CCST

Cisco® Certified Support Technician

STUDY GUIDE

CYBERSECURITY EXAM

Includes one year of FREE access after activation to the interactive online learning environment and study tools:

Custom practice exam

100 electronic flashcards

Searchable key term glossary

TODD LAMMLE
JON BUHAGIAR
DONALD ROBB
TODD MONTGOMERY

SYBEX®
A Wiley Brand

CCST

Cisco® Certified Support Technician

Study Guide

Cybersecurity Exam

Todd Lammle
Jon Buhagiar
Donald Robb
Todd Montgomery

SYBEX®
A Wiley Brand

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

The manufacturer's authorized representative according to the EU General Product Safety Regulation is Wiley-VCH GmbH, Boschstr. 12, 69469 Weinheim, Germany, e-mail: Product_Safety@wiley.com.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002. For product technical support, you can find answers to frequently asked questions or reach us via live chat at https://sybexsupport.wiley.com.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Control Number applied for:

Paperback ISBN: 9781394207350
ePDF ISBN: 9781394207374
ePub ISBN: 9781394207367

Cover Image: © Jeremy Woodhouse/Getty Images
Cover Design: Wiley

Contents at a Glance

Contents

Acknowledgments

There were many people who helped us build the new Cisco certification books in 2023 and 2024. First, Kenyon Brown helped us put together the direction for the books and managed the internal editing at Wiley, so thank you, Ken. Kim Wimpsett was the development editor and worked diligently for many months keeping these books moving along.

We also thank content refinement specialist Sowmini Durairaj, the copyeditor Lori Martinsek, the proofreader Tiffany Taylor, and the indexer Tom Dinse.

About the Authors

Todd Lammle is the authority on Cisco certification and internetworking and is Cisco certified in most Cisco certification categories. He is a world-renowned author, speaker, trainer, and consultant. Todd has three decades of experience working with LANs, WANs, and large enterprise licensed and unlicensed wireless networks, and lately he's been implementing large Cisco Security networks using Firepower/FTD and ISE.

His years of real-world experience are evident in his writing; he is not just an author but an experienced networking engineer with very practical experience from working on the largest networks in the world, at such companies as Xerox, Hughes Aircraft, Texaco, AAA, Cisco, and Toshiba, among many others.

Todd has published over 130 books, including the very popular *CCNA: Cisco Certified Network Associate Study Guide, CCNA Wireless Study Guide, CCNA Data Center Study Guide, and CCNP Security*—among over a hundred more—all from Sybex. He runs an international consulting and training company based in northern Idaho where he spends his free time in the mountains playing with his golden retrievers.

You can reach Todd through his website at `www.lammle.com`.

Jon Buhagiar, BS/ITM, MCSE, CCNA, is an information technology professional with two decades of experience in higher education and the private sector.

Jon currently serves as supervisor of network operations and is currently the director of information technology at RareMed Solutions, Pittsburgh Technical College. In this his role, he manages projects related to the IT infrastructure and cloud services that serve multiple pharmacies operated by RareMed Solutions. In addition, he is responsible for the technology that support hundreds of care specialists that raise the quality of life for many patients all over the world.

He was previously the supervisor of network operations at Pittsburgh Technical College, where he managed the data center, network infrastructure operations, and IT operations and was involved in the management of projects supporting the quality of education at the College. He also served as an adjunct instructor in the College's School of Information Technology department, where he has taught courses for Microsoft and Cisco certification. Jon has been an instructor for 20+ years at several colleges in the Pittsburgh area, since the introduction of the Windows NT MCSE in 1998.

Jon earned a bachelor of science degree in information technology management from Western Governors University. He also achieved an associate degree in business management from Pittsburgh Technical College. His most recent certifications include Windows Server 2016 Microsoft Certified Solutions Expert (MCSE) and Cisco Certified Network Associate (CCNA). Other certifications include CompTIA Network+, CompTIA A+, and CompTIA Project+.

In addition to his professional and teaching roles, Jon has authored many books with Wiley Sybex over the past 10 years, including the Second Edition CCNA Certification Practice Tests 200-301 (Sybex 2023) Comp-TIA Network+ Study Guide: Exam N10-009 (Sybex Study Guide), along with Todd Lammle (Sybex 2024). Jon has spoken at several

conferences about spam and email systems. He is an active radio electronics hobbyist and has held a ham radio license for the past 20 years, KB3KGS. He experiments with electronics and has a strong focus on the Internet of Things (IoT).

