Save 10% on Exam Voucher

See Inside

PEARSON IT CERTIFICATION

Practice Tests

Flash Cards

Review Exercises

Study Planner

Cert Guide

Advance your IT career with hands-on learning

CompTIA®

Network+

N10-009

ANTHONY SEQUEIRA
CCIE® No.15626

FREE SAMPLE CHAPTER

Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, review exercises, Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

1. Go to www.pearsonITcertification.com/register by December 31, 2027.
2. Enter the **print book ISBN**: 9780135367889.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated with the book listing under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at **PearsonTestPrep.com**. Simply choose Pearson IT Certification as your product group and log into the site with the same credentials you used to register your book. Click the **Activate New Product** button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to **pearsonitp.echelp.org**.

This page intentionally left blank

CompTIA® Network+ N10-009 Cert Guide

Anthony Sequeira, CCIE No. 15626

CompTIA® Network+ N10-009 Cert Guide

Hoboken, New Jersey

ISBN-13: 978-0-13-536788-9

ISBN-10: 0-13-536788-3

Library of Congress Cataloging-in-Publication Data is on file.

$PrintCode

GM K12, Early Career and Professional Learning
Soo Kang

Director, ITP Product Management
Brett Bartow

Executive Editor
Nancy Davis

Development Editor
Christopher Cleveland

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Bill McManus

Indexer
Timothy Wright

Proofreader
Donna E. Mulder

Technical Editor
Chris Crayton

Publishing Coordinator
Cindy Teeters

Cover Designer
Chuti Prasertsith

Compositor
codeMantra

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Contents at a Glance

Table of Contents

About the Author

Anthony Sequeira (CCIE No. 15626) began his IT career in 1994 with IBM in Tampa, Florida. He quickly formed his own computer consultancy, Computer Solutions, and then discovered his true passion: teaching and writing about networking technologies. Anthony lectured to massive audiences around the world while working for Mastering Computers. Anthony has never been happier in his career than he is now, as a senior technical instructor for ACI Learning. ACI is a leader in audit, cybersecurity, and IT pro training in self-paced and instructor-led formats.

Dedication

This book is dedicated to my daughter, Bella Sequeira, who inspires me to do great work every day.

Acknowledgments

I cannot thank Nancy Davis and Chris Cleveland enough for their patience as I created this latest edition of the text. Also, huge thanks to my editors, Chris Crayton and Bill McManus. Their work on this text improved it dramatically.

About the Technical Reviewer

Chris Crayton is a technical consultant, trainer, author, and industry-leading technical editor. He has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has authored several print and online books on PC repair, CompTIA A+, CompTIA Security+, and Microsoft Windows. He has also served as technical editor and content contributor on numerous technical titles for several of the leading publishing companies. He holds numerous industry certifications, has been recognized with many professional and teaching awards, and has served as a state-level SkillsUSA final competition judge. Chris tech edited and contributed to this book to make it better for students and those wishing to better their lives.

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

Reader Services

Register your copy of *CompTIA Network+ N10-009 Cert Guide* for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonITcertification.com/register and log in or create an account.* Enter the product ISBN 9780135367889 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*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

The CompTIA Network+ certification is a popular certification for those entering the computer networking field. Although many vendor-specific networking certifications are popular in the industry, the CompTIA Network+ certification is unique in that it is vendor neutral. It does not focus its content on the techniques and technologies of any one specific network vendor. The CompTIA Network+ certification often acts as a stepping-stone to more specialized and vendor-specific certifications, such as those offered by Cisco Systems.

On the CompTIA Network+ exam, the topics are mostly generic in that they can apply to networking equipment regardless of vendor. Although the CompTIA Network+ certification is vendor neutral, network software and systems are implemented by multiple independent vendors. Therefore, several of the exercises, examples, and simulations in this book include using particular vendors' configurations and technologies, such as Microsoft Windows operating systems or Cisco Systems routers and switches. More detailed training for a specific vendor's software and hardware can be found in books and training specific to that vendor.

Who Should Read This Book?

This book was written with two audiences in mind: those who want to learn all they can about networking technology and those who want to pass the CompTIA Network+ exam. I think that both groups are going to be very impressed with the breadth of technologies this book details. Although it would be impossible to cover every topic in networking today, this book manages to cover all the massive areas that make networking an exciting field that many people want to learn.

Readers will range from people who are attempting to attain a position in the IT field to people who want to keep their skills sharp or perhaps retain their job when facing a company policy that mandates they take the new exams. This book is also for those who want to acquire additional certifications beyond the Network+ certification (for example, the Cisco Certified Network Associate [CCNA] certification and beyond). The book is designed to enable an easy transition to future certification studies.

Resources

This book comes with a wealth of digital resources to help you review, practice, and assess your knowledge. The end of each chapter contains a review section that references several of these tools, and you should be sure to use them as you complete each chapter to help reinforce what you are learning. You can use them again after

you finish the book to help review and make sure you are fully prepared for the exam.

Here's a list of resources available on the companion website:

- Interactive glossary flash card application
- Interactive exam essentials appendix
- The Pearson Test Prep (PTP) practice test app
- Video training on key exam topics
- Memory table review exercises and answer keys
- A study planner tool
- Instructions to redeem your Network+ certification exam voucher, which provides a 10% discount on the exam

To access the companion website, follow these steps:

Step 1. Go to **https://www.pearsonITcertification.com/register** by December 31, 2027.

Step 2. Either log in to your account if you have an existing account already or create a new account.

Step 3. Enter the ISBN of this book (**9780135367889**) and click **Submit**.

Step 4. Answer the challenge questions to validate your purchase.

Step 5. In your account page, click the **Registered Products** tab and then click the **Access Bonus Content** link.

How to Access the Pearson Test Prep (PTP) App

You have two options for installing and using the Pearson Test Prep application: a web app and a desktop app. To use the Pearson Test Prep application, start by finding the registration code that comes with the book. You can find the code in these ways:

- You can get your access code by registering the print ISBN (9780135367889) on pearsonITcertification.com/register. Make sure to use the print book ISBN regardless of whether you purchased an eBook or the print book. Once you register the book, your access code will be populated on your account page under the Registered Products tab. Instructions for how to redeem the code are available on the book's companion website by clicking the Access Bonus Content link.

- Premium Edition: If you purchase the Premium Edition eBook and Practice Test directly from the Pearson IT Certification website, the code will be populated on your account page after purchase. Just log in at pearsonITcertification.com, click Account to see details of your account, and click the digital purchases tab.

NOTE After you register your book, your code can always be found in your account under the Registered Products tab.

Once you have the access code, to find instructions about both the PTP web app and the desktop app, follow these steps:

Step 1. Open this book's companion website as shown earlier on the first page of the book, under the "Companion Website and Pearson Test Prep Access Code" heading.

Step 2. Click the **Practice Exams** button.

Step 3. Follow the instructions listed there for both installing the desktop app and for using the web app.

Note that if you want to use the web app only at this point, just navigate to pearsontestprep.com, log in using the same credentials used to register your book or purchase the Premium Edition, and register this book's practice tests using the registration code you just found. The process should take only a couple of minutes.

Customizing Your Exams

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

- **Study mode:** Enables you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you would use first to assess your knowledge and identify information gaps.
- **Practice Exam mode:** Locks certain customization options, as it is presenting 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 do, so you should not use it if you are trying to 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. You can have the test engine serve up exams from all test banks or just from one individual bank by selecting the desired banks in the exam bank area.

