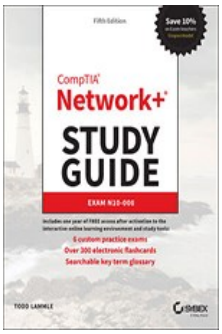


# CompTIA Network+ Study Guide: Exam N10-008, 5th Edition

by Todd Lammle



---

# Introduction

## Overview

If you're like most of us in the networking community, you probably have one or more network certifications. If that's you, you're very wise in choosing a CompTIA Network+ (N10-008) certification to proudly add to your repertoire because this achievement will make you all the more valuable as an employee.

In these challenging economic times, keeping ahead of the competition—even standing out among your present colleagues—could make a big difference in whether you gain a promotion or possibly keep your job instead of being the one who gets laid off! Or maybe this is your first attempt at certification because you've decided to venture into a new career in information technology (IT). You've realized that getting into the IT sector is a good way to go because as the information age marches on, the demand for knowledgeable professionals in this dynamic field will only intensify dramatically.

Either way, certification is one of the best things you can do for your career if you are working in, or want to break into, the networking profession because it proves that you know what you're talking about regarding the subjects in which you're certified. It also powerfully endorses you as a professional in a way that's very similar to a physician being board-certified in a certain area of expertise.

In this book, you'll find out what the Network+ exam is all about because each chapter covers a part of the exam. I've included some great review questions at the end of each chapter to help crystallize the information you learned and solidly prepare you to ace the exam.

A really cool thing about working in IT is that it's constantly evolving, so there are always new things to learn and fresh challenges to master. Once you obtain your Network+ certification and discover that you're interested in taking it further by getting into more complex networking (and making more money), the Cisco CCNA certification is definitely your next step; you can get the skinny on that and even more in-depth certifications on my blog at `www.lammle.com`.

Note For Network+ training with Todd Lammle, both instructor-led and online, please see `www.lammle.com`.

## What is the Network+ Certification?

Network+ is a certification developed by the Computing Technology Industry Association (CompTIA) that exists to provide resources and education for the computer and technology community. This is the same body that developed the A+ exam for PC technicians.

The Network+ exam was designed to test the skills of network technicians with 18 to 24 months of experience in the field. It tests areas of networking technologies such as the definition of a protocol, the Open Systems Interconnection (OSI) model and its layers, and the concepts of network design and implementation—the minimum knowledge required for working on a network and some integral prerequisites for network design and implementation.

## Why Become Network+ Certified?

Because CompTIA is a well-respected developer of vendor-neutral industry certifications, becoming Network+ certified proves you're competent in the specific areas covered by the Network+ objectives.

Four major benefits are associated with becoming Network+ certified:

- **Proof of Professional Achievement** Networking professionals are pretty competitive when it comes to collecting more certifications than their peers. And because the Network+ certification broadly covers the entire field of networking, technicians want this certification a lot more than they want just Microsoft certifications—Network+ is a lot more prestigious and valuable. Because it's rare to gain something that's worth a lot with little effort, I'll be honest—preparing for the Network+ exam isn't exactly a lazy day at the beach. (However, beaches do happen to be really high on my personal list of great places to study!) And people in IT know that it isn't all that easy to pass the Network+ exam, so they'll definitely respect you more and know that you've achieved a certain level of expertise about vendor-independent, networking-related subjects.
- **Opportunity for Advancement** We all like to get ahead in our careers—advancement results in more responsibility and prestige, and it usually means a fatter paycheck, greater opportunities, and additional options. In the IT sector, a great way to make sure all that good stuff happens is by earning a lot of technology certifications, including Network+.

- **Fulfillment of Training Requirements** Network+, because of its wide-reaching industry support, is recognized as a baseline of networking information. Some companies actually specify the possession of a Network+ certification as a job requirement before they'll even consider hiring you, or it may be specified as a goal to be met before your next review.
- **Customer Confidence** As companies discover the CompTIA advantage, they will undoubtedly require qualified staff to achieve these certifications. Many companies outsource their work to consulting firms with experience working with security. Firms that have certified staff have a definite advantage over firms that don't.

## How to Become Network+ Certified

As this book goes to press, Pearson VUE is the sole Network+ exam provider. The following is the necessary contact information and exam-specific details for registering. Exam pricing might vary by country or by CompTIA membership.

| Vendor | Website | Phone Number |
|---|---|---|
| Pearson VUE | `https://www.pearsonvue.com/comptia` | US and Canada: 877-551-PLUS (7587) |

When you schedule the exam, you'll receive instructions regarding appointment and cancellation procedures, ID requirements, and information about the testing center location. In addition, you'll receive a registration and payment confirmation letter. Exams can be scheduled up to six weeks out or as soon as the next day (or, in some cases, even the same day).

