EXAM CRAM

CCNP® and CCIE® Enterprise Core

ENCOR 350-401


Cram Sheet


Flash Cards


Practice Tests

DONALD BACHA

CCNP® and CCIE® Enterprise Core

ENCOR 350-401

Special Offers

ENHANCE YOUR EXAM PREPARATION

Save 70% on Complete Video Course

The *CCNP and CCIE Enterprise Core ENCOR 350-401 Complete Video Course, Complete Video Course*, available for both streaming and download, provides you with hours of expert-level instruction mapped directly to exam objectives. Put your knowledge to the test with full practice exams powered by the Pearson Test Prep practice test software, module quizzes, and more.

Save 80% on Premium Edition eBook and Practice Test

The *CCNP and CCIE Enterprise Core ENCOR 350-401 Exam Cram Premium Edition eBook and Practice Test* provides three eBook files (PDF, EPUB, and MOBI/Kindle) to read on your preferred device and an enhanced edition of the Pearson Test Prep practice test software. You will also receive two additional practice exams with links for every question mapped to the PDF eBook.

Pearson Test Prep online system requirements:

Browsers: Browsers: Chrome version 73 and above, Safari version 12 and above, Microsoft Edge 44 and above.

Devices: Desktop and laptop computers, tablets running Android v8.0 and above or iPadOS v13 and above, smartphones running Android v8.0 and above or iOS v13 and above with a minimum screen size of 4.7". Internet access required.

Pearson Test Prep offline system requirements:

Windows 10, Windows 8.1; Microsoft .NET Framework 4.5 Client; Pentium-class 1 GHz processor (or equivalent); 512 MB RAM; 650 MB disk space plus 50 MB for each downloaded practice exam; access to the Internet to register and download exam databases

---

See card insert in the back of the book >>
for your Pearson Test Prep activation code and special offers.

EXAM CRAM

CCNP and CCIE Enterprise Core ENCOR 350-401 Exam Cram

Donald Bacha

Pearson

CCNP and CCIE Enterprise Core ENCOR 350-401 Exam Cram

ISBN-13: 978-0-13-689193-2

ISBN-10: 0-13-689193-4

Library of Congress Control Number: 2021924388

ScoutAutomatedPrintCode

Editor-in-Chief
Mark Taub

Director, ITP Product Management
Brett Bartow

Executive Acquisitions Editor
James Manly

Development Editor
Ellie Bru

Managing Editor
Sandra Schroeder

Project Editor
Mandie Frank

Copy Editor
Kitty Wilson

Indexer
Erika Millen

Proofreader
Gill Editorial Services

Technical Editor
Raymond Lacoste

Publishing Coordinator
Cindy Teeters

Designer
Chuti Prasertsith

Compositor
codeMantra

Pearson's Commitment to Diversity, Equity, and Inclusion

Pearson is dedicated to creating bias-free content that reflects the diversity of all learners. We embrace the many dimensions of diversity, including but not limited to race, ethnicity, gender, socioeconomic status, ability, age, sexual orientation, and religious or political beliefs.

Education is a powerful force for equity and change in our world. It has the potential to deliver opportunities that improve lives and enable economic mobility. As we work with authors to create content for every product and service, we acknowledge our responsibility to demonstrate inclusivity and incorporate diverse scholarship so that everyone can achieve their potential through learning. As the world's leading learning company, we have a duty to help drive change and live up to our purpose to help more people create a better life for themselves and to create a better world.

Our ambition is to purposefully contribute to a world where

- Everyone has an equitable and lifelong opportunity to succeed through learning
- Our educational products and services are inclusive and represent the rich diversity of learners
- Our educational content accurately reflects the histories and experiences of the learners we serve
- Our educational content prompts deeper discussions with learners and motivates them to expand their own learning (and worldview)

While we work hard to present unbiased content, we want to hear from you about any concerns or needs with this Pearson product so that we can investigate and address them.

Please contact us with concerns about any potential bias at https://www.pearson.com/report-bias.html.

Figure Credit

Figure 5-1; Figure 5-2	Courtesy of Cisco Systems, Inc.
Figure 5-3; Figure 5-4	
Figure 5-5	
Figure 5-6	Screenshot of Monitor Section for a Cisco WLC © Cisco Systems, Inc
Figure 5-7	Courtesy of Cisco Systems, Inc.
Figure 9-1; Figure 9-2;	Courtesy of Cisco Systems, Inc.
Figure 9-3; Figure 9-4;	
Figure 9-5; Figure 9-6;	
Figure 9-7; Figure 9-8;	
Figure 9-9; Figure 9-10;	
Figure 9-11; Figure 9-12;	
Figure 9-13	
Figure 15-2; Figure 15-3;	Courtesy of Cisco Systems, Inc.
Figure 15-4	
Figure 20-6	Courtesy of Cisco Systems, Inc.
Figure 22-3	Screenshot of The Cisco vManage Main Dashboard © Cisco Systems, Inc
Figure 23-1	Screenshot of Cisco DNA Center © Cisco Systems, Inc
Figure 24-2	Screenshot of Cisco WLC QoS profiles © Cisco Systems, Inc
Figure 26-2; Figure 26-3	© 2022 VMware, Inc
Figure 26-5a; Figure 26-5b	Courtesy of Cisco Systems, Inc.
Figure 26-5c	
Figure 31-2; Figure 31-3;	Courtesy of Cisco Systems, Inc.
Figure 31-4	

Contents at a Glance

Table of Contents

About the Author

Donald Bacha is a systems engineer with a health research organization. He's the technical lead responsible for the design and implementation of networking, compute, virtualization, storage, and disaster recovery systems. Over the past 18 years, Donald has supported cloud services provider, enterprise, and data center environments by contributing to complex routing and switching, data center, storage, and virtualization projects in both greenfield and brownfield deployments. His certifications include CCNP Enterprise, CCNP Data Center, and VCAP-DCV. He holds a master's of business administration. Donald can be found at www.allthingsvirtual.net and on Twitter at @donald_bacha.

Dedication

First, I dedicate this book to our Lord and Savior Jesus Christ (I can do all things through Christ which strengthens me.—Philippians 4:13). He has blessed me with the opportunity to learn, write, and share my knowledge. To my father and mother, thank you for always supporting and encouraging me.

Acknowledgments

A debt of gratitude goes out to executive acquisitions editor James Manly for giving me the opportunity to author this book and for his guidance. A special thank you to my development editor, Ellie Bru, who did well working to get this title out and for making it as strong as it can be. Many thanks go out to Mandie Frank and Kitty Wilson for ensuring that this book looks good and reads easily. I would like to thank the entire Pearson team and those who contributed in one way or another to this project.

About the Technical Reviewer

Raymond Lacoste has dedicated his career to developing the skills of those interested in IT. In 2001, he began to mentor hundreds of IT professionals pursuing their Cisco certification dreams. This role led to teaching Cisco courses full time. Raymond is currently master instructor for Cisco Enterprise Routing and Switching, AWS, and ITIL at StormWind Studios. Raymond treats all technologies as an escape room, working to uncover every mystery in the protocols he works with. Along this journey, Raymond has passed more than 110 exams, and his office wall includes certificates from Microsoft, Cisco, ISC2, ITIL, AWS, and CompTIA. If you were visualizing Raymond's office, you'd probably expect the usual network equipment, certifications, and awards. Those certainly take up space, but they aren't his pride and joy. Most impressive, at least to Raymond, is his gemstone and mineral collection; once he starts talking about it, he just can't stop. Who doesn't get excited by a wondrous barite specimen in a pyrite matrix? Raymond presently resides with his wife and two children in eastern Canada, where they experience many adventures together.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: community@informit.com

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Introduction

Welcome to *CCNP and CCIE Enterprise Core ENCOR 350-401 Exam Cram*. This book is a late-stage preparation tool that covers the CCNP/CCIE ENCOR 350-401 certification exam. It provides the information you need to quickly and efficiently go over all the topics covered on the CCNP/CCIE ENCOR 350-401 exam. This *Exam Cram* provides concise and exam-focused coverage of all of the CCNP/CCIE ENCOR 350-401 exam domains and objectives. It allows you to assess your preparedness and helps you to practice through questions and examples of the exam topics. The information you find in this *Exam Cram* will aid you in your success as you build knowledge, gain experience, and review for the CCNP/CCIE ENCOR 350-401 exam.

About CCNP ENCOR 350-401 Exam Cram

This *Exam Cram* follows a predefined structure that makes the book easy to study as it provides the material in a concise manner. It also allows for the testing of knowledge as you go through each chapter, covering the various ENCOR domains and objectives. This book includes the following helpful elements:

- **Cram Sheet:** This foldout tear card that appears inside the front cover of the book presents important information that you should go over just before taking the exam. It is the most important "cram" element of the book and, as such, is presented as concisely as possible.
- **Chapter Topics:** Each chapter begins with a list of the exam objectives that are covered in the chapter as well as a list of the main topics in the chapters. The chapter's topics are then covered in a concise manner, with brief examples and figures where needed.
- **CramSavers:** Each chapter contains a short-answer quiz that allows you to assess how knowledgeable you are about the topics covered in the chapter. It helps you figure out if you should skip the entire chapter or skim the material and skip ahead to the Exam Alerts and CramQuizzes for particular sections.
- **Exam Alerts:** These notes provide exam-specific information that is important for you to know before you take the exam. Pay attention to Exam Alerts because the material they cover is likely to appear on the exam.