Donald Robb, widely recognized online as "The Packet Thrower," brings over two decades of experience in the IT industry. His career has spanned a diverse array of roles, beginning with help desk support and evolving into a position as one of the most respected consultants in the field. Donald has honed expert-level skills across various IT domains, including networking, security, collaboration, data center management, wireless technologies, and service providers. His depth of knowledge and technical expertise have made him a sought-after professional in the industry.

Currently, Donald is a principal network architect for Walt Disney Studios. In this role, he serves as a subject matter expert on various technologies, playing a critical role in shaping the company's network architecture and ensuring its reliability and performance. His work involves leading the design and implementation of complex networks and guiding teams and stakeholders through the technical intricacies of modern IT infrastructures.

Over the years, Donald has collaborated with major industry vendors and smaller, specialized companies, earning many advanced certifications along the way. His achievements include becoming a double JNCIE and obtaining most of Cisco's professional-level certifications, demonstrating his deep technical proficiency and commitment to continuous learning. His expertise has also been recognized through his selection as a Cisco Champion for four consecutive years, an honor awarded to top influencers in the networking community.

In addition to his hands-on work in the field, Donald has made significant contributions to IT education. He has had the privilege of working alongside Todd Lammle, a legendary figure in the IT world, coauthoring several books and developing courses that have helped countless professionals advance their careers. Through his extensive experience, certifications, and educational efforts, Donald Robb has solidified his reputation as a leading authority in the IT industry.

Todd Montgomery has been in the networking industry for more than 40 years. Todd holds many Cisco, AWS, CompTIA, and Juniper certifications. Todd has spent most of his career in the field working on-site in data centers throughout North America and around the world.

He has worked on the most advanced networks of equipment manufacturers, systems integrators, and end users in the data center and cloud computing environments of the private sector, service providers, and the government sector. Todd most recently worked as a data center network automation engineer in Austin, Texas, involved in network implementation and support of emerging data center technologies and AWS public cloud services.

Introduction

Welcome to the exciting world of security and your path toward Cisco certification. If you've picked up this book because you want to improve yourself and your life with a better, more satisfying, and secure job, you've chosen well!

Whether you're striving to enter the thriving, dynamic security sector or seeking to enhance your skill set and advance your position within it, being Cisco certified can seriously stack the odds in your favor to help you attain your goals. This book is a great start.

Cisco certifications are powerful instruments of success that also markedly improve your grasp of all things internetworking. As you progress through this book, you'll gain a strong, foundational understanding of security that reaches far beyond Cisco devices. And when you finish this book, you'll be ready to tackle the next step toward Cisco certification.

Essentially, by beginning your journey toward becoming Cisco certified, you're proudly announcing that you want to become an unrivaled security expert, a goal that this book will help get you underway to achieving.

Congratulations in advance for taking the first step toward your brilliant future!

To find your included bonus material, as well as additional Todd Lammle videos, and extra practice questions, please see `www.lammle.com/ccst`.

Cisco's CCST Certifications

It used to be that to secure the holy grail of Cisco certifications—the CCIE—you passed only one written test before being faced with a grueling, formidable hands-on lab. This intensely daunting, all-or-nothing approach made it nearly impossible to succeed and predictably didn't work out too well for most people.

Cisco responded to this issue by creating a series of new certifications, which not only created a sensible, stepping-stone-path to the highly coveted CCIE prize, but it also gave employers a way to accurately rate and measure the skill levels of prospective and current employees.

The CCNA and CCNP exams were then created as a stepping stone, and they are still the most popular certifications in the world. This exciting paradigm shift in Cisco's certification path truly opened doors that few were allowed through before!

Now Cisco has reached down and created a new introduction level certification program, below the CCNA, called the Cisco Certified Support Technician (CCST). There are two exams, two certs, called Network and Cybersecurity.

CCST Networking certification validates an individual's skills and knowledge of entry-level networking concepts and topics. The certification demonstrates foundational

knowledge and skills needed to show how networks operate, including the devices, media, and protocols that enable network communications.

The Cisco Certified Support Technician (CCST) Networking certification is also a first step toward working on achieving your CCNA Certification.

The Cisco Certified Support Technician (CCST) Cybersecurity certification validates a candidate's skills and knowledge of entry-level cybersecurity concepts and topics, including security principles, network security and endpoint security concepts, vulnerability assessment and risk management, and incident handling.

The Cisco Certified Support Technician (CCST) Cybersecurity certification is also a first step toward CyberOps Associate certification.

This book is a powerful tool to get you started in your Cisco certification studies, and it's vital to understand that material in it before you go on to conquer any other certifications!

Exam policies can change from time to time. We highly recommend that you check both the Cisco and Pearson VUE sites for the most up-to-date information when you begin your preparation, when you register, and again a few days before your scheduled exam date.