There are several other customizations you can make to your exam from the exam settings screen, such as the time of the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple-answer questions, and 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 while connected to the Internet, it checks if there are any updates to your exam data and automatically downloads any changes that were made since the last time you used the software.

Sometimes, due to many factors, the exam data may not fully download when you activate your exam. If you find that figures or exhibits are missing, you may need to manually update your exams. To update a particular exam you have already activated and downloaded, simply click the **Tools** tab and click the **Update Products** button. Again, this is only an issue with the desktop Windows application.

If you wish to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, simply click the **Tools** tab and click the **Update Application** button. This ensures that you are running the latest version of the software engine.

Goals and Methods

The goal of this book is to assist you in learning and understanding the technologies covered in the Network+ N10-009 blueprint from CompTIA. This book also helps you prepare for the N10-009 version of the CompTIA Network+ exam.

To aid you in mastering and understanding the Network+ certification objectives, this book uses the following methods:

- **Opening topics list:** This list spells out the Network+ objectives and topics that are covered in the chapter.
- **Foundation topics:** At the heart of a chapter, the sections under "Foundation Topics" explain the topics from hands-on and theory-based standpoints. These sections include in-depth descriptions, tables, and figures that build your knowledge so that you can pass the N10-009 exam. Each chapter is broken into multiple sections.
- **Key topics:** The "Review All Key Topics" section indicates important figures, tables, and lists of information that you need to review for the exam. Key Topic icons are sprinkled throughout each chapter, and a table at the end of each chapter lists the important parts of the text called out by these icons.
- **Memory tables:** You can find memory tables and their answer key on the book's companion website in Appendixes B and C, respectively. Use them to help memorize important information.
- **Key terms:** Key terms without definitions are listed at the end of each chapter. Write down the definition of each term and check your work against the definitions in the Glossary. On the companion website, you will find a flash card application with all the glossary terms separated by chapter, and you can use it to study key terms as well.
- **Practice exams:** As previously described, this book comes complete with several full-length practice exams available to you in the Pearson Test Prep practice test software, which you can download and install from the companion website. The Pearson Test Prep software is also available to you online, at www.PearsonTestPrep.com. Follow the directions at the beginning of the book under "Companion Website and Pearson Test Prep Access Code." Be sure to run through the questions in exam bank 1 as you complete each chapter in study mode. When you have completed the book, take a full practice test using exam bank 2 questions in practice exam mode to test your exam readiness.

For current information about the CompTIA Network+ certification exam, visit https://www.comptia.org/certifications/network.

Strategies for Exam Preparation

This book comes with a study planner tool on the companion website. It is a spreadsheet that helps you keep track of the activities you need to perform in each chapter and helps you organize your exam preparation tasks. As you read the chapters in this book, jot down notes with key concepts or configurations in the study planner. Each chapter ends with a summary and series of exam preparation tasks to help you reinforce what you have learned. These tasks include review exercises such as reviewing key topics, completing memory tables, defining key terms, answering review questions, and performing exercises. Make sure you perform these tasks as you complete each chapter to improve your retention of the material and record your progress in the study planner.

The book concludes with Chapter 26, "Final Preparation," which offers you guidance on your final exam preparation and provides you with some helpful exam advice. Make sure you read over that chapter to help assess your exam readiness and identify areas where you need to focus your review.

Download the current exam objectives by submitting a form on the following web page: https://www.comptia.org/certifications/network.

Use the practice exams, which are included on this book's companion website. As you work through the practice exams, use the practice test software reporting features to note the areas where you lack confidence and then review the related concepts. After you review those areas, work through the practice exams a second time and rate your skills. Keep in mind that the more you work through the practice exams, the more familiar the questions become, and the less accurately the practice exams judge your skills.

After you work through the practice exams a second time and feel confident with your skills, schedule the real CompTIA Network+ exam (N10-009).

CompTIA Network+ Exam Topics

Table I-1 lists general exam topics (*objectives*) and specific topics under each general topic (*subobjectives*) for the CompTIA Network+ N10-009 exam. This table lists the primary chapter in which each exam topic is covered. Note that many objectives and subobjectives are interrelated and are addressed in multiple chapters in the book.

Table I-1 CompTIA Network+ Exam Topics

Chapter	N10-009 Exam Objective	N10-009 Exam Subobjective
Chapter 1: The OSI Model and Encapsulation	1.0 Networking Concepts	1.1 Explain concepts related to the Open Systems Interconnection (OSI) reference model.
Chapter 2: Networking Appliances, Applications, and Functions	1.0 Networking Concepts	1.2 Compare and contrast networking appliances, applications, and functions.
Chapter 3: Cloud Concepts	1.0 Networking Concepts	1.3 Summarize cloud concepts and connectivity options.
Chapter 4: Networking Ports, Protocols, Services, and Traffic Types	1.0 Networking Concepts	1.4 Explain common networking ports, protocols, services, and traffic types.
Chapter 5: Transmission Media and Transceivers	1.0 Networking Concepts	1.5 Compare and contrast transmission media and transceivers.
Chapter 6: Network Topologies, Architectures, and Types	1.0 Networking Concepts	1.6 Compare and contrast network topologies, architectures, and types.
Chapter 7: IPv4 Addressing	1.0 Networking Concepts	1.7 Given a scenario, use appropriate IPv4 network addressing.
Chapter 8: Evolving Use Cases	1.0 Networking Concepts	1.8 Summarize evolving use cases for modern network environments.
Chapter 9: Routing Technologies	2.0 Network Implementation	2.1 Explain characteristics of routing technologies.
Chapter 10: Ethernet Switching Technologies	2.0 Network Implementation	2.2 Given a scenario, configure switching technologies and features.
Chapter 11: Configure Wireless Devices and Technologies	2.0 Network Implementation	2.3 Given a scenario, select and configure wireless devices and technologies.
Chapter 12: Physical Installations	2.0 Network Implementation	2.4 Explain important factors of physical installations.
Chapter 13: Organizational Processes and Procedures	3.0 Network Operations	3.1 Explain the purpose of organizational processes and procedures.
Chapter 14: Network Monitoring	3.0 Network Operations	3.2 Given a scenario, use network monitoring technologies.
Chapter 15: Disaster Recovery	3.0 Network Operations	3.3 Explain disaster recovery (DR) concepts.

Chapter	N10-009 Exam Objective	N10-009 Exam Subobjective
Chapter 16: IPv4 and IPv6 Network Services	3.0 Network Operations	3.4 Given a scenario, implement IPv4 and IPv6 network services.
Chapter 17: Network Access and Management Methods	3.0 Network Operations	3.5 Compare and contrast network access and management methods.
Chapter 18: Network Security Concepts	4.0 Network Security	4.1 Explain the importance of basic network security concepts.
Chapter 19: Types of Network Attacks	4.0 Network Security	4.2 Summarize various types of attacks and their impact to the network.
Chapter 20: Network Security Features	4.0 Network Security	4.3 Given a scenario, apply network security features, defense techniques, and solutions.
Chapter 21: A Network Troubleshooting Methodology	5.0 Network Troubleshooting	5.1 Explain the troubleshooting methodology.
Chapter 22: Troubleshoot Common Cabling Problems	5.0 Network Troubleshooting	5.2 Given a scenario, troubleshoot common cabling and physical interface issues.
Chapter 23: Troubleshoot Common Issues with Network Services	5.0 Network Troubleshooting	5.3 Given a scenario, troubleshoot common issues with network services.
Chapter 24: Troubleshoot Common Performance Issues	5.0 Network Troubleshooting	5.4 Given a scenario, troubleshoot common performance issues.
Chapter 25: Network Troubleshooting Tools	5.0 Network Troubleshooting	5.5 Given a scenario, use the appropriate tool or protocol to solve networking issues.