- **Cram Quizzes:** Each section of a chapter ends with a handful of multiple-choice questions that test your knowledge of the topics covered in that section. You will find the answers and explanations following each quiz.
- **Review Questions:** End-of-chapter review questions help you solidify what you have learned related to the topics for a particular chapter.

Chances are you have picked up this book in the early stage of your studies. The *Exam Cram* series was designed for late-stage study. So, unless you are very familiar with the technologies covered in the CCNP/CCIE ENCOR 350-401 exam and have considerable experience configuring and troubleshooting Cisco networks, it is highly recommended that you not use this book as your sole study resource. This *Exam Cram* is recommended for use after core knowledge has been built.

Both Cisco Press and Pearson IT Certification offer a number of CCNP/CCIE study materials to help you learn the core networking technologies covered on the CCNP/CCIE ENCOR 350-401 exam. The following highly recommended resources will help you gain core knowledge of the topics covered on the CCNP/CCIE ENCOR 350-401 exam:

- ***CCNP and CCIE Enterprise Core 350-401 Official Cert Guide*** **by Jason Gooley, Ramiro Garza Rios, Bradley Edgeworth, and David Hucaby (ISBN 978-1-58714-523-0):** This official cert guide provides in-depth coverage of the domains and objectives of the CCNP/CCIE ENCOR 350-401 exam.
- ***CCNP and CCIE Enterprise Core & CCNP Advanced Routing Portable Command Guide*** **by Patrick Gargano and Scott Empson (ISBN: 978-0-13-576816-7):** This book includes lots of configuration and verification examples to aid you in understanding the IOS commands you will encounter on the ENCOR and ENARSI exams.
- ***CCNP Enterprise Advanced Routing ENARSI 300-410 Official Cert Guide*** **by Raymond Lacoste and Brad Edgeworth (ISBN 978-1587145254):** I recommend that you read the routing-related chapters of this book (the first set of chapters, which covers EIGRP, OSPF, and BGP) to supplement your Layer 3 core knowledge.

The coauthor, Raymond Lacoste, is also the technical reviewer of this *Exam Cram*.

- **Cisco Modeling Labs (CML) Personal:** CML Personal (formerly Cisco VIRL) is a powerful network virtualization and orchestration platform you can use to study for Cisco certifications. CML Personal uses real Cisco IOS images and gives you the ability to simulate networks reliably. Both IOSv and IOSvL2 images are included. The majority of the topics that are coved in the CCNP/CCIE ENCOR 350-401 exam can be practiced using CML Personal. CML Personal allows up to 20 concurrent simulated nodes, and CML Personal Plus supports up to 40 concurrent simulated nodes. The majority of the examples in this *Exam Cram* were created using CML Personal. For more information on CML Personal, see https://developer.cisco.com/docs/modeling-labs. Cisco CML Personal can be purchased from the Cisco Learning Network Store at https://learningnetworkstore.cisco.com/cisco-modeling-labs-personal/cisco-cml-personal.

About the ENCOR 350-401 Exam

The material in this *Exam Cram* closely follows the official exam domains and objectives to ensure your success on the CCNP/CCIE ENCOR 350-401 exam. To earn the CCNP Enterprise certification, there is no formal prerequisite, although Cisco recommends that you have a good understanding of the exam topics before taking the exams. In addition, Cisco recommends that CCNP candidates have three to five years of experience implementing enterprise networking solutions.

To earn the CCNP Enterprise certification, you have to pass two exams: one required exam that covers core enterprise technologies and one enterprise concentration exam of your choice, based on your technical area of focus. Passing any of these concentration exams also allows you to earn an individual Specialist certification that helps recognize your accomplishments along the way to earning your CCNP Enterprise certification. These are the requirements for earning the CCNP Enterprise certification:

- Required exam: 350-401: Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR)
- One concentration exam:

- 300-410: Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)
- 300-415: Implementing Cisco SD-WAN Solutions (ENSDWI)
- 300-420: Designing Cisco Enterprise Networks (ENSLD)
- 300-425: Designing Cisco Enterprise Wireless Networks (ENWLSD)
- 300-430: Implementing Cisco Enterprise Wireless Networks (ENWLSI)
- 300-435: Implementing Automation for Cisco Enterprise Solutions (ENAUI)

This book focuses on the required 350-401 (ENCOR) exam. It is a 120-minute exam that tests your knowledge of enterprise infrastructure, including dual-stack architecture, virtualization, infrastructure, network assurance, security, and automation. The CCNP/CCIE ENCOR 350-401 exam is also the qualifying exam for the CCIE Enterprise Infrastructure and CCIE Enterprise Wireless certifications. Once you pass the CCNP/CCIE ENCOR 350-401 exam, you are automatically qualified to schedule and take the CCIE lab exam in those tracks.

Cisco ENCOR 350-401 Exam Topics

Table I-1 lists general exam topics (that is, objectives) and specific topics under each general topic (that is, subobjectives) for the CCNP/CCIE ENCOR 350-401 exam. This table also lists the chapter in which each exam topic is covered.

This *Exam Cram* covers every domain and objective of the CCNP/CCIE ENCOR 350-401 exam. It follows the official exam objectives closely to ensure your success on the CCNP/CCIE ENCOR 350-401 exam. As such, all of the contents, including CramSaver, Cram Quizzes, and Review Questions, map to specific objectives of the CCNP/CCIE ENCOR 350-401 exam. The latest CCNP/CCIE ENCOR 350-401 exam objectives can be found on the Cisco Learning Network at https://learningnetwork.cisco.com/s/encor-exam-topics.

TABLE I-1 **ENCOR 350-401 Exam Topics**

Chapter	ENCOR Exam Objectives
	1.0 Architecture
	1.1 Explain the different design principles used in an enterprise network
19: Enterprise Network Design Principles	1.1.a Enterprise network design such as Tier 2, Tier 3, and Fabric Capacity planning
19: Enterprise Network Design Principles	1.1.b High availability techniques such as redundancy, FHRP, and SSO
	1.2 Analyze design principles of a WLAN deployment
20: Wireless LAN Deployments	1.2.1 Wireless deployment models (centralized, distributed, controller-less, controller based, cloud, remote branch)
20: Wireless LAN Deployments	1.2.b Location services in a WLAN design
21: On-Premises vs. Cloud Infrastructure	1.3 Differentiate between on-premises and cloud infrastructure deployments
	1.4 Explain the working principles of the Cisco SD-WAN solution
22: SD-WAN	1.4.a SD-WAN control and data planes elements
22: SD-WAN	1.4.b Traditional WAN and SD-WAN solutions
	1.5 Explain the working principles of the Cisco SD-Access solution
23: SD-Access	1.5.a SD-Access control and data planes elements
23: SD-Access	1.5.b Traditional campus interoperating with SD-Access
	1.6 Describe concepts of wired and wireless QoS
24: QoS	1.6.a QoS components
24: QoS	1.6.b QoS policy
	1.7 Differentiate hardware and software switching mechanisms
25: Switching	1.7.a Process and CEF
25: Switching	1.7.b MAC address table and TCAM
25: Switching	1.7.c FIB vs. RIB
	2.0 Virtualization
	2.1 Describe device virtualization technologies
26: Basic Virtualization	2.1.a Hypervisor type 1 and 2
26: Basic Virtualization	2.1.b Virtual machine
26: Basic Virtualization	2.1.c Virtual switching

Chapter	ENCOR Exam Objectives
	2.2 Configure and verify data path virtualization technologies
27: VRF Instances, GRE, and IPsec	2.2.a VRF
27: VRF Instances, GRE, and IPsec	2.2.b GRE and IPsec tunneling
	2.3 Describe network virtualization concepts
28: Extending the Network Virtually	2.3.a LISP
28: Extending the Network Virtually	2.3.b VXLAN
	3.0 Infrastructure
	3.1 Layer 2
1: Understanding Layer 2	3.1.a Troubleshoot static and dynamic 802.1q trunking protocols
1: Understanding Layer 2	3.1.b Troubleshoot static and dynamic EtherChannels
1: Understanding Layer 2	3.1.c Configure and verify common Spanning Tree Protocols (RSTP and MST)
	3.2 Layer 3
2: Understanding Layer 3: IGPs	3.2.a Compare routing concepts of EIGRP and OSPF (advanced distance vector vs. link state, load balancing, path selection, path operations, metrics)
2: Understanding Layer 3: IGPs	3.2.b Configure and verify simple OSPF environments, including multiple normal areas, summarization, and filtering (neighbor adjacency, point-to-point and broadcast network types, and passive interface)
3: Understanding Layer 3: BGP	3.2.c Configure and verify eBGP between directly connected neighbors (best path selection algorithm and neighbor relationships)
	3.3 Wireless
5: Enterprise Wireless	3.3.a Describe Layer 1 concepts, such as RF power, RSSI, SNR, interference noise, band and channels, wireless client devices capabilities
5: Enterprise Wireless	3.3.b Describe AP modes and antenna types
5: Enterprise Wireless	3.3.c Describe access point discovery and join process (discovery algorithms, WLC selection process)
5: Enterprise Wireless	3.3.d Describe the main principles and use cases for Layer 2 and Layer 3 roaming

