec sessions or 75 simultaneous clientless sessions. Like the Cisco VPN 3005, encryption processing is performed in software, but the Cisco VPN 3015 is also field-upgradeable to the Cisco VPN 3030 and 3060 models.

- **Cisco VPN 3020 Concentrator**—The Cisco VPN 3020 Concentrator is a VPN platform designed for medium to large organizations with bandwidth requirements from full T1/E1 through T3/E3 (50 Mbps maximum performance) with support for up to 750 simultaneous IPSec sessions or 200 simultaneous clientless sessions. Specialized SEP modules (SEP-E) perform hardware-based acceleration. The Cisco VPN 3020 cannot be upgraded to other products in the family. Redundant and nonredundant configurations are available.

- **Cisco VPN 3030 Concentrator**—The Cisco VPN 3030 Concentrator is a VPN platform designed for medium to large organizations with bandwidth requirements from full T1/E1 through T3/E3 (50 Mbps maximum performance) with support for up to 1,500 simultaneous IPSec sessions or 500 simultaneous clientless sessions. Specialized SEP modules perform hardware-based acceleration. The Cisco VPN 3030 can be upgraded to the Cisco VPN 3060 in the field. Redundant and nonredundant configurations are available.

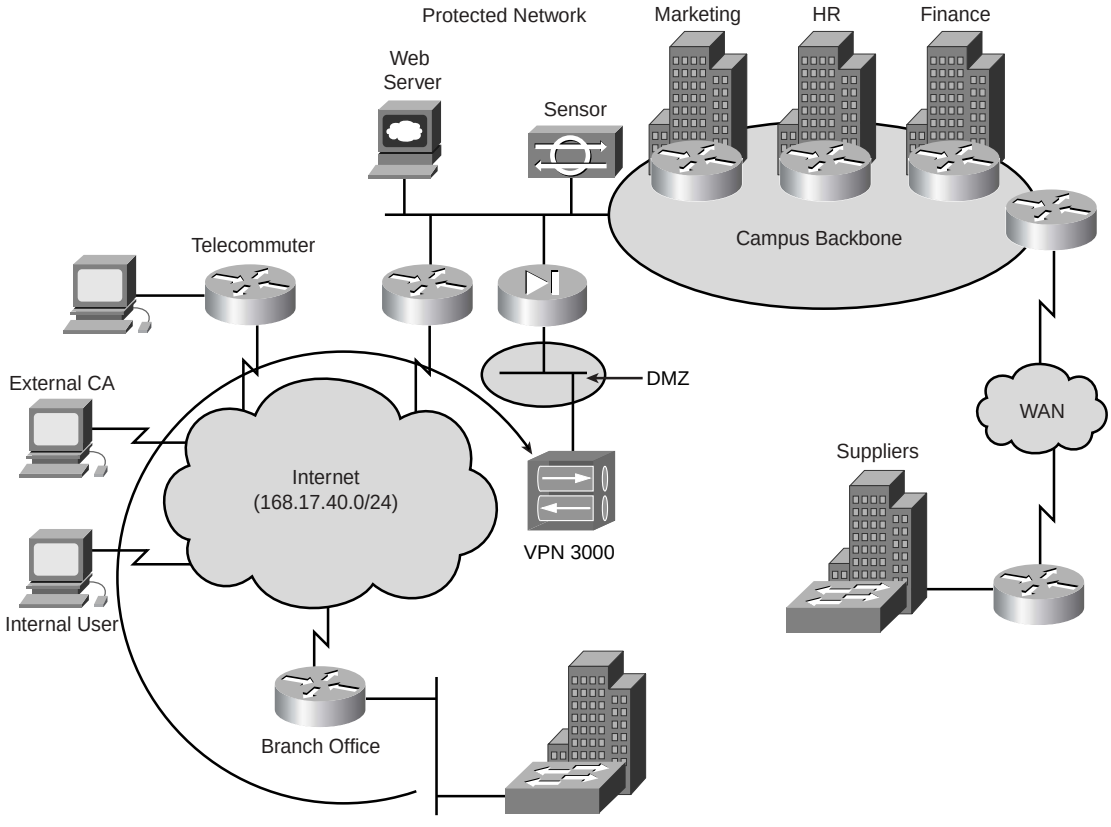
- **Cisco VPN 3060 Concentrator**—The Cisco VPN 3060 is a VPN platform designed for large organizations demanding the highest level of performance and reliability, with high-bandwidth requirements from fractional T3 through full T3/E3 or greater (100 Mbps maximum performance) with support for up to 5,000 simultaneous IPSec sessions or 500 simultaneous clientless sessions. Specialized SEP modules perform hardware-based acceleration. Redundant and nonredundant configurations are available.

- **Cisco VPN 3080 Concentrator**—The Cisco VPN 3080 Concentrator is optimized to support large enterprise organizations that demand the highest level of performance combined with support for up to 10,000 simultaneous IPSec sessions or 500 simultaneous clientless sessions. Specialized SEP modules perform hardware-based acceleration. The VPN 3080 is available in a fully redundant configuration only.

Figure 5-6 displays a complex network whereby users from many different locations, such as Internet cafes, remote branch offices, and telecommuters using wireless networks, need to gain access to the campus network.

To configure the VPN Concentrator, you have two methods: via the CLI or via the web. The web is the preferred management option. This section shows how to configure a VPN 3000 Concentrator for typical settings to allow telecommuters access to the corporate network.

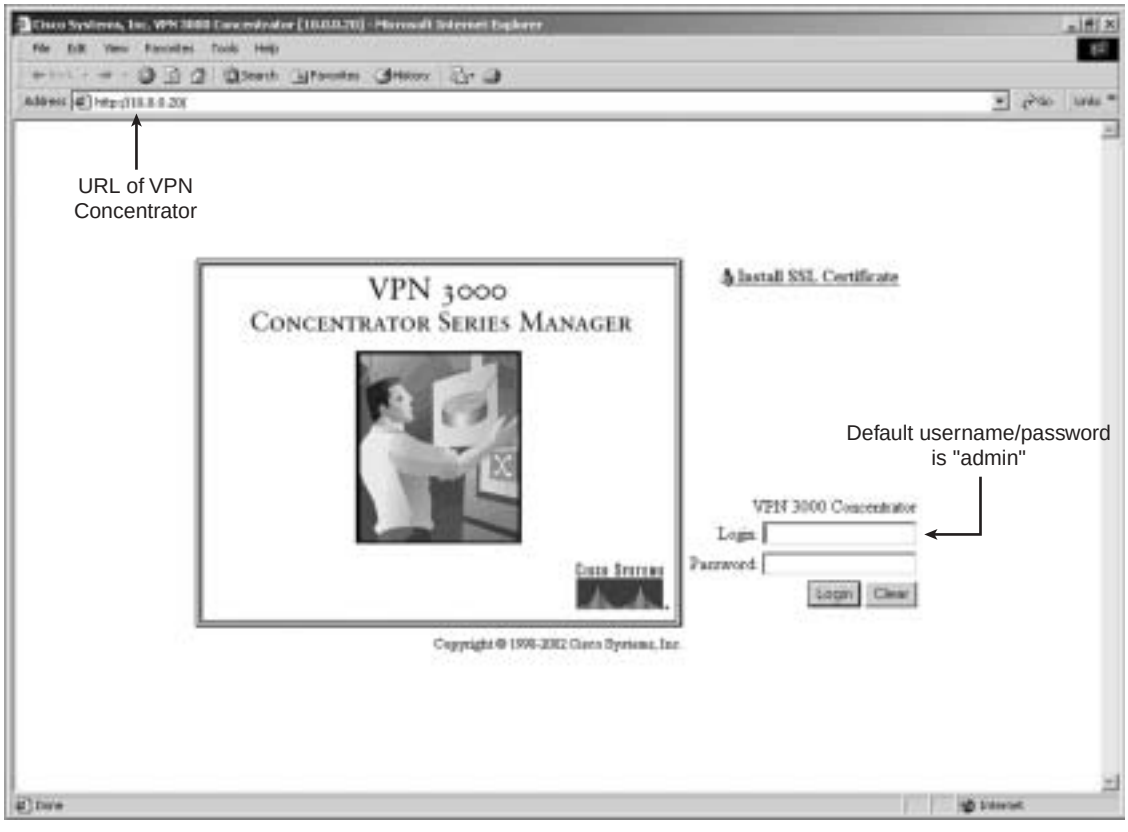
Figure 5-6 *Placement of a VPN Concentrator*



NOTE The lab exam will *not* have any preconfiguration on any security appliances, including VPN 3000. This means candidates need to be aware of how to configure a VPN 3000 out of the box. Use the CLI (console) to initialize (bootstrap). Review Chapter 8 for VPN 3000 configuration and ensure that you also have CLI console experience for the lab. The written exam does not require a candidate to be an expert with the CLI.

Figure 5-7 displays an HTML session to a VPN Concentrator.

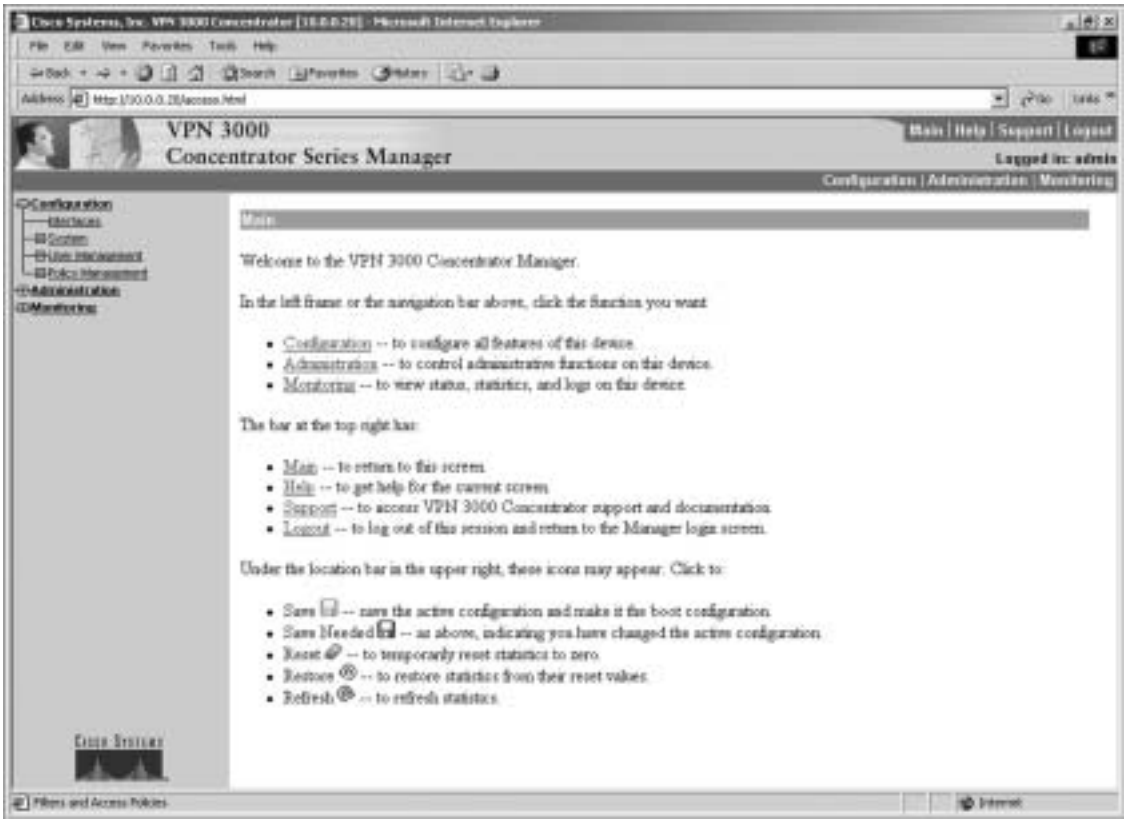
Figure 5-7 *VPN Concentrator Configuration Login Page*



By using the default username/password pair of admin, the configuration screen is displayed next. Figure 5-8 displays the home configuration page for a VPN 3000.

Figure 5-8 displays Configuration, Administration, and Monitoring navigation text in the upper-left corner. The VPN 3000 Concentrator is a favorite topic of the lab exam. There are numerous examples and screen shots on how the VPN 3000 is configured at Cisco.com to help you study for the lab exam.

Figure 5-8 *VPN Concentrator Configuration Home Page*



Consider an example of a typical VPN 3000 Concentrator configuration that allows remote telecommuters access to the campus network. The telecommuter in Figure 5-6 is attempting to connect to the corporate backbone via a Cisco Secure VPN Client on a PC. To connect, the telecommuter user must install the Cisco Secure VPN Client. (You can use other clients—for example the Windows IPSec client—but for the exam, the only tested mechanism is the Cisco Secure VPN Client. The next section covers the Cisco Secure VPN Client and configuration.) The Windows IPSec client is only supported using L2TP over IPSec.

Prior to allowing VPN terminations, the VPN Concentrator must be configured for IP and polices. Figure 5-9 displays the first configuration step, in which the interfaces are assigned an IP.

Figure 5-9 *Concentrator Interface Screen*

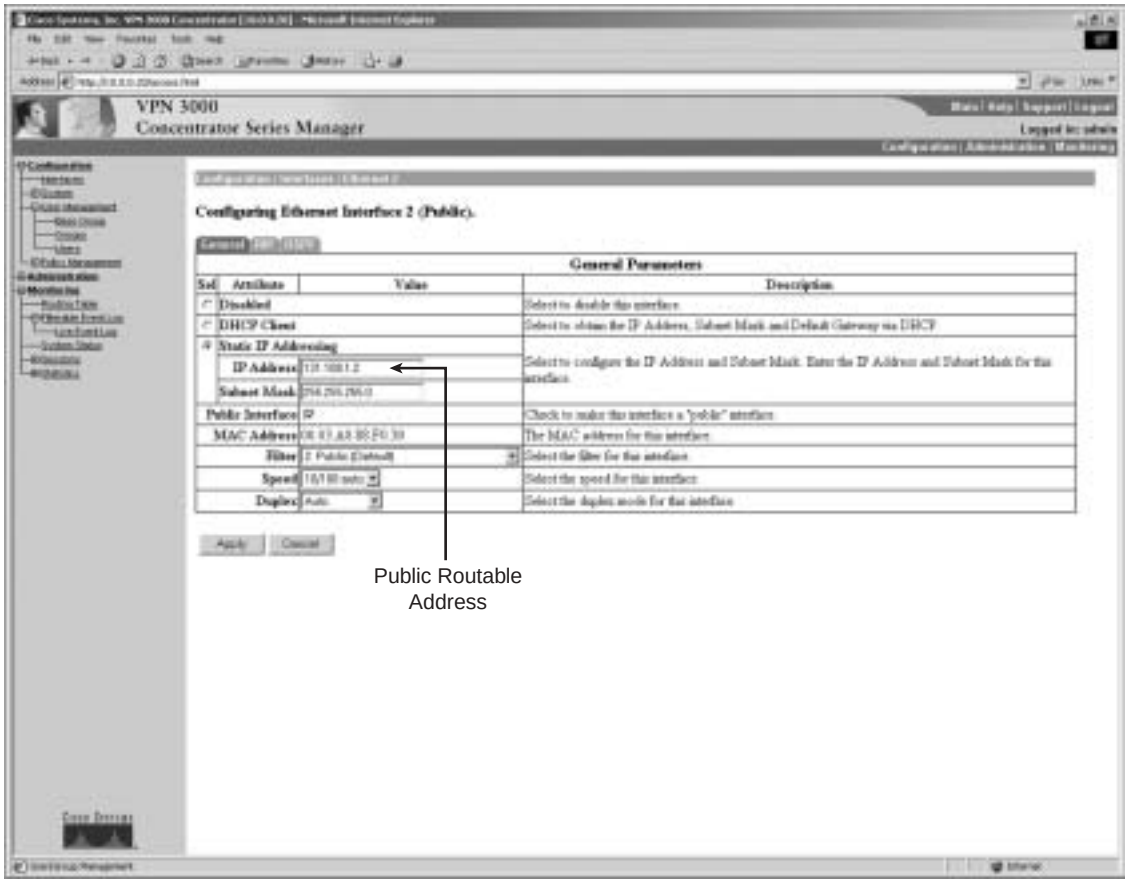


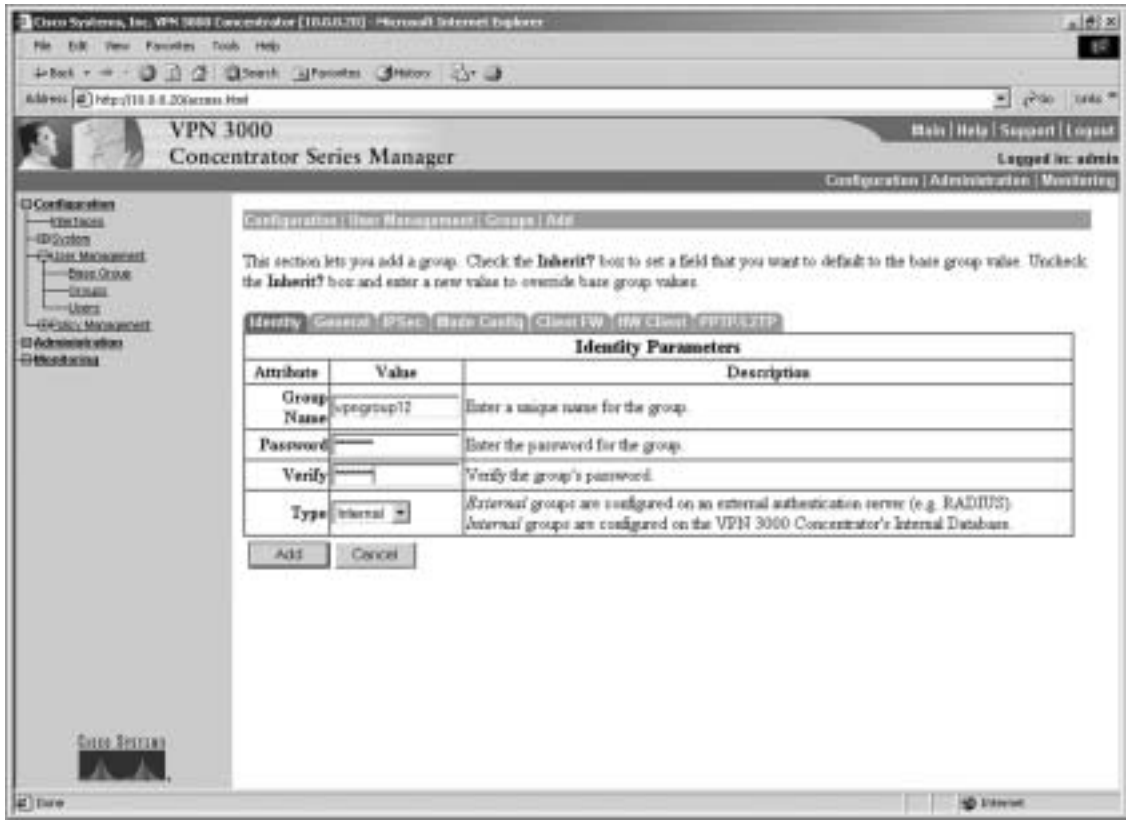
Figure 5-9 shows how to assign the static public IP address 131.108.1.2. You can also set the speed and the mode of the interface on that screen. The other remaining options are left at their default settings for this example.

Now you have to perform the same steps for the private interface.

Once the interfaces are configured, you have to add a group and a user to the Concentrator. To do this, choose **Configuration > User Management**. Choose **Groups**, because you have to define a group before you can add users to that group. Figure 5-10 displays this configuration step. When you configure the VPN Client in the next section, it will be a lot clearer why Groups are important.

The dialog box in Figure 5-10 has several tabs. You will configure the first three tabs, Identity, General, and IPSec.

Figure 5-10 *Concentrator Group Screen*



The option group password in Figure 5-10 is also the shared key that the client uses to log into the Concentrator. You also have to define the type of authentication that is used for this group. Users can be authenticated via the following four methods:

- RADIUS servers
- Windows NT domain controllers
- Concentrator internal server
- SecureID

In this example, you use the internal VPN 3000 server authentication database, so the next step is to add a user to the Concentrator on the internal server.

Figure 5-11 displays the network administrator selecting the General tab.

Figure 5-11 *Concentrator Group Screen, General Tab*

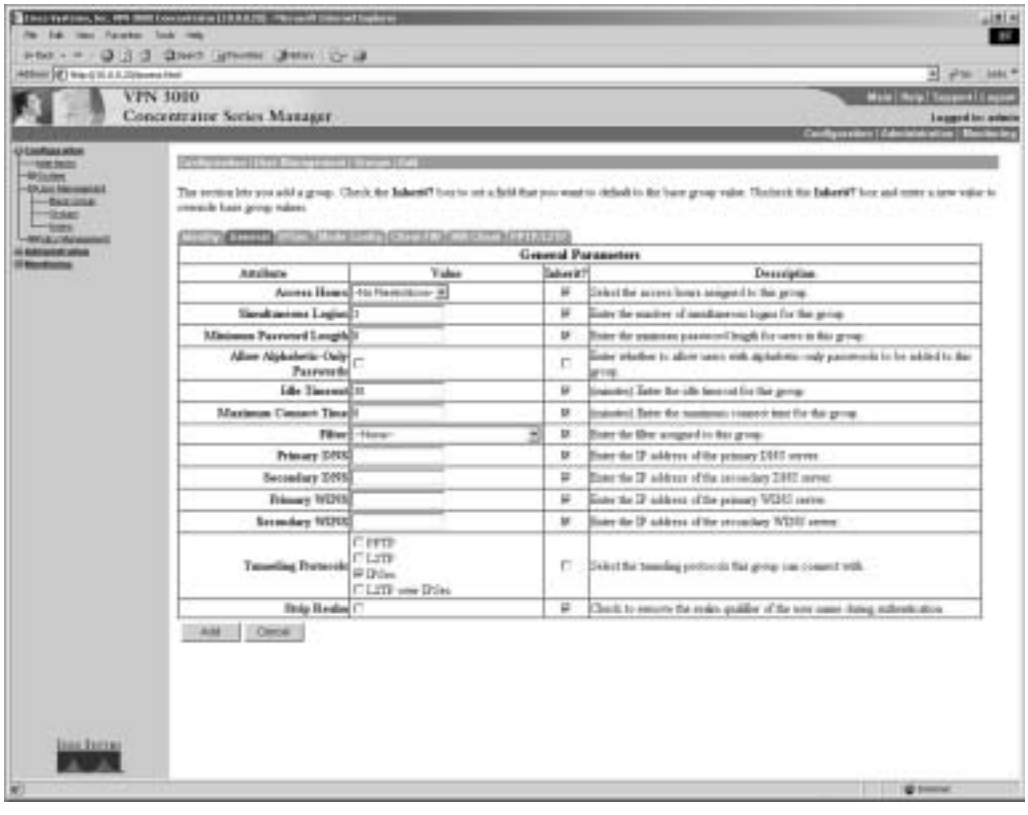


Figure 5-11 displays a number of configurable options:

- **Access Hours**—Selected from the drop-down menu, this attribute determines when the Concentrator is open for business for this group. It is currently set to No Restrictions, but you could also select Never, Business Hours (9 a.m. to 5 p.m., Monday through Friday), or a named access hour range that you created elsewhere in the VPN Manager.
- **Simultaneous Logins**—The default is 3, and the minimum is 0. There is no upper limit, but security and prudence would suggest that you limit this value to 1.
- **Minimum Password Length**—The allowable range is 1 to 32 characters. A value of 8 provides a good level of security for most applications.
- **Allow Alphabetic-Only Passwords**—Notice that the box has been unchecked. The default is to allow alphabetic-only passwords, which is a security risk. This value has been modified.

- **Idle Timeout**—30 minutes is a good value here. The minimum allowable value is 1, and the maximum is a value that equates to more than 4,000 years. Zero disables idle timeout.
- **Maximum Connect Time**—Zero disables maximum connect time. The range here is again 1 minute to more than 4,000 years.
- **Filter**—A filter applies its rules to data packets coming through the system, in the order the rules are arranged on the filter.
- **Primary/Secondary DNS/WINS**—These have been modified from the base group's default settings.
- **Tunneling Protocols**—IPSec has been selected, but you could allow the group to use PPTP, L2TP, and L2TP over IPSec as well.
- **Strip Realm**—The default operation of the VPN Concentrator verifies users against the internal database using a combination of the username and realm qualifier, as in *username@group*. The *@group* portion is called the realm.

Once these options are configured, the final page you need to configure covers the IPSec parameters. Figure 5-12 displays a sample configuration.

Figure 5-12 *Concentrator Group Screen, IPSec Tab*

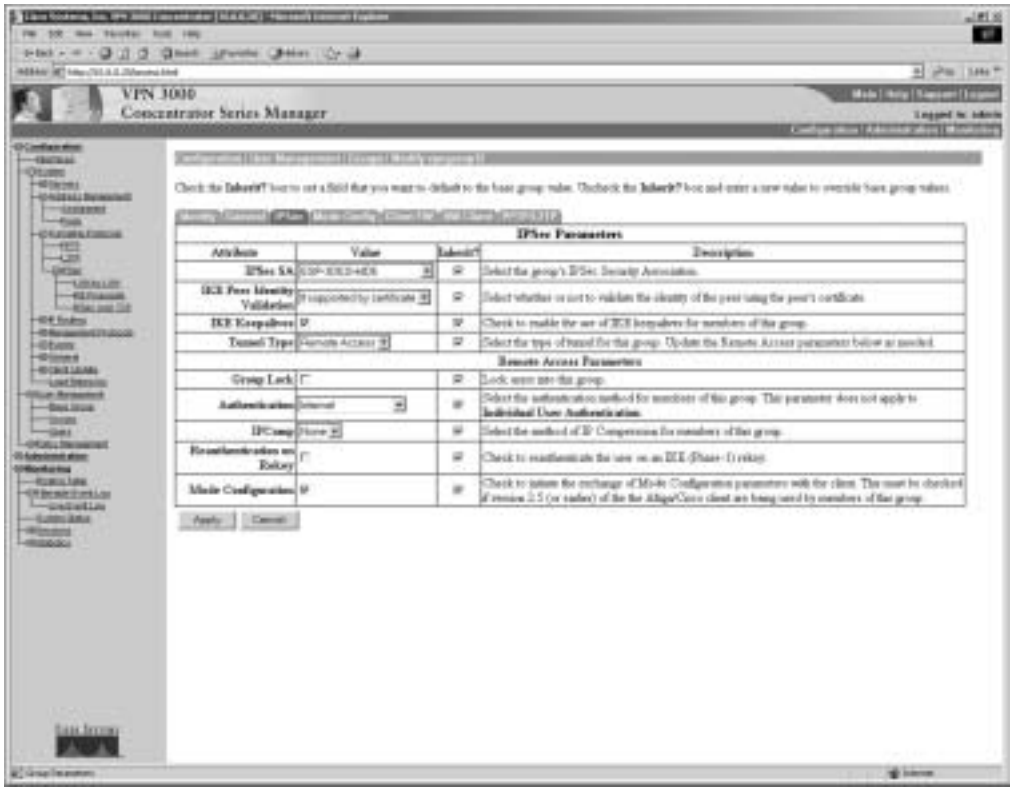


Figure 5-12 has a number of configurable options:

- **IPSec SA**—For remote-access clients, you must select an IPSec Security Association (SA) from this list of available combinations. The client and server negotiate an SA that governs authentication, encryption, encapsulation, key management, and so on based on your selection here. These are the default selections supplied by the VPN Concentrator:
  - **None**—No SA assigned.
  - **ESP-DES-MD5** —This SA uses DES 56-bit data encryption for both the IKE tunnel and IPSec traffic.
  - Other options include ESP/MD5/HMAC-128, MD5/HMAC-128, ESP-3DES-MD5, ESP/IKE-3DES-MD5, ESP/MD5/HMAC-128, ESP-3DES-NONE, ESP-L2TP-TRANSPORT, ESP/MD5/HMAC-128, and ESP-3DES-MD5-DH7. DH refers to the Diffie-Hellman algorithm.
- **IKE Peer Identity Validation**—This option applies only to VPN tunnel negotiation based on certificates. This field enables you to hold clients to tighter security requirements.
- **IKE Keepalives**—This option monitors the continued presence of a remote peer and notifies the remote peer that the Concentrator is still active. If a peer no longer responds to the keepalives, the Concentrator drops the connection, preventing hung connections that could clutter up the Concentrator.
- **Tunnel Type**—You can select either LAN-to-LAN or Remote Access as the tunnel type.
- **Group Lock**—Checking this field forces the user to be a member of this group when authenticating to the Concentrator.
- **Authentication**—This field selects the method of user authentication to use. The available options are as follows:
  - **None**—No user authentication occurs. Use this with L2TP over IPSec.
  - **RADIUS**—Uses an external RADIUS server for authentication.
  - **RADIUS with Expiry**—Uses an external RADIUS server for authentication. Applied to allow Microsoft as the Client-Vendor to get support for the Microsoft Vendor-Specific Attributes (VSA).
  - **NT Domain**—Uses an external Windows NT Domain system for user authentication.
  - **SDI**—Uses an external RSA Security, Inc. SecureID system for user authentication.
  - **Internal** (option selected)—Uses the internal VPN Concentrator authentication server for user authentication.

- **IPComp**—Permits the use of the LZS compression algorithm for IP traffic.

Finally, to permit users to authenticate to the VPN Concentrator, you must create users. Figure 5-13 displays the user configuration page.

Figure 5-13 *Concentrator User Screen*

In Figure 5-13, the user "gschauwe" and a password (hidden) are configured. The user is then assigned to the group you previously made (vpngroup12). You must then click the **Apply** button to make the changes take effect. Now that the VPN Concentrator is ready to terminate VPN IPSec tunnels, you simply need to enable the clients on the end workstations, namely by configuring the

VPN Client. The next section covers the end-station client configuration using the Cisco Secure VPN Client.

NOTE To be a real expert, rather than just pass the written exam, you are encouraged to research more details on the Cisco VPN Concentrator at http://www.cisco.com/security/ and in Chapter 8 of this book.

Cisco Secure VPN Client

The Cisco Secure VPN Client is a low-cost application available to the Internet community. You may need to purchase a license at a minimal cost. The VPN Client is free when you buy a VPN gateway and support contract, and is included with all models of Cisco VPN 3000 Series Concentrators and most Cisco PIX 500 Security Appliances. Customers with Cisco SMARTnet support contracts and encryption entitlement may download the Cisco Secure VPN Client from the Cisco Software Center at no additional cost.

The Cisco Secure VPN Client allows for an IPSec termination to Cisco VPN Concentrators. Additionally, the VPN Client supports:

- Dynamically pushed VPN-policy configuration on a per-group basis, which eliminates the need for manual client configuration
- Internal IP addresses, primary and secondary Windows Internet Name Service (WINS), and Domain Name System (DNS)
- Split-tunnel or no-split-tunnel options on a per-group basis
- Policy-database support either locally on the router or via RADIUS
- Authentication of users via extended authentication
- The latest revisions of the mode configuration and extended authentication IKE extensions

Once the application is installed on the operating system platform, you then start the VPN Client by clicking **Start > Programs > Cisco Systems VPN Client > VPN Dialer**.

Note for Version 4.x the path is **Start > Programs > Cisco Systems VPN Client > VPN Client**.

For Microsoft Windows platforms, this brings you to the screen shown in Figure 5-14.

Figure 5-14 *Cisco Secure VPN Client*

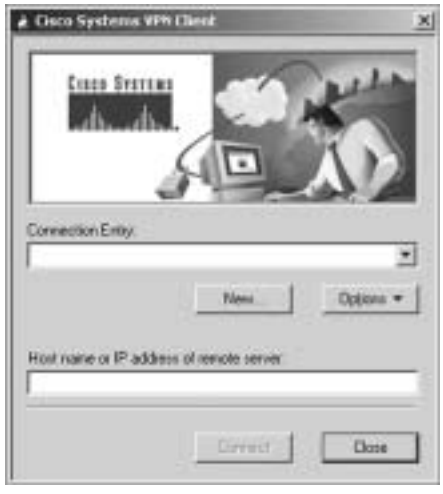


Figure 5-14 displays a blank connection; by clicking the New button, you are presented with configurable options. Figure 5-15 displays the first of these options.

Figure 5-15 *Cisco Secure VPN Client Configurable Options*

The IP address you enter in Figure 5-15 is that of the publicly routable address. In this scenario, that IP address is 131.108.1.2 (see Figure 5-9).

Finally, you need to define the groups. Figure 5-16 configures the VPN Group (vpngroup12) to match the setting configured on the VPN Concentrator (see Figure 5-10).

Figure 5-16 *Cisco Secure VPN Client Group Options*

For completeness, you should also read about the Cisco VPN Hardware Client. Details can be found at http://cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a0080094cf8.shtml. The VPN Hardware Client is a feature available to the PIX Firewalls and is used to create an IPSec tunnel with a VPN 3000 Concentrator. This is a task you will surely be asked to complete in the CCIE Security lab exam.

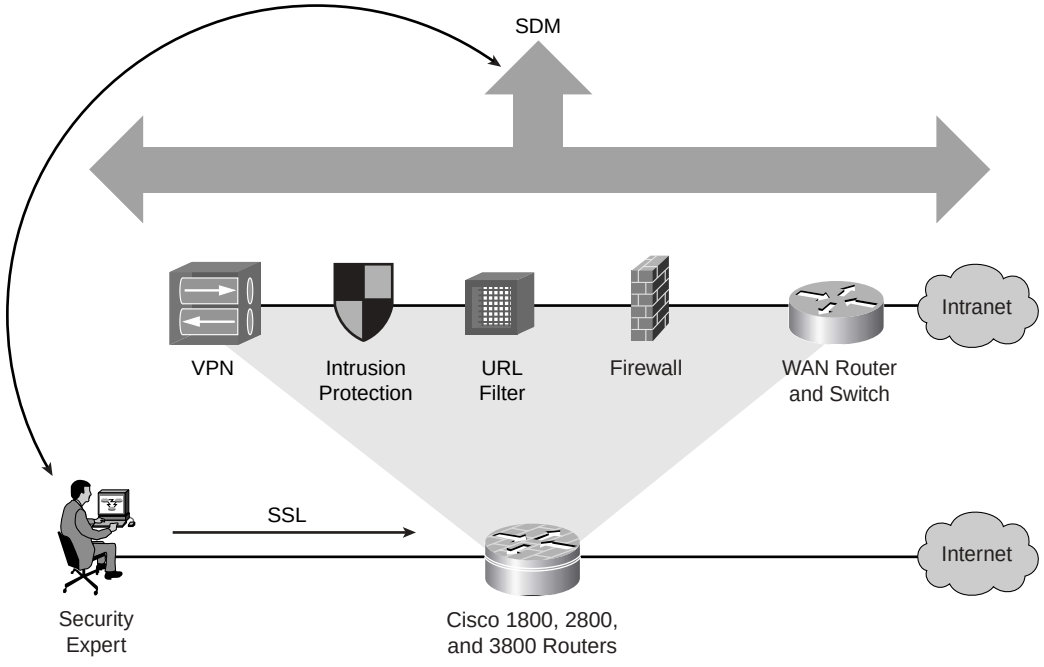
Cisco Router and Security Device Manager

Cisco Router and Security Device Manager (SDM) is an intuitive, secure, web-based embedded device manager of Cisco IOS–enabled devices. SDM provides intelligent wizards, detects misconfigured devices, steps security managers through firewall and VPN configurations, and has been certified and recommended by some key organizations within Cisco, such as the Cisco Network Supported Accounts (NSA), a group of expert engineers within Cisco whose services are sold to high-end clients.

SDM is the TAC recommended method to install and configure security. Figure 5-17 displays the features supported by SDM on a Cisco IOS–enabled router.

The router in Figure 5-17 connected to the Internet in a typical example of today's complex networks can be configured for IP routing, acts as LAN switch, terminates IPSec VPN, performs stateful firewall and IDS duties, and acts as a WAN backup. To configure such a complex device, SDM provides the key to simplifying the configuration process. The network security manager uses the SSL application protocol to secure the connection.

Figure 5-17 *SDM All-in-One Web Tool*



Cisco SDM is currently shipping in Cisco IOS and on the Cisco 1800, 2800, and 3800 Series Integrated Service Routers (ISR). Cisco SDM is also available with firewall appliances such as the PIX Firewall (PIX version is called the PIX Device Manager [PDM]). The ISR platforms are implemented only on Cisco hardware, and no other vendor in the marketplace today can match the same functionality. SDM is also supported on legacy platforms such as the 1700 and 3600/3700 series routers.

NOTE You can certainly expect that CCIE Security lab candidates will soon be configuring routers such as the ISR 3800 instead of the legacy 2600 and 3700 routers in place today.

Cisco SDM is an enhancing tool for both network and security administrators. Cisco SDM is available at http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm. SDM 2.0 is currently the most recent version; 2.1 is due for release in 2004.

SDM provides embedded services management of routing and switching, security, and QoS. SDM is web-based and ships on all new routers.

By simply typing in the IP address of the Cisco IOS–enabled router, the administrator will be presented with the SDM home page (administrators will use https://*ip-address* with their web client).

The SDM home page displays a typical router, such as the popular 1721, the DRAM memory size (64 MB), total Flash (16 MB), and SDM version, to name a few of the most critical details of this particular router.

SDM provides a number of excellent features:

- **Intelligent Wizards**—Auto-detect misconfigurations with proposed fixes
- **1-Step Router Lockdown**—Securing devices allowing ease of use to ensure devices are not compromised.
- **1-Step VPN and Firewall**—Including tools for expert users such as an ACL editor and VPN tunnel quality monitoring
- **Security Audit**—NSA, ICSA, TAC recommended security configuration

The Security Audit option, for example, provides details on configuration problems and suggestions to fix security deficiencies. With a single click, the network security manager can control Telnet and SSH access within the Security Audit.

The following is a description of the major SDM Wizard Mode options:

- **Overview**—View IOS version, hardware installed, and configuration summary.
- **LAN Configuration**—Configure the LAN interfaces and DHCP.
- **WAN Configuration**—Configure PPP, Frame Relay, and HDLC WAN interfaces.
- **Firewall**—Two types of firewall wizards are simple inside/outside or more complex inside/outside/DMZ with multiple interfaces.
- **VPN**—Three types of wizards to create a secure site-to-site VPN, Easy VPN, and GRE tunnel with IPSec.
- **Security Audit**—Perform a router security audit and get easy instructions on how to lock down the insecure features found.
- **Reset**—Restore to factory default settings.

SDM is a core application loaded in Cisco IOS and needs to be loaded into the system Flash to allow security managers to quickly install routers as well.

You are encouraged to view more details at Cisco.com. At the time of writing this book, Cisco announced SDM version 2.1 for the year ending 2004. More details on SDM can be found as follows:

- **Latest SDM-related product information**—http://www.cisco.com/go/sdm
- **SDM primary features and benefits**—http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_data_sheet0900aecd800fd118.html

Security Information Monitoring System

This section covers how Cisco IDS can monitor and identify intruder-based attacks and how security information is monitored and acted upon.

Cisco IDS uses multilayer protection options to prevent an attack from successfully reaching the end target system such as a file server or desktop computer. After the attack or intruder-based traffic is identified and determined to be intrusive, the network administrator can stop the attack before any serious damage occurs. This can involve dropping the packet, resetting the TCP session (terminating the session), modifying real-time ACLs on routers and switches, or dynamically modifying the firewall policy to shun (stop) the intruder.

Analyzing the log files can be a daunting task for any security expert. Cisco IDS 4.0 and above now provides a more detailed information database about the alarms triggered, providing the user with forensics data and advanced analysis data to simplify the support process.

The scenario at the end of this chapter details a typical attack scenario and how to decipher the details provided. This is the best method to demonstrate the capabilities of the IDS sensors, and the exam performs the same testing procedures on candidates. CCIE Security candidates can expect to be given similar scenarios and asked to answer questions based on the information provided.

Foundation Summary

The "Foundation Summary" is a condensed collection of material for a convenient review of this chapter's key concepts. If you are already comfortable with the topics in this chapter and decided to skip most of the "Foundation Topics" material, the "Foundation Summary" will help you recall a few details. If you just read the "Foundation Topics" section, this review should help further solidify some key facts. If you are doing your final preparation before the exam, the "Foundation Summary" offers a convenient and quick final review.

The following list summarizes the features of Cisco Secure for NT Windows:

- Supports centralization of AAA access for all users, including routers and firewalls.
- Can support a number of network access servers and is limited purely by load. The practical limit for a single Cisco Secure ACS authenticating against all its databases, internal and external, is 300,000 to 500,000 users.
- Can manage Telnet access to routers and switches.
- Supports many different Cisco platforms, including access servers and routers.

Table 5-2 *Cisco Secure IDS Components*

Component	Meaning
Cisco Secure IDS Sensor	High-speed device that analyzes the contents of data being transported across a network and determines whether that traffic is authorized or unauthorized. Unauthorized traffic includes ping requests from intruders.
Cisco IDS Device Manager	Provides real-time response to intruders in the network by blocking access to the network and terminating any active data sessions. The IDM collects the real-time information from the sensor.

The following summarizes the Cisco VPN/Security Management Solution (VMS) capabilities:

- Manage VPNs
- Manage firewalls
- Manage network-based IDSs
- Manage host-based IPSs
- Monitor security

Table 5-3 *IDS Terminology*

Term	Description
False positive (benign trigger)	Occurs when the IDS reports certain benign activity as malicious, requiring human intervention to diagnose the event.
False negative	Can occur when the IDS sensor does not detect and report a malicious activity, but the system allows it to pass as nonintrusive behavior. This can be catastrophic for network operation and therefore minimizing false negatives is the highest priority.
True positive	The opposite of a false negative. In this case, an alarm has been correctly sent in response to malicious activity. These alarms cause the most concern for a network administrator.
True negative	Not an actual alarm but rather a situation in which the IDS in place does not trigger an alarm for activity permitted within a network.

Table 5-4 *IDS Tuning*

Step	Description
1	Identify potential locations for sensors
2	Apply an initial configuration
3	Monitor the sensor while tuning
4	Analyze alarms, tune out false positives, and implement signature tuning (if needed)
5	Selectively implement response actions
6	Update sensors with new signatures

Q & A

The Q & A questions are designed to help you assess your readiness for the topics covered on the CCIE Security written exam and those topics presented in this chapter. This format should help you assess your retention of the material. A strong understanding of the answers to these questions will help you on the CCIE Security written exam. You can also look over the questions at the beginning of the chapter again for further review. As an additional study aid, use the CD-ROM provided with this book to take simulated exams, which draw from a database of over 500 multiple-choice questions.

Answers to these questions can be found in Appendix A, "Answers to Quiz Questions."

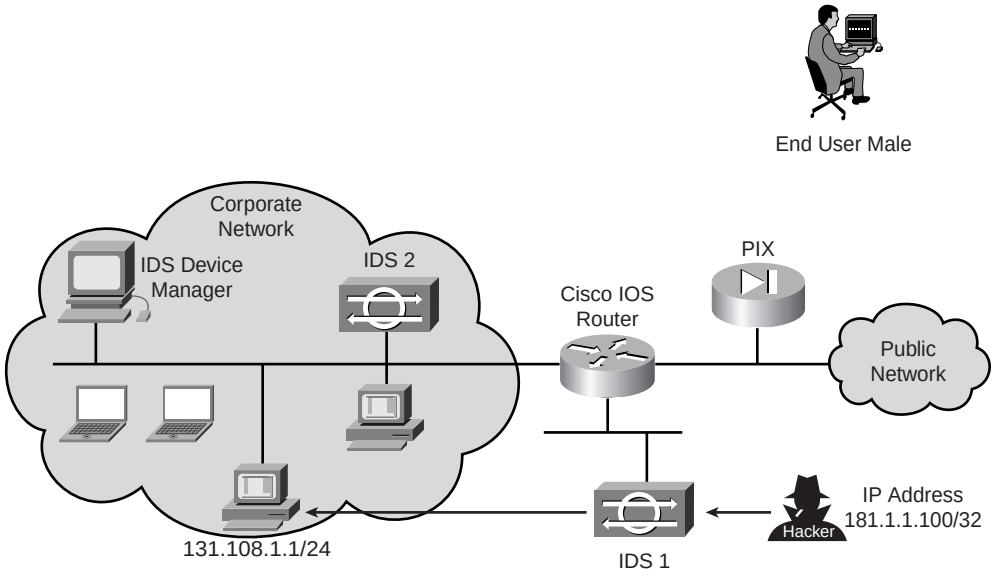
1. Define the terms Cisco Secure IDS Sensor and IDS Device Manager and explain their uses.
2. What LAN interfaces can be supported on a Cisco IDS Device Manager?
3. What is the default username and password combination for a Cisco IDSM?
4. What is the default username and password combination for a Cisco VPN 3000 Concentrator?
5. What are three typical forms of attacks that are committed by unauthorized individuals?
6. What is the function of the signature-based IDS?

Scenario

Scenario: Cisco Secure IDS Database Event

Figure 5-18 displays a typical network under attack from an intruder trying to destabilize the network host with the IP address 131.108.1.1/24.

Figure 5-18 *Sample IDS Event*



The security manager has e-mailed to you several files. The first is TCPDUMP output details. TCPDUMP is a powerful tool that allows you to sniff network packets and make some statistical analysis out of those dumps. (The written exam has a few questions based on the output from this program.) The manager also e-mailed to you log files taken from an IDS Sensor database and the logging entries from the Cisco IOS router.

You receive these files from IDS 1 in Figure 5-18 and the Cisco WAN router and you are required to provide details on what kind of attack this is and on what TCP/UDP ports are opened to the outside world.

Example 5-1 displays the captured entries the security manager would like identified and what ports are currently opened. Note that Example 5-1 only displays traffic from the Internet host 181.1.1.100 to the inside host 141.108.1.1 to simplify the display.

NOTE The signature is not shown but you can assume a customized signature ID. Also note that Cisco IDS provides similar exported formats for viewing by security managers and administrators.

Example 5-1 *TCPDUMP Output*

```
Time        Source/Destination TCP port  Destination/Source TCP port TCP fields
>10:39:01   181.1.1.100/53 > 131.108.1.1/41000 ACK 1 Win 0 (May Defragment)
>10:39:02   181.1.1.100/53 > 131.108.1.1/41001 ACK 1 Win 0 (May Defragment)
>10:39:03   181.1.1.100/53 > 131.108.1.1/41002 ACK 1 Win 0 (May Defragment)
>10:39:04   181.1.1.100/53 > 131.108.1.1/41003 ACK 1 Win 0 (May Defragment)
>10:39:05   181.1.1.100/53 > 131.108.1.1/41004 ACK 1 Win 0 (May Defragment)
>10:39:06   181.1.1.100/53 > 131.108.1.1/51001 ACK 1 Win 0 (May Defragment)
>10:39:06   181.1.1.100/53 > 131.108.1.1/51002 ACK 1 Win 0 (May Defragment)
>10:39:06   181.1.1.100/53 > 131.108.1.1/51003 ACK 1 Win 0 (May Defragment)
>10:39:07   181.1.1.100/53 > 131.108.1.1/51003 ACK 1 Win 0 (May Defragment)
>10:39:02   181.1.1.100/80 > 131.108.1.1/21001 ACK 34000 Win 2048
>10:39:03   181.1.1.100/3176 > 131.108.1.1/31002 ACK 10000 Win 4096
>10:39:04   181.1.1.100/3279 > 131.108.1.1/51001 ACK 11235 Win 4096
```

Example 5-2 displays the suspicious activity requiring immediate forensic analysis for the host with the IP address 131.108.1.1. The logging entries on the router are displayed in Example 5-2.

Example 5-2 *Log File Entry*

```
%IDS-4-TCP_FRAG_SYN_FIN_SIG: Sig:3043:Fragmented SYN/FIN Packet - from
 [181.108.1.100] to [131.108.1.1]
%IDS-4-TCP_SYN_ATTACK_SIG: Sig:3050:Half-Open Syn Flood - from
 [181.1.1.100] to [131.108.1.1]
```

Scenario Answers

Scenario Solutions

Based on Example 5-1, you can clearly identify ports that are open and closed by the Acknowledgement number and agreed TCP windows sizes. When TCP negotiates a session, the first acknowledgement is typically a random value and an Acknowledgment of 1 is extremely suspicious. Typically, window devices, for example, calculate a random number much higher than 1. When the window size is zero, that means the TCP window size parameter has *not* been negotiated. In other words, the connection is not permitted. Example 5-3 displays port 53 as being unauthorized or closed as the window size is 0.

Example 5-3 *TCP Closed Ports (TCPDUMP Output)*

```
>10:39:01    181.1.1.100/53 131.108.1.1/41000 ACK 1 Win 0 (May Defragment)
```

Example 5-4 displays the open and active sessions as the window sizes have been negotiated and there are active segments. TCP ports 80, 3178, and 3179 are opened by the firewall in this organization and passed through the IDS.

Example 5-4 *Open TCP Ports*

```
>10:39:02    181.1.1.100/80 131.108.1.1/21001 ACK 34000 Win 2048
>10:39:03    181.1.1.100/3176 131.108.1.1/31002 ACK 10000 Win 4096
>10:39:04    181.1.1.100/3279 131.108.1.1/51001 ACK 11235 Win 4096
```

Example 5-2 displays a single TCP fragment packet between the outside host with the IP address 181.1.1.100 to the inside routable address 131.108.1.1. This error message indicates a single fragmented TCP packet with the SYN and FIN flags set. This action is indicative that a reconnaissance sweep of your network is in progress. This type of packet indicates an attempt to conceal the TCP port sweep (port 53 in this case, DNS). This may be the prelude to a more serious attack. The security engineer is well advised to immediately note the action and log into Cisco.com and search for the recommended action. For example, you could perform the following actions:

Step 1 Note the Signature IDs. In Example 5-2, they are 3043 and 3050.

Step 2 Open an Internet browser.

Step 3 Go to http://www.cisco.com/pcgi-bin/front.x/ipsalerts/ipsalertsHome.pl or search for the latest database of IPS signature IDs.

Step 4 Click the List Signatures by Signature ID link (Cisco.com password required).

Step 5 Locate the signature number following Sig:, 3043 in Example 5-2, in the error message text for more information on the nature of the error and corrective actions to perform.

The log message regarding the TCP half-open connections is another suspicious packet requiring immediate attention. In this case the number of half-open TCP connections has exceeded the high-water mark. There are no known sources that would legitimately generate this traffic pattern, so it is regarded as a form of attack. The recommended action in this case is to block the resource IP address during the course of the investigation to ensure network resources are not depleted and stop legitimate TCP session (that is valid data connections from valid users) becoming active. This sort of attack can be considered a denial of service attack.

Hopefully this simple scenario has shown you the power of the details provided by IDS-enabled devices, the ease of using these devices, and the powerful search engines available at Cisco.com. The error messages are somewhat intuitive and if you come across a difficult question in the exam make sure you apply a commonsense approach. Obviously you will not have Internet access during the exam, so it is safe to assume Cisco will not test your knowledge of every obscure signature or scenario out there, but some common examples are presented in this simple scenario.

Exam Topics in This Chapter

- Concepts—security best practices
- Packet filtering
- Cisco PIX and IOS authentication proxies
- Port Address Translation (PAT)
- Network Address Translation (NAT)
- Firewalls
- Content filters
- Public Key Infrastructure (PKI)
- Authentication technologies
- Authorization technologies
- Virtual private networks (VPNs)
- Network IDS anomaly, signature, passive, inline
- Host intrusion prevention
- Cisco Threat Response
- Cisco Secure PIX Firewall
- Cisco IOS Firewall feature set

You can find a list of all of the exam topics in the introduction to this book. For the latest updates on exam topics, visit Cisco.com.

CHAPTER 6

Security Technologies

This chapter covers some of today's most widely used technologies that enable network administrators to ensure that sensitive data is secured from unauthorized sources.

Cisco security products are also covered, as are all the fundamental foundation topics you need to understand to master the security CCIE Security written exam.

This chapter covers the following topics:

- **Advanced Security Concepts**—Describes advanced security policies in demilitarized zones (DMZs).
- **Packet Filtering, Proxies, NAT, and PAT**—Explains packet filtering, proxies, and how to hide addresses using Network Address Translation (NAT) and Port Address Translation (PAT).
- **Cisco PIX Firewall and Cisco IOS Firewall Feature Set**—Covers the Cisco PIX Firewall and the Cisco IOS Firewall feature set available on Cisco routers. Includes information on IOS authentication proxies.
- **Public Key Infrastructure**—Covers PKI, followed by a description of VPN networks and a typical design example.
- **Virtual Private Networks**—Explains how a VPN enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another.
- **Network-Based Intrusion Detection System**—Covers network intrusion detection, signatures, and how IDS can be used to thwart intruders.
- **Cisco Security Agent and Host-Based IDS**—Describes Cisco Security Agent (CSA), the front-line defense in the Cisco self-healing strategy of defending networks.
- **Cisco Threat Response**—Introduces the Cisco technology that provides an automated response when networks have been compromised. Covers some of the advanced features available on Cisco power networks.

"Do I Know This Already?" Quiz

The purpose of this assessment quiz is to help you determine how to spend your limited study time.

If you can answer most or all of these questions, you might want to skim the "Foundation Topics" section and return to it later, as necessary. Review the "Foundation Summary" section and answer the questions at the end of the chapter to ensure that you have a strong grasp of the material covered.

If you already intend to read the entire chapter, you do not necessarily need to answer these questions now. If you find these assessment questions difficult, read through the entire "Foundation Topics" section and review it until you feel comfortable with your ability to answer all of these questions and the "Q & A" questions at the end of the chapter.

Answers to these questions can be found in Appendix A, "Answers to Quiz Questions."

1. DMZ stands for what?
   a. Demilitarized zone
   b. Demitted zone
   c. Domain main zone
   d. Domain name
2. When defining an extended access list, what TCP port numbers can you use?
   a. Only predefined Cisco keywords
   b. 0 to 65,000
   c. 0 to 65,535
   d. 1 to 65,534
   e. None of these
3. When defining an extended access list, what UDP port numbers can you use?
   a. Only predefined Cisco keywords
   b. 0 to 65,000
   c. 0 to 65,535
   d. 1 to 65,534
   e. None of these

4. Which of the following is *not* a TCP service?
   a. who
   b. whois
   c. finger
   d. ftp
   e. pop3
5. Which of the following is *not* a UDP service?
   a. BGP
   b. echo
   c. domain
   d. discard
   e. RIP
   f. SNMP
6. For about how many translations does PAT (for a PIX Firewall) allow you to use one IP address?
   a. 32,000
   b. 64,000
   c. 96,000
   d. 128,000
   e. 256,000
7. PAT translates all private addresses based on what?
   a. Source port
   b. Destination port
   c. Both source and destination ports
   d. None of these
8. NAT is which of the following?
   a. Network Architectural Language
   b. National anthem of Latvia
   c. Network translation
   d. Network Address Translation

9. NAT is defined in which RFC?
   a. 1700
   b. 1701
   c. 2002
   d. 1631
   e. 1613
10. The following defines which NAT terminology: "A legitimate registered IP address as assigned by the InterNIC"?
   a. Inside local address
   b. Outside global address
   c. Inside global address
   d. Outside local address
11. NAT might often be broken in what common scenario?
   a. Only with VoIP
   b. With PAT only
   c. By traffic that carries the source/destination IP address in the application data fields
   d. Only with HTTPS
   e. When all multimedia applications fail
   f. All of these
   g. Only with VoIP or when all multimedia applications fail
12. When will the command **overload**, applied to NAT configurations, possibly break a network application?
   a. Never
   b. With some HTTP applications
   c. With all FTP connections
   d. With some UDP connections
   e. With some multimedia applications
   f. All of these

13. Firewalls can operate at what three layers of the OSI model?

    a. 1, 2, 3
    b. 3, 4, 5
    c. 5, 6, 7
    d. 7, 4, 3
    e. 3, 4, 6

14. What is the main advantage of using NAT on a firewall or Cisco IOS router?

    a. No advantage; it makes a network complex
    b. Enables RFC 1918–based privately defined IP addresses to be configured and enables access to the Internet
    c. Ensures the device increases in performance
    d. Decreases performance
    e. Consumes CPU to allow IP packets to traverse the network forever
    f. All of these

15. When using the IOS NAT **overload** command, how many inside sessions can be translated?

    a. 10,000
    b. 20,000
    c. 64,000
    d. 65,534
    e. None
    f. Depends on Cisco IOS revision

16. What IOS command defines a pool of IP addresses for Network Address Translation (NAT)?

    a. **ip nat inside**
    b. **ip nat outside**
    c. **ip nat pool**
    d. **ip nat inside pool**
    e. **ip nat outside pool**

17. PIX stands for what?

    a. Protocol interchange
    b. Cisco Private Internet
    c. Private Internet Exchange
    d. Public Internet Exchange

18. To define how a PIX will route IP data, what is the correct syntax for a PIX?
    a. **ip route**
    b. **route**
    c. **ip route enable**
    d. **default-network**
19. If you configure NAT on a Cisco IOS router, what command is used to enable PAT?
    a. **pat**
    b. **nat**
    c. **ip route**
    d. **overload**
    e. **extended**
20. Cisco IOS–based NAT provides all of the following functions *except* one; which one?
    a. Provides safety for inside hosts from becoming an attack target
    b. It can be traced or viewed by an outside address
    c. Prevents the source from being traced from the Internet
    d. Prevents an inside host from becoming a reflector of an attack
21. Which of the following is not considered a security device?
    a. PIX
    b. Switch
    c. IDS appliance
    d. Microsoft Windows XP Professional
    e. VPN Concentrator
    f. All of these are security devices
22. What extended IP access list will prevent the internal subnet 10.0.0.0/8 from being spoofed on a Cisco IOS–enabled router? (Assume **permit** statements are applied to allow legitimate traffic.)
    a. **access-list 1 permit 10.0.0.0 0.0.0.255 0.0.0.0 255.255.255.255**
    b. **access-list 100 deny 10.0.0.0 0.0.0.255 0.0.0.0 255.255.255.255 any**
    c. **access-list 99 tcp deny 10.0.0.0 0.0.0.255 0.0.0.0 any**
    d. **access-list 100 ip deny 10.0.0.0 0.0.0.255 0.0.0.0 any**
    e. None of these

23. What is the **alias** command's function on a PIX Firewall?

- **a.** To define a local host name.
- **b.** To define the DNS server.
- **c.** The **alias** command is used in NAT environments where one IP address is translated into another.
- **d.** Only applicable to Cisco IOS.

24. CBAC stands for what?

- **a.** CBAC is not a valid term.
- **b.** Cisco Business Architectural Center.
- **c.** Context-Based Access Control.
- **d.** Context-Based Accelerated Controller.
- **e.** Content-Based Arch. Centre.

25. What is IKE used to accomplish?

- **a.** NAT translations
- **b.** To ensure that data is not sourced by the right sources
- **c.** To ensure that data is not viewable by unauthorized sources
- **d.** No use
- **e.** NAT translations and to ensure that data is not sourced by the wrong sources

26. To create a simple VPN tunnel (unencrypted) between two sites, what must you do on a Cisco router?

- **a.** Create a GRE tunnel
- **b.** Create a routing map
- **c.** Nothing; use a PIX
- **d.** Create an IPSec tunnel

27. PIX Firewall software version 6.3 can support which of the following routing protocols? (Choose the best three answers.)

- **a.** BGP
- **b.** OSPF
- **c.** RIP version 1
- **d.** RIP version 2
- **e.** EIGRP

28. To support OSPF on a PIX Firewall version 6.3–capable firewall, what additional OSPF authentication mechanisms are possible? (Choose the best two answers.)

- **a.** MD5
- **b.** Area
- **c.** Password
- **d.** RADIUS
- **e.** TACACS+
- **f.** Kerberos

29. What PIX command can be used for a dual NAT environment?

- **a.** **conduit**
- **b.** **pix**
- **c.** **alias**
- **d.** **sysopt permit dnat**
- **e.** **pat** [**dnat**] **ip address** *alias*
- **f.** None of these

30. What PIX command is used on a PIX Firewall to view address mappings when NAT is enabled?

- **a.** **show nat**
- **b.** **show pat**
- **c.** **show late**
- **d.** **show xlate**
- **e.** **show ip nat**
- **f.** **show ip pat**
- **g.** None of these

31. If a PIX Firewall is configured without a conduit or an access list, data from the inside interface is dropped. In effect, the PIX Firewall is acting like which of the following? (Select the best two answers.)

- **a.** Router
- **b.** Bridge
- **c.** Bridge and router
- **d.** Bit bucket
- **e.** Black hole router
- **f.** None of these

32. After viewing the PIX syslog with the command **show logging**, the following output is discovered:

```
14:25:02 10.1.1.1 : %PIX-7-7100006: TCP request discarded from 6.3.62.119/
57000 to inside:10.1.1.1/www
```

Assuming the inside interface on the PIX is configured for the IP address 10.1.1.1/24, which of the following answers best describes what *might* be going on in the network?

- **a.** Nothing, this level is normal as the level is 7.
- **b.** IP addresses on the inside have all launched an attack against the PIX outside address.
- **c.** A host on the inside has launched a denial of service (DoS) attack generating random source addresses aimed at the PIX inside interface.
- **d.** Several zombie hosts have been activated on the outside of the PIX and are trying to crash the PIX HTTP server.
- **e.** A host on the outside has been compromised and is attempting to log onto the PIX HTTP server.

33. Which of the following statements best describes Cisco Threat Response (CTR)?

- **a.** CTR reads IDS alarms and performs automated forensics on hosts or servers that may have been compromised.
- **b.** CTR logs into real devices and searches for log entries.
- **c.** CTR determines if network IDS alarms are valid or invalid by using Telnet.
- **d.** CTR is an inline device that does deep packet inspection looking for attacks on Cisco network devices such as routers and switches.
- **e.** CTR is not an application but a hardware IDS device.

34. Which of the following best describes Cisco Security Agent (CSA)?

- **a.** CSA is the best antivirus tool available.
- **b.** CSA uses a set of predefined rules to protect host-based systems such as PCs or servers.
- **c.** CSA is a server-based system only that recognizes network attacks.
- **d.** CSA takes no action when an attack occurs.
- **e.** CSA is a passive device and does little besides stop the IP stream.

35. Which of the following describes the default rules a host version of the Cisco Security Agent accomplishes? (Choose the best three answers.)

- **a.** Prevents writing to the system directory
- **b.** Stops unauthorized systems from initiating network connections to the CSA-protected host
- **c.** Provides deep packet inspection to prevent Internet viruses
- **d.** Provides deep packet inspection to prevent worms
- **e.** Prevents updates to the system registry

36. IEEE 802.1X is primarily used for what purpose?

- **a.** Prevent writing to the system directory
- **b.** Authenticate MAC or Layer 3 addresses
- **c.** Layer 7 authentication
- **d.** Allow Layer 3 communication and authenticate clients
- **e.** VLAN assignment
- **f.** Prevent updates to the system registry

37. What device initiates the first communication in IEEE 802.1X?

- **a.** The IOS router
- **b.** The IOS switch
- **c.** The end workstation connected to the switch
- **d.** The RADIUS server
- **e.** The TACACS+ server
- **f.** None of these

38. CSA is supported on what two platforms?

- **a.** Windows
- **b.** UNIX
- **c.** Macintosh
- **d.** Printers
- **e.** PDAs

39. How does anomaly-based intrusion detection recognize that a network attack is in progress?

- **a.** Packets are matched with a signature and then logged.
- **b.** The IDS normalizes network traffic and sends alarms when sampled traffic falls out of that norm.
- **c.** Protocol adherence rules are established by the administrator and any deviation from that is flagged as a potential attack.
- **d.** The IDS normalizes network traffic.

Foundation Topics

Advanced Security Concepts

A wealth of security concepts have been covered in the previous chapters; now, you are ready to look at some of the techniques that are used to secure areas of your network that are vulnerable to attacks, in particular the demilitarized zone (DMZ).

The DMZ is defined as an isolated part of the network that is easily accessible to hosts outside of the network, such as the Internet.

Figure 6-1 displays a typical network design where a DMZ is defined with a number of bastion hosts (first line of defense for hosts that can be scarified in case of a network attack or attacks).

Figure 6-1 *DMZ Design*

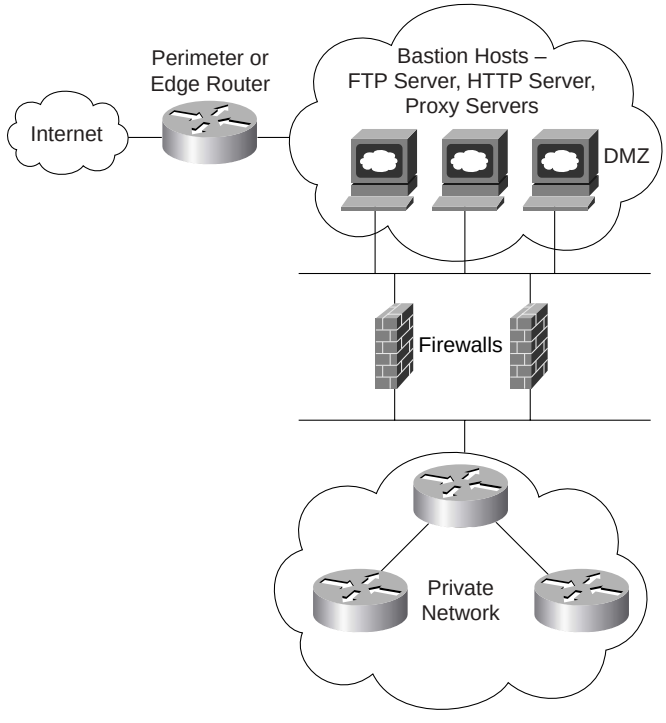


Figure 6-1 displays a typical perimeter network in which the DMZ is separated by a firewall. *Firewalls* are network devices such as Cisco Private Internet Exchange (PIX) Firewall, discussed later in this chapter. Firewalls are designed to protect the internal (or private) parts of a network from the public domain. Firewalls can operate at several levels of the OSI model, namely the application layer (7), network layer (3), and transport layer (4). Another popular design option is to configure the DMZ on a third interface of the firewall so that the firewall can protect both the DMZ servers and the internal network.

The aim of all firewalls is to accomplish the following:

- **Serve as a traffic point**—The traffic or choke point from inside and outside the network must pass through the traffic point.
- **Authorize traffic**—Permits only authorized traffic.
- **Designed to be immune from penetration**—Firewalls are designed to be immune from attacks. However, firewalls are still often attacked by outside hosts.
- **Provide invisibility**—Ensures that the private network is invisible to the outside world.

As shown in Figure 6-1, the perimeter router sits between the DMZ and the public domain. Typically, a high-performance router or routers will be located here, performing various duties, including the following:

- Ensure that access to IP is restricted using access lists.
- Restrict TCP services.
- Prevent attacks on firewall systems.
- Prevent DoS attacks on bastion hosts and the private network.
- Permit only authorized traffic to the bastion hosts.
- Log all network events to external or internal systems.
- Perform address translation (NAT/PAT).
- Run static or dynamic routing protocols; Cisco PIX release 6.3 is no longer limited to RIP and static routing but now supports OSPF. PIX Firewall software version 6.3 is now capable of supporting RIP versions 1 and 2 along with OSPF.

NOTE Proxy servers are designed to shield internal devices from outside intruders by replacing the internal hosts' IP addresses with its own IP address. Most new vendors (supplying routers) now allow routers to act as proxy servers. Proxy servers have scalability and speed issues, because all packets must be examined and IP headers must be modified for packet delivery.

Firewalls and perimeter routers have the additional function of packet filtering. A *packet filter* is a device that inspects all incoming and outgoing packets based on IP source address, destination IP address, and protocol type, such as TCP or UDP. Based on configurable options, the filter decides whether to reject traffic or allow traffic to pass through the device.

Table 6-1 summarizes the main functions of a perimeter and firewall router.

Table 6-1 *Perimeter/Firewall Router Functions*

Protection Service	Method
Sniffer or snooping capabilities	Control eavesdropping with the TCP/IP service and network layer encryption (IPSec).
Control unauthorized access	Use authentication, authorization, and accounting (AAA), and Cisco Secure ACS. Also, use access list filtering and PIX Firewall.
Control session replay	Control which TCP/IP sessions are authorized. Block SNMP, IP source routing, and finger services to outside hosts.
Control inbound connections	Filter internal address as the source from the outside world. Filter all private addresses. Filter Bootp, Trivial File Transfer Protocol (TFTP), and traceroute commands. Allow connections only for required services. Allow TCP connections established from the inside network. Permit inbound traffic to DMZ only.
Control outbound connections	Allow only valid IP addresses to the outside world and filter remaining illegal addresses and outbound service requests.
Packet filtering	Use predefined access lists that control the transmission of packets from any given interface, control vty lines and access, and ensure that routing updates are authenticated.

Cisco IOS routers can filter TCP or UDP protocol types. Example 6-1 displays the variety of TCP services that you can filter on a Cisco IOS router using extended access lists.

Example 6-1 *TCP Services Filtered on Cisco IOS Routers*

```
R1(config)#access-list 100 permit tcp any any eq ?
  <0-65535>    Port number
  bgp          Border Gateway Protocol (179)
  chargen      Character generator (19)
  cmd          Remote commands (rcmd, 514)
  daytime      Daytime (13)
  discard      Discard (9)
  domain       Domain Name Service (53)
  echo         Echo (7)
  exec         Exec (rsh, 512)
```

continues

Example 6-1 *TCP Services Filtered on Cisco IOS Routers (Continued)*

```
  finger       Finger (79)
  ftp          File Transfer Protocol (21)
  ftp-data     FTP data connections (used infrequently, 20)
  gopher       Gopher (70)
  hostname     NIC hostname server (101)
  ident        Ident Protocol (113)
  irc          Internet Relay Chat (194)
  klogin       Kerberos login (543)
  kshell       Kerberos shell (544)
  login        Login (rlogin, 513)
  lpd          Printer service (515)
  nntp         Network News Transport Protocol (119)
  pim-auto-rp  PIM Auto-RP (496)
  pop2         Post Office Protocol v2 (109)
  pop3         Post Office Protocol v3 (110)
  smtp         Simple Mail Transport Protocol (25)
  sunrpc       Sun Remote Procedure Call (111)
  syslog       Syslog (514)
  tacacs       TAC Access Control System (49)
  talk         Talk (517)
  telnet       Telnet (23)
  time         Time (37)
  uucp         Unix-to-Unix Copy Program (540)
  whois        Nicname (43)
  www          World Wide Web (HTTP, 80)
```

Example 6-2 displays the extended access list when filtering services based on the UDP protocol suite of services.

Example 6-2 *UDP Services Filtered on Cisco IOS Routers*

```
R1(config)#access-list 101 permit udp any any eq ?
  <0-65535>    Port number
  biff         Biff (mail notification, comsat, 512)
  bootpc       Bootstrap Protocol (BOOTP) client (68)
  bootps       Bootstrap Protocol (BOOTP) server (67)
  discard      Discard (9)
  dnsix        DNSIX security protocol auditing (195)
  domain       Domain Name Service (DNS, 53)
  echo         Echo (7)
  isakmp       Internet Security Association and Key Management Protocol (500)
  mobile-ip    Mobile IP registration (434)
  nameserver   IEN116 name service (obsolete, 42)
  netbios-dgm  NetBios datagram service (138)
  netbios-ns   NetBios name service (137)
  netbios-ss   NetBios session service (139)
```

Example 6-2 *UDP Services Filtered on Cisco IOS Routers (Continued)*

```
ntp          Network Time Protocol (123)
pim-auto-rp  PIM Auto-RP (496)
rip          Routing Information Protocol (router, in.routed, 520)
snmp         Simple Network Management Protocol (161)
snmptrap     SNMP Traps (162)
sunrpc       Sun Remote Procedure Call (111)
syslog       System Logger (514)
tacacs       TAC Access Control System (49)
talk         Talk (517)
tftp         Trivial File Transfer Protocol (69)
time         Time (37)
who          Who service (rwho, 513)
xdmcp        X Display Manager Control Protocol (177)
```

Examples 6-1 and 6-2 clearly indicate that a network administrator has flexibility when designing perimeter security based on particular port numbers, as defined in RFC 1700.