How This Book Is Organized

Although this book could be read cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need more work with. However, if you do intend to read all the chapters, the order in the book is an excellent sequence to use:

- **Chapter 1: The OSI Model and Encapsulation**—This chapter details the OSI model and its seven layers. This chapter also presents the encapsulation and deencapsulation processes associated with this important model.
- **Chapter 2: Networking Appliances, Applications, and Functions**—This chapter presents commonly used physical and virtual appliances in use in

networks today. This chapter also covers commonly used applications and network functions.

- **Chapter 3: Cloud Concepts**—This chapter covers some of the most important cloud concepts used in modern networking. Just some of the topics covered include deployment models, service models, and cloud connectivity options.
- **Chapter 4: Networking Ports, Protocols, Services, and Traffic Types**—This chapter ensures you are familiar with some of the most popular ports, protocols, and services in use today. This chapter also covers the traffic types of unicast, multicast, anycast, and broadcast.
- **Chapter 5: Transmission Media and Transceivers**—This chapter is all about the wireless and wired connections we make in modern networks. This chapter also covers the transceivers and connector types we often see in our networks today.
- **Chapter 6: Network Topologies, Architectures, and Types**—This chapter covers common network topologies, including mesh, hybrid, hub and spoke, and more. This chapter also covers common traffic flow types found in today's networking environments.
- **Chapter 7: IPv4 Addressing**—This chapter is all about IPv4 addressing. This includes coverage of public versus private IP addressing, subnetting, and the IPv4 address classes.
- **Chapter 8: Evolving Use Cases**—This chapter is all about some of the more cutting-edge technologies appearing in our most modern of networks today. Just some of the technologies that are covered include software-defined networking, Virtual Extensible Local Area Network (VXLAN), and IPv6 addressing.
- **Chapter 9: Routing Technologies**—This chapter tackles technologies that are specific to routing in our networks. This includes such topics as static versus dynamic routing, route selection, address translation, and first hop redundancy protocols.
- **Chapter 10: Ethernet Switching Technologies**—This chapter describes technologies related to switching in today's networks. This includes such topics as VLANs, switch interface configurations, and Spanning Tree Protocol.
- **Chapter 11: Configure Wireless Devices and Technologies**—This chapter examines topics related to Wi-Fi in networks today. This includes topics such as frequency options, network types, encryption, and many more.

- **Chapter 12: Physical Installations**—This chapter examines several important factors you should consider when you are planning and operating physical installations for networking equipment. This chapter includes topics like power and environmental factors.
- **Chapter 13: Organizational Processes and Procedures**—This chapter focuses on the purpose of organizational processes and procedures. Topics like documentation, life-cycle management, change management, and configuration management are all covered.
- **Chapter 14: Network Monitoring**—This chapter presents many different options and methods when it comes to monitoring modern networks. Topics include SNMP, SIEMs, and many more.
- **Chapter 15: Disaster Recovery**—This chapter focuses on disaster recovery (DR) topics. This includes things like DR metrics, DR sites, and high-availability approaches.
- **Chapter 16: IPv4 and IPv6 Network Services**—This chapter presents many examples of popular IPv4 and IPv6 services found in networks today. Topics in this chapter include dynamic addressing options, name resolution services, and time protocols.
- **Chapter 17: Network Access and Management Methods**—This chapter presents various options available today for network access and network management. Topics include VPNs, connection methods, and specific technologies like jump boxes.
- **Chapter 18: Network Security Concepts**—This chapter is a big one. Why? It tackles the hugely important topic of basic network security concepts. Here you will learn about things like logical security, physical security, and common security terminology.
- **Chapter 19: Types of Network Attacks**—What are some of the most common network attacks in use today? This chapter addresses this question head on and covers such topics as DoS and DDoS attacks, social engineering attacks, and many, many more.
- **Chapter 20: Network Security Features**—This chapter covers network security features, defense techniques, and solutions. This includes a discussion of device hardening, network access controls, key management, security rules, and zones.
- **Chapter 21: A Network Troubleshooting Methodology**—This chapter provides guidance on a well-planned and effective troubleshooting methodology. This methodology begins with problem identification and ends with the documentation of findings.

- **Chapter 22: Troubleshoot Common Cabling Problems**—This chapter covers troubleshooting common cabling and physical interface issues. The chapter focuses on three main areas: cable issues, interface issues, and hardware issues.
- **Chapter 23: Troubleshoot Common Issues with Network Services**—This chapter focuses on troubleshooting common issues with network services. This includes the two main areas of switching- and routing-based services.
- **Chapter 24: Troubleshoot Common Performance Issues**—These days, a network that is performing poorly can be nearly as disruptive as a network that is not functioning at all. This chapter guides you through troubleshooting the most common of performance issues. Both wired and wireless networks are discussed.
- **Chapter 25: Network Troubleshooting Tools**—This chapter focuses on the use of network troubleshooting tools that can help you solve common issues. This includes the three main categories of tools: software tools, hardware tools, and basic networking device commands.

Figure Credits

Evolving Use Cases

Are you excited to learn about some of the newer technologies featured in this version of the CompTIA Network+ exam? As the title of this chapter suggests, here we are going to focus on some of the latest evolving technologies taking the networking world by storm (and no, not a broadcast storm).

This chapter begins with a look at software-defined networking (SDN) and a very specific implementation called the software-defined wide area network (SD-WAN). As you will learn, these technologies make it much simpler to operate modern networks with all their sophisticated capabilities and features.

Next, this chapter explores the latest evolution in virtual local area networks. It is called virtual extensible local area network, or VXLAN. As you will learn, VXLAN is a network virtualization technology that encapsulates Ethernet frames in UDP packets to create a scalable Layer 2 overlay network across Layer 3 infrastructures. It enables the extension of VLANs beyond traditional boundaries, supporting large-scale cloud and data center environments by allowing for more flexible and dynamic network segmentation.

As one would guess, another important area of evolving technologies for networking is in the space of security. In this part of the chapter, we examine some of the latest advancements in network security. These include zero trust architecture (ZTA), Secure Access Secure Edge (SASE), and Security Service Edge (SSE).

Next, this chapter describes many aspects and benefits of infrastructure as code (IaC). Infrastructure as code is a method of managing and provisioning computing infrastructure through machine-readable configuration files, enabling automation and consistency across environments. Treating infrastructure configurations as code allows for version control, collaborative development, and efficient scaling of IT resources.

Although IPv4 is the most widely deployed Layer 3 addressing scheme in today's networks, its scalability limitations are causing available IPv4 addresses to quickly become depleted. Fortunately, a newer version of IP, IPv6, is scalable beyond anything you will need in your lifetime. This chapter concludes by introducing you to the fundamental characteristics of IPv6 addressing.

Foundation Topics

SDN and SD-WAN

Never before in my decades of studying and teaching computer networking have I seen more fear from students regarding the elimination of their jobs due to automation and cutting-edge technologies. In this author's opinion, artificial intelligence (AI) and computers are not going to be eliminating the need for you (a human) in the network any time soon. While ***software-defined networking (SDN)*** allows you to add more and more automation and orchestration to a network, there will still be a need for you and your skills.

Key Topic

Software-Defined Networking (SDN)

Software-defined networking, which has been around for a very long time, is making a huge resurgence and being implemented in many parts of large and small networks today. For example, consider your wireless LAN. Perhaps you are using lightweight access points and wireless LAN controllers (WLCs). If so, you are seeing a very strict separation of the data, management, and control planes. The WLC is the primary control plane intelligence of the solution. (The specific SDN planes of operation are covered in more detail later in this chapter.)