Chapter	ENCOR Exam Objectives
5: Enterprise Wireless	3.3.e Troubleshoot WLAN configuration and wireless client connectivity issues
	3.4 IP Services
4: IP Services	3.4.a Describe Network Time Protocol (NTP)
4: IP Services	3.4.b Configure and verify NAT/PAT
4: IP Services	2.4.c Configure first hop redundancy protocols, such as HSRP and VRRP
4: IP Services	3.4.d Describe multicast protocols, such as PIM and IGMP v2/v3
	4.0 Network Assurance
29: Troubleshooting	4.1 Diagnose network problems using tools such as debugs, conditional debugs, trace route, ping, SNMP, and syslog
30: Monitoring	4.2 Configure and verify device monitoring using syslog for remote logging
30: Monitoring	4.3 Configure and verify NetFlow and Flexible NetFlow
30: Monitoring	4.4 Configure and verify SPAN/RSPAN/ERSPAN
31: IP SLA and DNA Center	4.5 Configure and verify IPSLA
31: IP SLA and DNA Center	4.6 Describe Cisco DNA Center workflows to apply network configuration, monitoring, and management
32: NETCONF and RESTCONF	4.7 Configure and verify NETCONF and RESTCONF
	5.0 Security
	5.1 Configure and verify device access control
6: Device Access Control	5.1.a Lines and password protection
6: Device Access Control	5.1.b Authentication and authorization using AAA
	5.2 Configure and verify infrastructure security features
7: Infrastructure Security	5.2.a ACLs
7: Infrastructure Security	5.2.b CoPP
8: Securing REST APIs	5.3 Describe REST API security
	5.4 Configure and verify wireless security features
9: Wireless Security	5.4.a EAP
9: Wireless Security	5.4.b WebAuth
9: Wireless Security	5.4.c PSK
	5.5 Describe the components of network security design

Chapter	ENCOR Exam Objectives
10: Network Security Design	5.5.a Threat defense
10: Network Security Design	5.5.b Endpoint security
10: Network Security Design	5.5.c Next-generation firewall
10: Network Security Design	5.5.d TrustSec, MACsec
11: Network Access Control	5.5.e Network access control with 802.1X, MAB, and WebAuth
	6.0 Automation
12: Anatomy of Python	6.1 Interpret basic Python components and scripts
13: Building JSON Files	6.2 Construct valid JSON encoded file
14: YANG Data Modeling	6.3 Describe the high-level principles and benefits of a data modeling language, such as YANG
15: DNA Center and vManage APIs	6.4 Describe APIs for Cisco DNA Center and vManage
16: Interpreting REST API Codes	6.5 Interpret REST API response codes and results in payload using Cisco DNA Center and RESTCONF
17: EEM Applets	6.6 Construct EEM applet to automate configuration, troubleshoot, or data collection
18: Configuration Management and Orchestration	6.7 Compare agent vs. agentless orchestration tools, such as Chef, Puppet, Ansible, and SaltStack

Booking and Taking the ENCOR 350-401 Exam

Because this *Exam Cram* is a late-stage study material, by the time you are reading it, you have probably already registered to take the CCNP/CCIE ENCOR 350-401 exam. If not, my recommendation is that you go ahead and register and use that registration as motivation to prepare for the exam. If you find yourself not feeling fully prepared, or if some other circumstance comes up before the exam, you can cancel your registration. Pearson Vue allows you to cancel your registration up until 24 hours before you are scheduled to take the exam without a penalty.

At this writing, Pearson Vue allows you to take the exam at one of its testing sites or from home using the OnVUE online proctoring system, where a live proctor monitors you through the webcam of your computer. If you are using the online

proctoring system, you should run the system test and exam simulation before registering. You can register online at https://home.pearsonvue.com/cisco, over the phone, or as a Pearson Vue walk-in, where available. In the United States and Canada, you can schedule your exam up to six weeks in advance, and you must wait five calendar days from the end of your first attempt before retaking the same exam. Hopefully, with the help of this *Exam Cram* and the other recommended resources, you will not have to worry about that!

To register for the exam, you need the following information:

- Legal name (from a government-issued ID)
- Cisco certification ID (for example, CSCO00000001) or test ID number
- Valid email address
- Method of payment

At this writing, the cost of the CCNP/CCIE ENCOR 350-401 exam is US$400.

What to Expect from the Exam

If you haven't taken a certification test, the process can be a little unnerving. Even if you've taken numerous tests, it is not much better. Mastering the inner mental game often can be as much of a battle as knowing the material. Knowing what to expect before heading in can make the process a little more comfortable.

Certification tests are administered on a computer system at a VUE authorized testing center. The format of the exams is straightforward: Each question has several possible answers to choose from. The questions in this book provide a good example of the types of questions you can expect on the exam. If you are comfortable with them, the test should hold few surprises.

As you take the CCNP/CCIE ENCOR 350-401 exam, be sure to review each answer before moving on to the next question. After you answer a question, you cannot go back at a later time to make changes.

You can expect to see several types of questions on the ENCOR exam:

- **Multiple-choice, single answer:** This type of question requires you to choose only one answer for a question. Once you select the radio button for your answer, click Next to move on to another question.
- **Multiple-choice, multiple answers:** This type of question shows you how many answers you need to select. To select the answers, you click the

small squares next to the answers of your choice to insert checkmarks. Once you choose the correct number of questions, you can click Next to move on to the next question.

- **Drag and drop:** This type of question requires you to select an option on the left and drag and drop it to its appropriate drop zone on the right. Sometimes only some of the options on the left are used.
- **Fill-in-the-blank:** This type of question requires you to insert your answer in a text box. Sometimes you may have to fill in multiple text boxes.
- **Testlet:** This type of question is scenario based. It involves reading a scenario and then answering the question(s) related to the scenario. Testlet questions are typically some variation of multiple-choice questions.

Cisco has published two exam tutorial videos that provide a walk-through demonstration on the various exam question types and how they function. You can find these short videos at https://learningnetwork.cisco.com/s/certification-exam-tutorials.

A Few Exam-Day Details

It is recommended that you arrive at the examination room at least 15 minutes early, although a few minutes earlier certainly would not hurt. This will give you time to prepare and will give the test administrator time to answer any questions you might have before the test begins. Many people suggest that you review the most critical information about the test you're taking just before the test. (Exam Cram books provide a reference—the Cram Sheet, located inside the front of this book—that lists the essential information from the book in distilled form.) Arriving a few minutes early will give you some time to compose yourself and mentally review this critical information.

You will be asked to provide two forms of ID, one of which must be a photo ID. Both of the forms of ID you choose should have signatures. You also might need to sign in when you arrive and sign out when you leave.

Be warned: The rules are clear about what you can and cannot take into the examination room. Books, laptops, note sheets, and so on are not allowed in the examination room. The test administrator will hold these items, to be returned after you complete the exam. You might receive either a wipe board or a pen and a single piece of paper for making notes during the exam. The test administrator will ensure that no paper is removed from the examination room.

After the Test

Whether you want it or not, as soon as you finish your test, your score displays on the computer screen. In addition to the results appearing on the computer screen, a hard copy of the report prints for you. Like the onscreen report, the hard copy displays the results of your exam and provides a summary of how you did on each section and on each technology. If you were unsuccessful, this summary can help you determine the areas you need to brush up on. After you have taken the CCNP/CCIE ENCOR 350-401 exam, please note the following:

- Every written proctored exam passed equals a Specialist certification.
- Within 24 hours of passing your certifying exam, you will receive an email advising you on the next steps. You must complete the steps to trigger the fulfillment process.
- The Cisco Certification Tracking System records exam and certification status. Be sure to keep your contact information up to date if you want to receive notifications.
- After you're certified, you will be authorized to use the Cisco Certification logo that identifies your status, provided that you read and acknowledge the Cisco Certifications Logo Agreement. You can download logos through the Certifications Tracking System.
- Visit the Certification and Fulfillment Benefits page to learn more about the certification fulfillment process and the benefits you'll receive.