Note Exam prices and codes may vary based on the country in which the exam is administered. For detailed pricing and exam registration procedures, refer to CompTIA's website at `www.comptia.org`.

After you've successfully passed your Network+ exam, CompTIA will award you a certification. Within four to six weeks of passing the exam, you'll receive your official CompTIA Network+ certificate and ID card. (If you don't receive these within eight weeks of taking the test, contact CompTIA directly using the information found in your registration packet.)

## Tips for Taking the Network+ Exam

Here are some general tips for taking your exam successfully:

- 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.
- On form-based tests (nonadaptive), because the hard questions will take the most time, save them for last. You can move forward and backward through the exam.

## Who Should Read This Book?

You—if want to pass the Network+ exam, and pass it confidently! This book is chock-full of the exact information you need and directly maps to Network+ 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, I've included some really great tips and solid wisdom to equip you even further to successfully work in the real IT world.

## What Does This Book Cover?

This book covers everything you need to know to pass the CompTIA Network+ exam. But in addition to studying the book, it's a

good idea to practice on an actual network if you can.

Here's a list of the 25 chapters in this book:

- **Chapter 1, "Introduction to Networks"** This chapter includes an introduction to networks and an overview of the most common physical network topologies you'll find in today's networks.
- **Chapter 2, "The Open Systems Interconnection Specifications"** This chapter covers the OSI model, what it is, what happens at each of its layers, and how each layer works.
- **Chapter 3, "Networking Connectors and Wiring Standards"** This chapter covers the various networking media and topologies, plus the cable types and properties used in today's networks.
- **Chapter 4, "The Current Ethernet Specifications"** This chapter covers how a basic Ethernet LAN works and describes and categorizes the different Ethernet specifications.
- **Chapter 5, "Networking Devices"** It's important for you to understand all the various devices used in today's networks, and this chapter will describe how hubs, routers, switches, and some other devices work within a network.
- **Chapter 6, "Introduction to the Internet Protocol"** This is your introduction to the all-important IP protocol stack.
- **Chapter 7, "IP Addressing"** This chapter will take up from where Chapter 6 left off and move into IP addressing. It also contains information about public versus private addressing and DHCP.
- **Chapter 8, "IP Subnetting, Troubleshooting IP, and Introduction to NAT"** This chapter will continue the subject from Chapter 7 and also will tackle IP subnetting. But no worries here—I've worked hard to make this not-so-popular-yet-vital topic as painless as possible.
- **Chapter 9, "Introduction to IP Routing"** This is an introduction to routing that basically covers what routers do and how they do it. Along with Chapter 10 and Chapter 11, this chapter covers routing and switching in much more detail than what is necessary to meet the CompTIA Network+ objectives because this knowledge is so critical to grasp when working with today's networks.
- **Chapter 10, "Routing Protocols"** This chapter goes into detail describing the protocols that run on routers and that update routing tables to create a working map of the network.
- **Chapter 11, "Switching and Virtual LANs"** This chapter covers layer 2 switching, the Spanning Tree Protocol (STP), and virtual LANs. I went deeper than needed for the exam with the routing chapters, and in this chapter I'll cover switching and virtual LANs (which are also vital in today's corporate networks) more thoroughly as well.
- **Chapter 12, "Wireless Networking"** Because wireless is so important for both home and business networks today, this chapter is loaded with all the information you need to be successful at wireless networking at home and work.
- **Chapter 13, "Using Statistics and Sensors to Ensure Network Availability"** In this chapter you'll learn what sort of data you should be monitoring and some of the ways to do so.
- **Chapter 14, "Organizational Documents and Policies"** In this chapter you'll learn that plans and procedures should be developed to manage operational issues such as change management, incident response, disaster recovery, business continuity, and the system life cycle. You'll also learn the standard operating procedures that should be developed to guide each of these processes.
- **Chapter 15, "High Availability and Disaster Recovery"** In this chapter you will learn about redundancy concepts, fault tolerance, and the process of disaster recovery.
- **Chapter 16, "Common Security Concepts"** In this chapter you will learn the basic concepts, terms, and principles that all network professionals should understand to secure an enterprise network.
- **Chapter 17, "Common Types of Attacks"** In this chapter you will learn the common types of attacks that all network professionals should understand to secure an enterprise network.
- **Chapter 18, "Network Hardening Techniques"** In this chapter you'll learn best practices for hardening devices and for hardening the network environment in which these devices reside. At the end of the chapter, you'll learn about the newest challenge to secure, the Internet of Things (IoT).