The growth of the Internet and increased ease of information transfer has also meant a proliferation of network hacking tools. Whisker, Nmap and strobe are perfect examples of this fact. A simple search on the Internet reveals many more tools. Firewalls are your first line of defense but should not be your last.

Intrusion detection systems (IDSs) are the next level of security now being added to secure IP networks, providing even greater awareness of IP packet flow through a network. IDSs are covered later in this chapter. The next section introduces basic NAT and PAT.

Network Address Translation and Port Address Translation

NAT is a router function, which allows it to translate the addresses of hosts behind a firewall. This also helps to overcome IP address shortage, and provides security by hiding the entire network and its real IP addresses.

NAT is typically used for internal IP networks that have unregistered (not globally unique) IP addresses. NAT translates these unregistered addresses into legal addresses on the outside (public) network.

PAT provides additional address expansion but is less flexible than NAT. With PAT, one IP address can be used for up to 64,000 hosts by mapping several IP port numbers to one IP address. PAT is secure because the inside hosts' source IP addresses are hidden from the outside world. The perimeter router typically provides the NAT or PAT function.

NOTE PAT uses unique source port numbers on the inside global IP address to distinguish between translations. Because the port number is encoded in 16 bits, the total number of ports could theoretically be as high as 65,536 per IP address. PAT will attempt to preserve the original source port. If this source port is already allocated, PAT will attempt to find the first available port number starting from the beginning of the appropriate port group, 0–511, 512–1023, or 1024–65535. If there is still no port available from the appropriate group and more than one IP address is configured, PAT will move to the next IP address and try to allocate the original source port again. This continues until it runs out of available ports and IP addresses. (From http://www.cisco.com/warp/public/cc/pd/iosw/ioft/ionetn/prodlit/1195_pp.htm.)

NAT is defined in RFC 1631, the text of which can be read at http://www.ietf.org/rfc/rfc1631.txt. Cisco devices started supporting NAT in Cisco IOS versions 11.2 and higher. NAT basically provides the capability to retain your network's original IP addressing scheme while translating that scheme into a valid Internet IP address to ensure that intruders never view your private address.

NOTE Cisco IOS 12.0 and higher support full NAT functionality in all images. Version 11.2 and higher need "Plus" image for a NAT feature set.

NAT changes the Layer 3 address when the packet is sent out to the Internet. This is a function no other protocol will do (that is, alter the Layer 3 source address).

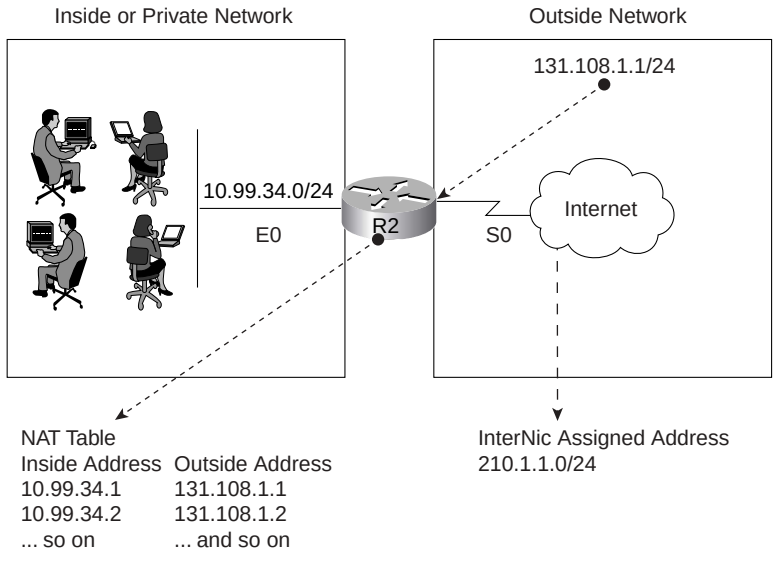
For your review and to fully prepare you for the exam, Table 6-2 explains some of the terminology used in a NAT environment.

Table 6-2 *NAT Terminology*

Term	Meaning
Inside local address	An IP address that is assigned to a host on the internal network; that is, the logical address that is not being advertised to the Internet. A local administrator generally assigns this address. This address is *not* a legitimate Internet address.
Inside global address	A legitimate registered IP address that represents one or more inside local IP addresses as assigned by the InterNIC.
Outside local address	The IP address of an Internet's outside host that is being translated as it appears to the inside network.
Outside global address	The IP address assigned to a host on the outside of the network before it is translated by the router's owner.

Figure 6-2 displays a typical scenario where a private address space is deployed that requires Internet access. The Class A 10.0.0.0/8 address is not routable in the Internet.

Figure 6-2 *Typical NAT Scenario*



The users in Figure 6-2 are configured with the inside local addresses ranging from 10.99.34.1/24 to 10.99.34.254/24. To allow Internet access, NAT (PAT could also be configured if only one IP address was allocated by InterNIC) is configured on Router R1 to permit the inside local addresses access to the Internet. Advantages of using NAT include the following:

- You can hide the Class A address space 10.99.34.0/24.

  To view the NAT translation table on the Cisco router, apply the EXEC command **show ip nat translations** on the CLI.

- You can connect a nonroutable network to the Internet.
- You can use unregistered address space and NAT to the Internet.
- You can use both NAT and PAT on the same router.
- You can have 64,000 inside hosts per allocated IP address.

The InterNIC is an Internet authority that is assigned the task of allocating IP address space to the public. For example, Figure 6-2 assumes that the InterNIC assigned the address space 210.1.1.0/24 for use.

NOTE Disadvantages of NAT/PAT include the following:

- Drain on CPU processing power.
- Layer 3 header and source address changes.
- Some multimedia-intensive applications do not support NAT, especially when the data stream inbound is different from the outbound path (for example, in multicast environments).

NAT Operation on Cisco Routers

When a packet leaves the inside network, NAT translates the inside address to a unique InterNIC address for use on the outside network, as previously shown in Figure 6-2.

The R1 Router in Figure 6-2 will be configured for an address translation and will maintain a NAT table. When an IP packet returns from the outside network, the NAT router will then perform an address translation from the valid InterNIC address to the original local inside address.

Several internal addresses can be translated to only one or a few external addresses by using PAT, which is also referred to as *overload* in Cisco IOS configuration syntax.

With Cisco IOS, the **overload** commands allow up to 64,000 connections to be translated per IP address. The **overload** command does not work well with certain applications such as multimedia streams, because some video applications, for example, have an inbound data stream that is different from the outgoing stream. For example, if the application contains the source and destination IP addresses in the data portion of the IP packet (Layer 7, for example), NAT will change the Layer 3 header, which may cause the application to fail.

Cisco IOS NAT functionality prevents the inside of your network from becoming a potential easy target. Because the internal addresses (for example, IP subnets in the range 10.0.0.0/8) are not routable through to the Internet, Cisco IOS NAT can also prevent an inside address from launching an attack or becoming active in attacking other hosts. Most importantly, Cisco IOS NAT prevents inside hosts behind a NAT interface from being sourced from the outside world.

Most secure organizations also prevent the 10.0.0.0/8 nonroutable network from being spoofed with an access list on the outside interface, such as the following (one of the ranges defined in RFC 1918, noting we deny 10.0.0.0/8 first followed by permit statements):

```
access-list 100 ip  deny 10.0.0.0 0.0.0.255  any log
access-list 100 ….permit statements
```

Notice that the keyword **log** is applied so that a security administrator can monitor spoofed addresses as well. The **log** statement does have an impact on the CPU of the router because it causes all packets to be process switched, so use the command with caution.

Dynamic NAT Configuration Task List

This section looks at the steps required to configure dynamic NAT on a Cisco router. Dynamic NAT maps any unregistered IP addresses to a registered IP address from a group of registered IP addresses. Dynamic NAT creates active translation entries in a NAT table when a packet crosses from an IP NAT inside interface to an IP NAT outside interface, or vice versa.

The basic configuration tasks are as follows:

Step 1 Determine the network addresses to be translated.

Step 2 Configure the inside network with the following IOS command:

```
ip nat inside
```

Step 3 Configure the outside network with the following IOS command:

```
ip nat outside
```

Step 4 Define a pool of addresses to be translated with the following IOS command:

```
ip nat pool pool-name start-ip-address end-ip-address mask
```

Step 5 Define the addresses that are allowed to access the Internet with the following IOS command:

```
ip nat inside source list access-list-number pool pool-name
```

For a more specific illustration, configure NAT on Router R1. In Figure 6-2, the NAT pool name is going to be CCIE. (You can use any name you want.) Assume that the InterNIC has assigned to you the Class C address of 210.1.1.0/24.

Your Internet service provider (ISP) has also supplied you with the unique address 131.108.1.0/30 (this address will be the NAT address 131.108.1.1 or 131.108.1.2) to use on your serial connection.

Example 6-3 provides a sample NAT configuration for this setup.

Example 6-3 *Sample NAT Configuration on R1*

```
hostname R1
ip nat pool CCIE 210.1.1.1 210.1.1.254 netmask 255.255.255.0
ip nat inside source 1 pool CCIE
interface ethernet0
ip address 10.99.34.1 255.255.255.0
ip nat inside
interface serial 0
ip address 131.108.1.1 255.255.255.252
ip address 210.1.1.1 255.255.255.0 secondary
ip nat outside
access-list 1 permit 10.99.34.0 0.0.0.255
```

It is assumed that you have an IP routing protocol to advertise the IP networks shown in the sample, which are 131.108.1.0/30 and 210.1.1.0/24, to the remote ISP router through R1's serial 0 interface.

The configuration shown in Example 6-3 translates the inside addresses 10.99.34.0/24 into globally unique addresses ranging from 210.1.1.1/24 to 210.1.1.254.

Monitoring NAT Operations with show Commands

To monitor the operation of NAT, you can use the following commands:

```
show ip nat translation [verbose]
show ip nat statistics
```

The **show ip nat translation** command displays the current active transactions. The **show ip nat statistics** command displays NAT statistics, such as how many translations are currently taking place.

There are four different versions of NAT translations:

- **Static NAT**—Maps an unregistered IP address to a registered IP address on a one-to-one basis. This is particularly useful when a device needs to be accessible from outside the network to an internal unregistered address.
- **Dynamic NAT**—Maps an unregistered IP address to a registered IP address from a group of registered IP addresses.
- **Overloading**—A form of dynamic NAT that maps multiple, unregistered IP addresses to a single registered IP address by using different ports.
- **Overlapping**—When the IP addresses used on your internal network are registered IP addresses in use on another network, the router must maintain a lookup table of these addresses so that it can intercept them and replace them with registered unique IP addresses.

For more quality examples on NAT, visit http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Internetworking:NAT.

For demonstrations of when you can use NAT over an IPSec tunnel, visit www.cisco.com/warp/customer/707/overload_private.shtml.

NOTE TCP load distribution is typically used in large IP networks that have server farms. You might want to distribute the network load across many servers but advise users to use only one IP address to target. TCP load distribution ensures that all servers are equally loaded. For details on NAT order of operation, which describes how NAT operates in full detail, visit http://www.cisco.com/en/US/partner/tech/tk648/tk361/technologies_tech_note09186a0080133ddd.shtml.

Cisco PIX Firewall

The Cisco Private Internet Exchange (PIX) Firewall and Cisco IOS Firewall feature set are designed to further enhance a network's security. The PIX Firewall prevents unauthorized connections between two or more networks. The latest versions of Cisco code for the PIX Firewall also perform many advanced security features, such as AAA services, access lists, VPN configuration (IPSec), FTP, logging, and Cisco IOS-like interface commands. In addition, the PIX Firewall can support multiple outside or perimeter networks in the DMZs.

NOTE When reading Cisco documentation about PIX Firewalls, realize that "inside networks" and "outside networks" both refer to networks to which the PIX Firewall is connected.

For example, inside networks are protected by the PIX Firewall, but outside networks are considered the "bad guys." Consider them as trusted and untrusted, respectively.

A PIX Firewall permits a connection-based security policy. For example, you might allow Telnet sessions from inside your network to be initiated from within your network but not allow them to be initiated into your network from outside your network.

The PIX Firewall's popularity stems from the fact that it is dedicated solely to security. A router is still required to connect to WANs, such as the Internet. Some companies use PIX Firewalls for internal use only where they might have sensitive networks, such as a payroll or human resources department.

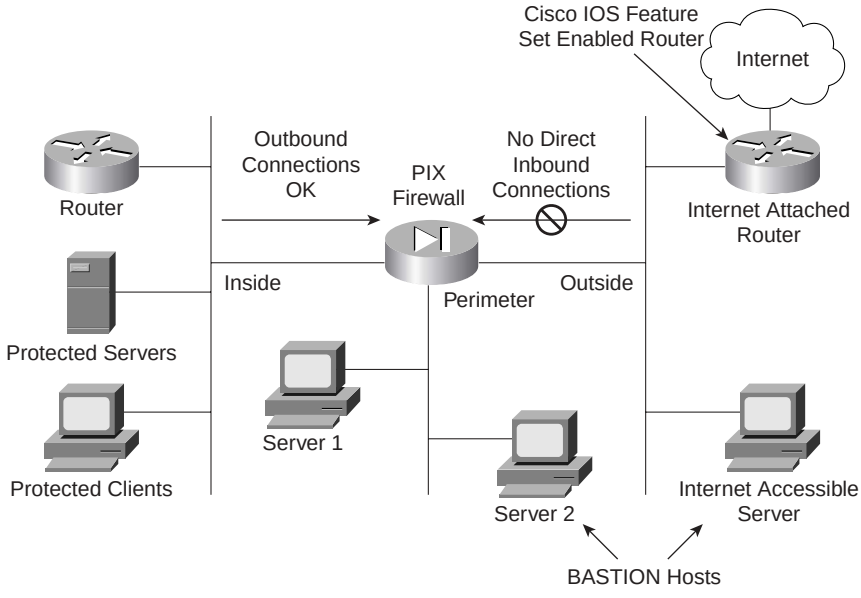
Figure 6-3 shows a typical network scenario in which a PIX Firewall is implemented between an inside network and an outside network.

Although optional, it is recommended that you install the Cisco IOS Firewall software on the router directly connected to the Internet. The Cisco IOS Firewall feature set is discussed later in this chapter. Be aware that there are performance ramifications when enabling the Firewall feature sets.

Each connection through a PIX Firewall requires memory. You can support up to 7500 connections with 16 MB of RAM installed on a PIX Firewall; 32 MB of memory can support up to 25,000 connections; 256 MB can support up to 280,000 connections; and 1 GB can support up to 500,000 connections.

DMZs usually exist as part of a network that the Internet community or general public can access, such as a web, FTP, or SMTP server. For example, FTP servers allow external users to access public files, such as Cisco IOS Software files, which are available online at ftp.cisco.com. Your remaining servers are protected by the firewall typically with a third firewall interface called the DMZ.

Figure 6-3 *Figure 6-3PIX Firewall Location*



The PIX Firewall logic is engineered around the Adaptive Security Algorithm (ASA). Every inbound packet is checked against the ASA and against connection state information in memory. This stateful approach to security is regarded in the industry as being far more secure than a stateless packet-screening approach.

Examples of the stateful approach to security include the following:

- No packets can traverse the PIX Firewall without a connection and state.
- Outbound connections or states are allowed, except those specifically denied by ACLs. An outbound connection is one where the originator, or client, is on an interface with higher security than that of the interface on which the receiver, or server, resides. The highest-security interface is always the inside interface (value 100), and the lowest is the outside interface (value 0). Any perimeter interfaces can have security levels between the inside and outside values (for example, 50).
- Inbound connections or states are denied, except those specifically allowed. An inbound connection or state is one where the originator, or client, is on an interface with lower security than that of the interface/network on which the receiver, or server, resides. You can apply multiple exceptions to a single xlate (translation). This lets you permit access from an arbitrary machine, network, or any host on the Internet to the host defined by the xlate.

- All Internet Control Message Protocol (ICMP) packets are denied unless specifically permitted. ICMP packets to the PIX Firewall itself are allowed unless explicitly denied by an ICMP access control entry.
- All attempts to circumvent the previous rules are dropped and a message is sent to syslog.

When an outbound packet arrives at a PIX Firewall higher-security-level interface (security levels can be viewed with the **show nameif** command; by default, the outside interface has a security level set to 0, or untrusted, and the inside interface is set to 100, or trusted), the PIX Firewall checks whether the packet is valid based on the ASA, and whether previous packets have come from that host. If not, the packet is for a new connection, and the PIX Firewall creates a translation slot in its state table for the connection. The information that the PIX Firewall stores in the translation slot includes the inside IP address and a globally unique IP address assigned by NAT, PAT, or identity (which uses the inside address as the outside address). The PIX Firewall then changes the packet's source IP address to the globally unique address, modifies the checksum and other fields as required, and forwards the packet to the lower-security-level interface.

When an inbound packet arrives at an external interface such as the outside interface, it must first pass the PIX Firewall ASA criteria. If the packet passes the security tests, the PIX Firewall removes the destination NAT IP address, and the internal IP address is inserted in its place. The packet is forwarded to the protected interface.

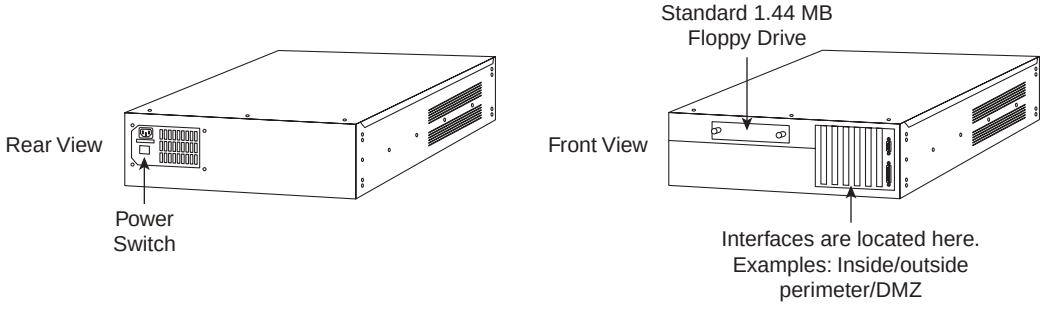
NOTE The PIX Firewall supports NAT, which provides a globally unique address for each inside host, and PAT, which shares a single globally unique address for up to 64,000 simultaneously accessing inside hosts. The following is a list of current models that Cisco supports (not required knowledge for the examination):

- PIX 501
- PIX 506/506E
- PIX 515/515E
- PIX 520
- PIX 525
- PIX 535

For a full feature list of the PIX Firewall, visit http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/config/overvw.htm#wp1008066.

Figure 6-4 displays a sample PIX Firewall, which is used in the current CCIE Security lab exam. PIX Firewall devices are based on the Intel Pentium processor, which is basically a PC with Cisco-installed PIX Firewall software.

Figure 6-4 *Cisco PIX Firewall*

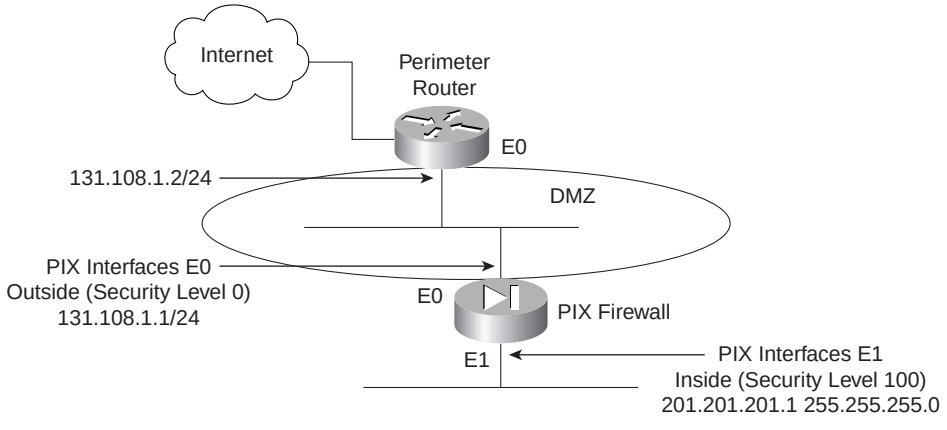


Configuring a PIX Firewall

This section takes a look at configuring the PIX Firewall software and the six basic commands used to configure a PIX Firewall.

Figure 6-5 displays a typical DMZ and perimeter network between the inside (protected) and outside (public) networks.

Figure 6-5 *Typical PIX Firewall Logical Setup*



PIX Firewall Configuration Task List

The following steps show you how the PIX Firewall software is configured for the scenario in Figure 6-5:

Step 1 Name the inside and outside interfaces and assign the security levels (in global configuration mode):

```
nameif hardware_id if_name security_level vlan_id
```

The **nameif** command lets you assign a name to an interface. You can use this command to assign interface names if you have more than two network interface circuit boards in your PIX Firewall. The first two interfaces have the default names **inside** and **outside**. The **inside** interface has default security level 100, and the **outside** interface has default security level 0.

Table 6-3 describes the PIX Firewall command **nameif** as documented on the Cisco Documentation CD-ROM**.**

Table 6-3 **nameif** *Command and Required Fields*

Syntax	Description
hardware_id	The hardware name for the network interface that specifies the interface's slot location on the PIX Firewall motherboard. Interface boards are numbered from the leftmost slot nearest the power supply as slot 0. The internal network interface must be in slot 1. The lowest *security_level* external interface board is in slot 0, and the next lowest *security_level* external interface board is in slot 2.
if_name	A name for the internal or external network interface of up to 48 characters in length. This name can be upper- or lowercase. By default, the PIX Firewall names the inside interface **inside**, the outside interface **outside**, and any perimeter interface **intfn**, where n is 2 through 5.
security_level	Either **0** for the outside network or **100** for the inside network. Perimeter interfaces can use any number between **1** and **99**. By default, the PIX Firewall sets the security level for the inside interface to **security100**, and the outside interface to **security0**. The first perimeter interface is initially set to **security10**, the second to **security15**, the third to **security20**, and the fourth to **security25**. Check the latest Cisco IOS bulletins for the number of hardware interfaces supported per PIX Firewall.
vlan_id	The VLAN identifier; for example, vlan10, vlan20, etc. The VLAN identifier is configured with the **interface** command.

Step 2 Identify the hardware interfaces, speed, and duplex type installed with the following interface command:

```
interface hardware_id [hardware_speed] [shutdown]
```

In Figure 6-5, the following commands are configured:

```
interface ethernet0 10full
interface ethernet1 10full
```

Table 6-4 defines and describes the options for the **interface** command, as documented on the Cisco Documentation CD-ROM.

Table 6-4 **interface** *Command Options*

Option	Description
hardware_id	Identifies the network interface type. Possible values are **ethernet0**, **ethernet1** to **ethernet***n*, or **gb-ethernet***n,* depending on how many network interfaces are in the PIX Firewall.
hardware_speed	Network interface speed (optional).
shutdown	Disables an interface.

Step 3 Define the inside and outside IP addresses.

The **ip address** *if_name ip_address* [*netmask*] command lets you assign an IP address to each interface.

Use the **show ip** command to view which addresses are assigned to the network interfaces.

In Figure 6-5, the IP address assignment is defined as follows:

```
ip address inside 201.201.201.1 255.255.255.0
ip address outside 131.108.1.1 255.255.255.0
```

Table 6-5 defines the options and meaning of the **interface** command.

Table 6-5 **interface** *Command*

Option	Description
if_name	The internal or external interface name designated by the **nameif** command
ip_address	PIX Firewall unit's network interface IP address
netmask	Network mask of *ip_address*

Step 4 Define NAT with the **nat** command.

The **nat** command lets you enable or disable address translation for one or more internal addresses. Address translation means that when a host starts an outbound connection, the IP addresses in the internal network are translated into global addresses. NAT lets your network have any RFC 1918 IP addressing scheme, and the firewall protects these addresses from visibility on the external network.

The command syntax is as follows:

```
nat [(if_name)] nat_id local_ip [netmask [max_conns [em_limit]]]
[norandomseq]
```

In Figure 6-5, the following pool is assigned to the PIX Firewall:

```
nat (inside) 1 0.0.0.0 0.0.0.0
```

This command enables all inside hosts to access the Internet.

Table 6-6 defines the options of the **nat** command, as documented on the Cisco Documentation CD-ROM.

Table 6-6 **nat** *Command Options*

Option	Description
if_name	Any internal network interface name.
nat_id	An arbitrary positive number between 0 and 2 billion. Specify **0** with IP addresses and netmasks to identify internal networks that desire only outbound identity address translation. Use **0** with the **access-list** option to specify traffic that should be exempt from NAT. The access list should already be defined, otherwise PIX Firewall gives an error message.
local_ip	Internal network IP address to be translated. You can use **0.0.0.0** to allow all hosts to start outbound connections. You can abbreviate **0.0.0.0** *local_ip* as **0**.
netmask	Network mask for *local_ip*. You can use **0.0.0.0** to allow all outbound connections to translate using IP addresses from the global pool.
max_conns	The maximum TCP connections permitted from the interface you specify.
em_limit	The embryonic connection limit. The default is **0**, which means unlimited connections. Set it lower for slower systems and higher for faster systems.
norandomseq	Do not randomize the TCP packet's sequence number. Use this option only if another inline firewall is also randomizing sequence numbers and the result is scrambling the data. Use of this option opens a security hole in the PIX Firewall.

Step 5 Define the global pool.

The **global** command defines a pool of global addresses. The global addresses in the pool provide an IP address for each outbound connection, and for those inbound packets resulting from outbound connections.

If the **nat** command is used, you must also use the **global** command. Basically, when an outbound IP packet is sent from the inside network, the PIX Firewall extracts the source address and compares that address to the list of current NAT translations. If there is no entry, a new entry is created. If a NAT entry already exists, the packet is forwarded.

The PIX syntax for the **global** command is defined as follows:

```
global [(if_name)] nat_id global_ip [-global_ip] [netmask global_mask]
[interface]
```

In Figure 6-5, the pool of addresses is defined as follows:

```
global (outside) 1 192.192.1.2-192.192.1.30 netmask 255.255.255.224
```

The pool of addresses is typically assigned to you by the InterNIC or your ISP.

Table 6-7 defines the options of the **global** command, as documented on the Cisco Documentation CD-ROM.

Table 6-7 **global** *Command Options*

Option	Description
if_name	The external network where you use these global addresses.
nat_id	A positive number shared with the **nat** command that groups the **nat** and **global** command statements together. The valid ID numbers can be any positive number up to 2,147,483,647.
global_ip	One or more global IP addresses that the PIX Firewall shares among its connections. If the external network is connected to the Internet, each global IP address must be registered with the InterNIC. You can specify a range of IP addresses by separating the addresses with a dash (**-**). You can create a PAT **global** command statement by specifying a single IP address. You can have more than one PAT **global** command statement per interface. A PAT can support up to 64,000 xlate objects.
netmask	Reserved word that prefaces the network *global_mask* variable.
global_mask	The network mask for *global_ip*. If subnetting is in effect, use the subnet mask; for example, 255.255.255.128. If you specify an address range that overlaps subnets, **global** will not use the broadcast or network addresses in the pool of global addresses. For example, if you use 255.255.255.224 and an address range of 209.165.201.1 to 209.165.201.30, the 209.165.201.31 broadcast address and the 209.165.201.0 network address will not be included in the pool of global addresses.
interface	Specifies PAT using the IP address at the interface.

Step 6 Finally, define how to route IP data with the **route** command.

Use the **route** command to enter a default or static route for an interface. The PIX Firewall syntax is as follows:

```
route if_name ip_address netmask gateway_ip [metric]
```

Configuring Static Routing on a PIX Firewall

Figure 6-5 defines all routes via the perimeter router as follows:

```
route outside 0.0.0.0 0.0.0.0 131.108.1.2
```

Table 6-8 defines the options of the **route** command, as documented on the Cisco Documentation CD-ROM.

Table 6-8 **route** *Command Options*

Option	Description
if_name	The internal or external network interface name.
ip_address	The internal or external network IP address. Use **0.0.0.0** to specify a default route. You can abbreviate the **0.0.0.0** IP address as **0**.
netmask	Specify a network mask to apply to *ip_address*. Use **0.0.0.0** to specify a default route. The **0.0.0.0** netmask can be abbreviated as **0**.
gateway_ip	Specify the IP address of the gateway (the next-hop address for this route).
metric	Specify the number of hops to *gateway_ip*. In Figure 6-5, this is 1.

Example 6-4 displays the full working configuration of the PIX Firewall shown in Figure 6-5. The shaded portions of this display are configuration commands we have entered, and the nonshaded portions are default configurations. One of the advantages of the PIX Firewall, like the Catalysts Ethernet switch, is that you can view the full working and default configuration, unlike Cisco IOS routers, for which the default configuration is not displayed.

Example 6-4 *PIX Firewall Full Working Configuration*

```
pix# write terminal
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
hostname pixfirewall
 fixup protocol ftp 21
 fixup protocol http 80
 fixup protocol smtp 25
 fixup protocol h323 1720
 fixup protocol rsh 514
 fixup protocol sqlnet 1521
 names
 name 1.1.1.1 abcd
 name 1.1.1.2 a123456789
 name 1.1.1.3 a123456789123456
 pager lines 24
 logging timestamp
 no logging standby
 logging console debugging
 no logging monitor
 logging buffered debugging
 no logging trap
 logging facility 20
 logging queue 512
 interface ethernet0 10full
 interface ethernet1 10full
 mtu outside 1500
 mtu inside 1500
```

continues

Example 6-4 *PIX Firewall Full Working Configuration (Continued)*

```
ip address inside 201.201.201.1 255.255.255.0
ip address outside 131.108.1.1 255.255.255.0
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 arp timeout 14400
global (outside) 1 192.192.1.2-192.192.1.30 netmask 255.255.255.224
nat  (inside) 1 0.0.0.0 0.0.0.0
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 route outside 0.0.0.0 0.0.0.0 131.108.1.2 1
 timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00 udp 0:02:00
 timeout rpc 0:10:00 h323 0:05:00
 timeout uauth 0:00:00 absolute
 no snmp-server location
 no snmp-server contact
 snmp-server community public
 no snmp-server enable traps
 telnet timeout 5
 terminal width 80
: end
```

NOTE Note the order of preference for the PIX Firewall when NAT is enabled:

- NAT 0 access list
- Static NAT
- Static PAT
- Policy NAT
- Regular NAT

Miscellaneous PIX Firewall Commands

Three other important commands that are commonly used in PIX Firewall configurations are the **static**, **conduit**, and **alias** commands.

The **static** command creates a permanent mapping (Cisco documentation names or calls this a translation slot or xlate) between a local IP address and a global IP address. Use the **static** and **conduit** commands when you are accessing an interface of a higher security level from an interface of a lower security level; for example, when accessing the inside interface from the outside interface.

The command syntax is as follows:

```
static [(internal_if_name, external_if_name)] global_ip local_ip [netmask
network_mask] [max_conns [em_limit]] [norandomseq]
```

Table 6-9 defines the options of the **static** command, as documented on the Cisco Documentation CD-ROM.

Table 6-9 **static** *Command Options*

Option	Description
internal_if_name	The internal network interface name. The higher-security-level interface you are accessing.
external_if_name	The external network interface name. The lower-security-level interface you are accessing.
global_ip	A global IP address. This address cannot be a PAT IP address. The IP address on the lower-security-level interface you are accessing.
local_ip	The local IP address from the inside network. The IP address on the higher-security-level interface you are accessing.
netmask	Reserved word required before specifying the network mask.
network_mask	Pertains to both *global_ip* and *local_ip*. For host addresses, always use 255.255.255.255. For network addresses, use the appropriate class mask or subnet mask; for example, for Class A networks, use 255.0.0.0. An example subnet mask is 255.255.255.224.
max_conns	The maximum number of connections permitted through the static connection at the same time.
em_limit	The embryonic connection limit. An embryonic connection is one that has started but not yet completed. Set this limit to prevent attack by a flood of embryonic connections. The default is **0**, which means unlimited connections.
norandomseq	Do not randomize the TCP/IP packet's sequence number. Use this option only if another inline firewall is also randomizing sequence numbers and the result is scrambling the data. Use of this option opens a security hole in the PIX Firewall.

An example of the command is as follows:

```
static (inside,outside) 192.192.1.33  201.201.201.10
```

The **static** command should be used in conjunction with either **conduit** or **access-list**. A **conduit** command statement creates an exception to the PIX Firewall ASA mechanism by permitting connections from one firewall network interface to access hosts on another.

NOTE If a conduit or access list is not configured on the PIX Firewall, then by default all traffic will be dropped, resulting in the PIX Firewall acting like a black hole or bit bucket router. By default, the PIX Firewall will drop all traffic unless configured otherwise.

The **clear conduit** command removes all **conduit** command statements from your configuration.

The **conduit** command syntax is defined as follows:

```
conduit {permit | deny} protocol global_ip global_mask [operator port [port]]
    foreign_ip foreign_mask [operator port [port]]
```

Table 6-10 displays the options and command syntax for the **conduit** command, as documented on the Cisco Documentation CD-ROM.

Table 6-10 **conduit** *Command Options*

Option	Description
permit	Permits access if the conditions are matched.
deny	Denies access if the conditions are matched.
protocol	Specifies the transport protocol for the connection. Possible literal values are **icmp**, **tcp**, **udp**, or an integer in the range 0 through 255, representing an IP protocol number. Use **ip** to specify all transport protocols.
global_ip	A global IP address previously defined by a **global** or **static** command. You can use **any** if the *global_ip* and *global_mask* are 0.0.0.0 0.0.0.0. The **any** option applies the **permit** or **deny** parameters to the global addresses.
global_mask	Network mask of *global_ip*. The *global_mask* is a 32-bit, four-part dotted-decimal address, such as 255.255.255.255. Use 0s in a part to indicate bit positions to be ignored. Use subnetting, if required. If you use 0 for *global_ip*, use 0 for *global_mask*; otherwise, enter the *global_mask* appropriate to *global_ip*.
foreign_ip	An external IP address (host or network) that can access the *global_ip*. You can specify 0.0.0.0 or 0 for any host. If both the *foreign_ip* and *foreign_mask* are 0.0.0.0 0.0.0.0, you can use the shorthand **any** option.
foreign_mask	Network mask of *foreign_ip*. The *foreign_mask* is a 32-bit, four-part dotted-decimal address, such as 255.255.255.255. Use 0s in a part to indicate bit positions to be ignored. Use subnetting, if required.
operator	A comparison operand that lets you specify a port or a port range. Use without an operator and port to indicate all ports. For example, **conduit permit tcp any any**. By default, all ports are denied until explicitly permitted.
port	Service(s) you permit to be used while accessing *global_ip or foreign_ip*. Specify services by the port that handles them, such as **smtp** for port 25, **www** for port 80, and so on. You can specify ports by either a literal name or a number in the range of 0 to 65,535. You can specify all ports by not specifying a port value (for example: **conduit deny tcp any any**).

PIX Firewall software version 6.2 allows NAT of external source IP addresses for packets traveling from the outside interface to the inside interface. All functionality available with traditional NAT, such as fixups, stateful failover, dynamic NAT, static NAT, and PAT, are available bidirectionally in this release.

The **alias** command translates one address into another. The **alias** command is used when registered addresses have been used in a private network and access is required to the registered address space on the Internet. Consider the following example: the inside network contains the IP subnet address 64.236.16.0/24. Assume this belongs to the website at www.cnn.com.

When inside clients try to access www.cnn.com, the packets do not go to the firewall because the client thinks 64.236.16.0/24 is on the local inside network. To correct this, a net **alias** is created as follows with the **alias** command:

```
alias (inside) 64.236.16.0 131.108.2.0 255.255.255.0
```

When the inside network client 64.236.16.0 connects to www.cnn.com, the DNS response from an external DNS server to the internal client's query would be altered by the PIX Firewall to be 131.108.2.1-254/24.

NOTE The **alias** command is replaced in newer versions with a **dns** keyword in **static** and **nat** commands.

Advanced Cisco PIX Commands

Table 6-11 summarizes some of the other useful features on a Cisco PIX Firewall, as documented on the Cisco Documentation CD-ROM.

Table 6-11 *PIX Firewall Advanced Features*

Command	Use
ca	Configure the PIX Firewall to interoperate with a Certificate Authority (CA).
clear xlate	Clear the contents of the translation slots.
show xlate	Display NAT translations. The **show xlate** command displays the contents of only the translation slots.
crypto dynamic-map	Create, view, or delete a dynamic crypto map entry.
failover [*active*]	Use the **failover** command without an argument after you connect the optional failover cable between your primary firewall and a secondary firewall.
fixup protocol	The **fixup protocol** commands let you view, change, enable, or disable the use of a service or protocol through the PIX Firewall.

continues

Table 6-11 *PIX Firewall Advanced Features (Continued)*

Command	Use
kill	Terminate a Telnet session. Telnet sessions to the PIX Firewall must be enabled.
telnet ip_address [**netmask**] [*if_name*]	Specify the permitted host devices for PIX Firewall console access via Telnet.

Troubleshooting PIX Firewall Log Files

The PIX Firewall can be configured to send system messages to three different output locations. The first is the hardware-based console. Typically, organizations always maintain a remote connection to the console interface of the core firewall within their network. The second is through an active Telnet session, which is insecure, of course, because Telnet is a clear-text protocol. Finally to gather system log messages is through the PIX Device Manager (PDM). PIX logs can also be sent through SSH sessions, sent to the buffer, and sent as SNMP traps.

Messages can be sent from the PIX via TCP or UDP to a host-based system running a daemon such as syslogd on a UNIX server. Telnet is often used to view log files in a troubleshooting scenario. The preferred method is via the PDM or by sending SNMP traps from the firewall.

The PDM is a client/server application that provides a GUI for monitoring and managing the PIX Firewall.

The PIX Firewall events that can be reported via SNMP are contained in the Cisco SYSLOG MIB. Reading log messages on a PIX Firewall is similar to the way they are read on Cisco IOS routers. Syslog messages are of the following form:

```
%FACILITY-SEVERITY-CODE: Message-text
```

FACILITY identifies the message facility. PIX is the facility code for messages generated by the PIX Firewall.

SEVERITY reflects the severity of the condition described by the message. The lower the number, the more serious the condition. There are eight defined severity levels:

- **0**—Emergency (system unusable)
- **1**—Alert (immediate action needed)
- **2**—Critical (critical condition)
- **3**—Error (error condition)
- **4**—Warning (warning condition)

- **5**—Notification (normal but significant condition)
- **6**—Informational (informational message only)
- **7**—Debugging (appears during debugging only)

The severity levels do not apply for syslog messages sent to the console, monitor, or buffer.

Example 6-5 displays a few serious log messages that require urgent action from the security team within an organization.

Example 6-5 *Sample Log Message from a PIX Firewall*

```
pix(config)# show logging
Syslog logging: enabled
Timestamp logging: disabled
Standby logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level debugging, 4 messages logged
Trap logging: disabled
History logging: disabled
402103: identity doesn't match negotiated identity (ip) dest_addr= 10.10.10.10,
   src_addr= 192.168.1.2, prot= icmp, (ident) local=172.18.124.128,
   remote=172.18.124.141, local proxy=0.0.0.0/0.0.0.0/0/0,
   remote_proxy=192.168.1.1/255.255.255.0/0/0
08:00:011 0.1.1.254 : %PIX-7-402101: TCP request discarded from
    86.3.2.19/57088 to inside:10.1.1.1/www
```

The first shaded line in Example 6-5 is that of the PIX buffer and the second shaded line is being read from a syslog server.

Example 6-5 displays two log messages of interest—namely IPSec message 10.10.10.10 and the more serious log message stating that an inside source address 86.3.2.10 is trying to illegally send a TCP request to an inside interface on the PIX Firewall configured with the IP address 10.1.1.1 using HTTP or the World Wide Web.

Typically, the log messages are informative and easily deciphered. You can see some of the thousands of possible log outputs at http://www.cisco.com/en/US/partner/products/sw/secursw/ps2120/products_system_message_guide_book09186a00801582a9.html. Note that the version of PIX Firewall is not critical for the written exam but it is critical for the lab exam. Hence the link is placed here for your lab exam preparation only. Prior to taking the lab exam, review some of the more severe levels for version 6.3 on the PIX Firewall software.

Cisco PIX Firewall Software Features

A list of the current features of the Cisco PIX Firewall product follows:

- State-of-the-art Adaptive Security Algorithm (ASA) and stateful inspection firewalling.
- Cut-through proxy authenticates and authorizes connections, while enhancing performance.
- Easy-to-use web-based interface for managing PIX Firewalls remotely; using the web-based interface is not a suggested practice by Cisco for medium to large networks.
- Support for up to 10 Ethernet interfaces ranging from 10BASE-T, 10/100 Fast Ethernet to Gigabit Ethernet.
- Stateful firewall failover capability with synchronized connection information and product configurations.
- True NAT, as specified in RFC 1631.
- PAT further expands a company's address pool—one IP address supports 64,000 hosts.
- Support for IPSec and L2TP/PPTP-based VPNs.
- Support for high-performance URL filtering via integration with Websense-based URL filtering solutions.
- Mail Guard removes the need for an external mail relay server in the perimeter network.
- Support for broad range of authentication methods via TACACS+, RADIUS, and Cisco Access Control Server (ACS) integration.
- Domain Name System (DNS) Guard transparently protects outbound name and address lookups.
- Flood Guard and Fragmentation Guard protect against DoS attacks.
- Support for advanced Voice over IP (VoIP) standards.
- Java blocking eliminates potentially dangerous Java applets (not compressed or archived), extending AAA capabilities.
- Net Aliasing transparently merges overlapping networks with the same IP address space.
- Capability to customize protocol port numbers.
- Integration with Cisco IDSs for shunning connections of known malicious IP addresses.
- Enhanced customization of syslog messages.
- Simple Network Management Protocol (SNMP) and syslog for remote management.

- Reliable syslogging using either TCP or UDP.
- Extended transparent application support (both with and without NAT enabled) includes the following:
  - Sun Remote Procedure Call (RPC)
  - Microsoft networking client and server communication (NetBIOS over IP) using NAT
  - Multimedia, including RealNetworks' RealAudio, Xing Technologies' Streamworks, White Pines' CuSeeMe, Vocal Tec's Internet Phone, VDOnet's VDOLive, Microsoft's NetShow, VXtreme Web Theatre 2; and Intel's Internet Video Phone and Microsoft's NetMeeting (based on H.323 standards)
  - Oracle SQL*Net client and server communication
- VoIP/multimedia
- PAT for H.323 and Session Initiation Protocol (SIP)
- Dynamic Host Configuration Protocol (DHCP) server support for Cisco IP Phones
- Internet Locator Service (ILS) fixup

Cisco also publishes loopholes found in PIX Firewall software, such as the PIX Mail Guard feature, which was designed to limit SMTP messages but can be exploited by intruders. You can find the Cisco publications at http://www.cisco.com/en/US/partner/products/products_security_advisories_listing.html**.**

NOTE When troubleshooting why certain applications such as SMTP mail or L2TP (TCP 1701) tunnels are not working, a good starting point is always to look at which TCP or UDP ports are filtered by the PIX Firewall, because, by default, you must configure any TCP/UDP ports you will permit through the PIX Firewall with the **conduit** or **static translations** commands.

CCSP Self-Study: Cisco Secure PIX Firewall Advanced (CSPFA), 2nd Edition, by Behzad Behtash (Cisco Press, ISBN 1587051494), is an excellent resource if you want to learn more about the PIX Firewall.

Cisco IOS Firewall Feature Set

Cisco has developed a version of IOS with security-specific features integrated in current IOS software. It is available on only some Cisco IOS devices.

NOTE The need to provide firewall functionally in existing router models led Cisco down a path of enabling IOS to be security aware. Not many folks think of Cisco as a software company but, in fact, it sells more software than hardware.

The Cisco IOS Firewall feature set consists of the following:

- Context-Based Access Control (CBAC) provides to internal users secure, per-application-based access control for all traffic across perimeters, such as between private enterprise networks and the Internet.
- Java blocking protects against unidentified, malicious Java applets.
- DoS detection and prevention defends and protects router resources from common attacks, checking packet headers and dropping suspicious packets.
- Audit trail details transactions, recording time stamp, source host, destination host, ports, duration, and the total number of bytes transmitted.
- Real-time alerts log alerts in case of DoS attacks or other preconfigured conditions.

You can use the Cisco IOS Firewall feature set to configure your Cisco IOS router as the following bulleted points demonstrate:

- An Internet firewall
- A firewall between groups in your internal network
- A firewall providing secure connections to or from branch offices
- A firewall between your company's network and your company's partners' networks

For example, when a user authenticates from the Cisco IOS Firewall proxy, authentication is completed by HTTP and access lists are downloaded from a AAA server to authorized or rejected connections. The Cisco IOS Firewall feature set has many different applications for today's IP networks.

CBAC provides secure, per-application access control across the network. CBAC is designed to enhance security for TCP and UDP applications, and supports protocols such as H.323, RealAudio, and SQL-based applications, to name a few.

CBAC can filter TCP/UDP packets based on application layer, transport layer, and network layer protocol information. Traffic is inspected for sessions that originate on any given interface and also inspect traffic flowing through a firewall. CBAC can inspect FTP, TFTP, or SMTP traffic, but does

not inspect ICMP packet flows. Additionally, network administrators can debug network issues by using ICMP without concern that possible intruders may enter the network. Cisco IOS Firewall uses stateful inspection to trust ICMP messages that are generated within a private network and to permit the associated ICMP replies.

CBAC can even manually open and close openings (configure conduits, for example) in the firewall to test security in a network.

The following list provides samples of protocols supported by CBAC:

- TFTP
- SMTP
- Java Blocking
- Oracle SQL
- RealAudio
- H.323
- FTP
- StreamWorks
- VDOLive

The other major benefits of the Cisco IOS Firewall feature set include the following:

- Integrated solutions and no need for a PIX Firewall for investments already made in Cisco IOS routers.
- No new hardware is required (just a software upgrade).
- Allows for full IP routing capabilities.
- Cisco customers are already aware of IOS command structure.
- Low cost.

Cisco IOS Firewall feature-enabled routers should always maintain the same secure polices described in Chapter 7, “Network Security Policies, Vulnerabilities, and Protection,” such as password encryption and disabling nonessential services such as HTTP or DHCP.

CBAC Configuration Task List

Configuring CBAC requires the following tasks:

1. Pick an interface: internal or external.
2. Configure IP access lists at the interface.
3. Configure global timeouts and thresholds.
4. Define an inspection rule.
5. Apply the inspection rule to an interface.
6. Configure logging and audit trail.
7. Following other guidelines for configuring a firewall.
8. Verify CBAC (optional).

Example 6-6 shows a router named R1 with two Ethernet interfaces, one defined as the inside interface (Ethernet0) and the other defined as the outside interface (Ethernet1). For this example, CBAC is being configured to inspect Real-Time Streaming Protocol (RTSP) and H.323 protocol traffic inbound from the protected network on a router with two Ethernet interfaces. Interface Ethernet0 is the protected network, and interface Ethernet1 is the unprotected network. The security policy for the protected site uses ACLs to inspect TCP/UDP protocol traffic. Inbound access for specific protocol traffic is provided through dynamic access lists, which are generated according to CBAC inspection rules.

Example 6-6 *Access List* Definition

```
R1(config)# access-list 199 permit tcp any any  eq telnet
R1(config)# access-list 199 deny udp any any  eq  syslog
R1(config)# access-list 199 deny any any echo-reply
R1(config)# access-list 199 deny any any echo
R1(config)# access-list 199 deny any any time-exceeded
R1(config)# access-list 199 deny any any packet-too-big
R1(config)# access-list 199 permit any any traceroute
R1(config)# access-list 199 permit any any unreachable
R1(config)# access-list 199 permit deny ip any any
```

ACL 199 permits TCP and UDP traffic from any source or destination, while denying specific ICMP traffic and permitting ICMP trace route and unreachable messages. The final **deny** statement is not required but is included for explicitness—the final entry in any ACL is an implicit denial of all IP traffic. Example 6-6 defines access-list 199 on Router R1, which has two Ethernet interfaces: Ethernet0 and Ethernet1.

ACL 199 is applied inbound at interface Ethernet 1 to block all access (beside permitting Telnet, ICMP traceroute, and ICMP unreachables) from the unprotected network to the protected network. Example 6-7 configures the inbound ACL on R1.

Example 6-7 *R1 Access List Inbound Configuration*

```
R1(config)# interface ethernet1
R1(config-if)# ip access-group 199 in
```

An inspection rule is created for "users" that covers two protocols: RTSP and H.323. Example 6-8 configures R1 to inspect RTSP and H.323 traffic.

Example 6-8 *Inspected Traffic*

```
R1(config)# ip inspect name users rtsp
R1(config)# ip inspect name users h323
```

The inspection rule is applied inbound at interface Ethernet1 to inspect traffic from users on the protected network. When CBAC detects multimedia traffic from the protected network, CBAC creates dynamic entries in access-list 199 to allow return traffic for multimedia sessions. Example 6-9 configures the R1 unprotected network to inspect traffic on interface Ethernet0.

Example 6-9 *Inspects Traffic on R1 Protected Interface*

```
R1(config)# interface Ethernet0
R1(config-if)# ip inspect users out
```

You can view the CBAC logs by three methods:

- Debugging output (refer to the Cisco Documentation CD-ROM for full details)
- Syslog messages (IOS command is **show logging**)
- Console messages (system messages)

NOTE More advanced details on CBAC can be found at http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7c5.html.

After you complete the inspection of traffic, you can turn off CBAC with the global IOS command **no ip inspect**. The Cisco IOS Firewall feature set also supports AAA, TACACS+, and Kerberos authentication protocols. Port to Application Mapping (PAM) allows you to customize TCP or

UDP port numbers for network services or applications. The information in the PAM table enables CBAC-supported services to run on nonstandard ports.

NOTE Active audit and content filters are used with NetRanger and NetSonar (end of life) products to allow administrators to decipher (read and analyze) or reply (to the conversation between two devices) to networks when an intruder has accessed the network. CBAC is just another useful tool in Cisco IOS that allows a quick audit of an IP network. CBAC inspects traffic that travels through a firewall and can be used to discover and manage state information for TCP/UDP sessions.

Public Key Infrastructure

In the new digital environment, Public Key Infrastructure (PKI) ensures that sensitive electronic communications are private and protected from tampering. It provides assurances of the identities of the participants in those transactions, and prevents them from later denying participation in the transaction.

PKI does the following:

- Protects privacy by ensuring that the data is not read, but it can't stop someone from intercepting it. (If you can't read something, what's the use of that data?)
- Assures the integrity of electronic communications by ensuring that they are not altered during transmission.
- Verifies the identity of the parties involved in an electronic transmission.
- Ensures that no party involved in an electronic transaction can deny involvement in the transaction. (Collectively these last three bulleted points are known as nonrepudiation.)

Before you send data over the public Internet, you want to make sure that the data, no matter how sensitive, won't be read by the wrong source. PKI enables data to be sent encrypted by use of a public key, cryptography, and digital signatures.

Public key cryptography ensures the confidentiality of sensitive information or messages using a mathematical algorithm, or key, to scramble (encrypt) data, and a related mathematical key to unscramble (decrypt) it. In public key cryptography, authorized users receive special encryption software and a pair of keys, one an accessible public key, and the other a private key, which the user must keep secret.

A digital signature standard (DSS) is an electronic identifier comparable to a traditional, paper-based signature—it is unique and verifiable, and only the signer can initiate it.

Before any communication can take place, both parties involved in the data communication must obtain a digital certificate from a Certificate Authority (CA), a trusted third party responsible for issuing digital certificates and managing them throughout their lifetime.

Consider the following example: a user named Simon wants to communicate with a user named Sharon. Simon already has his digital certificate but Sharon has yet to obtain one. Sharon must identify herself to the CA to obtain a certificate. This is analogous to a passport when you travel internationally. When Sharon obtains her digital certificate, it contains a copy of her public key, the certificate's expiration date, and the CA's digital signature. Each of these details is public.

Sharon creates a private key, which is not shared with anyone. If Sharon wants to create an asymmetric key pair, she would generate the pair, keep the private key locked via password, and send the public key to the CA for its signature. Now that both parties have a DSS, they can communicate and encrypt data using their public key, but they can decrypt only the data using their respective private keys. Pretty Good Privacy (application layer tool) is an excellent example of this type of communication. I suggest that you install the software (free demonstration version) and try PKI for yourself. You can find the free software at http://www.pgp.com.

Virtual Private Networks

A virtual private network (VPN) enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level. VPN communication is encrypted, private and secure, even though it traverses the public network.

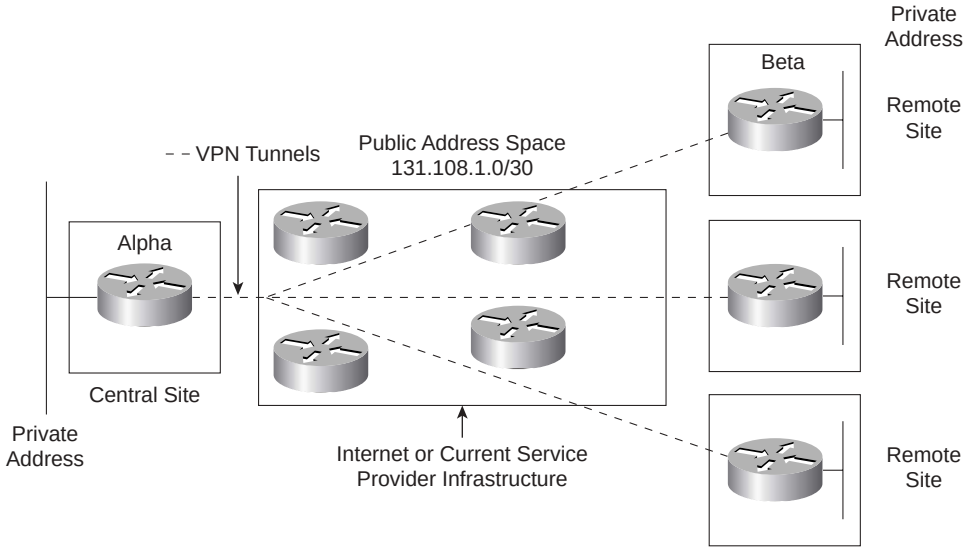
VPN is very loosely defined as a network in which a customer or end user connects to one or more sites through a public infrastructure, such as the Internet or World Wide Web.

VPNs are typically set up permanently between two or more sites. Figure 6-6 displays a typical VPN design.

Figure 6-6 displays a typical hub (central site) to spoke (remote site) model, where the existing public infrastructure transports data. IP generic routing encapsulation (GRE) tunnels can be set up between the hub and spoke routers, and any protocol can run over the IP tunnel.

Consider an example where the router, Alpha, needs to communicate with the remote site, Router Beta. At no time should the private address space be advertised to any public domain. Assuming that IP routing is enabled and configured, we can configure an IP GRE tunnel between Alpha and Beta.

Figure 6-6 *VPN Model*



Assume that you have a client who wants to create a VPN across your network. The client's main network is attached via Alpha over the Internet IP cloud. The client has a group of employees in its own IP space on the Ethernet interface. The client has a classless interdomain routing (CIDR) block of 192.1.64.0/20 for the network attached to the Alpha router, and the CIDR block 141.108.32.0/20 to the network attached to the Beta router. The network 131.108.1.0/30 is assigned between the routers and is pingable.

Example 6-10 configures Alpha with a GRE tunnel pointing to the remote IP address 131.108.1.2/30 (Beta's Serial IP address) and uses 131.108.1.5 for the loopback interface.

Example 6-10 *Alpha GRE Tunnel*

```
hostname Alpha
!
interface Loopback0
 ip address 131.108.1.5 255.255.255.255
! IP GRE tunnel configuration follows
interface Tunnel0
Description Non overlapping subnet
 ip address 192.1.63.1 255.255.255.0
 tunnel source Loopback0
 tunnel destination 131.108.1.2
!
interface Ethernet0/0
 ip address 192.1.65.1 255.255.240.0
```

Example 6-10 *Alpha GRE Tunnel (Continued)*

```
!
interface Serial0
Description Link to Beta via Internet Cloud
ip address 131.108.1.1 255.255.255.252
!
router ospf 1
network 192.1.64.0 0.0.15.255 area 0

End
```

Example 6-11 configures Beta with a GRE tunnel pointing to the remote IP addresses 131.108.1.1/30 and 131.108.1.6/32 for loopback use.

Example 6-11 *Beta GRE Tunnel*

```
hostname Beta
!
interface Loopback0
 ip address 131.108.1.6 255.255.255.255
! IP GRE tunnel configuration follows
interface Tunnel0
 ip address 192.1.63.2 255.255.255.0
tunnel source Loopback0
 tunnel destination 131.108.1.1
!
interface Ethernet0/0
 ip address 141.108.32.1 255.255.240.0
!
router ospf 1
network 192.1.64.0 0.0.15.255 area 0
interface Serial0
Description Link to Alpha via Internet Cloud
ip address 131.108.1.2 255.255.255.252
!
End
```

The IP GRE tunnel is now configured between the routers Alpha and Beta. While using public address space for the source and destination of the VPN tunnel, the reserved CIDR block 192.1.64.0/20 will not be advertised or routable over the public domain. The private traffic can now flow between both hub site and remote site securely.

The next section introduces another new objective of the CCIE Security blueprint, namely network IDS, including anomalies, signatures, passive, and inline.

Network-Based Intrusion Detection Systems

You will be forgiven for looking at this new blueprint objective and wondering what exactly is to be expected of a candidate taking the new CCIE Security written exam. This section unravels this objective and provides you with the best preparation possible to ensure that you pass this portion of the exam on your first attempt.

Network-based intrusion detection has been defined by many security vendors, such as Cisco, which has defined IDS as a method of detecting an illegal packet within your network. Ensuring that IP packets and TCP segments are valid can be an enormous task in today's ever-evolving networks because all organizations need to be connected to the public domain, the World Wide Web. To effectively run e-commerce within an organization, the basic aim of the Cisco network-based IDS (NIDS) solution is to proactively detect network packets and segment what may be illegal and to alert the security team within the organization. For the CCIE Security written exam, your basic knowledge of how the Cisco network-based IDS functions is what you can expect to be tested upon.

First, the following list defines a few basic terms you should be aware of:

- **Signature**—A set of conditions that, when met, indicates some type of intrusion event.
- **Pattern matching**—Searching for a fixed sequence of bytes within an IP packet (encompassing, of course, TCP or UDP details).
- **Stateful pattern matching**—A far more sophisticated method of searching for certain patterns is stateful pattern matching–based analysis. Instead of looking at only one packet, this method looks at the actual flow of packets between two end systems.
- **Protocol decode–based analysis**—Protocol decode–based signatures are in many ways intelligent extensions to stateful pattern matches. This class of signature is implemented by decoding the various elements in the same manner as would the client or server in the conversation. When the elements of the protocol are identified, the IDS applies rules defined by the RFCs to look for violations.
- **Heuristic-based analysis**—Heuristic-based signatures use some type of algorithmic logic on which to base their alarm decisions. A port sweep is a typical attack that will be detected.
- **Anomaly-based analysis**—Anomaly-based signatures are typically geared to look for network traffic that is a variation from the normally expected data types. Typically, a strong differentiation is required between normal and abnormal.

These methods have their pros and cons. To date, the Cisco strategy for NIDS is to blend the use of pattern matching, stateful pattern matching, protocol decodes, and heuristic-based signatures.

Passive or Inline IDS?

A passive IDS module receives copies of all the traffic passing through the backplane—for example, on a Cisco 2600 or 3600 router. The IDS sensor simply analyzes all captured data and compares it to set defined rules, called signatures.

An inline IDS module analyzes all traffic passing from one network to another, such as through a PIX Firewall.

Cisco supplies a new agent with every Cisco CallManager installation and recommends its use in any network, namely Cisco Security Agent (CSA), discussed next.

You will now cover the Cisco CSA agent and Host-Based IDS systems.

Cisco Security Agent and Host-Based IDS

CSA provides threat protection for servers and PCs. CSA identifies and prevents malicious behavior, thereby eliminating known and unknown security risks. Typically, devices with antivirus software do not detect the latest worms or code violations. CSA fills in this gap by triggering an alert to the system or the management server any time an application or packet tries to use the kernel inside a Windows-based system. CSA also blocks the attack. CSA can be installed as a standalone client or in a client/server-based model.

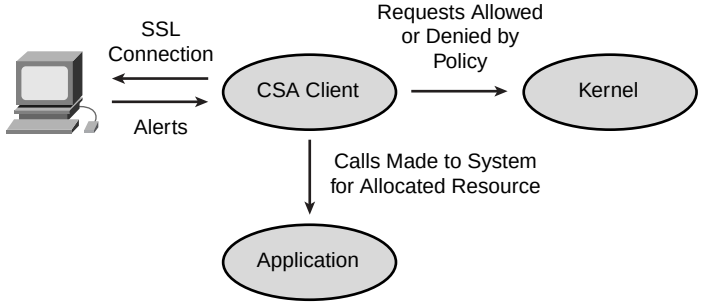
CSA is best defined as a set of predefined rules that protect a host-based system such as a PC or server. CSA is a host-based intrusion prevention system (HIPS) that provides a third layer of depth to any network defense by ensuring that security measures in place actually behave as required by the defined security policy. The following features enable CSA to stop attacks missed at other levels of security:

- CSA proactively blocks intrusive attacks.
- CSA is not dependent upon signatures and does not require updates to stop the latest viruses or worms.
- CSA effectively reduces the number of false positives within a network.

Figure 6-7 displays how CSA intercepts system calls to the operating system kernel.

Figure 6-7 displays the CSA architecture model, whereby the Management Center for Cisco Security Agents (CSA MC) allows the administrator to divide network hosts into groups by function and security requirements. The CSA software is installed on the client PC and continually monitors local system activity and ensures proper analysis is made of the end workstation. The administrative workstation ensures that all communication to the client is secured by using the SSL protocol. CSA is supported on Windows- and UNIX-based platforms.

Figure 6-7 *HIPS and CSA*



As a HIPS application, CSA provides host intrusion prevention, distributed firewall capabilities, malicious mobile code protection, operating system integrity assurance, and audit log consolidation.

CSA relies on analyzing all types of behavior rather than on signature matching. Typically that is what antivirus tools rely on. Hence, any unknown behavior is denied automatically.

For example, Code Red and SQL Slammer worms have penetrated many systems, resulting in network outages, as widely reported in the press. Traditional defense mechanisms have proven to be insufficient against these worms. CSA would have stopped these worms from malicious activity by denying the application access to any resources on the host and terminating the program immediately.

Typically a new worm tries to accomplish an attack with a five-staged approach:

1. Probe
2. Penetrate
3. Persist
4. Propagate
5. Paralyze

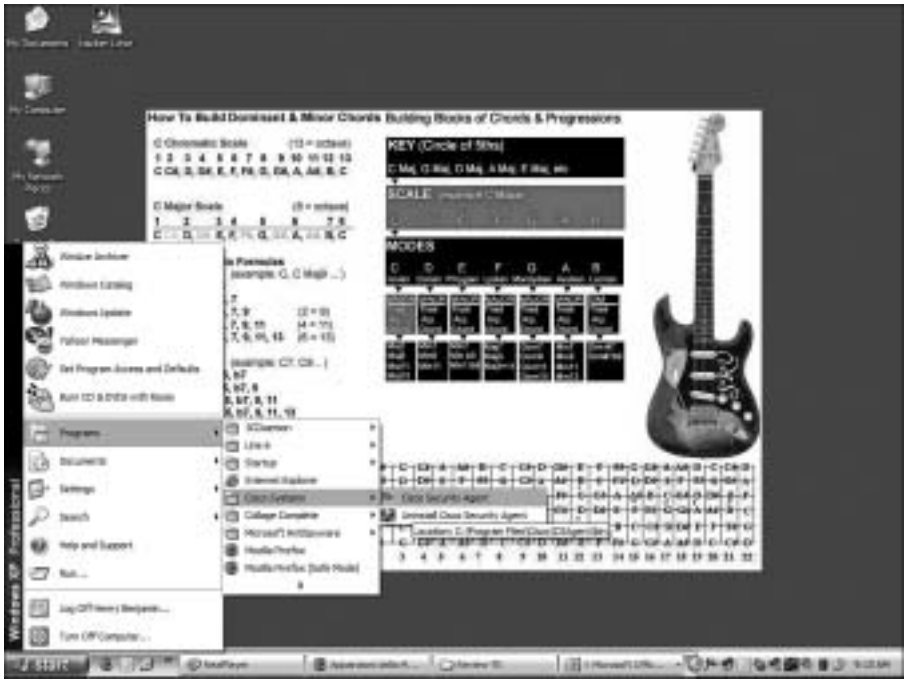
The types of attacks that can be stopped by CSA are numerous. The following points demonstrate how CSA responds to the stages and what countermeasures it uses:

- **Probes**—CSA prevents scanning of ports and ping packets.
- **Penetration**—CSA prevents unauthorized mail attachments from running, buffer overflows, ActiveX controls, network installs, backdoors, guessing passwords, and guessing of mail users.

- **Persist**—CSA prevents new file creation, modification of existing files, and register trap doors.
- **Propagate**—CSA prevents mail clients from sending out e-mails to propagate the attack, web connections, FTP, and infecting file shares.
- **Paralyze**—CSA does not permit deletion or modification of files and prevents drilling of security holes (opening new doors to provide an opening into your network or device).

Figure 6-8 displays a client PC running CSA. The agent runs in the background and cannot be suspended or terminated unless permitted to do so by the CSA management station.

Figure 6-8 *CSA Agent in System Tray*



When a suspicious activity occurs, a balloon message or pop-up window appears on the client and requests action, if it is not already defined on the management station. Figure 6-9 displays a suspicious activity for which a message appears.

Figure 6-9 *CSA Preventative Action*

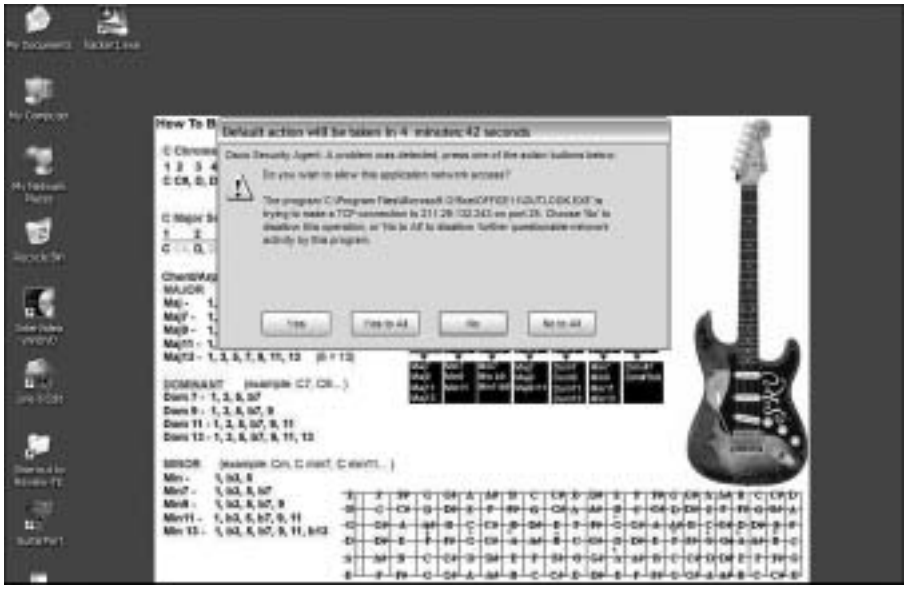


Figure 6-10 *CSA Balloon Message*

Figure 6-10 displays CSA in action after a suspicious application is launched by the client host (the balloon message is displayed by right-clicking the CSA icon in the system tray). If the action required is suspicious, the end user should deny the request, at which time CSA will ensure that the application is terminated. CSA will not permit the same application to run again and sends an alert to the host management station for action by your security team. A log message is also saved locally.

Cisco training has a very good course on HIPS named "Securing Hosts by Using CSA." Go to Cisco.com and search by the course name for more details. This is a good course for those interested in deploying this tool across a large or medium IP network.

Cisco has recently released Cisco Trust Agent (CTA) as part of its self-defending network strategy. CTA allows Network Admission Control (NAC) to determine if CSA or antivirus software is installed and current, and can determine current OS version and patch levels. For more details on CTA and Cisco self-defending solutions, go to http://www.cisco.com/security/.

Cisco Threat Response

Cisco security and IDS provide a mechanism to detect when an intrusion has occurred. The only problem in an HIDS is that a lot of alarms are false positives, especially in a large installation base of CSA clients. In other words, many alarms need not cause your security team to investigate a normal IP packet or TCP segment, for example. A CCIE candidate, however, must be able to tune out normal IP packets and TCP segments in the CCIE lab portion of this certification. The main concern is to ensure that valid attacks are identified and that the network infrastructure is protected.

The Cisco Threat Response (CTR) server-based application is an intelligent technology that eliminates false alarms and ensures that attacks are reported correctly and in real time. CTR is a software-based application.

The three-phased approach used by CTR is as follows:

1. Basic investigation to target vulnerability
2. Advanced investigation of target
3. Forensic data capture

The end goal of CTR is to be able to classify alarms coming into a destination device or system and validate them based on operating system types, patch levels, and actual log files on the end systems.

CTR ensures that your network is constantly monitored and that threats are immediately reported. This ensures that your significant investment in IDS is enhanced.

Ensuring that only real-time, valid threats are investigated means that the network infrastructure can be fully protected from most forms of attacks in an efficient manner. The best way to describe the CTR tool is to say that CTR reads IDS alarms and performs automated forensics on hosts or servers that may have been compromised.

For more details on CTR, visit http://www.cisco.com/en/US/partner/products/sw/secursw/ps5054/index.html or search on the keywords "Cisco Threat Response" at Cisco.com.

Cisco Threat Response IDS Requirements

CTR works in conjunction with intrusion detection systems. Your network should have an installation of either or both of the following IDSs:

- Cisco Intrusion Detection System version 3.x or higher
- Internet Security Systems RealSecure—CTR has been tested with RealSecure versions 6.5 and 7.0

You can access the CTR GUI from any computer in your environment; CTR uses an SSL connection under Microsoft Internet Explorer. For example, to access the CTR server with an IP address of 192.168.100.100, simply type this URL in your Explorer address box:

https://192.168.100.100

HTTPS specifies that your application should use SSL.

With the need for greater security between devices and switches, the IEEE committee came up with a new technology, 802.1X authentication.

Authorization Technologies (IOS Authentication 802.1X)

IEEE 802.1X is a new standard that defines enhanced security for IP networks. IEEE 802.1X specifically defines a client/server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports.

802.1X works by authenticating every client on the network—that is, every device connected to a switch port. After successful authentication, the individual switch port is assigned a VLAN. Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol

over LAN (EAPOL) traffic. After successful authentication, normal traffic can pass through the switch port. The primary purpose of 802.1X is to permit Layer 3 connectivity, that is, IP connectivity. 802.1X is initiated only when a device is connected to a switch port, and can also be used in a wireless network through an access point.

Figure 6-11 displays a typical scenario whereby a user has connected a device such as a PC to an available switch port.

Figure 6-11 *IEEE 802.1X Functions*

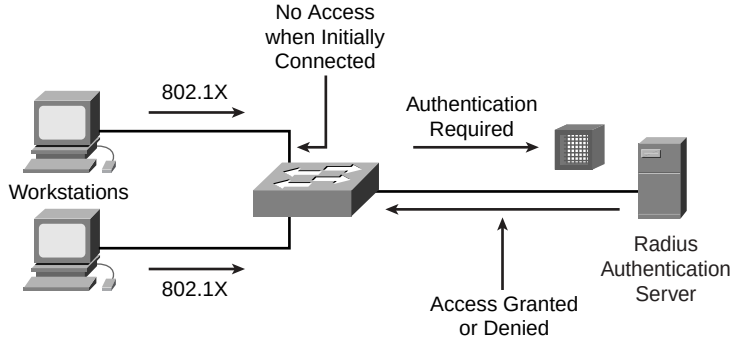


Figure 6-11 displays the various functions carried out by each device. The client workstation initially requests access to the LAN. The client is enabled for 802.1X. For example, Microsoft Windows XP has support for 802.1X. Simply configure your network card for 802.1X support using the operating system's instructions.