Last-Minute Exam Tips

Studying for a certification exam is no different than studying for any other exam, but a few hints and tips can give you the edge on exam day:

- **Read all the material:** Read each question carefully and entirely before answering.
- **Watch for the Exam Alerts:** The CCNP/CCIE ENCOR 350-401 exam objectives include a wide range of technologies. Exam Alerts found throughout each chapter of this book are designed to highlight exam-related hot spots. Skim the book for Exam Alerts when preparing for the exam.
- **Use the questions to assess your knowledge:** Don't just read the chapter content; use the CramSaver questions to find out what you know and what you don't. If you struggle to answer any of these questions, read the entire chapter, including Exam Alerts, and complete the Cram Quiz

at the end of each section and the Review Questions at the end of the chapter.

- **Review the exam objectives:** Develop your own questions and examples for each topic listed. If you can develop and answer several questions for each topic, you should not find it difficult to pass the exam.

Good luck with your CCNP/CCIE ENCOR 350-401 exam studies, and thank you for selecting the *CCNP and CCIE Enterprise Core ENCOR 350-401 Exam Cram*.

Companion Website

Register this book to get access to the Pearson Test Prep practice test software and other study materials plus additional bonus content. Check this site regularly for new and updated postings written by the author that provide further insight into the more troublesome topics on the exams. Be sure to check the box that you would like to hear from us to receive updates and exclusive discounts on future editions of this product or related products.

To access this companion website, follow these steps:

1. Go to **www.pearsonITcertification.com/register** and log in or create a new account.
2. Enter the ISBN **9780136891932**.
3. Answer the challenge question as proof of purchase.
4. Click the **Access Bonus Content** link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

Please note that many of our companion content files, especially image and video files, can be very large.

If you are unable to locate the files for this title by following these steps, please visit www.pearsonITcertification.com/contact and select the Site Problems/Comments option. Our customer service representatives will assist you.

Pearson Test Prep Practice Test Software

This book comes complete with the Pearson Test Prep practice test software, containing two full exams. These practice tests are available to you either online or in an offline Windows application. To access the practice exams that

were developed with this book, please see the instructions in the card inserted in the sleeve in the back of the book. This card includes a unique access code that enables you to activate your exams in the Pearson Test Prep practice test software.

> **Note**
>
> The cardboard sleeve in the back of this book includes a piece of paper. The paper lists the activation code for the practice exams associated with this book. Do not lose the activation code. On the opposite side of the paper from the activation code is a unique, one-time-use coupon code for the purchase of the Premium Edition eBook and Practice Test.

Accessing the Pearson Test Prep Software Online

The online version of this software can be used on any device with a browser and connectivity to the Internet, including desktop machines, tablets, and smartphones. To start using your practice exams online, simply follow these steps:

1. Go to **http://www.PearsonTestPrep.com**.
2. Select **Pearson IT Certification** as your product group.
3. Enter your email and password for your account. If you don't have an account on PearsonITCertification.com or CiscoPress.com, you need to establish one by going to **PearsonITCertification.com/join**.
4. In the **My Products** tab, click the **Activate New Product** button.
5. Enter the access code printed on the insert card in the back of your book to activate your product. The product is then listed in your My Products page.
6. Click the Exams button to launch the exam settings screen and start the exam.

Accessing the Pearson Test Prep Software Offline

If you wish to study offline, you can download and install the Windows version of the Pearson Test Prep software. You can find a download link for this software on the book's companion website, or you can just enter this link in your browser:

http://www.pearsonitcertification.com/content/downloads/pcpt/engine.zip

To access the book's companion website and the software, simply follow these steps:

1. Register your book by going to PearsonITCertification.com/register and entering the ISBN **9780136891932**.
2. Respond to the challenge questions.
3. Go to your account page and select the **Registered Products** tab.
4. Click on the **Access Bonus Content** link under the product listing.
5. Click the **Install Pearson Test Prep Desktop Version** link in the Practice Exams section of the page to download the software.
6. When the software finishes downloading, unzip all the files onto your computer.
7. Double-click the application file to start the installation, and follow the onscreen instructions to complete the registration.
8. When the installation is complete, launch the application and click the **Activate Exam** button on the My Products tab.
9. Click the **Activate a Product** button in the Activate Product Wizard.
10. Enter the unique access code from the card in the sleeve in the back of your book and click the **Activate** button.
11. Click **Next** and then click the **Finish** button to download the exam data to your application.
12. You can now start using the practice exams by selecting the product and clicking the **Open Exam** button to open the exam.

Note that the offline and online versions sync together, so saved exams and grade results recorded on one version will be available to you in the other version as well.

Customizing Your Exams

When you are in the exam settings screen, you can choose to take exams in one of three modes:

- Study mode
- Practice Exam mode
- Flash Card mode

Study mode allows you to fully customize an exam and review answers as you are taking the exam. This is typically the mode you use first to assess your knowledge and identify information gaps. Practice Exam mode locks certain customization options in order to present a realistic exam experience. Use this mode when you are preparing to test your exam readiness. Flash Card mode strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation, when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode does not provide the detailed score reports that the other two modes provide, so it is not the best mode for helping you identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all of the chapters, or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. The two exams printed in the book are available to you, as are two additional exams of unique questions. You can have the test engine serve up exams from all four banks or just from one individual bank by selecting the desired banks in the exam bank area.

You can make several other customizations to your exam from the exam settings screen, such as the time of the exam, the number of questions, whether to randomize questions and answers, whether to show the number of correct answers for multiple answer questions, or whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software, it will check to see if there are any updates to your exam data and automatically download any changes made since the last time you used the software. This requires you to be connected to the Internet at the time you launch the software.

Sometimes, due to a number of factors, the exam data might not fully download when you activate your exam. If you find that figures or exhibits are missing, you might need to manually update your exams.

To update a particular exam you have already activated and downloaded, simply select the **Tools** tab and click the **Update Products** button. Again, this is only an issue with the desktop Windows application.

If you want to check for updates to the Windows desktop version of the Pearson Test Prep exam engine software, simply select the **Tools** tab and click the **Update Application** button. Doing so allows you to ensure that you are running the latest version of the software engine.

Assessing Exam Readiness

Exam candidates never really know whether they are adequately prepared for the exam until they have completed about 30% of the questions. At that point, if you are not prepared, it is too late. The best way to determine your readiness is to work through the CramSaver quiz at the beginning of each chapter and review the topics presented in each chapter. It is best to work your way through the entire book unless you can complete each subject without having to do any research or look up any answers.

Premium Edition eBook and Practice Tests

This book includes an exclusive offer for 70% off the Premium Edition eBook and Practice Tests edition of this title. Please see the coupon code included with the cardboard sleeve for information on how to purchase the Premium Edition.

CHAPTER 6

Device Access Control

This chapter covers the following official ENCOR 350-401 exam objectives:

- 5.1 Configure and verify devices access control
- 5.1.a Lines and password protection
- 5.1.b Authentication and authorization using AAA

This chapter is divided into two sections. The first section looks at the configuration and verification of network device access control with usernames and passwords. It also covers the configuration and verification of role-based access control (RBAC) using privilege levels. The second section covers authentication, authorization, and accounting (AAA). It looks at the configuration and verification of network device access control on Cisco IOS devices using TACACS+ and RADIUS.

This chapter covers the following technology topics:

- Cisco IOS CLI Session Overview
  - Protection of Access to Cisco IOS EXEC Modes
  - Secured Access with SSH
  - Privilege Levels and Role-Based Access Control (RBAC)
- Authentication, Authorization, and Accounting (AAA) Overview
  - TACACS+ Overview
  - RADIUS Overview
  - AAA Configuration for Network Devices

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the CramQuiz at the end of each section and the Review Questions at the end of the chapter. If you are in doubt at all, read everything in this chapter!

1. What are the first steps in securing user EXEC access to allow for secure network device access?
2. Which command option on remote CLI sessions is used to limit the session to use only a secure connection method?
3. What protocol does TACACS+ use for communication between a TACACS+ client (network device) and a TACACS+ server?
4. What are two of the high-level benefits of using a remote AAA server over local AAA services on each network device individually?

Answers

1. Configure passwords for local and remote CLI sessions.
2. **transport input ssh**
3. TCP port 49
4. Scalability and standardized authentication methods using RADIUS and TACACS+

Cisco IOS CLI Session Overview

Cisco IOS software provides several features that you can use to implement basic security for network devices' command-line sessions. These features include:

- Using different levels of authorization for CLI sessions to control access to commands that can modify the status of the networking device and for commands that are used to monitor the device
- Assigning passwords to CLI sessions
- Requiring users to log in to a networking device with a username
- Changing the privilege levels of commands to create new authorization levels for CLI sessions

You can establish IOS CLI sessions on Cisco IOS devices in two ways:

- **Local CLI sessions:** Local CLI sessions require direct access to the console port of the networking device. Local CLI sessions start in user EXEC mode. All of the tasks needed to configure and manage a networking device can be done using a local CLI session. The most common method for establishing a local CLI session is to connect a laptop to the console port of the networking device and then launch a terminal emulation application, like Putty, on the computer. The type of cable and connectors required and the settings for the terminal emulation application depend on the type of networking device that you are configuring. Some devices have an auxiliary (aux) port for remote administration through a dial-up modem. In most cases, this should be disabled with the **no exec** command under **line aux 0**.
- **Terminal lines and remote CLI sessions:** A remote CLI session is created between a host and a networking device by using a remote terminal access application, such as Telnet or SSH. Most of the tasks required to configure and manage a networking device can be done using a remote CLI session. The exceptions are tasks that interact directly with the console port (such as recovering from a corrupted operating system by uploading a new OS image over the console port) and interacting with the networking device when it is in ROMMON mode. SSH is a more secure alternative to Telnet. SSH provides encryption for the session traffic between the local management device and the networking device you are managing. Encrypting the session traffic with SSH prevents anyone who may have intercepted the traffic from decoding it.