SDN is changing the landscape of traditional networks. A well-implemented software-defined network allows the administrator to implement features, functions, and configurations without the need to do command-line configuration on the individual network devices. The front end that the administrator interfaces with can alert the administrator to what the network is currently doing, and then, through that same graphical user interface, the administrator can indicate what he or she wants done; behind the scenes, the software-defined network implements the detailed configurations across multiple network devices.

A key component in most software-defined networking solutions is an SDN controller. This appliance-based device is responsible for distributing control plane instructions to network devices downstream for configuration and management.

While many different approaches can be taken to SDN, almost everyone agrees that the best strategy is to separate the network into different discrete planes or layers of operation:

- **Application plane:** This is where all the technology that involves the applications resides. Today, it is not uncommon for an application to be powered by tiny microservices running as containers in a heavily virtualized cloud

environment. But of course, there are plenty of other options for powering this layer. Many of them can even be much more traditional.

- **Control plane:** Although this layer of operation is often described as the "brains" of the operation, you are still the true brains of the operation. In fact, you are likely to use a "single pane of glass" solution that provides the correct application programming interface (API) calls to the controller. The controller turns these API commands into calls to the network devices in order to monitor or configure them properly. The API calls from you to the controller are referred to as *northbound* operations, and the commands from the controller to the network devices are referred to as *southbound operations*. The controller is always considered to be in the middle. Examples of control layer functions include routing and switching intelligence, and common control layer protocols include Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Rapid Spanning Tree Protocol (RSTP).
- **Data plane:** The data plane (sometimes called the infrastructure plane) contains the hardware and software that power the enterprise. In it, you often find legacy and dated technologies. This infrastructure is now being controlled in a new and exciting way.
- **Management plane:** It is necessary to perform a lot of routine maintenance in a network, and the management plane is for these "boring" tasks. The management plane allows administrators to see their devices and traffic flows and react as needed to manage data plane behavior. This can be done automatically through configuration apps that can, for example, add more bandwidth if it looks as if edge components are getting congested. Note that the management plane manages and monitors processes across all layers of the network stack.

All the layers of operation are critically important, and each plays an important role. The layers of operation work seamlessly together as one to get the various jobs done. Figure 8-1 shows these commonly defined planes of operations with software-defined networking.

Software-Defined Wide Area Network (SD-WAN)

For many years, new technologies and improvements have been made in local area networks (LANs). Sadly, there were not many innovations in a very important part of the network—the wide area network (WAN). Thanks to software-defined networking improvements, we now have a celebrated and popular new improvement called the ***software-defined wide area network (SD-WAN)***.

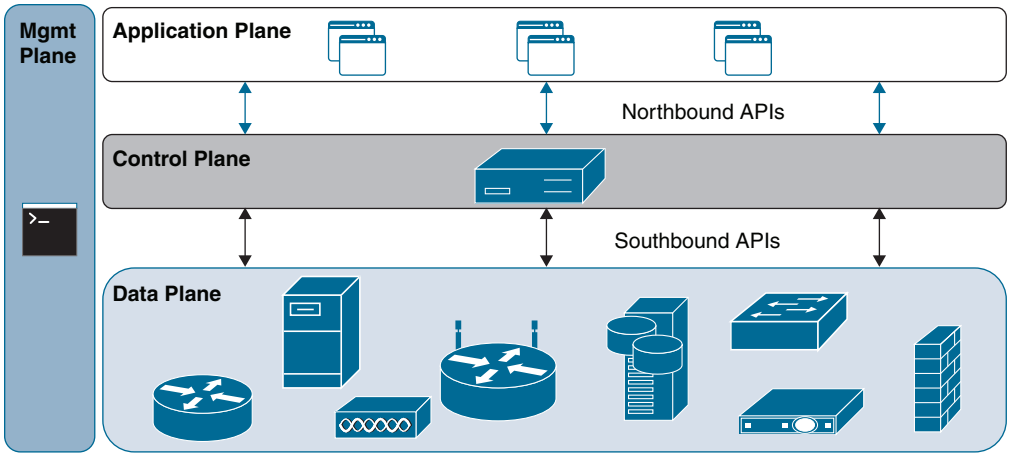

Figure 8-1 Software-Defined Networking

The SD-WAN is a transformative approach to managing and optimizing wide area networks. Unlike traditional WANs, which rely on proprietary hardware and inflexible connectivity options, SD-WAN utilizes software-defined networking principles to create a more adaptable and efficient network infrastructure. SD-WAN abstracts the network layer from the hardware, enabling centralized control and dynamic management of network traffic across multiple connection types, such as broadband, Multiprotocol Label Switching (MPLS), Long-Term Evolution (LTE), and more. This abstraction enhances performance, reduces costs, and improves overall agility, making it particularly valuable for enterprises with distributed branch locations.

One of the key features of SD-WAN is its ***application awareness***. This capability allows the network to identify and prioritize traffic based on the application, ensuring that critical applications, such as video conferencing and VoIP, receive the necessary bandwidth and low latency for optimal performance. Application awareness in SD-WAN is achieved through deep packet inspection and real-time analytics, which categorize and manage traffic flows according to predefined policies. This feature not only improves the quality of experience for end users but also enhances overall network efficiency by intelligently routing traffic based on application requirements and current network conditions.

Zero-touch provisioning (ZTP) is another significant feature of SD-WAN, simplifying the deployment and management of network devices. With ZTP, network administrators can configure and deploy new branch devices without manual intervention. This process typically involves shipping a preconfigured device to a location, where it automatically connects to the SD-WAN controller, downloads its configuration, and becomes operational with minimal human involvement. ZTP

significantly reduces deployment time and operational costs, enabling rapid scaling of the network to meet the needs of growing businesses and facilitating easier maintenance and updates.

SD-WAN is designed to be ***transport agnostic***, meaning it can leverage any available connectivity option, such as broadband, MPLS, LTE, or even satellite links. This flexibility allows organizations to choose the most cost-effective and efficient connectivity for each location, without being tied to a specific provider or technology. Transport agnosticism enhances the resilience and redundancy of the network, as SD-WAN can dynamically route traffic across multiple links to maintain performance and availability, even in the event of a link failure or degradation.

Central policy management is a cornerstone of SD-WAN architecture, providing a unified platform for defining and enforcing network policies across all connected devices and locations. Through a centralized management console, administrators can easily set rules for traffic prioritization, security, and compliance, ensuring consistent policy application throughout the network. This centralized approach simplifies network management, improves security by standardizing configurations, and enables quick adjustments to network policies in response to changing business needs or threats. Central policy management also allows for real-time monitoring and analytics, providing valuable insights into network performance and usage.

Virtual Extensible Local Area Network (VXLAN)

Key Topic

Virtual Extensible Local Area Network (VXLAN) is a network virtualization technology designed to address the limitations of traditional VLANs in large-scale data center environments and the cloud. It operates by encapsulating Layer 2 Ethernet frames within Layer 3 UDP packets, enabling the extension of Layer 2 networks over a Layer 3 infrastructure. This encapsulation allows for the creation of large-scale, logical Layer 2 networks across geographically dispersed data centers, which facilitates the movement of virtual machines (VMs) and workloads without reconfiguring the underlying physical network.

At its core, VXLAN provides a way to overcome the scalability limitations of traditional VLANs, which are restricted to a maximum of 4096 segments due to the 12-bit VLAN ID field. By using a 24-bit segment identifier known as a VXLAN Network Identifier (VNI), VXLAN can support up to 16 million distinct segments. This significant increase in segmentation capacity is crucial for modern cloud environments and large enterprise data centers, where thousands of tenants and millions of isolated networks might coexist.