- **Chapter 19, "Remote Access Security"** In this chapter you'll learn the importance of providing both fault tolerance and high availability. You'll also learn about VPN architectures. These include site-to-site VPNs, client-to-site VPNs, clientless VPNs, split tunnel vs. full VPN, and SSH VPNs.
- **Chapter 20, "Physical Security"** In this chapter you will learn the basic concepts, terms, and principles that all network professionals should understand to physically secure a network.
- **Chapter 21, "Data Center Architecture and Cloud Concepts"** In this chapter, I'll talk a lot about the documentation aspects of network administration. The chapter will start off discussing physical diagrams and schematics and move on to the logical form as well as configuration-management documentation. You'll learn about the importance of these diagrams as well as the simple to complex forms they can take and the tools used to create them—from pencil and paper to high-tech AutoCAD schematics. You'll also find out a great deal about creating performance baselines.
- **Chapter 22, "Ensuring Network Availability"** In this chapter you'll learn about network availability and some of the ways to achieve a stable network. I'll talk about how environmental parameters, CPU load, and memory utilization can cause low-performance problems.
- **Chapter 23, "Cable Connectivity Issues and Tools"** Specialized tasks require specialized tools, and installing network components is no exception. We use some of these tools on an everyday basis, but most of the hardware tools I'll be covering in this chapter are used mainly in the telecommunications industry.
- **Chapter 24, "Network Troubleshooting Methodology"** In this chapter, you'll learn about all things troubleshooting, such as how to sleuth out and solve a lot of network problems.
- **Chapter 25, "Network Software Tools and Commands"** This chapter introduces you to the network tools you will use to help you run your networks. Specialized tasks require specialized tools and installing network components is no exception. We use some of these tools, like network scanners, on an everyday basis, but as with the hardware tools covered in Chapter 23, most of the software tools I'll be covering in this chapter are used mainly in the telecommunications industry.

## What's Included in the Book

I've 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** Later in this introduction is an 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 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.
- **Written Lab** Each chapter includes a written lab. These are short exercises that map to the exam objectives. The answers to these can be found in Appendix A.
- **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 Appendix B. You can go back to reread the section that deals with each question you got wrong to ensure that you answer correctly the next time you're tested on the material.

## Interactive Online Learning Environment and Test Bank

The interactive online learning environment that accompanies *CompTIA Network+ Study Guide: Exam N10-008* 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 are six practice exams. Use these questions to test your knowledge of the study guide material. The online test bank runs

on multiple devices.

- **Flashcards** Approximately 300 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.
- **Glossary** A glossary of key terms from this book and their definitions are available as a fully searchable PDF.

Note Go to `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 Network+ exam, then look no further because I've 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 explanation for any question you get wrong and make note of the chapter 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. Complete the written lab at the end of each chapter. Do *not* skip these written exercises because they directly map to the CompTIA objectives and what you've got to have nailed down to meet them.
4. 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.
5. Try your hand at the practice exams. Before you take your test, be sure to visit my website for questions, videos, audios, and other useful information.
6. Test yourself using all the electronic flashcards. This is a brand-new and updated flashcard program to help you prepare for the latest CompTIA Network+ exam, and it is a really 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.

If you follow the steps listed here and study with the review questions, practice exams, electronic flashcards, and all the written labs, you would almost have to try to fail the CompTIA Network+ exam. However, studying for the Network+ exam is like training for a marathon—if you don't go for a good run every day, you're not likely to finish very well.

## N10-008 Exam Objectives

Speaking of objectives, you're probably pretty curious about those, right? CompTIA 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 and divided into five domains.