The Cisco IOS–based switch is also enabled for 802.1X through IOS software. The switch then responds to the request of the client to join the LAN.

The RADIUS authentication server actually performs the authentication of the end workstation or client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. This means the switch becomes the transparent proxy by sending all frames to the RADIUS server and back from the RADIUS server to the workstation. RADIUS (with Extensible Authentication Protocol [EAP] extensions) is the protocol used to authenticate the client. Because the switch acts as the proxy, the authentication service is transparent to the client. (The client is referred to as the supplicant in the 802.1X documentation.)

The Cisco IOS–based switch (also called the authenticator and back-end authenticator) controls the physical access to the network based on the authentication status of the client. The switch acts and verifies information between the workstation and the RADIUS server.

The switch port state can be in one of three states:

- **Authorized**—Successful authentication and normal packet flow.
- **Unauthorized 802.1X**—If a client device does not support 802.1X authentication, the port is left unauthorized.
- **802.1X enabled**—If a client is enabled for 802.1X but the switch port is not configured for 802.1X support, the client initiates but will not receive a reply. The client then sends packets, assuming that the authorization was granted.

802.1X is still new to the IP community, and the uptake has been rather slow, but it is more common in North America. The rest of the world is trying to catch up.

Foundation Summary

The "Foundation Summary" is a condensed collection of material for a convenient review of this chapter's key concepts. If you are already comfortable with the topics in this chapter and decided to skip most of the "Foundation Topics" material, the "Foundation Summary" will help you recall a few details. If you just read the "Foundation Topics" section, this review should help further solidify some key facts. If you are doing your final preparation before the exam, the "Foundation Summary" offers a convenient and quick final review.

Table 6-12 *Perimeter or Firewall Router Functions*

Function	Method
Sniffer or snooping capabilities	Control eavesdropping with TCP/IP service and network layer encryption (IPSec).
Control unauthorized access	Use AAA and Cisco Secure ACS. Also, use access-list filtering and PIX Firewall.
Control session replay	Control which TCP/IP sessions are authorized. Block SNMP, IP source routing, and finger services to outside hosts.
Control inbound connections	Filter internal address as the source from the outside world. Filter all private addresses. Filter Bootp, TFTP, and traceroute commands. Allow connections only for required services. Allow TCP connections established from the inside network. Permit inbound traffic to DMZs only.
Control outbound connections	Allow only valid IP addresses to the outside world and filter remaining illegal addresses and outbound service requests.
Packet filtering	Use predefined access lists that control the transmission of packets from any given interface, control vty lines and access, and ensure that routing updates are authenticated.

Table 6-13 *NAT Configuration Steps*

Step	Description
1	Determine the network addresses to be translated.
2	Configure the inside interface with the IOS **ip nat inside** command.
3	Configure the outside interface with the IOS **ip nat outside** command.
4	Define a pool of addresses to be translated with the following IOS command: **ip nat pool** *pool-name start-ip-address end-ip-address mask*
5	Define the addresses allowed to access the Internet with the following IOS command: **ip nat inside source list** *access-list-number* **pool** *pool-name*

Table 6-14 *Cisco PIX Model Numbers*

PIX 501
PIX 506/506E
PIX 515/515E
PIX 520
PIX 525
PIX 535

Table 6-15 *PIX Firewall Configuration Steps*

Step	Description
1	Name the inside/outside interfaces and security levels.
2	Identify the hardware interfaces and speed/duplex.
3	Define the IP address for inside and outside interfaces.
4	Define NAT/PAT.
5	Define the global pool.
6	Define the IP route path.
7	Define statics or static/access lists (for outside networks to access inside hosts or networks).

Table 6-16 *PIX Command Options*

Option	Use
ca	Configure the PIX Firewall to interoperate with a CA.
clear xlate	Clear the contents of the translation slots.
show xlate	Display NAT translations. The **show xlate** command displays the contents of only the translation slots.
crypto dynamic-map	Create, view, or delete a dynamic crypto map entry.
failover [*active*]	Use the **failover** command without an argument after you connect the optional failover cable between your primary firewall and a secondary firewall.
fixup protocol	View, change, enable, or disable the use of a service or protocol through the PIX Firewall.
kill	Terminate a Telnet session. Telnet sessions to the PIX must be enabled and are sent as clear text.
telnet *ip_address* [**netmask**] [*if_name*]	Specify the internal host for PIX Firewall console access through Telnet.

Table 6-17 *Cisco IOS Firewall Feature Set*

Feature	Function
CBAC	Provides to internal users secure, per-application-based access control for all traffic across perimeters, such as between private enterprise networks and the Internet. CBAC supports the following: • TFTP • SMTP • Java blocking • Oracle SQL • RealAudio • H.323 • VoIP/multimedia • PAT for H.323 and SIP • DHCP server support for Cisco IP Phones • Internet Locator Service (ILS) fixup
Java blocking	Protects against unidentified, malicious Java applets.
DoS detection and prevention	Defends and protects router resources against common attacks, by checking packet headers and dropping suspicious packets.
Audit trail	Details transactions, recording time stamp, source host, destination host, ports, duration, and total number of bytes transmitted.
Real-time alerts	Logs alerts in case of DoS attacks or other preconfigured conditions (intrusion detection).
Firewall	An Internet firewall.

Table 6-18 *PIX Syslog*

Level	Function
0	**Emergency**—System unusable
1	**Alert**—Immediate action needed
2	**Critical**—Critical condition
3	**Error**—Error condition
4	**Warning**—Warning condition
5	**Notification**—Normal but significant condition
6	**Informational**—Informational message only
7	**Debugging**—Appears during debugging only

Table 6-19 *Network IDS Terminology*

Term	Description
Signature	A set of conditions that, when met, indicates some type of intrusion event.
Pattern matching	Searching for a fixed sequence of bytes within an IP packet (encompassing TCP or UDP details).
Stateful pattern matching	A far more sophisticated method of searching for certain patterns.
Protocol decode–based analysis	Protocol decode–based signatures are in many ways intelligent extensions to stateful pattern matches. This class of signature is implemented by decoding the various elements in the same manner as would the client or server in the conversation. When the elements of the protocol are identified, the IDS applies rules defined by the RFCs to look for violations.
Heuristic-based analysis	Heuristic-based signatures use some type of algorithmic logic on which to base their alarm decisions.
Anomaly-based analysis	Anomaly-based signatures are typically geared to look for network traffic that is a variation from the normally expected data types.

Table 6-20 *Five Stages of Attack*

Method	Mitigated by CSA
Probe	CSA prevents scanning of ports and ping packets.
Penetrate	CSA prevents unauthorized mail attachments running, buffer overflows, ActiveX controls, network installs, backdoors, guessing passwords, and guessing of mail users.
Persist	CSA prevents new file creation, modification of existing files, and register trap doors.
Propagate	CSA prevents mail clients from sending out e-mails to propagate the attack, web connections, FTP, and infecting file shares.
Paralyze	CSA does not permit deletion or modification of files and prevents drilling of security holes (opening new doors to provide an opening into your network or device).

Q & A

The Q & A questions are designed to help you assess your readiness for the topics covered on the CCIE Security written exam and those topics presented in this chapter. This format should help you assess your retention of the material. A strong understanding of the answers to these questions will help you on the CCIE Security written exam. You can also look over the questions at the beginning of the chapter again for further review. As an additional study aid, use the CD-ROM provided with this book to take simulated exams, which draw from a database of over 500 multiple-choice questions.

Answers to these questions can be found in Appendix A, "Answers to Quiz Questions."

1. What does the term DMZ refer to?
2. What is the perimeter router's function in a DMZ?
3. Extended access lists filter the services of what two main transport layer protocols?
4. Which of the following is *not* a TCP service?
   a. Ident
   b. FTP
   c. pop3
   d. pop2
   e. echo
5. Name five UDP services that can be filtered with an extended access list.
6. What RFC defines NAT?
7. In NAT, what is the inside local address used for?
8. What does the IOS command **ip nat inside source list** accomplish?
9. What are the four possible NAT translations on a Cisco IOS router?
10. How many connections can be translated with a PIX Firewall for the following RAM configurations: 16 MB, 32 MB, and 256 MB?
11. When the **alias** command is applied to a PIX Firewall, what does it accomplish?
12. What security features does the Cisco IOS Firewall feature set allow a network administrator to accomplish?

13. What does CBAC stand for?
14. Name the eight possible steps to take when configuring CBAC.
15. What is a virtual private network?
16. What type of attacks can be mitigated by CSA?
17. What are the three possible states with an 802.1X connection?

Scenario

Scenario: Configuring a Cisco PIX Firewall for NAT

The following configuration is installed on a PIX 520. Users from the inside network 10.0.0.0/8 report to you that they cannot browse the Internet. What is the problem, and what command or commands will rectify the problem?

```
pix# write terminal
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
hostname pix
 fixup protocol ftp 21
 fixup protocol http 80
 fixup protocol smtp 25
 fixup protocol h323 1720
 fixup protocol rsh 514
 fixup protocol sqlnet 1521
  logging timestamp
 no logging standby
 logging console debugging
 no logging monitor
 logging buffered debugging
 no logging trap
 logging facility 20
 logging queue 512
 interface ethernet0 10full
 interface ethernet1 10full
 mtu outside 1500
 mtu inside 1500
ip address inside 201.201.201.1 255.255.255.0
ip address outside 131.108.1.1 255.255.255.0
route inside 10.0.0.0 255.0.0.0 201.201.201.2
route outside 0.0.0.0 0.0.0.0 131.108.1.2
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 arp timeout 14400
global (outside) 1 192.192.1.2-192.192.1.30 netmask 255.255.255.224
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00 udp 0:02:00
 timeout rpc 0:10:00 h323 0:05:00
 timeout uauth 0:00:00 absolute
 no snmp-server location
 no snmp-server contact
 snmp-server community public
 no snmp-server enable traps
 telnet timeout 5
 terminal width 80
: end
```

Scenario Answer

Scenario Solution

Cisco PIX Firewalls need to be enabled for NAT for any nonregistered IP address spaces such as the addresses listed in RFC1918. In particular, the Class A 10.0.0.0/8 is not routable in the Internet, so you must use NAT to permit access, or you could re-address your entire network, which clearly is not an exercise you will do often. Even if you re-addressed your entire network, you would still need to configure **nat**, **nat 0**, **nat 0 acl**, or **statics** on the firewall to permit IP traffic.

The following command will configure the PIX Firewall for NAT, on the inside addresses:

```
nat  (inside) 1 0.0.0.0 0.0.0.0
```

Before you can access the Internet, you must also configure the PIX Firewall for routing (remember, the PIX Firewall is not as intelligent as a router until version 6.3, where OSPF is supported); RIP can be configured by the network administrator, and you must route IP data with the command shown here:

```
route outside 0.0.0.0 0.0.0. 131.018.1.2
```

This command installs a default route where IP datagrams will be sent, typically, the perimeter router or ISP router.

Exam Topics in This Chapter

- Policies—Security Policy Best Practices
- Standards Bodies—IETF
- Vulnerability Discussions
- Attacks and Common Exploits—recon, priv escalation, penetration, cleanup, backdoor

You can find in this book's introduction a list of all of the exam topics. For the latest updates on exam topics, visit Cisco.com.

CHAPTER 7

Network Security Policies, Vulnerabilities, and Protection

This chapter reviews today's most common Cisco security policies and mechanisms available to the Internet community to combat cyber attacks. The security standards body, CERT/CC, is covered, along with descriptions of Cisco IOS–based security methods that ensure that all attacks are reported and acted upon. This chapter will cover, in detail, common exploits such as attacks based on common vulnerabilities, reconnaissance attacks, backdoors, and protocol weaknesses. Cisco Security applications, such as Intrusion Detection System, are covered to finally lay all the building blocks and knowledge you need to master the topics in the CCIE Security written exam.

This chapter covers the following topics:

- **Network Security Policies**—Describes standard security policies that should be deployed in any IP network**.**
- **Standards Bodies and Incident Response Teams**—Introduces some of the standards bodies that are designed to help the Internet community tackle intrusion, as well as some forums and e-mail aliases that can help a network security architect.
- **Vulnerabilities, Attacks, and Common Exploits**— Presents some of the vulnerabilities that are exploited to attack IP networks, some methods of exploitation, and some of the ways in which data can be misused after a successful attack
- **Intrusion Detection System (IDS)**—Describes how an IDS (Cisco IDS, in particular) can be implemented to help deter intruders from gaining access to secure data, including details on how to prevent back doors and protocol weaknesses.
- **Protecting Cisco IOS from Intrusion**—Presents some of the standard configurations that should be considered for every Cisco IOS–enabled router connected to the Internet to avoid intruders gaining access to unauthorized material.

"Do I Know This Already?" Quiz

The purpose of this assessment quiz is to help you determine how to spend your limited study time.

If you can answer most or all of these questions, you might want to skim the "Foundation Topics" section and return to it later, as necessary. Review the "Foundation Summary" section and answer the questions at the end of the chapter to ensure that you have a strong grasp of the material covered.

If you already intend to read the entire chapter, you do not necessarily need to answer these questions now. If you find these assessment questions difficult, read through the entire "Foundation Topics" section and review it until you feel comfortable with your ability to answer all of these questions and the "Q & A" questions at the end of the chapter.

Answers to these questions can be found in Appendix A, "Answers to Quiz Questions."

1. A remote user tries logging into a remote network but fails after three additional tries and is disconnected. What useful information should the network administrator gather? (Select the best two answers.)
   a. Username
   b. Invalid password
   c. Invalid username
   d. Valid username
2. If a remote user Telnets to a router but accidentally types the incorrect password or username, which of the following events is *not* required by the security administrator in this organization? (Select the best two answers.)
   a. Invalid password
   b. Invalid username
   c. Access denied
   d. Authorization failure
   e. Authentication failure
3. What is the first step that should be implemented in securing any network?
   a. Create a database of secure passwords.
   b. Create the IP address scheme.
   c. Run NetRanger or NetSonar.
   d. Define a security policy.
   e. Configure access lists on all routers.
4. Why would a security administrator decide to install a stateful firewall?
   a. Stateful firewalls are cheap.
   b. By default, all stateful firewalls deny all traffic.

c. Stateful firewalls ensure that all traffic returning from a router originated inside the network, unless a static policy on the firewall permits otherwise.

d. Stateful firewalls cannot be compromised.

e. Stateless firewalls are more secure than stateful firewalls.

5. What primary security method can be designed and deployed to secure and protect any IP network after an attack has been documented?

a. Security policy

b. IP policy

c. Countermeasures

d. Measurement

e. Logging passwords

6. A security administrator notices that a log file stored on a local router has increased in size from 32 kb to 64 kb in a matter of seconds. What should the network administrator do?

a. Increase the buffer to 64 kb.

b. Decrease the buffer to 16 kb.

c. Log the event as suspicious and notify the incident response team.

d. Nothing, this is normal.

7. What is the primary responsibility of CERT/CC?

a. Define access lists for use on routers

b. Set security standards

c. Coordinate attacks on secure networks

d. Maintain a security standard for networks

e. Nothing to do with security

8. Who can use network scanners and probes? (Select the best two answers.)

a. Intruders

b. Security managers

c. End users

d. Cable service providers

9. What is a bastion host?

a. Firewall device supported by Cisco only

b. Network's last line of defense

c. Network's first line of defense

d. IP host device designed to route IP packets

10. A TCP SYN attack is what type of attack?
    a. ICMP
    b. DoS
    c. Telnet/Kerberos attack
    d. Ping attack only
11. When an intruder sends a large amount of ICMP echo (ping) traffic using IP broadcasts, this type of DoS attack is known as what?
    a. Bastion
    b. Land.C
    c. Man-in-the-middle
    d. Smurf
    e. Ping of death
12. Assuming two devices are running IPSec over the Internet, what form of attack is likely to compromise any data sent over the Internet?
    a. Ping of death
    b. Smurf
    c. Land.C
    d. Man-in-the-middle
    e. Birthday attack
13. What kind of attack sends a large number of ICMP echo request packets with the intent of overflowing the input buffers of the destination machine and causing it to crash?
    a. Ping of death
    b. Smurf
    c. Land.C
    d. Man-in-the-middle
    e. Birthday attack
14. In the context of intrusion detection, what is an exploit signature?
    a. DoS attack
    b. An attack that is recognized and detected on the network
    c. The same as a Smurf attack
    d. The same as a man-in-the-middle attack

15. A network scanner can be used for what primary function?

    a. To exploit HTTPs passwords

    b. To exploit network signatures

    c. To exploit network vulnerabilities

    d. To find hackers and intruders on the network

    e. To advise security management when a network is compromised

16. If a network manager believes that a host has been compromised, on a router or host device, and wishes to have the Certificate Authority certificate revoked, how can the security team accomplish this?

    a. Ask the ISP for help.

    b. Contact the Certificate Authority administrator and be prepared to change the secret password.

    c. Type the command **no crypto ca revoke** *name* on the router.

    d. Do nothing, because the client software takes decisive action by rebooting the router.

    e. Change the Cisco IOS code.

    f. Uninstall the IPSec software on the host and router.

17. What is the best mechanism against sniffer-type programs that try to determine the network passwords between hosts and clients? (Select, at most, three answers.)

    a. Hard-coded passwords

    b. IPSec

    c. One-time passwords

    d. Kerberos or SSH

18. What is the main goal of a Trojan horse application?

    a. Nothing, as security policies are implemented everywhere in the Internet

    b. A malicious piece of code or programming designed to capture usernames and passwords

    c. A way to add usernames to a host system

    d. Trojan horses ensure a device can be compromised for audit trails after a hacker has gained access to a host

19. Which of the following are traditional defense-in-depth security options? (Select the best two answers.)

    a. Use of paper trails
    b. Use of clear-text passwords
    c. Gathering security assessments of your network
    d. Use of authentication
    e. Implementing a perimeter defense

20. To stop spam e-mail from overwhelming an e-mail server, what step can you take?

    a. Ask the ISP for help.
    b. Nothing, because spam e-mail is too difficult to stop to be worth the effort.
    c. Install an intrusion detection system that has a signature for spam e-mail.
    d. Nothing, because the client software takes care of this.
    e. Change the Cisco IOS code.
    f. Configure the bastion host to stop spam e-mail.

21. What is an SYN flood attack?

    a. No such type of attack exists
    b. By setting the flag bits in all TCP packets with SYN/FIN bits set to 0
    c. A flood of TCP connection requests with randomized ports and addresses
    d. A flood of TCP connection requests with randomized ports only
    e. A flood of TCP connection requests with randomized IP source addresses only
    f. Smurf attack

22. View the following ARP table:

```
SimonRules#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.135.11           -   00b0.8ef5.9038  ARPA   E0
Internet  10.1.31.1              -   00b0.8ef5.908c  ARPA
Internet  10.1.30.1              -   00b0.8ef5.9070  ARPA   Cable4/0
Internet  10.1.30.106          200   0010.7bb3.fb7b  ARPA   E0
Internet  10.1.30.108          200   0001.64ff.eb3d  ARPA   E0
Internet  10.1.30.109           -   0002.fdfa.0a63  ARPA    E0
```

    What address do you suspect might be involved in launching an attack of some form? (Select the best two answers.)

    a. 10.1.135.11
    b. 10.1.30.106
    c. 10.1.30.108
    d. 10.1.30.109

23. Which of the following describes an attack that falsifies a broadcast ICMP echo request and may include a primary and secondary victim?

- **a.** None of these
- **b.** Man-in-the-middle
- **c.** Land.C
- **d.** A home attack
- **e.** A smurf attack

24. What are the common drawbacks of antivirus software such as Norton AntiVirus? (Select the best two answers.)

- **a.** The software is difficult to keep up to date when new viruses are released.
- **b.** The software cannot take any action against a known virus.
- **c.** Antivirus software is hardware dependent.
- **d.** Attackers frequently re-code their programs to bypass antivirus systems.

Foundation Topics

Network Security Policies

IP networks are susceptible to unsecured intruders using a variety of different methods to gain entry. Through the campus, by dialup, and through the Internet, an intruder can view IP data and attack vulnerable network devices.

IP networks must provide network security for the following reasons:

- **Inherent technology weaknesses**—All network devices and operating systems have inherent vulnerabilities.
- **Configuration weaknesses**—Common configuration mistakes can be exploited to open up protocol weaknesses.
- **Network policy vulnerabilities**—The lack of a network policy or an incomplete network policy can lead to vulnerabilities, such as poor password security.
- **Outside/inside intruders**—Unfortunately, you must assume that there are internal and external people who want to exploit your network resources and retrieve sensitive data.

Every IP network architecture should be based on a sound security policy that is designed to address all of these weaknesses and threats. This sound security policy must be in place before remote access to the network is allowed. Network vulnerabilities must be constantly sought out, found, and addressed, because they define points in the network that are potential security weak points (or loopholes) that can be exploited by intruders or hackers.

Technologies such as TCP/IP, which is an open and defined standard, allow intruders to devise programs that send IP packets looking for responses and intruders can act on them. Countermeasures can be designed and deployed to secure and protect a network.

Intruders are typically individuals who have a broad skill set. Intruders may be skilled in coding programs in Java, UNIX, DOS, C, and C++. Their knowledge of TCP/IP may be exceptional, and they may be have extensive experience in using the Internet to search for security loopholes. Sometimes, the biggest security threat comes from within an organization, particularly disgruntled former employees who may have access to usernames and passwords.

An intruder's motivation may be based on any number of reasons, which makes any network a possible target:

- Cash profit
- Revenge
- Vandalism
- Cyber terrorism
- Challenge, to gain prestige or notoriety
- Curiosity, to gain experience, or to learn the tools of trade
- Hacktivism, to gain an advantage or notoriety for an organization's ideology

Countermeasures against protocol or application vulnerabilities ensure that a policy, procedure, or specific technology is implemented so that networks are not fully exploited. A countermeasure against any particular vulnerability ensures that that vulnerability is not exploited.

The ever-changing nature of attacks is another major challenge facing network administrators. Intruders today are well organized and trained, and Internet sites are easy targets and offer low risk to intruders. The tools used by intruders (see "Vulnerabilities, Attacks, and Common Exploits," later in this chapter) are increasingly sophisticated, easy to use, and designed for large-scale attacks.

Now that you are aware of some of the reasons a network must have a sound security policy and some of the motives intruders (hackers) may have to exploit a poorly designed network, consider some of the standards bodies that are designed to help network administrators fend off intruders.

Standards Bodies and Incident Response Teams

Numerous standards bodies today help a network administrator design a sound security policy. The two main entities that are helpful are the Computer Emergency Response Team Coordination Center (CERT/CC) and the various newsgroups that enable you to share valuable security information with other network administrators.

CERT/CC is a U.S. federally-funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. Following the infamous worm incident (Morris Worm — a virus developed to spread itself within any IP network), which brought 10 percent of Internet systems to a halt in November 1988, CERT/CC has helped to establish incident-handling practices that have been adopted by more than 200 incident response teams around the world (incident response teams are described in depth later in the chapter).

CERT/CC works with the Internet community to facilitate responses to incidents involving the Internet and the hosts that are attacked. CERT/CC is designed to take proactive steps to ensure that future attacks and vulnerabilities are communicated to the entire Internet community. CERT/CC also conducts research aimed at improving the security of existing systems.

CERT/CC also helped technology managers with Y2K compliance and with various well-known viruses, such as the Melissa virus. CERT/CC does not focus on the intruders themselves, or on the arrest of individuals responsible for causing havoc; rather, it ensures that vulnerabilities and loopholes are closed as soon as possible. CERT/CC does not maintain any security standards (these are left for RFCs); also, it does not provide any protocols to help network administrators.

CERT/CC has relationships with various other organizations, such as law enforcement and Internet security experts, and with the general public, so that any information gathered by the teams involved in stifling attacks is communicated quickly.

Examples of intruders actually overcoming network security include the famous Barclay Bank attack in July 2001, where the company's home page was defaced. *The New York Times* website was altered in September 1998. In February 2000, Yahoo also came under attack. In response to attacks like these and the increased concern brought about by them, Cisco Systems decided to release a new CCIE Security certification.

Cisco also provides a website (for the Cisco Product Security Incident Response Team) where customers can report any security concerns regarding flaws in Cisco IOS products:

http://www.cisco.com/en/US/products/products_security_advisories_listing.html

You can also e-mail the Cisco Product Security Incident Response Team directly for emergency issues, at security-alert@cisco.com, and for nonemergencies, at psirt@cisco.com.

NOTE *Social engineering* is a widely used term that refers to the act of tricking or coercing employees into providing information, such as usernames, mail user identifications, and even passwords. First-level phone-support personnel typically are the employees who are called by intruders, pretending to work for the company, to gain valuable information. The following URL takes you to the "2004 E-Crime Watch Survey," which details the level of electronic crime. It is an excellent document you can give to upper management to show how important security should be regarded in any organization connected to the Internet:

http://www.cert.org/archive/pdf/2004eCrimeWatchSummary.pdf

In 1998, CERT/CC handled 4,942 incidents involving intruders. In 2001, CERT/CC handled over 52,000 incidents resulting is 2,437 incident reports. In 2004, through the month of November, there were over 2,680 incidents reported in a single month.

If you have never heard of CERT/CC, now is the time to read more and ensure that you are alerted to vulnerabilities. For more details on CERT/CC, visit http://www.cert.org. CERT/CC claims that over 95 percent of intrusions can be stopped with countermeasures and monitoring tools in place.

Incident Response Teams

Incident response teams are too often set up only after an incident or intrusion occurs. However, sound security administration requires that such teams should already be set up to monitor and maintain network security.

Incident response teams do the following:

1. Verify the incident.
2. Determine the magnitude of the incident (hosts affected and how many).
3. Assess the damage (for example, determine if public servers have been modified).
4. Gather and protect the evidence.
5. Inspect systems to determine damage.
6. Remove hostile or destructive code.
7. Reload necessary operating system software.
8. Restore configurations.
9. Restore and test operations.
10. Patch the system to reduce vulnerability.
11. Inspect applications to determine damage.
12. Reload software if necessary.
13. Test functionality.
14. Inspect files to determine damage.
15. Restore files from backup if necessary.
16. Replicate damaged files if no backup is available.
17. Confirm with users that data is restored.

After this data has been collected in relation to the incident discovered by the security administrators, the incident response team determines whether there is enough trace data to track the intruders. The actual data you discover might be only a small part of the entire puzzle. For example, initially, you might have only a log file or notice that a log file size increased or decreased during the incident.

The data should be sent to upper management, to the operations groups within an organization, to all affected sites, and to organizations such as CERT/CC. Organizations such as Cisco or Microsoft typically do not release a statement to the press detailing any attacks, the recent IOS code thefts are an excellent example.

After the information flows to all parts of an organization, the incident response team restores programs and data from the vendor-supplied media and backup device storage media. The data restored needs to be securely configured (such as routers; see the example in "Protecting Cisco IOS from Intrusion," later in this chapter), which includes installing all relevant patches for all application-based programs.

Finally, the incident response team prepares a report and provides it to the law enforcement organization if prosecution is required. More details on Cisco incident response teams can be viewed at

http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/networking_solutions_audience_business_benefit09186a008010e5cb.html

Internet Newsgroups

Another important body for both network administrators and intruders themselves is Internet newsgroups. Newsgroups are mailing list-type forums where individuals share ideas and past incidents to keep current with the latest security concerns and protection policies. As a network administrator, you must be aware of both standards and topics that intruders are discussing.

The following mailing lists and newsgroups are CERT/CC recommended:

- **Bugtraq**—A full-disclosure computer security mailing list. Subscribe through http://www.securityfocus.com/.
- **NTBugtraq**—A moderated forum created to invite the free and open discussion of Windows NT security exploits and bugs. To subscribe, send an e-mail message to listserv@listserv.ntbugtraq.ntadvice.com with "subscribe ntbugtraq *firstname lastname*" in the body of the message.
- **RussNTSecurity**—An open mailing list, lightly moderated, and dedicated to Windows NT security topics. To subscribe, send an e-mail message to listserv@listserv.ntbugtraq.com with "subscribe ntsecurity" in the body of the message.
- **VIRUS-L**—A moderated mailing list with a focus on computer virus issues. To be added to the mailing list, send an e-mail message to listserv@lehigh.edu.

CERT/CC recommends the following newsgroups:

- **alt.security**—Lists computer security issues and other security issues, such as car locks and alarm systems
- **comp.risks**—Moderated forum on the risks to the public in computers and related systems
- **comp.security.announce**—Computer security announcements, including new CERT advisories, summaries, and vendor-initiated bulletins
- **comp.security.misc**—A variety of issues related to computer and network security
- **comp.security.unix**—Security information related to the UNIX operating system
- **comp.virus**—Computer viruses and related topics

NOTE The following sites also contain a great wealth of information. Although not security specific, they can help you identify the mechanism used to infiltrate technologies such as TCP/IP:

- **Internet Domain Survey (http://www.isc.org/ds/)**—Includes Host Count History and pointers to other sources of Internet trend and growth information
- **Internet Engineering Task Force (IETF) (http://www.ietf.org/)**—Offers technical papers, best practices, standards, and more
- **Internet Society (ISOC) (http://www.isoc.org/internet/)**—Provides an overview of the Internet, including its history and how it works

Vulnerabilities, Attacks, and Common Exploits

This section covers some of the vulnerabilities in TCP/IP and the tools used to exploit IP networks.

TCP/IP is an open standard protocol, which means that both network administrators and intruders are aware of the TCP/IP architecture and vulnerabilities.

NOTE There are a number of network vulnerabilities, such as insufficient password protection, lack of authentication mechanisms, use of unprotected routing protocols, and firewall holes. This section concentrates on TCP/IP vulnerabilities.

Network intruders can capture, manipulate, and replay data. Intruders typically try to cause as much damage to a network as possible by using the following methods:

- **Vandalizing**—Accessing the web server and altering web pages.
- **Manipulating or modifying data**—Altering the files on a network device.

- **Masquerading**—Manipulating TCP/IP segments to pretend to be at a valid IP address.
- **Session replay**—Capturing, altering, and replaying a sequence of packets to cause unauthorized access. This method identifies weaknesses in authentication.
- **Session hijacking**—Defining himself with a valid IP address after a session has been established to the real IP address, by spoofing IP packets and manipulating the sequence number in IP packets.
- **Rerouting**—Routing packets from one source to an intruder source or altering routing updates to send IP packets to an incorrect destination, allowing the intruder to read and use the IP data inappropriately.

The following are some of the attack methods and types of attacks intruders use:

- Probes and scans
- Denial-of-service (DoS) attacks
- Compromises
- Malicious code (such as viruses)
- Misconfiguration of protocols
- Network monitor tools to log all packets

As described in Chapter 5, "Operating Systems and Cisco Security Applications," network scanners and tools are available to both network administrators and intruders. These tools can be used and placed at strategic points in the network to gain access to sensitive data. Cisco Secure Scanner, for example, can be used to find network vulnerabilities; therefore, intruders can use it to do as much harm as it does network administrators good if you aren't aware of these vulnerabilities.

DoS attacks are the most common form of attack used by intruders and can take many forms. The intruder's goal is to ultimately deny access to authorized users and tie up valuable system resources.

Figure 7-1 displays several techniques deployed in DoS attacks.

Figure 7-1 *Forms of Denial-of-Service Attack*

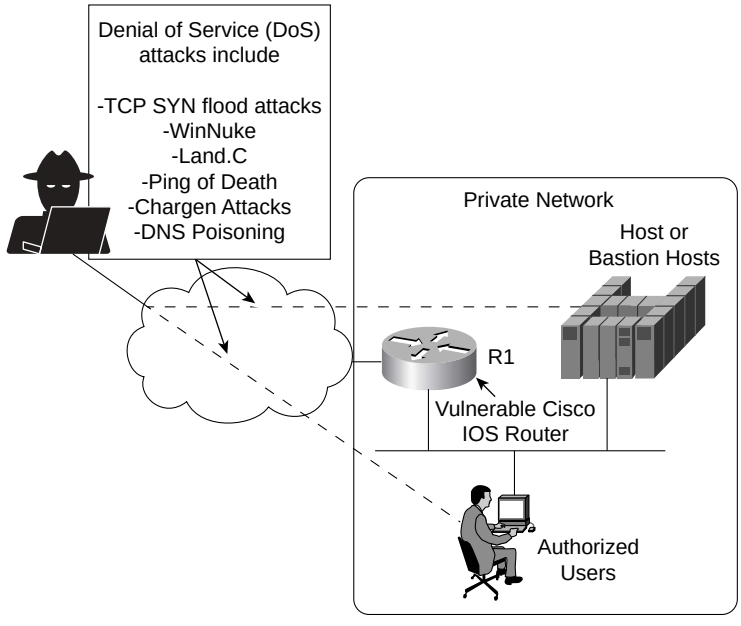


Figure 7-1 displays a typical network scenario in which a router is connected to the Internet and all users have access to hosts in a public domain. A *bastion host* is a computer or host, such as a UNIX host, that plays a critical role in enforcing any organization's network security policy. Because bastion hosts are directly exposed to untrusted and unknown networks, and thus the first line of defense in the network, they are typically highly secured (including physically, in secure computer rooms). Bastion hosts often provide services to Internet users, such as web services, and provide public access systems, such as FTP or SMTP mail. Because these computers are likely to be attacked, they are often referred to as *sacrificial hosts.*

The intruder in Figure 7-1 attacks the authorized users and hosts (or bastion hosts) behind a router by using a number of methods, including the following:

- **Ping of death**—Attack that sends an improperly large Internet Control Message Protocol (ICMP) echo request packet with the intent of overflowing the input buffers of the destination machine and causing it to crash. The IP header field is set to 1, the last fragment bit is set, and the data length is greater than 65,535, which is greater than the maximum allowable IP packet size.

- **TCP SYN flood attack**—DoS attack that randomly opens a number of TCP ports, ensuring that network devices are using CPU cycles for bogus requests. By tying up valuable resources on the remote host, the CPU is tied up with bogus requests, and legitimate users experience poor network response or are denied access. This type of attack can make the host unusable.

- **E-mail attack**—DoS attack that sends a random number of e-mails to a host. E-mail attacks try to fill an inbox with bogus e-mails, ensuring that the end user cannot send mail while thousands (or an e-mail bomb) of e-mails are received. The most recent style of e-mail attack is the e-mail bounce attack. This is achieved by sending a large attachment to a list of bogus e-mail addresses and putting your victim in the Reply To field using options in the mail client. Helpful, high-capacity e-mail servers (such as AOL) return the attachment. Thus, you send one copy out and the victim gets back one for every name on the Cc list.

- **CPU-intensive attack**—DoS attack that ties up a system's resources by using a program, such as a *Trojan horse* (a program designed to capture usernames/passwords from a network), or enabling viruses to disable remote systems. A new variation of this attack, called BOINK, sends a file with one data byte per packet, and sends them out of sequence. The host CPU utilization then goes to 100 percent as the destination host tries to reassemble the file. By sending many simultaneous BOINK packets, the attacker can crash a very high-powered server and cause loss of data.

- **Teardrop**—Exploits an overlapping IP fragment implementation bug in various operating systems. The exploit causes the TCP/IP fragmentation reassembly code to improperly handle overlapping IP fragments, causing the host to hang or crash.

- **DNS poisoning**—Exploits the DNS server, causing the server to return a false IP address to a domain name query.

- **UDP bomb**—Sends an illegal Length field in the packet header, causing kernel panic and crash. This is an old attack but attackers do upgrade their own attack tools.

- **Distributed denial-of-service (DDoS) attack**—DoS attack that the attacker runs on multiple hosts. The attacker first compromises vulnerable hosts using various tools and techniques. Then, the actual DOS attack on a target is run from the pool of all the compromised hosts.

- **Chargen attack**—Establishes a connection to a host via TCP or UDP and attempts to generate a stream of data output. Typically, the command used is **telnet** *ip-address* **chargen**. Most security conscious networks turn this service off on all Cisco IOS–enabled devices.

- **Attack via dialup (out of band)**—Using any form of dialup access exposes your network to attackers, because dialup connections are allocated an IP address, thus making your network vulnerable. Although less common these days, because the Internet has expanded so dramatically, attack via dialup is still a cause for concern if the connection is not secured correctly. Even the most basic step, turning off the modem when not in use, is a valid security option. Other forms of security include using RSA tokens and certificates.

- **Land.C attack**—A program designed to send TCP SYN packets (TCP SYN is used in the TCP connection phase) that specify the target's host address as both source and destination.

NOTE Some of the attacks in this list are old and are described here as examples only. Ensure that you check the http://www.cert.org website for the latest style of attacks reported.

DoS attacks are designed to send traffic to host systems so that they cannot respond to legitimate traffic by overwhelming the end device through a number of incomplete and illegal connections or requests. DoS attacks send more traffic than is possible to process and can send excessive mail requests, excessive UDP packets, and excessive ICMP pings with very large data packet sizes to render a remote host unusable.

Many other known and unknown attack methods and terms exist. Here are a few more you should be aware of for the written exam:

- **Spoof attack**—The attacker creates IP packets with an address obtained (or spoofed) from a legitimate source. This attack is powerful in situations where a router connects to the Internet with one or more internal addresses. The real solution to this form of attack is to track down the source device and stop the attack. The spoofed address is actually a valid address for the network. RFC 1918/2827 should be implemented to avoid this style of attack.

- **Smurf attack**—Named after its exploit program, the smurf attack is one of the most recent in the category of network-level attacks against hosts. In this attack, an intruder sends a large amount of ICMP echo (ping) traffic to IP broadcast addresses, which all have a victim's spoofed source address. For more recent details on this form of attack and many others, go to http://www.cert.org/advisories/.

  Smurf attacks include a primary and secondary victim and are extremely damaging to any IP network. Smurf attacks result in a large number of broadcast ICMP packets, and if routers are configured to forward, broadcasts can result in a degraded network and poor performance between the primary and secondary device. A quick solution is to disable **ip-directed broadcasts**. This command is enabled by default in Cisco IOS 12.1 and higher.

- **Man-in-the-middle attack**—An attack in which an attacker is able to read and modify at will messages between two parties without either party knowing that the link between them has been compromised. The attacker must be able to observe and intercept messages going between the two victims. Man-in-the-middle attacks are particularly problematic for devices in the public domain running cryptography. An attacker may create mischief and compromise the integrity of data flowing between two trusted devices.

- **Birthday attack**—Class of brute-force attacks. It gets its name from the surprising fact that the probability that two or more people in a group of 23 share the same birthday is greater than 50 percent; such a result is called a *birthday paradox*. The attacker presents what appears

to be a trusted source for signing. After the device has signed, the attacker takes the signature and attaches it to the fraudulent contract. This signature then "proves" that the trusted and compromised host signed the fraudulent contract.

Intrusion Detection System

Intrusion detection systems (IDSs) are designed to detect and thwart network attacks. Based on their location, IDSs can be either of the following:

- **Network-based IDS (NIDS)**—Examines or sniffs every packet flowing across the network and generates an alarm upon detection of a network attack signature.
- **Host-based IDS (HIDS)**—Examines operating system information, such as logs or system processes, against a base line. When the system deviates from the normal values because of an attack, alarms are generated.

Chapter 6, "Security Technologies," defines some of the network prevention and host intrusion detection mechanisms that you can use in an IP network, namely Cisco Intrusion Prevention and Cisco Security Agent.

Cisco IDS delivers a comprehensive, pervasive security solution for combating unauthorized intrusions, malicious Internet worms, and bandwidth and e-business application attacks.

Recently, Cisco announced a number of new products to support IDS:

- **Cisco Security Agent (CSA)**—Analyzes behavior rather than relying on signature matching. This ensures that tasks are checked against the system-based policies before the system kernel is used, thus stopping worms and viruses from spreading. CSA is covered in detail in Chapter 6.
- **Cisco IDS 4250 Appliance Sensor**—Raises the performance bar for high-throughput gigabit protection in a performance-upgradeable IDS chassis.
- **Cisco IDS 4235 Appliance Sensor**—Provides enterprise-class intrusion protection at new price/performance levels.
- **Cisco IDS 4.1 Sensor Software**—Delivers powerful web-based, embedded device management, graphical security analysis, and data-mining capabilities. Version 4.1 of the IDS software includes support for 2600/3600/3700 routers. IDS is built in on the new platforms, namely the 2800 and 3800 series routers.

NOTE In addition to the Cisco IDS 4200 series of IDS appliances, Cisco also has the following IDS sensors:

- Cisco IOS with IPS (Intrusion Prevention Systems) feature set for routers
- Catalyst 6500 IDS module for switch-based sensor (IDSM-2 module)
- PIX Firewall with version 6.x with built-in IDS sensor; Version 7.x will be available in 2005
- Cisco IDS Host sensor for Windows, Solaris OS, desktops, and web servers, such as IIS and Apache

You are not expected to know these details for the written exam; they are presented here for completeness only.

Each Cisco IDS sensor can be configured to support a number of different signatures. A signature engine is a component of the Cisco IDS sensor that is designed to support many signatures in a certain category. An engine is composed of a parser and an inspector. Each engine has a set of legal parameters that have allowable ranges, or sets of values. Exploit signatures are an identifiable pattern of attack detected by your network device, such as a Cisco IDS Network sensor.

Table 7-1 lists and describes the signature engines available with Cisco IDS Version 4.1.

Table 7-1 *Cisco IDS Signature Engines**

ATOMIC.ARP	ARP simple and cross-packet signatures.
ATOMIC.ICMP	Simple ICMP alarms based on the following parameters: Type, Code, Sequence, and ID.
ATOMIC.IPOPTIONS	Simple alarms based on the decoding of Layer 3 options.
ATOMIC.L3.IP	Simple Layer 3 IP alarms.
ATOMIC.TCP	Simple TCP packet alarms based on the following parameters: Port, Destination, Flags, and single packet Regex. Use SummaryKey to define the address view for MinHits and Summarize counting. For best performance, use a StorageKey of xxxx.
ATOMIC.UDP	Simple UDP packet alarms based on the following parameters: Port, Direction, and DataLength.
FLOOD.HOST.ICMP	ICMP floods directed at a single host.
FLOOD.HOST.UDP	UDP floods directed at a single host.
FLOOD.NET	Multiprotocol floods directed at a network segment. IP addresses are wildcarded for this inspection.
OTHER	Used to group generic signatures so that common parameters can be changed. It defines an interface into common signature parameters.

continues

Table 7-1 *Cisco IDS Signature Engines* (Continued)*

SERVICE.DNS	Analyzes the DNS service.
SERVICE.FTP	FTP service special decode alarms.
SERVICE.GENERIC	Custom service/payload decode. For expert use only.
SERVICE.HTTP	HTTP decode-based string engine. Includes anti-evasive URL deobfuscation.
SERVICE.IDENT	IDENT service (client and server) alarms.
SERVICE.MSSQL	Microsoft SQL service inspection engine.
SERVICE.NTP	Network Time Protocol–based signature engine.
SERVICE.RPC	Analyzes the RPC service.
SERVICE.SMB	SMB SuperInspector signatures.
SERVICE.SMTP	Inspects SMTP protocol.
SERVICE.SNMP	Inspects SNMP traffic.
SERVICE.SSH	SSH header decode signatures.
SERVICE.SYSLOG	Processes syslogs.
STATE.STRING.CISCO LOGIN	Telnet-based Cisco login inspection engine.
STATE.STRING.LPR FORMATSTRING	Inspects LPR protocol.
STRING.ICMP	Generic ICMP-based string search engine.
STRING.TCP	Generic TCP-based string search engine.
STRING.UDP	Generic UDP-based string search engine.
SWEEP.HOST.ICMP	A single host sweeping a range of nodes using ICMP.
SWEEP.HOST.TCP	Detects host and service sweeps over TCP.
SWEEP.MULTI	Conducts cross-protocol sweeps.
SWEEP.OTHER.TCP	Conducts fingerprint scans.
SWEEP.PORT.TCP	Detects port sweeps between two nodes.
SWEEP.PORT.UDP	Detects UDP connections to multiple destination ports between two nodes.

*The information in Table 7-1 is from the Cisco.com page at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids10/idmiev/swappa.htm.

An IDS can be used, for example, to detect spam e-mail and still allow regular e-mail. Most ISPs do not detect or remove spam e-mail, so it is up to the security administrator to ensure that spam e-mail is not permitted or used as a DoS attack.

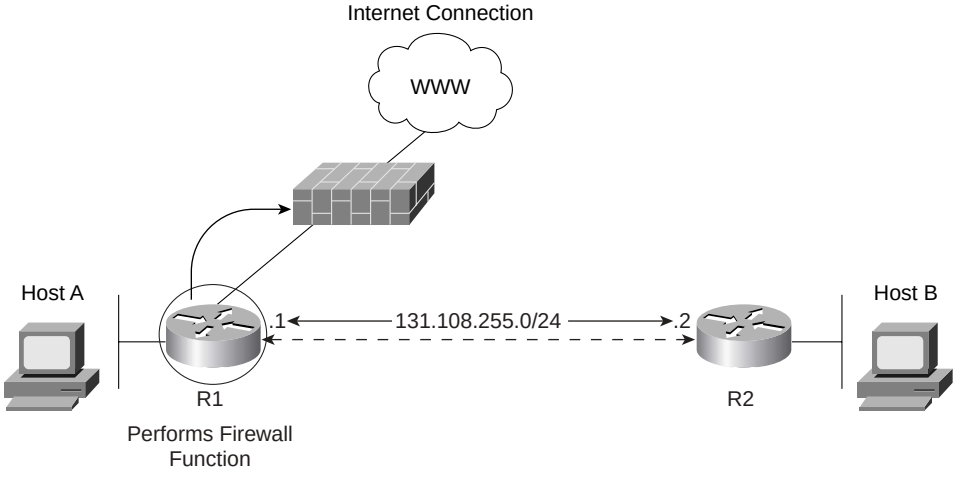
Protecting Cisco IOS from Intrusion

Now that you have a snapshot of modern security concerns, look at Cisco IOS and the configuration commands you can use to deny intruders the ability to harm valuable network resources that are typically connected behind a Cisco router. In particular, this section covers how you can stop DoS attacks.

There are, of course, various Cisco IOS vulnerabilities that can only be protected against by new software releases and regular Cisco IOS bulletins and e-mail blasts from Cisco Systems to ensure customers are not compromised.

Figure 7-2 displays a typical network scenario. This shows how to configure the router, separating the public and private networks so that the private network is not vulnerable.

Figure 7-2 *Typical Internet Connection on R1*



The Nagle algorithm helps alleviate the small tcp packet problem in TCP.

Example 7-1 configures the Router R1 to enable the Nagle algorithm defined in RFC 896.

Example 7-1 *Enable Nagle Algorithm*

```
service nagle
service tcp-keepalives-in
service tcp-keepalives-out
```

Cisco.com defines the Nagle algorithm as follows (www.cisco.com/univercd/cc/td/doc/product/software/ios100/rpcg/36053.htm):

John Nagle's algorithm (RFC-896) helps alleviate the small-packet problem in TCP. In general, it works this way: The first character typed after connection establishment is sent in a single packet, but TCP holds any additional characters typed until the receiver acknowledges the previous packet. Then the second, larger packet is sent, and additional typed characters are saved until the acknowledgment comes back. The effect is to accumulate characters into larger chunks, and pace them out to the network at a rate matching the round-trip time of the given connection. This method is usually effective for all TCP-based traffic. However, do not enable the Nagle slow packet avoidance algorithm if you have XRemote users on X Window sessions.

Enabling this algorithm along with the **service tcp keepalive** command ensures that no TCP connections on any router get hung.

NOTE To generate keepalive packets on idle incoming network connections (initiated by the remote host), use the **service tcp-keepalives-in** global configuration command.

To generate keepalive packets on idle outgoing network connections (initiated by a user), use the **service tcp-keepalives-out** global configuration command.

Example 7-2 configures R1 to disable (on by default) TCP/UDP small servers.

Example 7-2 *Disable TCP/UDP Small Servers*

```
no service udp-small-servers
no service tcp-small-servers
```

By default, the TCP servers for Echo, Discard, Chargen, and Daytime services are disabled.

When the minor TCP/IP servers are disabled, access to the Echo, Discard, Chargen, and Daytime ports causes the Cisco IOS software to send a TCP reset packet to the sender and discard the original incoming packet. When the commands in Example 7-2 are entered, they do not display the IOS commands just entered when you view the configuration, because the default is to disable TCP/UDP servers.

NOTE When a Cisco IOS router is configured to disable the UDP small servers, access to Echo, Discard, and Chargen ports enable the router to send ICMP port-unreachable messages to the source device, and the incoming packet is discarded. It is up to the source station to act on the ICMP port-unreachable messages. In other words, if this is from an unauthorized host, you will be sending information to the same device.

Example 7-3 configures R1 to encrypt all passwords configured on a Cisco router.

Example 7-3 *Encrypting All Passwords*

```
service password-encryption
enable secret 5 $1$CNqo$C4bT4/zR.iJF0YEpqMhPF/
enable password 7 13061E010803
```

This ensures that if anyone (intruder or insider) views the configuration file, the passwords are hidden. Then, define the secret password, because it is hidden using a stronger authentication (MD5) than the enable password.

Example 7-4 configures R1 to disable DHCP, which is enabled by default.

Example 7-4 *Disable DHCP*

```
no service dhcp
```

Cisco has enabled routers to act as DHCP servers to clients by default. This is not a necessary service to have running, so it should be disabled to stop any intruder from receiving a valid IP address.

Example 7-5 enables R1 to log any debug output and define each entry with a timestamp.

Example 7-5 *Logging Router System Changes and Events*

```
service timestamps debug
service timestamps log
logging buffered 64000 debugging
logging rate-limit console 10 except errors
no logging console
logging trap debugging
logging 1.1.1.1
logging 141.108.1.1
logging 5.5.5.5
```

Make sure that the router's clock is set to the correct time, via NTP or manual entry with the **clock set** command. This allows you to look at the log after any incident has occurred. Also, because you are logging to a remote host or hosts and locally to the buffer, you can disable the debug output to the console port so that messages do not overwhelm the router. You are logging to three different remote hosts. You can also buffer and output the log file for viewing at a time favorable to the network administrator.

You can enable a Cisco IOS router to log messages with the command **logging on**. The command **logging buffered** enables the router to store logged messages, such as configuration to a local file

stored in NVRAM, for later viewing. To view a logging message buffered to memory, use the **show logging** command. Note that **trap debug level logging** to three different hosts can significantly increase the load on a router's CPU. You may limit logging to one or two hosts or only when troubleshooting. For the purposes of this example, assume that the highest level is used.

Example 7-6 configures R1 with the **service sequence** command.

Example 7-6 *Enable Sequence Numbering*

```
service sequence-numbers
```

The service category is quite useful. Essentially, enabling it means that your syslog entries will be numbered to ensure that they are not tampered with. R1 is configured for TACACS via the remote host 131.108.1.1.

Example 7-7 configures R1 for AAA.

Example 7-7 *AAA Configuration*

```
username cisco pass ciSc0
aaa new-model
aaa authentication login default group tacacs+ local-case
aaa authentication enable default group tacacs+ enable
aaa authorization commands 15 default group tacacs+ local
aaa accounting exec default stop-only group tacacs+
aaa accounting commands 15 default stop-only group tacacs+
aaa accounting network default stop-only group tacacs+
tacacs-server host 131.108.1.1
tacacs-server key myguitarrocksthisworld
!A backup username is added here in case the tacacs+ server is not reachable.
username cisco pass cisco
```

Example 7-7 configures R1 for AAA authentication, if in the event TACACS+ fails to use local authentication with the command **username** *cisco* **password** *cisco*.

By default, Cisco IOS software permits a number of default TCP/IP services. Example 7-8 disables some common services.

Example 7-8 *Disable Services on by Default*

```
no ip http server
no ip finger
no service pad
no ip source-route
no ip bootp server
```

Example 7-8 disables R1 for an HTTP server. The **finger** command service allows remote users to view the output (equivalent to the **show users** [**wide**] command). When **ip finger** is configured, the router responds to a **telnet** *a.b.c.d* **finger** command from a remote host by immediately displaying the output of the **show users** command and then closing the connection. You should turn this service off. The **service pad** command enables all packets to be assembled or disassembled between packet assembler/disassembler (PAD) devices and access servers. The command **no ip source-route** causes the system to discard any IP datagram containing a source-route option. When you disable the BOOTP server, access to the BOOTP ports causes the Cisco IOS software to send an ICMP port unreachable message to the sender and discard the original incoming packet. If the Cisco router is enabled for helper addresses, then BOOTP requests will now fail, so you might need to leave this command enabled if you are sending DHCP requests to another server.

Example 7-9 enables TCP intercept.

Example 7-9 *TCP Intercept*

```
ip tcp intercept list 100
ip tcp intercept connection-timeout 60
ip tcp intercept watch-timeout 10
ip tcp intercept one-minute low 1800
ip tcp intercept one-minute high 5000
access-list 100 permit ip any any
```

TCP intercept helps prevent SYN flood attacks by intercepting and validating TCP connection requests. In intercept mode, the TCP intercept software intercepts TCP SYN packets from clients to servers that match an extended access list. The router responds; if it is a valid connection, the devices are allowed to communicate.

The **low** and **high** commands identify when TCP intercept should deactivate or activate (TCP aggressive mode).

In this case, the Cisco IOS command **ip tcp intercept one-minute high 5000** defines the number of connection requests (5000) received in the minute before the Cisco IOS software enters aggressive mode. The Cisco IOS command **ip tcp intercept one-minute low 1800** defines the number of connection requests (1800) below which the software leaves aggressive mode.

Example 7-10 configures R1 to dump the router's memory contents in case of a router crash.

Example 7-10 *Allowing Core Dumps*

```
ip ftp username rooter
ip ftp password $%&#*&^$$%&$
exception core-file secure-r01-core-dump
exception protocol ftp
exception dump 3.3.3.3
```

It is important to be able to look at the reasons a router crashed, especially a router that provides a security wall to the outside world. Core dumps can be given to Cisco personnel who in turn can decipher the main reason the router crashed. The Cisco IOS command **exception core-file secure-r01-core-dump** sets the filename generated when the router actually crashes. The Cisco IOS command **exception protocol ftp** defines the protocol used to send the memory dump. The Cisco IOS command **exception dump 3.3.3.3** defines the remote host where the file will be copied; in this case, the file will be copied via FTP to remote host 3.3.3.3. Cisco Systems TAC engineers will use the memory dump to try to decipher why the router crashed.

Example 7-11 shows R1 configured for some common parameters for packets sent to unknown destinations and networks that do not exist. Cisco Discover Protocol (CDP) is also disabled, to stop other Cisco devices from discovering details about this router.

Example 7-11 *IP Unreachables and Routes to Null0*

```
interface Ethernet0
 ip address 3.3.3.3 255.255.255.255
 no ip redirects
 no ip unreachables
 ip verify unicast reverse-path
 no cdp enable
no ip proxy-arp
no ip mask-reply
interface null0
no ip unreachables
ip route 131.0.0.0 255.0.0.0 null0
```

The Cisco IOS command **no ip redirects** disables the Cisco router from sending ICMP redirect messages to a device's source from the same interface.

The Cisco IOS command **no ip unreachables** disables the router from sending ICMP unreachable messages for packets it is not configured for. The **ip route** command ensures that packets received for the network 131.10.0.0/12 are thrown away and not acted on. This can stop a routing loop and an intruder trying to spoof (pretend) to belong to network 131.10.0.0/12.

The **ip verify unicast reverse-path** command helps mitigate problems caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address.

The **no ip proxy-arp** command disables proxy ARP on the interface. Proxy ARP is a technique in which one host, usually a router, answers ARP requests intended for another machine. Attackers can exploit this by sending a large number of proxy ARP requests, pretending to be a real host by "assuming" or "faking" its identity. Disabling proxy ARP prevents the router from accepting responsibility for routing packets to the "real" destination. Proxy ARP, when used correctly, can help machines on a subnet reach remote subnets without configuring routing or a default gateway. Typically, this issue is resolved by DHCP or statically configured gateways, so you can disable this option on all Cisco IOS–enabled devices. Proxy ARP is defined in RFC 1027.

Disabling mask replies, with the command **no ip mask-reply**, ensures that the Cisco IOS software does not respond to ICMP mask requests by not allowing ICMP mask reply messages.

Loopback interfaces are the source of log messages. Loopbacks are often used for routing protocols, as well, because a logical interface does not go down and is reliable. Assign an IP address that uniquely identifies this router. Then, configure and activate the null0 interface as a place to send unknown destination packets. This becomes the trap for packets; they can route in but they can't route out if an intruder is spoofing networks from valid IP networks.

The configurations shown in Examples 7-1 through 7-11 are just some of the techniques you can use to ensure that vulnerable routers are secure. Just imagine all the routers in the Internet that do not contain this level of security, and you will be aware of the challenges faced in the day-to-day running of the World Wide Web and the reasons why organizations like CERT/CC are an invaluable resource.

Sometimes even the most basic security can help an organization mitigate a virus. For example, assume that your company uses 135.15.0.0/16 as its network. In that case, any traffic from the outside (Internet) with a 135.15.0.0/16 address must be bogus unless initiated from inside of the network; similarly, any traffic from inside with an address other than 135.15.0.0 would be bogus. These should be logged. In the case of repeat offenders inside, the systems are either being used by a hacker or, more likely, have been infected with a worm that spoofs source addresses.

For more details on improving security on Cisco devices, visit http://www.cisco.com/warp/public/707/21.html.

Foundation Summary

The "Foundation Summary" is a condensed collection of material for a convenient review of this chapter's key concepts. If you are already comfortable with the topics in this chapter and decided to skip most of the "Foundation Topics" material, the "Foundation Summary" will help you recall a few details. If you just read the "Foundation Topics" section, this review should help further solidify some key facts. If you are doing your final preparation before the exam, the "Foundation Summary" offers a convenient and quick final review.

Table 7-2 *Key Reasons that Networks Should be Secured*

Policy Reason	Meaning
Inherent technology weaknesses	All network devices and operating systems have inherent vulnerabilities.
Configuration weaknesses	Common configuration mistakes can be exploited to open weaknesses.
Network policy vulnerabilities	The lack of network policies can lead to vulnerabilities such as lax password security.
Outside/inside intruders	There are always internal and external people wanting to exploit network resources and retrieve sensitive data.

Table 7-3 *Intruder/Hacker Motivations*

Intruder/Hacker Motivation	Explanation
Cash profit	To make money from attacks, such as by transferring funds
Revenge	To get back at employers or individuals
Vandalism	To cause damage for personal satisfaction
Hacktivism	To gain an advantage or notoriety for an organization's ideology
For a challenge	To act on peer pressure or challenges set by other hackers to gain notoriety
Curiosity	To learn the tools of the trade, possibly to gain experience for bigger challenges
Cyber terrorism	To attack a critical part of the infrastructure, such as crashing or denying service to online banking or brokerage servers

Table 7-4 *Incident Response Team Actions*

Step	Description
1	Verify the incident.
2	Determine the magnitude of the incident (hosts affected and how many).
3	Assess the damage (for example, determine if public servers have been modified).
4	Gather and protect the evidence.
5	Inspect systems to determine damage.
6	Remove hostile or destructive code.
7	Reload necessary operating system software.
8	Restore configurations.
9	Restore and test operations.
10	Patch system to reduce vulnerability.
11	Inspect applications to determine damage.
12	Reload software if necessary.
13	Test functionality.
14	Inspect files to determine damage.
15	Restore files from backup if necessary.
16	Replicate damaged files if no backup is available.
17	Confirm with users that data is restored.

Table 7-5 *Network Attacks**

Attack	Meaning
Ping of death	Sends an improperly large ICMP echo request packet with the intent of overflowing the destination machine's input buffers and causing it to crash. The IP header field is set to 1, the last fragment bit is set, and the data length is greater than 65,535, greater than the maximum allowable IP packet size.
TCP SYN flood attack	DoS attack that randomly opens a number of TCP ports, ensuring that network devices are using CPU cycles for bogus requests and denying other legitimate users access.
Teardrop	Exploits an overlapping IP fragment implementation bug in various operating systems. The bug causes the TCP/IP fragmentation re-assembly code to improperly handle overlapping IP fragments, causing the host to hang or crash.
Land.C attack	A program designed to send TCP SYN packets (TCP SYN is used in the TCP connection phase) that specify the target's host address as both source and destination. This program can use TCP port 113 or 139 (source/destination), which can also cause a system to stop functioning.

continues

Table 7-5 *Network Attacks* (Continued)*

Attack	Meaning
DNS poisoning	Exploits the DNS server, causing the server to return a false IP address to a domain name query.
UDP bomb	Sends illegal Length field in the packet header, causing kernel panic and crash.
E-mail attack	DoS attack that sends a random number of e-mails to a host.
CPU-intensive attack	DoS attack that ties up system resources by using a program such as a Trojan horse (a program designed to capture usernames or passwords from a network) or enabling viruses to disable remote systems.
Chargen attack	Establishes UDP services by producing a high character input. This can cause congestion on a network.
Attack via dialup (out of band)	Applications, such as Windows 95, have built-in vulnerabilities on data port 139 (known as WinNuke), if the intruders can ascertain the IP address.
Distributed DoS	DoS attack that is run by multiple hosts. The attacker first compromises vulnerable hosts by using various tools and techniques. Then, the actual DoS attack on a target is run from the pool of all these compromised hosts.

*Note that there are constantly new attacks created. To keep up date, visit http://www.cert.org/advisories.

Table 7-6 *Protecting Cisco IOS Routers*

Cisco IOS Command	Meaning
service nagle	Enables the Nagle algorithm.
no service udp-small-servers and **no service tcp-small-servers**	By default, the TCP/UDP servers for Echo, Discard, Chargen, and Daytime services are disabled.
service password-encryption	Ensures that all passwords are encrypted and not viewable when viewing the Cisco IOS configuration file.
service timestamps debug **service timestamps log**	Enables the router to log any debug output and define each entry with a timestamp.
service sequence-numbers	Allows the syslog entries to be numbered to ensure that they are not tampered with.
ip tcp intercept list 100	Enables TCP intercept.
no ip redirects	Disables the Cisco router from sending ICMP redirect messages to a device's source from the same interface.
no cdp enable	Disables the Cisco CDP protocol.

Q & A

The Q & A questions are designed to help you assess your readiness for the topics covered on the CCIE Security written exam and those topics presented in this chapter. This format should help you assess your retention of the material. A strong understanding of the answers to these questions will help you on the CCIE Security written exam. You can also look over the questions at the beginning of the chapter again for further review. As an additional study aid, use the CD-ROM provided with this book to take simulated exams, which draw from a database of over 500 multiple-choice questions.

Answers to these questions can be found in Appendix A, "Answers to Quiz Questions."

1. Define four reasons why networks must be secured.
2. What is the function of the CERT/CC organization, and what are its primary objectives?
3. What are the primary steps completed by incident response teams?
4. Name common methods used by intruders to disrupt a secure network.
5. In security, what is TCP session hijacking?
6. In security terms, what is a man-in-the-middle attack?
7. What is a signature engine?
8. What is social engineering?
9. What is a ping of death attack?
10. What is a Land.C attack?
11. What does the following Cisco IOS code accomplish on a Cisco IOS router?

```
no service udp-small-servers
no service tcp-small-servers
```

12. What is the secret password for the following Cisco IOS configuration?

```
enable secret %$@$%&^$@*$^*@$^*
enable pass cisco
```

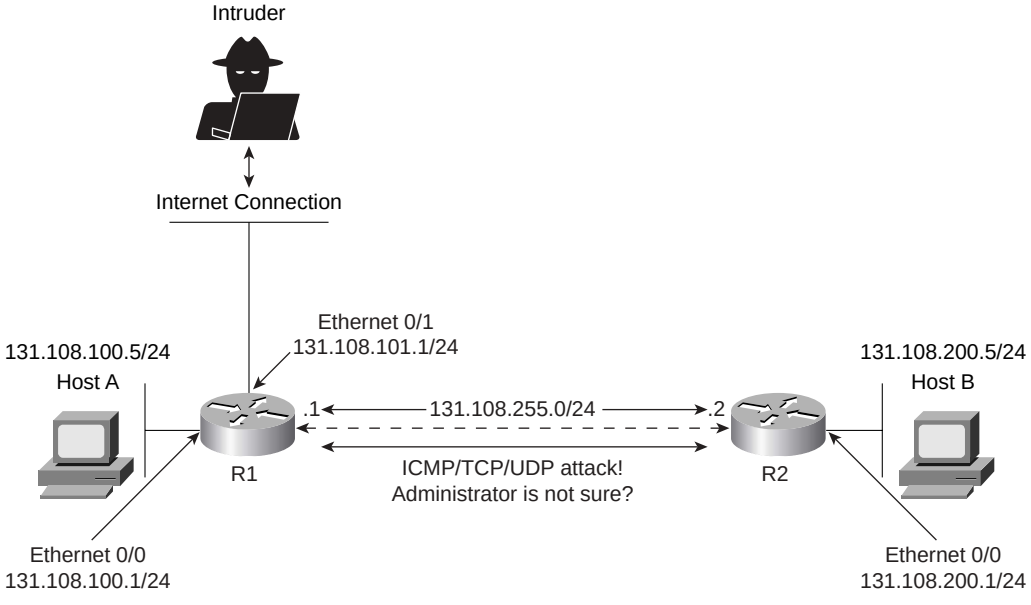
13. What is the purpose of the command **service sequence-numbers**?

Scenario

Scenario: Defining Cisco IOS Commands to View DoS Attacks in Real Time

Figure 7-3 displays a typical two-router topology with an external connection to the Internet via R1.

Figure 7-3 *Two-Router Network Attacked by External Intruder*



In this scenario, a Cisco IOS router is subjected to ICMP, TCP, or UDP IP packets. The network administrator is not sure of what type but notices the log file that is buffered to Router R2 has just increased from 1 MB to 2.5 MB in less than 5 seconds. What can be done to characterize the traffic and detect the type of denial-of-service attack?

Scenario Answers

Scenario Solutions

The network administrator can quickly configure an extended access list permitting all ICMP, UDP, or TCP, as shown in Example 7-12, applying the access list to the inbound interface on R2, Serial0/0. (The configuration is truncated to focus on the critical configuration.)

Example 7-12 *Access List Configuration on R2*

```
Hostname R2
!
interface Serial0/0
 ip address 131.108.255.2 255.255.255.0
 ip access-group 100 in
!
access-list 100 permit icmp any any log-input
access-list 100 permit tcp any any log-input
access-list 100 permit udp any any log-input
!
End
```

To determine the traffic type, access list 100 allows ICMP, UDP, and TCP inbound on Serial0/0. Logging is also enabled with the keyword **log-input**. Assuming that the DoS attack is taking place, by viewing the access list 100 with the command **show ip access-list 100**, you can get an idea which protocol type is being used. The displays in Example 7-13 are taken from R2 while the DoS attack is taking place. The command **show ip access-list 100** is entered a few times on R2 to view the statistics and crucial bits of data that enable you to verify the source of the attack and the method, whether it is ICMP, TCP, or UDP. Logging has been enabled, so the display in Example 7-13 describes what packet matches have been made and incremented each time a packet match is made on access list 100.

NOTE When enabling the keyword **log** or **log-input** on an ACL, you must be aware of the impact on the CPU and how to view the entries. For example, an IP packet matching the ACL will be counted in the ACL log as well as the syslog buffer and to a syslog server if present. Typically, this is a troubleshooting scenario impacting your network, so it is safe to assume that once the administrator determines the root cause, the **log-input** keyword will be removed to ensure that CPU resources on the router are not impacted indefinitely.

Example 7-13 **show ip access-list 100** *on R2 (Repeated Five Times in Real Time)*

```
r2#show ip access-lists 100
Extended IP access list 100
    permit icmp any any log-input (5000 matches)
    permit tcp any any log-input (100 matches)
    permit udp any any log-input (23 matches)
r2#show ip access-lists 100
Extended IP access list 100
    permit icmp any any log-input (25000 matches)
    permit tcp any any log-input (100 matches)
    permit udp any any log-input (24 matches)
r2#show ip access-lists 100
Extended IP access list 100
    permit icmp any any log-input (35500 matches)
    permit tcp any any log-input (100 matches)
    permit udp any any log-input (25 matches)
r2#show ip access-lists 100
Extended IP access list 100
    permit icmp any any log-input (45500 matches)
    permit tcp any any log-input (100 matches)
    permit udp any any log-input (26 matches)
r2#show ip access-lists 100
Extended IP access list 100
    permit icmp any any log-input (67000 matches)
    permit tcp any any log-input (100 matches)
    permit udp any any log-input (26 matches)
r2#
```

Example 7-13 clearly shows that ICMP packets are increasing at an alarming rate. This indicates that an intruder could be attempting a Smurf attack (by sending a large number of ICMP requests). Now that you have identified the protocol type, you can take steps to stop ICMP packets from being sent to R2, by configuring the access list 100 on R1's outbound interface to R2, as displayed in Example 7-14.

Example 7-14 *R1's Access List 100 Configuration*

```
Hostname R1
!
interface Serial0/0
 ip address 131.108.255.2 255.255.255.0
 ip access-group 100 out
!
access-list 100 deny icmp any any log-input
access-list 100 permit tcp any any log-input
access-list 100 permit udp any any log-input
!
End
```

You can also configure R1 from the inbound Internet connection with the same access list denying ICMP inbound requests. The **log-input** optional command is applied so that you can monitor traffic matching the ICMP, TCP, or UDP frame formats. This will help you to identify the root cause. Note that all Internet routers should have ACLs already configured securely, permitting only traffic to and from the Internet. This scenario is aimed at showing you the power of Cisco IOS ACLs. Adding the **log** command can severely impact a router's performance, so care should always be taken. Consult the Cisco Technical Support or Cisco documentation for more details.

This scenario is a simple one that clearly demonstrates the power of extended access lists and the simplest use of **show** commands that can be deployed in any midsize or large IP network to quickly identify and prevent some DoS attacks.


Catalyst 6500

CHAPTER 8

CCIE Security Self-Study Lab

This chapter is designed to assist you in your final preparation for the CCIE Security exam by providing you with an extensive lab that incorporates many of the technologies and concepts covered throughout this book. This lab requires a broad perspective and knowledge base. Any knowledge you have acquired through the practical examples presented in this guide and real-life network implementations will help you achieve the end goal: a *routable* network according to the security design criteria.

The CCIE lab exam was traditionally a 2-day lab held in various world-wide locations such as Sydney and Brussels along with the traditional sites based in San Jose and Raleigh. However, when the CCIE Security lab exam was introduced, it contained only a 1-day lab portion. In the 1-day CCIE Security lab practical exam, the candidate is presented with a number of simple and complex tasks, starting from the physical layer of the OSI model and continuing up to the application layer. Recent changes to the CCIE Security lab remove some of the fundamental routing and switching components to ensure that candidates are thoroughly tested for security rather than their knowledge of routing and switching, which is still a core skill. Hence, the exam is, by far, more difficult than the CCIE Routing and Switching lab. This sample lab still presents those fundamental tasks so that the reader can appreciate the level of difficulty in the practical exam.

When you are given the exam paper, it may appear that the questions are relatively easy, but as you read further into the paper, you will discover that the questions become increasingly more difficult. The lab questions were created so that highly complex questions have some hidden aspects to them, as you will discover in this sample lab exam.

To become a CCIE in the Security track, a candidate must successfully gain 80 exam points from a possible 100 points in 8 hours. What is not mentioned in many exam books and websites is the mental strength and drive required to maintain a high level of concentration for 8 hours. The exam is written so that readers start with basic tasks and build up gradually to more complex scenarios. Some tasks are dependant on prior questions being successfully completed, so it may be very easy to become lost very quickly in a lab exam environment.