The key mechanism that makes VXLAN powerful is its ability to perform ***Layer 2 encapsulation***. In VXLAN, a Layer 2 Ethernet frame from a VM or host is encapsulated into a Layer 3 UDP packet. This packet includes an outer IP header, which

can route across a Layer 3 network, and an outer UDP header, which facilitates the tunneling mechanism. The encapsulated packet is then transmitted over the existing Layer 3 infrastructure. This process allows for Layer 2 segments to be extended across different Layer 3 networks, creating a seamless and scalable virtual network that behaves as if all connected hosts are on the same local network. Figure 8-2 shows the Layer 2 encapsulation used with VXLAN technology.

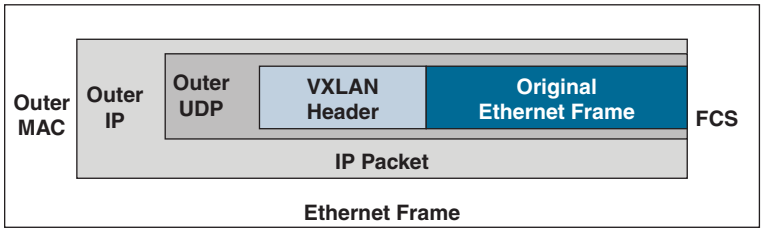

Figure 8-2 VXLAN Encapsulation

One of the primary applications of VXLAN is in ***data center interconnect (DCI)***. DCI involves connecting multiple data centers to provide a unified infrastructure, allowing for efficient resource sharing, workload mobility, and disaster recovery. VXLAN is particularly suited for DCI because it enables the extension of Layer 2 networks over Layer 3 distances, thus facilitating the seamless migration of VMs and applications between data centers. This capability is crucial for businesses that need to maintain high availability and disaster resilience by distributing workloads across multiple locations.

VXLAN also integrates well with modern network management and automation tools, supporting dynamic and programmable networking. The VXLAN gateways or Virtual Tunnel Endpoints (VTEPs) play a critical role in encapsulating and decapsulating traffic and can be implemented in both hardware (switches) and software (hypervisors). This flexibility makes VXLAN an essential component in the architecture of software-defined networks (SDNs) and network functions virtualization (NFV), where it provides the necessary overlay networks that decouple virtual network management from physical network hardware.

Key Topic

Zero Trust Architecture (ZTA)

Zero trust architecture (ZTA) is a security model centered on the principle that no entity, whether inside or outside the network, should be trusted by default. Instead, verification is required from everyone trying to access resources within the network, ensuring robust and granular security. Unlike traditional security models that rely on a trusted internal network and a less trusted external network, ZTA treats all network traffic as untrusted, continuously validating users and devices before granting

access to sensitive data and systems. This model significantly mitigates the risk of cyber threats by ensuring that access is granted only to those who genuinely need it and are properly authenticated.

In zero trust architecture, ***policy-based authentication*** is a crucial component. This approach ensures that all access requests are dynamically authenticated using predefined security policies that consider a variety of factors. These factors include the identity of the user, the device being used, the location of the access request, and the nature of the resource being accessed. Each access attempt is subjected to rigorous authentication checks, which may include multifactor authentication (MFA) and contextual data analysis. For instance, a user attempting to access a corporate resource from an unfamiliar location or device might be required to provide additional verification to ensure they are who they claim to be. By implementing policy-based authentication, ZTA enhances security by dynamically adjusting access requirements based on the context and potential risks associated with each request.

Once authentication is successfully achieved, ZTA moves to policy-based ***authorization***, which governs what authenticated users are permitted to do within the network. Authorization policies are designed to be granular and specific, ensuring that users have access only to the resources necessary for their roles and tasks. These policies are enforced in real time, continually reassessing user permissions based on their current context and behavior. For example, if a user's behavior deviates from their usual patterns, such as accessing sensitive data they don't typically handle, the system may prompt for additional verification or deny access altogether. This dynamic and context-aware approach to authorization helps prevent unauthorized access and reduces the risk of data breaches by ensuring that permissions are strictly aligned with business needs and security requirements.

Central to the ZTA model is the concept of ***least privilege access***. This principle dictates that users and devices should be granted the minimum level of access required to perform their functions and no more. By limiting access rights, ZTA minimizes the potential damage that could be caused by compromised credentials or malicious actors. Implementing least privilege access involves meticulously defining user roles, responsibilities, and the associated access permissions. For instance, a financial analyst may need access to financial records but not to customer personal information, while an IT administrator might need access to system logs but not to employee payroll data. Regular reviews and adjustments of access levels are also essential to accommodate changes in roles and responsibilities, ensuring that access permissions remain tightly controlled and aligned with the principle of least privilege access.

SASE and SSE

Secure Access Secure Edge (SASE) is a transformative architectural framework designed to meet the demands of modern networking and security. It is a cloud-native service model that converges wide area networking and network security services like Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA), and Firewall as a Service (FWaaS) into a single cloud-based service. This convergence allows organizations to securely connect users, devices, and applications over a global network. The SASE framework was first conceptualized by Gartner in 2019 as a response to the evolving IT landscape, where traditional network and security models were becoming increasingly insufficient for the dynamic, distributed, and cloud-centric environments.

At its core, SASE provides secure and optimized access to applications and resources regardless of the user's location. This is crucial in the current era where remote work and cloud adoption have surged, making traditional perimeter-based security models obsolete. SASE combines networking and security functionalities in a unified platform, delivered as a service from the cloud. This integration simplifies the complexity of managing multiple standalone solutions, reduces costs, and provides consistent security policies across all edges of the network, including data centers, branches, mobile users, and Internet of Things (IoT) devices.

A key aspect of SASE is its emphasis on zero trust security principles. Unlike traditional network security models that focus on defending a defined perimeter, zero trust assumes that threats can originate from both outside and inside the network. SASE implements zero trust by verifying the identity and integrity of users and devices before granting access to applications and data. This ensures that only authenticated and authorized entities can access sensitive resources, mitigating risks associated with internal and external threats. Furthermore, SASE continuously monitors and enforces security policies based on user behavior, device status, and network context to dynamically adapt to changing threat landscapes.

SASE also addresses the need for optimized network performance by integrating SD-WAN capabilities. By leveraging the global presence of SASE providers, organizations can benefit from reduced latency, improved application performance, and enhanced user experience, regardless of the user's geographical location.

SASE also supports a holistic approach to data protection and compliance. By consolidating security functions into a single framework, SASE provides comprehensive visibility and control over data flows across the network. This enables organizations to enforce data loss prevention (DLP) policies, detect and respond to threats in real time, and ensure compliance with regulatory requirements. The centralized management of security policies also simplifies the auditing process and facilitates the rapid implementation of policy changes to adapt to evolving compliance demands.

Security Service Edge (SSE) is a cloud-native cybersecurity framework that provides a comprehensive suite of security services to protect data, applications, and users in a distributed, cloud-centric environment. Introduced by Gartner as a distinct subset of the broader Secure Access Service Edge (SASE) model, SSE focuses specifically on delivering security services without encompassing the networking components such as SD-WAN. It is designed to address the challenges of modern IT architectures, where traditional perimeter-based security is inadequate for safeguarding against sophisticated cyber threats targeting a dispersed workforce and cloud-hosted resources.