This table gives you the extent by percentage that each domain is represented on the actual examination.

| Objective | Percentage of Exam |
|---|---|
| 1.0 Networking Fundamentals | 24% |
| 2.0 Network Implementations | 19% |
| 3.0 Network Operations | 16% |
| 4.0 Network Security | 19% |
| 5.0 Network Troubleshooting | 22% |

## Objective Map

The following table shows where each objective is covered in the book.

| Objective Number | Objective | Chapter |
|---|---|---|
| **1.0** | **Networking Fundamentals** | |
| 1.1 | Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts. | 2, 6 |
| 1.2 | Explain the characteristics of network topologies and network types. | 1 |
| 1.3 | Summarize the types of cables and connectors and explain which is the appropriate type for a solution. | 3, 4 |
| 1.4 | Given a scenario, configure a subnet and use appropriate IP addressing schemes. | 7, 8 |
| 1.5 | Explain common ports and protocols, their application, and encrypted alternatives. | 6 |
| 1.6 | Explain the use and purpose of network services. | 5 |
| 1.7 | Explain basic corporate and datacenter network architecture. | 21 |
| 1.8 | Summarize cloud concepts and connectivity options. | 21 |
| **2.0** | **Network implementations** | |
| 2.1 | Compare and contrast various devices, their features, and their appropriate placement on the network. | 5, 10, 11, 12 |
| 2.2 | Compare and contrast routing technologies and bandwidth management concepts. | 9, 10 |
| 2.3 | Given a scenario, configure and deploy common Ethernet switching features. | 10, 11 |
| 2.4 | Given a scenario, install and configure the appropriate wireless standards and technologies. | 12 |
| **3.0** | **Network Operations** | |
| 3.1 | Given a scenario, use the appropriate statistics and sensors to ensure network availability. | 13, 22 |
| 3.2 | Explain the purpose of organizational documents and policies. | 14 |
| 3.3 | Explain high availability and disaster recovery concepts and summarize which is the best solution. | 15 |
| **4.0** | **Network Security** | |
| 4.1 | Explain common security concepts. | 16 |
| 4.2 | Compare and contrast common types of attacks. | 17 |
| 4.3 | Given a scenario, apply network hardening techniques. | 18 |
| 4.4 | Compare and contrast remote access methods and security implications. | 19 |
| 4.5 | Explain the importance of physical security. | 20 |
| **5.0** | **Network Troubleshooting** | |
| 5.1 | Explain the network troubleshooting methodology. | 24 |
| 5.2 | Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools. | 23 |
| 5.3 | Given a scenario, use the appropriate network software tools and commands. | 25 |
| 5.4 | Given a scenario, troubleshoot common wireless connectivity issues. | 24 |
| 5.5 | Given a scenario, troubleshoot general networking issues. | 11, 24 |

## Assessment Test

**1.** What is the basic purpose of a local area network (LAN)?

A. To interconnect networks in several different buildings

B. To connect one or more computers together so they can share resources

C. To interconnect 2 to 10 routers

D. To make routers unnecessary

**2.** You need a topology that is easy to troubleshoot and scalable. Which would you use?

A. Bus

B. Star

C. Mesh

D. Ring

**3.** IP resides at which layer of the OSI model?

A. Application

B. Data Link

C. Network

D. Physical

**4.** Layer 2 of the OSI model is named _____. ?

A. Application layer

B. Network layer

C. Transport layer

D. Data Link layer

**5.** Which RG rating of coax is used for cable modems? ?

A. RG-59

B. RG-58

C. RG-6

D. RG-8

**6.** Which UTP wiring uses four twisted wire pairs (eight wires) and is rated for 250 MHz? ?

A. Category 3 UTP

B. Category 5 STP

C. Category 5 UTP

D. Category 6 UTP

**7.** If you are running half-duplex Internet, which of the following is true? (Choose all that apply.) ?

A. Your digital signal cannot transmit and receive data at the same time.

B. Hosts use the CSMA/CD protocol to detect collisions.

C. The physical connection consists of one wire pair.

D. None of the above.

**8.** You need to connect a hub to a switch. You don't like this idea because you know that it will create congestion. What type of cable do you need to use to connect the hub to the switch? ?

A. EtherIP

B. Crossover

C. Straight-through

D. Cable Sense, Multiple Access

**9.** Your boss asks you why you just put in a requisition to buy a bunch of switches. He said he just bought you a bunch of hubs five years ago! Why did you buy the switches? ?

A. Because each switch port is its own collision domain.

B. The cable connecting devices to the hub wore out, and switches were cheaper than new cable.

C. There were too many broadcast domains, and a switch breaks up broadcast domains by default.

D. The hubs kept repeating signals but quit recognizing frames and data structures.

**10.** Which device would connect network segments together, creating separate collision domains for each segment but only a single broadcast domain? ?

A. Hub

B. Router

C. Switch

D. Modem

**11.** Most Application layer protocols use only UDP or TCP at the Transport layer. Which of the following could use both? ?