Fortunately, you have, in your hands, a lab written by two former CCIE Security proctors, so this sample lab is a great start. If you can simulate exam conditions and successfully complete

this lab with a score of 80 points or more, you are well on your way to achieving your end goal after reading this book.

Each major task is given a point value, with no partial credit possible. This is as close as you will come to the real lab without having to actually sit in the lab and pay the lab fee of over U.S.$1,000.

This sample lab is presented in sections. A solution appears following each section. At the end of this sample CCIE Security lab (after the final configurations), I provide you with some additional sample CCIE Security questions to demonstrate other possible topics. No solutions are provided, so you can research and attempt to answer them on your own as you would if you were sitting in the real CCIE Security lab.

At the end of the main lab section, the final configurations are presented for your reference. If you have any questions on this lab, e-mail me at henry.benjamin@optusnet.com, and I will try to help clarify any questions you might have.

NOTE This lab draws together much of the content covered throughout this book. Keep in mind that there is not always one right or wrong way to accomplish many of the tasks presented here, but you should follow the parameters that are stipulated. You should also modify the tasks to make them even harder so that you are prepared for the worst-case scenario in the real lab.

How to Use This Chapter

This lab contains a five-router network, an intrusion detection system (IDS), and a PIX Firewall 520 (ISP) providing a connection to the Internet. This lab is designed to ensure that you have all the practical skills to achieve almost any IP routing and security requirements in real-life networks, and to test your practical skill set so that you can confidently pass the CCIE Security exam.

Preparing for this Lab

You can use any combination of routers and switches to complete this lab as long as you fulfill the requirement for a properly routing and secure topology. If you do not have some of the equipment, the example displays will show you what you should expect to see in a working CCIE lab topology, which will be an invaluable resource and study guide.

NOTE As of July, 2004, the hardware types you can expect to see in the real CCIE Security lab exam, as documented by Cisco, are as follows:

- 2600 series routers
- 3600 series routers
- 3700 series routers
- Catalyst 3550 series switches running Cisco IOS version 12.1EA
- PIX Firewall
- Certificate Authority support
- Cisco Secure Access Control System (ACS)
- Cisco Secure Intrusion Detection System
- VPN Concentrators
- IDS sensors

Because Cisco IOS can be driven by various different platforms, you can simulate the real environment in this lab scenario even if you cannot match exactly the Cisco-recommended devices used in this lab. Simply substitute as best as you can a Cisco IOS–enabled device with the Security and VPN software feature set, especially in terms of routers and switches presented in this chapter. There is no VPN Concentrator in this sample lab because the configuration of this device is relatively easy compared to the IOS security features on the router, PIX, and the IDS.

Goal of This Lab

This lab should assist you in your final preparation for the CCIE Security lab exam.

Sample solutions are provided here, but you need to research other various solutions on your own. Feel free to modify the questions to suit any design scenario and discover new IOS commands by using the Cisco Universe CD-ROM. This lab is not the only tool you should use; rather, it is provided here to demonstrate the minimum level of difficulty you will encounter when attempting the CCIE Security lab exam.

This lab builds on the sample Routing and Switching labs presented in Appendixes C and D. This is intentional because the CCIE Security lab exam builds on your routing skills and requires you to build a secure IP network. The CCIE Security lab exam is a difficult exam because the routing and switching topics are assumed knowledge. You can think of the CCIE Security lab exam as two lab exams built into one difficult security exam.

The end goal of any CCIE lab is a working solution, although you might be restricted by certain parameters. Candidates often ask me how best to prepare for the CCIE Security lab exam. My answer is to practice and configure every feature available and then practice some more. Of course, not every feature will be tested, and you are encouraged to read the most up-to-date information at http://www.cisco.com/en/US/learning/le3/ccie/security/index.html for the latest information regarding the CCIE Security certification. In particular, always look for new details on new Cisco IOS technologies and hardware.

NOTE The CCIE Security lab doesn't require you to configure any Token Ring devices or Token Ring interfaces, nor any non-IP protocols, such as IPX or DLSW.

Effective November 4, 2002, CCIE labs worldwide employ Catalyst 3550 with Cisco IOS v12.1 using the Enhanced Multilayer Image.

CCIE Security Self-Study Lab Part I Goals

The goal of Part I of this sample lab is to ensure that you provide a working IP network solution quickly and adhere to the guidelines given. You should take no longer than 4 hours to complete Part I. Starting in October 2004, the CCIE Security lab exam has some of the basic Frame Relay and routing protocols already configured, to allow candidates more time on security features. The following is a list of technology topics now preconfigured for the lab candidate:

- Bridging and switching
- Basic Frame Relay configuration
- Catalyst VLAN configuration
- Catalyst VTP configuration
- Port-VLAN assignments
- Basic ATM configuration
- IGP routing
- OSPF, EIGRP, and RIP configurations
- BGP
- Basic IBGP, EBGP, and BGP backbone configurations

This section is preserved, however, to allow readers to appreciate the level of expertise required in this most difficult CCIE certification track.

CCIE Security Self-Study Lab Part II Goals

Part II builds on the working IP network and requires security features such as IPSec and PIX. RIP routing is also required. You will also notice the addition of an IDS sensor. Expect to be tested on IDS sensors and the VPN Concentrator in the lab exam. You are likely to be asked to configure both devices. Part II of this lab does not include the VPN Concentrator, however. Review the additional advanced topics questions for possible exam scenarios for the VPN Concentrator. You should take no longer than 4 hours to complete Part II.

For more sample labs and detailed security lab study, consider the following Cisco Press publications (www.ciscopress.com):

- *CCIE Security Practice Labs* (ISBN: 1-58705-134-6)
- *CCIE Practical Studies: Security* (ISBN: 1-58705-110-9)

General Lab Guidelines and Setup

Follow these general guidelines during this lab:

- Static and default routes are not permitted unless directly stated in a task. This includes floating static routes.
- Use the DLCIs provided in the Frame Relay diagram (presented shortly).
- All routers and switches should be able to ping any interface using the *optimal routing path.*
- Do not configure any authentication or authorization on any console or aux ports unless specified.
- Routes to Null0 generated by any routing protocol are permitted.
- Full access to the two AAA servers from your workstation is permitted. The user ID is admin, and the password is cisco.
- The Class B address 144.254.0.0/16 is used throughout the network.

Some configuration tasks are now preconfigured in the Security lab exam. In this sample lab, these tasks are still outlined for practice, but are given a zero point value to indicate that in the real Cisco Security exam you can expect these features to be preloaded for you.

NOTE In the actual CCIE Security lab, beginning October 1, 2004, the equipment in the rack assigned to you is physically cabled and should not be tampered with. Router host names, basic IP addressing, **no exec-timeout**, and passwords on the con, aux, and vty lines have been preconfigured. The Catalyst has a preconfigured prompt and enable passwords. All preconfigured passwords are cisco and should not be changed unless explicitly stated in a question.

Figure 8-1 displays the topology of the routed network.

Figure 8-1 *Lab Topology*

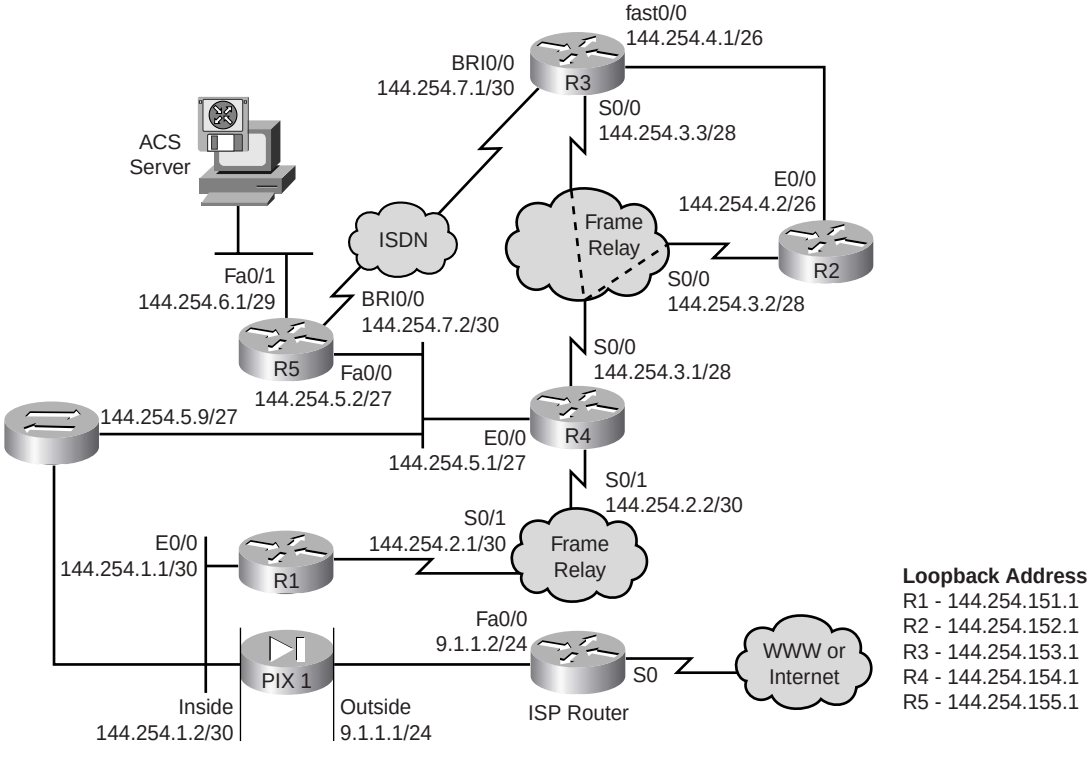


Figure 8-2 displays the Frame Relay topology setup.

NOTE Not all CCIE labs require a communication server to be configured. In fact, most sites will have the communications already configured and you can have separate windows for each router, allowing you to configure more than one router at a time. The IP address assignment is also preconfigured. Understanding IP subnetting is a critical topic that all network designers must master.

Figure 8-2 *Frame Relay DLCI Assignment*

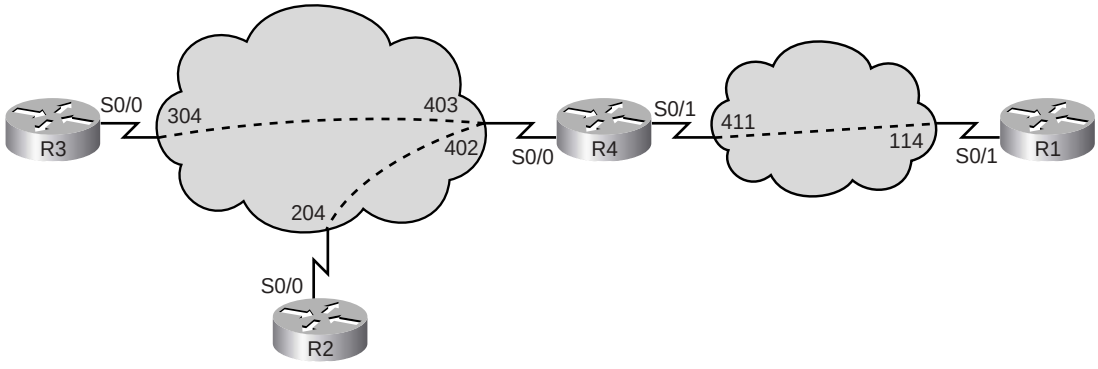


Table 8-1 displays the IP address assignment for the network topology in Figure 8-1.

Table 8-1 *IP Address Assignment*

Router Interface	IP Address
R1 E0/0	144.254.1.1/30
R1 S0/1	144.254.2.1/30
R2 E0/0	144.254.4.2/26
R2 S0/0	144.254.3.2/28
R3 Fast0/0	144.254.4.1/26
R3 S0/0	144.254.3.3/28
R3 BRI0/0	144.254.7.1/30
R4 E0/0	144.254.5.1/27
R4 S0/0	144.254.3.1/28
R4 S0/1	144.254.2.2/30
R5 FaEth0/0	144.254.5.2/27
R5 FaEth0/1	144.254.6.1/29
R5 BRI0/0	144.254.7.2/30
PIX inside	144.254.1.2/30
PIX outside	9.1.1.1/24
ISP router FastEth0/0	9.1.1.2/24

Each router, R1–R5, is to be configured for a loopback interface. Table 8-2 displays the IP address assignment for each router.

Table 8-2 *Loopback IP Address Assignment*

Router	Loopback IP Address
R1	144.254.151.1/24
R2	144.254.152.1/24
R3	144.254.153.1/24
R4	144.254.154.1/24
R5	144.254.155.1/24

After you complete your IGP confirmation, you must be able to ping or telnet to each router loopback from any given router.

NOTE Because of recent changes to the CCIE Security exam, the candidate is not required to configure IP addressing. However, the subject is presented here to ensure that potential CCIE candidates have a good understanding of IP address spaces and subnetting. Quickly perform a spot check on all of your routers to ensure that the CCIE Security exam documentation matches what is configured on your CCIE lab rack.

Communications Server (0 Points)

Configure the communication server (R1) so that when you type the host name of a router on the communications server, you are connected across the console port to that router:

- Disable the **break** command on R1 so that R1 will not permit an intruder to issue a **break** command and perform password recovery. (Hint: Change the configuration register to 0x2002.)
- Set up the routers, as shown in Figure 8-1.
- Configure R1 as the communication server using the **ip host** command.
- Communication server ports 2 to 5 are connected to Routers R2 to R5, respectively.
- Communication server port 8 connects to the Catalyst 3550 series switch.

Communications Server Solution

Router R1 is configured for reverse Telnet. To enable reverse Telnet on the async lines 1 through 16, you must first enable Telnet. Example 8-1 allows reverse Telnet through lines 1 through 16.

Example 8-1 *Enable Reverse Telnet on R1*

```
Line 1 16
transport input all
```

After allowing for reverse Telnet (you could also apply the **transport input telnet** command, which permits Telnet only) on the async lines, define the reverse Telnet name and TCP port number. Line 1 uses TCP port 2001, line 2 TCP port 2002, and so on.

R2 is connected to Line 2, TCP port 2002, so the IOS command is as follows:

```
ip host R2 2002 local-ip- address
```

R3 is connected to Line 3, TCP port 2003, so the IOS command is as follows:

```
ip host R3 2003 local-ip-address
```

The local IP address must be an active interface, so choose the loopback IP address. If the local IP address is assigned to a LAN or WAN interface and that interface happens to fail, your reverse Telnet connection will not work. R1 is assigned the loopback address 144.254.151.1/24. The full configuration for R1 is displayed in Example 8-2. The PIX is connected to line 15, or TCP port 2015; the Ethernet switch is on line 8, or TCP port 2008 on the local router, R1. Example 8-2 configures R2 for local name lookup.

Example 8-2 *Communication Server Solution on R1*

```
ip host R2 2002 144.254.151.1
ip host R3 2003 144.254.151.1
ip host R4 2004 144.254.151.1
ip host R5 2005 144.254.151.1
ip host CAT5K 2008 144.254.151.1
ip host PIX 2015 144.254.151.1
line 1 16
transport input telnet
```

Example 8-3 displays a reverse Telnet connection on R1 to Router R2.

Example 8-3 *Reverse Telnet to R2 on R1*

```
R1>R2
Trying 144.254.151.1 2002 ... Open
User Access Verification

Password: cisco
R2>
```

CCIE Security Self-Study Lab Part I: Basic Network Connectivity (4 Hours)

Mimicking the real CCIE Security lab exam, Part I requires you to enable physical and logical connectivity. The section requires full network connectivity between all routers and switches, including the PIX Firewall. You can test this by pinging the assigned loopbacks from any given routers, switch, or PIX.

Basic Frame Relay Setup (5 Points)

Configure the network in Figure 8-2 for basic physical Frame Relay connectivity. The following are the parameters:

- You must use static Frame Relay maps for IP and disable Frame Relay inverse ARP. (Hint: Use **no frame-relay inverse-arp** on all frame-enabled interfaces.)
- For the connection between R1 and R4, you are not permitted the keyword **broadcast** when mapping IP between the R1/R4 Frame Relay link.
- No dynamic mapping is permitted.
- No Frame Relay subinterfaces are permitted on any router.
- Assume that RIP or IGRP will be configured over this link sometime in the next month. You are permitted to use any IOS command to accomplish this task. (Hint: Use the keyword **broadcast**.)
- Assign a subnet to each link from your Class B range, as described in Table 8-1.
- Use LMI type ANSI only. You can rely on auto-sensing the LMI type on all routers.
- All router interface types are set to DTE. The Frame Relay switch interface type is DCE.
- Ensure that you can also ping the local and remote IP interfaces from each router configured for Frame Relay.
- Table 8-1 displays the IP address assignments for the Frame Relay network in Figure 8-1.

Users in VLAN_D are sending large IP packets across the Frame Relay circuit. The Frame Relay provider has asked you to set the discard eligibility when any IP packets larger than 768 bytes are sent to R4 across the Frame Relay connection.

(Hint: Set the discard eligibility, DE, bit to packets greater than 768 bytes on R2/R3.)

Basic Frame Relay Setup Solution

The topology in Figure 8-2 defines a number of Frame Relay PVCs. R1 is connected to R4 through the local DLCI number 114. Example 8-4 configures R1 to map the remote IP address 144.254.2.2 through DLCI 114. Note the local mapping to allow local pings to the assigned IP address. In this case R1 will be able to ping its local Frame Relay IP address of 144.254.2.1.

Example 8-4 *Frame Relay Configuration R1*

```
interface Serial0/1
 ip address 144.254.2.1 255.255.255.252
 encapsulation frame-relay
 ip split-horizon
 frame-relay map ip 144.254.2.1 114
 frame-relay map ip 144.254.2.2 114
 frame-relay interface-dlci 114
 no frame-relay inverse-arp
```

Example 8-4 displays the configuration on R1 to enable Frame Relay encapsulation on R1 followed by static Frame Relay map statements (no **broadcast** keyword is permitted, as requested). The DLCI interface is defined as 114, and the command **no frame-relay inverse-arp** ensures that no dynamically learned mapping will be discovered. Make sure you use the **clear frame-relay-inarp** IOS command to remove any dynamically learned Frame Relay inverse ARP mappings. Another option to clear all dynamically learned Frame Relay mappings is to bounce the interface by shutting and then enabling the interface—worse case scenario if that fails is to reload all your routers.

By default, on a physical Cisco Frame Relay interface, Cisco IOS routers disable split horizon. You need to enable split horizon so that routing updates are not received from the originating router. IP split horizon is critical to distance vector protocols like RIP or IGRP.

Example 8-5 displays the Frame Relay configuration required on R4.

Example 8-5 *R4 Frame Relay Configuration*

```
interface Serial0/1
 ip address 144.254.2.2 255.255.255.252
 encapsulation frame-relay
 ip split-horizon
! Note two map statements so exec users can ping local and remote IP addresses
 frame-relay map ip 144.254.2.1 411
 frame-relay map ip 144.254.2.2 411
 frame-relay interface-dlci 411
```

R4 is configured for Frame Relay encapsulation for interface Serial0/1 and Frame Relay map statements for the local and remote IP addresses. Frame Relay inverse ARP is disabled with the **no frame-relay inverse-arp** command.

Example 8-6 confirms IP connectivity between R1 and R4, and that there are only static Frame Relay circuits.

Example 8-6 *Connectivity Between R1 and R4*

```
R1#show frame-relay map
Serial0/1 (up): ip 144.254.2.1 dlci 114(0x72,0x1C20), static,
              CISCO, status defined, active
Serial0/1 (up): ip 144.254.2.2 dlci 114(0x72,0x1C20), static,
              CISCO, status defined, active
R1#ping 144.254.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/10/12 ms
R1#ping 144.254.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
R1#
```

As requested by the lab parameters, both local and remote IP connectivity are active. Subinterfaces have not been used either.

Example 8-7 confirms the interface statistics on R1 and the LMI type setting at ANSI; because of LMI auto-sense, you do not need to define the LMI type explicitly.

Example 8-7 **show interface serial0/1** *on R1*

```
R1#show interfaces serial0/1
Serial0/1 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 144.254.2.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set
  Keepalive set (10 sec)
  LMI enq sent  111797, LMI stat recvd 111798, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 0  LMI type is ANSI Annex D  frame relay DTE

  FR SVC disabled, LAPF state down
  Broadcast queue 0/64, broadcasts sent/dropped 2/0, interface broadcasts 0
```

Example 8-7 **show interface serial0/1** *on R1 (Continued)*

```
  Last input 00:00:02, output 00:00:02, output hang never
  Last clearing of "show interface" counters 1w5d
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     378917 packets input, 17810137 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     409981 packets output, 28541580 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
     2 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Example 8-7 confirms the interface state as active (Serial0/1 is up, line protocol is up) and that the LMI type is set to ANSI (LMI type is ANSI). The physical state, signals DCD/DSR/DTR/RTS/CTS, indicates that the interface is operational at Layer 1 of the OSI model.

The same configuration steps are completed on the remaining routers. In this case, you are not restricted with Frame Relay static map statements. Use the keyword **broadcast** with remote IP addresses so that routing protocols, such as OSPF, can establish neighbor adjacencies.

Example 8-8 displays the Frame Relay configuration for R2.

Example 8-8 *R2 Frame Relay Configuration*

```
interface Serial0/0
 ip address 144.254.3.2 255.255.255.240
 encapsulation frame-relay
ip split-horizon
 frame-relay map ip 144.254.3.1 204 broadcast
 frame-relay map ip 144.254.3.2 204 broadcast
 frame-relay map ip 144.254.3.3 204 broadcast
 frame-relay interface-dlci 204
 no frame-relay inverse-arp
 frame-relay lmi-type ansi
```

R2 has three Frame Relay map statements: one is to remote Router R4, another to remote Router R3, and one to the local IP address on R2 itself. Also, in this configuration, the LMI type is manually set.

Example 8-9 displays the Frame Relay configuration for R3.

Example 8-9 *R3 Frame Relay Configuration*

```
interface Serial0/0
 ip address 144.254.3.3 255.255.255.240
 encapsulation frame-relay
 ip split-horizon
 frame-relay map ip 144.254.3.1 304 broadcast
 frame-relay map ip 144.254.3.2 304 broadcast
 frame-relay map ip 144.254.3.3 304 broadcast
 frame-relay interface-dlci 304
 no frame-relay inverse-arp
```

R3 is configured for Frame Relay, and the three map statements to maintain connectivity to R4, R2, and the local IP address are assigned to Serial0/0. R2 and R3 have been configured for split horizon in case a distance vector protocol is deployed in the future.

R4 is the hub router between R2 and R3. Because a subinterface is not permitted, you must define the two local DLCIs, 402 and 403. By default, when Frame Relay is enabled on a main Cisco IOS interface, split horizon is disabled. Because R4 is connected to R2 and R3, R4 must send information it receives from R2 to R3 and from R3 to R2. If a distance vector protocol is used, you must leave split horizon disabled. Because R2 and R3 have split horizon enabled, you will not have a routing loop because both R2 and R3 will reject any networks advertised by R4 that are local (as split horizon is enabled and the main purpose is to reject networks advertised by a local router). In this lab, OSPF is configured between R4, R2, and R3, and you do not need to be concerned about split horizon; it is added here to bring to your attention the possibility of routing loops when distance vector routing protocols, such as RIP, are used in Frame Relay networks.

Example 8-10 displays the Frame Relay working configuration on R4.

Example 8-10 *R4 Frame Relay Configuration*

```
interface Serial0/0
 ip address 144.254.3.1 255.255.255.240
 encapsulation frame-relay
 frame-relay map ip 144.254.3.1 402 broadcast
 frame-relay map ip 144.254.3.2 402 broadcast
 frame-relay map ip 144.254.3.3 403 broadcast
 frame-relay interface-dlci 402
 frame-relay interface-dlci 403
 no frame-relay inverse-arp
 frame-relay lmi-type ansi
 no ip split-horizon
```

Now that R2, R3, and R4 have been configured for Frame Relay, ensure that IP connectivity is enabled by pinging all the interfaces on each router.

Example 8-11 displays a successful ping request on R4 to R2 and R3, as well as the local interface on R4.

Example 8-11 *Ping Request to R2, R3, and Local IP Address*

```
R4#show frame map
Serial0/0 (up): ip 144.254.3.1 dlci 402(0x192,0x6420), static,
              CISCO, status defined, active
Serial0/0 (up): ip 144.254.3.2 dlci 402(0x192,0x6420), static,
              broadcast,
              CISCO, status defined, active
Serial0/0 (up): ip 144.254.3.3 dlci 403(0x193,0x6430), static,
              broadcast,
              CISCO, status defined, active
Serial0/1 (up): ip 144.254.2.1 dlci 411(0x19B,0x64B0), static,
              CISCO, status defined, active
Serial0/1 (up): ip 144.254.2.2 dlci 411(0x19B,0x64B0), static,
              CISCO, status defined, active
R4#ping 144.254.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/9/12 ms
R4#ping 144.254.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
R4#ping 144.254.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
R4#
```

R4 has only static Frame Relay statements, as required by the lab.

The final step is to enable Routers R2 and R3 to set the discard eligibility (DE) when users from VLAN_D send frames larger than 768 bytes. The ISP typically sets and acts on the DE.

Example 8-12 enables R2 and R3 to set the DE bit when frames larger than 768 are received from VLAN_D. This is a global configuration command.

NOTE In Cisco IOS 12.2T and higher, the Frame Relay DE group functionality is being replaced by the Modular QoS CLI (MQC) DE marking functionality. For information about the MQC commands that are used to configure Frame Relay DE marking, refer to the "Cisco IOS Quality of Service Configuration Guide" and "Cisco IOS Quality of Service Command Reference."

Example 8-12 *DE Set on R2 and R3*

```
frame-relay de-list 5 protocol ip gt 768
```

This completes the Frame Relay configuration.

Physical Connectivity (0 Points)

Your network is already physically patched. Construct your network, as shown in Figure 8-1 and Figure 8-2.

Configure the following characteristics for the topology in Figure 8-1 and Figure 8-2:

- Routers R3 and R5 are connected to an ISDN service with the switch type defined as basic-5ess. R3 connects to number plan 7775010 and R5 connects to number plan 7775020.
- Routers R1 through R5 are connected to the Catalyst Ethernet switch (Catalyst 3350 series switch) as follows:

Interface	Switch-1
R1 E0/0	Fa0/1
R2 E0/0	Fa0/2
R3 Fa0/0	Fa0/3
R4 E0/0	Fa0/4
R5 Fa0/0	Fa0/5
R5 Fa0/1	Fa0/6
PIX inside	Fa0/7
PIX outside	Fa0/8
Backbone 1	Not in use
Backbone 2	Not in use
IDS control interface	Fa0/11
IDS sniffing interface	Fa0/12

No solution is provided on the physical setup. In the lab, all physical connections are precabled; this section is provided for readers who have access to real Cisco equipment and want to practice.

Catalyst Ethernet Switch Setup I (5 Points)

Configure the Ethernet switch for five VLANs:

- VLAN 2, named VLAN_A, is connected to R1 and PIX inside.
- VLAN 3, named VLAN_B, is connected to R4 and R5 Eth0/0.
- VLAN 4, named VLAN_C, is connected to R5 FastEth0/1 (switch port Fast0/6).
- VLAN 5, named VLAN_D, is connected to R2 and R3.
- VLAN 6, named VLAN_E, is connected to the PIX outside interface and to the ISP managed router.
- Ensure that the IDS is also in the correct VLANs for the sniffing and control interfaces.

Using VLAN_D (VLAN 5), configure the management interface sc0 with the address 144.254.4.3/26. Ensure that all devices in your network can ping the switch even if R2 or R3 is down.

Make sure the switch is configured in the VTP domain, SecCCIE.

The switch will never be permitted to create any more VLANS, so ensure that after you set up these VLANs, only a VTP server configuration change will allow VLAN additions to this switch.

Ensure that the only routers that can telnet to the switch are the loopback IP interfaces on R1 through R5 and the directly attached networks on R2 and R3.

Catalyst Ethernet Switch Setup I Solution

Creating VLANs on a Catalyst 3550 switch requires the VTP domain name to be set up first.

Example 8-13 configures the Catalyst 3550 in the VTP domain, SecCCIE, and mode server. You must enable new VLANs.

Example 8-13 *Enable VTP Domain Name and Server Mode*

```
switch#configuration terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)#vtp domain SecCCIE
switch(config)#vtp mode ?
  client       Set the device to client mode.
  server       Set the device to server mode.
  transparent  Set the device to transparent mode.
switch(config)#vtp mode server
```

Now that the switch is enabled for VTP and VLAN creation, you can create the five VLANs. Example 8-14 configures the switch for the five VLANs in global configuration mode.

Example 8-14 *VLAN Creation*

```
switch#configuration terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#vlan
switch(config)#vlan 2
switch(config-vlan)#name VLAN_A
switch(config-vlan)#vlan 3
switch(config-vlan)#name VLAN_B
switch(config-vlan)#vlan 4
switch(config-vlan)#name VLAN_C
switch(config-vlan)#vlan 5
switch(config-vlan)#name VLAN_D
switch(config-vlan)#vlan 6
switch(config-vlan)#name VLAN_E
switch(config-vlan)#exit
switch(config)#
switch#config terminal
```

After you create all the VLANs, you must disable VLAN creation by configuring the switch as a VTP client only. The central switch in the network (VTP server) creates and deletes VLANs, as required in the future.

Example 8-15 disables local VLAN creation on the Catalyst switch.

Example 8-15 *VTP Client Setup*

```
switch#configuration terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)#vtp domain SecCCIE
switch(config)#vtp mode ?
  client       Set the device to client mode.
  server       Set the device to server mode.
  transparent  Set the device to transparent mode.
switch(config)#vtp mode client
```

The Catalyst 3550 command, **switchport**, configures port assignments for each VLAN. Notice that each Fast Ethernet interface is given a description for completeness, which helps you to troubleshoot in the future.

Example 8-16 configures the VLAN assignment on the Ethernet switch.

Example 8-16 *VLAN Port Assignment*

```
interface FastEthernet0/1
Description connection to R1 Ethernet 0/0
! The following commands assign the VLAN
switchport mode a
 switchport access vlan 2
! The following command assigns the port as an access port, layer 2.
 switchport
 switchport mode access
!
interface FastEthernet0/2
Description connection to R2 Fast Ethernet 0/0
 switchport switchport access vlan 5
 switchport mode access
!
interface FastEthernet0/3
Description connection to R3 Fast Ethernet 0/0
 switchport
 switchport access vlan 5
 switchport mode access
!
interface FastEthernet0/4
Description connection to R4 Ethernet 0/0
 switchport switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/5
Description connection to R5 Fast Ethernet 0/0
 switchport
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/6
Description connection to R5 Ethernet 0/1
 switchport
 switchport access vlan 4
 switchport mode access
!
interface FastEthernet0/7
Description connection to PIX inside
 switchport
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/8
Description connection to PIX outside
 switchport
 switchport access vlan 6
 switchport mode access
```

continues

Example 8-16 *VLAN Port Assignment (Continued)*

```
!Note interfaces 9 and 10 not used nor shown here
interface FastEthernet0/11
Description connection IDS control
 switchport
 switchport access vlan 3
 switchport mode access
interface FastEthernet0/12
Description connection to IDS sniffing
 switchport access vlan 2
 switchport mode access
```

Configure the management interface (VLAN 5) on the Catalyst switch with the following Catalyst command:

set interface sc0 [*vlan*] [*ip_addr* [*netmask* [**broadcast**]]] **interface** *VLAN* **(***tag***)**

The configuration of the interface in VLAN_D (VLAN 5) is defined in Example 8-17.

Example 8-17 *Defining the Management Interface*

```
interface Vlan5
 ip address 144.254.4.3 255.255.255.192.0
```

Example 8-18 confirms the IP address assignment and correct VLAN to all interfaces. Notice the 12 Fast Ethernet ports and two Gigabit interfaces.

Example 8-18 **show interface** *Command on the Ethernet Switch*

```
Switch1#show ip interface brief
Interface              IP-Address      OK?  Method  Status                Protocol
Vlan1                  unassigned      YES  unset   administratively down down
Vlan5                 144.254.4.3      YES  manual  up                    up
FastEthernet0/1        unassigned      YES  unset   up                    up
FastEthernet0/2        unassigned      YES  unset   up                    up
FastEthernet0/3        unassigned      YES  unset   up                    up
FastEthernet0/4        unassigned      YES  unset   up                    up
FastEthernet0/5        unassigned      YES  unset   up                    up
FastEthernet0/6        unassigned      YES  unset   up                    up
FastEthernet0/7        unassigned      YES  unset   up                    up
FastEthernet0/8        unassigned      YES  unset   up                    up
FastEthernet0/9        unassigned      YES  unset   down                  down
FastEthernet0/10       unassigned      YES  unset   down                  down
FastEthernet0/11       unassigned      YES  unset   up                    up
FastEthernet0/12       unassigned      YES  unset   up                    up
GigabitEthernet0/1     unassigned      YES  unset   down                  down
GigabitEthernet0/2     unassigned      YES  unset   down                  down
```

Example 8-18 also confirms connectivity to all the routers, PIX, and IDS server as the line protocol state for those interfaces is UP.

You can ping the management interface (VLAN 5) and the local routers (R2/R3) to ensure connectivity to the rest of the network; you must also enable a default route. The Catalyst switch on VLAN_D is connected to R2 and R3, so you can provide two default gateways, one through R2 and another through R3; in case of network failure, the switch will still be managed either by R2 or R3.

Example 8-19 configures a default gateway point to R2 and R3 Ethernet address and also displays a successful ping request to R2 and R3.

Example 8-19 *Default Gateway Configuration and Ping Request*

```
ip route 0.0.0.0 0.0.0.0 144.254.4.2
ip route 0.0.0.0 0.0.0.0 144.254.4.1 100
```

Example 8-20 confirms the default routes (via the preferred route of 144.254.4.2) with the Catalyst command **show ip route**.

Example 8-20 **show ip route** *on the Catalyst Switch*

```
Switch1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 144.254.4.2 to network 0.0.0.0

     144.254.0.0/24 is subnetted, 1 subnets
C       144.254.5.0 is directly connected, Vlan5
S*   0.0.0.0/0 [1/0] via 144.254.4.2
```

Notice in Example 8-20 that only the active default route is shaded.

The final configuration request is to permit only the VLAN_D users and the assigned loopbacks on R1 through R5. To complete this on a Catalyst switch, you need to enable a vty line access inbound list, which defines what IP addresses are permitted access to the management interface via the vty lines.

Example 8-21 displays the configuration required to ensure that only the loopbacks from R1–R5 are permitted access.

Example 8-21 *Vty Access List Inbound*

```
access-list 5 permit 144.254.151.1
access-list 5 permit 144.254.152.2
access-list 5 permit 144.254.153.3
access-list 5 permit 144.254.154.4
access-list 5 permit 144.254.155.5
! Vlan D users
access-list 5 permit 144.254.4.0 0.0.0.64
!
line vty 0 4
 access-class 5 in
 password cisco
 login
line vty 5 15
 access-class 5 in
 password cisco
 login
```

Example 8-21 configures an access list numbered 5 with the only source permitted IP addresses defined as the loopbacks of routers R1–R5 and VLAN_D.

Example 8-22 confirms the permitted networks and hosts with the Catalyst command **show ip permit**.

Example 8-22 **show ip permit** *Command*

```
C5K> (enable) show ip permit
IP permit list feature enabled.
Permit List        Mask
----------------   ----------------
144.254.4.0        255.255.255.192
144.254.151.1
144.254.152.1
144.254.153.1
144.254.154.1
144.254.155.1
Denied IP Address   Last Accessed Time    Type
-----------------   ------------------    ------
144.254.2.1         09/30/02,15:13:44     Telnet
C5K> (enable)
```

The default mask on the loopback is actually 255.255.255.255, but it is not displayed in Example 8-22.

Example 8-23 displays a successful telnet from R2 to the VLAN 5 management interface or the Catalyst SC0 interface. Notice the requirement to define the source interface as the R2 loopback address.

Example 8-23 *Telnet to 144.254.4.3 or R3 from R2*

```
R2#telnet 144.254.4.3 /source-interface loopback0
Trying 144.254.4.3 ... Open
password: cisco
switch1> quit
[Connection to 144.254.4.3 closed by foreign host]
```

Example 8-24 displays an unsuccessful telnet when the source interface is not defined on the Catalyst 3550.

Example 8-24 *Denied Telnet to Catalyst 3550*

```
R1#telnet 144.254.4.3
Trying 144.254.4.3 ... Open
Access not permitted. Closing connection...
[Connection to 144.254.4.3 closed by foreign host]
R1#
```

Catalyst Ethernet Switch Setup II (6 Points)

Configure the following security features on the Catalyst 3550:

- Ensure that all of your interfaces are secure and that, if a secure breach occurs, the network administrator should take the strictest action possible.
- Set the Ethernet ports 0/1–8 to forward data immediately after a device is plugged in or activated.
- Set all interfaces such that unnecessary broadcast traffic will be suppressed once the switch has anything over 50 percent of total traffic.

Catalyst Ethernet Switch Setup II Solution

The Catalyst 3550 switch has a feature known as port security. If a MAC address is changed, for instance, the interface can be set to take action such as shutting down the interface. Example 8-25 displays the command to enable port security.

Example 8-25 *Enabling Port Security*

```
Switch(config)#interface fastethernet0/1
switch(config-if)# switchport port-security
```

The following is the IOS command to take immediate action once a breach occurs:

```
Router(config-if)# switchport port-security violation {protect ¦ restrict ¦ shutdown}
```

Example 8-26 configures the Catalyst 3550 switch for port security on all enabled interfaces and sets the action as shutdown if a violation does occur. Notice the use of the **range** command to simplify the confirmation tasks.

Example 8-26 *Switch Port Security*

```
 switch#config terminal
 switch(config)#interface range FastEthernet0/1 - 12
switch(config-if-range)# switchport port-security
switch(config-if-range)# switchport port-security violation shutdown
```

Finally, the last task required is to suppress broadcast traffic once traffic exceeds 50 percent. Once again we will use the **range** command to set the interfaces to stop sending broadcast traffic once a limit of 50 percent (broadcast traffic, that is) has been reached.

Example 8-27 configures the Catalyst 3550 for broadcast traffic to 50 percent.

Example 8-27 *Broadcast Suppression at 50 Percent*

```
switch#config terminal
switch(config)#interface range FastEthernet0/1 - 12
switch(config-if-range)# storm-control broadcast level 50.00
```

IP Host Lookup and Disable DNS (1 Point)

Configure local IP host addresses on each router (R1 through R5) so that when an EXEC or privileged user types the router name (R1, R2, R3, R4, or R5), the user can ping or telnet without having to type the full IP address.

Do not configure a DNS server on any router, and disable DNS lookup entries so that incorrect commands on the EXEC or PRIV prompt are not sent to any DNS server. (Hint: This saves you time as well; the IOS command **no ip domain-lookup** disables DNS queries.)

IP Host Lookup and Disable DNS Solution

To configure local host lookups, use the IOS command **ip host** *name ip address*.

Example 8-28 configures Router R2 for IP host lookup for all routers, including itself.

Example 8-28 **ip host** *Command on R2*

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip host r5 144.254.155.1
R2(config)#ip host r4 144.254.154.1
R2(config)#ip host r3 144.254.153.1
R2(config)#ip host r2 144.254.152.1
R2(config)#ip host r1 144.254.151.1
```

Example 8-29 disables DNS lookups for the remote DNS server.

Example 8-29 **no ip domain-lookup** *on R2*

```
R2(config)#no ip domain-lookup
```

The same commands are installed on R1, R3, R4, and R5. See the full working configuration at the end of this chapter.

This completes the physical setup for this sample lab. You can now start configuring IP network routing on the PIX followed by the routers.

PIX Configuration (6 Points)

PIX1 is connected to R1 by the inside interface, and the outside interface is connected to a managed router through a 10-Mbps connection on the outside interface. Use the IP address 144.254.1.2/30 for the inside interface; the outside interface should be set to 9.1.1.1/24.

PIX1 should use RIPv2 to communicate to R1 and supply a default route to R1. (Note that with PIX 6.3 in the current exam, OSPF may be required also. Ensure that you have the skill set for OSPF as well.)

Ensure that all RIP updates are authenticated using MD5.

You can configure a static route on the PIX to network 144.254.0.0/16 through R1 and the Internet through 9.1.1.2. Note that the PIX cannot handle more than one default route.

All inside hosts should be able to ping, but only R1 is permitted to telnet to the PIX.

Configure NAT on the PIX so that inside users can reach the Internet.

PIX Configuration Solution

Example 8-30 configures the inside and outside IP address on PIX1. The host name is set to PIX1.

Example 8-30 *Inside/Outside IP Address Configuration*

```
pixfirewall# config terminal
pixfirewall(config)# hostname PIX1
! Set the name and security level for the PIX interfaces
PIX1(config)# nameif ethernet0 outside security0
PIX1(config)# nameif ethernet1 inside security100
! enable the interfaces and set the speed
PIX1(config)# interface ethernet0 auto
PIX1(config)# interface ethernet1 auto
! configure the interface IP address
PIX1(config)# ip address outside 9.1.1.1 255.255.255.0
PIX1(config)# ip address inside 144.254.1.2 255.255.255.252
```

Example 8-31 confirms the IP address configuration with the PIX command **show interface** (note that version 6.3 displays a little differently).

Example 8-31 **show interface** *Command on the PIX*

```
PIX1# show interface
interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82558 ethernet, address is 0090.2742.ff83
  IP address 9.1.1.1, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit full duplex
        166 packets input, 52434 bytes, 0 no buffer
        Received 80 broadcasts, 0 runs, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        83 packets output, 5872 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
interface ethernet1 "inside" is up, line protocol is up
  Hardware is i82558 ethernet, address is 0090.2743.01ab
  IP address 144.254.1.2, subnet mask 255.255.255.252
  MTU 1500 bytes, BW 10000 Kbit full duplex
        34046 packets input, 2265846 bytes, 0 no buffer
        Received 33958 broadcasts, 0 runs, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        92 packets output, 6508 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
PIX1#
```

To enable RIPv2 on the PIX, enter the following command on the PIX:

```
rip inside passive version 2 authentication md5 secret-key key-id
```

Example 8-32 configures the PIX Firewall for RIPv2 and MD5 authentication. Two static routes are configured, also pointing to network 144.254.0.0/8 and the Internet.

Example 8-32 *RIP Version 2 Configuration on the PIX*

```
rip inside passive version 2 authentication md5 ccie 1
rip inside default version 2 authentication md5 ccie 1
route outside 0.0.0.0 0.0.0.0 9.1.1.2
route inside 144.254.0.0 255.255.0.0 144.254.1.1
```

The MD5 password is set to ccie. The second configuration line supplies a default RIP route to R1. The final two commands enable static routes for the internal network and the Internet through 144.254.1.1 and 9.1.1.2, respectively.

You must now configure Router R1 for RIP authentication.

Example 8-33 configures a key chain named cisco, and the MD5 password is ccie. RIP is enabled on the Ethernet0/0 interface connecting to the inside interface on the PIX Firewall.

Example 8-33 *Key Chain Configuration on R1*

```
Hostname R1
key chain cisco
 key 1
  key-string ccie
interface Ethernet0/0
 ip rip authentication mode md5
 ip rip authentication key-chain cisco
```

To enable inside hosts to ping and telnet to the PIX, allow ICMP and Telnet to the PIX on the inside interface only. By default, the PIX will not permit ICMP and Telnet to any interface.

Example 8-34 permits ICMP and Telnet from the inside hosts.

Example 8-34 *Allowing ICMP and Telnet on the PIX*

```
icmp permit any echo inside
```

Example 8-35 permits R1 to telnet to the PIX with the **telnet** command.

Example 8-35 **telnet** *Command on the PIX for R1 Only*

```
telnet  144.254.1.1 255.255.255.255 inside
```

Example 8-36 displays the Telnet request from R1 to the PIX Firewall; the enable password has not been set, so you simply press Return.

Example 8-36 *Telnet to 144.254.1.2 from R1*

```
R1#telnet 144.254.1.2
Trying 144.254.1.2 ... Open

PIX passwd: cisco
Welcome to the PIX firewall

Copyright  1996-2000 by Cisco Systems, Inc.

                Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
 of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
 (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

                Cisco Systems, Inc.
                170 West Tasman Drive
                San Jose, California 95134-1706

Type help or '?' for a list of available commands.
PIX1> enable
Password:
PIX1#
```

The **telnet** command is used on the PIX to enable which hosts are permitted to telnet to the PIX. By default, inside hosts do not require IPSec to remotely manage the PIX, but outside hosts do. In earlier versions of PIX code, it was possible to telnet only from an inside interface. By default, the Telnet password is set to cisco. You may also, of course, use SSH rather than Telnet.

All outside hosts (hosts that are untrusted, such as Internet devices) need to be configured for IPSec to the PIX to enter the management console by Telnet. Telnet through IPSec is only required on the outside interface. In a real-life network, however, SSH should be used on the outside interface instead.

To enable NAT on all inside hosts on the PIX, the following command is first required on the PIX:

```
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

The **nat** command associates a network with a pool of global IP addresses. The following is the full PIX OS syntax:

```
nat [(if_name)] nat_id local_ip [netmask [max_conns [em_limit]]] [norandomseq]
nat [(if_name)] 0 access-list acl_name
nat [(if_name)] 0 local_ip [netmask [max_conns [em_limit]]] [norandomseq]
no nat [[(if_name)] nat_id local_ip [netmask [max_conns [em_limit]]]]
    [norandomseq]
no nat [(if_name)] 0 access-list acl_name
```

Table 8-3 summarizes the available options with the **nat** command.

Table 8-3 **nat** *Command Syntax Description*

Syntax	Description
if_name	The internal network interface name. If the interface is associated with an access list, *if_name* is the higher-security-level interface name.
nat_id	All **nat** command statements with the same *nat_id* are in the same NAT group. Use *nat_id* in the global command statement; for example: **nat (inside) 1 0 0** **global (outside) 1 10.1.1.0 10.1.1.254 netmask 255.255.255.224** This example associates the **nat** command with the global command by *nat_id*. *nat_id* is an arbitrary positive number between 0 and 2 billion. This number can be the same as the ID used with the **outbound** and **apply** commands. Specify **0** with IP addresses and netmasks to identify internal networks that desire only outbound identity address translation. Specify **0** with the **access-list** option to specify traffic that should be exempted from NAT.
access-list	Associates an **access-list** command statement with the **nat 0** command.
local_ip	Internal network IP address to be translated. You can use **0.0.0.0** to allow all hosts to start outbound connections. The **0.0.0.0** *local_ip* can be abbreviated as **0**.
netmask	Network mask for *local_ip*. You can use **0.0.0.0** to allow all outbound connections to translate with IP addresses from the global pool.
max_conns	The maximum TCP connections permitted from the interface you specify.
em_limit	The embryonic connection limit. The default is **0**, which means unlimited connections. Set it lower for slower systems and higher for faster systems.
norandomseq	Do not randomize the TCP packet's sequence number. Use this option only if another inline firewall is also randomizing sequence numbers and the result is scrambling the data. Use of this option opens a security hole in the PIX Firewall.

See the following Cisco.com page for more details on how NAT/PAT can be configured on a Cisco PIX:

www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/index.htm

More PIX tasks appear later in this CCIE Security self-study lab.

IGP Routing (18 Points)

After this section is completed, all routers must have full IP connectivity between every routing domain, including the ISDN backup interfaces when operational.

Basic RIP Configuration (6 of 18 Points)

Configure RIP on Router R1 and the PIX only:

- Authenticate RIP between R1 and the PIX.
- VLAN_A resides in a RIPv2 domain only.
- Redistribute the RIP routes into the IGP network.
- Make sure that you can see distributed RIP routes throughout your topology and that the OSPF cost metric is set to 1000 for all RIP routes redistributed from R1.
- Use a route map to set the cost.

RIP Configuration Solution

Example 8-37 enables RIPv2 only on R1 and redistributes the EIGRP routes into RIP.

Example 8-37 *Enable RIP on R1*

```
router rip
 version 2
 redistribute eigrp 333 metric 5
 passive-interface Serial0/1
 network 144.254.0.0
 no auto-summary
```

R1 is configured for RIPv2 only; notice that only Serial0/1 (link to R4 through EIGRP) is configured in a passive state where no RIP route will be sent to R4, as this link resides in EIGRP only.

Example 8-38 configures MD5 authentication between R1 and the PIX Firewall.

Example 8-38 *MD5 RIP Authentication on R1*

```
interface Ethernet0/0
ip rip authentication mode md5
ip rip authentication key-chain cisco
```

Example 8-39 confirms RIP connectivity (**show ip route rip** command) between the PIX and R1. Notice the default route supplied by the PIX.

Example 8-39 **show ip route rip** *on R1*

```
R1#show ip route rip
R*   0.0.0.0/0 [120/1] via 144.254.1.2, 00:00:10, Ethernet0/0
R1#
```

Example 8-39 displays a default RIP route via 144.254.1.2 on the PIX inside interface.

EIGRP Configuration (5 of 18 Points)

Configure EIGRP between R1 and R4 Frame Relay connections only:

- Configure EIGRP in AS 333.
- Ensure that EIGRP is authenticated across the Frame Relay connections.
- Redistribute the EIGRP routes into the OSPF domain with a varying OSPF cost metric.
- Configure R1 with the following additional loopback interfaces and corresponding IP addresses:
  - Loopback 1—131.108.1.1/24
  - Loopback 2—131.108.2.1/24
  - Loopback 3—131.108.3.1/24

Configure the above loopbacks to be in EIGRP domain 333. Ensure that all routers in your network can ping these loopbacks.

EIGRP Configuration Solution

EIGRP is to be enabled on the link between R1 and R4 only, so you must make all other interfaces passive. The real problem here, though, is the fact that you are not permitted to use the Frame Relay **broadcast** keyword when mapping IP across the Frame Relay cloud. EIGRP sends updates as broadcasts, so even if you enable EIGRP on the serial link, no updates will be sent, because

broadcasts have been disabled. Remember that by default a Cisco router interface drops all broadcast frames. To enable EIGRP to maintain a neighbor relationship in this scenario, you can tunnel EIGRP over an IP GRE tunnel.

Example 8-40 configures R1 for EIGRP and an IP GRE tunnel to obtain EIGRP neighbors to R4.

Example 8-40 *Enable EIGRP and Tunnel Interface on R1*

```
Hostname R1

interface Tunnel0
 ip unnumbered Serial0/1
 tunnel source Serial0/1
 tunnel destination 144.254.2.2
router eigrp 333
  passive-interface Ethernet0/0
  network 144.254.0.0
  network 131.108.0.0
  eigrp log-neighbor-changes
  no auto-summary
```

Example 8-41 configures R4 for EIGRP and the IP GRE tunnel to obtain EIGRP neighbors to R1.

Example 8-41 *Enable EIGRP and Tunnel Interface on R4*

```
Hostname R4
interface Tunnel0
 ip unnumbered Serial0/1
 tunnel source Serial0/1
 tunnel destination 144.254.2.1
router eigrp 333
passive-interface Ethernet0/0
 passive-interface Serial0/0
 passive-interface Loopback0
 network 144.254.0.0
 network 131.108.0.0
 eigrp log-neighbor-changes
```

Example 8-42 confirms the EIGRP relationship over the newly created tunnel interface.

Example 8-42 **show ip eigrp neighbor** *Command on R1 and R4*

```
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 333
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q  Seq Type
                                        (sec)         (ms)       Cnt Num
0   144.254.2.2             Tu0           12 1w6d       15  5000  0  155
```

Example 8-42 **show ip eigrp neighbor** *Command on R1 and R4 (Continued)*

```
R1#

R4#show ip eigrp neighbors
IP-EIGRP neighbors for process 333
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q  Seq Type
                                        (sec)         (ms)       Cnt Num
0   144.254.2.1             Tu0           13 1w6d       62  5000  0  165
R4#
```

To enable authentication of EIGRP packets, use the following **ip authentication key-chain eigrp** interface configuration command:

ip authentication key-chain eigrp *as-number key-chain*

To specify the type of authentication used in EIGRP packets, use the following **ip authentication mode eigrp** interface configuration command:

ip authentication mode eigrp *as-number* **md5**

Example 8-43 configures R1 with a new key chain and EIGRP authentication. First, the key chain is defined, and then the authentication is applied to the interface tunnel 0, not the serial link, because the EIGRP neighbors are established over the tunnel interface and not the nonbroadcast serial interface.

Example 8-43 *EIGRP Authentication on R1*

```
R1(config)#key chain  ?
  WORD  Key-chain name
R1(config)#key ?
  chain       Key-chain management
  config-key  Set a private configuration key
R1(config)#key chain eigrp
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string ccie
R1(config-keychain-key)#exit
R1(config-keychain)#interface tunnel0
R1(config-if)#ip authentication key-chain eigrp 333 eigrp
R1(config-if)# ip authentication key-chain ?
  eigrp  Enhanced Interior Gateway Routing Protocol (EIGRP)

R1(config-if)# ip authentication key-chain eigrp ?
  <1-65535>  Autonomous system number

R1(config-if)# ip authentication key-chain eigrp 333 ?
  LINE  name of key-chain
```

continues

Example 8-43 *EIGRP Authentication on R1 (Continued)*

```
R1(config-if)# ip authentication key-chain eigrp 333 eigrp ?
LINE    <cr>

R1(config-if)# ip authentication key-chain eigrp 333 eigrp
```

The secret key is set to ccie.

Example 8-44 configures R4 for the same parameters.

Example 8-44 *R4 EIGRP Authentication*

```
R4(config)#key chain eigrp
R4(config-keychain)# key 1
R4(config-keychain-key)#  key-string ccie
R4(config-keychain-key)#interface Tunnel0
R4(config-if)# ip unnumbered Serial0/1
R4(config-if)# ip authentication mode eigrp 333 md5
R4(config-if)# ip authentication key-chain eigrp 333 eigrp
```

Example 8-45 confirms EIGRP neighbor relations after the changes.

Example 8-45 **show ip eigrp neighbors** *Command on R1*

```
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 333
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q  Seq Type
                                        (sec)         (ms)       Cnt Num
0   144.254.2.2             Tu0           10 00:00:36  687  5000  0  161
R1#
```

The final section requires three additional loopbacks configured on R1 and redistribution into OSPF. Example 8-46 enables the three additional loopbacks on R1.

Example 8-46 *Loopback Addition on R1*

```
interface Loopback1
 ip address 131.108.1.1 255.255.255.0
!
interface Loopback2
 ip address 131.108.2.1 255.255.255.0
!
interface Loopback3
 ip address 131.108.3.1 255.255.255.0
router eigrp 333
  network 131.108.0.0
```

Notice in Example 8-46 that the networks (the three loopbacks) are placed into EIGRP AS 333.

Example 8-47 enables R4 to redistribute the EIGRP routes into OSPF with a metric type 1, or varying metric type.

Example 8-47 *R4 Redistribution into OSPF*

```
router ospf 1
 redistribute eigrp 333 metric 100 metric-type 1 subnets
```

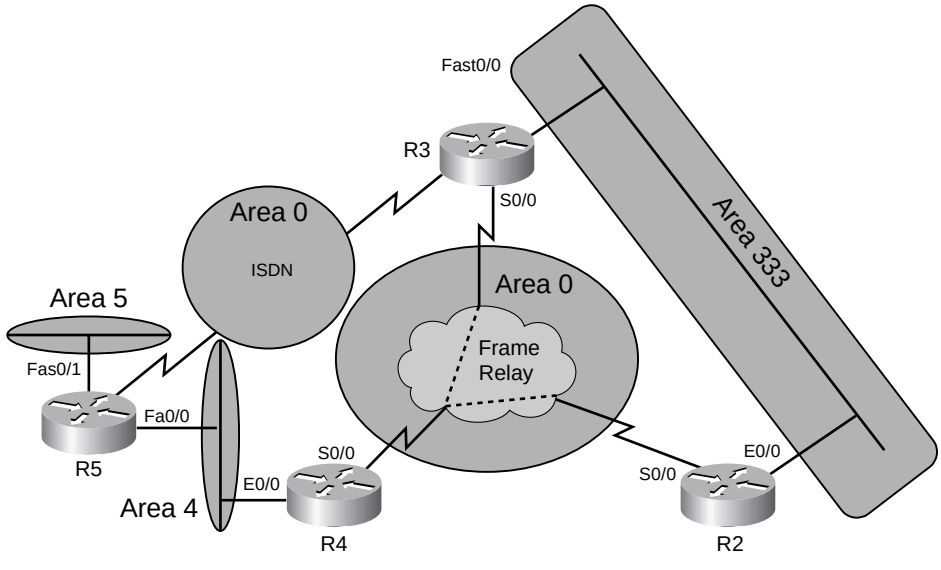
R4 is configured to redistribute the EIGRP networks with a cost metric of 100, metric type E1, and the keyword **subnets** allows the subnetted routes (131.108.0.0 and 144.254.0.0) to be injected into the OSPF domain.

You will confirm IP routing connectivity after all IGP routing protocols are configured.

OSPF Configuration (7 of 18 Points)

Configure OSPF, as described in Figure 8-3. Do not create any nonspecified OSPF areas. There are two OSPF backbones.

Figure 8-3 *OSPF Area Assignments*



For loopback interfaces, place the interfaces in the appropriate OSPF area already assigned to the router. For Example, R4 resides in areas 0 and 4; place R4 Loopback 0 in area 0, and so forth.

When applying an inverse mask, apply the following on all interfaces configured in OSPF, 0.0.0.0:

- Configure the OSPF backbone over the Frame Relay network between the three Routers R2, R3, and R4.
- Do not change the network type on any Frame Relay interface.
- The ISDN link between R3 and R5 resides in area 0.0.0.0.
- The Ethernet link between R4 and R5 is in area 4.
- The Ethernet segment named VLAN_C will reside in area 5.
- Ensure that all OSPF routes are redistributed and reachable in the RIP and EIGRP domains.
- Make sure that the OSPF backbone in the Frame-Relay cloud is authenticated using the strongest authentication possible.
- Ensure that R2 will never be the DR on all segments.
- Ensure that the ISDN link is active only if OSPF neighbors are lost between R3 and R4. Do not use the **backup** command or **dialer-watch** commands to accomplish this task. Only IP traffic is permitted across the ISDN link. See the "Basic ISDN Configuration" section before completing the ISDN setup.
- Ensure that R4 is the DR in the OSPF Frame Relay backbone network.
- Ensure that the router ID of all OSPF-enabled routers is the loopback address. Do not assume that this will be the case, but make sure that no matter what IP address is assigned, the router ID is set to Loopback 0.
- Advertise the loopbacks as 24-bit subnets; do not use the command **redistributed connected** to accomplish this task.
- Do not create any additional areas.
- Set the dead interval between the R2 and R4 link to 100 seconds. Do not use the **ip ospf dead-interval** command to accomplish this task.
- Set the Hello interval on the R2 Ethernet segment to 20 seconds.

The Ethernet connection between R5 and R4 has been experiencing packet loss. Configure the OSPF process such that the neighbor relationship between R4 and R5 will remain established if at least one OSPF Hello packet is received every 60 seconds.

OSPF security is a concern on VLAN B. Configure the strongest form of OSPF security on VLAN B so that someone with a packet tracer cannot read OSPF packet exchanges between R4 and R5.

OSPF Configuration Solution

The first challenge of any OSPF design is the need for all areas to be connected to area 0 or the backbone. In Figure 8-3, there are two backbones, but the ISDN link is used only if R3 loses OSPF neighbor connectivity to R5. Area 5 is not connected to the backbone under normal OSPF operation. (In other words, you need a virtual link between area 5 and area 0.)

Start by enabling OSPF on Router R2 followed by R3, R4, and R5.

Example 8-48 configures OSPF on R2.

Example 8-48 *Enabling OSPF on R2*

```
Hostname R2
interface Loopback0
 ip address 144.254.152.1 255.255.255.0
 ip ospf network point-to-point
interface Ethernet0/0
 ip address 144.254.4.2 255.255.255.192
 ip ospf priority 0
ip ospf hello-interval 20
interface Serial0/0
 ip address 144.254.3.2 255.255.255.240
ip ospf message-digest-key 1 md5 cisco
ip ospf authentication message-digest
ip ospf hello-interval 25
! Four times this value give 100 sec
 ip ospf priority 0
router ospf 1
 router-id 144.254.152.1
 log-adjacency-changes
 area 0 authentication message-digest
 network 144.254.3.2 0.0.0.0 area 0
 network 144.254.4.2 0.0.0.0 area 333
 network 144.254.152.1 0.0.0.0 area 0
```

As per requirements in the question, the network mask applied to all interfaces in OSPF is 0.0.0.0, or exact match, which means you must also supply the actual IP address. The loopback interface is configured for point-to-point so the interface is advertised as a /24 subnet and not a stub host (/32) by default. R2 serial link to R4 is configured for MD5 authentication, and the OSPF priority is set to 0 so that R4 is the designated router. MD5 is the strongest authentication mechanism available to OSPF. R2 priority on Ethernet 0/0 is also set to 0 so that R2 will never be the DR on

any LAN or WAN segment. R2 router ID is manually set to the loopback interface. The dead interval needs to be set to 100 seconds, but the use of the **ip ospf dead-interval** command is not allowed. Because, by default, the dead interval is four times the Hello interval, set the Hello interval to 25 seconds. This will make the dead interval 100 seconds. The command **ip ospf hello-interval** accomplishes this. In any exam, you should always think outside the square for questions such as this one, if you are familiar with how each routing protocol is designed.

Also, R4 and R3 require the same command, as R2, R3, and R4 are part of the same nonbroadcast network. All OSPF routers require the same change of the Hello interval to 25 seconds. The same applies to OSPF authentication, as R2, R3, and R4 reside in area 0, and OSPF requires all routers in the same area configured for authentication to be enabled with the secret key. (In this case, MD5 encrypts or hashes the password ccie.) Similarly, you are asked to change the Hello interface on the R2 segment to 20 seconds; this requires R3 to be changed, as well, so that OSPF neighbor adjacency is maintained. OSPF will not become adjacent if the Hello intervals are not the same.

Example 8-49 enables OSPF on Router R3.

Example 8-49 *9R3 OSPF Configuration*

```
Hostname R3
interface Loopback0
 ip address 144.254.153.1 255.255.255.0
 ip ospf network point-to-point
!
interface fastethernet0/0
ip ospf hello-interval 20
interface Serial0/0
 ip address 144.254.3.3 255.255.255.240
ip ospf message-digest-key 1 md5 cisco
ip ospf authentication message-digest
ip ospf hello-interval 25
 ip ospf priority 0
 router ospf 1
 router-id 144.254.153.1
 area 0 authentication message-digest
 network 144.254.3.3 0.0.0.0 area 0
 network 144.254.4.1 0.0.0.0 area 333
network 144.254.7.1 0.0.0.0 area 0
 network 144.254.153.1 0.0.0.0 area 0
 log-adjacency-changes
```

The OSPF configuration for the ISDN BRI is covered in the next ISDN section. R3 requires the loopback interface advertised as /24 and the manual router ID set up to the Loopback 0 interface.

Example 8-50 configures OSPF on R4.

Example 8-50 *R4 OSPF Configuration*

```
Hostname R4
!
interface Loopback0
 ip address 144.254.154.1 255.255.255.0
 ip ospf network point-to-point
!
!
interface Ethernet 0/0
ip ospf hello-interval 60
interface Serial0/0
 ip address 144.254.3.1 255.255.255.240
 encapsulation frame-relay
 ip ospf message-digest-key 1 md5 cisco
ip ospf authentication message-digest
 ip ospf hello-interval 25
 ip ospf priority 255
!
!
router eigrp 333
 redistribute ospf 1 metric 1544 20000 255 1 1500

router ospf 1
 router-id 144.254.154.1
 log-adjacency-changes
area 0 authentication message-digest
area 4 virtual-link 144.254.155.1 authentication message-digest
area 4 virtual-link 144.254.155.1 message-digest-key 1 md5 cisco
 redistribute eigrp 333 metric 100 metric-type 1 subnets
 network 144.254.3.1 0.0.0.0 area 0
 network 144.254.5.1 0.0.0.0 area 4
 network 144.254.154.1 0.0.0.0 area 0
 neighbor 144.254.3.3
 neighbor 144.254.3.2
```

Example 8-50 displays the fact that R4 is the DR to R2/R3, and because you are not permitted to change the network type in the core Frame Relay backbone network, you must configure OSPF for neighbors using the **neighbor** command. R4 also redistributes EIGRP routes into OSPF. R4 Ethernet0/0 segment has an OSPF Hello interval set to 60 seconds so that only one Hello packet every minute is sufficient to maintain OSPF adjacencies to R5, as requested by the question. The virtual link between R4 and R5 is required so that area 5 is visible to the backbone when the ISDN link is not in operation.

Example 8-51 displays the OSPF configuration on R5.

Example 8-51 *SPF Configuration on R5*

```
Hostname R5
interface Loopback0
 ip address 144.254.155.1 255.255.255.0
 ip ospf network point-to-point
!
interface FastEthernet0/0
 ip ospf hello-interval 60
ip ospf authentication-message-digest
ip ospf message-digest-key 1 md5 cisco

!
!
interface FastEthernet0/1
 ip address 144.254.6.1 255.255.255.248
!
!
router ospf 1
 router-id 144.254.155.1
area 0 authentication message-digest
area 4 virtual-link 144.254.154.1 authentication message-digest
area 4 virtual-link 144.254.154.1 message-digest-key 1 md5 cisco
network 144.254.5.2 0.0.0.0 area 4
 network 144.254.6.1 0.0.0.0 area 5
 network 144.254.7.2 0.0.0.0 area 0
 network 144.254.155.1 0.0.0.0 area 4
```

R5 is configured for a virtual link over transit area 4. Notice that good OSPF design always sets the router ID so that virtual links can be configured by network administrators, knowing that a failure of any physical interface will not bring down a virtual link. Area 0 on R5 is configured for authentication because the core Frame Relay network between R2, R3, and R4 in area 0 is configured for authentication; in particular, R3 will not become adjacent because R3 is part of the core backbone where MD5 authentication is configured. IP redistribution is used to route between different routing domains.

Now that all IGP routing protocols are completed and redistribution is enabled, ensure that there is IP connectivity between all routers by viewing the IP routing tables and pinging all loopback interfaces from Router R4.

Example 8-52 displays the IP routing table on R4.

Example 8-52 **show ip route** *on R4*

```
R4#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 144.254.2.1 to network 0.0.0.0

     144.254.0.0/16 is variably subnetted, 12 subnets, 5 masks
O IA    144.254.6.0/29 [110/11] via 144.254.5.2, 00:04:11, Ethernet0/0
O       144.254.7.0/30 [110/1572] via 144.254.5.2, 00:04:42, Ethernet0/0
O IA    144.254.4.0/26 [110/49] via 144.254.3.3, 00:04:11, Serial0/0
C       144.254.5.0/27 is directly connected, Ethernet0/0
C       144.254.2.0/30 is directly connected, Serial0/1
C       144.254.3.0/29 is directly connected, Serial0/0
D       144.254.1.0/30 [90/297270016] via 144.254.2.1, 00:49:09, Tunnel0
C       144.254.154.0/24 is directly connected, Loopback0
O       144.254.155.0/24 [110/11] via 144.254.5.2, 00:04:13, Ethernet0/0
O       144.254.152.0/24 [110/49] via 144.254.3.2, 00:04:43, Serial0/0
O       144.254.153.0/24 [110/49] via 144.254.3.3, 00:04:43, Serial0/0
D       144.254.151.0/24 [90/297372416] via 144.254.2.1, 00:49:09, Tunnel0
     131.108.0.0/24 is subnetted, 3 subnets
D       131.108.3.0 [90/297372416] via 144.254.2.1, 00:49:09, Tunnel0
D       131.108.2.0 [90/297372416] via 144.254.2.1, 00:49:09, Tunnel0
D       131.108.1.0 [90/297372416] via 144.254.2.1, 00:49:09, Tunnel0
D*EX 0.0.0.0/0 [170/302364416] via 144.254.2.1, 00:49:09, Tunnel0
R4#
```

R4 has OSPF, EIGRP, and connected routes to all parts of the network. By pinging all the loopback interfaces from any given router, you can be sure that IP routing is configured correctly. Notice that the EIGRP routes from R1 are learned over the tunnel interface. A default router is advertised by the PIX to the World Wide Web.

Example 8-53 pings all the remote loopbacks from R4 to ensure IP connectivity.

Example 8-53 *Ping Loopbacks from R4*

```
R4#ping 144.254.151.1

Type escape sequence to abort.
```

continues

Example 8-53 *Ping Loopbacks from R4 (Continued)*

```
Sending 5, 100-byte ICMP Echos to 144.254.151.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/8 ms
R4#ping 144.254.152.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.152.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
R4#ping 144.254.153.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.153.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
R4#ping 144.254.154.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.154.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R4#ping 144.254.155.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.155.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R4#
```

Example 8-54 pings all the remote loopbacks from R1 to ensure IP connectivity.

Example 8-54 *Ping Loopbacks from R1*

```
R1#ping 144.254.151.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.151.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1#ping 144.254.152.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.152.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/11/12 ms
R1#ping 144.254.153.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.153.1, timeout is 2 seconds:
```

Example 8-54 *Ping Loopbacks from R1 (Continued)*

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/10/12 ms
R1#ping 144.254.154.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.154.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/8 ms
R1#ping 144.254.155.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.155.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/8 ms
R1#
```

Now, test IP connectivity from R2, but use host names you configured earlier. Example 8-55 pings the remote and local loopbacks from R2.

Example 8-55 *R2 Ping Test Connectivity*

```
R2#ping r1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.151.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/10/12 ms
R2#ping r2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.152.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R2#ping r3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.153.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/9/12 ms
R2#ping r4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.154.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
R2#ping r5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.155.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
R2#
```

Example 8-56 confirms OSPF neighbor adjacencies between R4 and R2 and R4 and R5.

Example 8-56 **show ip ospf neighbor** *on R4*

```
R4#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
144.254.153.1     0   FULL/DROTHER    00:01:17    144.254.3.3     Serial0/0
144.254.152.1     0   FULL/DROTHER    00:01:22    144.254.3.2     Serial0/0
144.254.155.1     1   FULL/DR         00:03:47    144.254.5.2     Ethernet0/0
R4#
```

This completes the IP routing requirement. In a typical CCIE Security lab, you are expected to have this sort of network active in a short period (less than 4 hours is ideal). At this stage, no security technologies have been extensively covered except for routing algorithm–based authentication with RIP, OSPF, and EIGRP. The remainder of this CCIE Security self-study lab concentrates on security topics and some miscellaneous IOS features, such as DHCP and ISDN.

Basic ISDN Configuration (6 Points)

The basic ISDN configuration task information is as follows:

- ISDN switch information:
  - ISDN switch type: basic-5ess
- ISDN numbering:
  - R3: 7775010
  - R5: 7775020
- SPIDs are not required.

Configure the ISDN interfaces on R3 and R5 as follows:

- Ensure that only R3 can call R5, and R3 should never challenge R5 for a username or password pairing.
- ISDN switch type is basic-5ess. Do not configure any SPIDs.
- If traffic exceeds more than 65 percent, the second ISDN B channel will be used. (Hint: Enable **ppp multilink**.)
- If there is an error rate of 20 percent or higher, the interface on R3 should show only a DOWN status when the command **show interface bri0/0** is displayed. (Hint: Use the **ppp quality** command.)
- R5 cannot call R3 under any circumstance. If R3 OSPF adjacency goes down, make sure that the ISDN link is operational and that all OSPF routing is accomplished through the ISDN link. Use **ospf demand circuit** and not **static** or **dialer-watch** statements.

- Use PPP encapsulation and the strongest authentication available.
- When the ISDN is active, all routers must be able to ping and telnet the local ISDN interfaces on R3 and R5.
- Ensure that OSPF neighbors are not keeping the ISDN call active unless the neighbor over the Frame-Relay link is not adjacent. (Hint: Apply the **no peer neighbor-route** IOS command on R3 and R5.)
- Use the command **show isdn status** to confirm when any ISDN calls are activated or deactivated.