With Cisco IOS networking devices, the word "lines" is used to refer to the software components that manage local and remote CLI sessions. You use the **line console 0** global configuration command to enter line configuration mode to configure options such as a password for the console port. Remote CLI sessions use lines that are referred to as vty lines. You use the **line vty** *line-number* [*ending-line-number*] global configuration command to enter line configuration mode to configure options such as a password for remote CLI sessions. Once you are in the line configuration mode, you can set the protocol you will be connecting over (for example, SSH).

Example 6.1 shows the console, auxiliary, and vty lines in the running configuration that are available on R1.

EXAMPLE 6.1 **Console, Auxiliary, and vty Lines in the Running Configuration**

```
R1#
R1# show running-config | section line
line con 0
line aux 0
line vty 0 4
R1#
```

Before we look at how to protect access to Cisco IOS EXEC modes, let's take a look at the five different types of passwords available in Cisco IOS:

- **Type 0 passwords:** Type 0 passwords are not encrypted and are stored in plaintext in the device configuration. The **enable password** command uses type 0 passwords. Type 0 passwords should not be used in a production environment.
- **Type 5 passwords:** Type 5 passwords use an MD5 hashing algorithm. These passwords are easily reversible with tools available on the Internet. The **enable secret** and **username** *username* **secret** commands use type 5 passwords.
- **Type 7 passwords:** Type 7 passwords uses the Vigenère cipher encryption algorithm, which is known to be weak. These passwords are easily reversible (in under 1 second) with tools available on the Internet. Type 7 password encryption is enabled with the **service password encryption** command.
- **Type 8 passwords:** Type 8 passwords use a Password-Based Key Derivation Function 2 (PBKDF2) with a SHA-256 hashed secret. Type 8 password security is considered good.
- **Type 9 passwords:** Type 9 passwords use the SCRYPT hashing algorithm. Type 9 passwords are considered the best passwords and should be used when supported.

Type 4 passwords were deprecated in IOS 15.3(3). The type 4 password hash was weaker than the type 5 (MD5) hash. Therefore, type 4 passwords should never be used. IOS 15.3(3) introduced support for type 8 and type 9 passwords, and these password types should always be used when supported.

Protection of Access to Cisco IOS EXEC Modes

This section looks at the steps you can take to secure both user and privileged EXEC modes.

The first step in creating secure network device access is to protect the user EXEC mode by configuring passwords for local and remote CLI sessions. You start by entering line configuration mode by selecting the line number for the console port (for example, **line console 0**). Once you are in that mode, you use the **password** command to assign a password to **line console 0**. You use the **login** command at **line console 0** to enable password checking at login.

Next, let's look at configuring a password for remote CLI sessions. After a password is configured for remote CLI sessions, the IOS device prompts for a password the next time you establish a remote CLI session with that device. Cisco IOS networking devices require that a password be configured for remote CLI sessions. If you attempt to start a remote CLI session with a device that does not have a password configured for remote CLI sessions, you get a message indicating that a password is required and that the password is not set. The remote CLI session will be terminated by the remote host.

To configure a password for remote CLI sessions, you start by entering the line configuration mode and selecting the vty line (for example, **line vty 0 4**). When you are in that mode, you use the **password** command as you do for the console line. You use the **login** command at the vty line to enable password checking at login.

Example 6.2 shows how to assign a password to the console, auxiliary, and vty lines and verify it in the running configuration.

EXAMPLE 6.2 **Configuring and Verifying Line Passwords**

```
R1#
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# line con 0
R1(config-line)# password Cisco123
R1(config-line)# login
R1(config-line)# line aux 0
R1(config-line)# password Cisco123
R1(config-line)# login
R1(config-line)# line vty 0 4
```

```
R1(config-line)# password Cisco123
R1(config-line)# login
R1(config-line)# end
R1#
R1# show running-config | section line
line con 0
 password Cisco123
 login
line aux 0
 password Cisco123
 login
line vty 0 4
 password Cisco123
 login
R1#
```

The previous section covers protection of access to both local and remote CLI sessions in user EXEC mode using line passwords. Now let's look at how to protect access to privileged EXEC mode. To add an additional layer of security, particularly for passwords that cross a network or that are stored with the configuration on a TFTP server, you can use the **enable secret** global configuration command.

Cisco recommends the use of the **enable secret** command over the **enable password** command because it uses an improved encryption algorithm. When you configure the **enable secret** command, it takes precedence over the **enable password** command. The two commands cannot be in effect simultaneously.

Let's look at the use of the **enable password** command to configure a password for privileged EXEC mode. The password you enter with the **enable password** command is stored as plaintext in the device's running configuration. You can encrypt the password for the **enable password** command in the configuration file of the networking device by using the **service password-encryption** command. However, the type 7 encryption level used by the **service password-encryption** command can be decrypted using tools available on the Internet, so it is not recommended for production deployments. The recommendation is to use the **enable secret** command because it provides strong encryption by hashing the password using type 5 passwords by default. However, on modern platforms, you can use type 8 or 9 passwords as well. You configure a password in privileged EXEC mode by using the command **enable secret** [**level** *level*] *unencrypted-password* | *encryption-type encrypted-password.* You can use the **show privilege** command to display the current level of privilege.

Example 6.3 shows the configuration and verification of protection of privileged EXEC mode using the **enable password** command. Note in the

verification that the password is stored in the running configuration in plaintext. This is because the default password, of type 0, was used. You can also set a type 7 password or set the EXEC level here. The command **service password-encryption** would make the password unreadable in the running configuration.

EXAMPLE 6.3 **Protecting Privileged EXEC with enable password**

```
R1#
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# enable password ?
  0       Specifies an UNENCRYPTED password will follow
  7       Specifies a HIDDEN password will follow
  LINE    The UNENCRYPTED (cleartext) 'enable' password
  level   Set exec level password

R1(config)# enable password ExamCram123
 WARNING: Command has been added to the configuration using a type 0
password. However, type 0 passwords will soon be deprecated. Migrate
to a supported password type
R1(config)#
*Oct 28 23:00:00.922: %AAAA-4-CLI_DEPRECATED: WARNING: Command has
been added to the configuration using a type 0 password. However, type
0 passwords will soon be deprecated. Migrate to a supported password
type

R1(config)# do show run | include password
enable password ExamCram123
R1(config)#
R1(config)# service password-encryption
R1(config)# do show run | include password
enable password 7 106B11180834000A01557878
R1(config)# end
R1#
```

Example 6.4 shows the configuration and verification of protection of privileged EXEC mode using the **enable secret** command. This provides stronger encryption and is the recommended method to use. This example uses type 9 encryption. When using type 9, you need to type in the encrypted password or use the **algorithm-type** command to hash a plaintext **enable** secret. Note that the verification output shows the encrypted type 9 password.

EXAMPLE 6.4 **Protecting Privileged EXEC with enable secret**

```
R1#
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
R1(config)# enable ?
  algorithm-type  Algorithm to use for hashing the plaintext 'enable'
secret
  password        Assign the privileged level password (MAX of 25
                  characters)
  secret          Assign the privileged level secret (MAX of 25
                  characters)

R1(config)# enable algorithm-type scrypt secret ?
  LINE   The UNENCRYPTED (cleartext) 'enable' secret
  level  Set exec level password

R1(config)# enable algorithm-type scrypt secret ExamCram123
R1(config)# do sho run | include secret
enable secret 9 $9$QlfhhreZrBM56f$VX4YG.yR/jHO/3gLFfTPqAw.
cdraNRDSKJoEOtCrC3Q
R1(config)# end
R1#
```

After you have protected access to user EXEC mode and privileged EXEC mode by configuring passwords for them, you can further increase the level of security on the device by creating usernames. You configure usernames to limit access to CLI sessions to a networking device to specific users. This is especially important if you are configuring a device to allow first-line technical support user access. These users typically would not need to run all commands available in privileged EXEC mode. For example, suppose you want technical support staff to be able to view the configuration on a device that will help them to troubleshoot network problems without being able to modify the configuration. In this case, you can create a username, configure it with privilege level 15, and configure it to run the **show running-config** command automatically. When a user logs in with the username, the running configuration will be displayed automatically.