SSE is particularly relevant in the context of today's hybrid and remote work environments, where employees access corporate resources from various locations and devices. Traditional security solutions that rely on a fixed perimeter are insufficient in such scenarios, as they cannot effectively protect against threats targeting remote users or cloud-hosted data. SSE addresses this challenge by extending security controls to the edge, ensuring that all users, regardless of their location, are subject to the same rigorous security policies. This approach not only improves security but also simplifies the management of security infrastructure by consolidating it into a single cloud-based service.

Another significant aspect of SSE is its focus on data protection and regulatory compliance. With the increasing volume of sensitive data being stored and processed in the cloud, organizations face greater risks of data breaches and regulatory fines. SSE helps mitigate these risks by providing advanced data protection capabilities such as encryption, data loss prevention, and threat detection. These features ensure that sensitive data is safeguarded against unauthorized access and exfiltration, and that organizations can maintain compliance with data privacy regulations like GDPR, CCPA, and HIPAA.

Infrastructure as Code (IaC)

One of the most exciting developments in technology today is ***infrastructure as code (IaC)***. When your infrastructure (often in the cloud) is all virtualized, it can be easily created (and destroyed) as well as maintained by using scripts (code). This makes it possible for you to "spin up" test environments or pilot tests with ease. Think about how much easier it is to create a duplicate site for high availability (HA) needs when using IaaS and IaC than when using physical devices.

The large public cloud providers make it simple for you to implement IaC. They provide tools (such as CloudFormation from AWS) that permit you to easily generate the code required to script the creation of useful (and even complex) infrastructures. Thanks to this capability, you can easily automate—and even orchestrate—common networking tasks that used to take weeks or months to carry out.

For example, say that you need to spin up 50 servers for a test project. Thanks to IaC, you can now do this with a few clicks of the mouse instead of using a massive (and often) expensive deployment of physical servers.

There is a difference between automation and orchestration:

- ***Automation*** refers to the automated completion of a task or tasks.
- *Orchestration* refers to the scheduling and monitoring of many different automations. It is, basically, automating the automation.

NOTE IaC is also known as *programmable infrastructure* to indicate that the infrastructure configuration can be incorporated into application code. IaC enables DevOps teams to test applications in production-like environments from the beginning of the development cycle.

Key components of automation in IaC include playbooks, templates, and reusable tasks, which facilitate the creation, maintenance, and scaling of infrastructure in a consistent manner. Additionally, automation helps address challenges such as configuration drift, compliance, and upgrades, and supports dynamic inventories for flexible resource management. Here are more details on the key components and advantages of automation with IaC:

Key Topic

- ***Playbooks*:** Playbooks are a fundamental tool in IaC automation, particularly in tools like Ansible. They provide a structured way to define a series of tasks that automate the provisioning, configuration, and management of infrastructure. Playbooks are written in YAML and describe the desired state of the infrastructure in a declarative manner. This allows for complex workflows to be automated, such as deploying applications, configuring servers, and managing network devices.

NOTE Ansible is a software tool that enables infrastructure as code. It is open source and includes modules for software provisioning, configuration management, and application deployment functionality. YAML is a human-readable data serialization language. It is commonly used for configuration files and in applications where data is being stored or transmitted.

- ***Templates*:** Templates in IaC are used to define infrastructure resources in a reusable and consistent manner. Tools like Terraform and AWS CloudFormation utilize templates to describe cloud resources and their relationships. These templates can include variables, allowing for parameterization and flexibility in resource configurations. For example, a template might define a

virtual machine with specific attributes like instance type, security groups, and attached storage. By using templates, organizations can ensure that infrastructure components are created with a consistent configuration across different environments, reducing the risk of configuration errors and making it easier to replicate and scale infrastructure.

- ***Reusable tasks*:** Reusable tasks are a key aspect of IaC automation that promote efficiency and maintainability. In tools like Ansible, reusable tasks can be defined in roles, which are collections of tasks, variables, and templates organized in a structured format. Roles can be shared across multiple playbooks and projects, allowing for the reuse of common configurations and deployment steps. For example, a role might encapsulate the tasks required to set up a web server, including installing packages, configuring services, and managing firewall rules.
- ***Configuration drift*:** Configuration drift occurs when the actual state of the infrastructure deviates from the desired state defined in the IaC. This can happen due to manual changes, system updates, or environmental factors. Automation in IaC helps mitigate configuration drift by regularly applying the desired state to the infrastructure. Tools like Terraform and Ansible can perform periodic checks and reapply configurations to ensure consistency. This not only helps maintain the reliability and predictability of the infrastructure but also reduces the time and effort required to troubleshoot and resolve issues caused by drift. Automation ensures that the infrastructure remains aligned with the defined state, minimizing the risks associated with unintended changes.
- ***Compliance*:** Compliance with industry standards and regulatory requirements is a critical aspect of infrastructure management. Automation in IaC enables organizations to enforce compliance by embedding policies and controls directly into the infrastructure code. For example, security configurations, access controls, and data protection measures can be defined in the IaC templates and playbooks. Automated tools can continuously monitor the infrastructure for compliance with these policies, generating reports and alerts when deviations occur.
- ***Upgrades*:** Upgrading infrastructure components, such as software versions, operating systems, and hardware configurations, can be a complex and error-prone process. IaC automation simplifies upgrades by allowing organizations to define the desired state of the infrastructure, including the required versions and configurations. Upgrades can be tested in a staging environment using the same IaC definitions before being applied to production, reducing the risk of disruptions.

- ***Dynamic inventories*:** Dynamic inventories are a feature of IaC automation that allows the infrastructure to be dynamically discovered and managed based on current configurations and states. This is particularly useful in cloud environments, where resources can be created and terminated frequently. Tools like Ansible support dynamic inventories, which can query cloud providers or other data sources to generate an up-to-date list of resources for configuration management tasks.

Because the C in IaC stands for code, it is of no surprise that IaC systems tend to take advantage of ***source control*** systems. These systems tend to feature the following:

- ***Version control*:** Version control is at the heart of source control systems and is vital for managing IaC. It enables teams to track changes to infrastructure code over time, maintaining a history of modifications, additions, and deletions. Each change is recorded with a unique identifier, often called a *commit*, along with metadata such as the author, timestamp, and a message describing the change.
- ***Central repository*:** A central repository in a source control system acts as the single source of truth for all infrastructure code. This repository stores the master copies of the code and provides a central location where all team members can access, contribute to, and collaborate on the infrastructure codebase.
- ***Conflict identification*:** Conflict identification is an essential feature of source control systems, especially in collaborative IaC environments, where multiple team members may work on the same code simultaneously. Conflicts occur when changes made by different users overlap or are incompatible with each other.
- ***Branching*:** Branching is a powerful feature of source control systems that allows teams to create isolated copies of the codebase for different purposes. This is particularly useful in IaC environments for managing multiple streams of development and experimentation without affecting the main codebase.

IP Version 6

With the global proliferation of IP-based networks, available IPv4 addresses are rapidly becoming exhausted. Fortunately, IPv6 provides enough IP addresses for many generations to come. This section introduces ***IPv6 addressing*** with a deep dive into IPv6's address structure and a discussion of some of its unique characteristics.

Need for IPv6

With the worldwide depletion of IP version 4 (IPv4) addresses, many organizations have migrated, are in the process of migrating, or are considering migrating their IPv4 addresses to IPv6 addresses. IPv6 dramatically increases the number of available IP addresses. In fact, IPv6 offers approximately 5×10^{28} IP addresses for each person on the planet.