Basic ISDN Configuration Solution

R3 and R5 are connected to an ISDN switch. All the ISDN parameters are provided so that you can configure them easily. An OSPF demand circuit is enabled between R3 and R5.

Example 8-57 configures R3 for ISDN connectivity to R5.

Example 8-57 *ISDN Configuration for R3*

```
Hostname R3
!
username R5 password 0 cisco
!
isdn switch-type basic-5ess
interface BRI0/0
 description 7775010
 ip address 144.254.7.1 255.255.255.252
 encapsulation ppp
ip ospf message-digest-key 1 md5 cisco
ip ospf authentication message-digest
ip ospf demand-circuit
ip ospf network point-to-point
 ppp quality 80
 dialer map ip 144.254.7.2 name R5 broadcast 7775020
 dialer load-threshold 165 either
no peer neighbor-route
 dialer-group 1
 isdn switch-type basic-5ess
ppp authentication chap callin
ppp multilink
!Global command below permits IP traffic only
dialer-list 1 protocol ip permit
```

In Example 8-57, R3 is configured for OSPF demand circuit. Only when OSPF is adjacent to R3 and R4 is down, will R3 make an outgoing ISDN call to R5. IP data is permitted to cross the ISDN

link via the **dialer** group command. OSPF authentication is enabled because area 0 requires all interfaces configured for authentication to have authentication configured and enabled with the correct secret key. PPP CHAP authentication is used because CHAP encrypts all passwords with MD5. The **ppp quality** command ensures that if error rates on the interface are reaching 20 percent (80 percent or less is good traffic), the interface will be brought down. This is a specific IOS command.

Example 8-58 enables R5 to receive the call.

Example 8-58 *R5 ISDN Configuration*

```
hostname R5
!
username R3 password 0 cisco
!
interface BRI0/0
 description 7775020
 ip address 144.254.7.2 255.255.255.252
 encapsulation ppp
 ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
 dialer load-threshold 165 either

 dialer map ip 144.254.7.1 name R3 broadcast
 ip ospf network point-to-point
dialer-group 1
 isdn switch-type basic-5ess
 no peer neighbor-route
 ppp authentication chap callin
ppp multilink
!
dialer-list 1 protocol ip permit
```

R5 cannot make an outgoing call because the **dial map** statement contains no valid ISDN number. The **ppp multilink** command is enabled so that two B channels can be active when R3 outbound traffic reaches 65 percent or more. The **ppp authentication chap callin** command checks only for R3 username and password, and ensures that R3 does not challenge R5 for a username or password. Notice that R5 is not configured for OSPF demand circuit because R3 makes the outgoing call, and, to obtain OSPF adjacency, only the remote edge router needs to have demand circuit enabled.

Example 8-59 displays the OSPF exchange when the Frame-Relay link is not active or when the OSPF dead interval expires between R3 and R4.

Example 8-59 *ISDN Call on R3*

```
R3#show debug
Dial on demand:
  Dial on demand events debugging is on
IP routing:
  OSPF adjacency events debugging is on
  OSPF events debugging is on
3w6d: OSPF: 144.254.153.1 address 144.254.3.3 on Serial0/0 is dead, state DOWN
3w6d: OSPF: Neighbor change Event on interface Serial0/0
3w6d: OSPF: DR/BDR election on Serial0/0
3w6d: OSPF: Elect BDR 0.0.0.0
3w6d: OSPF: Elect DR 144.254.154.1
3w6d:        DR: 144.254.154.1 (Id)   BDR: none
3w6d: OSPF: 144.254.154.1 address 144.254.3.1 on Serial0/0 is dead, state DOWN
3w6d: %OSPF-5-ADJCHG: Process 1, Nbr 144.254.154.1 on Serial0/0 from FULL to DOW
N, Neighbor Down: Interface down or detached^Z
R3#
3w6d: OSPF: Neighbor change Event on interface Serial0/0
3w6d: OSPF: DR/BDR election on Serial0/0
3w6d: OSPF: Elect BDR 0.0.0.0
3w6d: OSPF: Elect DR 0.0.0.0
3w6d:        DR: none    BDR: none
3w6d: OSPF: Remember old DR 144.254.154.1 (id)
3w6d: OSPF: Build router LSA for area 0, router ID 144.254.153.1, seq 0x80000269
3w6d: OSPF: Send with youngest Key 0
3w6d: BR0/0 DDR: Dialing cause ip (s=144.254.7.1, d=224.0.0.5)
3w6d: BR0/0 DDR: Attempting to dial 7775020
3w6d: %LINK-3-UPDOWN: Interface BRI0/0:2, changed state to up
3w6d: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
3w6d: Vi1 DDR: Dialer statechange to up
3w6d: Vi1 DDR: Dialer call has been placed
3w6d: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0:2, changed state to
 up
3w6d: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed s
tate to up
3w6d: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state t
o down
3w6d: OSPF: Send with youngest Key 0
3w6d: %ISDN-6-CONNECT: Interface BRI0/0:2 is now connected to 7775020 R5
```

Example 8-59 displays the debug output when an ISDN call is made to R5 after OSPF neighbor adjacencies between R3 and R4 are terminated. The debug output shows that the neighbor adjacency state to R4 failing and an outgoing call to R3 being made followed by a successful OSPF adjacency.

Example 8-60 confirms OSPF neighbor adjacency to R5 and the fact that IP routing is now over the ISDN interface BRI0/O.

Example 8-60 **show ip ospf neighbor** *on R3*

```
R3#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
144.254.155.1     1   FULL/  -            -        144.254.7.2     BRI0/0
144.254.152.1     0   FULL/DROTHER    00:01:19    144.254.4.2     FastEthernet0/
0
R3#show ip route ospf
     144.254.0.0/16 is variably subnetted, 12 subnets, 5 masks
O IA    144.254.6.0/29 [110/1563] via 144.254.7.2, 00:03:29, BRI0/0
O IA    144.254.5.0/27 [110/1563] via 144.254.7.2, 00:03:29, BRI0/0
O E1    144.254.2.0/30 [110/1663] via 144.254.7.2, 00:03:29, BRI0/0
O       144.254.3.0/29 [110/1611] via 144.254.7.2, 00:03:29, BRI0/0
O E1    144.254.1.0/30 [110/1663] via 144.254.7.2, 00:03:29, BRI0/0
O       144.254.154.0/24 [110/1564] via 144.254.7.2, 00:03:29, BRI0/0
O IA    144.254.155.0/24 [110/1563] via 144.254.7.2, 00:03:29, BRI0/0
O       144.254.152.0/24 [110/1612] via 144.254.7.2, 00:03:29, BRI0/0
O E1    144.254.151.0/24 [110/1663] via 144.254.7.2, 00:03:29, BRI0/0
     131.108.0.0/24 is subnetted, 3 subnets
O E1    131.108.3.0 [110/1663] via 144.254.7.2, 00:03:29, BRI0/0
O E1    131.108.2.0 [110/1663] via 144.254.7.2, 00:03:29, BRI0/0
O E1    131.108.1.0 [110/1663] via 144.254.7.2, 00:03:29, BRI0/0
R3#
```

Finally, ensure that when ISDN is active, the ISDN subnet, 144.254.7.0/30, is reachable from all parts of the network.

Example 8-61 confirms the subnet in the routing table on the furthest router from R3, namely R1.

Example 8-61 **show ip route** *on R1*

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
```

Example 8-61 **show ip route** *on R1 (Continued)*

```
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 144.254.1.2 to network 0.0.0.0

     144.254.0.0/16 is variably subnetted, 12 subnets, 5 masks
D EX    144.254.6.0/29 [170/302364416] via 144.254.2.2, 02:06:49, Tunnel0
D EX    144.254.7.0/30 [170/302364416] via 144.254.2.2, 00:16:26, Tunnel0
D EX    144.254.4.0/26 [170/302364416] via 144.254.2.2, 01:26:04, Tunnel0
D       144.254.5.0/27 [90/297270016] via 144.254.2.2, 02:06:49, Tunnel0
C       144.254.2.0/30 is directly connected, Serial0/1
D       144.254.3.0/29 [90/297756416] via 144.254.2.2, 02:06:49, Tunnel0
C       144.254.1.0/30 is directly connected, Ethernet0/0
D       144.254.154.0/24 [90/297372416] via 144.254.2.2, 02:06:50, Tunnel0
D EX    144.254.155.0/24 [170/302364416] via 144.254.2.2, 01:23:27, Tunnel0
D EX    144.254.152.0/24 [170/302364416] via 144.254.2.2, 02:06:50, Tunnel0
D EX    144.254.153.0/24 [170/302364416] via 144.254.2.2, 00:16:17, Tunnel0
C       144.254.151.0/24 is directly connected, Loopback0
     131.108.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       131.108.3.0/24 is directly connected, Loopback3
C       131.108.2.0/24 is directly connected, Loopback2
C       131.108.1.0/24 is directly connected, Loopback1
D       131.108.0.0/22 is a summary, 02:57:04, Null0
R*   0.0.0.0/0 [120/1] via 144.254.1.2, 00:00:01, Ethernet0/0
```

Example 8-62 displays a successful ping request from R1 to R3 BRI0/0 and R5 BRI0/0.

Example 8-62 *Ping 144.254.7.1 and 144.254.7.2 from R1*

```
R1#ping 144.254.7.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.7.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/38/40 ms
R1#ping 144.254.7.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.7.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
R1#
```

NOTE The **show isdn status** IOS command details if any calls are active. R3 must have a call active only when the Frame-Relay connection to R4 is not routing IP.

The following display is taken when the Frame-Relay link is operational:

```
R3#show isdn status
Global ISDN Switchtype = basic-5ess
ISDN BRI0/0 interface
        dsl 0, interface ISDN Switchtype = basic-5ess
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 64, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 0 CCBs = 0
    The Free Channel Mask:  0x80000003
    Total Allocated ISDN CCBs = 0
R3#
```

Currently, there are no Layer 3 calls. When the ISDN interface is operational, you should see, at most, two calls. The following display is taken when one ISDN B channel is active:

```
R3#show isdn status
Global ISDN Switchtype = basic-5ess
ISDN BRI0/0 interface
        dsl 0, interface ISDN Switchtype = basic-5ess
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 64, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        1 Active Layer 3 Call(s)
        CCB:callid=803F, sapi=0, ces=1, B-chan=1, calltype=DATA
    Active dsl 0 CCBs = 1
    The Free Channel Mask:  0x80000002
    Total Allocated ISDN CCBs = 1
R3#
```

You should also use **show** commands in any CCIE lab to make sure you have satisfied the questions, as just seen, in the case of ensuring ISDN is active only when a failure occurs.

DHCP Configuration (3 Points)

A number of Windows XP users on VLAN_D support DHCP and the ability to receive more than one IP gateway. Configure R2 to provide only a pool of DHCP addresses with the following criteria:

- The IP addresses pool ranges from 144.254.4.0/26 shared between R2 and R3.
- The DNS servers are 139.134.2.2 and 139.134.1.1.

- The domain name is cisco.com.
- Default gateway of 144.254.4.1 or 144.254.4.2 only.
- Hosts must retain DHCP-assigned addresses forever.
- The predefined addresses 144.254.4.1, 144.254.4.2, and 144.254.4.3 are never allocated to DHCP clients.

You can assume that you have Windows XP clients only and support more than one gateway if any one router fails.

DHCP Configuration Solution

VLAN_D contains the subnet 144.254.4.0/26 with the allocated IP addresses, one each to R2 E0/0, R3 Fast0/0, and the Catalyst 3550 management interface. You must ensure that any DHCP servers (R2, in this case) do not allocate these three preassigned address.

Example 8-63 configures R2 for DHCP pool allocation.

Example 8-63 *DHCP Configuration on R2*

```
ip dhcp excluded-address 144.254.4.1
ip dhcp excluded-address 144.254.4.2
ip dhcp excluded-address 144.254.4.3
!
ip dhcp pool ccie
   network 144.254.4.0 255.255.255.192
   domain-name cisco.com
   dns-server 139.134.2.2 139.134.1.1

default-router 144.254.4.1 144.254.4.2
   lease infinite
```

R2 provides the DNS domain name and two default gateways. Notice that the lease is enabled to be used forever by DHCP clients with the IOS command **lease infinite**. If R2 fails, all DHCP clients with existing IP addresses will route through Router R3 with the default gateway 144.254.4.1.

BGP Routing Configuration (6 Points)

After finishing this section, make sure that all configured interfaces and subnets are consistently visible on all pertinent routers, even in the event of network failure of any one router.

Basic IBGP Configuration

Configure IBGP on all routers in your network:

- Do not use any WAN IP interfaces for IBGP sessions, because your network is prone to failures across the Frame Relay cloud.
- Configure R4 as the route reflector and ensure that remote routers peer to R4 only.
- Minimize IBGP configurations as much as possible.
- The IBGP connection between R2 and R4 must use MD5 authentication to authenticate the IBGP peer.
- You can disable BGP synchronization.
- Use AS 333 on all IBGP routers.
- As long as there is IP connectivity in your network, ensure that BGP is active in all routers.
- Using the **network** command only, make sure only the loopback interfaces on Routers R1 through R5 are advertised by BGP to the route reflector, R4. Ensure that each router has a corresponding BGP table entry for all loopbacks.
- Do not change the BGP administrative distance to complete this task.
- Make sure you have full IBGP connectivity.
- Ensure that all routers have BGP routing entries in their respective BGP tables.

NOTE R4's BGP table (not IP routing table) should look like this:

```
R4#show ip bgp
BGP table version is 11, local router ID is 144.254.154.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i144.254.151.0/24 144.254.151.1            0    100      0 i
*>i144.254.152.0/24 144.254.152.1            0    100      0 i
*>i144.254.153.0/24 144.254.153.1            0    100      0 i
*> 144.254.154.0/24 0.0.0.0                  0         32768 i
```

Basic IBGP Configuration Solution

Router R4, the hub of this network, provides BGP (internal) information to R1, R2, R3, and R5.

Example 8-64 configures R4 as the route reflector to remote peers R1, R2, R3, and R5 using the loopback interface as the source address. Next-hop address could be used, but in the event of a

WAN failure (in particular for R3), the BGP session would be inactive, so it is better to use the loopback.

Example 8-64 *IBGP Configuration on R4*

```
router bgp 333
 no synchronization
 network 144.254.154.0 mask 255.255.255.0
 neighbor 144.254.151.1 remote-as 333
 neighbor 144.254.151.1 update-source Loopback0
 neighbor 144.254.151.1 route-reflector-client
 neighbor 144.254.152.1 remote-as 333
 neighbor 144.254.152.1 password cisco
 neighbor 144.254.152.1 update-source Loopback0
 neighbor 144.254.152.1 route-reflector-client
 neighbor 144.254.153.1 remote-as 333
 neighbor 144.254.153.1 update-source Loopback0
 neighbor 144.254.153.1 route-reflector-client
 neighbor 144.254.155.1 remote-as 333
 neighbor 144.254.155.1 update-source Loopback0
 neighbor 144.254.155.1 route-reflector-client
```

R4 is configured as the route reflector to four remote routers in AS 333. Notice that MD5 authentication is enabled between R4 and R2, as stated in the question criteria. The **network** command is used to inject Loopback 0 on R4 into the BGP routing table.

Example 8-65 enables IBGP on R2 with MD5 authentication to R4.

Example 8-65 *IBGP Configuration on R2*

```
router bgp 333
 no synchronization
 network 144.254.152.0 mask 255.255.255.0
 neighbor 144.254.154.1 remote-as 333
 neighbor 144.254.154.1 password cisco
 neighbor 144.254.154.1 update-source Loopback0
```

R2 is configured as an IBGP peer to R4 with MD5 authentication to ensure that the IBGP session is authenticated. The **network** command is used to inject the loopback of R2 into the BGP table.

Example 8-66 confirms the BGP table on R2 with the command **show ip bgp**.

Example 8-66 **show ip bgp** *on R2*

```
R2#show ip bgp
BGP table version is 22, local router ID is 144.254.152.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
```

continues

Example 8-66 **show ip bgp** *on R2 (Continued)*

```
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i144.254.151.0/24 144.254.151.1            0    100      0 i
*> 144.254.152.0/24 0.0.0.0                  0         32768 i
*>i144.254.153.0/24 144.254.153.1            0    100      0 i
*>i144.254.154.0/24 144.254.154.1            0    100      0 i
*>i144.254.155.0/24 144.254.155.1            0    100      0 i
R2#
```

Example 8-67 confirms the BGP table on R4 with the command **show ip bgp**.

Example 8-67 **show ip bgp** *on R4*

```
R4#show ip bgp
BGP table version is 14, local router ID is 144.254.154.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i144.254.151.0/24 144.254.151.1            0    100      0 i
*>i144.254.152.0/24 144.254.152.1            0    100      0 i
*>i144.254.153.0/24 144.254.153.1            0    100      0 i
*> 144.254.154.0/24 0.0.0.0                  0         32768 i
*>i144.254.155.0/24 144.254.155.1            0    100      0 i
R4#
```

Example 8-68 confirms the IBGP on R4, as established with the summary BGP command **show ip bgp summary**.

Example 8-68 **show ip bgp summary** *on R4*

```
R4#show ip bgp summary
BGP router identifier 144.254.154.1, local AS number 333
BGP table version is 14, main routing table version 14
5 network entries and 5 paths using 665 bytes of memory
2 BGP path attribute entries using 120 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP activity 8/31 prefixes, 8/3 paths, scan interval 15 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
144.254.151.1   4   333   14192   14204       14    0    0 1w2d        1
144.254.152.1   4   333   14191   14202       14    0    0 1w2d        1
144.254.153.1   4   333   14189   14198       14    0    0 1w2d        1
144.254.155.1   4   333   14189   14199       14    0    0 1w2d        1
R4#
```

Five networks are installed in the BGP table, one local (next hop 0.0.0.0) and four remote (next hops for R1, R2, R3, and R5 loopback IP addresses).

NOTE For more examples of CCIE questions on BGP, refer to Appendix C for a sample Routing and Switching lab endorsed by the CCIE content management team.

You will notice that the Routing and Switching topics presented in the first half of this lab are valued at approximately half of the points (56 points). The next section is based on Security features and is also valued at approximately half of the points (44 points). As you can see, a candidate weak in Routing and Switching but proficient in Security features or vice versa will still likely fail because a total of 80 points is needed to pass.

CCIE Security Self-Study Lab Part II: Advanced Security Design (4 Hours)

Part II concentrates on the advanced security topics that are possible in the CCIE Security exam. Now that Part I has been configured and all devices are communicating, you can add security to the network and ensure that the network is safe from intruders or hackers.

IP Access List (4 Points)

On R5, configure an access list that meets the following criteria and contains the *fewest* configuration lines as possible:

- Apply the access list on the outbound interface on R5's Fast Ethernet link to R4.
- Deny any TCP packet with source address 129.57.204.0/24.
- Deny any TCP packet with source address 129.57.140.0/24.
- Deny any TCP packet with source address 225.133.29.0/24.
- Deny any TCP packet with source address 161.133.29.0/24.
- Deny every even subnet in 182.133.0.0/16.
- Deny every odd subnet in 182.133.0.0/16.
- Permit all other IP traffic.

Confirm access to the network after applying the access list. (Hint: Use at most four lines of access list configuration.)

State how you can review any access violations.

IP Access List Solution

The access list required here is somewhat tricky. The requirement that you use the least number of lines possible means that you should start looking for similarities in the subnets so that you can configure the correct mask.

Because you are denying TCP, you must use an extended access list, because standard access lists are based on IP only.

The first two subnets (129.57.140.0/24 and 129.57.204.0/24), when displayed in binary, look like the following. Notice that the first two octets are the same:

140 in binary is 10001100
204 in binary is 11001100

Only one bit (bit 2) is different (it could be 0 or 1 and hence is a don't care bit), so you can apply the mask as follows (remember, 0 means match and 1 means do not care):

10001100 (140 in decimal)
11001100 (204 in decimal)
01000000 (64 in decimal)

Example 8-69 configures the first access list line code to encompass the two networks, 129.57.140.0/24 and 129.57.204.0/24, with one line of IOS code.

Example 8-69 *First Access List Line*

```
access-list 100 deny  tcp 129.57.140.0 0.0.64.255 any log
```

The inverse mask, 0.0.64.255, means the first two octets (129 and 57) must match, followed by either 140 or 204, and you do not care about the last octet (255 or all 111111111).

The same principle of binary bit notation is followed with the second pair of networks:

11100001 (225 in decimal)
11000001 (161 in decimal)
01000000 (64 in decimal)

Example 8-70 configures the second access list line code to encompass the two networks, 225.133.29.0/24 and 161.133.29.0/24, with one line of IOS code.

Example 8-70 *Second Access List Line*

```
access-list 100 deny tcp 161.133.29.0 64.0.0.0 any log
```

The final two conditions are met with a **deny** statement for all networks on 182.133.0.0/16 and an implicit **permit** on all other networks. Example 8-71 displays the final two IOS coded lines.

Example 8-71 *Final Two Statements*

```
access-list 100 deny   tcp 182.133.0.0 0.0.255.255 any log
access-list 100 permit ip any any log
```

The **log** keyword ensures that any packets matching the access list are logged and available for further investigation when required. Ensure that all other legitimate IP data, such as OSPF routing updates, is encompassed in the last statement by implicitly allowing all other traffic.

Finally, apply the access list to the outbound interface on R5. Example 8-72 applies the access number 100 on the outbound interface to R5.

Example 8-72 *Access List Applied to R5 Serial0/0*

```
R5(config)#interface fastEthernet 0/0
R5(config-if)# ip access-group 100 out
```

Telnet to R5 and review the access list log. You should see the number of access list violations that were entered as a result of the failed access.

To view access list violations, use the IOS command **show ip access-list 100**.

Prevent Denial-of-Service Attacks (4 Points)

Legitimate users from Company A no longer have access to their internal website on VLAN_A. A network sniffer analyzer advises that attacks have taken place on VLAN_A in your network subnet 144.254.1.0/30. E-mail server and FTP services (VLAN 2) are unavailable because a hacker is flooding the server with a number of requests for connections. Configure your router to prevent TCP servers from accepting TCP SYN attacks and flooding VLAN_A.

Prevent Denial-of-Service Attacks Solution

TCP Intercept will stop this DoS attack. The IOS command syntax is as follows:

```
ip tcp intercept mode intercept
ip tcp intercept list 100


access-list 100 permit ip any subnet-being-attacked
```

R1 is configured with TCP Intercept mode. Example 8-73 enables R1 for TCP Intercept mode.

Example 8-73 *TCP Intercept on R1*

```
R1(config)# ip tcp intercept mode intercept
R1(config)#ip tcp intercept list 100
R1(config)#access-list 100 permit ip any 144.254.1.0 0.0.0.3
```

Example 8-74 displays the output of a sample **show tcp intercept connections** EXEC command.

Example 8-74 **show tcp intercept connections** *Command*

```
R1# show tcp intercept connections
 Incomplete:
Client                  Server                State    Create   Timeout  Mode
172.19.160.17:58190     10.1.1.30:23          SYNRCVD  00:00:09 00:00:05 I
172.19.160.17:57934     10.1.1.30:23          SYNRCVD  00:00:09 00:00:05 I

Established:
Client                  Server                State    Create   Timeout  Mode
171.69.232.23:1045       10.1.1.30:23           ESTAB     00:00:08 23:59:54 I
```

Table 8-4 describes significant fields shown in the display.

Table 8-4 **show tcp intercept connections** *Description*

Output	Description
Incomplete	Rows of information under Incomplete indicate connections that are not yet established.
Client	The client's IP address and port.
Server	IP address and port of the server being protected by TCP Intercept.
State	**SYNRCVD**—establishing with client. **SYNSENT**—establishing with server. **ESTAB**—established with both, passing data.
Create	Hours:minutes:seconds since the connection was created.
Timeout	Hours:minutes:seconds until the retransmission timeout.
Mode	**I**—intercept mode. **W**—watch mode.
Established:	Rows of information under Established indicate connections that are established. The fields are the same as those under Incomplete except for the Timeout field, described next.
Timeout	Hours:minutes:seconds until the connection will time out, unless the software sees a FIN exchange, in which case this indicates the hours:minutes:seconds until the FIN or RESET timeout.

Table 8-5 displays other useful TCP Intercept configuration and monitoring commands.

Table 8-5 *TCP Intercept–Related Commands*

Command	Description
ip tcp intercept connection-timeout	Changes how long a TCP connection will be managed by the TCP Intercept after no activity
ip tcp intercept first-timeout	Changes how long after receipt of a reset or FIN-exchange the software ceases to manage the connection
ip tcp intercept list	Enables TCP Intercept
show tcp intercept statistics	Displays TCP Intercept statistics

NOTE You can find more details on TCP Intercept at the following:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/scfdenl.htm

TCP Intercept is available on Enterprise and SP feature set images only.

Time-Based Access List (4 Points)

Employees connected to VLAN_C on R5 don't need web access while at work. Block web traffic from Monday through Friday between the hours of 7:00 a.m. and 5:00 p.m.

Time-Based Access List Solution

On Fast Ethernet 0/1 VLAN_C, you need to apply an extended access list. Example 8-75 displays the extended access list configuration on R5 Fast0/1. Use a named access list to make things a little more interesting and easy to read.

Example 8-75 *Access List Configuration on R5*

```
R5(config)#interface fastethernet 0/1
R5(config-if)#ip access-group web-traffic in
R5(config-if)#exit
```

Example 8-76 configures and defines the extended access list named web-traffic.

Example 8-76 *Extended Access List Configuration*

```
R5(config)#ip access-list extended web-traffic
R5(config-ext-nacl)#deny ?
  <0-255>  An IP protocol number
  ahp      Authentication Header Protocol
  eigrp    Cisco's EIGRP routing protocol
  esp      Encapsulation Security Payload
```

continues

Example 8-76 *Extended Access List Configuration (Continued)*

```
  gre      Cisco's GRE tunneling
  icmp     Internet Control Message Protocol
  igmp     Internet Gateway Message Protocol
  igrp     Cisco's IGRP routing protocol
  ip       Any Internet Protocol
  ipinip   IP in IP tunneling
  nos      KA9Q NOS compatible IP over IP tunneling
  ospf     OSPF routing protocol
  pcp      Payload Compression Protocol
  pim      Protocol Independent Multicast
  tcp      Transmission Control Protocol
  udp       User Datagram Protocol
```

After you select the TCP option (HTTP runs over TCP port 80), you are presented with the time range options. Example 8-77 configures R5 to set a time range for World Wide Web access.

Example 8-77 *Specify Time Range for World Wide Web Access*

```
R5(config-ext-nacl)#deny tcp any any ?
  ack          Match on the ACK bit
  dscp         Match packets with given dscp value
  eq           Match only packets on a given port number
  established  Match established connections
  fin          Match on the FIN bit
  fragments    Check non-initial fragments
  gt           Match only packets with a greater port number
  log          Log matches against this entry
  log-input    Log matches against this entry, including input interface
  lt           Match only packets with a lower port number
  neq          Match only packets not on a given port number
  precedence   Match packets with given precedence value
  psh          Match on the PSH bit
  range        Match only packets in the range of port numbers
  rst          Match on the RST bit
  syn          Match on the SYN bit
  time-range   Specify a time-range
  tos          Match packets with given TOS value
  urg          Match on the URG bit
  <cr>

R5(config-ext-nacl)#deny tcp any eq any 80 time-range ?
WORD  Time-range entry name

R5(config-ext-nacl)#deny tcp any  eq 80 any time-range web-timing
R5(config-ext-nacl)#permit ip any any
R5(config-ext-nacl)#exit
R5(config)#time-range  ?
  WORD  Time range name
```

Finally, the **time-range** global configuration command defines specific times of the day and week. Example 8-78 enables the **time-range** command on R5.

Example 8-78 **time-range** *Command on R5*

```
R5(config)#time-range  web-timing
R5(config-time-range)#?
Time range configuration commands:
  absolute  absolute time and date
  default   Set a command to its defaults
  exit      Exit from time-range configuration mode
  no        Negate a command or set its defaults
  periodic  periodic time and date
R5(config-time-range)#periodic weekdays  7:00 to 17:00
```

Dynamic Access List/Lock and Key Feature (5 Points)

Make sure that during normal operation it is not possible to ping from R2 (Ethernet0/0) to R3 (FastEthernet0/0). After a Telnet login from R2 to R3, pings are allowed, but make sure that after 5 minutes of inactivity normal operation is restored. Routing should still be in place in both circumstances.

Dynamic Access List/Lock and Key Feature Solution

This is an example where dynamic access lists are used to allow access only after a valid username/password has been entered. Access is denied again after a period (5 minutes, in this case) of inactivity.

Example 8-79 configures R3 with an extended access list, 100.

Example 8-79 *Extended Access List Configuration on R3*

```
R3(config)#access-list 100 ?
  deny     Specify packets to reject
  dynamic  Specify a DYNAMIC list of PERMITs or DENYs
  permit   Specify packets to forward
  remark   Access list entry comment
R3(config)#access-list 100 dynamic ?
  WORD  Name of a Dynamic list
R3(config)#access-list 100 dynamic blockping ?
  deny     Specify packets to reject
  permit   Specify packets to forward
  timeout  Maximum time for dynamic ACL to live
R3(config)#access-list 100 dynamic blockping timeout 5 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
R3(config)#$access-list 100 dynamic blockping timeout 5 permit icmp host
    144.254.4.2 host 144.254.4.1
R3(config)#access-list 100 deny icmp host 144.254.4.2 host 144.254.4.1 echo
R3(config)#access-list 100 permit ip any any
```

After the access list is defined, you must apply the access list to the vty lines on R3.

After the ACL is defined, you must apply the ACL to the interface, followed by the **auto command** under vty lines on R3. Example 8-80 displays applying the ACL to the interface and the vty line configuration.

Example 8-80 *Vty Configuration*

```
R3(config)#line vty 0 4
R3(config-line)#autocommand ?
  LINE                    Appropriate EXEC command
  no-suppress-linenumber  Display service linenumber message
R3(config-line)#autocommand access-enable-after-ping  ?
LINE    <cr>
R3(config-line)#autocommand access-enable-after-ping  host timeout 5
```

Example 8-81 displays a failed ping request from R2 to R3.

Example 8-81 **ping 144.254.4.1** *from R2*

```
R2#ping 144.254.4.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.4.1, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
```

The ping requests are not permitted because a successful Telnet connection is required before ICMP pings are permitted.

Example 8-82 telnets from R2 to R3, passes authentication, and is automatically dropped out by R3.

Example 8-82 *Telnet from R2 to R1*

```
R2#telnet 144.254.4.1
Trying 144.254.4.1 ... Open
User Access Verification
Password: cisco
[Connection to 144.254.4.1 closed by foreign host]
```

Example 8-83 now pings R3 from R2 successfully.

Example 8-83 **ping 144.254.4.1** *from R2*

```
R2#ping 144.254.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.4.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R2#ping 144.254.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 144.254.4.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R2#
```

To monitor the access violations, use the IOS command **show ip access-list 100**.

Example 8-84 displays the accesses and violations on R3.

Example 8-84 **show ip access-list 100** *Command on R3*

```
R3#show ip access-lists
Extended IP access list 100
    Dynamic blockping permit icmp host 144.254.4.2 host 144.254.4.1
      permit icmp host 144.254.4.2 host 144.254.4.1 (30 matches) (time left 269)
    deny icmp host 144.254.4.2 host 144.254.4.1 echo (8 matches)
    permit ip any any (260 matches)
R3#
```

Cisco IOS Firewall Configuration on R5 (6 Points)

Translate the following policy into a working CBAC configuration on R5 (assuming this router's FastEth0/1 is connected to another ISP):

- Allow all TCP and UDP traffic initiated on the inside from network 144.254.5.0 to access the Internet. ICMP traffic will also be allowed from the same network. Other networks (inside) must be denied. For traffic initiated on the outside, allow everyone to access only HTTP to host 144.254.5.3.
- All other traffic must be denied.

Cisco IOS Firewall Configuration on R5 Solution

CBAC intelligently filters TCP and UDP packets based on application layer protocol session information. You can configure CBAC to permit specified TCP and UDP traffic through a firewall

only when the connection is initiated from within the network you want to protect. CBAC can inspect traffic for sessions that originate from either side of the firewall, and CBAC can be used for intranet, extranet, and Internet perimeters of your network.

To configure CBAC, perform the following tasks:

- Pick an interface: internal or external (required).
- Configure IP access lists at the interface (required).
- Configure global timeouts and thresholds (required).
- Define an inspection rule (required).
- Apply the inspection rule to an interface (required).
- Configure logging and audit trail (required).
- Follow other guidelines for configuring a firewall (required).
- Verify CBAC (optional).

Example 8-85 configures R5 for CBAC outbound connections.

Example 8-85 *R5 Outbound Connections*

```
R5(config)#ip inspect name OUTBOUND tcp
R5(config)#ip inspect name OUTBOUND udp
R5(config)#access-list 101 permit ip 144.254.5.0 0.0.0.0.31 any
R5(config)#interface FastEthernet0/0
R5(config-if)#ip inspect OUTBOUND in
R5(config-if)#ip access-group 101 in
```

Example 8-86 configures R5 for inbound connections.

Example 8-86 *Inbound Connections from the Internet*

```
R5(config)#access-list 102 permit icmp any host 144.254.5.3
R5(config)#access-list 102 permit tcp any host 144.254.5.3 eq www
R5(config)#interface FastEthernet0/1
R5(config-if)#ip access-group 102 in
```

Monitoring and Maintaining CBAC

To assist CBAC debugging, you can turn on audit trail messages that will be displayed on the console after each CBAC session closes. The IOS command **ip inspect audit-trail** turns on CBAC audit trail messages.

Many other **debug** commands are available, including the following:

- Generic **debug** commands
- Transport-level **debug** commands
- Application protocol **debug** commands

For more details on CBAC, visit:

www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/scfcbac.htm#xtocid21

IPSec Configuration (6 Points)

The Frame Relay network between R2, R3, and R4 requires IPSec to ensure that no data between these routers is susceptible to intruders.

Set up IPSec using preshared keys between R2, R3, and R4, and ensure that the following points are taken into account:

- Use MD5 as the hashing algorithm.
- Authentication will be preshared.
- The authentication key is CciE; use a 56-bit key.
- Use SHA to calculate the hashes on the actual packet payloads in ESP.
- Set up IPSec in transport mode.
- Set the security association lifetime to 300 seconds.
- Ensure that all IP data between the R2, R3, and R4 is encrypted using IPSec (over the Frame Relay network only). (Hint: Apply the crypto map to the Serial links only and not to the ISDN link.)
- Use one transform set on each router.

IPSec Configuration Solution

To start, configure IKE on Routers R4, R2, and R3. Example 8-87 displays the IKE configuration on R4. Remember that IKE policies define a set of parameters to be used during IKE negotiation. The shaded portion in Example 8-87 matches the criteria in the question.

Example 8-87 *IKE Configuration on R4*

```
R4(config)#crypto isakmp policy 1
R4(config-isakmp)#hash ?
  md5  Message Digest 5
  sha  Secure Hash Standard
R4(config-isakmp)#hash md5
R4(config-isakmp)#authentication ?
  pre-share  Pre-Shared Key
  rsa-encr   Rivest-Shamir-Adleman Encryption
  rsa-sig    Rivest-Shamir-Adleman Signature
R4(config-isakmp)#authentication pre-share
```

Example 8-88 configures the preshared key to be set to CCiE.

Example 8-88 *Preshared Key on R4 Set to CCiE*

```
R4(config)#crypto isakmp key ?
  WORD  pre-shared key
R4(config)#crypto isakmp key CCiE ?
  address   define shared key with IP address
  hostname  define shared key with hostname
R4(config)#crypto isakmp key CCiE address 144.254.3.2 ?
  A.B.C.D  Peer IP subnet mask
  <cr>
R4(config)#crypto isakmp key CCiE address 144.254.3.2
R4(config)#crypto isakmp key CCiE address 144.254.3.3
```

The preshared key value (password) is CCiE, and the peer address of the remote IPSec peer is 144.254.3.2 (R2) and 144.254.3.3 (R3).

Preshared Keys Versus Manual Keys

This is an example of preshared keys where IKE is used to negotiate all SA parameters. You can also define IPSec not to use IKE; this is referred to as *manual IPSec* or *manual keys*. Cisco strongly recommends that you use IKE or preshared keys because ensuring that all SA parameters match between remote peers is very difficult. The DH algorithm is a more secure method when generating secret keys between peers. Manual keys are prone to insiders and unauthorized sources that gain entry to Cisco configuration files. Another major disadvantage of manual keys is that the IOS **crypto map** command that is used to establish security associations (SAs) does not expire.

Example 8-89 defines the transform set, which indicates to use transport mode and SHA and ESP encapsulation.

Example 8-89 *SHA/ESP and Transport Mode Configuration on R4*

```
R4(config)#crypto ipsec transform-set anyname1 ?
  ah-md5-hmac   AH-HMAC-MD5 transform
  ah-sha-hmac   AH-HMAC-SHA transform
  comp-lzs      IP Compression using the LZS compression algorithm
  esp-des       ESP transform using DES cipher (56 bits)
  esp-md5-hmac  ESP transform using HMAC-MD5 auth
  esp-null      ESP transform w/o cipher
  esp-sha-hmac  ESP transform using HMAC-SHA auth
  <cr>
R4(config)#crypto ipsec transform-set anyname1 esp-des ?
  ah-md5-hmac   AH-HMAC-MD5 transform
  ah-sha-hmac   AH-HMAC-SHA transform
  comp-lzs      IP Compression using the LZS compression algorithm
  esp-md5-hmac  ESP transform using HMAC-MD5 auth
  esp-sha-hmac  ESP transform using HMAC-SHA auth
  <cr>
R4(config)#crypto ipsec transform-set anyname1 esp-des esp-sha-hmac
R4(cfg-crypto-trans)#mode ?
  transport  transport (payload encapsulation) mode
  tunnel     tunnel (datagram encapsulation) mode

R4(cfg-crypto-trans)#mode transport
```

The **transform set** command defines an acceptable combination of security protocols and algorithms; this example applies ESP-DES (ESP with the 56-bit DES encryption algorithm) and ESP with the SHA (HMAC variant) authentication algorithm.

You need to define the crypto map and the access list to encompass the networks you want to encrypt. On R4 only, the network 144.254.3.0/28 is encrypted. Example 8-90 configures R4 with a crypto map and access list 150.

Example 8-90 *Crypto Map and Access List Configuration on R4*

```
crypto map anyname 1 ipsec-isakmp
 set peer 144.254.3.2
 set peer 144.254.3.3
 set security-association lifetime seconds 300
 set transform-set anyname1
 match address 150
access-list 150 permit ip any any
```

Access list 150 ensures that all IP data is encrypted from R4 to R2 and R3.

Finally, on R4, you must apply the crypto map to the physical interface Serial0/0 on R4. Example 8-91 applies the crypto map to Serial0/0 on R4.

Example 8-91 *Crypto Map Interface Configuration on R4*

```
R4#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#interface serial0/0
R4(config-if)#crypto map anyname
```

R2 and R3 need to be configured exactly the same way.

Example 8-92 displays the full IPSec configuration on R2.

Example 8-92 *R2 IPSec Configuration*

```
crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key CCiE address 144.254.3.1
!
!
crypto ipsec transform-set anyname1onR2 esp-des esp-sha-hmac
 mode transport
!
crypto map anyname 1 ipsec-isakmp
 set peer 144.254.3.1
 set security-association lifetime seconds 300
 set transform-set anyname1onR2
 match address 150
interface Serial0/0
crypto map anyname
access-list 150 permit ip any any
```

Example 8-93 displays the full IPSec configuration on R3.

Example 8-93 *R3 IPSec Configuration*

```
crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key CCiE address 144.254.3.1
!
crypto ipsec transform-set anyname1onR3 esp-des esp-sha-hmac
 mode transport
```

Example 8-93 *R3 IPSec Configuration (Continued)*

```
!
crypto map anyname 1 ipsec-isakmp
 set peer 144.254.3.1
 set security-association lifetime seconds 300
 set transform-set anyname1onR3
 match address 150
interface Serial0/0
crypto map anyname
access-list 150 permit ip any any
```

To display the status of all crypto engine active connections, use the IOS command **show crypto engine connections active**.

Example 8-94 displays the current active crypto connections on R4.

Example 8-94 **show crypto engine connections active** *on R4*

```
R4#show crypto engine connections active
  ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
   3 <none>          <none>          set    HMAC_MD5+DES_56_CB        0        0
   6 Serial0/0       144.254.3.1     set    HMAC_MD5+DES_56_CB        0        0
   7 Serial0/0       144.254.3.1     set    HMAC_MD5+DES_56_CB        0        0
2008 Serial0/0       144.254.3.1     set    HMAC_SHA+DES_56_CB        0    27531
2009 Serial0/0       144.254.3.1     set    HMAC_SHA+DES_56_CB    27529        0
2010 Serial0/0       144.254.3.1     set    HMAC_SHA+DES_56_CB        0      988
2011 Serial0/0       144.254.3.1     set    HMAC_SHA+DES_56_CB     1243        0

R4#
```

Example 8-95 displays the current active crypto connections on R2.

Example 8-95 **show crypto engine connections active** *on R2*

```
R2#show crypto engine connections active

  ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
   1 <none>          <none>          set    HMAC_MD5+DES_56_CB        0        0
2006 Serial0/0       144.254.3.2     set    HMAC_SHA+DES_56_CB        0    71250
2007 Serial0/0       144.254.3.2     set    HMAC_SHA+DES_56_CB    60250        0
R2#
```

Example 8-96 displays the current active crypto connections on R3.

Example 8-96 **show crypto engine connections active** *on R3*

```
R3#show crypto  engine connections active
  ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
   2 <none>          <none>          set    HMAC_MD5+DES_56_CB        0        0
2006 Serial0/0       144.254.3.3     set    HMAC_SHA+DES_56_CB        0     1243
2007 Serial0/0       144.254.3.3     set    HMAC_SHA+DES_56_CB      988        0

R3#
```

The preceding examples confirm that R2, R3, and R4 maintain an IPSec connection.

There are a number of Cisco IOS **show** commands when monitoring IPSec. Here are a few examples.

To view the parameters for each Internet Key Exchange policy, use the **show crypto isakmp policy** EXEC command.

Example 8-97 displays the sample output when issued on R4.

Example 8-97 **show crypto isakmp policy** *on R4*

```
R4#show crypto isakmp policy
Protection suite of priority 1
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
R4#
```

To view the crypto map configuration, use the **show crypto map** EXEC command.

Example 8-98 displays a sample output of the command **show crypto map** when applied to R2.

Example 8-98 **show crypto map** *on R2*

```
R2#show crypto map
Crypto Map "anyname" 1 ipsec-isakmp
        Peer = 144.254.3.1
        Extended IP access list 150
            access-list 150 permit ip any any
        Current peer: 144.254.3.1
        Security association lifetime: 4608000 kilobytes/300 seconds
        PFS (Y/N): N
        Transform sets={ anyname1onR2, }
        Interfaces using crypto map anyname:
                Serial0/0
```

You can also verify the crypto map configuration by viewing the configuration with the command **show running-config**. Example 8-99 displays configured crypto map configurations when viewing the running configuration.

Example 8-99 **show running-config** *(Truncated) on R2*

```
Hostname R2
!
crypto map anyname 1 ipsec-isakmp
 set peer 144.254.3.1
 set security-association lifetime seconds 300
 set transform-set anyname1onR2
 match address 150
```

Refer to Chapter 4, "Security Protocols," or the following URL for more crypto commands:

www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_r/fipsencr/index.htm

Advanced PIX Configuration (5 Points)

In any security exam, you can be sure that the PIX will be a core device (only one PIX Firewall in the real CCIE exam), so the next few question highlight the areas of the PIX you should be proficient with to ensure that you are ready for the many scenarios that you might be asked to configure. The next section concentrates on a sample PIX topology to guide you in areas you should concentrate on in your study preparation.

Configuring SSH on the PIX

Configure the PIX to accept SSH connections. Make sure sessions are killed after 2 hours of inactivity. Limit only VLAN_D hosts to SSH to the PIX. The domain name is cisco.com. Set all passwords to cisco.

Configuring SSH on the PIX Solution

Four steps are required when enabling SSH on a Cisco PIX Firewall:

Step 1 Assign a host name and a domain name. This is required so that an RSA key is generated. The PIX commands are as follows:

```
hostname PIX1
domain-name cisco.com
```

Step 2 Generate the RSA key with the following PIX command:

```
ca generate any-key-name rsa key 2048
```

Step 3 Define the hosts that are permitted access with the following PIX command:

```
ssh ip_address [netmask] [interface_name]
```

Step 4 Set the enable and Telnet password (optional).

Example 8-100 configures the PIX Firewall for SSH connections from VLAN_D or network 144.254.4.0/26. To set a timeout value, use the PIX command **ssh timeout** *seconds*, in this case 2 minutes or 120 seconds.

Example 8-100 *SSH Configuration on the PIX*

```
Pixfirewall(config)#hostname PIX1
PIX1(config)#domain-name cisco.com
PIX1(config)#ca generate rsa key 2048
PIX1(config)#ssh 144.254.4.0 255.255.255.192 inside
PIX1(config)#ssh timeout 120
```

Configuring the PIX for Intrusion Detection

Configure the PIX according to the following Cisco Secure Intrusion Detection System (IDS) policy:

- For the outside interface, enable all informational signatures but drop the packet, and send a message to the syslog server. Attack signatures should be enabled on both the outside and inside interface. More specifically, for the outside interface, drop the packet, send a syslog message, and generate TCP resets in both directions.
- For the inside interface, drop the packet and send an alert to the syslog server.

Configuring the PIX for Intrusion Detection Solution

The PIX command syntax to enable IDS is as follows:

```
ip audit attack [action [alarm] [drop] [reset]]
ip audit info [action [alarm] [drop] [reset]]
ip audit interface if_name audit_name
ip audit name audit_name attack [action [alarm] [drop] [reset]]
ip audit name audit_name info [action [alarm] [drop] [reset]]
ip audit signature signature_number disable
```

Table 8-6 summarizes the command's syntax.

Table 8-6 *IP Audit Syntax Description*

Syntax	Description
audit attack	Specify the default actions to be taken for attack signatures.
audit info	Specify the default actions to be taken for informational signatures.
audit interface	Apply an audit specification or policy (using the **ip audit name** command) to an interface.
audit name	Specify informational signatures, except those disabled or excluded by the **ip audit signature** command, as part of the policy.
audit signature	Specify which messages to display, attach a global policy to a signature, and disable or exclude a signature from auditing.
action *actions*	The **alarm** option indicates that when a signature match is detected in a packet, the PIX Firewall reports the event to all configured syslog servers. The **drop** option drops the offending packet. The **reset** option drops the offending packet and closes the connection if it is part of an active connection. The default is **alarm**.
audit_name	Audit policy name viewed with the **show ip audit name** command.
signature_number	IDS signature number.

Example 8-101 enables the PIX for IDS configuration matching the conditions outlined in the task.

Example 8-101 *IDS Configuration on the PIX Named PIX1*

```
PIX1(config)# ip audit name Attack-outside attack action alarm drop
PIX1(config)# ip audit name Information-inside info action alarm drop
PIX1(config)# ip audit name Attack-inside attack action alarm reset
PIX1(config)# ip audit interface inside Attack-inside
PIX1(config)# ip audit interface inside Information-inside
PIX1(config)# ip audit interface outside Attack-outside
PIX1(config)# ip audit info action alarm
PIX1(config)# ip audit attack action alarm
```

Table 8-7 displays the available **show** commands that monitor IDS on a Cisco PIX Firewall.

Table 8-7 **show ip audit** *Commands and Output*

show Command	show Command Output
show ip audit attack	Displays the default attack actions: ■ PIX1# **show ip audit attack** ■ ip audit attack action alarm
show ip audit info	Displays the default informational actions: ■ PIX1# **show ip audit info** ■ ip audit info action alarm
show ip audit interface	Displays the interface configuration: ■ PIX1# **show ip audit interface** ■ ip audit interface outside Attack-inside ■ ip audit interface inside Information-inside ■ ip audit interface inside Attack-outside
show ip audit name [*name* [**info** | **attack**]]	Displays all audit policies or specific policies referenced by name and possibly type: ■ PIX1# **show ip audit name** ■ ip audit name Attack-inside attack action alarm reset ■ ip audit name Information-inside info action alarm drop ■ ip audit name Attack-outside attack action alarm drop

NOTE For more details on IDS, go to:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/cmdref/gl.htm#wp1101884

ACS Configuration (5 Points)

The AAA ACS server is located on the R5 network with the IP address 144.254.6.2, and the server key is set to ccie.

Non-AAA Authentication Methods

Configure the Router R2 so that it provides a TACACS-like username and encrypted password authentication system for networks that cannot support TACACS+. Limit this only to users on VLAN_D.

Non-AAA Authentication Methods Solution

Cisco IOS routers can be configured to authorize usernames with the following command:

```
username name password password encryption-type
```

This IOS command establishes username authentication with encrypted passwords.

To define an access list so that only VLAN_D users can access the router, use the following command:

```
username name access-class number
```

Example 8-102 configures Router R2 for local-based authentication for users from VLAN_D only.

Example 8-102 *Configuring Non-AAA Authentication Methods on R2*

```
R2#show running
hostname R2
aaa new-model
aaa authentication login default local

enable password cisco
!
username Erik access-class 1 password 0 Erik
ip subnet-zero
!

!
access-list 1 permit 144.254.4.0
!
R2#
```

Example 8-103 displays the debug output when an EXEC user on Router R2 telnets to Router R3.

Example 8-103 **debug aaa authentication** *on R2*

```
R2#debug aaa authentication
AAA Authentication debugging is on
R2#show debugging
General OS:
  AAA Authentication debugging is on
Oct 11 16:27:41: AAA: parse name=tty130 idb type=-1 tty=-1
Oct 11 16:27:41: AAA: name=tty130 flags=0x11 type=5 shelf=0 slot=0 adapter=0 por
t=130 channel=0
Oct 11 16:27:41: AAA/MEMORY: create_user (0x62C7BDA8) user='' ruser='' port='tty
130' rem_addr='144.254.4.3' authen_type=ASCII service=LOGIN priv=1
Oct 11 16:27:41: AAA/AUTHEN/START (4131783264): port='tty130' list='' action=LOG
IN service=LOGIN
Oct 11 16:27:41: AAA/AUTHEN/START (4131783264): using "default" list
```

continues

Example 8-103 **debug aaa authentication** *on R2 (Continued)*

```
Oct 11 16:27:41: AAA/AUTHEN/START (4131783264): Method=LOCAL
Oct 11 16:27:41: AAA/AUTHEN (4131783264): status = GETUSER
Oct 11 16:27:47: AAA/AUTHEN/CONT (4131783264): continue_login (user='(undef)')
Oct 11 16:27:47: AAA/AUTHEN (4131783264): status = GETUSER
Oct 11 16:27:47: AAA/AUTHEN/CONT (4131783264): Method=LOCAL
Oct 11 16:27:47: AAA/AUTHEN (4131783264): status = GETPASS
Oct 11 16:27:49: AAA/AUTHEN/CONT (4131783264): continue_login (user='Massimo')
Oct 11 16:27:49: AAA/AUTHEN (4131783264): status = GETPASS
Oct 11 16:27:49: AAA/AUTHEN/CONT (4131783264): Method=LOCAL
Oct 11 16:27:49: AAA/AUTHEN (4131783264): status = PASS
R2#
```

NOTE When using this form of authentication, usernames and passwords are sent in plain text (Massimo, in this example).

Login Authentication Methods

Configure R2 so that when a user is prompted to enter a password when trying to connect via the vty lines, the following display is visible: "Enter your password within 15 seconds:"

Login Authentication Methods Solutions

To define a message on R2 for Telnet (vty users), use the following IOS command:

```
aaa authentication password-prompt "Enter your password within 15 seconds:"
```

Example 8-104 displays the configuration commands on R2.

Example 8-104 *R2 Message Banner*

```
hostname R2
!
aaa new-model
aaa authentication password-prompt "Enter your password within 15 seconds:"
aaa authentication login default local
enable password cisco
!
username gert password 0 gert
username Erik password 0 Erik
```

Example 8-105 displays the message banner when a PRIV user on R3 telnets to R2.

Example 8-105 *Telnet from R3 to R2*

```
R3#telnet 144.254.4.2
Trying 144.254.4.2 ... Open



User Access Verification

Username: Erik
Enter your password within 15 seconds:
Password:*****
R2>
```

Example 8-106 displays the debug output once the Telnet connection is made to R2. Notice that you have 15 seconds to enter a valid password; otherwise, the Telnet connection is closed.

Example 8-106 *Debugging TACACS+ Operation on R2*

```
R2#debug tacacs ?
  events  TACACS+ protocol events
  <cr>
R2#debug tacacs events
TACACS+ events debugging is on
R1#debug tacacs
TACACS access control debugging is on
R2#debug aaa authentication
AAA Authentication debugging is on
R2#show debugging
General OS:
  TACACS access control debugging is on
  TACACS+ events debugging is on
  AAA Authentication debugging is on
R2#
R2#
Oct 11 16:40:44: AAA: parse name=tty130 idb type=-1 tty=-1
Oct 11 16:40:44: AAA: name=tty130 flags=0x11 type=5 shelf=0 slot=0 adapter=0 por
t=130 channel=0
Oct 11 16:40:44: AAA/MEMORY: create_user (0x62C7BDA8) user='' ruser='' port='tty
130' rem_addr='144.254.4.3' authen_type=ASCII service=LOGIN priv=1
Oct 11 16:40:44: AAA/AUTHEN/START (1269435710): port='tty130' list='' action=LOGIN
service=LOGIN
Oct 11 16:40:44: AAA/AUTHEN/START (1269435710): using "default" list
Oct 11 16:40:44: AAA/AUTHEN/START (1269435710): Method=LOCAL
Oct 11 16:40:44: AAA/AUTHEN (1269435710): status = GETUSER
Oct 11 16:40:48: AAA/AUTHEN/CONT (1269435710): continue_login (user='(undef)')
Oct 11 16:40:48: AAA/AUTHEN (1269435710): status = GETUSER
Oct 11 16:40:48: AAA/AUTHEN/CONT (1269435710): Method=LOCAL
Oct 11 16:40:48: AAA/AUTHEN (1269435710): status = GETPASS
```

continues

Example 8-106 *Debugging TACACS+ Operation on R2 (Continued)*

```
Oct 11 16:40:52: AAA/AUTHEN/CONT (1269435710): continue_login (user='Erik')
Oct 11 16:40:52: AAA/AUTHEN (1269435710): status = GETPASS
Oct 11 16:40:52: AAA/AUTHEN/CONT (1269435710): Method=LOCAL
Oct 11 16:40:52: AAA/AUTHEN (1269435710): status = PASS
```

Example 8-106 displays a successful telnet from R3 to R2.

Login Authentication Using TACACS+

Configure R2 to use TACACS+ for authentication at the login prompt. If TACACS+ returns an error, the user is authenticated using the local database.

Login Authentication Using TACACS+ Solution

R2 must be configured for a login name and login method with the following IOS command:

```
aaa authentication login name tacacs+  local
```

Then, the vty lines on R2 must be configured for authentication with the following IOS command:

```
line vty 0 4
login authentication name
```

Example 8-107 configures R2 for login authentication.

Example 8-107 *AAA Authentication on R2 (Truncated)*

```
hostname R2
aaa new-model
aaa authentication login default group tacacs+ local
enable password cisco
!
!
tacacs-server host 144.254.6.2
tacacs-server key ccie
end
```

Example 8-108 displays a successful login attempt when an EXEC user telnets from R3 to R2.

Example 8-108 *Login Authentication Using TACACS+*

```
Oct 11 12:26:56: TAC+: send AUTHEN/START packet ver=192 id=3375296121
Oct 11 12:26:56: TAC+: Using default tacacs server-group "tacacs+" list.
Oct 11 12:26:56: TAC+: Opening TCP/IP to 144.254.6.2/49 timeout=5
Oct 11 12:26:56: TAC+: Opened TCP/IP handle 0x62C8424C to 144.254.6.2/49
Oct 11 12:26:56: TAC+: periodic timer started
Oct 11 12:26:56: TAC+: 144.254.6.2 req=62C81284 Qd id=3375296121 ver=192 handl
```

Example 8-108 *Login Authentication Using TACACS+ (Continued)*

```
e=0x62C8424C (ESTAB) expire=5 AUTHEN/START/LOGIN/ASCII queued
Oct 11 12:26:56: TAC+: 144.254.6.2 (3375296121) AUTHEN/START/LOGIN/ASCII queue
d
Oct 11 12:26:56: TAC+: 144.254.6.2 ESTAB id=3375296121 wrote 38 of 38 bytes
Oct 11 12:26:56: TAC+: 144.254.6.2 req=62C81284 Qd id=3375296121 ver=192 handl
e=0x62C8424C (ESTAB) expire=4 AUTHEN/START/LOGIN/ASCII sent
Oct 11 12:26:56: TAC+: 144.254.6.2 ESTAB read=12 wanted=12 alloc=12 got=12
Oct 11 12:26:56: TAC+: 144.254.6.2 ESTAB read=28 wanted=28 alloc=28 got=16
Oct 11 12:26:56: TAC+: 144.254.6.2 received 28 byte reply for 62C81284
Oct 11 12:26:56: TAC+: req=62C81284 Tx id=3375296121 ver=192 handle=0x62C8424C (
ESTAB) expire=4 AUTHEN/START/LOGIN/ASCII processed
Oct 11 12:26:56: TAC+: (3375296121) AUTHEN/START/LOGIN/ASCII processed
Oct 11 12:26:56: TAC+: periodic timer stopped (queue empty)
Oct 11 12:26:56: TAC+: ver=192 id=3375296121 received AUTHEN status = GETUSER
Oct 11 12:27:00: TAC+: send AUTHEN/CONT packet id=3375296121
Oct 11 12:27:00: TAC+: periodic timer started
Oct 11 12:27:00: TAC+: 144.254.6.2 req=62C81230 Qd id=3375296121 ver=192 handl
e=0x62C8424C (ESTAB) expire=5 AUTHEN/CONT queued
Oct 11 12:27:00: TAC+: 144.254.6.2 (3375296121) AUTHEN/CONT queued
Oct 11 12:27:00: TAC+: 144.254.6.2 ESTAB id=3375296121 wrote 21 of 21 bytes
Oct 11 12:27:00: TAC+: 144.254.6.2 req=62C81230 Qd id=3375296121 ver=192 handl
e=0x62C8424C (ESTAB) expire=4 AUTHEN/CONT sent
Oct 11 12:27:00: TAC+: 144.254.6.2 ESTAB read=12 wanted=12 alloc=12 got=12
Oct 11 12:27:00: TAC+: 144.254.6.2 ESTAB read=28 wanted=28 alloc=28 got=16
Oct 11 12:27:00: TAC+: 144.254.6.2 received 28 byte reply for 62C81230
Oct 11 12:27:00: TAC+: req=62C81230 Tx id=3375296121 ver=192 handle=0x62C8424C (
ESTAB) expire=4 AUTHEN/CONT processed
Oct 11 12:27:00: TAC+: (3375296121) AUTHEN/CONT processed
Oct 11 12:27:00: TAC+: periodic timer stopped (queue empty)
Oct 11 12:27:00: TAC+: ver=192 id=3375296121 received AUTHEN status = GETPASS
Oct 11 12:27:04: TAC+: send AUTHEN/CONT packet id=3375296121
Oct 11 12:27:04: TAC+: periodic timer started
Oct 11 12:27:04: TAC+: 144.254.6.2 req=62C81230 Qd id=3375296121 ver=192 handl
e=0x62C8424C (ESTAB) expire=5 AUTHEN/CONT queued
Oct 11 12:27:04: TAC+: 144.254.6.2 (3375296121) AUTHEN/CONT queued
Oct 11 12:27:04: TAC+: 144.254.6.2 ESTAB id=3375296121 wrote 21 of 21 bytes
Oct 11 12:27:04: TAC+: 144.254.6.2 req=62C81230 Qd id=3375296121 ver=192 handl
e=0x62C8424C (ESTAB) expire=4 AUTHEN/CONT sent
Oct 11 12:27:05: TAC+: 144.254.6.2 ESTAB read=12 wanted=12 alloc=12 got=12
Oct 11 12:27:05: TAC+: 144.254.6.2 ESTAB read=18 wanted=18 alloc=18 got=6
Oct 11 12:27:05: TAC+: 144.254.6.2 received 18 byte reply for 62C81230
Oct 11 12:27:05: TAC+: req=62C81230 Tx id=3375296121 ver=192 handle=0x62C8424C (
ESTAB) expire=3 AUTHEN/CONT processed
Oct 11 12:27:05: TAC+: (3375296121) AUTHEN/CONT processed
Oct 11 12:27:05: TAC+: periodic timer stopped (queue empty)
Oct 11 12:27:05: TAC+: ver=192 id=3375296121 received AUTHEN status = PASS
Oct 11 12:27:05: TAC+: Closing TCP/IP 0x62C8424C connection to 144.254.6.2/49
R2#
```

Example 8-108 displays a successful login attempt. Notice that TCP packets are exchanged because TACACS+ runs over TCP.

Figure 8-4 displays the ACS configuration for AAA and TACACS+. ACS is an intuitive software application.

Figure 8-4 *Figure 8-4Configure Cisco ACS for TACACS+*

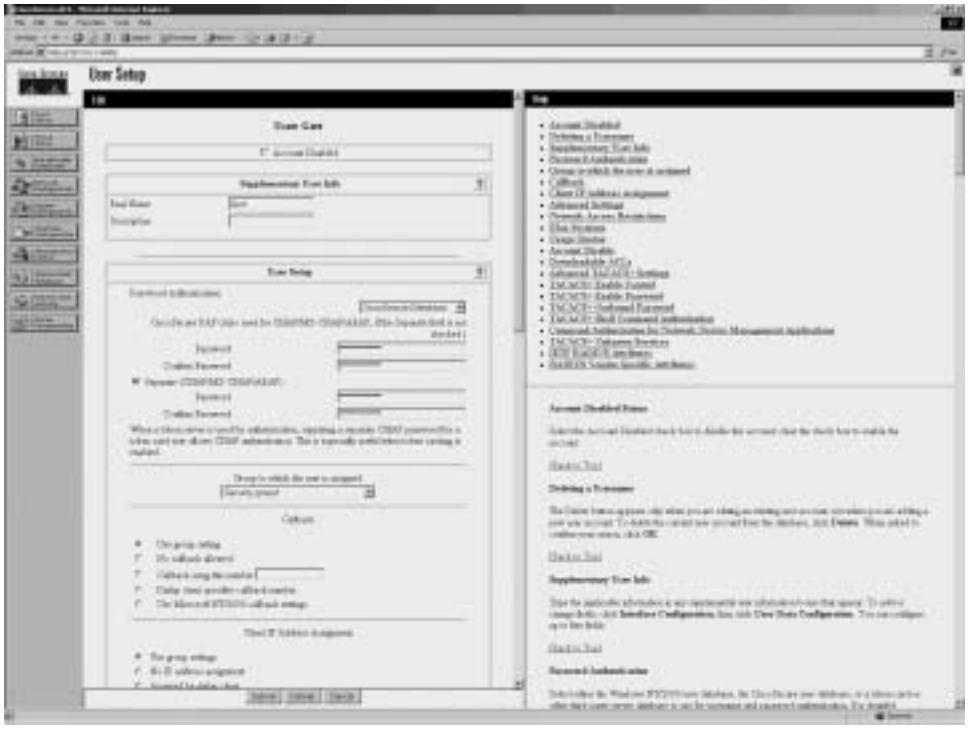


Figure 8-4 displays the creation of a remote username named “Gert” and password creation.

Figure 8-5 displays the ACS network configuration that allows Router R2 (IP address 144.254.152.1) to use the TACACS+ server daemon.

Figure 8-5 *TACACS+ Network Configuration*

ACS Configuration: Login Authentication Using RADIUS

Configure R3 to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database. Also, make sure the display "Enter your name:" is visible when logging in.

ACS Configuration: Login Authentication Using RADIUS Solution

RADIUS commands (similar to previous tasks on TACACS+) are as follows:

```
aaa new-model
aaa authentication login name group radius local
aaa authentication username-prompt "Enter your name:"

vty 0 4
login authentication name
```

Example 8-109 configures R3 for RADIUS authentication.

Example 8-109 *Login Authentication Using RADIUS*

```
hostname R3
!

aaa new-model
aaa authentication username-prompt "Enter your name:"
aaa authentication login radius group radius local
enable password cisco
!
username Gert password 0 gert
ip subnet-zero
!
<snip>
!
radius-server host 144.254.6.2 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key ccie
line vty 0 4
 login authentication radius
```

R3 must first be enabled for AAA and for the RADIUS server and RADIUS key.

Example 8-110 shows sample debug displays when a successful login attempt is made to R3. R2 is used to telnet to R3.

Example 8-110 *Telnet from R2 to R3*

```
R3#debug aaa authentication
AAA Authentication debugging is on
R3#show debugging
General OS:
  AAA Authentication debugging is on
Radius protocol debugging is on
R3#
R2#144.254.4.1
Trying 144.254.4.1 ... Open

Enter your name:Gert
Password: *****

R3>enable
Password:****
! Debug output follows
2d23h: AAA: parse name=tty66 idb type=-1 tty=-1
```

Example 8-110 *Telnet from R2 to R3 (Continued)*