There are three ways you can configure a username on a Cisco IOS device:

- Using the command **username** *username* **password** *password* configures a plaintext password (type 0).
- Using the command **username** *username* **secret** *password* provides type 5 encryption.
- Using the command **username** *username* **algorithm-type** [**md5** | **sha256** | **scrypt**] **secret** *password* provides type 5, type 8, or type 9 encryption, respectively.

The last option provides the highest level of security since it allows for the highest level of password encryption (type 8 or type 9). If the final option is not supported on a network device, then the second option should be used since it provides MD5 encryption. The first option should be avoided because it configures a plaintext password.

When you enable password authentication on a line by using the **password** command, you need to enable password checking. You do so by using the **login** command. This is what allows password use on the line. Once you have an alternate connection to the device, you can test the login. It is a good idea to have an alternate connection to a device if there is a problem logging in again using the line you made the changes on. The **login local** command allows for username/password pairs stored locally on the router to be used for the lines. By using the command **login local**, you can disable any password configured on lines.

To enable username and password authentication on a line, you need to do the following configuration:

- Create the user with the **username** command in global configuration mode, using one of the three options listed earlier in this section.
- Use the **login local** command in line configuration mode.

For remote CLI sessions, you can further protect the lines by using the **transport input** command. This command controls what protocols are allowed to access the vty lines. This can be configured with the command **transport input** {**all** | **none** |**telnet** | **ssh**}. The **all** option allows both Telnet and SSH access; **none** blocks Telnet and SSH; **telnet** allows only Telnet; and **ssh** allows only SSH access. Using **telnet ssh** allows both Telnet and SSH access. For the most secure access, the vty lines should be limited to SSH.

Example 6.5 shows the configuration and verification of usernames. The user **user1** is configured with a type 0 password, **admin1** is configured with a type 9 password, **tier1admin** is configured with a type 9 password (scrypt in this case), and **tier2admin** is configured with a type 8 password (sha256 in this case). The **login local** command is configured under the vty lines to tell it to use the router local user account database for authentication.

In this example, take note of the configured user accounts and the password types. **user1** with the type 0 password is shown in running configuration in plaintext. Privilege level 15 gives access to all commands, such as the **reload** command, and allows a user to make configuration changes on the device.

EXAMPLE 6.5 **Configuring Usernames and Passwords**

```
R1#
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# username user1 password weakpassword
 WARNING: Command has been added to the configuration using a type 0
password. However, type 0 passwords will soon be deprecated. Migrate
to a supported password type
R1(config)# username admin1 privilege 15 secret admin1secret
R1(config)# username tier1admin algorithm-type scrypt secret
tier1adminsecret
R1(config)# username tier2admin algorithm-type sha256 secret
tier2adminsecret
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# end
R1#
R1# show running-config | include username
username user1 password 0 weakpassword
username admin1 privilege 15 secret 9 $9$iVS2wE3FxvTvDv$6k.
NoCSCi2af4T8HpWeO1lBaTUnJzelT8S6xEETp7AI
username tier1admin secret 9 $9$bIFEJkC8eW9Xyf$vXBZD.8ZSiHTcjpNVfuMWwX
vveegKfHCfNXgLZUYA9w
username tier2admin secret 8 $8$PLF4/9DTLkfoTf$820AEmeaZA2mNh1oNJjAYk6
bYKSlLhUn9pULnifodyo
R1#
```

Example 6.6 shows how to establish a Telnet session from R2 to R1 by using username-based authentication with the **tier1admin** username and type 9 password created earlier. You can see here that you can successfully connect and authenticate by using the **tier1admin** account.

EXAMPLE 6.6 **Verifying Username-Based Authentication for vty Lines**

```
R2#
R2# telnet 100.1.1.1
Trying 100.1.1.1 ... Open


User Access Verification

Username: tier1admin
Password:

! Password entered is not displayed by the router
R1>

R1#
```

```
R1# show line
  Tty Typ     Tx/Rx  A Modem  Roty AccO AccI  Uses  Noise Overruns Int
*   0 CTY            -    -      -    -    -    0      0   0/0      -
    1 AUX 9600/9600  -    -      -    -    -    0      0   0/0      -
*  578 VTY           -    -      -    -    -    2      0   0/0      -
   579 VTY           -    -      -    -    -    0      0   0/0      -
   580 VTY           -    -      -    -    -    0      0   0/0      -
   581 VTY           -    -      -    -    -    0      0   0/0      -
   582 VTY           -    -      -    -    -    0      0   0/0      -

Line(s) not in async mode -or- with no hardware support:
2-577
! the * in the output of the showline command indicates that the first
vty (0) is in use
! vty 0 is mapped to vty 578 automatically

R1#
```

ExamAlert

For the ENCOR exam, it is important to know the differences between the two SSH versions as well as the high-level steps for SSH configuration on Cisco devices.

Secured Access with SSH

SSH is a far more secure option than Telnet. Although Telnet is the most popular protocol used to access Cisco IOS devices, it is an insecure protocol. Its session packets are carried in plaintext, making it easy for someone to sniff and capture session information as it traverses the network. SSH provides encryption for session traffic between a device and a terminal access application. This prevents others from being able to intercept and decode the traffic.

SSH is available in two versions:

- **SSH Version 1 (SSHv1):** SSHv1 should be avoided because there are some flaws in its implementation, including its weak CRC-32 integrity check.
- **SSH Version 2 (SSHv2):** SSHv2 should be used when it is supported. The SSHv2 enhancement for RSA supports RSA-based public key authentication for a client and a network device. SSHv2 is not compatible with SSHv1.

Let us now take a look at the steps that are needed to set up a Cisco IOS device to run SSH:

1. Configure a hostname for the device, using the **hostname** *hostname* command.
2. Configure a domain name for the device, using the **ip domain-name** *domain-name* command.
3. Generate an RSA crypto key. Generating a key pair on the IOS device automatically enables SSH. When you generate an RSA key, you are prompted to enter a modulus length. A longer modulus length takes longer to generate, but it is more secure. You generate an RSA key with the **crypto key generate rsa** command.

Those three steps are mandatory. After you have taken those steps, you may need to set SSH to Version 2 because it is at SSHv1 by default on some platforms. You do this with the **ip ssh version 2** command. The other settings you can configure for the SSH service running on a device are the SSH timeout value and the authentication retries number. You do so with the command **ip ssh timeout** *seconds* **authentication-retries** *number*. Next, you set the transport input at the vty lines by using the **transport input ssh** command. Finally, also at the vty lines, you use the **login local** command to cause the local username and password on the router to be used for authentication.

For verification, you can use the **show ip ssh** command to view the version and configuration information for the SSH server. We can also use the **show ssh** command to show the status of the SSH server.

Example 6.7 demonstrates how to configure SSH, secure the vty lines to allow only SSH access, and verify connectivity from R2 to R1.

EXAMPLE 6.7 **Configuring and Verifying vty Access with SSH**

```
R1#
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# username admin2 secret Cisco123
R1(config)# ip domain-name cisco.com
R1(config)# crypto key generate rsa
The name for the keys will be: R1.cisco.com
Choose the size of the key modulus in the range of 360 to 4096 for
your General Purpose Keys. Choosing a key modulus greater than 512 may
take a few minutes.
```

```
How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

R1(config)# ip ssh version 2
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# end
R1#

R2# ssh ?
  -c    Select encryption algorithm
  -l    Log in using this user name
  -m    Select HMAC algorithm
  -o    Specify options
  -p    Connect to this port
  -v    Specify SSH Protocol Version
  -vrf  Specify vrf name
  WORD  IP address or hostname of a remote system

R2# ssh -l admin2 -v 2 100.1.1.1


Password:
! Password entered is not displayed by the router

R1>
```

Finally, you can set a timeout for EXEC sessions that are left idle, which may pose a security risk. Under the line confirmation mode, you can use the **exec-timeout** *minutes seconds* command to set the timeout. The default setting is 10 minutes. Using **exec-timeout 0 0** and **no exec-timeout** disables the EXEC timeout. You should not use these commands this way in a production environment.

The **absolute-timeout** *minutes* command in the line configuration mode sets the interval for closing the EXEC session after a specified time has elapsed. This session is closed even if it is being used at the time of termination. You can use the **logout-warning** *seconds* command with the **absolute-timeout** command to notify users of an impending logout. By default, the user is given 20 seconds' notice before the session is terminated.

Example 6.8 shows how to configure EXEC and absolute timeouts and logout warning. For **line con 0**, a timeout value of 4 minutes is configured. For the vty lines, a value of 3 minutes and 30 seconds is configured. For the vty lines,

an absolute timeout of 10 minutes is configured, with a 120-second logout warning.