A. TCP

B. Microsoft Word

C. Telnet

D. DNS

**12.** HTTP, FTP, and Telnet work at which layer of the OSI model? ?

A. Application

B. Presentation

C. Session

D. Transport

**13.** IPv6 uses multiple types of addresses. Which of the following would describe an anycast address used by an IPv6 host? ?

A. Communications are routed to the most distant host that shares the same address.

B. Packets are delivered to all interfaces identified by the address. This is also called one-to-many addressing.

C. This address identifies multiple interfaces, and the anycast packet is only delivered to one address. This address can also be called one-to-one-of-many.

D. Anycast is a type of broadcast.

**14.** Which of the following IP addresses are not allowed on the Internet? (Choose all that apply.) ?

A. 11.255.255.1

B. 10.1.1.1

C. 172.33.255.0

D. 192.168.0.1

**15.** What is the subnetwork address for a host with the IP address 200.10.5.168/28? ?

A. 200.10.5.156

B. 200.10.5.132

C. 200.10.5.160

D. 200.10.5.0

E. 200.10.5.255

**16.** If you wanted to verify the local IP stack on your computer, what would you do? ?

A. Ping 127.0.0.0

B. Ping 127.0.0.1

C. Telnet 1.0.0.127

D. Ping 169.5.3.10

E. Telnet 255.255.255.255

**17.** The OSI model uses an encapsulation method to describe the data as it is encapsulated at each layer. What is the encapsulation named at the Data Link layer? ?

A. Bits

B. Packets

C. Frames

D. Data

E. Segments

**18.** Where does a Data Link layer frame have to carry a Network layer packet if the packet is destined for a remote network? ?

A. Router

B. Physical medium

C. Switch

D. Another host

**19.** Which of the following are not distance-vector routing protocols? (Choose all that apply.) ?

A. OSPF

B. RIP

C. RIPv2

D. IS-IS

**20.** Which of the following uses both distance-vector and link-state properties? ?

A. IGRP

B. OSPF

C. RIPv1

D. EIGRP

E. IS-IS

**21.** You need to break up broadcast domains in a layer 2 switched network. What strategy will you use? ?

A. Implement a loop-avoidance scheme.

B. Create a flatter network structure using switches.

C. Create a VLAN.

D. Disable the spanning tree on individual ports.

**22.** Why do most switches run the Spanning Tree Protocol by default? ?

A. It monitors how the network is functioning.

B. It stops data from forwarding until all devices are updated.

C. It prevents switching loops.

D. It manages the VLAN database.

**23.** Which of the following describes MIMO correctly? ?

A. A protocol that requires acknowledgment of each and every frame

B. A data-transmission technique in which several frames are sent by several antennas over several paths and are then recombined by another set of antennas

C. A modulation technique that allows more than one data rate

D. A technique that packs smaller packets into a single unit, which improves throughput

**24.** Which practices help secure your wireless access points from unauthorized access? (Choose two.) ?

A. Assigning a private IP address to the AP

B. Changing the default SSID value

C. Configuring a new administrator password

D. Changing the mixed-mode setting to single mode

E. Configuring traffic filtering

**25.** You can view top talkers on your network by using which service listed below?

A. NetFlow

B. SIEM

C. Syslog

D. SNMP

**26.** You want to see the normal operating capacity for your whole network. Which chart can refer to the standard level?

A. Normal

B. Target

C. Baseline

D. Utilization

**27.** Which of the following are device hardening techniques? (Choose three.)

A. Remove unnecessary applications.

B. Block unrequired ports.

C. Deploy an access control vestibule.

D. Disable unnecessary services.

**28.** You want to automatically log users out that that have been logged in for a specified period without activity, so which policy would you configure?

A. Password complexity

B. Password history

C. Password length

D. Authentication period

**29.** Which protocol will help you have redundancy with your physical routers?

A. FHRP

B. NAT

C. NAC

D. CMS

**30.** Which of the following provides a method to join multiple physical switches into a single logical switching unit?

A. Stacking

B. Daisy chaining

C. Segmenting

D. Federating

**31.** An attack that no one knows about has just started coming into your corporate network in real time. What is this called?

A. RGE

B. Right Now Attack

C. Nothing; just escalate to a senior tech ASAP

D. Zero-day

**32.** What database describes each entry of a security vulnerability in detail using a number and letter system?

A. ISACA

B. WHOIS

C. CVE

D. NIST

**33.** Someone calls you and asks for your mother's maiden name because a credit card company is having problems with your account. You give them this information and later find out that you were scammed. What type of attack is this? ?