```
2d23h: AAA: name=tty66 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=66 channe
l=0
2d23h: AAA/MEMORY: create_user (0x8271FE78) user='' ruser='' port='tty66' rem_ad
dr='144.254.4.2' authen_type=ASCII service=LOGIN priv=1
2d23h: AAA/AUTHEN/START (503012338): port='tty66' list='radius' action=LOGIN ser
vice=LOGIN
2d23h: AAA/AUTHEN/START (503012338): found list radius
2d23h: AAA/AUTHEN/START (503012338): Method=radius (radius)
2d23h: AAA/AUTHEN (503012338): status = GETUSER
2d23h: AAA/AUTHEN/CONT (503012338): continue_login (user='(undef)')
2d23h: AAA/AUTHEN (503012338): status = GETUSER
2d23h: AAA/AUTHEN (503012338): Method=radius (radius)
2d23h: AAA/AUTHEN (503012338): status = GETPASS
2d23h: AAA/AUTHEN/CONT (503012338): continue_login (user='Gert')
2d23h: AAA/AUTHEN (503012338): status = GETPASS
2d23h: AAA/AUTHEN (503012338): Method=radius (radius)
2d23h: RADIUS: ustruct sharecount=1
2d23h: RADIUS: Initial Transmit tty66 id 2 144.254.6.2:1645, Access-Request, l
en 76
2d23h:         Attribute 4 6 96640115
2d23h:         Attribute 5 6 00000042
2d23h:         Attribute 61 6 00000005
2d23h:         Attribute 1 6 47657274
2d23h:         Attribute 31 14 3135302E
2d23h:         Attribute 2 18 74DEA58C
2d23h: RADIUS: Received from id 2 144.254.6.2:1645, Access-Accept, len 20
2d23h: RADIUS: saved authorization data for user 8271FE78 at 826F6E2C
2d23h: AAA/AUTHEN (503012338): status = PASS
```

The successful user in Example 8-110 was authenticated by the RADIUS (ACS server) server.

Figure 8-6 displays the username creation on the ACS server.

Figure 8-6 *Username Creation on the ACS for RADIUS*

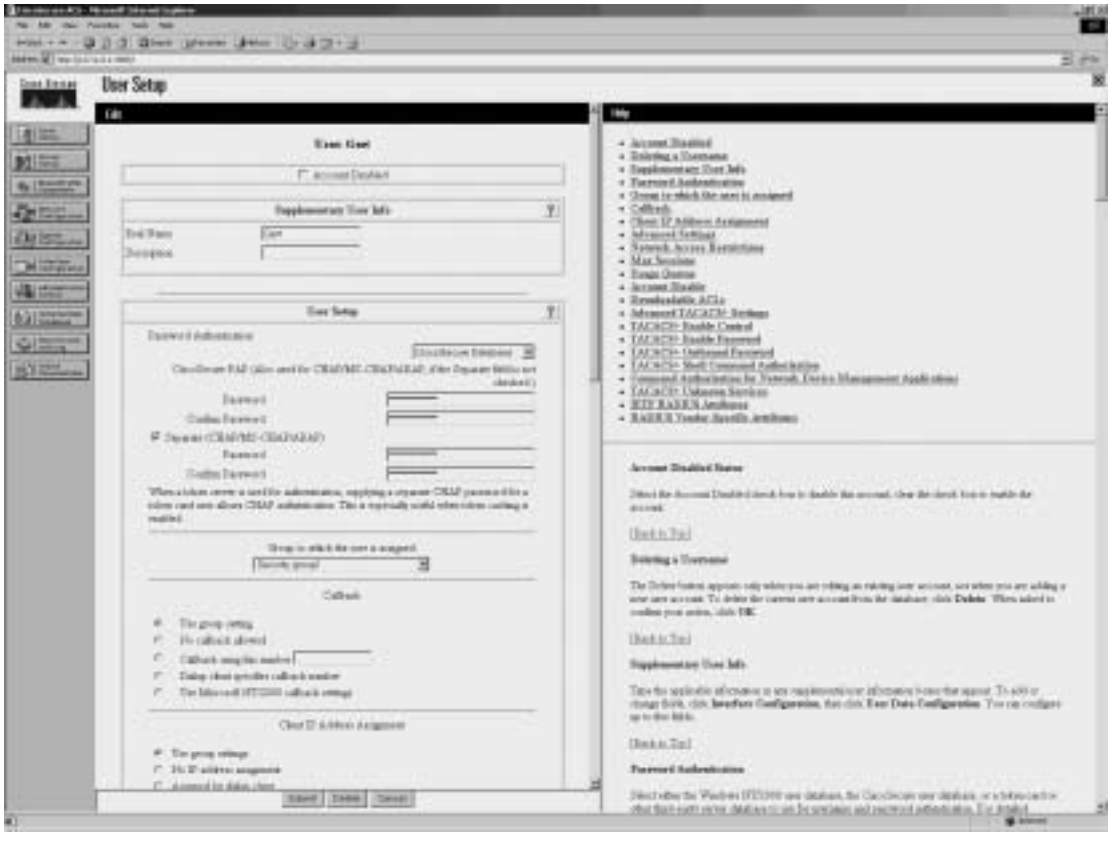
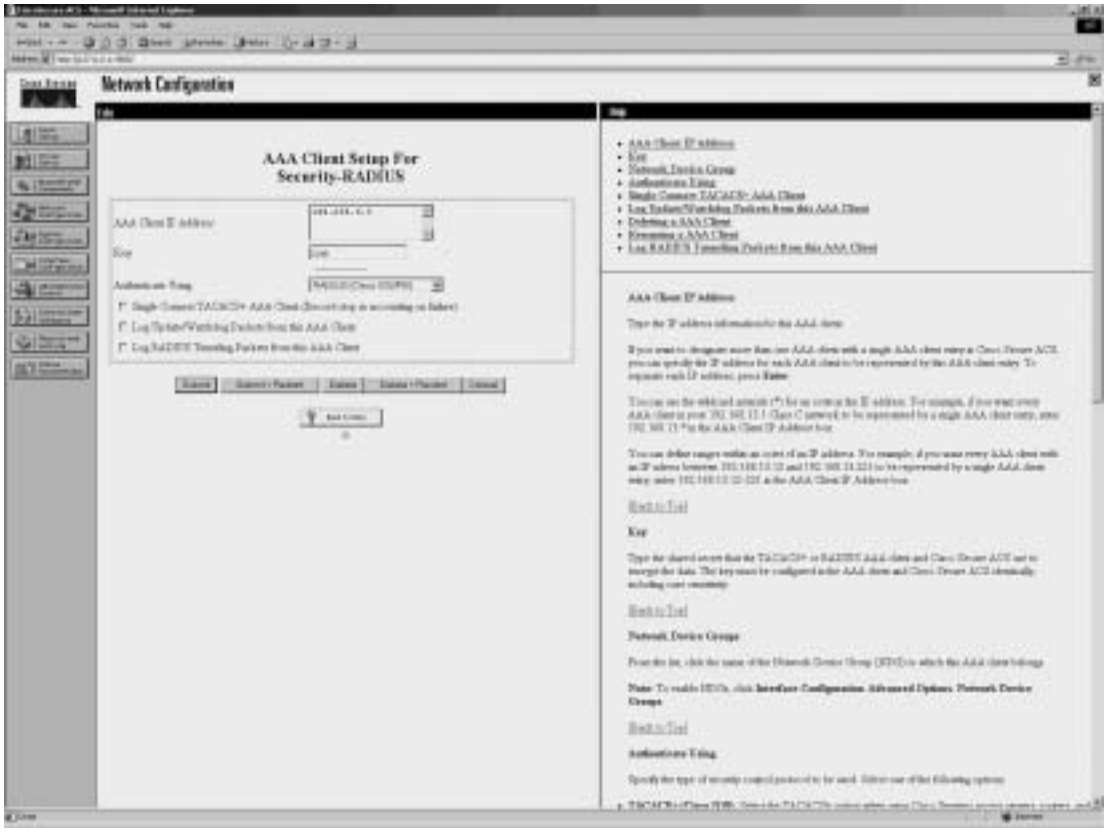


Figure 8-7 displays enabling RADIUS on the ACS server so that Router R3 can authenticate users.

Figure 8-7 *Radius Network Configuration*

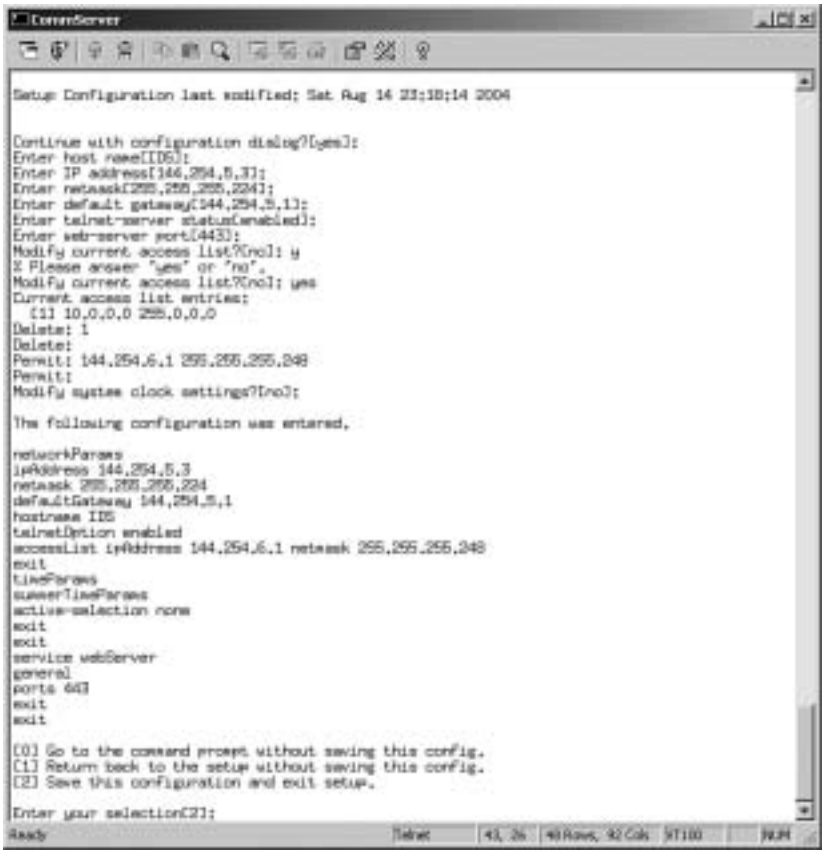


Cisco Intrusion Detection System (5 Points)

The Cisco intrusion detection system is connected to the inside interface of the PIX and the segment connecting R4 and R5.

The IDS in Figure 8-1 is configured for IP. Figure 8-8 displays all the details you need to complete this section.

Figure 8-8 *IDS Configuration*



The following list outlines key details to answer the lab exam questions:

- The IP address of the control interface is 144.254.5.3/27.
- The sniffing interface is connected to the PIX and R1 LAN.
- Ensure that only the subnet 144.254.6.0/29 can manage the IDS device.
- Change the custom signature 50000 to trigger a severity level of high when a Telnet session tries to change the password on any device. (By default, the IDS sniffing interface is shut down. You need to un-shut the interface to receive the spanned traffic.)

Cisco Intrusion Detection System Solution

The IDS sensor has the IP address 144.254.5.3. You need to web browse the IDS device by using HTTPs. The URL you must enter with your browser is:

https://144.254.5.3/

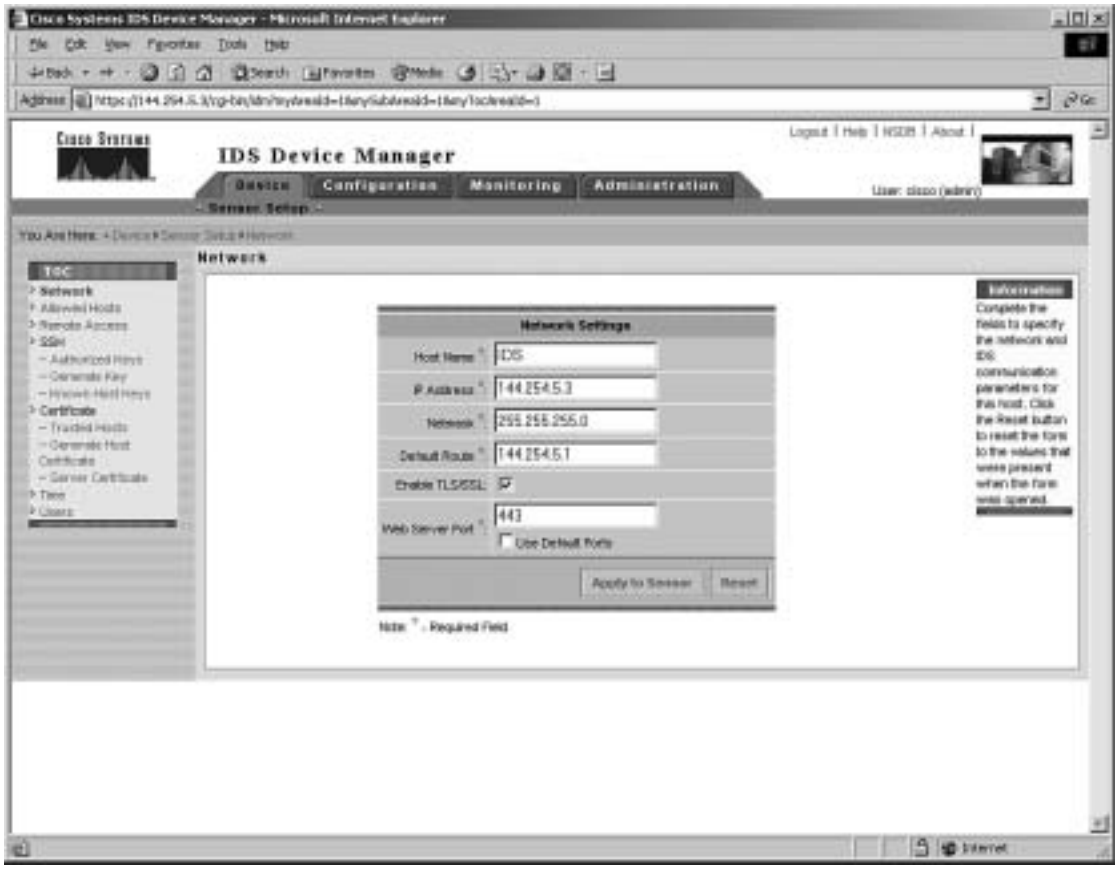
Figure 8-9 displays the opening screen after Internet Explorer (available in the CCIE lab) sessions to the IDS.

Figure 8-9 *IDS Device Manager Opening Screen*

Figure 8-9 displays the menu-driven welcome screen. Notice that the section labeled "You Are Here" advises you that your current screen location is the setting Device>Sensor Setup.

By clicking **Network**, you can confirm the IP address. Figure 8-10 confirms the correct IP address as 144.254.5.3/24.

Figure 8-10 *IDS Device Manager IP Address Confirmation*



Click **Allowed Hosts** to enter the permitted subnet 144.254.6.0/29 to manage the IDS, as Figure 8-11 confirms.

Figure 8-11 *IDS Device Manager Allowed Subnets/Hosts*

Finally, you need to create a custom IDS signature to monitor any IP packets that are changing the passwords on the network.

To create a custom signature, click the **Configuration** tab. Click **Signature Configuration Mode > Signature Wizard** on the left menu bar. Figure 8-12 displays the screen when creating a customized signature.

Figure 8-12 *Selecting the Signature Wizard*

The next eight figures display the simple procedure of creating a signature by following the intuitive steps the wizard walks you through.

Figure 8-13 displays the welcome screen when creating customized signatures. Click **Start the Wizard**.

Figure 8-13 *Custom Signature Wizard Welcome Screen*

Figure 8-14 displays the first wizard screen.

Figure 8-14 *Custom Signature Wizard First Screen*

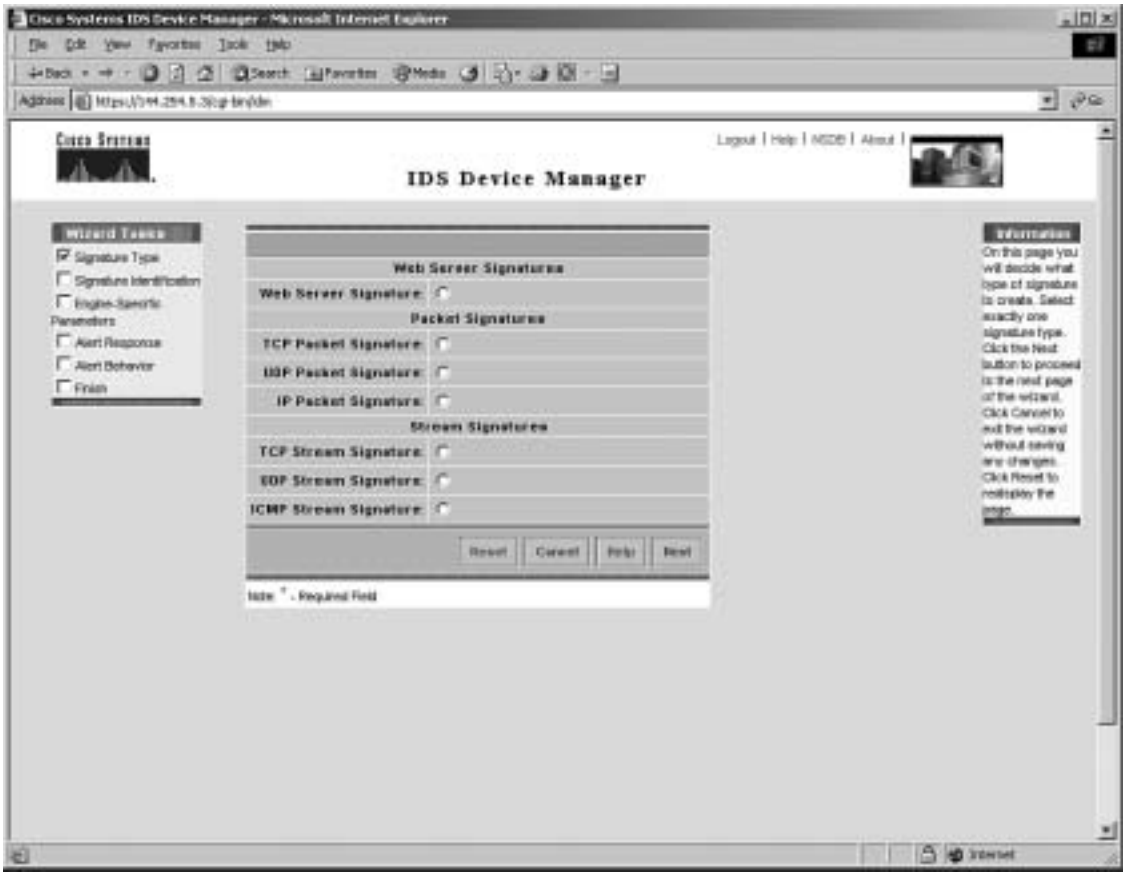


Figure 8-14 requires no changes; simply click the **Next** button to display the features available.

Figure 8-15 configures the IDS signature numbered 50000 and a random signature name of STRING.TCP.

Figure 8-15 *Custom Signature Wizard Signature Identification Screen*

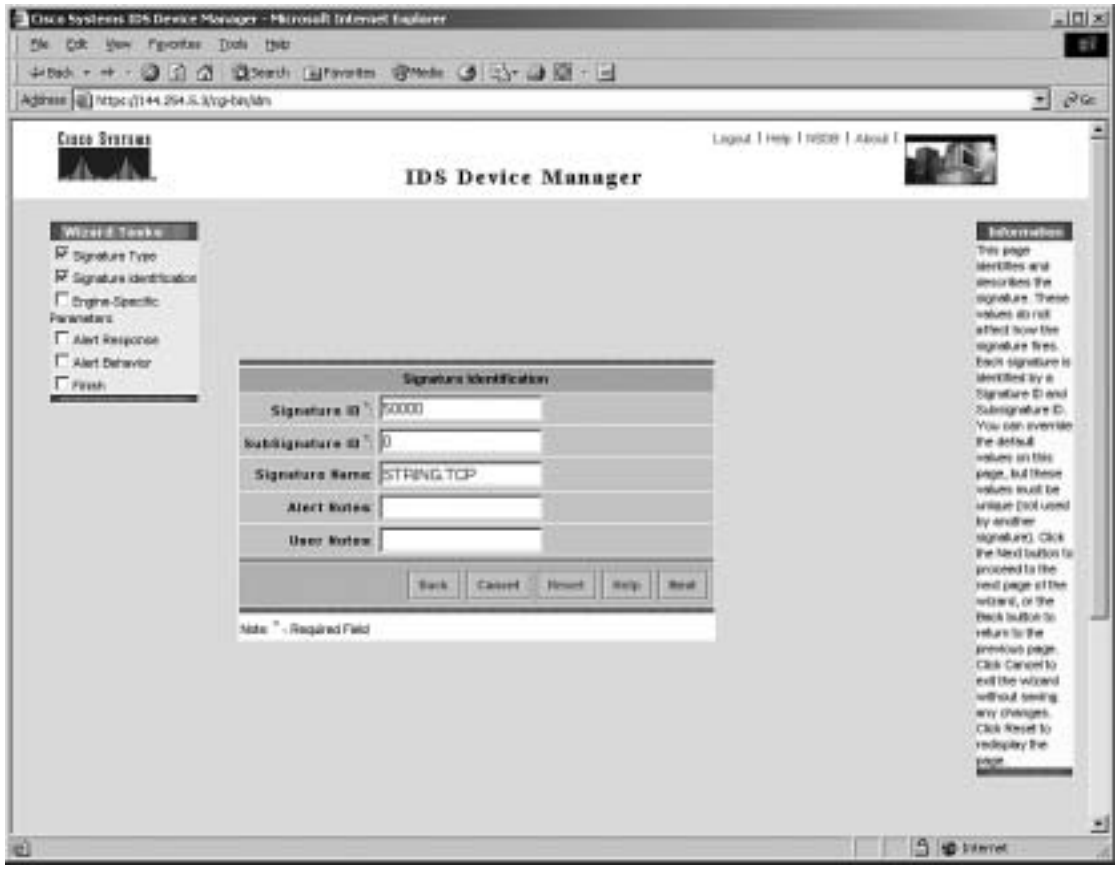


Figure 8-16 displays the configuration to alert administrators whenever the word "password" is shown in any Telnet connection. Cisco routers, for example, use the command **enable password** for setting the enable password, which will trigger an alert in this case.

Figure 8-16 *Custom Signature Wizard TCP Stream Signature Screen*

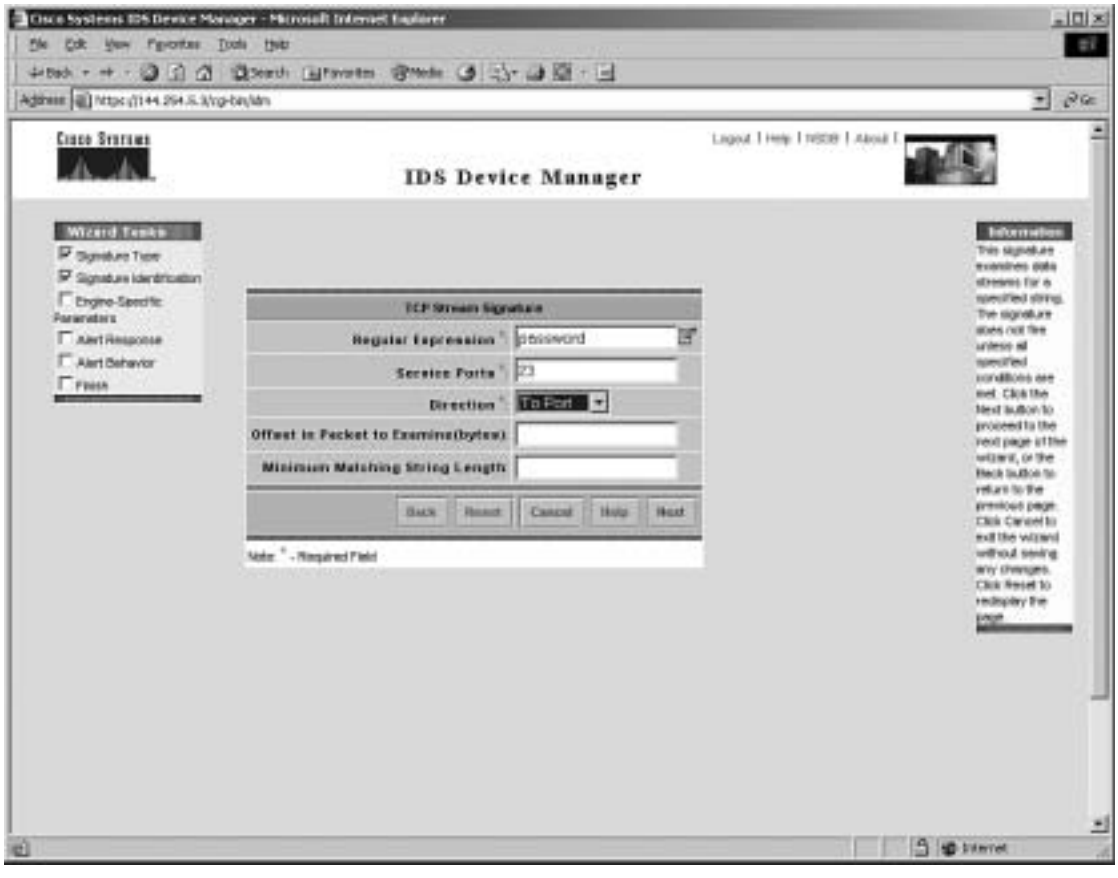
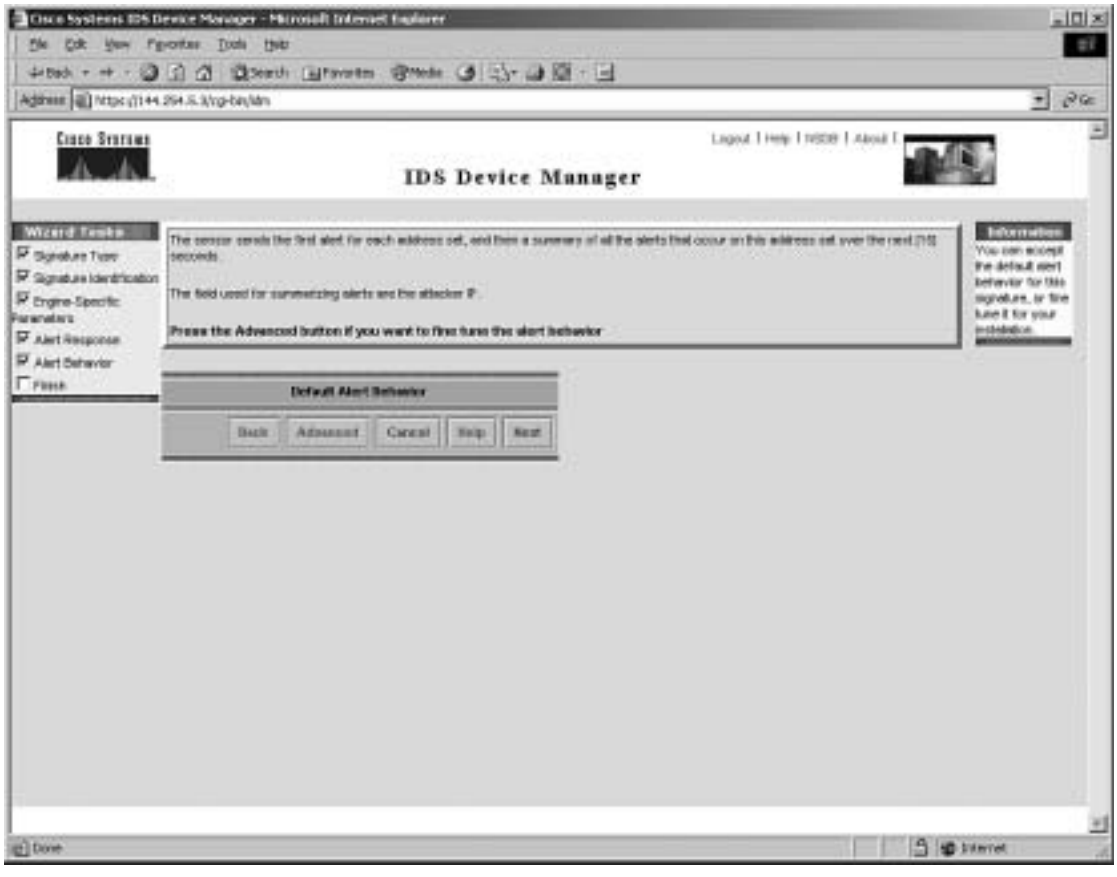


Figure 8-17 configures the severity level to **high** as required by this lab.

Figure 8-17 *Custom Signature Wizard Alert Response Actions Screen*

Figure 8-18 shows the alert behavior screen.

Figure 8-18 *Custom Signature Wizard*



Notice that the Wizard Tasks box on the left tracks your progress through the wizard as you advance through the screens. Advance through the next two screens to complete the final steps of the wizard. Figure 8-19 and Figure 8-20 confirm the wizard completion.

Figure 8-19 *Custom Signature Wizard Ready Confirmation Screen*

Figure 8-20 *Custom Signature Wizard Completion Screen*

Note that you must configure the switch port on the PIX inside interface to span (monitor or mirror) so that the IDS device can check all traffic. This completes the sample Security lab.

Final Configurations

Finally, all lab components have been completed. For your reference, here are the full working configuration files of all routers, the Catalyst 3550 switch, and the PIX Firewall. Please note that these configurations are a guide, and you might have found other correct solutions, as well. It is the end goal of every CCIE lab to provide a working solution, be it on routing, switching, security, or voice.

Example 8-111 displays the full working configuration for R1.

Example 8-111 *R1's Full Working Configuration*

```
Current configuration : 2627 bytes
version 12.1
service timestamps debug uptime
service timestamps log uptime
```

Example 8-111 *R1's Full Working Configuration (Continued)*

```
no service password-encryption
hostname R1
!
ip host R1 2001 144.254.151.1
ip host R2 2002 144.254.152.1
ip host R3 2003 144.254.153.1
ip host R4 2004 144.254.154.1
ip host R5 2005 144.254.155.1
ip host CAT5K 2008 144.254.151.1
ip host PIX 2015 144.254.151.1
enable password cisco
username cisco password 0 cisco
ip subnet-zero
no ip finger
ip tcp intercept list 100
no ip domain-lookup
ip domain-name cisco.com
ip host PIX 2015 144.254.151.1
!
ip audit notify log
ip audit po max-events 100
key chain cisco
 key 1
  key-string ccie
key chain eigrp
 key 1
  key-string ccie
call rsvp-sync
cns event-service server
!
interface Loopback0
 ip address 144.254.151.1 255.255.255.0
!
interface Loopback1
 ip address 131.108.1.1 255.255.255.0
!
interface Loopback2
 ip address 131.108.2.1 255.255.255.0
!
interface Loopback3
 ip address 131.108.3.1 255.255.255.0
!
interface Tunnel0
 ip unnumbered Serial0/1
 ip authentication mode eigrp 333
 ip authentication key-chain eigrp 333 eigrp
 tunnel source Serial0/1
```

continues

Example 8-111 *R1's Full Working Configuration (Continued)*

```
 tunnel destination 144.254.2.2
!
interface Ethernet0/0
 ip address 144.254.1.1 255.255.255.252
ip ospf authentication message-digest-key 1 md5 cisco
 ip ospf authentication-key cisco
 half-duplex
!
interface Serial0/0
 no ip address
 shutdown
!
interface Ethernet0/1
 no ip address
 shutdown
 half-duplex
!
interface Serial0/1
 ip address 144.254.2.1 255.255.255.252
 encapsulation frame-relay
 ip split-horizon
 ip summary-address eigrp 333 131.108.0.0 255.255.252.0 5
 frame-relay map ip 144.254.2.1 114
 frame-relay map ip 144.254.2.2 114
 frame-relay interface-dlci 102
 no frame-relay inverse-arp
!
router eigrp 333
 redistribute rip metric 1500 20000 255 1 1500
 passive-interface Ethernet0/0
 network 131.108.0.0
 network 144.254.0.0
 no auto-summary
 eigrp log-neighbor-changes
!
router rip
 version 2
 redistribute eigrp 333 metric 1
 passive-interface Serial0/1
 network 144.254.0.0
!
router bgp 333
 no synchronization
 bgp log-neighbor-changes
 network 144.254.151.0 mask 255.255.255.0
 neighbor 144.254.154.1 remote-as 333
 neighbor 144.254.154.1 update-source Loopback0
```

Example 8-111 *R1's Full Working Configuration (Continued)*

```
!
ip classless
no ip http server
!
access-list 100 permit ip any 144.254.1.0 0.0.0.3
!
line 1 16
transport input telnet
!
line con 0
 exec-timeout 0 0
 password cisco
 login
 transport input telnet
line aux 0
 exec-timeout 0 0
 password cisco
 login
 transport input telnet
line vty 0 4
 exec-timeout 0 0
 password cisco
 login local
 transport input telnet
!
end
```

Example 8-112 displays the full working configuration for R2.

Example 8-112 *R2's Full Working Configuration*

```
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R2
!
aaa new-model
username Erik access-class 1 password 0 Erik
username gert password 0 gert
aaa authentication login default local
aaa authentication password-prompt "Enter your password within 15 seconds:"
aaa authentication login default group tacacs+ local
enable password cisco
ip subnet-zero
no ip finger
```

continues

Example 8-112 *R2's Full Working Configuration (Continued)*

```
no ip domain-lookup
ip host r1 144.254.151.1
ip host r2 144.254.152.1
ip host r3 144.254.153.1
ip host r4 144.254.154.1
ip host r5 144.254.155.1
ip dhcp excluded-address 144.254.4.1
ip dhcp excluded-address 144.254.4.2
ip dhcp excluded-address 144.254.4.3
!
ip dhcp pool ccie
   network 144.254.4.0 255.255.255.192
   domain-name cisco.com
   default-router 144.254.4.1 144.254.4.2
   lease infinite
ip audit notify log
ip audit po max-events 100
frame-relay de-list 5 protocol ip gt 768
crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key CCiE address 144.254.3.1
crypto ipsec transform-set anyname1onR2 esp-des esp-sha-hmac
 mode transport
crypto map anyname 1 ipsec-isakmp
 set peer 144.254.3.1
 set security-association lifetime seconds 300
 set transform-set anyname1onR2
 match address 150
!
call rsvp-sync
cns event-service server
interface Loopback0
 ip address 144.254.152.1 255.255.255.0
 ip ospf network point-to-point
!
interface FastEthernet0/0
 ip address 144.254.4.2 255.255.255.192
 ip ospf hello-interval 20
 ip ospf priority 0
 half-duplex
!
interface Serial0/0
 ip address 144.254.3.2 255.255.255.240
 encapsulation frame-relay
ip ospf authentication message-digest-key 1 md5 cisco
 ip ospf authentication-key cisco
```

Example 8-112 *R2's Full Working Configuration (Continued)*

```
ip ospf hello-interval 25
 ip ospf priority 0
 frame-relay map ip 144.254.3.1 204 broadcast
 frame-relay map ip 144.254.3.2 204 broadcast
 frame-relay map ip 144.254.3.3 204 broadcast
 frame-relay interface-dlci 204
 no frame-relay inverse-arp
 frame-relay lmi-type ansi
 crypto map anyname
!
!
router ospf 1
 router-id 144.254.152.1
 log-adjacency-changes
ip ospf message-digest-key 1 md5 cisco
ip ospf message-digest-key 1 md5 cisco

 network 144.254.3.2 0.0.0.0 area 0
 network 144.254.4.2 0.0.0.0 area 333
 network 144.254.152.1 0.0.0.0 area 0
!
router bgp 333
 no synchronization
 bgp log-neighbor-changes
 network 144.254.152.0 mask 255.255.255.0
 neighbor 144.254.154.1 remote-as 333
 neighbor 144.254.154.1 password cisco
 neighbor 144.254.154.1 update-source Loopback0
!
ip classless
no ip http server
access-list 1 permit 144.254.4.0
access-list 150 permit ip any any
tacacs-server host 144.254
tacacs-server key ccie
dial-peer cor custom
line con 0
 exec-timeout 0 0
 password cisco
 login
 transport input telnet
line aux 0
 exec-timeout 0 0
 password cisco
 login
 transport input telnet
```

continues

Example 8-112 *R2's Full Working Configuration (Continued)*

```
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
 transport input telnet
!
end
```

Example 8-113 displays the full working configuration for R3.

Example 8-113 *R3's Full Working Configuration*

```
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname R3
logging rate-limit console 10 except errors
enable password cisco
username Gert password 0 gert
username R5 password 0 cisco
ip subnet-zero
aaa new-model
aaa authentication username-prompt "Enter your name:"
aaa authentication login radius group radius local
no ip finger
no ip domain-lookup
ip host r5 144.254.155.1
ip host r4 144.254.154.1
ip host r3 144.254.153.1
ip host r2 144.254.152.1
ip host r1 144.254.151.1
ip audit notify log
ip audit po max-events 100
frame-relay de-list 5 protocol ip gt 768
crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key CCiE address 144.254.3.1
crypto ipsec transform-set anyname1onR3 esp-des esp-sha-hmac
 mode transport
crypto map anyname 1 ipsec-isakmp
 set peer 144.254.3.1
 set security-association lifetime seconds 300
 set transform-set anyname1onR3
 match address 150
```

Example 8-113 *R3's Full Working Configuration (Continued)*

```
isdn switch-type basic-5ess
call rsvp-sync
cns event-service server
interface Loopback0
 ip address 144.254.153.1 255.255.255.0
 ip ospf network point-to-point
!
interface FastEthernet0/0
 ip address 144.254.4.1 255.255.255.192
 ip access-group 100 in
 ip ospf hello-interval 20
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 144.254.3.3 255.255.255.240
encapsulation frame-relay
 ip split-horizon
ip ospf authentication message-digest-key 1 md5 cisco
 ip ospf authentication-key cisco
 ip ospf hello-interval 25
 ip ospf priority 0
 frame-relay map ip 144.254.3.1 304 broadcast
 frame-relay map ip 144.254.3.2 304 broadcast
 frame-relay map ip 144.254.3.3 304 broadcast
 frame-relay interface-dlci 304
 no frame-relay inverse-arp
 crypto map anyname
!
interface BRI0/0
 description 7775010
 ip address 144.254.7.1 255.255.255.252
 encapsulation ppp
ip ospf authentication message-digest-key 1 md5 cisco
ip ospf authentication-key cisco
 ip ospf demand-circuit
 dialer map ip 144.254.7.2 name R5 broadcast 7775020
 dialer load-threshold 165 either
 dialer-group 1
 isdn switch-type basic-5ess
 no peer neighbor-route
 ppp quality 80
 ppp authentication chap
 ppp multilink
!
router ospf 1
 router-id 144.254.153.1
```

continues

Example 8-113 *R3's Full Working Configuration (Continued)*

```
 log-adjacency-changes
 ip ospf message-digest-key 1 md5 cisco
 ip ospf message-digest-key 1 md5 cisco

 network 144.254.3.3 0.0.0.0 area 0
 network 144.254.4.1 0.0.0.0 area 333
 network 144.254.4.2 0.0.0.0 area 333
 network 144.254.7.1 0.0.0.0 area 0
 network 144.254.153.1 0.0.0.0 area 0
!
router bgp 333
 no synchronization
 bgp log-neighbor-changes
 network 144.254.153.0 mask 255.255.255.0
 neighbor 144.254.154.1 remote-as 333
 neighbor 144.254.154.1 update-source Loopback0
!
ip classless
no ip http server
!
access-list 100 dynamic blockping timeout 5 permit icmp host 144.254.4.2 host 14
4.254.4.1
access-list 100 deny   icmp host 144.254.4.2 host 144.254.4.1 echo
access-list 100 permit ip any any
access-list 150 permit ip any any
dialer-list 1 protocol ip permit
radius-server host 144.254.6.2 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key ccie
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input none
line aux 0
 exec-timeout 0 0
 password cisco
 login
 transport input telnet
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
 autocommand  access-enable host timeout 5
```

Example 8-113 *R3's Full Working Configuration (Continued)*

```
 transport input telnet
!
no scheduler allocate
end
```

Example 8-114 displays the full working configuration for R4.

Example 8-114 *R4's Full Working Configuration*

```
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname R4
logging rate-limit console 10 except errors
enable password cisco
ip subnet-zero
no ip finger
no ip domain-lookup
ip host r1 144.254.151.1
ip host r2 144.254.152.1
ip host r3 144.254.153.1
ip host r4 144.254.154.1
ip host r5 144.254.155.1
ip audit notify log
ip audit po max-events 100
crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key CCiE address 144.254.3.2
crypto isakmp key CCiE address 144.254.3.3
crypto ipsec transform-set anyname1 esp-des esp-sha-hmac
 mode transport
crypto map anyname 1 ipsec-isakmp
 set peer 144.254.3.2
 set peer 144.254.3.3
 set security-association lifetime seconds 300
 set transform-set anyname1
 match address 150
key chain eigrp
 key 1
  key-string ccie
call rsvp-sync
cns event-service server
!
interface Loopback0
```

continues

Example 8-114 *R4's Full Working Configuration (Continued)*

```
 ip address 144.254.154.1 255.255.255.0
 ip ospf network point-to-point
!
interface Tunnel0
 ip unnumbered Serial0/1
 ip authentication mode eigrp 333 md5
 ip authentication key-chain eigrp 333 eigrp
 tunnel source Serial0/1
 tunnel destination 144.254.2.1
!
interface Ethernet0/0
 ip address 144.254.5.1 255.255.255.224
 ip ospf hello-interval 60
 half-duplex
!
interface Serial0/0
 ip address 144.254.3.1 255.255.255.240
 encapsulation frame-relay
ip ospf authentication message-digest-key 1 md5 cisco
 ip ospf authentication-key cisco
ip ospf hello-interval 25
 ip ospf priority 255
 frame-relay map ip 144.254.3.1 402
 frame-relay map ip 144.254.3.2 402 broadcast
 frame-relay map ip 144.254.3.3 403 broadcast
 frame-relay interface-dlci 402
 frame-relay interface-dlci 403
 no frame-relay inverse-arp
 frame-relay lmi-type ansi
 crypto map anyname
!
!
interface Serial0/1
 ip address 144.254.2.2 255.255.255.252
 encapsulation frame-relay
 ip split-horizon
 frame-relay map ip 144.254.2.1 411
 frame-relay map ip 144.254.2.2 411
 frame-relay interface-dlci 201
 no frame-relay inverse-arp
!
router eigrp 333
 redistribute ospf 1 metric 1544 20000 255 1 1500
 passive-interface Ethernet0/0
 passive-interface Serial0/0
 passive-interface Loopback0
 network 144.254.0.0
```

Example 8-114 *R4's Full Working Configuration (Continued)*

```
 no auto-summary
 no eigrp log-neighbor-changes
!
router ospf 1
 router-id 144.254.154.1
 log-adjacency-changes
 ip ospf message-digest-key 1 md5 cisco
 ip ospf message-digest-key 1 md5 cisco

 area 4 virtual-link 144.254.155.1
 redistribute eigrp 333 metric 100 metric-type 1 subnets
 network 144.254.3.1 0.0.0.0 area 0
 network 144.254.5.1 0.0.0.0 area 4
 network 144.254.154.1 0.0.0.0 area 0
 neighbor 144.254.3.3
 neighbor 144.254.3.2
!
router bgp 333
 no synchronization
 bgp log-neighbor-changes
 network 144.254.154.0 mask 255.255.255.0
 neighbor 144.254.151.1 remote-as 333
 neighbor 144.254.151.1 update-source Loopback0
 neighbor 144.254.151.1 route-reflector-client
 neighbor 144.254.152.1 remote-as 333
 neighbor 144.254.152.1 password cisco
 neighbor 144.254.152.1 update-source Loopback0
 neighbor 144.254.152.1 route-reflector-client
 neighbor 144.254.153.1 remote-as 333
 neighbor 144.254.153.1 update-source Loopback0
 neighbor 144.254.153.1 route-reflector-client
 neighbor 144.254.155.1 remote-as 333
 neighbor 144.254.155.1 update-source Loopback0
 neighbor 144.254.155.1 route-reflector-client
!
ip classless
no ip http server
access-list 150 permit ip any any
dial-peer cor custom
!
line con 0
 exec-timeout 0 0
 password cisco
 login
 transport input telnet
line aux 0
```

continues

Example 8-114 *R4's Full Working Configuration (Continued)*

```
 exec-timeout 0 0
 password cisco
 login
 transport input telnet
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
 transport input telnet
!
end
```

Example 8-115 displays the full working configuration for R5.

Example 8-115 *R5's Full Working Configuration*

```
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname R5
logging rate-limit console 10 except errors
enable password cisco
username R5 password 0 cisco
username R3 password 0 cisco
ip subnet-zero
no ip finger
no ip domain-lookup
ip host r5 144.254.155.1
ip host r4 144.254.154.1
ip host r3 144.254.153.1
ip host r2 144.254.152.1
ip audit notify log
ip audit po max-events 100
isdn switch-type basic-5ess
interface Loopback0
 ip address 144.254.155.1 255.255.255.0
 ip ospf network point-to-point
interface FastEthernet0/0
 ip address 144.254.5.2 255.255.255.224
 ip access-group 100 out
 ip ospf hello-interval 60
 duplex auto
 speed auto
!
!
interface BRI0/0
```

Example 8-115 *R5's Full Working Configuration (Continued)*

```
 description 7775020
 ip address 144.254.7.2 255.255.255.252
 encapsulation ppp
ip ospf authentication message-digest-key 1 md5 cisco
 ip ospf authentication-key cisco
Ciscodialer load-threshold 165 either
 dialer map ip 144.254.7.1 name R3 broadcast
 dialer-group 1
 isdn switch-type basic-5ess
 no peer neighbor-route
 ppp authentication chap callin
 ppp multilink
!
interface FastEthernet0/1
 ip address 144.254.6.1 255.255.255.248
 ip access-group 101 in
 ip access-group web-traffic out
 ip inspect OUTBOUND in
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
!
router ospf 1
 router-id 144.254.155.1
 log-adjacency-changes
 ip ospf message-digest-key 1 md5 cisco
 ip ospf message-digest-key 1 md5 cisco

 area 4 virtual-link 144.254.154.1
 network 144.254.5.2 0.0.0.0 area 4
 network 144.254.6.1 0.0.0.0 area 5
 network 144.254.7.2 0.0.0.0 area 0
 network 144.254.155.1 0.0.0.0 area 4
!
router bgp 333
 no synchronization
 bgp log-neighbor-changes
 network 144.254.155.0 mask 255.255.255.0
 neighbor 144.254.154.1 remote-as 333
!
ip classless
no ip http server
ip access-list extended web-traffic
```

continues

Example 8-115 *R5's Full Working Configuration (Continued)*

```
 deny   tcp any any time-range web-timing
 permit ip any any
access-list 100 deny   tcp 129.57.140.0 0.0.64.255 any log
access-list 100 deny   tcp 161.133.29.0 64.0.0.0 any log
access-list 100 deny   tcp 182.133.0.0 0.0.255.255 any log
access-list 100 permit ip any any log
access-list 101 permit ip 0.0.0.0 255.255.255.192 any
dialer-list 1 protocol ip permit
dial-peer cor custom
line con 0
 exec-timeout 0 0
 password cisco
 login
 transport input telnet
line aux 0
 exec-timeout 0 0
 password cisco
 login
 transport input telnet
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
 transport input telnet
!
!
end
```

Example 8-116 displays the full working configuration for the PIX Firewall.

Example 8-116 *PIX Firewall Full Working Configuration*

```
PIX Version 5.2(3)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX1
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
pager lines 24
```

Example 8-116 *PIX Firewall Full Working Configuration*

```
logging on
no logging timestamp
no logging standby
no logging console
no logging monitor
no logging buffered
no logging trap
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
icmp permit any inside
mtu outside 1500
mtu inside 1500
ip address outside 9.1.1.1 255.255.255.0
ip address inside 144.254.1.2 255.255.255.252
ip audit name Attack-inside attack action alarm reset
ip audit name Information-inside info action alarm drop
ip audit name Attack-outside attack action alarm drop
ip audit interface outside Attack-inside
ip audit interface inside Information-inside
ip audit interface inside Attack-outside
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
rip outside passive version 1
rip inside passive version 2 authentication md5 ccie 1
rip inside default version 2 authentication md5 ccie 1
route outside 0.0.0.0 0.0.0.0 9.1.1.2
route inside 144.254.0.0 255.255.0.0 144.254.1.1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 si
p 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
```

continues

Example 8-116 *PIX Firewall Full Working Configuration*

```
floodguard enable
no sysopt route dnat
isakmp identity hostname
telnet 144.254.1.1 255.255.255.255 inside
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:7827bfd3d2885989e9a789c8c9a4c6d6
: end
```

Example 8-117 displays the full working configuration for the Catalyst 3550 switch configuration.

Example 8-117 *Catalyst 3550 Switch Configuration*

```
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname switch
!
enable password cisco
!
ip subnet-zero
ip routing
spanning-tree extend system-id
!
!
interface FastEthernet0/1
Description connection to R1 Ethernet 0/0
!The following commands assigns the VLAN
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security violation shutdown
 storm-control broadcast level 50.00
 duplex Full

!
interface FastEthernet0/2
Description connection to R2 Fast Ethernet 0/0
 switchport access vlan 5
 switchport mode access
 switchport port-security
```

Example 8-117 *Catalyst 3550 Switch Configuration (Continued)*

```
 switchport port-security violation shutdown
 storm-control broadcast level 50.00
 duplex full

!
interface FastEthernet0/3
Description connection to R3 Fast Ethernet 0/0
 switchport access vlan 5
 switchport mode access
 switchport port-security
 switchport port-security violation shutdown
 storm-control broadcast level 50.00
!
interface FastEthernet0/4
Description connection to R4 Ethernet 0/0
 switchport access vlan 3
 switchport mode access
 switchport port-security
 switchport port-security violation shutdown
 storm-control broadcast level 50.00
 duplex full
!
interface FastEthernet0/5
Description connection to R5 Fast Ethernet 0/0
 switchport access vlan 3
 switchport mode access
 witchport port-security
 switchport port-security violation shutdown
 storm-control broadcast level 50.00
!
interface FastEthernet0/6
Description connection to R5 Ethernet 0/1
 switchport access vlan 4
 switchport mode access
 switchport port-security
 switchport port-security violation shutdown
 storm-control broadcast level 50.00
!
interface FastEthernet0/7
Description connection to PIX inside
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security violation shutdown
 storm-control broadcast level 50.00
!
```

continues

Example 8-117 *Catalyst 3550 Switch Configuration (Continued)*

```
interface FastEthernet0/8
Description connection to PIX outside
 switchport access vlan 6
 switchport mode access
 switchport port-security
 switchport port-security violation shutdown
 storm-control broadcast level 50.00

! Note interfaces 9 and 10 not used here
interface FastEthernet0/9
no ip address
shutdown
 switchport port-security
 switchport port-security violation shutdown
 storm-control broadcast level 50.00

!
interface FastEthernet0/10
no ip address
shutdown
 switchport port-security
 switchport port-security violation shutdown
 storm-control broadcast level 50.00

!
interface FastEthernet0/11
Description connection IDS control
 switchport access vlan 3
 switchport mode access
 switchport port-security
 switchport port-security violation shutdown
 storm-control broadcast level 50.00

interface FastEthernet0/12
Description connection to IDS sniffing
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security violation shutdown
 storm-control broadcast level 50.00

!
interface GigabitEthernet0/1
 no ip address

interface GigabitEthernet0/2
```

Example 8-117 *Catalyst 3550 Switch Configuration (Continued)*

```
 no ip address
!
interface Vlan1
 no ip address
!
interface Vlan5
 ip address 144.254.4.3 255.255.255.192
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 144.254.4.2
ip route 0.0.0.0 0.0.0.0 144.254.4.1 100
no ip http server
!
!
access-list 5 permit 144.254.151.1
access-list 5 permit 144.254.152.2
access-list 5 permit 144.254.153.3
access-list 5 permit 144.254.154.4
access-list 5 permit 144.254.155.5
access-list 5 permit 144.254.4.0 0.0.0.64
!
line vty 0 4
 access-class 5 in
 password cisco
 login
line vty 5 15
 access-class 5 in
 password cisco
 login
end
```

NOTE The routers in this network were Cisco 2600 and 3600 series. The switch was a Cisco Catalyst 3550 switch. In theory, you can use any Cisco IOS router, switch, IDS, and PIX Firewall. You can easily replace your lab switch with any switch running native IOS. For example, a 3750 or 6506 works if you are lucky enough to have one in your test lab.

Additional Advanced Lab Topics (No Solutions Provided)

Presented here are some advanced CCIE Security questions with no lab solutions so that you may investigate and try to solve them on your own, just as you would have to do in the lab exam. These bonus CCIE Security lab topics are added because they are not covered in the main section of this chapter. Hopefully they will provide you with some example questions and help you discover your own exam techniques to help you achieve maximum success in the CCIE Security lab.

In every CCIE lab exam that I have attempted, and I have been through many of them, I have found that a candidate must be capable of addressing topics they have not configured or studied prior to the lab; in essence, you must be prepared to use the Documentation CD-ROM to help you past the topics you are not comfortable with. So in keeping with the high level of difficulty of any CCIE exam, here are some bonus advanced questions with an indicative point score you could expect in any CCIE lab exam. (These points do not count toward the main lab already presented.) Research them and try to implement solutions. Ensure that you read the question carefully, because they have some hidden traps representative of most CCIE lab exams. Enjoy them!

Advanced Security Lab Topics (4 Points)

Configure IPSec LAN-to-LAN connectivity between the PIX Firewall and R1. The only traffic to be encrypted between these two devices should be traffic using UDP port number 45555. Ensure that the IPSec frame format is the most secure format available, where data is encrypted, not just authenticated.

Content Filtering (2 Points)

Set up the PIX to make sure that the protected network behind the PIX cannot receive Java or ActiveX applets.

FTP Issues (3 Points)

There are PC clients both behind and in front of the PIX Firewall that are reporting slow FTP connection times going across the PIX. Upon investigation, it is noted that there is a port 113 request coming from some FTP servers.

This results in an approximately 2-minute lag in connection times, but files do eventually load.

Ensure that the PIX is configured to address this major issue with regard to slowness.

Routing Table Authenticity (4 Points)

Ensure that router R1 forwards only the packets that have a source address found in its routing table. Ensure that packets that do not meet this requirement are logged.

Ensure also that packets from the RFC 1918 address space are dropped and logged also.

Access Control on R2 Ethernet Interface (4 Points)

Configure an extended named access list on R2's Ethernet interface blocking traffic from the outside that satisfies the following criteria:

- Routing protocol traffic is permitted.
- Ensure that World Wide Web and FTP traffic is permitted both ways.
- ICMP is permitted one way only. Assume R2 sends the ping request.
- Telnet sessions are permitted only from outside to hosts on VLAN 5, and only for an employee with the username of henrytripleccie. This access should not remain in place indefinitely.
- All other incoming traffic is denied and logged.

Conclusion

You should be able to complete this CCIE Security self-study lab within 8 hours. The difficulty level presented here is the very minimum of what you can expect in any CCIE lab exam. Focus your attention on time management and your ability to configure a number of IOS features quickly. If you can complete this lab successfully, modify the tasks and try again. Change the IP routing algorithm, for example, or configure the PIX for IPSec termination from the Internet. Make sure you are familiar with Cisco ACS and are comfortable with TACACS+ and RADIUS, IDS devices, and VPN Concentrators. Ensure that you stay informed about changes made to the lab blueprint; typically, recent new IOS enhancements are incorporated in CCIE lab exams within 6 months.

You should plan for 10-20 percent of any lab exam to really test your skill set. If you are not experienced enough and you cannot confidently complete this lab, consider taking more time to study before investing your hard-earned money.

Your ability to complete any design scenario is what will ensure that you are a master of CCIE, rather than someone who has just passed an 8-hour exam. In today's environment, being a CCIE might not be marketable enough. Demonstrating to a prospective employer your skills of designing any network topology in any network condition will ensure that you are ahead of the rest.

Best of luck to you in your endeavors to become a CCIE Security expert and beyond. When you do pass the exam, please e-mail me at henry.benjamin@optusnet.com so that I, too, can share in your great accomplishment.


Catalyst 6500

APPENDIX A

Answers to Quiz Questions

Chapter 1

Do I Know This Already?

1. Which layer of the OSI model is responsible for converting frames into bits and bits into frames?

   Answer: e. Data link

   The data link layer performs bit conversion to pass to the MAC sublayer.

2. Routing occurs at which layer of the OSI model?

   Answer: b.Network

   Routing is a Layer 3 (network layer) function.

3. Bridging occurs at which layer of the OSI model?

   Answer: d. Data link

   The data link layer is where bridging is performed.

4. Which of the following is not part of the OSI model?

   Answer: c. Operational layer

   The operational layer is not one of the seven OSI layers. The OSI model layers are physical, data link, network, transport, session, presentation, and application.

5. IP operates at which layer of the OSI model?

   Answer: c. Layer 3

   IP operates at the network layer (Layer 3) and provides a path to a destination.

6. On which layer of the OSI model is data commonly referred to as segments?

   Answer: a. Layer 4

   The data on Layer 4 is commonly referred to as segments.

7. On which layer of the OSI model is data commonly referred to as packets?

   Answer: d. Layer 3

   The data on Layer 3 is commonly referred to as packets.

8. Which layer of the OSI model transmits raw bits?

   Answer: a. Layer 1

   At Layer 1, the lowest layer of the OSI model, bits are transferred across the wire.

9. Which of the following protocols is *not* routable?

   Answer: c. NetBEUI

   NetBEUI is not a routed protocol and must be bridged.

10. Which of the following is *not* a required step to enable Fast EtherChannel (FEC)?

    Answer: a. Ensure that all ports share the same speed at 10 Mbps.

    FEC uses full-duplex Fast Ethernet (100 Mbps) links.

11. How is Fast EtherChannel best defined?

    Answer: d. The ability to bundle 100-Mbps ports into a logical link

    The Fast EtherChannel feature bundles 100-Mbps Fast Ethernet ports into a logical link between two devices, such as Catalyst switches.

12. On what OSI layer does bridging occur?

    Answer: b. Layer 2

    Bridging occurs at the data link layer (Layer 2) of the OSI model.

13. In the spanning tree protocol, what is a BPDU?

    Answer: c. A bridge protocol data unit

14. An incoming frame on a Layer 2 switch is received on port 10/1 on a Catalyst 5000. If the destination address is known through port 10/2, what happens?

Answer: b. The frame is sent via port 10/2.

The destination MAC address has already been discovered through port 10/2, so the frame will be sent only to the known port or slot 10, port 2.

15. Which of the following are the four possible states of spanning tree?

Answer: d. Listening, learning, blocking, forwarding

16. How many bits make up an IP address?

Answer: c. 32 bits

17. Identify the broadcast address for the subnet 131.108.1.0/24.

Answer: c. 131.108.1.255

131.108.1.0/24 is a Class B address with a Class C mask, and the all (all binary 1s) broadcast address is 131.108.1.255 (11111111).

18. Convert the address 131.1.1.1/24 to binary:

Answer: a. 10000011.1.1.1

131.108.1.1 in binary is 10000011.00000001.00000001.00000001 or 10000011.1.1.1

19. How many subnets are possible in VLSM if the Class C address 131.108.255.0 is used with the subnet mask 255.255.255.252 in the fourth octet field? (Allow for subnet zero.)

Answer: h. 64

$2^6 = 64$. This allows for subnet zero. If subnet zero is not permitted, then 62 subnets would be available.

20. How many hosts are available when a /26 subnet mask is used?

Answer: b. 62

$2^6 - 2 = 64 - 2 = 62$.

21. How many hosts are available in a Class C or /24 network?

Answer: b. 254

A Class C or /24 network has $2^8 - 2 = 256 - 2 = 254$ addresses available for host devices.

22. You require an IP network to support, at most, 62 hosts. What subnet mask will accomplish this requirement?

Answer: d. 255.255.255.192

62 hosts require 62 + 2 = 64 addresses. This IP Network needs 6 bits borrowed from the subnet mask. In binary, that number is 11000000.

23. Which of the following are multicast addresses? (Choose all that apply.)

Answers: a. 224.0.0.5

b. 2240.0.6

224.0.0.5 and 224.0.0.6 are multicast addresses.

24. Which of the following routing protocols does not support VLSM?

Answer: a. RIPv1

RIP version 1 is classful and does not carry subnet masks in routing updates.

25. What is the source TCP port number when a Telnet session is created by a PC to a Cisco router?

Answer: b. A value higher than 1024

The source TCP port is a random number above 1024 (1025–65535); the destination port is 23.

26. What best describes the ARP process?

Answer: b. Mapping an IP address to a MAC address

27. If two Cisco routers are configured for HSRP and one router has a default priority of 100 and the other 99, which router assumes the role of active router?

Answer: b. The router with a higher priority.

28. A Cisco router has the following route table:

```
R1#show ip route
     131.108.0.0/16 is variably subnetted, 17 subnets, 2 masks
C       131.108.255.0/24 is directly connected, Serial0/0
C       131.108.250.0/24 is directly connected, Serial0/1
O       131.108.254.0/24 [110/391] via 131.108.255.6, 03:33:03, Serial0/1
                         [110/391] via 131.108.255.2, 03:33:03, Serial0/0
R       131.108.254.0/24 [120/1] via 131.108.255.6, 03:33:03, Serial1/0
                         [120/1] via 131.108.255.2, 03:33:03, Serial1/1
```

What is the preferred path to 131.108.254.0/24? (Choose the best two answers.)

Answers: a. Via Serial0/0

b. Via Serial0/1

OSPF is chosen because of the lower administrative distance of 110 compared to RIP's 120. Notice the OSPF load balancing between Serial 0/0 and Serial 0/1. RIP has also dynamically discovered the same routers over two paths, but because the AD is higher or less trusted, OSPF will be the preferred routing path. If, for example, the serial interfaces S0/1 and S0/0 fail, then the remaining path will be Serial 1/0 and Serial 1/1 or via RIP. (The written examination always advises you how many answers to select. Practice on the CD provided.)

29. IP RIP runs over what TCP port number?

Answer: e. None of these

IP RIP does not use TCP port numbers; it uses UDP.

30. IP RIP runs over what UDP port number?

Answer: d. 520

IP RIP runs over UDP 520.

31. An OSPF virtual link should _____.

Answer: c. allow partitioned areas access to the backbone

Virtual links allow access to areas not directly connected to the backbone or partitioned areas. A partitioned OSPF area is defined as an area assignment by the network administrator not connected to area 0. It is the area that is associated with the OSPF address range. It can be specified as either a decimal value or an IP address. If you intend to associate areas with IP subnets, you can specify a subnet address as the value of the *area-id* argument.

32. What is the BGP version most widely used today?

Answer: d. 4

BGP4 is the most widely used version.

33. What is the destination port number used in a Telnet session?

Answer: a. 23

Telnet, an application layer protocol, uses destination port 23.

34. In what field or fields does the IP checksum calculate the checksum value?

Answer: c. Header only

The IP checksum calculation covers only the IP header.

35. The TCP header checksum ensures integrity of what data in the TCP segment?

Answer: c. The data and header.

The TCP checksum calculation covers the TCP header and data.

36. ISDN BRI channels are made up of what?

Answer: c. 2 × 64-kbps channels and one D channel at 16 kbps

ISDN Basic Rate Interface (BRI) is two 64-kbps data channels and one signaling channel (D channel at 16 kbps).

37. What services can ISDN carry?

Answer: d. Data, voice, and video

38. Place the following steps in the correct order for PPP callback, as specified in RFC 1570.

1. A PC user (client) connects to the Cisco access server.

2. The Cisco IOS Software validates callback rules for this user/line and disconnects the caller for callback.

3. PPP authentication is performed.

4. Callback process is negotiated in the PPP Link Control Protocol (LCP) phase.

5. The Cisco access server dials the client.

Answer: d. 1, 5, 4, 3, 2

RFC 1570 dictates how PPP callback is to be followed. For more information, refer to http://www.cse.ohio-state.edu/cgi-bin/rfc/rfc1570.html.

39. What hardware port is typically designed to connect a Cisco router for modem access?

Answer: c. The auxiliary port

The auxiliary port on Cisco routers can be used for modem access. The console port can also be used but, typically, the auxiliary port is applied for remote access or dialup access for network failures.

40. The AS5300 series router can support which of the following incoming connections?

Answer: d. All of these

The AS5300 series router can support both digital (ISDN) and analog connections, and also supports voice traffic.

41. Which of the following routing protocols are protected by an authentication mechanism?

Answers: a. OSPF

b. RIPv2

d. EIGRP

f. EBGP

g. IBGP

h. BGP

RIPv2, OSPF, EIGRP, and all forms of BGP—that is, internal and external—support authentication mechanisms, namely Message Digest 5 (MD5).

42. What UDP port range is used between Cisco IP Phones when a call is in progress?

Answer: e. 16384–32767

IP phones communicate via UDP, and the range is 16384–32767, *not 16384–32766.*

43. What two methods are commonly used to secure Voice over IP? (Choose two answers.)

Answers: a. Access lists

b. IDSs

The SAFE blueprint for voice networks defines access lists and IDSs as the two most crucial features that should be used when deploying VoIP.

44. Which of the following can be used by attackers to gain access to WLANs? (Select three answers.)

Answers: b. Audit the MAC address

d. Exploit flaws in the operating system

e. Use a sniffer tool with a wireless adapter

Auditing MAC addresses, exploiting operating system flaws, and using sniffer tools are today's most common ways to access WLANs. Service Set Identifier (SSIDs) alone cannot access the network, nor can calling the Technical Assistance Center (TAC).

45. Which of the following is *not* a method used to secure a wireless network? (Select the best three answers.)

Answers: a. Deploy WEP with a static key only

d. Disable MAC authentication

e. Nothing, wireless is inherently secure

Answer: The question clearly asks for methods that are not secure. Deploying a static WEP key is very insecure, disabling MAC authentication can lead to rogue devices becoming associated with the access points, and doing nothing is very insecure.

Q & A

1. What are the seven layers of the OSI model?

Answer: The seven layers of the OSI model are as follows:

- Application
- Presentation
- Session
- Transport
- Network
- Data link
- Physical

2. What layer of the OSI model is responsible for ensuring that IP packets are routed from one location to another?

Answer: The network layer is primarily responsible for routing IP packets from one destination to another.

3. What mechanism is used in Ethernet to guarantee packet delivery over the wire?

Answer: Carrier Sense Multiple Access/Collision Detection (CSMA/CD) is the Ethernet mechanism used to ensure that when devices detect collisions, other devices on the segment are sent a jam signal. CSMA/CD ensures that when collisions occur, other devices (such as PCs or routers) back off (do not transmit) for a specified period of time. When a device receives a jam signal, it will wait a random amount of time to retransmit. This lowers the chance of another collision. All devices that detect a jam signal can transmit up to 16 times before sending an error message to the application layer.

4. Name two physical characteristics of 10BASE-T.

Answer: 10BASE-T is an Ethernet physical layer standard that defines a maximum length of 100 m and a network speed of 10 Mbps.

5. What Catalyst command displays the bridging or CAM table on a Cisco 3550 series switch?

Answer: The command is

```
show mac-address-table dynamic [address mac_addr ¦ interface type slot/port ¦
  protocol protocol ¦ Vlan vlan_id]
```

The basic command is **show mac-address-table**.

6. What are the possible states of spanning tree?

Answer: The possible states of spanning tree are as follows:

- **Disabled**—The port is not participating in spanning tree and is not active.
- **Listening**—The port has received data from the interface and will listen for frames. In this state, the bridge only receives data and does not forward any frames to the interface or to other ports.
- **Learning**—The bridge still discards incoming frames. The source address associated with the port is added to the CAM table. BPDUs are sent and received.
- **Forwarding**—The port is fully operational; frames are sent and received.
- **Blocking**—The port has been through the learning and listening states and, because this particular port is a dual path to the root bridge, the port is blocked to maintain a loop-free topology.

The order of spanning tree states is listening, then learning, and, finally, forwarding or blocking. Typically, each state takes around 15 seconds on Cisco Catalyst switches.

7. Fast EtherChannel (FEC) allows what to occur between Cisco Catalyst switches?

   Answer: FEC is a Cisco method that bundles 100-Mbps Fast Ethernet ports into a logical link between Cisco Catalyst switches, such as the Catalyst 5000 or 6000 series switches.

   Up to four ports can be bundled together to scale bandwidth up to 800 Mbps.

8. Does an IP packet include a known and common field that guarantees data delivery? If so, what is this field?

   Answer: The IP frame format has no setting that guarantees packet delivery, so IP is termed connectionless. The error check is performed on the IP header fields only, not on the data in the packet.

9. Name some examples of connection-orientated protocols used in TCP/IP networks.

   Answer: Connection-orientated protocols include TCP, FTP, and Telnet.

10. Given the address 131.108.1.56/24, what are the subnet and broadcast addresses? How many hosts can reside on this network?

    Answer: The subnet address is 131.108.1.0 and the broadcast address is 131.108.1.255. The number of hosts is defined by the formula $2^8 – 2 = 256 – 2 = 254$.

11. How many hosts can reside when the subnet mask applied to the network 131.108.1.0 is 255.255.255.128 (or 131.108.1.0/25)?

    Answer: The number of hosts is $2^7 – 2 = 128 – 2 = 126$.

12. Name five routing protocols that support VLSM.

    Answer: Routing protocols that support VLSM include the following:

    - RIPv2
    - OSPF
    - IS-IS
    - EIGRP
    - BGP4

13. What is the destination port number used in a Telnet session?

Answer: The TCP port number is 23, and the source port is a random number (above 1023) generated by the host device.

14. What TCP/IP services are common in today's large IP networks?

Answer: TCP/IP has a number of applications or services in use:

- Address Resolution Protocol (ARP)
- Reverse Address Resolution protocol (RARP)
- Dynamic Host Configuration Protocol (DHCP)
- Hot Standby Router Protocol (HSRP)
- Internet Control Message Protocol (ICMP)
- Telnet
- File Transfer Protocol (FTP)
- Trivial File Transfer Protocol (TFTP)

15. What Cisco IOS command displays the IP ARP table on a Cisco IOS router?

Answer: The Cisco IOS command is **show ip arp**. This command displays IP ARP entries only. The Cisco IOS command **show arp** displays all ARP entries for all protocols in use.

16. Cisco IOS routers use what mechanism to determine the routing selection policy for remote networks if more than one routing protocol is running?

Answer: Cisco IOS routers use administrative distance, which defines a set number for every routing protocol in use. The lower the AD, the more trustworthy the network. For example, a static route (AD is 1) is preferred to an OSPF (AD is 110) discovered route. A static route pointing to a directly connected interface, for example, via Ethernet0, has an AD set to 0, the same as a directly connected interface even though a static route is enabled.

17. What is the administrative distance for OSPF, RIP, and external EIGRP?

Answer: The AD for OSPF is 110, for RIP is 120, and for external EIGRP is 170 (internal EIGRP is 90).

18. Name five characteristics of distance vector routing protocols and provide two examples of routing protocols classified as distance vector.

Answer: Distance vector characteristics and example protocols are as follows:

Periodic updates	Periodic updates are sent at a set interval; for IP RIP, this interval is 30 seconds.
Broadcast updates	Updates are sent to the broadcast address 255.255.255.255. Only devices running routing algorithms will listen to these updates.
Full table updates	When an update is sent, the entire routing table is sent.
Triggered updates	Also known as Flash updates, triggered updates are sent when a change occurs outside the update interval.
Split horizon	This method stops routing loops. Updates are not sent out an outgoing interface from which the route was received. This also saves bandwidth.
Maximum Hop Count limit	For RIP, the limit is 15, and for IGRP it's 255.
Algorithm	An example is Bellman-Ford for RIP.
Examples	RIP and IGRP.

19. IP RIP runs over what protocol and port number when sending packets to neighboring routers?

Answer: IP RIP runs over UDP port number 520 when sending packets to neighboring routers.

20. How many networks can be contained in an IP RIP update?

Answer: An IP RIP update can contain up to 25 networks.

21. Specify the main differences between RIPv1 and RIPv2.

Answer: RIPv1 does not support VLSM, authentication, or multicast updates. RIPv2 supports VLSM, authentication, and multicast updates (and unicast updates to remote routers).

22. What is an EIGRP feasible successor?

Answer: An EIGRP feasible successor is a neighboring EIGRP Cisco router with a lower advertised metric.

23. What is the metric used by OSPF?

Answer: The metric used by OSPF is cost and is defined by the formula $10^8 \div$ bandwidth for a given interface. The cost to a remote path is the sum of all the costs that a packet will traverse to reach the remote network.

24. If OSPF is configured for one area, what area assignment should be used?

Answer: Good OSPF design defines area 0, or the backbone, as the core area, and area 0 should always be used. If the OSPF network resides in one area only, theoretically, any area assignment is possible.

25. What LSA types are not sent in a total stubby area?

Answer: Totally stubby areas block LSA types 3, 4, and 5. Although similar to a stub area, a totally stubby area blocks LSAs of type 3, as well. This solution is Cisco proprietary and is used to further reduce a topological database. The only link-state advertisement (LSA) type permitted is a specific type 3 LSA advertising a default router only.

26. What Cisco IOS command disables an interface from participating in the election of an OSPF DR/BDR router?

Answer: To disable an interface on a Cisco router when electing a DR, the Cisco IOS command is **ip ospf priority 0**. The router with the highest priority (range is between 0 and 255) will be elected the DR.

27. On an Ethernet broadcast network, a DR suddenly reboots. When the router recovers and discovers neighboring OSPF routers, will it be the designated router once more?

Answer: Once the router fails, the backup DR (BDR) assumes the functions of the DR and another OSPF router (if it exists) is elected the BDR. After the failed router recovers, neighboring OSPF Hello packets will advise that a DR/BDR already exists and there is no need to assume the functions of DR or BDR until another election process is initiated.

28. What Layer 4 protocol does BGP use to guarantee routing updates, and what destination port number is used?

Answer: BGP4 uses TCP and the destination port number is 179.

29. What are ISDN BRI and PRI?

Answer: ISDN can be supplied by a carrier in two main forms: Basic Rate Interface (BRI) and Primary Rate Interface (PRI). An ISDN BRI consists of two 64-kbps services (B channels) and one 16-kbps signaling channel (D channel). An ISDN PRI consists of 23 B or

30 B channels and a 64-kbps D channel, depending on the country. In North America and Japan, a PRI service consists of 23 B channels for a total bit rate of up to 1.544 Mbps. In Asia and Australia, a PRI delivers 30 B-channels and one 64-kbps D channel, delivering a total bit rate of 2.048 Mbps.

30. What are the three phases that occur in any PPP session?

Answer: The following are the three phases that occur in any PPP session:

- **Link establishment**—Link Control Protocol (LCP) packets are sent to configure and test the link.
- **Authentication (optional)**—After the link is established, authentication can be used to ensure that link security is maintained.
- **Network layers**—In this phase, NCP packets determine which protocols will be used across the PPP link. An interesting aspect of PPP is that each protocol (IP, IPX, and so on) supported in this phase is documented in a separate RFC that discusses how it operates over PPP.

31. Define what BECN and FECN mean in a Frame Relay network?

Answer: Backward explicit congestion notification (BECN)—Bit set by a Frame Relay network device in frames traveling in the opposite direction of frames encountering a congested path. DTE receiving frames with the BECN bit set can request that higher-level protocols take flow-control action, as appropriate.

Forward explicit congestion notification (FECN)—Bit set by a Frame Relay network device to inform DTE receiving the frame that congestion was experienced in the path from source to destination. DTE receiving frames with the FECN bit set can request that higher-level protocols take flow-control action, as appropriate.

32. Frame Relay DLCI values are used for what purpose?

Answer: The data-link connection identifier (DLCI) value specifies a PVC or SVC in a Frame Relay network. DLCIs are locally significant. There are globally significant DLCIs used for LMI communication between Frame Relay switches.

33. What is the IP address range used in IP multicast networks?

Answer: The range of networks is from 224.0.0.0 to 239.255.255.255.

34. What type of network environment typically uses an AS5300?

Answer: The AS5300, or universal access server, is a versatile data communications platform that provides the functions of an access server, router, and digital modem in a single modular chassis. Internet service providers typically use an AS5300 to allow clients to use ISDN or PSTN when accessing the Internet. The AS5300 also supports voice communication.

35. What is the best method you can easily deploy to protect CCMs from unauthorized access?

    Answer: Cisco IOS access lists and intrusion detection systems are the main tools used to secure VoIP networks.

36. What is WEP? Is WEP inherently secure or insecure?

    Answer: WEP is Wired Equivalent Privacy. WEP is an 802.11 standard that describes the communication that occurs in wireless LANs. The WEP algorithm is used to protect wireless communication from eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network; this function is not an explicit goal in the 802.11 standard, but it is frequently considered to be a feature of WEP. WEP uses the RC4 encryption algorithm, which is known as a stream cipher.

Chapter 2

Do I Know This Already?

1. RFC 1700 defines what well-known ports for DNS?

   Answer: e. TCP/UDP port 53

   DNS is permitted by RFC 1700 to use both TCP and UDP port 53. DNS applications use TCP port 53 for zone transfers and when the DNS replies are greater than 512 bytes.

2. What supplies DNS security?

   Answer: e. None of these

   DNS has no form of security, so any device can request name-to-IP address mappings.

3. What Cisco IOS command will stop a Cisco router from querying a DNS server when an invalid Cisco IOS command is entered at the EXEC or PRIV prompt?

   Answer: a. **no ip domain-lookup**

   To disable DNS query lookup, the Cisco IOS command in global configuration mode is **no ip domain-lookup**.

4. What does the following Cisco IOS global configuration mode line accomplish?

   ```
   ip host SimonisaCCIE 131.108.1.1 131.108.1.2
   ```

   Answer: a. Defines a local host name, SimonisaCCIE, mapped to IP addresses 131.108.1.1 and 131.108.1.2

The **ip host** *name ipaddress1* [*ipaddress2 ipaddress3 ipaddress4 ipaddress5 ipaddress6 ipaddress7 ipaddress8*] command configures a local address lookup for the name SimonisaCCIE. Up to eight addresses can be used. The router will try 131.108.1.1 first and, if no response is made by the remote host, the second address, 131.108.1.2, will be attempted from the command-line interface (CLI).

5. TFTP uses what predefined UDP port number?

Answer: e. 69

TFTP uses UDP port number 69 for the initial connection, and then data transfer occurs between two random higher-numbered UDP ports.

6. What Cisco IOS command will copy a Cisco IOS image from the current system flash to a TFTP server?

Answer: b. **copy flash tftp**

To copy a Cisco IOS image from the routers to system flash, the correct Cisco IOS command is **copy flash tftp**.

7. Suppose a client calls and advises you that an FTP data transaction is not allowing the client to view the host's directory structure. What are the most likely causes of the problem? (Choose all that apply.)

Answers: b. The client's FTP data port is not connected.

e. An access list is stopping port 20 from detailing the directory list.

The FTP data port is used to view the directory and could be blocked because of an access list or a fault with the client's software when establishing the FTP 20 connection.

8. FTP runs over what Layer 4 protocol?

Answer: b. TCP

The FTP application is a connection-orientated protocol and is part of the TCP/IP protocol suite. FTP ensures that data is delivered by using TCP, which is another connection-oriented protocol.

9. HTTPs traffic uses what TCP port number?

Answer: b. 443

HTTPs runs over TCP port 443.

10. SNMP is restricted on Cisco routers by what Cisco IOS command?

Answer: b. **snmp-server community** *string*

To restrict SNMP access, the correct Cisco IOS command is **snmp-server community** *string*. Without the correct string, network management system (NMS) stations cannot access a router with SNMP queries. You can disable SNMP on a router and restrict SNMP access with the Cisco IOS command **no snmp-server**. Access lists can be applied to further restrict access to certain hosts and IP subnet ranges.

11. TFTP uses which of the following?

Answer: d. Can use UDP/TCP and port 69

The TFTP port number is defined in RFC 1700 (the protocol is defined in RFC 1350) and TFTP is permitted to use TCP/UDP port 69 only. Most applications, such as Cisco TFTP Server, use UDP port 69. Beware of such tricky questions for the examination.

12. Which of the following statements is true regarding SSL?

Answer: b. Encryption is used after a simple handshake is completed; that is, after the client is authenticated.

After the hosts have negotiated with valid username/password pairs, SSL starts to encrypt all data. After the handshake, packets are not authenticated. SSL uses TCP port 443.

13. What is the **HELO** SMTP command used for?

Answer: b. To identify SMTP clients.

The **HELO** command identifies the client to the SMTP server.

14. POP3 clients can do what?

Answer: b. Retrieve mail.

POP3 clients retrieve mail from POP3 servers. SMTP is not part of the POP3 standard. POP3 allows a client to retrieve e-mail from a POP3 server. There is no provision to send e-mail in POP3.

15. NTP uses what well-known TCP port as defined by RFC 1700?

Answer: e. 123

NTP uses UDP or TCP, and the port number is 123. Typically, however, NTP applications only use UDP port 123; RFC 1700 allows for either TCP or UDP to be applied. All applications in use today use UDP.

16. Secure Shell (SSH) is used to do what?

Answer: c. Protect the TCP/IP host with an encrypted channel.

SSH is used to establish a secure session to a TCP/IP host, thereby ensuring it is protected against packet-snooping tools. SSH provides an encrypted communication channel between the client and server device.

17. Which of the following protocols can be authenticated? (Select the best four answers.)

Answers: a. Telnet

b. HTTP

c. HTTPs

f. FTP

Telnet, HTTP, HTTPs, and FTP require the user to enter a username and password pair to gain access to restricted hosts. Spanning tree is a Layer 2 mechanism with no authentication mechanism, and TFTP has no username/password pair requirement.

18. What is the community string value when the following Cisco IOS commands are entered in global configuration mode?