EXAMPLE 6.8 **Configuring EXEC and Absolute Timeouts**

```
R1#
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# line con 0
R1(config-line)# exec-timeout 4 0
R1(config-line)# line vty 0 4
R1(config-line)# exec-timeout 3 30
!next we configure absolute timeout and logout warning
R1(config-line)# absolute-timeout 10
!logout warning is configured in seconds
R1(config-line)# logout-warning 120
R1(config-line)# end
R1#
```

Privilege Levels and Role-Based Access Control (RBAC)

Now that we have examined the various ways of securing user and privileged EXEC modes, let's take a look at the use of privilege levels and RBAC. By default, Cisco IOS devices have three privilege levels:

- **Privilege level 0:** Privilege level 0 allows for the use of five commands: **enable**, **disable**, **help**, **logout**, and **exit**.
- **Privilege level 1:** Privilege level 1 is the user EXEC mode that you saw configured earlier in this chapter, in the section "Protection of Access to Cisco IOS EXEC Modes." In this mode, it is not possible to make configuration changes.
- **Privilege level 15:** Privilege level 15 is the privileged EXEC mode you saw configured earlier in this chapter, in Example 6.5. (It is also configured in the next example.) In this mode, all of the IOS CLI commands are available.

The commands that you can run in user EXEC mode at privilege level 1 are a subset of the commands that you can run in privileged EXEC mode at privilege 15. You can configure additional privilege levels from 2 through 14 to provide customized access control. For example, you might want to allow a group of

technical support staff to configure only a specific set of interface-level commands on interfaces while preventing device-wide configuration privileges. You could configure this in global configuration mode by using the command **privilege** *mode* **level** *level* [*command string*]. After you create that technical support user and assign this privilege, the user will be allowed to enter the interface and execute the commands specified in the command string. You can verify the configuration with the **show privilege** command.

Example 6.9 shows how to set up privileges to allow a network operation staff member to do basic manipulation of an interface. This example shows how to create the user **user1noc** with a type 9 password and privilege level 5 configured. In this particular case, a user with the **user1noc** username will be allowed to shut, unshut, and assign an IP address on the interface because these are the only commands this configuration allows in privilege level 5 in interface configuration mode. A user who tries to type a command that is not allowed (such as the **description** command) gets the message "Invalid input detected."

EXAMPLE 6.9 **Configuring and Verifying a Username and a Privilege Level**

```
R1#
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# username user1noc privilege 5 algorithm-type scrypt secret
Cisco123
R1(config)# privilege exec level 5 configure terminal
R1(config)# privilege configure level 5 interface
R1(config)# privilege interface level 5 shutdown
R1(config)# privilege interface level 5 no shutdown
R1(config)# privilege interface level 5 ip address
R1(config)# end
R1#

R2# telnet 100.1.1.1
Trying 100.1.1.1 ... Open

User Access Verification

Username: user1noc
Password:

R1# show privilege
Current privilege level is 5
R1#
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
R1(config)# interface GigabitEthernet 0/0

!The options to configure on the interface are limited
R1(config-if)# ?
Interface configuration commands:
  default   Set a command to its defaults
  exit      Exit from interface configuration mode
  help      Description of the interactive help system
  ip        Interface Internet Protocol config commands
  no        Negate a command or set its defaults
  shutdown  Shutdown the selected interface

R1(config-if)# description test
                ^
% Invalid input detected at '^' marker.
R1(config-if)# end
R1#
```

CramQuiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Which of these commands can you use to force the vty lines to only allow remote connections via a protocol that supports encryption?
   - ❍ **A. transport input telnet**
   - ❍ **B. transport input ssh**
   - ❍ **C. crypto key generate rsa**
   - ❍ **D. ip ssh version 2**

2. What type of encryption does the **service password encryption** command provide?
   - ❍ **A.** Type 0
   - ❍ **B.** Type 5
   - ❍ **C.** Type 7
   - ❍ **D.** Type 9

3. True or false: SSH Version 1 implementation is compatible with SSH Version 2 implementation.
   - ❍ **A.** True
   - ❍ **B.** False

Answers

1. **B** is correct. You can restrict the terminal line for SSH only by using the **transport input ssh** command in line configuration mode.
2. **C** is correct. Type 7 password encryption is enabled with the **service password encryption** command.
3. **B** is correct. SSHv2 is not compatible with SSHv1.

Authentication, Authorization, and Accounting (AAA) Overview

Using line and local authentication as well as privilege levels works fine for controlling access on a small number of devices. However, this solution does not scale well as the number of devices grows. It becomes cumbersome and introduces the risk of inconsistent access control configurations across devices. To help simplify configuration and maintain consistency as the number of Cisco IOS devices grows, you can use an authentication, authorization, and accounting (AAA) solution.

There are many AAA protocol implementations, but this chapter focuses on the two most popular of them: RADIUS and TACACS+.

With AAA, network devices use a centralized RADIUS or TACACS+ server to authenticate users, authorize the commands users can run on a device, and provide accounting information. As a fallback mechanism, it is recommended that you still use local authentication in case the AAA server becomes unavailable at some point.

Let's briefly examine the AAA framework and how each part of it provides security functions:

- **Authentication:** Authentication provides identity verification before access to a network device is granted. It is the process of verifying the identity of the person or device accessing a network device, and it is based on the username and password combination provided by the entity trying to gain access.
- **Authorization:** Authorization provides access control. It is the process of assembling a set of attributes that describes what the user is authorized to perform. RADIUS and TACACS+ authorize users for specific rights by associating attribute/value (AV) pairs, which define the rights and the appropriate users.
- **Accounting:** Accounting provides a method for collecting information, logging the information locally on a network device, and sending the information to an AAA server for billing, auditing, and reporting. The accounting feature tracks and maintains a log of every management session used for access. You can use this information to generate reports for troubleshooting and auditing purposes.

Some of the high-level benefits of using a remote AAA server over local AAA services on each network device individually are highlighted next:

- Increased flexibility and control of access configuration
- Scalability
- Standardized authentication methods using RADIUS and TACACS+
- Ease of setup, since RADIUS and TACACS+ may have already been deployed across the enterprise
- More efficiency, since you can create user attributes once centrally and use them across multiple devices

Next, let's touch on the high points of TACACS+ and RADIUS before looking at their configuration.

TACACS+ Overview

TACACS+ implementation provides for separate and modular authentication, authorization, and accounting facilities. It allows for a single access control server (referred to as the TACACS+ daemon) to provide authentication, authorization, and accounting to the network access server (NAS) independently. Typically, a client of a TACACS+ server is referred to as a NAS. A NAS may be a router, a switch, or an access point.

The TACACS+ protocol uses TCP port 49 for communication between the TACACS+ client (network device) and the TACACS+ server. A network administrator typically uses a workstation using Telnet, SSH, or the console to connect to a Cisco IOS device that needs to be managed. In this process, the TACACS+ client communicates with the TACACS+ server using the TACACS+ protocol. The TACACS+ protocol ensures confidentiality because all protocol exchanges between a TACACS+ client and a TACACS+ server are encrypted.

RADIUS Overview

The Cisco implementation of RADIUS provides for a RADIUS client that runs on a Cisco IOS device to send an authentication request to a central RADIUS server that contains all user authentication and network service access information. RADIUS can be used with other AAA security protocols, such as local username lookup and TACACS+.

There are two implementations of RADIUS: Cisco's implementation and the industry-standard implementation. Cisco's implementation uses UDP port

1645 for authentication and authorization and UDP port 1646 for accounting. The industry-standard implementation uses UDP port 1812 for authentication and authorization and UDP port 1813 for accounting. The industry-standard implementation of the RADIUS protocol provides the distinction of working in a multi-vendor environment. Network devices from different vendors can connect to the same RADIUS server for AAA services. RADIUS can also be more convenient for AAA than TACACS+ since some organizations may already have it deployed.

As it relates to the privilege levels examined earlier in the chapter, TACACS+ and RADIUS can also be implemented when using AAA. For example, TACACS+ provides two ways to control the authorization of the network device commands on a per-user or per-group basis. One way is to assign privilege levels to commands and have the router verify with the TACACS+ server whether the user is authorized at the specified privilege level. Another way is to explicitly specify in the TACACS+ server, on a per-user or per-group basis, the allowed commands.

Cisco's TACACS+ and RADIUS implementations used to occur through the implementation of Cisco Secure Access Control Server (ACS), where RADIUS was used for network access control and TACACS+ was used for network devices access control. However, Cisco Identity Services Engine (ISE) is now the preferred implementation for AAA servers to support both TACACS+ and RADIUS protocols.

AAA Configuration for Network Devices

In this section, you will see how both TACACS+ and RADIUS are configured from a Cisco IOS device. This section does not cover the configuration of a TACACS+ or RADIUS server because that is beyond the scope of this chapter.

There are two parts to configuring TACACS+ support: a TACACS+ server (for example, Cisco ISE) and a Cisco IOS device. At a high level, to configure a Cisco IOS device to support TACACS+, the following steps are involved:

1. Create a local user that will serve as the fallback if the TACACS+ server is not available or if you accidentally lock yourself out after enabling the AAA command. As highlighted previously, this is done with the command **username** *username* **privilege 15 algorithm-type {md5 | sha256 | scrypt} secret** *password*.
2. Enable the AAA function with the **aaa new-model** global configuration command.