Beyond the increased address space, IPv6 offers many other features:

- Simplified header:
  - The IPv4 header uses 12 fields.
  - The IPv6 header uses 5 fields.
- No broadcasts
- No fragmentation (performs MTU discovery for each session)
- Can coexist with IPv4 during a transition:
  - ***Dual stack*** (running IPv4 and IPv6 simultaneously on a network interface or device)
  - IPv6 over IPv4 (tunneling IPv6 over an IPv4 tunnel)

Even if you are designing a network based on IPv4 addressing, it is a good practice to consider how readily an IPv6 addressing scheme could be overlaid on that network at some point in the future. Using Teredo ***tunneling***, an IPv6 host could provide IPv6 connectivity even when the host is directly connected to an IPv4-only network. Miredo is a client that can be used to implement the Teredo protocol and is included in many versions of Linux. IPv6/IPv4 tunneling is often referred to as 6to4 or 4to6 tunneling, depending on which protocol is being tunneled (IPv4 or IPv6). These are just some of the many tunneling mechanisms devised to ensure a smooth transition from IPv4 to IPv6. In fact, thanks to dual stack and tunneling features, it is very unlikely that you will see IPv4 ever completely go away in your lifetime.

Since there are so many available IPv6 addresses, network address translation (NAT) is not nearly as required in IPv6. One way it can be useful is in transition between the two versions, however. Network address translation from IPv6 to IPv4 (***NAT64***) is a technology that facilitates communication between IPv6-only clients and IPv4-only servers, bridging the gap between the two distinct IP address families. It is yet another component in the transition from the older IPv4 protocol to the newer IPv6 protocol, allowing IPv6 networks to access resources on IPv4 networks without requiring the end systems to support both protocols. NAT64 works by translating

IPv6 packets to IPv4 packets and vice versa, using a predefined prefix to generate an IPv6 address that maps to an IPv4 address.

IPv6 Address Structure

An IPv6 address has the following address format, where *X* is a hexadecimal digit in the range of 0 to F:

XXXX:*XXXX*:*XXXX*:*XXXX*:*XXXX*:*XXXX*:*XXXX*:*XXXX*

A hexadecimal digit is 4 bits in size (4 binary bits can represent 16 values). Notice that an IPv6 address has eight fields, and each field contains four hexadecimal digits. The following formula reveals why an IPv6 address is a 128-bit address:

4 bits per digit × 4 digits per field × 8 fields = 128 bits in an IPv6 address

IPv6 addresses can be difficult to work with because of their size. Fortunately, the following rules (often collectively referred to as *shorthand notation*) exist for abbreviating these addresses:

Key Topic

- Leading 0s in a field can be omitted.
- Contiguous fields containing all 0s can be represented with a double colon. (Note that this can be done only once for a single IPv6 address.)

For example, consider the following IPv6 address:

ABCD:0123:4040:0000:0000:0000:000A:000B

Using the rules for abbreviation, the IPv6 address can be rewritten as follows:

ABCD:123:4040::A:B

An exciting feature of IPv6 is the Extended Unique Identifier (EUI-64) format, which permits a device to automatically populate the low-order 64 bits of an IPv6 address based on an interface's MAC address. You will read more about this capability later in this chapter.

IPv6 Address Types

The following are some of the many unique aspects of IPv6 addressing and interesting address types:

- IPv6 globally routable unicast addresses start with the first four hex characters in the range 2000 to 3999.
- An IPv6 link-local address is also used on each IPv6 interface. The link-local address begins with FE80.

- Multicast addresses begin with FF as the first two hex characters.
- IPv6 can use autoconfiguration to discover the current network and select a host ID that is unique on that network. Automatic generation of a unique host ID is made possible through a process known as *EUI-64*, which uses the 48-bit MAC address on the device to aid in the generation of the unique 64-bit host ID. Notice that the autoconfiguration capabilities described here permit you to create an IPv6 network free of DHCP-type services. The ability of IPv6 to replace the need for DHCP services like this is known as stateless address autoconfiguration (SLAAC). You will learn more about SLAAC in Chapter 16, "IPv4 and IPv6 Network Services."
- IPv6 can also use a special version of DHCP for IPv6. Not surprisingly, this version is called *DHCPv6*.
- The protocol that is used for *network discovery*—that is, to discover the network address and learn the Layer 2 addresses of neighbors on the same network—is Neighbor Discovery Protocol (NDP).

NDP is hugely important in IPv6. It defines five ICMPv6 packet types for important jobs:

- **Router Solicitation:** Hosts inquire with Router Solicitation messages to locate routers on an attached link.
- **Router Advertisement:** Routers advertise their presence together with various link and Internet parameters, either periodically or in response to a Router Solicitation message.
- **Neighbor Solicitation:** Neighbor solicitation messages are used by nodes to determine the link layer address of a neighbor or to verify that a neighbor is still reachable via a cached link layer address.
- **Neighbor Advertisement:** Neighbor advertisement messages are used by nodes to respond to a Neighbor Solicitation message.
- **Redirect:** Routers may inform hosts of a better first-hop router for a destination.

IPv6 Data Flows

You might recall from our discussion of IPv4 traffic flows in Chapter 4 that there are unicast, broadcast, multicast, and anycast methods of communication possible with IP version 4. IPv6 uses just three of the four types of data flows:

Key Topic

- Unicast
- Multicast
- Anycast

Just like in IPv4, IPv6 uses special address types for these data flows. The following sections summarize the characteristics of each address type.

Unicast

With unicast, a single IPv6 address is applied to a single interface, as illustrated in Figure 8-3. The communication flow can be thought of as a one-to-one communication flow.

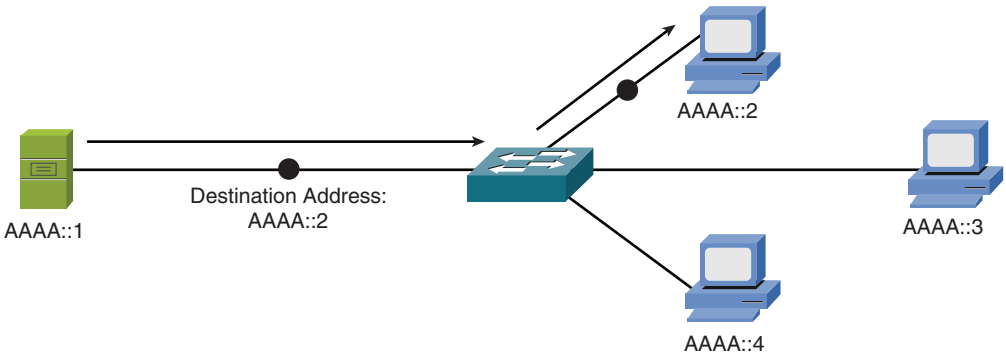

Figure 8-3 IPv6 Unicast Example

In Figure 8-3, a server (AAAA::1) is sending traffic to a single client (AAAA::2).

Multicast

With multicast, a single IPv6 address (a multicast group) can represent multiple devices on a network, as shown in Figure 8-4. The communication flow is a one-to-many communication flow.

In Figure 8-4, a server (AAAA::1) is sending traffic to a multicast group (FF00::A). Two clients (AAAA::2 and AAAA::3) have joined this group. Those clients receive the traffic from the server, and any client that did not join the group (for example, AAAA::4) does not receive the traffic.

IPv6 replaces broadcast behavior with multicast, thanks to the "all nodes" multicast group. This reserved address is FF01:0:0:0:0:0:0:1 (FF01::1). All IPv6 nodes join this group. This is a simple and efficient method for sending traffic to all nodes.