A. Phishing

B. Calling scam

C. Analog scam

D. Trust-exploration attack

E. On-path attack

F. Rogue access point

**34.** Which of the following are types of denial of service attacks? (Choose all that apply.) ?

A. Ping of Death

B. Stacheldraht

C. SYN flood

D. Virus FloodSyn

**35.** Which of the following is NOT referred to as whitelisting? (Choose three.) ?

A. Implicit allow

B. Least privilege

C. Implicit deny

D. Need to know

**36.** You want to grant rights and permissions for a group of users. What type of access control describes granting rights and permissions required for users to perform their job? ?

A. MAC

B. RBAC

C. DAC

D. BBAC

**37.** Which of the following allow you access to the GUI through a remote connection? (Choose all that apply.) ?

A. RDP

B. LogMeIn

C. SSH

D. GoToMyPC

**38.** Split tunnel and full tunnel are examples of which type of VPN? ?

A. Site-to-site

B. Client-to-site

C. RDP VPN

D. Clientless VPN

**39.** Which of the following occurs when an illegitimate user is allowed access in a biometric system? ?

A. False negative

B. True negative

C. True positive

D. False positive

**40.** Which of the following are not considered an access control vestibule? (Choose three.)

A. Trapdoor

B. Mantrap

C. Smart door

D. Turnstile

**41.** You have just tested your theory of a problem to determine the cause. Based on the standard troubleshooting methodology, what is your next step?

A. Question the obvious.

B. Establish a theory of probable cause.

C. Establish a plan of action to resolve the problem and identify potential effects.

D. Verify full system functionality, and if applicable, implement preventative measures.

**42.** Which network performance optimization technique can delay packets that meet certain criteria to guarantee usable bandwidth for other applications?

A. Traffic shaping

B. Jitter control

C. Logical network mapping

D. Load balancing

E. Access lists

**43.** Which of the following is a software management application running on servers that analyzes the received information from your network and puts the information in a type of phone book of information?

A. Syslog

B. NetFlow

C. SPAN

D. SNMP

**44.** Which of the following is an Application layer protocol that provides a message format for agents on a variety of devices to communicate with network management stations (NMSs)?

A. Syslog

B. NetFlow

C. SPAN

D. SNMP

**45.** You are using a TDR. Which of the following actions can you do with this device? (Choose all that apply.)

A. Estimate cable lengths.

B. Find splice and connector locations and their associated loss amounts.

C. Display unused services.

D. Define cable-impedance characteristics.

**46.** Which of the following is not considered a cabling issue? ?

A. Crosstalk

B. Shorts

C. Open impedance mismatch

D. DNS configurations

**47.** What is step 7 of the seven-step troubleshooting methodology? ?

A. Establish a theory of probable cause.

B. Implement the solution or escalate as necessary.

C. Establish a plan of action to resolve the problem and identify potential effects.

D. Document findings, actions, outcomes, and lessons learned.

**48.** What is step 4 of the seven-step troubleshooting methodology? ?

A. Establish a theory of probable cause.

B. Implement the solution or escalate as necessary.

C. Establish a plan of action to resolve the problem and identify potential effects.

D. Document findings, actions, outcomes, and lessons learned.

**49.** Which two `arp` utility switches perform the same function? ?

A. `-g`

B. `-Z`

C. `-d`

D. `-a`

E. `-h`

F. `-b`

**50.** You want to see a table that tells packets a direction in which to flow. Which command will show you this table? ?

A. `route print`

B. `ping`

C. `show telnet`

D. `show table direction`

## Answers

1. B. LANs generally have a geographic scope of a single building or smaller. They can be simple (two hosts) to complex (with thousands of hosts). See Chapter 1 for more information.
2. B. Star topologies are the easiest to troubleshoot and can easily scale to large sizes. See Chapter 1 for more information.
3. C. IP is a Network layer protocol. HTTPS is an example of an Application layer protocol, Ethernet is an example of a Data Link layer protocol, and T1 can be considered a Physical layer protocol. See Chapter 2 for more information.
4. D. Layer 2 of the OSI model is the Data Link layer, which provides the physical transmission of the data and handles error notification, network topology, and flow control. See Chapter 2 for more information.
5. C. Cable modems use RG-6 coax cables. See Chapter 3 for more information.
6. D. To get the high data-transfer speed, like 1 Gbps, you need to use a wire standard that is highly rated, such as Category 5e, 6, 7 and 8. See Chapter 3 for more information.
7. A, B, C. With half-duplex, you are using one wire pair with a digital signal either transmitting or receiving (but not both at once). Carrier Sense Multiple Access with Collision Detection (CSMA/CD) helps packets that are transmitted simultaneously from different hosts share bandwidth evenly. See Chapter 4 for more information.
8. B. To connect two switches together or a hub to a switch, you need a crossover cable. See Chapter 4 for more information.
9. A. For the most part, switches are not cheap; however, one of the biggest benefits of using switches instead of hubs in your internetwork is that each switch port is actually its own collision domain. A hub creates one large collision domain. Switches still can't break up broadcast domains