3. Add a TACACS+ server.
4. Define the method lists for TACACS+ authentication by using the **aaa authentication** global configuration command.
5. Use the **line** and **interface** commands to apply the defined method lists to various interfaces.
6. If needed, use the **aaa authorization** global command to configure authorization for the device. Unlike with authentication, which can be configured per line or per interface, authorization is configured globally for an entire device.
7. If needed, use the **aaa accounting** command to enable accounting for TACACS+ connections.

Example 6.10 shows how to configure an IOS device with TACACS+ for device access control based on these steps. This example demonstrates basic authentication, authorization, and accounting configuration. Once the command **aaa-new model** is configured, there is no line authentication anymore on the vty lines as the default login method becomes AAA. The console port defaults to no authentication. If you were to disable this with the **no aaa new-model** command afterward, the login method would switch back to line authentication. However, you would not see **login local** under vty line; you would see just **login** (meaning just the line password will be checked, and not the local user database that is configured locally on the router).

EXAMPLE 6.10 **Configuring TACACS+**

```
R1#
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
!Authentication setup
!First we create a fallback user account
R1(config)# username fallback privilege 15 algorithm-type scrypt
secret Cisco123
R1(config)# aaa new-model
R1(config)# tacacs server TACACSSERVER1
R1(config-server-tacacs)# address ipv4 100.1.1.2
R1(config-server-tacacs)# key Cisco123
R1(config-server-tacacs)# exit
R1(config)# aaa group server tacacs+ TACACSGROUP1
R1(config-sg-tacacs+)# server name TACACSSERVER1
R1(config)# aaa authentication login default group TACACSGROUP1 local
!the default method list automatically applies to all lines, except
the ones that have a named method list explicitly define or in other
words, it gets applied unless a more specific named method list is
defined.
```

```
!we can also specify on the vty lines the login authentication METH-
ODLIST1 command then tacacs+ TACACSGROUP1 will be used as the primary
authentication method and the local user database is set as the backup
R1(config)# line vty 0 4
R1(config-line)# login authentication methodlist1
!Authorization setup
!Next, for authorization we create a method list TACACSAUTH1
!if-authentication option allows a user who is authenticated to be
placed in EXEC mode
R1(config)# aaa authorization exec TACACSAUTH1 group TACACSGROUP1
local if-authenticated
R1(config)# aaa authorization commands 15 TACACSAUTH1 group TACACS-
GROUP1 local
!The config-commands command indicates that the server must return
permission to use any router configuration command
R1(config)# aaa authorization config-commands
R1(config)# aaa authorization console
!The TACACSAUTH1 method list is applied to the vty lines for both EXEC
and level 15 command access
R1(config)# line vty 0 4
R1(config-line)# authorization exec TACACSAUTH1
R1(config-line)# authorization commands 15 TACACSAUTH1
R1(config-line)# exit
R1(config)#
!Accounting setup
 !Next, for accounting we create a method list TACACSACC1
 !User EXEC sessions will be recorded as they start and stop, along
with user information
R1(config)# aaa accounting exec TACACSACC1 start-stop group
TACACSGROUP1
!commands that are entered while a user is in privilege level 15
(enable mode) will be recorded
R1(config)# aaa accounting commands 15 TACACSACC1 start-stop group
TACSRVGROUP1
!The TACACSACC1 method list is applied to the vty lines for EXEC and
level 15 commands
R1(config)# line vty 0 4
R1(config-line)# accounting exec TACACSACC1
R1(config-line)# accounting commands 15 TACACSACC1
R1(config-line)# end
R1#
```

The AAA server also needs to be configured with the AAA client information (that is, the hostname, IP address, and key), the login credentials for the users, and the commands the users are authorized to execute on the device.

At a high level, to configure a Cisco IOS device to support RADIUS, the following steps are involved:

1. Enable AAA with the **aaa new-model** global configuration command.
2. Define the RADIUS server and specify the IP address and key.
3. Add the RADIUS server to a server group.
4. Define method lists for RADIUS authentication by using the **aaa authentication login** *method-list* global configuration command.
5. Create a named method list and add a RADIUS server group as the primary and local database as backup by using the **aaa authentication login** command.
6. Use the **line** and **interface** commands to enable the defined method lists to be used. For example, Example 6.11 specifies the **login authentication** *method-list* command on the vty lines, and then the RADIUS server group will be used as the primary authentication method, and the local user database is set as the backup.

Example 6.11 shows the configuration of an IOS device with RADIUS for device access control based on these steps (which are nearly identical to the steps for TACACS+ configuration). This example demonstrates basic authentication configuration.

EXAMPLE 6.11 **Configuring RADIUS**

```
R1#
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# aaa new-model
R1(config)# radius server RADIUSSERVER1
R1(config-radius-server)# address ipv4 100.1.1.2
R1(config-radius-server)# key Cisco123
R1(config-radius-server)# exit
R1(config)# aaa group server radius RADIUSGROUP1
R1(config-sg-radius)# server name RADIUSSERVER1
R1(config-sg-radius)# exit
R1(config)# aaa authentication login METHODLIST2 group RADIUSGROUP1
local
!the default method list automatically applies to all lines, except
the ones that have a named method list explicitly define or in other
words, it gets applied unless a more specific named method list is
defined.
!we can also specify on the vty lines the login authentication METHOD-
LIST2 command then RADIUSGROUP1 will be used as the primary authenti-
cation method and the local user database is set as the backup
```

```
R1(config-line)# line vty 0 4
R1(config-line)# login authentication METHODLIST2
R1(config-line)# end
R1#
```

CramQuiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Which of the following is not one of the benefits of AAA?
   - ❍ **A.** Increased flexibility and control of access configuration
   - ❍ **B.** Scalability
   - ❍ **C.** Standardized authentication methods using RADIUS and TACACS+
   - ❍ **D.** Complete removal of the need for local user creation on IOS devices

2. In the industry-standard implementation of the RADIUS protocol, which port is used for accounting?
   - ❍ **A.** UDP port 1645
   - ❍ **B.** UDP port 1646
   - ❍ **C.** UDP port 1812
   - ❍ **D.** UDP port 1813

3. Which command is entered to enable AAA on a Cisco IOS device?
   - ❍ **A. aaa authentication**
   - ❍ **B. aaa authorization**
   - ❍ **C. aaa new-model**
   - ❍ **D. aaa accounting**

Answers

1. **D** is correct. As a fallback mechanism, it is recommended that you use local authentication in case the AAA server becomes unavailable at some point.
2. **D** is correct. The industry-standard implementation of RADIUS uses UDP port 1813 for accounting.
3. **C** is correct. When configuring both TACACS+ and RADIUS, you enable AAA functionality by using the **aaa new-model** global configuration command.

Review Questions

1. In implementing the TACACS+ protocol, which port is used for communication between a network device and a TACACS+ server?
   - ❍ **A.** UDP port 1645
   - ❍ **B.** TCP port 49
   - ❍ **C.** TCP port 389
   - ❍ **D.** UDP port 1813

2. In TACACS+ implementation, which of the following can serve as network access servers?
   - ❍ **A.** Routers
   - ❍ **B.** Switches
   - ❍ **C.** Access points
   - ❍ **D.** All of the above

3. Which of the following commands is used for configuring a vty line to use the method list name **list1**?
   - ❍ **A. aaa authentication**
   - ❍ **B. aaa authorization**
   - ❍ **C. login authentication list1**
   - ❍ **D. aaa new-model**

4. To add a TACACS+ server in IOS 15.x, what command follows **tacacs server** *name* if the IP address is 10.10.10.10?
   - ❍ **A. aaa tacacs 10.10.10.10**
   - ❍ **B. server 10.10.10.10**
   - ❍ **C. address ipv4 10.10.10.10**
   - ❍ **D. aaa server 10.10.10.10**

Answers to Review Questions

1. **B** is correct. The TACACS+ protocol uses TCP port 49 for communication between a TACACS+ client (network device) and a TACACS+ server.
2. **D** is correct. The clients of a TACACS+ server is referred to as a network access server (NAS). A NAS may be a router, a switch, or an access point.
3. **C** is correct. A method list enables logic authentication. To apply a custom list to a line, you use **login authentication** *custom-list name* in line configuration mode.

4. **C** is correct. To add a TACACS+ server in IOS 15.x, you need to specify the TACACS+ server name, specify the server IP address with the **address ipv4** *ip address* command (**address ipv4 10.10.10.10** in this case), and then specify the key string.

Further Reading

- *CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide*

What's Next?

If you want more practice on this chapter's exam objectives before you move on, remember that you can access all of the CramQuiz questions on the book's web page. The next chapter covers infrastructure security.

Index

Symbols

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z