```
snmp-server community publiC RO
snmp-server enable traps config
snmp-server host 131.108.255.254 isdn
```

Answer: c. publiC

The community string is defined by **command snmp-server community** *community strin*g, which, in this case, is set to publiC. The community string is case sensitive.

19. Which of the following best describes an SNMP inform request?

Answer: c. Requires an acknowledgment from the SNMP manager.

SNMP inform requests require an acknowledgment from the SNMP manager. SNMP hosts will continue sending the SNMP inform request until an acknowledgment is received.

20. What UDP port number will SNMP traps be sent from?

Answer: d. 162

SNMP traps are sent by SNMP agents (such as routers) over UDP port 162.

21. What TCP port number will an SNMP inform acknowledgment packet be sent to?

Answer: f. None of these

SNMP inform acknowledgments are sent over UDP (not TCP) port number 161.

22. To restrict SNMP managers from the source network 131.108.1.0/30, what Cisco IOS command is required?

Answer: c.

```
snmp-server community SimonisCool ro 4
  access-list 4 permit 131.108.1.0 0.0.0.3
```

The SNMP server community name must be defined with the following command:

```
snmp-server community string ro access-list-number
```

The access list number definition must follow (in this case, number 4). The access list range is between 1 and 99 only.

23. Cisco IOS SSH supports what version of SSH?

Answer: c. Both versions 1 and 2

Cisco IOS 12.2 or later supports SSH versions 1 and 2. You should be aware that 12.3T and higher versions of Cisco IOS only support SSH 2. Exam hot tip: If the question in the written exam does not mention Cisco IOS revisions, then select both SSH 1 and 2 as the examination may not be up to date.

24. When enabling Cisco IOS SSH on a Cisco IOS router, which of the following is not a required step?

Answer: c. Generate a secret and enable password.

Cisco IOS does not require a secret and enable password when enabling SSH; the DNS name and the **hostname** and **transport** commands are mandatory. SSH requires a crypto Cisco IOS image loaded on the router. You must also configure a username/password pair locally.

25. What Cisco IOS command will enable a SSH client session with the username cisco, encryption 3DES, and target IP address 10.1.1.1/24?

Answer: a. Simon**#ssh –c 3des –l cisco 10.1.1.1**

The Cisco IOS SSH client command syntax is

```
ssh [-l userid] [-c {des ¦ 3des}] [-o numberofpasswordprompts n] [-p portnum]
    {ipaddr ¦ hostname} [command]
```

26. SSH provides a security mechanism but lacks one certain feature. What feature is that?

Answer: c. Each transmission requires authentication

SSH provides a secure private channel for all messages. The end client to server is fact authenticated and an integrity check is made. The only limiting factor is that not every individual transmission is authenticated—just the initial request after a simple handshake using a secret key for data encryption.

27. What protocol allows network administrators to monitor IDS sensors and what two protocols can be used?

    Answer: a. RDEP and HTTP/SSL

    Remote Data Exchange Protocol (RDEP) allows the operator to monitor the network IDS sensors in place and communicate via a protocol named RDEP. RDEP uses HTTP and SSL to pass Extensible Markup Language (XML) documents over an encrypted session, between the sensor and the external system. If the session is encrypted, then only SSL can be used.

Q & A

1. According to RFC 1700, what is the well-known TCP/UDP port used by DNS?

   Answer: RFC 1700 defines the well-known ports for the whole TCP/IP protocol suite. For DNS, the well-known port for TCP/UDP is number 53. Typically, however, applications today deploy UDP port 53 only.

2. What does the Cisco IOS command **no ip domain-lookup** accomplish?

   Answer: This Cisco IOS command disables DNS queries for network administrators connected to a Cisco console or vty line.

3. What is the correct Cisco IOS syntax to specify local host mapping on a Cisco router?

   Answer: Local host mappings to IP addresses are accomplished using the following Cisco IOS command:

   ```
   ip host name [tcp-port-number] ip-address1 [ip-address2...ip-address8]
   ```

   Up to eight IP addresses can be assigned to one name.

4. TFTP uses what well-known, defined TCP/UDP port?

   Answer: TFTP uses UDP port number 69. RFC 1700 allows the use of TCP port 69 as well.

   What is the correct Cisco IOS command to copy a file from a TFTP server to the system flash? The Cisco IOS command is **copy tftp flash**. To copy a file from the system flash to the TFTP server, the Cisco IOS command is **copy flash tftp**.

5. Define the two modes of FTP.

   Answer: FTP can be configured for the following two modes:

   - Active mode (technical term is PORT mode)
   - Passive mode (technical term is PASV mode)

6. FTP uses what TCP port numbers?

   Answer: FTP uses well-known port numbers 20 and 21.

7. What well-known ports do Secure Sockets Layer (SSL) and Secure Shell (SSH) use?

   Answer: SSL uses well-known port number 443. Secure Shell uses well-known TCP port 22.

8. Define SNMP and give an example of how SNMP traps can be used to identify problems with Cisco IOS routers.

   Answer: Simple Network Management Protocol (SNMP) is an application layer protocol that is used to manage IP devices. SNMP is part of the TCP/IP application layer suite. SNMP enables network administrators to view and change network parameters and monitor connections locally and remotely. Cisco routers can be configured to send SNMP traps to network management system stations to alert administrators. For example, SNMP traps may indicate a router with low memory or high CPU usage.

9. What well-known UDP ports are used by SNMP?

   Answer: RFC 1700 defines the SNMP ports as 161 and 162. TCP can also be used, but vendors typically only implement SNMP with UDP. SNMP port 161 is used to query SNMP devices, and SNMP port 162 is used to send SNMP traps. SNMP runs over UDP and is secured by a well-known community string that is case sensitive.

10. What Cisco IOS command enables SNMP on a Cisco IOS router?

    Answer: The command syntax is **snmp-server community *string*** *access-rights*. The *access-rights* options are **RO** and **RW**. There is no default value specified.

11. Which TCP/UDP port numbers are defined for use by the Network Time Protocol (NTP)?

    Answer: NTP can use TCP and UDP port number 123. UDP is common in today's networks.

12. When defining a stratum value on a Cisco router, what is the range and what value is closest to an atomic clock?

    Answer: The stratum value ranges from 1 to 15. The value 1 represents an atomic clock, which is the most accurate clock available. The default stratum value on Cisco routers is 8.

13. SSH allows what to be accomplished when in use?

    Answer: Secure Shell (SSH) is a protocol that provides a secure connection to a router. Cisco IOS supports version 1 of SSH. SSH enables clients to make a secure and encrypted connection to a Cisco router. Newer Cisco IOS releases now support SSH version 2. SSHv2 was introduced with Cisco IOS Version 12.3(4)T.

14. What is the difference between an SNMP inform request and an SNMP trap?

Answer: The major difference between a trap and an inform request is that an SNMP agent (when ending a trap) has no way of knowing if an SNMP trap was received by the SNMP manager. On the other hand, an SNMP inform request packet is sent continually until the sending SNMP manager receives an SNMP acknowledgment.

15. What does the SNMP MIB refer to?

Answer: The Management Information Base (MIB) is a virtual information storage area for network management information, which consists of collections of managed objects. MIB modules are written in the SNMP MIB module language, as defined in STD 58, RFC 2578, RFC 2579, and RFC 2580.

16. What is the SNMP read-write community string for the following router configuration?

```
snmp-server community simon ro
snmp-server community Simon rw
```

Answer: The read-write community string is set to Simon. The read-only community attribute is set to simon. The community string is case sensitive.

17. Before you can TFTP a file from a Cisco router to a UNIX- or Windows-based system, what is the first step you must take after enabling the TFTP server daemon on either platform?

Answer: On a UNIX server where the TFTP server daemon is installed, the file to be copied must have the appropriate access rights. In UNIX, the **touch** command allows a TFTP request. In other words, to copy a file from a Cisco IOS router to a UNIX host, the file must already exist on the host. For a Windows-based platform, the software must be configured to permit file creation on the Windows-based file system. Typically, however, the applications do not have file access rights as UNIX does.

18. What Cisco IOS command can be implemented to restrict SNMP access to certain networks by applying access-lists? Can you apply standard, extended, or both to these access lists?

Answer: The Cisco IOS command is as follows:

```
snmp-server community string [view view-name] [ro ¦rw ] [number]
```

You can only apply a standard access list with this command.

number refers to a standard access list, ranging from 1 to 99 only, that defines the remote hosts or subnets that are permitted SNMP access. The correct SNMP community string must also be correctly configured on the SNMP manger and agent to allow SNMP communication.

19. Does TFTP have a mechanism for username and password authentication?

Answer: TFTP is a connectionless protocol (UDP) that has no method to authenticate a username or password. The TFTP packet format has no field enabling the username or password to be exchanged between two TCP/IP hosts. TFTP security (configurable on UNIX and Windows platforms) on the TFTP server is accomplished by allowing a predefined file (a file created on the hard disk partition) on the server to be copied to the host TFTP server.

20. Can you use your Internet browser to configure a Cisco router? If so, how?

Answer: Yes. To view the router's home page, use a web browser pointed to http://*a.b.c.d,* where *a.b.c.d* is the IP address of your router or access server. If a name has been set, use http://*router-name*, and use the DNS server to resolve the IP address.

To enable HTTP on a Cisco router, use the Cisco IOS command **ip http** in global configuration mode.

21. Suppose that a network administrator defines a Cisco router to allow HTTP requests but forgets to add the authentication commands. What is the default username and password pairing that allows HTTP requests on the default TCP port 80? Can you predefine another TCP port for HTTP access other than port 80?

Answer: By default Cisco IOS routers configured for HTTP access use the router's local host name as the username and use the enable or secret password as the password.

The Cisco IOS command **ip http** [*0-65535*] allows the network administrator to define a port number other than 80, which is the default setting.

22. What are the four steps to enable Cisco IOS SSH for a SSH server?

Answer: The following are the four steps required to enable SSH support on a Cisco IOS router:

1. Configure the hostname command.
2. Configure the DNS domain.
3. Generate the public RSA key to be used.
4. Enable SSH transport support for the vtys. SSH transport is enabled by default. A username/password pair should be enabled locally or on a AAA server to enable users to actually gain SSH access to the router. Remember, SSH is not new; it is simply that Cisco IOS now supports SSH access. Cisco IOS SSH is Cisco marketing terminology only and not a new feature. SSH has been around for years.

Chapter 3

Do I Know This Already?

1. What IOS command will display the System Flash?

   Answer: a. **show flash**

2. The network administrator has forgotten the enable password, and all passwords are encrypted. What should the network administrator do to recover the password without losing the current configuration?

   Answer: c. Reboot the router, press the Break key after the reload, and enter ROM mode and change the configuration register.

3. What is the enable password for the following router?

   ```
   enable password Simon
   ```

   Answer: b. Simon.

4. If the configuration register is set to 0x2101, where is the IOS image booted from?

   Answer: d. ROM

5. What IOS command will copy the running configuration to a TFTP server?

   Answer: c. **copy running-config tftp**

6. What **debug** command allows an administrator to debug only packets from the network 131.108.0.0/16?

   Answer: d.

   ```
   debug ip packet 1
   access-list 1 permit 131.108.0.0 0.0.255.255
   ```

7. After entering **debug ip packet**, no messages appear on your Telnet session. What is the likely cause?

   Answer: c. The **terminal monitor** command is required.

8. To change the configuration register to 0x2141, what is the correct IOS command?

   Answer: e. **config-register 0x2141**

9. Where is the startup configuration stored on a Cisco router?

   Answer: b. NVRAM

10. Which of the following statements is true?

Answer: a. The **enable secret** command overrides the **enable password** command.

11. A Cisco router has the following configuration:

```
line vty 0 4
login
```

What will happen when you telnet to the router?

Answer: c. You will not be able to access the router without the password set.

12. A Cisco router has the following configuration:

```
line vty 0 4
no login
password cIscO
```

When a Telnet user tries to establish a remote Telnet session to this router, what will happen?

Answer: b. The Telnet user will enter EXEC mode immediately.

13. A Cisco router has the following configuration:

```
line vty 0 1
no login
password cisco
line vty 2 4
login
password ciSco
```

When a third Telnet session is established to a remote router with the preceding configuration, what will happen?

Answer: b. You will be prompted for the login password, which is set to ciSco.

14. Which of the following access lists will deny any IP packets sourced from network 131.108.1.0/24 and destined for network 131.108.2.0/24 and permit all other IP-based traffic?

Answer: d.

```
access-list 100 deny ip 131.108.1.0 0.0.0.255 131.108.2.0 0.0.0.255
access-list 100 permit ip any any
```

15. Which of the following secure protocols are available to manage Cisco IOS software? (Choose the best three answers.)

Answers: b. SSH

c. HTTPS

e. IPSec-ESP

16. What types of attacks can intruders use to enable them to attack VLANs on a Layer 2 switched network?

    Answer: f. All of these

17. What information is stored in the CAM table?

    Answer: d. MAC information mapped to port interfaces

18. How can the CAM table be exploited by intruders?

    Answer: b. CAM tables can be used to forward all packets to certain interfaces by flooding the switch with the MAC address's source by one or more interfaces.

19. What is VLAN hopping?

    Answer: a. Using a trunk port to access all VLANs, thus bypassing an access control device

20. How is a DHCP starvation attack achieved?

    Answer: b. Broadcasting DHCP requests with spoofed MAC addresses

21. When preparing a security policy, what are the three core requirements?

    Answers: b. Create acceptable-usage policy statements.

    c. Conduct a risk analysis.

    d. Establish a security team structure.

22. An administrator notices a router's CPU utilization has jumped from 2 percent to 100 percent, and that a CCIE engineer was debugging. What IOS command can the network administrator enter to stop all debugging output to the console and vty lines without affecting users on the connected router?

    Answer: b. **undebug all**

Q & A

1. Where is the running configuration stored on a Cisco router?

   Answer: The running configuration is stored in RAM. For all newer Cisco hardware platforms, the running configuration is stored in dynamic RAM (DRAM).

2. What IOS command displays the startup configuration?

   Answer: The IOS command **show startup-config** or **show config** displays the configuration stored in NVRAM.

3. What IOS command provides the following output?

```
System flash directory:
File  Length   Name/status
  1   9558976  c2500-ajs40-l.12-17.bin
[9559040 bytes used, 7218176 available, 16777216 total]
16384K bytes of processor board System flash
```

Answer: The IOS command to display the System Flash is **show flash.**

4. What configuration register enables a Cisco router to ignore the startup configuration?

Answer: 0x2142 sets the IOS image to ignore the configuration stored in NVRAM; typically, this configuration register is used for password recovery.

5. To copy the startup configuration to the running configuration, what IOS command or commands are used?

Answer: The **copy startup-config running-config** command is used to copy the startup configuration to the running configuration.

6. What is the range for standard access lists and for extended IP access lists on Cisco IOS routers?

Answer: Standard IP access lists range from 1 through 99 and 1300 through 1999. Extended access lists range from 100 through 199 and 2000 through 2699.

7. What command displays the IP access lists configured on a Cisco router?

Answer: **show ip access-lists** displays all configured IP access lists. The **show access-lists** IOS command displays all configured access lists, not just IP access lists.

8. How do you disable all **debug** commands currently enabled on a Cisco router, assuming you are not sure what **debug** commands are enabled?

Answer: You use the **undebug all** (or **u all** in shorthand) command to disable all **debug** commands currently enabled. You can also use the **[no] debug** *specific-debug-enabled* commands for each specific debug that has been enabled. To quickly disable all **debug** commands, **undebug all** is typically used.

9. What must you be very careful of when enabling any form of debugging on a Cisco router?

Answer: You should make the **debug** command as specific as possible and ensure that you enable the output to the console (if disabled) and vty lines with the IOS command **terminal monitor**; this command is entered in privileged EXEC mode only. By default, Cisco IOS sends all debug output to the console port.

The CPU on Cisco routers gives the highest priority to debugging output. For this reason, debugging commands should be turned on only for troubleshooting specific problems or during troubleshooting sessions with technical support personnel. Excessive debugging output can render the router inoperable.

Try to use the most specific **debug** command possible, to reduce the load on the CPU.

10. What are the required steps when performing password recovery on a Cisco router?

Answer: The password recovery steps are as follows:

Step	Description
1	Power cycle the router.
2	Press the **Break** key (for Windows 2000, press **Control-Break**) to enter into boot ROM mode. The Control-Break key sequence must be entered within 60 seconds of the router restarting after a power cycle. Other terminal applications will have their own sequence, so make sure that you consult the help files.
3	After you are in ROM mode, change the configuration register value to ignore the startup configuration file that is stored in NVRAM. Use the **o/r 0x2142** command (2500 series routers). For Cisco IOS 12.2T (2600 models and higher) or later, the command is **confreg 0x2142**.
4	Allow the router to reboot by entering the **i** command.
5	After the router has finished booting up (you will be prompted to enter the setup dialog—answer **no** or press **Control-c** to abort the setup dialog) without its startup configuration, look at the **show startup-config** command output. If the password is encrypted, move to Step 6, which requires you to enter enabled mode (type **enable** and you will not be required to enter any password) and copy the startup configuration to the running configuration with the **copy startup-config running-config** command. Then, change the password. If the password is not encrypted and the **enable secret** command is not used, simply document the plain-text password and go to Step 8.
6	Because the router currently has no configuration in RAM, you can enter enabled mode by simply typing **enable** (no password is required). Copy the startup configuration to RAM with the IOS command **copy startup-config running-config.**
7	Enable all active interfaces.
8	Change the configuration register to 0x2102 (default) with the global IOS command **config-register 0x2102**. Note that this IOS command is automatically saved and there is no need to write changes to NVRAM when modifying the configuration register even though the IOS will prompt you to save when you do perform a reload.
9	After saving the configuration, you can optionally reload the router.
10	Check the new password if it is not encrypted. If the password is encrypted, simply enter enabled mode and verify your password.

11. What is the enable password for the following configuration?

```
enable password CiscO
```

Answer: Passwords are case sensitive, so the password is CiscO. If the secret password was set, you would not be able to read the password in clear text because Cisco IOS hashes the password using the MD5 encryption algorithm, as in the following example:

```
enable secret 5 $1$Aiy2$GGSCYdG57PdRiNg/.D.XI.
```

Notice that the password is not in clear text.

You cannot reverse-engineer the hashed password (1Aiy2$GGSCYdG57PdRiNg/.D.XI.). Hashing occurs when plain-text data is encrypted into cipertext (unreadable data) by some form of encryption algorithm.

12. What is the CAM table?

Answer: Cisco switches build Content-Addressable Memory (CAM) tables to store the MAC addresses available on physical ports along with their associated VLAN parameters; they are the Layer 2 equivalent of routing tables.

13. What are five methods used by intruders to compromise Cisco-based switches?

Answer: Switches are subjected to the following common attacks:

- CAM table overflow
- VLAN hopping
- Spanning Tree Protocol manipulation
- MAC address spoofing
- DHCP starvation

14. What IOS command enables port security for the interface FastEthernet0/1? The MAC address of the end station is 00-DE-AD-CC-EE-00. Ensure that the port is shut down if a violation occurs for more than one MAC address.

Answer: The following IOS configurations are required:

```
Router(config)#interface fastethernet0/1
Router(config-if)# switchport port-security
Router(config-if)# switchport port-security maximum 1
Router(config-if)# switchport port-security violation shutdown
Router(config-if)# switchport port-security MAC-address 00-DE-AD-CC-EE-00
```

15. How does a DHCP starvation attack work?

Answer: A DHCP starvation attack works by broadcasting DHCP requests with spoofed MAC addresses. Many tools are available on the Internet to send out these sorts of frames.

16. Prior to implementing a security policy, what three common steps should you accomplish?

Answer: Prior to implementing a security policy, you must do the following:

- **Create usage policy statements**—Outline user roles and functions within the organization.
- **Conduct a risk analysis**—Identify the risks to your current network, resources, and data devices.
- **Establish a security team structure**—Establish a cross-functional security team lead by a security manager, typically a virtual team (a team of experts that communicates over the phone, Internet, and e-mail), for global companies such as Cisco.

Chapter 4

Do I Know This Already?

1. What are the three components of AAA? (Choose the best three answers.)

Answer: AAA is used for authentication, authorization, and accounting.

a. Accounting
b. Authorization
c. Authentication

2. What Cisco IOS command must be issued to start AAA on a Cisco router?

Answer: The **aaa new-model** command starts AAA.

d. aaa new-model

3. What mathematical algorithm initiates an encrypted session between two routers by exchanging public keys over an insecure medium such as the Internet?

Answer: b. Diffie-Hellman algorithm

When using encryption between two routers, the Diffie-Hellman algorithm is used to exchange keys. This algorithm initiates the session between two routers and ensures that it is secure. The routing algorithm is used for routing, not for encryption. A switching engine is used to switch frames and has nothing to do with encryption. The stac compression algorithm is used by PPP; it compresses data on a PPP WAN link.

4. Can you configure RADIUS and TACACS+ to be used on the same router?

Answer: d. Yes, provided you have different list names applied to different interfaces.

You cannot apply the same list names and interfaces must be different.

5. How do you launch ACS remotely to a Windows 2000 device? (The remote IP address is 10.1.1.1 and the client is Internet Explorer.)

   Answer: c. Type **10.1.1.1:2002**.

   You can manage a remote ACS server on port 2002.

6. What RADIUS attribute is used by vendors and not predefined by RFC 2138?

   Answer: f. 26

   Attribute 26 is a vendor-specific attribute. Cisco uses vendor ID 9.

7. RADIUS can support which of the following protocols?

   Answer: a. PPP

   RADIUS supports PPP and none of the multiprotocols listed in the other options.

8. When a RADIUS server identifies the wrong password entered by the remote user, what packet type is sent?

   Answer: f. **ACCESS-REJECT**

   RADIUS sends an access-reject error if the password entered is invalid.

9. Identify the false statement about RADIUS.

   Answer: b. RADIUS runs over TCP port 1812.

   RADIUS does not deploy TCP. Note that the standard port for RADIUS accounting is 1813 (not 1646).

10. What is the RADIUS key for the following configuration? If this configuration is not valid, why isn't it? (Assume that this configuration is pasted into Notepad and not on an active router.)

```
aaa authentication login use-radius group radius local
aaa authentication ppp user-radius if-needed group radius
aaa authorization exec default group radius
aaa authorization network default group radius
radius-server 3.3.3.3
radius-server key IlovemyMum
```

    Answer: c. This configuration will not work because the command **aaa new-model** is missing.

    Because **aaa new-model** is not configured, this is not a valid configuration and no requests will be sent to the RADIUS server.

11. What is the RADIUS key for the following configuration?

```
aaa new-model
aaa authentication login use-radius group radius local
aaa authentication ppp user-radius if-needed group radius
aaa authorization exec default group radius
aaa authorization network default group radius
radius-server 3.3.3.3
radius-server key IlovemyMum
```

Answer: a. The RADIUS key is IlovemyMum.

The key is case-sensitive; the IOS command **radius-server key IlovemyMum** defines the key as IlovemyMum.

12. What versions of TACACS does Cisco IOS support? (Select the best three answers.)

Answers: a. TACACS+

b. TACACS

c. Extended TACACS

There is no Cisco Extended TACACS+ support.

13. TACACS+ is transported over which TCP port number?

Answer: e. 49

TACACS runs over TCP port 49. UDP port 520 is used by RIP, 23 for Telnet, and 20/21 for FTP.

14. What is the predefined RADIUS server key for the following configuration?

```
radius-server host 3.3.3.3
radius-server key CCIEsrock
```

Answer: e. CCIEsrock

The key is case sensitive and is defined by the IOS command **radius-server key CCIEsrock**.

15. What does the following command accomplish?

```
tacacs_server host 3.3.3.3
```

Answer: c. Nothing, because it is not a valid IOS command

The IOS command syntax to define a remote TACACS+ server is **tacacs-server host** *ip-address.*

16. Which of the following protocols does TACACS+ support?

Answer: d. All of these

TACACS+ has multiprotocol support for PPP, AppleTalk, NetBIOS, and IPX.

17. Which of the following key lengths are *not* supported by AES?

Answers: a. 64

e. 512

AES supports 128, 192, and 256 key lengths presently.

18. What is the number of bits used with a standard DES encryption key?

Answer: a. 56 bits

DES applies a 56-bit key. The documented time taken to discover the 56-bit key is 7 hours on a Pentium III computer, so DES is not a common encryption algorithm used in today's networks.

19. What is the number of bits used with a 3DES encryption key?

Answer: f. 168 bits

Triple DES (3DES) is today's standard encryption with a 168-bit key.

20. In IPSec, what encapsulation protocol encrypts only the data and not the IP header?

Answer: a. ESP

ESP encrypts only the data, not the IP header.

21. In IPSec, what encapsulation protocol encrypts the entire IP packet?

Answer: b. ESP

ESP encrypts the entire IP packet. The time to live (TTL) is not encrypted because this value decreases by one (1) every time a router is traversed. AH encrypts only the IP header, not the data.

22. Which of the following is AH's IP number?

Answer: d. 51

AH's IP number is 51. Unlike TCP, which has a port number at Layer 4, IP itself does not have a port number.

23. Which of the following is ESP's IP number?

Answer: c. 50

ESP's IP number is 50. Unlike TCP, which has a port number at Layer 4, IP itself does not have a port number.

24. Which of the following is *not* part of IKE phase I negotiations?

Answer: d. Negotiating SA parameters

IKE phase II negotiates SA parameters.

25. Which of the following is *not* part of IKE phase II?

Answer: c. Occasionally updating SAs (at most, once a day)

IKE phase II updates SAs at periodically defined intervals. This happens during IKE phase I.

26. Which is the fastest mode in IPSec?

Answer: c. Aggressive mode

Aggressive mode is faster than main mode but is less secure. They can both occur in phase I. Phase II only has quick mode. Fast mode does not exist in the IPSec standard set of security protocols.

27. Certificate Enrollment Protocol (CEP) runs over what TCP port number? (Choose the best two answers.)

Answers: a. Same as HTTP

b. Port 80

CEP uses the same port as HTTP, port 80.

28. Which of the following are new features aimed at increasing wireless security? (Choose the best four answers.)

Answers: a. TKIP

c. EAP

d. PEAP

e. MIC

Extensible Authentication Protocol (EAP), Protected EAP (PEAP), Message Integrity Check (MIC), and Temporal Key Integrity Protocol (TKIP) are new features aimed at increasing wireless security.

EAP, along with PEAP, enables the dynamic selection of the authentication mechanism at authentication time based on information transmitted in THE ACCESS-REQUEST. PPP also supports EAP during the link establishment phase.

TKIP defends against an attack on WEP in which the intruder uses an unencrypted segment called the initialization vector (IV) in encrypted packets to calculate the WEP key.

MIC is applied to detect forgeries such as bit flipping and altering packet source and destination.

Q & A

1. Define the AAA model and a typical application on a Cisco IOS router.

   Answer: Authentication, authorization, and accounting (pronounced triple A) provides security to Cisco IOS routers and network devices beyond the simple user authentication available on IOS devices.

   AAA provides a method to identify which users are logged into a router and each user's authority level. AAA also provides the capability to monitor user activity and provide accounting information.

   Typically, AAA is used to authenticate and authorize Cisco IOS commands, and provides accounting information to the network administrator.

2. Can you allow a remote user authorization before the user is authenticated with AAA?

   Answer: Before authorization occurs, the remote user must be authenticated. Cisco IOS routers allow you to configure AAA authorization, but no access will be permitted until the remote user is authenticated.

3. What IOS command is required when enabling AAA for the first time?

   Answer: **aaa new-model** must be entered globally before additional IOS commands are entered.

4. What is the privilege level of the following user? Assume AAA is not configured.

   ```
   R2>
   ```

   Answer: The privilege level ranges from 0 to 15 (the higher the level, the more commands are available). Because the user is not in PRIV EXEC mode, the default privilege level for an EXEC user is 1. Only basic **show** commands are available in privilege level 1.

   ```
   R2>show priv
   Current privilege level is 1
   ```

5. Define four possible RADIUS responses when authenticating the user through a RADIUS server.

   Answer: The four possible responses are as follows:

   - **ACCESS-ACCEPT**—The user is authenticated.
   - **ACCESS-REJECT**—The user is not authenticated and is prompted to re-enter the username and password, or access is denied. The RADIUS server sends this response when the user enters an invalid username/password pairing.
   - **ACCESS-CHALLENGE**—The RADIUS server issues a challenge. The challenge collects additional data from the user.
   - **CHANGE PASSWORD**—The RADIUS server issues a request asking the user to select a new password.

6. What are RADIUS attributes? Supply five common examples.

   Answer: RADIUS supports a number of predefined attributes that can be exchanged between client and server, such as the client's IP address. RADIUS attributes carry specific details about authentication.

   RFC 2865 (http://www.faqs.org/rfcs/rfc2865.html) defines a number of predefined RADIUS attributes, replacing the legacy RFC 2138.

   The following list provides details from the most common attributes:

   - **Attribute Type 1**—Username (defined usernames can be numeric, simple ASCII characters, or an SMTP address)
   - **Attribute Type 2**—Password (defines the password; passwords are encrypted using MD5)
   - **Attribute Type 3**—CHAP Password (only used in access-request packets)
   - **Attribute Type 4**—NAS IP address (defines the NAS server's IP address; only used in access-request packets)
   - **Attribute Type 5**—NAS port (not UDP port number; indicates that the NAS's physical port number ranges from 0 to 65535)
   - **Attribute Type 6**—Service-type (type of service requested or type of service to be provided; for Cisco devices is Callback and is not supported)
   - **Attribute Type 7**—Framed-Protocol (defines what framing is required; for example, PPP is defined when this attribute is set to 1, SLIP is 2)

- **Attribute Type 8**—Framed-IP-address (defines the IP address to be used by the remote user)
- **Attribute Type 9**— Framed-IP-Netmask (defines the subnet mask to be used by the remote user)
- **Attribute Type 10**—Framed-Routing
- **Attribute Type 13**—Framed-Compression
- **Attribute Type 19**—Callback number
- **Attribute Type 20**—Callback ID
- **Attribute Type 26**—Vendor-specific (Cisco [vendor-ID 9] uses one defined option, vendor type 1, named cisco-avpair)

7. What protocols does RADIUS use when sending messages between the server and client?

Answer: RADIUS transports through UDP destination port number 1812/1813.

8. What predefined destination UDP port number is RADIUS accounting information sent to?

Answer: UDP port 1813 (legacy 1646). For RADIUS accounting is 1813.

9. What does the following Cisco IOS software command accomplish on a Cisco IOS router?

```
aaa authentication ppp user-radius if-needed group radius
```

Answer: The **aaa authentication ppp user-radius if-needed group radius** command configures the Cisco IOS software to use RADIUS authentication for lines using PPP with CHAP or PAP, if the user has not already been authenticated. If the EXEC facility has authenticated the user, RADIUS authentication is not performed. User-radius is the name of the method list that defines RADIUS as the if-needed authentication method.

10. What is the RADIUS server IP address and key for the following configuration?

```
radius-server host 3.3.3.3
radius-server key GuitarsrocKthisplaneT
```

Answer: The **radius-server host** command defines the RADIUS server host's IP address. The IP address is 3.3.3.3.

The **radius-server key** command defines the shared secret text string between the NAS and the RADIUS server host. The key is case sensitive, like all passwords on Cisco IOS devices, so the key is defined as GuitarsrocKthisplaneT.

11. TACACS+ is transported over what TCP server port number?

Answer: TACACS+ is transported over TCP port 49.

12. What information is encrypted between a Cisco router and a TACACS+ server?

Answer: All data communication between TACACS+ devices is encrypted, excluding the IP or TCP header.

13. What are the four possible packet types from a TACACS+ server when a user attempts to authenticate a Telnet session to a Cisco router configured for AAA, for example?

Answer: The four packets types are as follows:

- **ACCEPT**—The user is authenticated and service can begin. If the NAS is configured to require authorization, authorization begins at this time.
- **REJECT**—The user has failed to authenticate. The user may be denied further access or may be prompted to retry the login sequence, depending on the TACACS+ daemon.
- **ERROR**—An error occurred at some time during authentication. This can be either at the daemon or in the network connection between the daemon and the NAS. If an ERROR response is received, the NAS typically tries to use an alternative method for authenticating the user.
- **CONTINUE**—The user is prompted for additional authentication information.

14. What is the significance of the sequence number in the TACACS+ frame format?

Answer: The sequence number is the number of the current packet flow for the current session. The sequence number starts with 1 and each subsequent packet increments by one. The client sends only odd numbers. TACACS+ servers send only even numbers.

15. What does the following IOS command accomplish?

```
aaa authentication ppp default if-needed group tacacs+ local
```

Answer: The **aaa authentication** command defines a method list, "default," to be used on serial interfaces running PPP. The keyword **default** means that PPP authentication is applied by default to all interfaces. The **if-needed** keyword means that if the user has already authenticated through the EXEC login procedure, PPP authentication is not necessary and can be skipped. If authentication is needed, the keyword **group tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the NAS.

16. What IOS command defines the remote TACACS+ server?

Answer: To define the TACACS+ server, IOS command **tacacs-server host** *ip-address.*

17. What are the major differences between TACACS+ and RADIUS?

Answer: The following table lists the major differences between TACACS+ and RADIUS.

	RADIUS	**TACACS+**
Packet delivery	UDP	TCP
Packet encryption	Encrypts only the password in the access-request packet from the client to the server.	Encrypts the entire body of the packet but leaves a standard TCP header.
AAA support	Combines authentication and authorization. Accounting is handled differently.	Uses the AAA architecture, separating authentication, authorization, and accounting.
Multiprotocol support	None.	Supports other protocols, such as AppleTalk, NetBIOS, and IPX.
Router management	Allows users to control which commands can be executed on a router. Can pass a privilege level down to the router, which can then be used locally for command authorization.	Enables network administrators to control which commands can be executed on a router.

18. What are the three most common threats from intruders that network administrators face?

Answer: The most common attacks are as follows:

- **Packet snooping (eavesdropping)**—When intruders capture and decode traffic, obtaining usernames, passwords, and sensitive data such as salary increases for the year.
- **Theft of data**—When intruders use sniffers, for example, to capture data over the network and steal that information for later use.
- **Impersonation**—When an intruder assumes the role of a legitimate device but, in fact, is not legitimate.

19. What is a hash in encryption terminology?

Answer: A hash is defined as the one-way mathematical summary of a message (data) such that the hash value cannot be easily reconstructed back into the original message.

20. Name the two modes of operation in IPSec and their characteristics.

    Answer: The two modes are the following:

    - **Transport mode**—Protects payload of the original IP datagram; typically used for end-to-end sessions.
    - **Tunnel mode**—Protects the entire IP datagram by encapsulating the entire datagram in a new IP datagram.

21. What does IKE accomplish?

    Answer: IKE negotiates and provides authenticated keys in a secure manner.

22. Certificate Enrollment Protocol is transported over what TCP port?

    Answer: CEP is transported over TCP port 80 (same as HTTP).

Chapter 5

Do I Know This Already?

1. In a secured network architecture, which of the following components are to be considered security devices? (Choose all that apply.)

   Answer: f. All of these

   Network security can be enabled on devices such as switches, routers, firewalls, IDSs, and by allowing remote IPSec tunnels through a VPN Concentrator.

2. Cisco Secure ACS supports what two security protocols? (Choose the best two answers.)

   Answers: a. RADIUS

   c. TACACS+

   Cisco Secure ACS supports RADIUS and TACACS+ (Cisco intellectual property).

3. The Cisco IDSM-2 has the following interfaces?

   Answer: d. IDSM-2 has no interfaces available.

   The IDSM-2 blade for the Catalyst 6500 has no user interface. You can manage the module with the **session** command.

4. In a secured network architecture, which of the following components is typically *not* considered a security appliance?

   Answer: f. Windows XP PC

   The PC is not typically considered a security appliance of a secured network infrastructure.

5. A VPN 3000 Concentrator is typically located in what part of a security network?

   Answer: a. The inside interface of a PIX Firewall

   VPN Concentrators are best placed on the inside interface of the PIX Firewall.

6. All but which of the following is a Cisco VPN model currently supported by Cisco?

   Answer: a. 3001

   The VPN 3001 was never a valid model number from Cisco.

7. All but which of the following is part of the Cisco SAFE Blueprint for IDS tuning?

   Answer: g. Remove the PIX Firewall.

   Removing the PIX Firewall is not part of the IDS tuning strategy.

8. What application layer protocol does a security manager use when using the Cisco Security Device Manager (SDM) application?

   Answer: d. SSL

   SDM connects to devices through Secure Sockets Layer (SSL) and SSHv2 (in SDM version 2.0), which are secure and encrypted.

9. What is the default username and password combination for a Catalyst 6500 ISDM-2 module(not the IDS 4.0)?

   Answer: d. cisco/cisco

   The default username and password are both set to cisco.

10. What is the default username and password combination for a VPN 3000 Concentrator?

    Answer: b. admin/admin

    The default username and password combination for the VPN 3000 Concentrator is admin/admin.

Q & A

1. Define the terms Cisco Secure IDS Sensor and IDS Device Manager and explain their uses.

   Answer: Cisco Secure IDS has two components:

   - **Cisco Secure IDS Sensor**—High-speed device that analyzes the content of data being transported across a network and determines whether that traffic is authorized or unauthorized. Unauthorized traffic includes ping requests from intruders. Traffic that is detected from unauthorized sources is sent directly to the Cisco IDS Device Manager, and the intruder is removed from the network (optional and set by network administrator).
   - **IDS Device Manager**—Manages up to 300 Cisco Secure Intrusion Detection System Sensors.

2. What LAN interfaces can be supported on a Cisco IDS Device Manager?

   Answer: Cisco IDS Device Manager supports Ethernet (10, 100, or 1000 MB) and no longer supports Token Ring and FDDI LAN interfaces.

3. What is the default username and password combination for a Cisco IDSM?

   Answer: The default username and password combination for a Cisco IDSM is cisco/cisco.

4. What is the default username and password combination for a Cisco VPN 3000 Concentrator?

   Answer: The default username and password combination for a Cisco VPN 3000 Concentrator is admin/admin.

5. What are three typical forms of attacks that are committed by unauthorized individuals?

   Answer: The three forms of common attacks are:

   - Reconnaissance attacks
   - Access attacks
   - Denial of service attacks

6. What is the function of the signature-based IDS?

   Answer: The signature-based IDS monitors the network traffic or observes the system and sends alarms if a known malicious event is happening. It does this by comparing the data flow against a database of known attack patterns. These signatures explicitly define what traffic or activity should be considered as malicious. An excellent white paper on signature-based IDS can be found at http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_white_paper09186a0080092334.shtml.

Chapter 6

Do I Know This Already?

1. DMZ stands for what?

   Answer: a. Demilitarized zone

2. When defining an extended access list, what TCP port numbers can you use?

   Answer: c. 0 to 65,535

   TCP port numbers from 0 to 65,535 can be used when defining an extended access list; devices such as PCs go from 1023 to 65535.

3. When defining an extended access list, what UDP port numbers can you use?

   Answer: c. 0 to 65,535

   UDP port numbers from 0 to 65,535 can be used when defining an extended access list.

4. Which of the following is *not* a TCP service?

   Answer: a. who

   who is a UDP service.

5. Which of the following is *not* a UDP service?

   Answer: a. BGP

   BGP runs over TCP port 179.

6. About how many translations does PAT (for a PIX Firewall) allow you to use for one IP address?

   Answer: b. 64,000

   Port Address Translation (PAT) occurs when the local port number is modified, allowing more than one host the ability to share one public address, for example. The port number in a TCP frame can be numbered from 0 to 65,535, so 64,000 is closest to the actual number of allowed translations.

7. PAT translates all private addresses based on what?

   Answer: c. Both source and destination ports

   PAT is based on source port; the destination port is not altered but is taken into consideration when making decisions. For example, a Telnet connection is based on the local port number (a random number generated by the device between 0 and 65,535) and the destination port number 23.

8. NAT is which of the following?

   Answer: d. Network Address Translation

9. NAT is defined in which RFC?

   Answer: d. 1631

   NAT is defined by Request for Comment (RFC) number 1631.

10. The following defines which NAT terminology: "A legitimate registered IP address as assigned by the InterNIC?"

    Answer: c. Inside global address

11. NAT might often be broken in what common scenario?

    Answer: c. By traffic that carries the source/destination IP address in the application data fields

    NAT does not work well if the application carries the details on local and remote ports in the data section, because the checksum will change and may cause CRC errors.

12. When will the command **overload**, applied to NAT configurations, possibly break a network application?

    Answer: e. With some multimedia applications

    NAT does not work well with some multimedia applications that send local and remote port details in the data stream.

13. Firewalls can operate at what three layers of the OSI model?

    Answer: d. 7, 4, 3

    Firewalls can operate at the application (7), transport (4), and network (3) layers.

14. What is the main advantage of using NAT on a firewall or Cisco IOS router?

Answer: b. Enables RFC 1918–based privately defined IP addresses to be configured and enables access to the Internet

The primary reason to use NAT is for Internet access and to hide internal IP addresses. RFC 1918 is based on privately defined IP addresses and enables access to the Internet by using NAT/PAT. It can also be used when one organization is merged with another in case the IP subnet address space is the same.

15. When using the IOS NAT **overload** command, how many inside sessions can be translated?

Answer: c. 64,000

16. What IOS command defines a pool of IP addresses for Network Address Translation (NAT)?

Answer: c. **ip nat pool**

To define a pool of IP addresses for NAT, use the **ip nat pool** command in global configuration mode. The **ip nat pool** command defines the actual registered IP addresses.

17. PIX stands for what?

Answer: c. Private Internet Exchange

18. To define how a PIX will route IP data, what is the correct syntax for a PIX?

Answer: b. **route**

A PIX can run RIP or be configured for static routing; a default route is typically required so that end-user data can be sent to the Internet, for example.

19. If you configure NAT on an Cisco IOS router, what command is used to enable PAT?

Answer: d. **overload**

The **overload** command enables the router to use one global address for many local addresses. When overloading is configured, the TCP or UDP port number of each inside host distinguishes between the multiple conversations using the same local IP address.

20. Cisco IOS–based NAT provides all of the following functions *except* one; which one?

Answer: b. It can be traced or viewed by an outside address

Cisco IOS–based NAT does not permit an inside host to be traced from an Internet or outside address.

21. Which of the following is not considered a security device?

Answer: d. Microsoft Windows XP Professional

PIX, switches, IDS, and VPN Concentrators are all considered devices that provide security.

22. What extended IP access list will prevent the internal subnet 10.0.0.0/8 from being spoofed on a Cisco IOS–enabled router? (Assume **permit** statements are applied to allow legitimate traffic.)

Answer: d. **access-list 100 ip deny 10.0.0.0 0.0.0.255 0.0.0.0 any**

The correct command to deny the 10.0.0.0/8 is **access-list 100 ip deny 10.0.0.0 0.0.0.255 0.0.0.0 any**. Of course, you must also apply the ACL to the interface.

23. What is the **alias** command's function on a PIX Firewall?

Answer: c. The **alias** command is used in NAT environments where one IP address is translated into another

The PIX **alias** command is used for NAT configurations. (The **alias** command is replaced in newer versions with a **dns** keyword in **static** and **nat** commands.) The **alias** command translates one IP address into another address. For example, one private network might be using unregistered IP address space, and to allow users access to outside address space, the **alias** command is used. This command is applied differently on a Cisco IOS router.

PIX Firewall software version 6.2 allows NAT of external source IP addresses for packets traveling from the outside interface to the inside interface. All functionality available with traditional NAT, such as fixups, stateful failover, dynamic NAT, static NAT, and PAT, are available bidirectionally in this release.

24. CBAC stands for what?

Answer: c. Context-Based Access Control

25. What is IKE used to accomplish?

Answer: c. To ensure that data is not viewable by unauthorized sources

Internet Key Exchange (IKE) ensures that network confidentiality is protected against unauthorized sources.

26. To create a simple VPN tunnel (unencrypted) between two sites, what must you do on a Cisco router?

Answer: a. Create a GRE tunnel

A simple VPN tunnel requires a generic routing encapsulation (GRE) tunnel between two Cisco routers.

27. PIX Firewall software version 6.3 can support which of the following routing protocols? (Choose the best three answers.)

Answers: b. OSPF

c. RIP version 1

d. RIP version 2

PIX Firewall software version 6.3 is now capable of supporting RIP versions 1 and 2 along with OSPF.

28. To support OSPF on a PIX Firewall version 6.3–capable firewall, what additional OSPF authentication mechanisms are possible? (Choose the best two answers.)

Answers: a. MD5

c. Password

OSPF can be tightened with secure options by enabling MD5 password authentications. OSPF will not become an adjacent neighbor with a device configured in the wrong area, but this cannot be regarded as an authentication mechanism. However, this can be viewed as a light security option as well. This is a very tricky question. RADIUS and the two other security application protocols cannot be used to secure OSPF.

29. What PIX command can be used for a dual NAT environment?

Answer: c. **alias**

The **alias** command can be used for two scenarios, dual NAT or DNS doctoring. PIX Firewall 6.3 now has bidirectional NAT, however the **alias** command is still being tested.

30. What PIX command is used on a PIX Firewall to view address mappings when NAT is enabled?

Answer: d. **show xlate**

31. If a PIX Firewall is configured without a conduit or an access list, data from the inside interface is dropped. In effect, the PIX Firewall is acting like which of the following? (Select the best two answers.)

Answers: d. Bit bucket

e. Black hole router

If there are no conduits/access lists, then any data from the outside interface will be dropped or thrown away, resulting in the PIX Firewall acting as a bit bucket or black hole router. A bit bucket is commonly referred to as a router throwing out bits or bytes. A black hole router is the same thing!

32. After viewing the PIX syslog with the command **show logging**, the following output is discovered:

```
14:25:02 10.1.1.1 : %PIX-7-7100006: TCP request discarded from 6.3.62.119/57000
      to inside:10.1.1.1/www
```

Assuming the inside interface on the PIX is configured for the IP address 10.1.1.1/24, which of the following answers best describes what *might* be going on in the network?

Answer: c. A host on the inside has launched a denial of service (DoS) attack generating random source addresses aimed at the PIX inside interface.

Severity level 7 is a debug message, and this particular message indicates an inside host is launching a random DoS attack aimed at the inside interface 10.1.1.1 using HTTP or the World Wide Web.

33. Which of the following statements best describes Cisco Threat Response (CTR)?

Answer: a. CTR reads IDS alarms and performs automated forensics on hosts or servers that may have been compromised.

Cisco Threat Response technology provides an automated, just-in-time, around-the-clock, real-time analysis of each targeted host to determine whether a compromise has occurred and to determine how to address it quickly. Additionally, CTR reads IDS alarms and performs automated tasks.

34. Which of the following best describes Cisco Security Agent (CSA)?

Answer: b. CSA uses a set of predefined rules to protect host-based systems such as PCs or servers.

35. Which of the following describes the default rules a host version of the Cisco Security Agent accomplishes? (Choose the best three answers.)

Answers: a. Prevents writing to the system directory.

b. Stops unauthorized systems from initiating network connections to the CSA-protected host.

e. Prevents updates to the system registry.

36. IEEE 802.1X is primarily used for what purpose?

Answer: d. Allow Layer 3 communication and authenticate clients

The primary function of IEEE 802.1X is to authenticate clients and permit Layer 3 communications.

37. What device initiates the first communication in IEEE 802.1X?

Answer: c. The end workstation connected to the switch

IEEE 802.1X is initiated by the end workstation connected to the active Layer 2/3 switch.

38. CSA is supported on what two platforms?

Answers: a. Windows

b. UNIX

CSA is supported on Windows and UNIX platforms only.

39. How does anomaly-based intrusion detection recognize that a network attack is in progress?

Answer: b. The IDS normalizes network traffic and sends alarms when sampled traffic falls out of that norm.

Anomaly-based IDS checks network traffic for patterns falling outside normal packet structures.

Q & A

1. What does the term DMZ refer to?

Answer: The DMZ, or demilitarized zone, is defined as an isolated part of the network that is easily accessible to hosts on the outside (Internet, for example).

2. What is the perimeter router's function in a DMZ?

Answer: The perimeter router sits between the DMZ and the public domain. It is typically a high-performance router (or routers) that performs a number of duties, including the following:

- Uses access lists to ensure access to IP is restricted
- Sets restrictions to TCP services
- Sets restrictions on what applications can be run
- Sets routing protocols (typically, BGP)

Typically the DMZ is a third interface on a firewall containing the inside and outside interface also.

3. Extended access lists filter the services of what two main transport layer protocols?

Answer: Extended access lists filter both TCP and UDP transport layer services.

4. Which of the following is *not* a TCP service?

   a. Ident

   b. FTP

   c. pop3

   d. pop2

   e. echo

   Answer: Echo is part of the UDP protocol suite. Ident, FTP, and pop2/pop3 are TCP services.

5. Name five UDP services that can be filtered with an extended access list.

   Answer: Cisco IOS can filter a number of UDP services, including the following:

   - **biff**—Biff (mail notification, comsat, 512)
   - **bootpc**—Bootstrap Protocol (BOOTP) client (68)
   - **bootps**—Bootstrap Protocol (BOOTP) server (67)
   - **discard**—Discard (9)
   - **dnsix**—DNSIX security protocol auditing (195)
   - **domain**—Domain Name Service (DNS, 53)
   - **echo**—Echo (7)
   - **isakmp**—Internet Security Association and Key Management Protocol (500)
   - **mobile-ip**—Mobile IP registration (434)
   - **nameserver**—IEN116 name service (obsolete, 42)
   - **netbios-dgm**—NetBIOS datagram service (138)
   - **netbios-ns**—NetBIOS name service (137)
   - **netbios-ss**—NetBIOS session service (139)
   - **ntp**—Network Time Protocol (123)
   - **pim-auto-rp**—PIM Auto-RP (496)
   - **rip**—Routing Information Protocol (router, in.routed, 520)
   - **snmp**—Simple Network Management Protocol (161)
   - **snmptrap**—SNMP traps (162)
   - **sunrpc**—Sun Remote Procedure Call (111)
   - **syslog**—System Logger (514)
   - **tacacs**—TAC Access Control System (49)

- **talk**—Talk (517)
- **tftp**—Trivial File Transfer Protocol (69)
- **time**—Time (37)
- **who**—Who service (rwho, 513)
- **xdmcp**—X Display Manager Control Protocol (177)

6. What RFC defines NAT?

Answer: Network Address Translation (NAT) is defined in RFC 1631.

7. In NAT, what is the inside local address used for?

Answer: The inside local address refers to the IP address that is assigned to a host on the internal network—that is, the logical address that is not being advertised to the Internet. A local administrator generally assigns this address. This address is not a legitimate Internet address.

8. What does the IOS command **ip nat inside source list** accomplish?

Answer: It defines the addresses that will be allowed to access the Internet. This command enables NAT of the inside source addresses. The **list** keyword helps define the access list to be used for determining the source addresses.

9. What are the four possible NAT translations on a Cisco IOS router?

Answer: The four NAT translation versions are as follows:

- **Static NAT**—Maps an unregistered IP address to a registered IP address on a one-to-one basis.
- **Dynamic NAT**—Maps an unregistered IP address to a registered IP address from a group of registered IP addresses.
- **Overloading**—A form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address using different ports. Known also as Port Address Translation (PAT), single address NAT, or port-level multiplexed NAT.
- **Overlapping**—When the IP addresses used on your internal network are registered IP addresses in use on another network, the router must maintain a lookup table of these addresses so that it can intercept them and replace them with registered unique IP addresses.

10. How many connections can be translated with a PIX Firewall for the following RAM configurations: 16 MB, 32 MB, and 256 MB?

Answer: You can support up to 7500 connections with 16 MB, 25,000 connections with 32 MB, and 280,000 connections with 256 MB.

11. When the **alias** command is applied to a PIX Firewall, what does it accomplish?

Answer: The **alias** command translates one address into another, and is used for translating unregistered IP addresses in a NAT environment. The PIX Firewall software version 6.2 and above allows NAT of external source IP addresses for packets traveling from the outside interface to the inside interface. All functionality available with traditional NAT, such as fixups, stateful failover, dynamic NAT, static NAT, and PAT, are available bidirectionally in this release.

12. What security features does the Cisco IOS Firewall feature set allow a network administrator to accomplish?

Answer: The Cisco IOS Firewall feature set consists of the following:

- **Context-based Access Control (CBAC)**—Provides to internal users secure, per-application-based access control for all traffic across perimeters, such as between private enterprise networks and the Internet.
- **Java blocking**—Protects against unidentified, malicious Java applets.
- **DoS detection and prevention**—Defends and protects router resources against common attacks, by checking packet headers and dropping suspicious packets.
- **Audit trail**—Details transactions, recording time stamp, source host, destination host, ports, duration, and total number of bytes transmitted.
- **Real-time alerts**—Logs alerts in case of DoS attacks or other preconfigured conditions.

13. What does CBAC stand for?

Answer: Context-Based Access Control

14. Name the eight possible steps to take when configuring CBAC.

Answer: To configure CBAC, the following tasks are required, except for the last task, which is optional:

1. Pick an internal or external interface.
2. Configure IP access lists at the interface.
3. Configure global timeouts and thresholds.

4. Define an inspection rule.
5. Apply the inspection rule to an interface.
6. Configure logging and audit trail.
7. Follow other guidelines for configuring a firewall.
8. Verify CBAC. (Optional)

15. What is a virtual private network?

Answer: A virtual private network (VPN) enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses tunneling to encrypt all information at the IP level.

16. What type of attacks can be mitigated by CSA?

Answer: The types of attacks that can be stopped by CSA are numerous. The following is a list of these attacks and the corresponding countermeasures taken by CSA:

- **Probes**—CSA prevents scanning of ports and ping packets.
- **Penetration**—CSA prevents unauthorized mail attachments from running, buffer overflows, ActiveX controls, network installs, backdoors, guessing passwords, and guessing of mail users.
- **Persist**—CSA prevents new file creation, modification of existing files, and registration of trap doors.
- **Propagate**—CSA prevents mail clients from sending out e-mails to propagate the attack, web connections, FTP, and infecting file shares.
- **Paralyze**—CSA does not permit deletion or modification of files and prevents drilling of security holes (opening new doors to provide an opening into your network or device).

17. What are the three possible states with an 802.1X connection?

Answer: The switch port can be in one of three states:

- **Authorized**—Successful authentication and normal packet flow.
- **Unauthorized 802.1X**—If a client device does not support 802.1X authentication, the port is left unauthorized.
- **802.1X enabled**—If a client is enabled for 802.1X but the switch port is not configured for 802.1X support, the client initiates but will not receive a reply. The client then sends packets, assuming that the authorization was granted.

Chapter 7

Do I Know This Already?

1. A remote user tries logging into a remote network but fails after three additional tries and is disconnected. What useful information should the network administrator gather? (Select the best two answers.)

   Answers: b. Invalid password

   c. Invalid username

   The network administrator needs the invalid username (because it is not an allowable username) and the invalid password used, to determine whether the intruder is using a text-based algorithm to generate usernames and passwords.

2. If a remote user Telnets to a router but accidentally types the incorrect password or username, which of the following events is *not* required by the security administrator in this organization? (Select the best two answers.)

   Answers: a. Invalid password

   b. Invalid username

   A security administrator does not want to receive details on valid users accidentally entering incorrect passwords but rather is more concerned with access denied messages, authorization failures, and authentication failures generated by the logon attempts of unauthorized users. A large number of retries would also raise a concern for any security manager, for both valid users and invalid users.

3. What is the first step that should be implemented in securing any network?

   Answer: d. Define a security policy.

   The first step in securing any network must be to define the security policy.

4. Why would a security administrator decide to install a stateful firewall?

   Answer: c. Stateful firewalls ensure that all traffic returning from a router originated inside the network, unless a static policy on the firewall permits otherwise.

   Each time a TCP connection is established from an inside host accessing the Internet through the PIX Firewall, the information about the connection is logged in a stateful session flow table. The table contains the source and destination addresses, port numbers, TCP sequencing information, and additional flags for each TCP connection associated with that particular host. Stateful firewalls are not cheap and can be compromised if configured incorrectly. Stateless firewalls treat each network frame (or packet) in isolation. A stateless firewall has no way of knowing whether any given packet is part of an existing connection, is trying to

establish a new connection, or is just an unauthorized packet. Note that stateful connections not only apply to TCP but also fit stateless firewalls that have the ability to check for the TCP SYN/ACK bits. The **established** keyword on extended lists does just that, but ACLs on routers are still considered stateless. DNS inquiries (UDP based, of course) are one of the main reasons stateful firewalls are so popular. When a user makes an outgoing inquiry, the stateless firewall can create a temporary incoming rule that allows DNS replies from the DNS server being queried, to the user who made the request, on the ephemeral port that the user chooses.

5. What primary security method can be designed and deployed to secure and protect any IP network after an attack has been documented?

Answer: c. Countermeasures

Countermeasures should be in place in every IP network. Examples of countermeasures are to back up sensitive data and application software and apply all the required patches.

6. A security administrator notices that a log file stored on a local router has increased in size from 32 kb to 64 kb in a matter of seconds. What should the network administrator do?

Answer: c. Log the event as suspicious and notify the incident response team.

Any log file that increases (more data to view) or decreases (for example, cleared by the intruder to hide his actions) should be regarded as suspicious activity.

7. What is the primary responsibility of CERT/CC?

Answer: d. Maintain a security standard for networks

CERT/CC's primarily responsibility is to aid in the security of any public network; go to http://www.cert.org for more details.

8. Who can use network scanners and probes? (Select the best two answers.)

Answers: a. Intruders

b. Security managers

Network scanners are used by intruders just as network administrators use them.

9. What is a bastion host?

Answer: c. Network's first line of defense

Bastion hosts are typically the first line of defense. Sometimes, they are sacrificed because they are typically public domain servers and can be quickly restored using backup methods.

10. A TCP SYN attack is what type of attack?

Answer: b. DoS

A TCP SYN attack is a form of denial-of-service (DoS) attack.

11. When an intruder sends a large amount of ICMP echo (ping) traffic using IP broadcasts, this type of DoS attack is known as what?

Answer: d. Smurf

A Smurf attack sends a large amount of ICMP or ping requests via a broadcast address, ensuring that all devices on the remote network respond and enabling the intruder to list the IP address that is connected to the network for further DOS-based attacks.

12. Assuming two devices are running IPSec over the Internet, what form of attack is likely to compromise any data sent over the Internet?

Answer: d. Man-in-the-middle

The man-in-the-middle attack can manipulate routing tables and have data re-sent to the wrong destination, thus compromising data. The end result is loss of data connectivity. All of the answers can result in data loss, but man-in-the-middle attack is the most correct answer.

13. What kind of attack sends a large number of ICMP echo request packets with the intent of overflowing the input buffers of the destination machine and causing it to crash?

Answer: a. Ping of death

A ping of death sends a large number of ICMP echo request packets, causing the end device to overflow and possibly causing a remote server to stop functioning for legitimate requests.

14. In the context of intrusion detection, what is an exploit signature?

Answer: b. An attack that is recognized and detected on the network

15. A network scanner can be used for what primary function?

Answer: c. To exploit network vulnerabilities

This is a typical example of the Cisco testing methodology. Because there is only one best answer, you must eliminate answers before picking the correct option. Option a, "To exploit HTTPs passwords," is clearly incorrect because HTTPs sessions are encrypted. Network signatures require more sophisticated tools than just network scanners. Scanners cannot find the location of intruders, and they cannot advise management of a threat, so option c, "To exploit network vulnerabilities," is the best possible option for this question. The *primary function* of network scanners is to exploit network vulnerabilities.

16. If a network manager believes that a host has been compromised on a router or host device and wishes to have the Certificate Authority certificate revoked, how can the security team accomplish this?

Answer: b. Contact the Certificate Authority administrator and be prepared to change the secret password.

If the CA certificate has been compromised, because the CA entity issues digital certificates and vouches for the binding between the data items in a certificate (for example, between a router and a PC), the CA certificate must be invalidated and a new CA certificate must be created. This is typically achieved by two administrators using a new secret password. The security manager or administrator contacts the CA administrator and has it revoke the certificate. A new public/private key pair is generated and then a new certificate is requested based on the new keys. This allows the hosts to be secured once more.

17. What is the best mechanism against sniffer-type programs that try to determine the network passwords between hosts and clients? (Select at most three answers.)

Answers: b. IPSec

c. One-time passwords

d. Kerberos or SSH

Sniffer password programs are useless if IPSec is in use, because the data is completely encrypted. One-time passwords ensure that even if an intruder does compromise the password, it will be invalid because it can be used only once. Finally, SSH and Kerberos are secure protocols and do not send data as clear text, as do applications such as Telnet and POP e-mail. One aspect of this exam's blueprint is that even though Kerberos is removed, it may still appear on the exam.

18. What is the main goal of a Trojan horse application?

Answer: b. A malicious piece of code or programming designed to capture usernames and passwords

A Trojan horse is a malicious piece of code or programming that is disguised as something benign. Typically, a Trojan horse masquerades as a program that claims to rid your computer of viruses but instead introduces a virus into your computer. A Trojan horse may be a piece of code used to capture usernames/passwords, or it may have another agenda, such as to erase your disk, capture your credit card numbers, or control your PC. *Trojan horse* refers to the wooden horse presented to the city of Troy as gift from the Greeks during the Trojan war, inside of which were Greek soldiers who then launched a sneak attack on Troy once the horse was within the city walls (not a likely test question, of course).

19. Which of the following are traditional defense-in-depth security options? (Select the best two answers.)

Answers: d. Use of authentication

e. Implementing a perimeter defense

Traditional defense-in-depth security measures typically include the use of authentication and perimeter defenses such as firewalls and routers with Cisco IOS–based security measures in place.

20. To stop spam e-mail from overwhelming an e-mail server, what step can you take?

Answer: c. Install an intrusion detection system that has a signature for spam e-mail.

Spam e-mail can be controlled with an IDS server.

21. What is an SYN flood attack?

Answer: c. A flood of TCP connection requests with randomized ports and addresses

This form of DoS attack randomly opens a number of TCP ports, ensuring that network devices are using CPU cycles for bogus requests; it also uses randomized source IP addresses. The key to this style of attack is the use of randomized IP addresses.

22. View the following ARP table:

```
SimonRules#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.135.11           -   00b0.8ef5.9038  ARPA   E0
Internet  10.1.31.1              -   00b0.8ef5.908c  ARPA
Internet  10.1.30.1              -   00b0.8ef5.9070  ARPA   Cable4/0
Internet  10.1.30.106          200   0010.7bb3.fb7b  ARPA   E0
Internet  10.1.30.108          200   0001.64ff.eb3d  ARPA   E0
Internet  10.1.30.109            -   0002.fdfa.0a63  ARPA    E0
```

What address do you suspect might be involved in launching an attack of some form? (Select the best two answers.)

Answers: b. 10.1.30.106

c. 10.1.30.108

In the Age column in the **show arp** output, anything locally connected to the router is indicated with the –. The two entries 10.1.30.106 and 10.1.30.108 are not locally connected devices, and the Age time set to such a high number of minutes indicates a high level of activity that should be considered suspicious.

23. Which of the following describes an attack that falsifies a broadcast ICMP echo request and may include a primary and secondary victim?

Answer: e. A smurf attack

A smurf attack is one in which an intruder sends to an IP broadcast address (or addresses) a large number of ICMP echo (ping) requests, all of which have a victim's spoofed source address.

24. What are the common drawbacks of antivirus software such as Norton AntiVirus? (Select the best two answers.)

Answers: a. The software is difficult to keep up to date when new viruses are released.

d. Attackers frequently re-code their programs to bypass antivirus systems.

Antivirus software is still a first form of defense but lacks basic update capability when new worms are created and cannot be easily reprogrammed when new forms of viruses are released by attackers.

Q & A

1. Define four reasons for why networks must be secured.

Answer: IP networks must provide network security for the following reasons:

- **Inherent technology weaknesses**—All network devices and operating systems have inherent vulnerabilities.
- **Configuration weaknesses**—Common configuration mistakes can be exploited to open weaknesses.
- **Security policy vulnerabilities**—The lack of security policies can lead to vulnerabilities, such as password security.
- **Outside/inside intruders**—There are always internal and external people who want to exploit network resources and retrieve sensitive data.

2. What is the function of the CERT/CC organization, and what are its primary objectives?

Answer: The CERT Coordination Center (CERT/CC) is a center of Internet security expertise, located at the Software Engineering Institute, a U.S. federally-funded research and development center operated by Carnegie Mellon University. CERT/CC provides information that helps you to protect your networks from potential problems, react to current problems, and predict and prepare for future problems. Its work involves handling computer security incidents and vulnerabilities, publishing security alerts, researching long-term changes in networked systems, developing security information, and even providing training to help you

improve security. CERT/CC does not concern itself with the identity and location of the intruder, but instead tries to restore and prevent similar attacks in the future. CERT/CC is regarded as the industry leader in security concerns.

3. What are the primary steps completed by incident response teams?

Answer: Incident responses teams do the following:

Step	Description
1	Verify the incident.
2	Determine the magnitude of the incident (hosts affected and how many).
3	Assess the damage (for example, determine if public servers have been modified).
4	Gather and protect the evidence.
5	Inspect systems to determine damage.
6	Remove hostile or destructive code.
Step	**Description**
7	Reload necessary operating system software.
8	Restore configurations.
9	Restore and test operations.
10	Patch system to reduce vulnerability.
11	Inspect applications to determine damage.
12	Reload software if necessary.
13	Test functionality.
14	Inspect files to determine damage.
15	Restore files from backup if necessary.
16	Replicate damaged files if no backup is available.
17	Confirm with users that data is restored.

Answer: The CCIE Security candidate is not expected to memorize these tasks but should have knowledge of the general points considered when an incident report is complied.

4. Name common methods used by intruders to disrupt a secure network.

   Intruders can use the following methods (and many more) to disrupt a secure network:

   - **Session hijacking**—The intruder defines himself with a valid IP address after a session has been established to the real IP address, by spoofing IP packets and manipulating the sequence number in an IP packet.
   - **Rerouting**—Packets from one source are routed to an intruder source. Routing updates are altered to send IP packets to an incorrect destination, allowing the intruder to read and use the IP data inappropriately.
   - **Denial-of-service (DoS) attack**—A service attack that is used in an attempt to deny legitimate users access to a network they have full rights to.
   - Probes and scans.
   - Malicious code.

5. In security, what is TCP session hijacking?

   Answer: TCP session hijacking is when an attacker or intruder takes over a TCP session between two machines. Because most authentication occurs at the start of a TCP session only, this attack allows the hacker to gain access to a machine by assuming the role of the trusted source.

6. In security terms, what is a man-in-the-middle attack?

   Answer: A man-in-the-middle attack abuses weak or nonexistent authentication mechanisms between two endpoints. By inserting himself between these endpoints, the attacker not only can view information passing back and forth, but can even modify or inject data going into such a connection.

7. What is a signature engine?

   Answer: A signature engine is a component designed to support many signatures in a certain category. An engine is composed of a parser and an inspector. Each engine has a set of legal parameters that have allowable ranges or sets of values. Exploit signatures are an identifiable pattern of attack.

8. What is social engineering?

   Answer: Social engineering is the act of tricking or coercing employees into providing information, such as usernames or mail user identifications and even passwords. First-level phone support personnel are typically called by intruders, pretending to work for the company, to gain valuable information.

9. What is a ping of death attack?

   Answer: A ping of death occurs when a large number of ping request packets cause the end device to overflow. For example, a ping of death can cause a remote server to stop functioning for legitimate requests.

10. What is a Land.C attack?

    Answer: A Land.C attack is a program designed to send TCP SYN packets (TCP SYN is used in the TCP connection phase) that specify the target's host address as both source and destination. This program can also cause a system to stop functioning.

11. What does the following Cisco IOS code accomplish on a Cisco IOS router?

```
no service udp-small-servers
no service tcp-small-servers
```

    Answer: These commands disable the minor TCP/UDP servers. When the minor TCP/UDP servers are disabled, access to the Echo, Discard, Chargen, and Daytime ports causes the Cisco IOS software to send a TCP Reset packet (only with the **tcp-small-servers** command) to the sender and discard the original incoming packet. When these commands are entered in global configuration mode, they do not display when you view the configuration (**show running-config** or **write terminal**) because the default is to disable TCP/UDP small servers. Unlike Cisco switches, Cisco IOS software does not display default configuration.

12. What is the secret password for the following Cisco IOS configuration?