Tips for Taking the CCST Cybersecurity Exam

Here are some general tips for taking your exam successfully (assuming you are going in person as online testing is available as well):

- This is not like the CCNA or other Cisco certification tests that are available on `www.vue.com`. You need to instead go to `https://www.certiport.com/locator` to both register and pay for your exam. You can take the exams in person at a center, or in your home or office, under direct video and audio supervision. For exams at home information and to sign up, call (800) 589-6871.
- Bring two forms of ID with you. One must be a photo ID, such as a driver's license. The other can be a major credit card or a passport. Both forms must include a signature.
- Arrive early at the exam center so you can relax and review your study materials, particularly tables and lists of exam-related information. After you are ready to enter the testing room, you will need to leave everything outside; you won't be able to bring any materials into the testing area.
- Read the questions carefully. Don't be tempted to jump to an early conclusion. Make sure you know exactly what each question is asking.
- Don't leave any unanswered questions. Unanswered questions are scored against you. There will be questions with multiple correct responses. When there is more than one correct answer, a message at the bottom of the screen will prompt you to either "choose two" or "choose all that apply." Be sure to read the messages displayed to know how many correct answers you must choose.

- When answering multiple-choice questions you're not sure about, use a process of elimination to get rid of the obviously incorrect answers first. Doing so will improve your odds if you need to make an educated guess.

Who Should Read This Book?

You—if want to pass the CCST Cybersecurity exam and pass it confidently! This book is chock-full of the exact information you need and directly maps to CCST Cybersecurity exam objectives, so if you use it to study for the exam, your odds of passing shoot way up.

And in addition to including every bit of knowledge you need to learn to pass the exam, We have included some really great tips and solid wisdom throughout the chapters, to equip you even further to successfully work in the real IT security world.

What's Included in the Book

We have included several study tools throughout the book:

Assessment Test At the end of this introduction is an assessment test that you can use to check your readiness for the exam. Take this test before you start reading the book; it will help you determine the areas you might need to brush up on. The answers to the assessment test questions appear on a separate page after the last question of the test. Each answer includes an explanation and a note telling you the chapter in which the material appears.

Objective Map and Opening List of Objectives In this introduction you'll find a detailed exam objective map showing you where each of the exam objectives is covered in this book. In addition, each chapter opens with a list of the exam objectives it covers. Use these to see exactly where each of the exam topics is covered.

Exam Essentials Each chapter, just after the summary, includes a number of exam essentials. These are the key topics you should take from the chapter in terms of areas to focus on when preparing for the exam.

Chapter Review Questions To test your knowledge as you progress through the book, there are review questions at the end of each chapter. As you finish each chapter, answer the review questions, and then check your answers—the correct answers and explanations are in the Appendix. You can go back to reread the section that deals with each question you got wrong to ensure that you correctly answer the next time you're tested on the material.

Interactive Online Learning Environment and Test Bank

The interactive online learning environment that accompanies CCST Cybersecurity provides a test bank with study tools to help you prepare for the certification exam—and increase your chances of passing it the first time! The test bank includes the following tools:

Sample Tests All of the questions in this book are provided, including the assessment test, which you'll find at the end of this introduction, and the chapter tests that include the review questions at the end of each chapter. In addition, there is a practice exam. Use these questions to test your knowledge of the study guide material. The online test bank runs on multiple devices.

Flashcards Approximately 100 questions are provided in digital flashcard format (a question followed by a single correct answer). You can use the flashcards to reinforce your learning and provide last-minute test prep before the exam.

Other Study Tools A glossary of key terms from this book and their definitions are available as a fully searchable PDF.

Go to `http://www.wiley.com/go/sybextestprep` to register and gain access to this interactive online learning environment and test bank with study tools.

How to Use This Book

If you want a solid foundation for the serious effort of preparing for the Cisco CCST Cybersecurity exam, then look no further because we have spent countless hours putting together this book with the sole intention of helping you pass it!

This book is loaded with valuable information, and you will get the most out of your study time if you understand how I put the book together. Here's a list that describes how to approach studying:

1. Take the assessment test immediately following this introduction. (The answers are at the end of the test, but no peeking!) It's okay if you don't know any of the answers—that's what this book is for. Carefully read over the explanations for any question you get wrong and make note of the chapters where that material is covered.
2. Study each chapter carefully, making sure you fully understand the information and the exam objectives listed at the beginning of each one. Again, pay extra-close attention to any chapter that includes material covered in questions you missed on the assessment test.
3. Answer all the review questions related to each chapter. Specifically note any questions that confuse you and study the corresponding sections of the book again. And don't just skim these questions—make sure you understand each answer completely.
4. Before you take your test, be sure to visit my website for questions, videos, audios, and other useful information.
5. Test yourself using all the electronic flashcards. This is a brand-new and updated flashcard program to help you prepare for the latest Cisco CCST Cybersecurity exam, and it is a great study tool.