(do you know which devices do?). Hubs do not recognize frames and data structures but switches do. See Chapter 5 for more information.

10. C. A switch creates separate collision domains for each port but does not break up broadcast domains by default. See Chapter 5 for more information.
11. D. DNS uses TCP for zone exchanges between servers and UDP when a client is trying to resolve a hostname to an IP address. See Chapter 6 for more information.
12. A. HTTP, FTP, and Telnet use TCP at the Transport layer; however, they are all Application layer protocols, so the Application layer is the best answer for this question. See Chapter 6 for more information.
13. C. Anycast is a newer type of communication that replaces broadcasts in IPv4. Anycast addresses identify multiple interfaces, which is the same as multicast; however, the big difference is that the anycast packet is delivered to only one address: the first one it finds defined in terms of routing distance. This address can also be called one-to-one-of-many. See Chapter 7 for more information.
14. B, D. The addresses in the ranges 10.0.0.0 through 10.255.255.255 and 172.16.0.0 through 172.31.255.255 as well as 192.168.0.0 through 192.168.255.255 are all considered private, based on RFC 1918. Use of these addresses on the Internet is prohibited so that they can be used simultaneously in different administrative domains without concern for conflict. See Chapter 7 for more details on IP addressing and information on private IP addresses.
15. C. This is a pretty simple question. A /28 is 255.255.255.240, which means that our block size is 16 in the fourth octet. 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, and so on. The host is in the subnet 160. See Chapter 8 for more information.
16. B. To test the local stack on your host, ping the loopback interface of 127.0.0.1. See Chapter 8 for more information.
17. C. The Data Link layer is responsible for encapsulating IP packets into frames and for providing logical network addresses. See Chapter 9 for more information.
18. A. Packets specifically have to be carried to a router in order to be routed through a network. On your local computer, the IP address of this router is displayed as the gateway address. See Chapter 9 for more information.
19. A, D. RIP and RIPv2 are distance-vector routing protocols. OSPF and IS-IS are link-state protocols. See Chapter 10 for more information.
20. D. EIGRP is called a hybrid routing protocol because it uses the characteristics of both distance-vector and link-state routing protocols. See Chapter 10 for more information.
21. C. Virtual LANs (VLANs) break up broadcast domains in layer 2 switched internetworks. See Chapter 11 for more information.
22. C. The Spanning Tree Protocol (STP) was designed to stop layer 2 loops. All enterprise model switches have STP by default. See Chapter 11 for more information.
23. B. Part of the 802.11n wireless standard, MIMO sends multiple frames by several antennas over several paths; they are then recombined by another set of antennas to optimize throughput and multipath resistance. This is called spatial multiplexing. See Chapter 12 for more information.
24. B, C. At a minimum, you need to change the default SSID value on each AP and configure new usernames and passwords on the AP. See Chapter 12 for more information.
25. A. NetFlow statistics can analyze the traffic on your network by showing the major users of the network, meaning top talkers, top listeners, top protocols, and so on. See Chapter 13 for more information.
26. C. In networking, baseline can refer to the standard level of performance of a certain device or to the normal operating capacity for your whole network. See Chapter 13 for more information.
27. A, B, D. An access control vestibule is an access control solution, not a device hardening technique. See Chapter 14 for more information.
28. D. Authentication period controls how long a user can remain logged in. If a user remains logged in for the specified period without activity, the user will be automatically logged out. See Chapter 14 for more information.
29. A. First-hop redundancy protocol (FHRP) works by giving you a way to configure more than one physical router to appear as if they were only a single logical one. This makes client configuration and communication easier because you can simply configure a single default gateway and the host machine can use its standard protocols to communicate. See Chapter 15 for more information.
30. A. Switch stacking is the process of connecting multiple switches together (usually in a stack) to be managed as a single switch. See Chapter 15 for more information.
31. D. This condition is known as a zero-day attack because it is the first day the virus has been released and therefore no known fix exists. This term may also be applied to an operating system bug that has not been corrected. This can turn into a Resume Generating Event (RGE) quickly! See Chapter 16 for more information.
32. C. A database of known vulnerabilities using this classification system is called Common Vulnerabilities and Exposures (CVE). It is maintained by the MITRE Corporation and each entry describes a vulnerability in detail, using a number and letter system to describe what it endangers, the environment it requires to be successful in, and in many cases the proper mitigation. See Chapter 16 for more information.
33. A. Social engineering, or phishing, refers to the act of attempting to illegally obtain sensitive information by pretending to be a credible source. Phishing usually takes one of two forms: an email or a phone call. See Chapter 17 for more information.
34. A, B, C. A denial of service (DoS) attack prevents users from accessing the system. All of the options are possible DoS attacks except Virus FloodSyn. See Chapter 17 for more information.
35. A, B, D. Implicit deny means that all traffic is denied unless it is specifically allowed by a rule. This is also called whitelisting or allow listing in that you are creating a whitelist or allow list of allowed traffic with the denial of all other traffic. See Chapter 18 for more information.
36. B. Role-based access control (RBAC) is commonly used in networks to simplify the process of assigning new users the permissions required to perform a job role. In this arrangement, users are organized by job role into security groups, which are then granted the rights and permissions required to perform that job. See Chapter 18 for more information.
37. A, B, D. A remote desktop connection gives one access to the desktop. SSH provides access to a command prompt. See Chapter 19 for more information.
38. B. When a client-to-site VPN is created, it is possible to do so in two ways, split tunnel and full tunnel. The difference is whether the user uses the VPN for connecting to the Internet as well as for connecting to the office. See Chapter 19 for more information.
39. D. One of the issues with biometrics is the occurrence of false positives and false negatives. A false positive is when a user that should not be allowed access is indeed allowed access. A false negative, on the other hand, is when an authorized individual is denied passage by mistake. See Chapter 20 for more information.
40. A, C, D. An access control vestibule (previously known as a mantrap) is used to control access to the vestibule of a building. It is a series of