```
enable secret %$@$%&^$@*$^*@$^*
enable pass cisco
```

    Answer: Secret passwords are encrypted using the MD5 hashing algorithm, so you cannot decipher the secret password, which overrides the enable password.

13. What is the purpose of the command **service sequence-numbers**?

    Answer: Essentially, this command enables your syslog entries to be numbered so that you can easily put them back in order.


Catalyst 6500

APPENDIX B

Study Tips for CCIE Security Examinations

This appendix describes some study tips and options for you to consider while preparing for the CCIE Security written and lab examinations.

CCIE is regarded as the most sought-after certification in the industry today; more and more vendors are devising their own certification programs and trying to catch up to the industry-leading Cisco Systems. Working in the CCIE program for the past two years, I have seen many changes and challenges facing potential CCIEs every day. At the end of 2004, there were over 11,000 CCIEs, and the number is growing rapidly. Of all the CCIEs, over 500 hold more than one CCIE certification. The majority of CCIEs are located in Europe and North America. The number of Security CCIEs is over 400. To view the latest CCIE security numbers, visit http://www.cisco.com/en/US/learning/le3/ccie/certified_ccies/worldwide.html.

Before you decide to take this step, you need to be aware of the challenges in front of you. You cannot hope to become a CCIE by simply buying a book or a series of books. Hands-on experience is required, and at least two years of internetworking experience is critical; even then, you must fully prepare for the difficult exams. The current five varieties of CCIE certification follow:

- CCIE Routing and Switching (released 1993)
- CCIE Security (released 2001)
- CCIE Service Provider (released 2001; also renamed several times)
- CCIE Storage Networking (released 2004)
- CCIE Voice (released 2004)

A new CCIE Design lab is in the pipeline and will be a more innovative approach to testing by Cisco in the future.

This discussion concentrates on the CCIE Security certification. The CCIE Security exam is one that you should consider tackling, especially in today's climate of Internet firewall frailty and demand for security experts.

NOTE For more information on the Security track, see the following:

http://www.cisco.com/en/US/learning/le3/ccie/security/index.html

Four CCIE tracks have been retired: ISP Dial, SNA, Design (will be re-released in a new format), and WAN Switching.

Steps Required to Achieve CCIE Security Certification

The CCIE Security certification requires a candidate to pass two exams:

- A 2-hour, computer-based written exam (#350-018) consisting of 100 questions. The pass mark is approximately 70 percent, but varies according to statistics and could float between 65 and 75 percent. This book is designed to help prepare you for this written exam.
- An 8-hour lab exam. The passing score is set at 80 percent. Historically, the lab exam was a full 2-day lab; that changed October 1, 2001. All CCIE lab exam versions are monitored closely and adapted where necessary to conform to the CCIE program standards, which are not publicly available. This book contains supplemental material intended to help you prepare for the lab exam, but does not focus on it.

CCIE Security Written Exam

The CCIE Security written exam uses the typical certification test format of asking multiple-choice questions with one or more correct answers per question. What makes some of the questions more difficult is that more than five answer choices are listed on some questions. This reduces the power of eliminating answers and choosing from those remaining. However, the number of required answers is given for each question. You might be required to give only one answer or select a couple of correct answers. Attempt to answer every question, even if you have to guess, to give yourself the best chance of passing.

After completing the test, you will be given a percentage for each section. You will be scored in the following sections:

- Security Protocols
- Application Protocols
- General Networking
- Security Technologies
- Cisco Security Applications
- Security General
- Cisco General

If you do not receive a passing score, compare your results with the table showing the CCIE Security written exam blueprint in this book's introduction to identify the areas you need to concentrate on for your next attempt.

You will also be given the passing mark, your score, and your grade. The grade is either a pass or fail.

The exam is similar to other Cisco certification exams, albeit it is a little more difficult because it has many more in-depth questions. You can view five sample questions from the exam at the following location:

http://www.cisco.com/en/US/learning/le3/ccie/security/sample_questions.html

The CCIE Security written exam requires test-taking skills that many of us learned in high school or college. This section is a refresher for many and important for all.

The first thing to focus on is time management during the test. The CCIE exam allows 120 minutes to complete the test. You have 100 questions, so if you allow 1 minute per question and 20 minutes to review your answers, you will be doing well.

Some questions require more time, so you can mark and skip them if you want and complete them later. Be sure, before moving on to the next question, that the application on the testing device permits a review of questions; Cisco can change this at any time.

Remember that a wrong answer incurs no extra penalty, so answer all the questions. Another advantage of marking difficult questions and returning to them at the end is that often the answer for a previously asked question will appear in a later question. I have also found that, at times, when I can't remember an answer that I should know, my memory is later refreshed by another question. Remember to just mark questions that you can't answer and come back to them at the end.

Read every question and all the possible answers carefully. The CCIE Security written exam has many questions that are designed to be tricky, so they require careful examination of the syntax. Many of the questions refer to exact commands required to implement a function on a router. It is important to know the different syntax and to recognize small differences in commands. This book has similarly formatted questions in each chapter and in the sample questions on the CD-ROM. Go through these questions, study areas of weakness, and go through the questions again to ensure your understanding of a subject.

Make sure you read every answer before choosing one. One answer might sound great; however, another answer could be more correct than the first. The fact that on these exams one answer can be more or less correct than another is a concept you should keep in mind when taking any Cisco

exam. In addition, saying questions out loud or writing them down on your scrap paper might help you understand the question easier than viewing it on a computer screen.

NOTE Occasionally, Cisco announces a beta trial for the written exams, and if you book the test, you pay only a small fee compared to the standard fee of approximately U.S.$350. The following link has more information:

http://www.cisco.com/en/US/learning/le3/ccie/announcements/index.html

Decoding Ambiguity

Cisco exams have a reputation for including questions that can be difficult to interpret, confusing, or ambiguous. In my experience with numerous exams, consider this reputation to be completely justified. The Cisco exams are deliberately tough.

The only way to beat Cisco at its own game is to be prepared. You'll discover that many exam questions test your knowledge of things that are not directly related to the issue that a question raises. This means that the answers you must choose from—even incorrect ones—are just as much a part of the skill assessment as the question itself. If you don't know something about most aspects of the CCIE Security written exam topics, you might not be able to eliminate obvious wrong answers. In other words, the more you know about Cisco IOS Software and securing Cisco internetworks, the easier it will be for you to tell a right answer from a wrong one.

Questions often give away their answers, but you have to be Sherlock Holmes to see the clues. Often, subtle hints appear in the question text in such a way that they seem almost irrelevant to the situation. You must realize that each question is a test unto itself, and you must inspect and successfully navigate each question to pass the exam. Look for small clues, such as access list modifications, problem isolation specifics (such as which layers of the OSI model are not functioning correctly), and invalid Cisco IOS commands. Little things like these can point to the right answer if properly understood; if missed, they can leave you facing a blind guess.

Another trick is to watch out for keywords, such as *not* or choose *the best*; these words will define the required answer. If you miss keywords, your answer will be correct in your mind but might not be the correct answer. Read questions out loud or write them down to ensure that you identify keywords and fully understand what the question is asking.

For questions requiring more than one answer, be sure to view how many answers are required and remove the obvious choices before making your selection. These questions are frequently ambiguous, and you need to be on your guard.

Another common difficulty with certification exams is vocabulary. Be sure to brush up on the key internetworking terms presented in this guide. You may also want to read through the Terms and Acronyms on the following Cisco.com web page:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm

The test questions appear in random order, and many elements or issues that receive mention in one question might also crop up in other questions. It is not uncommon to find that an incorrect answer to one question is the correct answer to another, or vice versa. Take the time to read every answer to each question, even if you recognize the correct answer to a question immediately.

Because you are taking a fixed-length test, you can revisit any question as many times as you like. If you are uncertain of the answer to a question, check the box that is provided to mark it for easy return later on. You should also mark questions you think might offer information that you can use to answer other questions. Candidates usually mark between 25 and 50 percent of the questions on exams. The testing software is designed to let you mark every question if you choose; use this framework to your advantage. Everything you want to see again should be marked; the testing software can help you return to marked questions quickly and easily. Be sure to check out the latest updates from Cisco, because policies like these can change; see the following URL for more details:

http://www.cisco.com/en/US/learning/le3/ccie/announcements/index.html

The best method to pass any Cisco written exam is to take a three-phase approach. In your first pass, go through each question and answer the questions that you are confident you know and mark the remaining questions. After you complete the 100 questions, review all of your marked questions.

On your second pass, survey more thoroughly the questions that you marked and begin to answer them systematically and consistently. Try to eliminate the choices that are way off base and make an educated guess for the remaining choices. Continue to mark and ignore the questions for which you have no clue. On your third pass, attack the remaining questions; by then, you might be able to make a more educated guess based on clues in the context of other questions you already answered.

If you have time, you can go back and check all your answers. Experience has shown me that my first reaction to a question is typically the best choice unless I see a glaring mistake upon reexamination.

Preparing for the Written Exam

The best way to prepare for the test—after you study—is to take practice exams until you feel comfortable with your results. This certification guide includes over 500 simulated test questions on the CD-ROM, which allows you to take the sample exam (in study and exam simulation modes)

as many times as you like until you are comfortable with the test format and your knowledge level. Try to identify subject areas where you are weak and use this book and other resources to study those areas more.

Give yourself 120 minutes to take the practice exam, keep yourself on the honor system, and don't look at text in the book or jump ahead to the answer key. When your time is up or you finish the questions, go back and review your correct and incorrect answers. You learn more by making mistakes in a simulation than from the real exam, which provides little feedback on incorrect answers. Study your incorrect answers very carefully. Practice the three-phase approach described in the preceding section (or, if you have your own strategy, practice it a few times) before attempting the real exam.

I have attempted to estimate the number of questions that are taken from each subject area to give you an idea of where to focus the majority of your time. Each chapter contains a weighted number of questions to match those on the exam, and similarly, the CD-ROM simulation exams are weighted, as well. For example, approximately 50 percent of the CD-ROM questions are based on Routing and Switching topics, and the remaining 50 percent are on Security topics, to mimic the questions on the real exam. The percentage of questions you get for any topic will vary. The passing score will also vary. If you concentrate on the questions and think clearly, you will not need to worry about the passing score.

Knowing how to recognize correct answers is good, but understanding why incorrect answers are wrong can be equally valuable.

I cannot stress enough how helpful getting hands-on experience with Cisco routers and switches is to passing not only the written exam, but also the more difficult lab exam. Using a small test bed with two Cisco routers and a PC is the best way to learn and reinforce your theoretical knowledge. I strongly recommend it even for the written exam, which, in turn, aids your preparation for the lab exam.

Cisco provides, with every shipment of Cisco hardware (for example a Cisco 3845 IOS router), a Cisco Documentation CD with a wealth of information that you can implement on test equipment. The documentation CD is a great study tool. It is provided for the laboratory exam, not the written exam. Understanding how a protocol works is only half your goal; you need to appreciate how Cisco routers and switches operate when a certain protocol is activated with Cisco IOS software.

Talk to all of your colleagues or friends who attempted the written exam and find out what they studied to help them. Of course, all who have taken the exam are bound by the nondisclosure agreement, so you cannot share specific details about exam content, but you can share study tips and habits.

Taking the Written Exam

On exam-day eve, you should relax and spend a maximum of one hour studying. Make sure you have prepared in advance enough that you don't sit up all night studying and worrying—if you want to do your best, you need to feel refreshed. Have a good meal, scan your study materials (such as the "Foundation Summary" sections in this book), and get a good night's sleep.

On the day of the exam, eat a well-balanced breakfast and briefly review your study notes. Make sure that you arrive at the testing center at least one hour before your scheduled time. Find a quiet corner to relax and mull over the main exam subjects.

When you are sitting in front of the testing computer, there is nothing you can do to increase your knowledge or preparation. Take a deep breath, stretch, and read the first question.

Don't rush; you have plenty of time to complete each question. Both easy and difficult questions are intermixed throughout the test in random order. Don't cheat yourself by spending too much time on a hard question early in the test, depriving yourself of the time you need to answer the questions at the end of the test.

On a fixed-length test, you can read through the entire test and, before returning to marked questions for a second visit, figure out how much time you have per question. As you answer each question, remove its mark. Continue to review the remaining marked questions until you run out of time or you complete the test.

After you complete the exam, your test will be scored immediately. A few moments after you finish, the computer will indicate whether you passed or failed.

You Passed!

Passing the CCIE Security exam means that you are ready to take the lab exam. Within 48 to 72 hours, Cisco will be notified of your result. There is no need to fax your result, as was previously required. To set a lab exam date, visit the following Cisco.com page and select the location and exam date you prefer:

http://www.cisco.com/en/US/learning/le3/ccie/security/scheduling_lab_exam.html

The lab exam is popular, and you might need to wait a month or more for an opening. Some locations have a waiting list of 6 months or more. For example, the Sydney, Australia CCIE lab is generally not fully booked, and you might get a seat at a time of your choice; in Brussels, Belgium, you might need to wait 6 months. Make sure you agree to a testing date that you feel comfortable with, and leave yourself plenty of time to study for the rigorous lab exam. After passing the written test, you have 18 months to pass the lab exam, so, if necessary, you can study for a few months

before taking it. After each lab attempt, you have an additional 12 months to pass the lab, you can have up to 3 years to pass the lab if you happen to fail the lab exam more than once. See http://www.cisco.com/en/US/learning/le3/ccie/policies/index.html for more details.

You Failed

If you fail the CCIE Security written exam, don't worry about the result. You can still take advantage of the situation. While the test is fresh in your mind, jot down problem areas on a notepad (the sooner you make notes for yourself the better). Try to remember questions you felt less comfortable with and study those areas before taking the exam again.

The CCIE Security written exam is not an easy exam to pass. In fact, this exam ranks among the toughest networking exams in today's certification market. If you really want to be a CCIE, a first-attempt failure should not discourage you. A failed attempt should encourage you to invest in some serious study time so that you can pass on your next attempt. A number of candidates have noted that the second attempt is much easier than the first. Remember that the reason Cisco Systems makes the written exam hard is to ensure that you are fully prepared for the challenging lab exam.

That's it for pointers. Next are some frequently asked questions about the written exam, followed by some bonus information on the lab exam.

FAQs About the CCIE Security Written Exam

This section answers some common questions about the written CCIE Security exam. These frequently asked questions should help dispel any confusion surrounding this exam.

1. How many questions are on the CCIE Security written exam?

   There are 100 questions. All questions are multiple choice. Some questions require a single answer, whereas other questions require more than one answer to earn a point.

2. What is a passing score?

   Cisco no longer publishes a set passing score for the written exam. Instead, Cisco supplies you with a pass or fail grade. The actual passing score (a percentage) is based on a statistical-analysis system that checks the scores of all candidates over 3 months and adjusts the score needed to pass accordingly. For example, the passing score for one candidate might be 70 percent, but it might be 75 percent for another candidate, depending on what results candidates are attaining in the same 3-month period.

3. Can I change an answer after working through all the questions?

   Yes, as long as time remains, you can return to any question.

4. How long is the exam?

   The exam is 2 hours long. Make sure you use your time wisely—you want to have an opportunity to answer as many questions as possible. If you find that you are spending too long on a single question, mark it and move on. If time permits, you can return to difficult questions later.

5. What happens when I finish the exam?

   The computer scores your test within minutes and indicates whether you passed or failed. You receive a printed score sheet with a grade for the entire exam and a percentage score for each of the topics. If you fail, you must wait at least 72 hours before retaking the exam.

6. Can I use Windows Calculator during the exam?

   No. You are not permitted to use any Windows tools. You are supplied with a pencil and some white paper or an erasable sheet.

7. How many times can I retake the written exam?

   You can retake the written exam as many times as you like. Each written exam attempt will cost you U.S.$300.

8. What do I do after I pass the written exam?

   You do not need to fax your test results to your nearest CCIE lab administrator. Visit the following URL to set a lab exam:

   http://www.cisco.com/en/US/learning/le3/ccie/security/scheduling_lab_exam.html

9. Where can I find further information about the CCIE Security exam?

   Cisco provides additional information online:

   http://www.cisco.com/en/US/learning/le3/ccie/security/index.html

CCIE Security Lab Exam

NOTE Although the focus of this book is to prepare you for the CCIE Security written exam only, you can find bonus material, such as this section, that helps start your preparation for the lab exam.

Passing the written exam is the easier part of the CCIE Security certification journey. For the lab exam, your life needs to change dramatically, and you need to study on routers full time for at least 3 to 6 months. The good news is that the format of the lab exam has changed from 2 full days to 1 day. You are no longer required to troubleshoot a network (regarded as the true method to test a

CCIE's ability to restore a network back to full IP connectivity); you are now required to configure more advanced features in a set number of Cisco IOS, PIX, and Catalyst devices. For example, basic Frame Relay, VLAN, VTP, and ATM configurations are now preconfigured for the candidate. This allows the examiners to test more advanced security features rather than basic routing and switching configurations. This also differentiates from the content of the routing and switching lab.

For details on what is configured or preconfigured, visit http://www.cisco.com/en/US/learning/le3/ccie/security/lab_exam_blueprint.html.

Upon entering the lab room, you will already have preconfigured router and switch host names and IP addressing, and the enable password and login commands will be set on all devices to **cisco**.

After you pass the written exam, you are eligible to sit for the lab exam. You can book your lab exam online as mentioned previously.

The lab exam contains the following devices:

- 2600 series routers
- 3600 series routers
- 3700 series routers
- Catalyst 3550 series switches running Cisco IOS Software Version 12.1EA
- Cisco PIX Firewall
- Certificate Authority Support
- Cisco Secure Access Control System
- Cisco Secure Intrusion Detection System
- VPN concentrators
- IDS sensors

Software versions are constantly updated. Be sure to verify revision levels at the following URL:

http://www.cisco.com/en/US/learning/le3/ccie/security/preparing_lab_exam.html

You should expect the CCIE lab exams to mirror the general deployment releases by Cisco.

Make sure you practice with and understand these devices. Practice configuring almost every Cisco IOS feature and fully understand what each Cisco IOS command actually enables, rather than just relying on limited experience with certain commands. Anyone can configure a Cisco router, but the ability to understand the full consequence of any Cisco IOS command is crucial to the CCIE Security lab exam.

CCIE Security Lab Exam FAQs

The following are some frequently asked questions about the difficult 1-day CCIE Security lab exam.

1. When did the lab format change from 2 days to 1 day?

   October 2001. All CCIE certification labs worldwide now test candidates in the 1-day format.

2. Where can I take the CCIE Security lab exam?

   Locations where you can take the CCIE Security lab exam follow:

   - Beijing, PRC
   - Brussels, Belgium
   - Research Triangle Park (RTP), North Carolina, USA
   - San Jose, California, USA
   - Sydney, Australia

   You can find more information at http://www.cisco.com/en/US/learning/le3/ccie/security/scheduling_lab_exam.html.

3. What is the maximum score and what is a passing score?

   The total exam is worth 100 points and the passing grade is 80 percent. The passing rate for first attempts is very low, so expect the possibility of taking the exam more than once. Cisco will not release the passing rate.

4. What if I have a question and cannot find the answer?

   E-mail your question to ccie@cisco.com. All questions receive a response from the CCIE team within 72 hours.

5. What happens after the exam?

   You will be escorted outside the lab. You receive an e-mail notification within 24 hours. The e-mail advises you to log on to Cisco.com and enter your written exam results (written exam date, score, and your candidate ID will be required), and you will be presented with a breakdown of the main sections and your percentage score in each section. You can fill in a critique regarding your lab experience; be sure to provide all the feedback you have—good

or bad. Candidates can receive free lab attempts for valid excuses or lab inconsistency and human errors. For the price of U.S.$1250 plus taxes, you want to make sure you have been given every opportunity to pass.

6. Can I use Notepad and Windows Calculator?

   Yes, you can, but you are not permitted to save any files. You can, however, cut and paste to and from Notepad. Calculator is very useful for determining subnets and bit boundaries or converting hexadecimal to decimal.

7. How many times can I take the lab exam?

   You must allow 30 days between lab exam attempts. There are no minimum score requirements.

8. What happens if I pass?

   In addition to becoming a CCIE, you also gain access to exclusive CCIE chat forums and merchandise, and you receive a CCIE plaque and certificate. Expect these to be mailed to you between 3 and 6 months after your test date, depending in what part of the world you reside.

9. What happens if I fail? Am I told in which areas I scored poorly?

   Cisco will not tell you specific areas of weakness; that is left to the candidate to decipher from the brief score report. You can, however, pay a fee (U.S.$250) to have your lab routers re-examined for accuracy. If you strongly feel you have passed, then the investment of $250 is well worth the expense. Even with a regrade, no additional information is provided to you—only a brief score report by e-mail and your new grade (pass or fail). Some candidates have e-mailed me to say they have successfully passed after being told they had not. A regrade is really a personal decision. If you feel you scored 75 or more, then I would recommend a regrade.

10. What materials can I bring into the lab?

    You are permitted to bring only necessary medication and a dictionary. No other materials are permitted. Cisco provides refreshments at all CCIE lab sites. Lunch is also provided during a lunch break (30 minutes). The lunch break is mandatory and CCIE staff escort you.

11. What is the proctor's role?

    You can seek clarification from a proctor if you do not understand a question or the objective of a question. The proctor cannot provide answers but can ensure that you understand the question. The proctor can also make any changes required in case of network hardware failures or exam mistakes. The proctor is there to ensure that you have the best possible chance of success and should not hinder your ability to pass the test. If you feel otherwise, you can e-mail your concerns to ccie-lab@cisco.com. The CCIE program manager's core responsibility is the welfare of the candidates, and you never know, your case might warrant a free future lab.

12. Where can I find out more about CCIE and the different certification tracks?

The following URL provides information about the CCIE tracks:

http://www.cisco.com/en/US/learning/le3/ccie/index.html

13. How often do I need to recertify?

You must recertify every 2 years to maintain your CCIE status; otherwise, your CCIE status will be changed from active to suspended and finally to inactive. An inactive CCIE means you cannot purchase CCIE merchandise or participate in the CCIE forum.

If your CCIE certification is suspended, you lose all CCIE benefits and CCIE privileges with Cisco.com until you recertify. After 1 year of suspended status, your certification becomes inactive and you will be required to retake both the written and lab exams in order to restore your active CCIE status.

14. What examinations or alternative methods can I take to recertify my CCIE?

Currently, you can use a couple different methods to recertify your CCIE:

- You can take any of a number of different written exams; for details on available written exams, visit http://www.cisco.com/en/US/learning/le3/ccie/recert/index.html
- You can achieve a CCIE recertification from a CCIE track you do not currently possess. For example, passing your Security lab exam will recertify the R&S track if you possess one.


Catalyst 6500

APPENDIX C

Sample CCIE Routing and Switching Lab I

NOTE Although the aim of this book is to help prepare you for the CCIE Security written exam, I include this appendix as bonus material for a few reasons. First, even though this is a sample lab for the CCIE Routing and Switching lab exam, it gives you an idea of the level of tasks involved in a CCIE lab examination. Second, being a triple CCIE myself, I recognize that if you are interested in attaining CCIE Security certification, you might be curious about the other CCIE options, as well.

This appendix is designed to assist you in your final preparation for the lab portion of the most popular CCIE certification to date, CCIE Routing and Switching (CCIE R&S).

There are two versions of the R&S lab in this guide. This appendix includes a complex routing lab designed for readers who have access to a generous amount of equipment. Appendix D, "Sample CCIE Routing and Switching Lab II," is a sample lab with the same level of difficulty but with only four routers. This gives you access to two sample R&S labs with various equipment requirements, and both provide an excellent guide to the level of difficulty you can expect in any CCIE laboratory exam.

Many books are published today on how CCIE R&S certification can be achieved, but, in reality, no matter how many books you purchase, it all comes down to your level of hands-on experience. The strict Non-Disclosure Agreement (NDA) policed by Cisco ensures that candidates do not share any information about the lab exam content, so very little is known before your first attempt.

For the first time ever, the CCIE team has approved this sample CCIE Multiprotocol lab so that you can be aware of the level of difficulty involved in the lab exam and prepare accordingly. *Solutions are not provided, at the request of the Cisco Systems CCIE department*. You are left to research the various solutions on your own. You may e-mail me at henry.benjamin@optusnet.com.au with any thoughts or queries you have, and together we can work through any problems you encounter. In researching the solutions, you learn more about each topic and commit the information to memory better. In the end, this ensures that you are as prepared as you can be for the lab if you decide to take it.

The end goal of any CCIE lab is a working solution. However, you might be restricted in the way in which you provide a working solution, as you discover in this sample CCIE R&S lab.

Candidates who prepare for the lab often ask me what is the best way to prepare. My answer to them is to practice configuring every feature available, and then practice some more. Of course, not every feature will be tested on the lab exam. You are encouraged to read the most up-to-date information about Cisco exams and certifications at

http://www.cisco.com/en/US/learning/le3/ccie/index.html

You must be able to provide a working solution quickly and adhere to the guidelines stated in the question. A good analogy is a driving test; imagine you're asked to drive down a 100-mile road that is perfectly straight, but instead of going down the road the way you think is best, a sign every 100 feet indicates an action you must take. The exam designer does not always ask for the best solution or your favorite solution, but might ask you to solve the problem in a very specific way. For this reason, you must have a broad knowledge of all Cisco IOS features. The lab exam is designed to discover if you are capable of configuring more challenging and difficult scenarios.

The CCIE lab changed format on October 1, 2001. The lab changed from a 2-day lab to a 1-day lab, which means that a candidate is no longer required to sit for a separate troubleshooting section but must configure a network in 8 hours. One of the most critical skills in the new format is time management. Troubleshooting is still regarded as a fundamental skill in today's most critical IP networks.

The R&S lab contains the following hardware and Cisco IOS revisions:

- 2600 series routers
- 3600 series routers
- 3700 series routers
- Catalyst 3550 series switches running Cisco IOS Software Version 12.1EA
- Cisco IOS Software Version 12.2 for all routers
- Cisco IOS Software Version 12.2T became eligible for testing on August 1, 2004
- IPv6 features in 12.2T become eligible for testing on January 1, 2005. Expect to be tested only lightly, though, on new advanced topics.
- To ensure the maximum possiblity of success, endeavor to install 12.2T on all of your lab routers and read the release notes on 12.2T, which can be found at the following URL:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/
  prod_release_notes_list.html

- As the candidate, you should be aware of the new features in the Cisco IOS software, because you may be asked to configure some of these new features in the lab.

NOTE Token Ring switching and legacy routing protocols, such as IPX and IGRP, are no longer tested in the CCIE R&S lab exam. DLSw+ over Ethernet remains a core test topic.

For more details on the CCIE R&S lab content blueprint, visit:

http://www.cisco.com/en/US/learning/le3/ccie/rs/lab_exam_blueprint.html

Each task in this sample CCIE R&S lab examination includes a recommendation for the amount of time that you should allocate to complete the task. This lab is designed to be completed within 8 hours. A designation of "No Time" in the section heading means that in the real CCIE lab, that particular section has already been completed for you. For example, this sample lab asks you to physically cable the network; no time allocation is provided because in the real CCIE lab, the physical cabling is already completed for you.

This sample lab's goal is a working IP network according to the set design criteria.

Figure C-1 displays the sample topology with nine Cisco IOS routers and the logical topology.

Figure C-1 *CCIE Lab Topology*

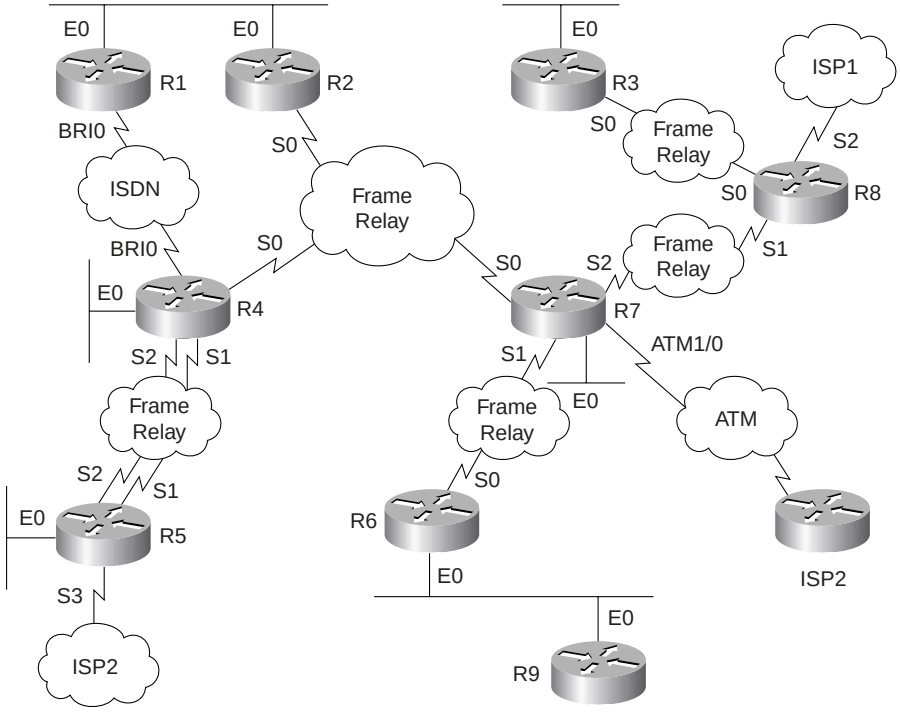
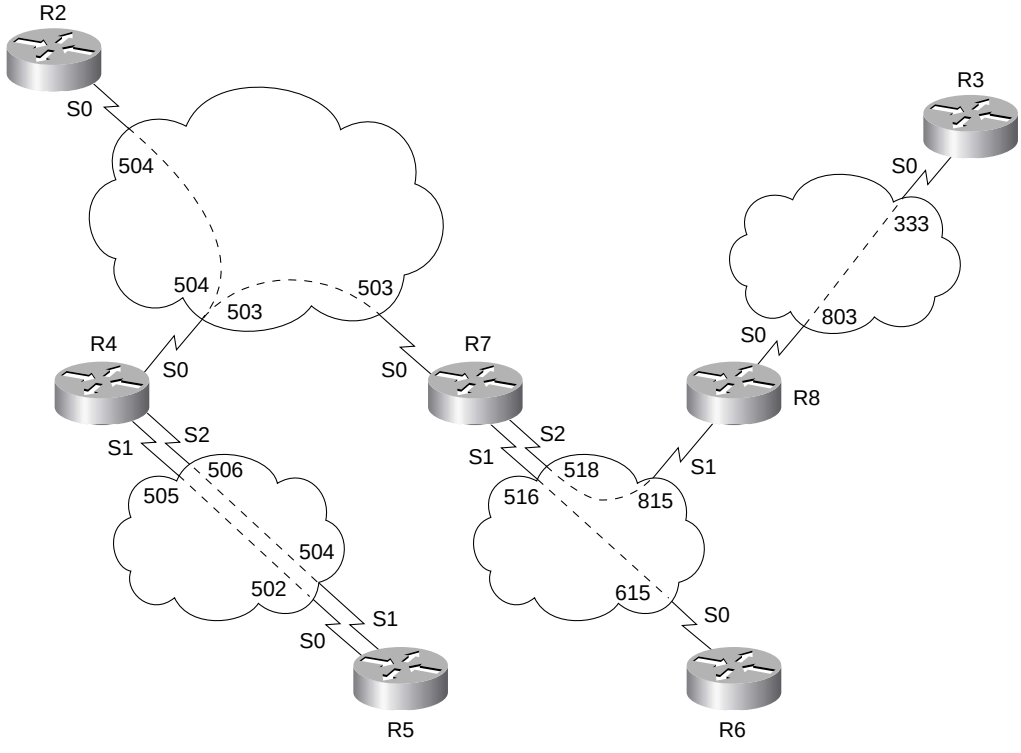


Figure C-2 displays the Frame Relay connections between the Cisco routers.

Figure C-2 *Frame Relay DLCI Assignment*



Basic Setup (1 Hour)

Configure the network in Figure C-1 for basic physical connectivity.

Communications Server (0.25 Hour)

NOTE Not all CCIE R&S labs require you to configure a communication server.

Configure the communication server so that when you type the host name of a router on the server, you are connected across the console port to that router. Set up the routers in Figure C-1 with the following physical attributes:

- Set up the routers, as shown in Figure C-1.
- Configure R1 as the communication server with the **ip host** command.

- Communication server ports 2 to 8 are connected to Routers R2 to R8, respectively.
- Communication server port 9 connects to the Catalyst Ethernet switch.
- R9 is a Catalyst 6509 switch with a Multilayer Switch Feature Card (MSFC) module installed.

Physical Connectivity (No Time)

NOTE From October 1, 2001 onward, a CCIE candidate is not required to physically cable up the lab network. Therefore, no time allocation is given to this section, which is added for completeness only.

The Security lab examination also has some elementary tasks, such as Frame Relay and basic IP routing, preconfigured to allow the candidate more time to configure more advanced features in Cisco IOS software. This is a great time saver for the candidate.

Your network is already physically patched. Construct your network, as shown in Figure C-1.

Configure the following characteristics for the topology in Figure C-1:

- A Frame Relay switch connects all serial links between routers. Use only the indicated DLCIs in Figure C-2 and disable Frame Relay inverse ARP for IP only.
- Routers R1 and R4 are connected to an ISDN service with the switch type defined as basic-5ess. R1 connects to number plan 0298017705 and R4 connects to number plan 0296307050.
- Routers R1 through R9 are connected to the Catalyst Ethernet switch (Catalyst 6509 series switch), according to Table C-1.

Table C-1 *Ethernet Interface Connections to the 6509*

Router	Catalyst Port
R1 Ethernet 0	3/1
R2 Ethernet 0	3/2
R3 Ethernet 0	3/3
R4 Ethernet 0	3/4
R5 Ethernet 0	3/5
R6 Ethernet 0	3/6
R7 Ethernet 0	3/7
R8 Ethernet 0	3/8
R9 Ethernet 0 (6509)	VLAN 6

Catalyst Ethernet Switch Setup I (0.25 Hour)

Configure the Ethernet switch for six VLANs.

- VLAN 2, named VLAN_A, is connected to R1 and R2.
- VLAN 3, named VLAN_B, is connected to R3.
- VLAN 4, named VLAN_C, is connected to R4.
- VLAN 5, named VLAN_D, is connected to R5.
- VLAN 6, named VLAN_E, is connected to R6 and R9.
- VLAN 7, named VLAN_F, is connected to R7.

Using VLAN_A, configure the management interface sc0 with the address 131.108.0.2/25. Ensure that all devices in your network can Telnet to the switch even if R1 or R2 is down.

Make sure the switch is configured in the VTP domain Cisc0_vTp and the switch can create and delete VLANs in the future.

For the connections to Routers R5 and R8, ensure that you have MAC-layer authentication enabled, 802.1x.

Catalyst Ethernet Switch Setup II (0.25 Hour)

Configure the following spanning-tree parameters on the Catalyst 6509:

- Ensure that the switch never becomes the root bridge on VLAN_D.
- Ensure that the switch has the best possible chance of becoming the root bridge in VLAN_E.
- Set all the Ethernet ports to forward data immediately after a device is plugged in or activated.
- Set the hello time on VLAN_B to 10 seconds.
- Set the max age on VLAN_F to 10 seconds.

Configure the following miscellaneous parameters:

- Disable Cisco Discovery Protocol on ports 3/1-8.
- Ensure that any IP phones installed or connected to Card 3 are supplied inline power.
- Ensure that the switches get a clock source from R1 using NTP.
- Make sure the only MAC address permitted to access the switch on port 3/23 is the MAC address 2010-2010-2010 or 4000-0000-4000.

- Disable power redundancy on the switch.
- Warn all Telnet clients that any "unauthorized access is not permitted" by displaying a warning message when any Telnet session is activated to the SC0 interface only.
- If any ports become disabled because of hardware errors, ensure that the switch automatically enables the affected ports after 10 minutes.

Catalyst Ethernet MSFC Setup (0.25 Hour)

NOTE The CCIE R&S lab contains two Catalyst 3550s per candidate rack, and the 6500 is purposefully configured here so that the difficulty level is much higher.

Configure R9 (6509 with an MSFC card) for IP routing.

Example C-1 displays the hardware profile on the Catalyst 6509 switch.

Example C-1 **show module** *on R9 (MSFC)*

```
Cat6509> (enable) show module
Mod Slot Ports Module-Type               Model               Sub Status
--- ---- ----- ------------------------- ------------------- --- --------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP1A-2GE    yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC         no  ok
3   3    48    10/100BaseTX Ethernet     WS-X6348-RJ-45      yes ok

9   9    8     1000BaseX Ethernet        WS-X6408-GBIC       no  ok
Mod Module-Name         Serial-Num
--- ------------------- -----------
1                       SAD0413022N
15                      SAD041501U6
2                       SAD041501U6
3                       SAD04270A8A
9                       SAD03479837
Mod MAC-Address(es)                         Hw     Fw          Sw
1   00-30-96-33-21-7e to 00-30-96-33-21-7f 3.1    5.3(1)      5.5(4)
    00-30-96-33-21-7c to 00-30-96-33-21-7d
    00-d0-01-b0-4c-00 to 00-d0-01-b0-4f-ff
15  00-30-96-33-24-84 to 00-30-96-33-24-c3 1.4    12.1(1)E,   12.1(1)E,
3   00-30-96-34-9b-48 to 00-30-96-34-9b-77 1.1    5.3(1)      5.5(4)
9   00-30-96-2b-e1-f4 to 00-30-96-2b-e1-fb 2.3    4.2(0.24)V 5.5(4)
Mod Sub-Type                Sub-Model           Sub-Serial  Sub-Hw
1   L3 Switching Engine     WS-F6K-PFC          SAD04150DYL 1.1
3   Inline Power Module     WS-F6K-VPWR                     1
```

Using the information displayed in Example C-1, configure the MSFC for IP routing in VLAN 6 only using RIPv2 only.

Do not route between any other interfaces.

IP Configuration and IP Addressing (No Time)

NOTE Because of recent changes to the CCIE exam, the candidate is not required to configure IP addressing. However, the subject is presented here to ensure that potential CCIE candidates have a good understanding of IP address spaces and subnetting. No time is projected for this section.

Use the Class B subnetted IP addresses 131.108.0.0 to 131.108.255.255 to design your network. You must use this address space for all addresses unless specified in a particular question. Read the entire task before designing your IP address space.

After your IP address space and IP routing is completed, it must be possible to reach all of your routers and switches. Set the enable password for all routers and switches to **cisco**.

Configure IP addresses on your remaining interfaces.

- Use a 25-bit mask for VLAN 2.
- Use a 27-bit mask for VLAN 3.
- Use a 28-bit mask for VLAN_D.
- Use a 24-bit mask for VLAN_E.
- Use a 24-bit mask for all other interfaces.
- Use a subnet with the least number of hosts for the ISDN link.
- Use a 29-bit mask for all Frame Relay connections running classless IP routing protocols.
- Use a 24-bit mask for all Frame Relay connections running classful IP routing protocols.
- Assign each router a 24-bit subnet to be used by the loopback address. It must be possible to ping and Telnet from any one router using the loopback address. This means that all loopback addresses must be routable to every device within your network.
- Configure local IP host addresses on each router so that an exec or privilege user can type the router name to ping or Telnet without having to type the full IP address.

Frame Relay Setup (0.5 Hour)

Configure IP across your Frame Relay network, as displayed in Figure C-2.

- You have to use static maps for each protocol. No dynamic mapping is permitted.
- *No* subinterfaces are allowed on any router.
- Use the most efficient subnetwork for IP addresses on the Frame Relay cloud.
- You can assign a subnet from your Class B range.
- Use LMI-type **Cisco only** and do not rely on auto-sensing the LMI type on any routers. All router interface types are DTE. The Frame Relay port type is DCE.
- Do not use the keyword **broadcast** for the Frame Relay link between R6 and R7 when mapping IP.
- Make sure you can also ping the local interface from each router configured for Frame Relay.

Basic ATM Configuration (0.5 Hour)

Configure ATM on R7 to connect to the ATM cloud.

- Your IP address for the ATM cloud is 197.1.1.1/24.
- One PVC is configured between your Router R9 and the remote ATM router. Your end of the PVC is VPI = 0 and VCI = 100.
- Configure RFC 1577 on R9.
- You must be able to ping the remote ATM router address of 192.1.7.2/24.

IGP Routing (3 Hours)

After this section is completed, all routers must have full IP connectivity between every routing domain, including the ISDN backup interfaces when operational.

RIPv2 Configuration (0.5 Hour)

Configure RIP version 2 (RIPv2) on Routers R6 and R9 only.

- Configure RIPv2 on R6 E0 and R9 E0.
- Make sure only unicast updates are sent and received.
- Authenticate any RIPv2 packets.

- Redistribute the RIPv2 route into the IGRP domain.
- Make sure you can see distributed RIPv2 routes throughout your topology.

IS-IS Configuration (0.5 Hour)

Configure IS-IS on Routers R6 and R7 only.

- The MAC address of the respective routers are the following:
  - R6 0050.5460.98e8 net ID is 00.0001.0050.5460.98e8.00
  - R7 00b0.64fc.d7bd net ID is 00.0001.00b0.64fc.d7bd.00
- Configure all routers in IS-IS area 1.
- Configure R6 as an IS-IS level 2 router only.
- Redistribute the IS-IS routes into the OSPF domain.
- Make sure you can see distributed IS-IS routes throughout your topology as type 1 OSPF routes.

EIGRP Configuration (0.5 Hour)

Configure EIGRP on Routers R3, R7, and R8 only.

- Configure EIGRP in domain 333 between the serial link on R7 to R8, R3 to R8, and VLAN 3.
- Summarize as much as possible to reduce the redistributed routes into OSPF, but make sure all routes appear in the IS-IS and RIP domains.
- Ensure that EIGRP is authenticated across the Frame Relay connections.
- Redistribute the EIGRP routes into the OSPF domain with a cost metric of 1000 seen on all OSPF routers.
- Ensure that R3 never sends any updates across the Ethernet (E0) segment.

OSPF Configuration (1.5 Hours)

Configure OSPF as follows; do not create any nonspecified OSPF areas:

- Configure the OSPF backbone over the Frame Relay network between Routers R2, R4, and R7.
- The ISDN link between R1 and R4 resides in the area 0.0.0.0.
- The link between R4 and R5 is in area 4.

- The Ethernet segment between R1 and R2 resides in area 1.
- The Ethernet segment on R4 resides in area 0.0.0.40.
- Make sure all OSPF routes are redistributed and reachable in the IS-IS, RIP, and EIGRP domains.
- Ensure that the OSPF backbone in the Frame Relay cloud is authenticated.
- Ensure that R1 is never the designated router (DR) on all segments.
- Make sure R4 is the DR in the OSPF backbone network.
- Ensure that the router ID of all OSPF-enabled routers is the loopback address.
- Do not create any additional areas.
- Set the hello interval between links R1 and R4 to 25 seconds.
- Set the hello interval on the R2 Ethernet segment to 20 seconds.
- Ensure that all loopbacks appear as /24-bit networks on all IP routing tables. Do not use the **redistribute connected** command on any router to accomplish this.
- Make sure area 0.0.0.40 is configured so that excessive CPU resources are not consumed on Router R4. You can assume that no other areas or routers are attached to this segment.

Basic ISDN Configuration (0.5 Hour)

ISDN switch information:

- ISDN switch type: basic-5ess.
- ISDN numbering:
  - R1: 0298017705
  - R4: 0296307050
- SPIDs are not required.

Configure the ISDN interfaces on R1 and R4 as follows:

- When R1's S0 goes down, R1 should place an outgoing call to R4.
- R4 cannot call R1 under any circumstance.
- Use PPP encapsulation for one B channel, HDLC on the second, and the strongest authentication available where applicable.

- Never bring up more than one B channel, to ensure that costs are kept to a minimum; you can use the interface configured with PPP for this purpose.
- When the Frame Relay link is restored, bring down the ISDN link after 25 minutes.
- When the ISDN link is active, all routers must be able to ping and Telnet the local ISDN interfaces on R1 and R4.

DLSw+ Configuration (0.5 Hour)

Configure DLSw+ on R1, R2, R5, and R6.

- VLANs 2, 5, and 6 should have DLSw configured to allow SNA devices to communicate between each other.
- Do not enable DLSw on R9, but allow any future segments connected to R9 reachability to VLAN 2 only.
- SNA/NetBIOS hosts reside on VLANs 2 and 5.
- Hosts on VLAN 2 are used only when VLAN 5 is not reachable.
- Make sure all routers peer to R1 and that only in a network failure will DLSw+ circuits terminate on R2 or R5.
- DLSw+ peers should be active only when user-based traffic (SNA/NetBIOS) is sent or received.
- If IP connectivity exists, ensure that DLSw+ remains established.
- Use a different virtual ring group on each router.
- Configure a filter that blocks NetBIOS packets with destination name SimonisaCCIE from leaving R5. Permit all other NetBIOS traffic starting with the name Simonis?***.
- Ensure that remote DLSw+ peers do not send too many queries for the destination MAC address 0200.0200.0200 on VLAN 6 or VLAN 2.
- Be sure the only SAPs enabled on R3 are null SAPs and SAP 08.

Flash Configuration (0.2 Hour)

The customer accidentally erased Router R1's system image in Flash memory. The customer has no Cisco IOS Software or TFTP server on hand. There is no Internet access. Restore the Cisco IOS image to the Flash on R1 and then reload R1.

R1 and R2 are running the same Cisco IOS code and are the same router hardware type (Cisco 2811 routers).

VTY Changes (0.2 Hour)

Configure all vty lines so that network administrators require no local authentication.

Administrators must still use the enable password ccieToBe on all routers to access privileged EXEC mode.

To allow nonprivileged users access to R1 and the ability to clear terminal server lines, ensure that all exec users can use the Cisco IOS command **clear** in privileged EXEC mode on Router R1 only.

HTTP Server (0.2 Hour)

Configure R1 to act as an HTTP server, but allow only clients from users on VLAN_A or VLAN_B.

Catalyst 6509 Password Recovery (0.2 Hour)

The enable password on the 6509 switch has been modified. Assuming you have access to the switch using password recovery on the switch, set the enable password to **ccie** and the access password to **cisco**.

Private Address Space Allocation (0.2 Hour)

Some users on VLAN_A have configured their PCs with the Class A addresses ranging from 10.10.1.1 to 10.10.1.255/24. Make sure the Class A address is never present in any routing table but R1, and allow the users to access the rest of the network.

Ensure that the remaining network can access the host with the IP address 10.10.1.100/24.

BGP Routing Configuration (1.0 Hour)

After finishing each of the following sections, make sure all configured interfaces/subnets are consistently visible on all pertinent routers, even in the event of network failure of any one router.

Basic IBGP Configuration (0.2 Hour)

Configure IBGP on all routers in your network.

- Do not use any WAN IP interfaces for IBGP sessions, because your network is prone to failures across the Frame Relay cloud.
- Configure R5 and R8 as route reflectors and ensure that all IP traffic has a preferred path that is via Router R5.

- Minimize IBGP configurations as much as possible.
- Do not disable BGP synchronization.
- Use AS 2002 on all IBGP routers.
- As long as your network has IP connectivity, ensure that BGP is active in all routers.
- Using the **network** command only, advertise all networks to route reflectors R5 and R3.
- Do not change the administrative distance on any interior routing protocol.
- Make sure you have full BGP connectivity.
- Be sure all routers have entries in their IP routing tables.

EBGP Configuration (0.2 Hour)

Configure EBGP on R5 and R8 as follows:

- R5's remote peer is 171.108.1.2/24 and remote AS is 1024.
- R8's remote peer is 191.200.1.2/30 and remote AS is 4345.
- ISP1 and ISP2 are advertising the full Internet routing table.
- The only route accepted is a default route and routes of the form 110.100.0.0 to 121.110.255.255.
- Set all routes in the range 110.100.0.0 to 121.110.255.255 with the following attributes:
  - BGP origin is set to IGP.
  - Prepend the AS paths 1000, 999, and 100.
  - Set the weight to 1000 for all even networks and 2000 for all odd networks.

QoS Configuration (0.25 Hour)

The Catalyst 6500 series switch needs to be configured for a large VoIP network. Ensure that module 3, which has inline power, has QoS configured to trust Cisco IP phones only and be sure to set any CoS and DSCP setting to 0 for any device attached to the IP phone. Ensure that voice traffic 802.1p settings are adhered to in your network.

Voice over IP (0.25 Hour)

Router R9 has been installed with two FX0 interfaces (traditional analogue handsets have also been attached) and requires the ports 2/0/0 and 2/0/1 configured with the extensions 1000 and 1001.

There is a dial IP peer with the IP address 100.1.1.1. Ensure that if extension 1000 calls the number 9801-7705, the number is translated to 6000. You can assume that all other phones are reachable via the dial peer 100.1.1.1.

Configure the second extension (1001) to automatically call the extension 1000 when the handset is picked up.

NOTE From January 1, 2005, VoIP will no longer be part of the R&S blueprint, effectively replaced by IPv6 instead.

IP Access List (0.1 Hour)

You decided to secure Routers R1 and R2 such that only hosts from your address space are allowed to Telnet to it.

In addition to securing these routers, you also need to make sure that the only source IP addresses that can be trusted are the predefined loopbacks on Routers R1 through R9. You *must* identify the denied attempts to Telnet to R1 or R2 to the local buffer log.

The security architect has decided to make the allowed hosts, when Telnetting to R1 or R2, be authenticated by the router locally. The username will be Admin and the password will be 8eaChe.

Additionally, you must ensure that RFC 1918 is adhered to on the serial links to ISP1 and ISP2. Configure the most appropriate access list to ensure that RFC 1918 is adhered to.

Ensure that your access list contains comments so that other engineers can see why you have installed specific configuration lines.

NOTE At the request of the CCIE department, solutions to this sample lab are not provided in this book. Consider this lab a source for understanding the type of testing you can expect on a CCIE lab exam. The material in this appendix is in no way intended to represent the exact material you will see on the actual lab examination.

Conclusion

You should be able to complete the sample CCIE Routing and Switching lab in this appendix within 8 hours. The difficulty level presented here is similar to what you can expect in any CCIE lab examination; in fact, the difficulty level here might be higher. Focus your attention on time management and the ability to configure a set number of Cisco IOS features very quickly. If you complete this lab successfully, try it again by modifying the questions and changing the IP routing algorithm. For example, configure multipoint Frame Relay connections or subinterfaces across the Frame Relay network in Figure C-2; try PPP over an ISDN connection.

Be familiar with Cisco IOS 12.2T. Also, be up to date with the latest features tested in the examination. Most candidates are intimidated by the recent CCIE content changes. You must have an overall conceptual view of all Cisco IOS features, because Cisco cannot possibly test all the more advanced features of all the content. Nor are there complex hardware models present in the lab. New content typically tests only the overall concepts. You must be able to competently search the Cisco Documentation CD, find any feature you need to configure, and quickly appreciate the use of any Cisco IOS command. Typically, a portion of any CCIE exam will be unknown to you, so you must be able to search the CD documentation provided in every lab quickly.

The ability to complete any design scenario efficiently, correctly, and per the given parameters ensures that you are a master of CCIE.


Catalyst 6500

APPENDIX D

Sample CCIE Routing and Switching Lab II

This appendix is designed to assist you in your final preparation for the lab portion of the most popular CCIE certification to date, CCIE Routing and Switching (CCIE R&S).

This second bonus version of the R&S lab examination contains only four routers, for those readers who do not have access to a large number of routers. This sample lab has been added after receiving many e-mails from readers who bought the previous edition of this book. I hope that it proves to be a useful alternative to helping you gauge your readiness for the lab exam. Feel free to send me your feedback so that I can continue to improve the quality of sample lab exams for the future.

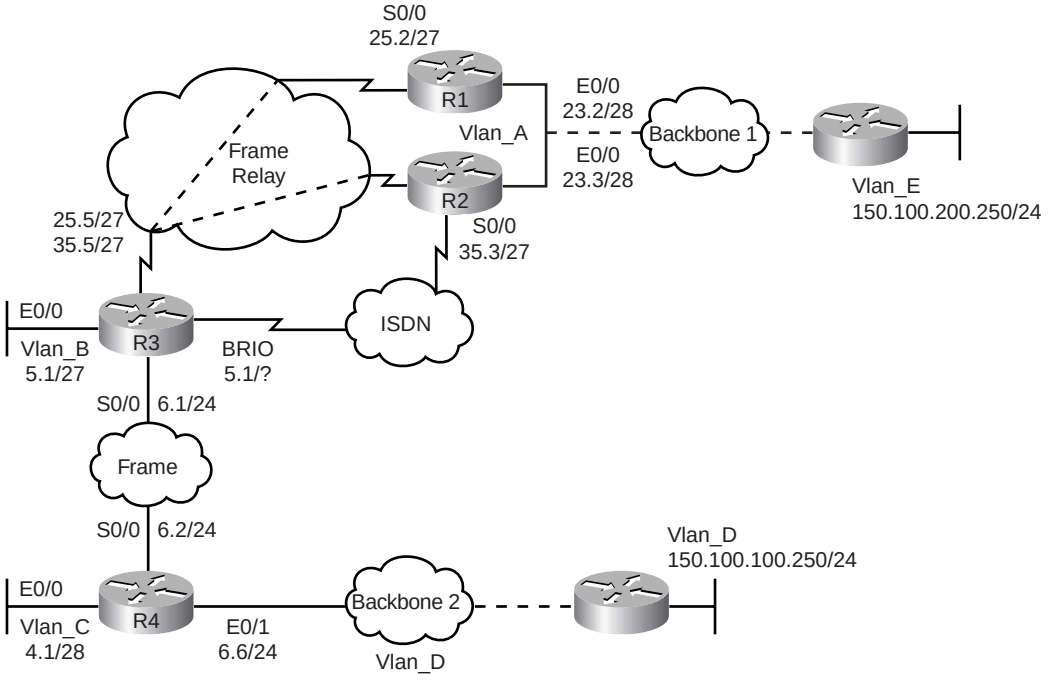
The following are some general guidelines typical of any CCIE lab examination:

- Static and default routes are not permitted unless directly stated in a question. This includes floating static routes (static routes with a defined administrative distance) and static routes to Null0
- Routes generated by any routing protocol are permitted; if you are unsure, ask the instructor.
- All router host names; basic IP addressing; and passwords on the console, auxiliary, and virtual terminal lines have been preconfigured.
- The Catalyst 3550 switch has preconfigured prompt and enable passwords. All preconfigured passwords are cisco and should not be changed unless explicitly stated in a question.
- Do not change any predefined passwords.
- There is no partial grading in this examination unless stated in the question.
- If you are unsure about a question, ask the instructor. The instructor may or may not answer your question.
- Each router is assigned a loopback address of the form 133.33.YY.YY/24, where YY is the router number. For example, for R1 the loopback address is 133.33.1.1/24, for R2 the loopback is 133.33.2.2/24, and so forth.

- If any given router requires secondary addressing, you are permitted to configure this address. However, the question may or may not specifically identify this feature.

Figure D-1 displays the sample four-router CCIE lab topology with Routers R1 through R4. The core of the network is connected to Frame Relay, with ISDN providing a backup mechanism between R2 and R3. You are required to configure the routers in Figure D-1 along with a Catalyst 3550 switch (not shown).

Figure D-1 *CCIE Lab Topology*



A major difference between this lab and the one in Appendix C is that a point-scoring system is in place rather than time allocation. There are 100 points available for these exercises. For questions with a 0 point value, the feature is assumed knowledge and is typically preconfigured and not required in the real exam. However, I have purposely included these here to ensure that you are 100 percent ready for anything and ensure that you have the basic competencies required for any future CCIE.

This lab ensures that you have the best of both worlds by combining an approved CCIE lab (Appendix C, "Sample CCIE Routing and Switching Lab I") with a lab written by a former CCIE proctor (this appendix). There are no solutions provided; this is a request of the CCIE department of Cisco for any CCIE sample labs. E-mail me at henry.benjamin@optusnet.com.au if you have any questions. The aim of the lab is to provide a working solution.

Basic Setup (9 Points)

Configure the network in Figure D-1 for basic physical connectivity.

Communications Server (0 Points)

NOTE Not all CCIE R&S labs require you to configure a communications server.

Configure the communications server so that when you type the host name of a router on the server, you are connected across the console port to that router. Set up the routers in Figure D-1 with the following physical attributes:

1. Configure R1 as the communication server with the **ip host** command.
2. Communication server ports 2 to 4 are connected to Routers R2 to R4, respectively.
3. Communication server port 9 connects to the Catalyst 3550 Ethernet switch.

Physical Connectivity (0 Points)

NOTE From October 1, 2001 onward, a CCIE candidate is not required to physically cable up the lab network. Therefore, no time allocation is given to this section, which is added for completeness only.

The Security lab examination also will have some elementary tasks such as Frame Relay and basic IP routing preconfigured to allow the candidate more time to configure more advanced features in Cisco IOS software. This is a great time saver for the candidate.

Your network is already physically patched. Construct your network, as shown in Figure D-1.

Configure the following characteristics for the topology in Figure D-1:

- A Frame Relay switch connects all serial links between routers. Use only the indicated DLCIs in Figure D-2 and disable Frame Relay inverse ARP for IP only.
- Routers R2 and R3 are connected to an ISDN service with the switch type defined as basic-5ess. R2 connects to number plan 0298017705 and R3 connects to number plan 0296307050.
- Routers R1 through R4 are connected to the Catalyst Ethernet switch (Catalyst 3550 series switch), according to Table D-1.

Figure D-2 *Frame Relay DLCI Assignment*

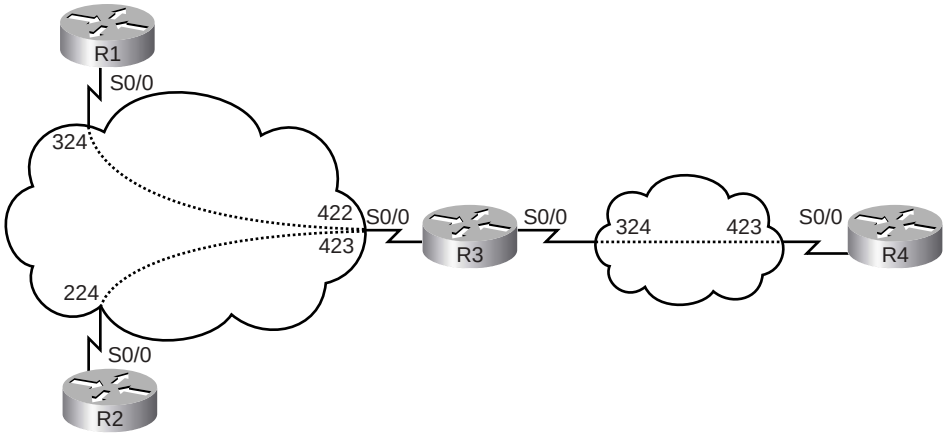


Table 8-1 *Ethernet Interface Connections to the 3550*

Router	Catalyst 3550 Port
R1 Ethernet 0/0	0/1
R2 Ethernet 0/0	0/2
R3 Ethernet 0/0	0/3
R4 Ethernet 0/0	0/4
Backbone segment 1	0/10
Backbone segment 2	0/11

Catalyst Ethernet Switch Setup I (0 Points)

Configure the Ethernet switch for three VLANs.

- VLAN 2 named VLAN_A is connected to R1, R2, and backbone segment 1.
- VLAN 3 named VLAN_B is connected to R3.
- VLAN 4 named VLAN_C is connected to R4 and backbone segment 2.
- VLAN D and E are preconfigured.

Using VLAN_A, configure the management interface sc0 with the address 133.33.0.2/25. Ensure that all devices in your network can Telnet to the switch even if R1 or R2 is down. (Note that you may need to configure an additional IP address to accomplish this task.)

Make sure the switch is configured in the VTP domain Cisc01_vTp and that the switch can create and delete VLANs in the future.

Catalyst Ethernet Switch Setup II (9 Points)

Configure the following spanning-tree parameters on the Catalyst 3550:

- Ensure that the switch never becomes the root bridge on VLAN_A.
- Configure the switch to be a VTP client once all VLANs have been created.
- Set the maximum spanning-tree age on VLAN_B to 15 seconds, the forward delay to 10 seconds, and the hello interval to 3 seconds for this instance of spanning tree only. Do not modify any other VLANs on the 3550.
- Ensure that the switch will be elected the root bridge for VLAN 1. Set all ports that are active with a broadcast control limit of 55 percent.
- In the future, IP phones will be connected to ports 15 and 16. Ensure that QoS is configured correctly so that RTP signal and data will be marked with CoS values 3 and 5; any devices attached to the phone must be marked with a CoS value of 1.
- Warn all Telnet clients that any "unauthorized access is not permitted" by displaying a warning message when any Telnet session is activated to the SC0 interface only.
- If any ports become disabled because of hardware errors, ensure that the switch automatically enables the affected ports after 10 minutes.

IP Configuration and IP Addressing (0 Points)

NOTE Because of recent changes to the CCIE exam, the candidate is not required to configure IP addressing. However, the subject is presented here to ensure that potential CCIE candidates have a good understanding of IP address spaces and subnetting. No time is projected for this section.

Use the Class B subnetted IP addresses 133.33.0.0 to 133.33.255.255 to design your network. You must use this address space for all addresses unless specified in a particular question. Read the entire task before designing your IP address space.

After your IP address space and IP routing are completed, it must be possible to reach all of your routers and switches. Set the enable password for all routers and switches to **cisco**.

Configure IP addresses on your remaining interfaces.

- Use a 28-bit mask for VLAN_A.
- Use a 27-bit mask for VLAN_B.

- Use a 28-bit mask for VLAN_C.
- Use a 24-bit mask for all other interfaces.
- Use a subnet with the least number of hosts for the ISDN link.
- Use a 25-bit mask for all Frame Relay connections running classless IP routing protocols.
- Assign each router a 24-bit subnet to be used by the loopback address. It must be possible to ping and Telnet from any one router using the loopback address.
- Configure local IP host addresses on each router so that an exec or privileged user can type the router name to ping or Telnet without having to type the full IP address.

Frame Relay Setup (8 Points)

Configure IP across your Frame Relay network, as displayed in Figure D-2.

- You have to use static maps for each protocol. No dynamic mapping is permitted.
- *No* subinterfaces are allowed on any router except on R3.
- You can assign a subnet from your Class B range.
- Use LMI-type **Cisco only** and do not rely on auto-sensing the LMI type on any routers. All router interface types are DTE. The Frame Relay port type is DCE.
- Do not use the keyword **broadcast** for the Frame Relay link between R3 and R4 when mapping IP. (Hint: use a tunnel interface for routing IP across this cloud.)
- Make sure that you can also ping the local interface from each router configured for Frame Relay.

IGP Routing (24 Points)

After this section is completed, all routers must have full IP connectivity between every routing domain, including the ISDN backup interfaces when operational.

NOTE The CCIE lab no longer tests for RIP version 1 and IGRP.

RIPv2 Configuration (9 Points)

Configure RIPv2 on Router R4 only.

- Backbone segment 2 is running RIPv2 for networks 150.100.100.0/24.
- Backbone segment 2 is running RIPv2 only. There is no RIPv2 password. You should be seeing routes of the form 199.168.32.0/16 from BB2.
- Redistribute the odd RIP routes into the IGP network from backbone segment 2.
- Make sure that you can see distributed RIP routes throughout your topology and that the OSPF cost metric is set to 1000 for all RIP routes redistributed.
- Use a route map named riptoospf to set the OSPF cost.
- Use the least number of Cisco IOS commands wherever possible.

EIGRP Configuration (7 Points)

Configure EIGRP on Routers R1, R2, and backbone router 1 only.

- Configure EIGRP in domain 333.
- Summarize as much as possible to reduce the redistributed routes into OSPF, but make sure all routes appear to all routers.
- Ensure that EIGRP is authenticated across backbone segment 1.
- Redistribute the EIGRP routes into the OSPF domain with a cost metric of 1000 seen on all OSPF routers.

OSPF Configuration (8 Points)

Configure OSPF as follows; do not create any nonspecified OSPF areas:

- Configure the OSPF backbone over the Frame Relay network between Routers R1, R2, and R3.
- The ISDN link between R2 and R3 resides in the area 0.0.0.0.
- The link between R1 and R2 resides in area 4 (note that this VLAN also runs EIGRP).
- The loopbacks on R1, R2, and R3 can reside in the most appropriate area. Do not configure any network in area 0 unless required.
- Make sure all OSPF routes are redistributed and reachable in the RIPv2 and EIGRP domains.
- Ensure that the OSPF backbone in the Frame Relay cloud is authenticated.

- Ensure that R1 or R2 is the designated router (DR) on all segments.
- Ensure that the router ID of all OSPF-enabled routers is the loopback address.
- Do not create any additional areas.
- Set the hello interval between links R1 and R2 to 20 seconds.
- Set the hello interval on the R3 Ethernet segment to 20 seconds.
- Ensure that all loopbacks appear as /24-bit networks on all IP routing tables. Do not use the **redistribute connected** command on any router to accomplish this.
- Ensure that any rogue devices running multicast OSPF do not impact any router resources.

Basic ISDN Configuration (10 Points)

The following is the ISDN switch information:

- ISDN switch type: basic-5ess.
- ISDN numbering:
  - R2: 0298017705
  - R3: 0296307050
- SPIDs are not required.

Configure the ISDN interfaces on R2 and R3 as follows:

- When R2's S0/0 goes down, R2 should place an outgoing call to R3.
- R3 cannot call R2 under any circumstance.
- Use PPP encapsulation and the strongest authentication available for the first B channel and HDLC on the second B channel.
- To ensure that costs are kept to a minimum, never bring up more than one B channel unless traffic exceeds 59 percent.
- When the Frame Relay link is restored, bring down the ISDN link after 25 minutes.
- When the ISDN link is active, all routers must be able to ping and Telnet the local ISDN interfaces on R2 and R3.
- You can use static or dynamic routing to complete this task.

VTY Changes (5 Points)

Configure all vty lines so that network administrators require local authentication.

Administrators must still use the enable password ccieToBe on all routers to access privilege mode. The username must be set to cisc0.

To allow nonprivileged users access to R1 and enable them to clear terminal server lines, ensure that all exec users can use the Cisco IOS command **clear** in exec mode on Router R1 only.

BGP Routing Configuration (18 Points)

After finishing each of the following sections, make sure all configured interfaces/subnets are consistently visible on all pertinent routers, even in the event of network failure of any one router.

Basic IBGP Configuration (4 Points)

Configure IBGP on Routers R1, R2, and R3 in your network (use AS 333):

- Do not use any WAN IP interfaces for IBGP sessions, because your network is prone to failures across the Frame Relay cloud.
- Configure R3 as route reflector.
- Minimize IBGP configurations as much as possible.
- Do not disable BGP synchronization.
- Use AS 333 on all IBGP routers.
- As long as there is IP connectivity in your network, ensure that BGP is active in all routers.
- Using the **network** command only, advertise all networks to route reflector R3.
- Do not change the administrative distance on any interior routing protocol.
- Make sure you have full BGP connectivity.
- Be sure all routers have entries in their IP routing tables.

EBGP Configuration (8 Points)

Configure EBGP on R3 and R4 as follows:

- Configure EBGP between R3 and R4.
- R3 resides in AS 333; R4 resides in AS 334.
- The neighbor on backbone segment 2 has an IP address of 150.100.200.25 and is in Autonomous System 2554.
- Configure EBGP between R4 and the external lab router on backbone segment 2.
- Permit only the registered address space as defined in the appropriate RFC as allowed networks from any EBGP-defined routers.

BGP Security (6 Points)

Configure all your BGP routers for BGP security using the password CCiE.

Ensure that if router R4 receives an update of more than 200 routes, a notification is sent to R3. Send the output of the most appropriate debug and copy the output to a local file on your PC named bgpdebug.txt.

Security and NetBIOS Filtering (26 Points)

The topics in this section include

- QoS configuration
- DHCP allocation on R4
- Access list configuration
- Firewall traffic
- NetBIOS filter

QoS Configuration (4 Points)

R1 requires congestion control. Configure R1 for the following Frame Relay parameters:

- Your provider will mark any traffic in excess of 128 kbps as discard eligible.
- Your measurement interval is 62.5 ms.

- Users on VLAN 2 are using the network to download large FTP files and also using Kazaa for unauthorized data transfer. Configure the Ethernet interfaces on R1 and R2 so that the following conditions are met:
  - All FTP data traffic is allocated 10 percent of total bandwidth.
  - All FTP control traffic is allocated 5 percent of total bandwidth.
  - All non-FTP network traffic is allocated only 1 percent of total bandwidth.
  - Any assumptions that are made must be outlined on R3. Use the **description** command to outline your assumptions.

Configure the core Frame Relay network (R1/R2 and R3) so that all traffic received with the IP precedence critical must be given the highest priority. You may use priority queuing to accomplish this task.

DHCP Allocation on R4 (5 Points)

There are a number of Windows XP users on VLAN_C that support DHCP and the ability to receive more than one IP gateway. Configure R4 to provide only a pool of DHCP addresses with the following criteria:

- IP addresses in the pool range 133.254.4.0/26
- DNS servers: 1.1.2.2 and 1.1.1.2
- Domain name: cisco.com
- Default gateway: 133.254.4.1
- Hosts must retain DHCP-assigned addresses forever.
- Ensure that the predefined addresses 133.254.4.1, 133.254.4.2, and 133.254.4.3 are never allocated to DHCP clients.

You can assume that you have only Windows XP clients and support more than one gateway.

Access List (6 Points)

On R1, configure an access list that meets the following criterion and contains the *minimum* number of configuration lines possible:

- Apply the access list on the outbound interface on R1's link to R3.
- Deny any TCP packet with source address 109.57.204.0/24.
- Deny any TCP packet with source address 109.57.140.0/24.

- Deny any TCP packet with source address 225.132.9.0/24.
- Deny any TCP packet with source address 161.132.9.0/24.
- Deny every even subnet in 108.13.0.0/16.
- Deny every odd subnet in 108.13.0.0/16.
- Permit all other IP and TCP traffic.

Confirm access to the network after applying the access list.

Log any access violations and ensure that the local buffer can log events as well.

Firewall Traffic (6 Points)

Configure an outgoing access list on the Ethernet 0/1 interface of R4 such that:

- Routing protocol traffic in use is permitted.
- Telnet sessions are permitted if they originate on backbone segment 1.
- The **trace** command should work through your firewall.
- R4 should be able to ping the backbone router on backbone segment 2, but not vice versa.
- All other traffic should be denied.

NetBIOS Filter (5 Points)

Ensure that any NetBIOS servers on segment VLAN_C are permitted access as long as the name is of the form simoniscool*xxx*, where *x* is any character.

NOTE At the request of the CCIE department, solutions to this sample lab are not provided in this book. Consider this lab a source for understanding the type of testing you can expect on a CCIE lab exam. The material in this appendix is in no way intended to represent the exact material you will see on the actual lab examination.

Conclusion

You should be able to complete the sample CCIE Routing and Switching lab in this appendix within 8 hours (this is the same allotted time for the real CCIE lab at Cisco). The difficulty level presented here is similar to what you can expect in any CCIE lab examination; in fact, the difficulty level here might be higher. Focus your attention on time management and the ability to configure a set number of Cisco IOS features very quickly. If you complete this lab successfully, try it again by modifying the questions and changing the IP routing algorithm. Together with Chapter 8, "CCIE Security Self-Study Lab," and Appendix C, "Sample CCIE Routing and Switching Lab I," you should now have a better understanding of the tasks you may be asked to undertake in a lab exam. Hopefully, Chapter 8, Appendix C, and this appendix will help you gauge your level of readiness. Because the real labs cost U.S.$1250 per attempt, these practice labs can be a valuable tool. Good luck and please feel free to e-mail me at henry.benjamin@optusnet.com.au with any questions, frustrations, or success stories.

INDEX

Symbols & Numerics

A

B

C

D

E

F

G

H

J-K

L

M

N

O

P

Q

R

S

W