I tell you no lies—learning every bit of the material in this book is going to require applying yourself with a good measure of discipline. So try to set aside the same time period every day to study, and select a comfortable and quiet place to do so. If you work hard, you will be surprised at how quickly you learn this material.

What Does This Book Cover?

This book covers everything you need to know to solidly prepare you for getting into your CCST studies. Be advised that just because much of the material in this book won't be official Cisco CCST objectives in the future doesn't mean you won't be tested on it. Understanding the foundational, real-world cybersecurity information and skills offered in this book is critical to your certifications and your career!

So, as you move through this book, here's a snapshot of what you'll learn chapter by chapter:

Chapter 1**: Security Concepts** In this chapter you will begin learning basic security concepts. The security concepts include vulnerabilities, threats, exploits, as well as the difference between these concepts. You will then learn about common threats and vulnerabilities, such as malware, ransomware, and other common tactics.

Chapter 2**: Network Security Devices** This chapter will describe network infrastructure and technologies that support network security, such as virtualization, honeypots, intrusion detection systems (IDS), and many other devices.

Chapter 3**: Network Security Concepts** Chapter 3 will cover a lot of common network concepts that you would find in the CCST Networking certification. However, the concepts will be explained and highlighted as they pertain to network security.

Chapter 4**: Network Device Access** This chapter will explain the difference between authentication, authorization, and accounting (AAA) that is used with Remote Authentication Dial-In User Service (RADIUS), as well as multifactor authentication (MFA), and password policies.

Chapter 5**: Secure Access Technology** This chapter will cover the various technologies that allow you to secure communications over an insecure network, such as access control lists (ACLs), firewalls, Virtual Private Network (VPN) connections, and Network Access Control (NAC). Encryption types and the protocols that use them will also be covered.

Chapter 6**: OS Basics and Security** This chapter will focus on the various operating systems and their various security features, such as Windows Defender, host-based firewalls, and file and directory permissions. In addition this chapter will cover the importance of software and hardware updates. To round this topic of operating system security, system logs will be covered in entirety.

Chapter 7**: Endpoint Security** This Chapter will take a deep dive into endpoint security, such as the various built-in tools that can help us collect data. This chapter will also cover the basics of hardware and software inventory, program deployments, data backups, regulatory compliance, and bring your own device (BYOD) strategies.
Chapter 8**: Vulnerability Management** Chapter 8 will focus on risk management strategies, such as risk ranking, approaching risk management, risk mitigations strategies, risk associated with data types, and the levels of risk. In addition, this chapter will give you a fundamental understanding of how to identify risk and mitigate risk.
Chapter 9**: Vulnerability Management** This chapter explains the various ways that you can manage vulnerabilities in your organization, such as identification, management, and mitigation. Threat intelligence techniques are also covered that explain how the industry catalogs vulnerabilities, identifies trends, and mitigates vulnerabilities.
Chapter 10**: Disaster Recovery** This chapter explains disaster recovery for business continuity and recovery. The chapter will cover how disasters might happen, what to do when it happens and the planning around disasters to get your organization operating again.
Chapter 11**: Incident Handling** This chapter explains how security events are found with the help of Security Information and Event Management (SIEM) systems. The chapter will also explain the importance of security orchestration, automation, and response (SOAR) systems to help automate and orchestrate a remediation to an event. Common compliance frameworks for incident handling are also explained along with their reporting and notification requirements.
Chapter 12**: Digital Forensics** This chapter will explain digital forensics and the attack attribution processes. Some of the concepts covered will be Cyber Kill Chain, MITRE ATT&CK Matrix, and tactics, techniques, procedures (TTPS), as well as evidence and the proper handling of evidence.
Chapter 13**: Incident Response** The last chapter will describe the elements of a cybersecurity incidence response. This chapter will include the National Institute of Standards and Technology (NIST) standard for incident response, and how to implement a policy, plan, and the various procedural elements.

Exam Objectives

Speaking of objectives, you're probably pretty curious about those, right? Cisco asked groups of IT professionals to fill out a survey rating the skills they felt were important in their jobs, and the results were grouped into objectives for the exam.

This is a list of objectives and which chapter the objectives are covered in. Remember that a single objective can be covered in multiple chapters.