two doors with a small room between them. The user is authenticated at the first door and then allowed into the room. At that point, additional verification will occur (such as a guard visually identifying the person) and then they are allowed through the second door. See Chapter 20 for more information.

41. C. Based on the standard troubleshooting methodology, the next step would be to establish a plan of action to resolve the problem and identify potential effects. See Chapter 21 for more information.
42. A. Traffic shaping, also known as packet shaping, is a form of bandwidth optimization. See Chapter 21 for more information.
43. B. NetFlow shows which devices are talking to each other and what the traffic flows look like; adds timestamps, traffic peaks, and valleys; and produces nice charts and graphs of the data flowing through your network. See Chapter 22 for more information.
44. D. SNMP agents send messages to the NMS station, which then either reads or writes information in the database that's stored on the NMS and called a management information base (MIB). See Chapter 22 for more information.
45. A, B, D. Due to sensitivity to any variation and impedance to cabling, options A, B, and D are all reasons you'd use a time-domain reflectometer (TDR). See Chapter 23 for more information.
46. D. Because most of today's networks still consist of large amounts of copper cable, they can continue to suffer from the physical issues (the options are not a complete list) that have plagued all networks since the very beginning of networking. See Chapter 23 for more information.
47. D. The steps, in order, are as follows:

    1. Identify the problem.
    2. Establish a theory of probable cause.
    3. Test the theory to determine cause.
    4. Establish a plan of action to resolve the problem and identify potential effects.
    5. Implement the solution or escalate as necessary.
    6. Verify full system functionality, and if applicable, implement preventative measures.
    7. Document findings, actions, outcomes, and lessons learned.

    See Chapter 24 for more information.
48. C. The steps, in order, are as follows:

    1. Identify the problem.
    2. Establish a theory of probable cause.
    3. Test the theory to determine cause.
    4. Establish a plan of action to resolve the problem and identify potential effects.
    5. Implement the solution or escalate as necessary.
    6. Verify full system functionality, and if applicable, implement preventative measures.
    7. Document findings, actions, outcomes, and lessons learned.

    See Chapter 24 for more information.
49. A, D. The `arp` utility's `-a` and `-g` switches perform the same function. They both show the current ARP cache. See Chapter 25 for more information.
50. A. `Route print` will show you the routing table. See Chapter 25 for more information.