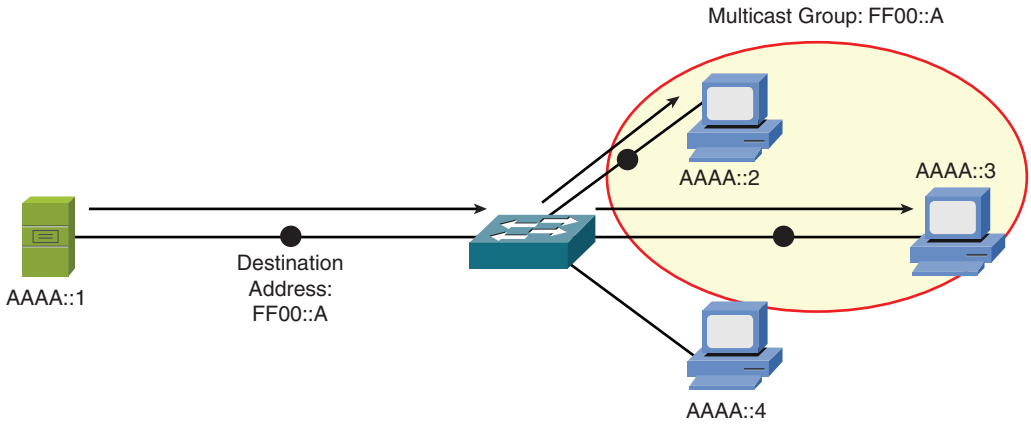

Figure 8-4 IPv6 Multicast Example

Anycast

With *anycast*, a single IPv6 address is assigned to multiple devices, as illustrated in Figure 8-5. It is a one-to-nearest (from the perspective of a router's routing table) communication flow.

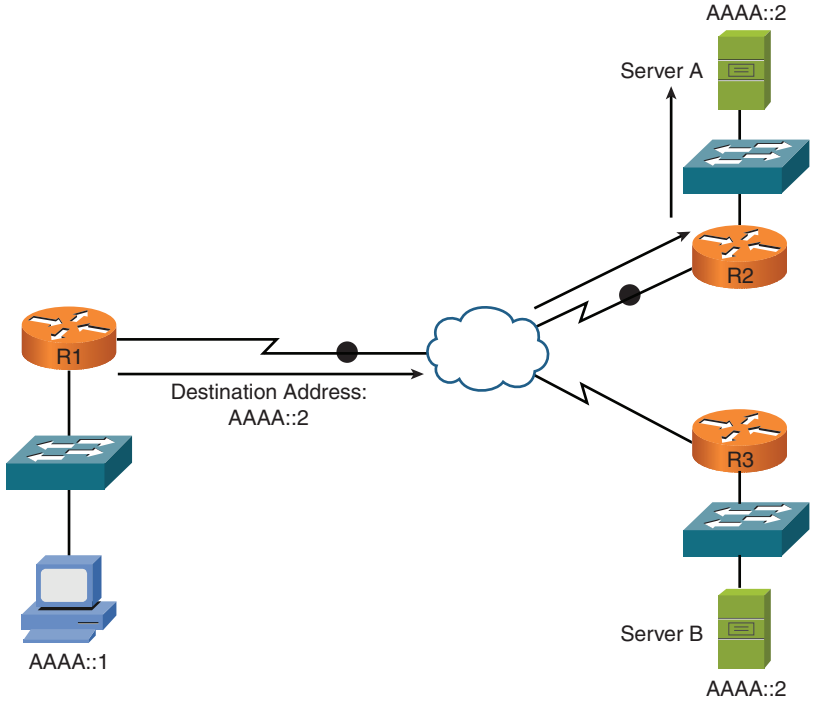

Figure 8-5 IPv6 Anycast Example

In Figure 8-5, a client with IPv6 address AAAA::1 wants to send traffic to destination IPv6 address AAAA::2. Notice that two servers (Server A and Server B) have the IPv6 address AAAA::2. In the figure, the traffic destined for AAAA::2 is sent to Server A, via router R2, because the network on which Server A resides appears to be closer than the network on which Server B resides, from the perspective of router R1's IPv6 routing table.

NOTE Remember that the dreaded broadcast frames and packets from IPv4 do not exist in an IPv6-only network. IPv6 uses only unicasts, multicasts, and anycasts, as described in this section. With IPv6, if you want to send a frame or packet to all nodes in the local network, you use the all-nodes IPv6 multicast address.

Real-World Case Study

Acme, Inc. is currently investigating the use of a software-defined wide area network (SD-WAN) to help revolutionize the legacy WAN infrastructure. Specifically, Acme is very interested in the enhanced network performance that this solution can bring. Acme would like the SD-WAN solution to dynamically route traffic over the best available path based on real-time network conditions, such as latency, jitter, and packet loss. This would ensure that critical applications, like video conferencing and cloud services, receive the bandwidth and low-latency routes they need, resulting in a better user experience.

Acme, Inc. is also actively exploring the implementation of a new zero trust architecture to enhance its cybersecurity posture and mitigate the risks associated with modern cyber threats. Unlike traditional security models that rely on a defined network perimeter, zero trust operates on the principle that no user or device, whether inside or outside the network, should be trusted by default. This approach aligns with Acme's goal of protecting sensitive data and resources in an increasingly complex and distributed IT environment. By adopting zero trust, Acme can ensure that all access requests are continuously verified and authenticated, regardless of the user's location or network. This is particularly important as Acme's workforce becomes more mobile and remote, accessing company resources from various devices and locations. Zero trust will enable Acme to enforce strict access controls and minimize the attack surface, thereby reducing the likelihood of unauthorized access and data breaches.

The move toward zero trust is also driven by Acme's desire to streamline compliance with regulatory requirements and enhance the overall resilience of its IT infrastructure. Zero trust architecture provides a comprehensive framework for implementing security policies that are consistent and enforceable across all endpoints and applications. This allows Acme to achieve greater visibility into user activities and data flows, ensuring that any suspicious behavior is promptly detected and addressed. Additionally, the granular control afforded by zero trust helps Acme to safeguard sensitive information and comply with regulations such as GDPR and HIPAA, which mandate stringent data protection measures. By integrating zero trust principles into its security strategy, Acme aims to build a robust and adaptable security model that not only protects against current threats but also evolves to address future challenges, ultimately supporting the company's growth and operational excellence.

Summary

Here are the main topics covered in this chapter:

- This chapter first provided a description of software-defined networking (SDN) and software-defined wide area networks (SD-WAN).
- This chapter next covered emerging technology of Virtual Extensible Local Area Networks (VXLAN). After describing the Layer 2 encapsulation that makes this technology function, this section described the common use case of the data center interconnect (DCI) functionality.
- This chapter then examined the emerging technology of the zero trust architecture (ZTA), including its major components of policy-based authentication, authorization, and least privilege access.
- This chapter defined the Secure Access Secure Edge (SASE) and Security Service Edge (SSE) solutions.
- This chapter covered the concept of infrastructure as code (IaC) and emphasized the features of IaC that rely on automation. This section of the chapter also discussed how source control can be critical to the IaC environment.
- The characteristics of IPv6 were highlighted, including the IPv6 address format and IPv6 data flows (unicast, multicast, and anycast).

Exam Preparation Tasks

Review All the Key Topics

Review the most important topics from this chapter, noted with the Key Topic icon in the outer margin of the page. Table 8-1 lists these key topics and the page number where each is found.

Key Topic

Table 8-1 Key Topics for Chapter 8

Key Topic Element	Description	Page Number
Section	Software-Defined Networking (SDN)	205
Section	Virtual Extensible Local Area Network (VXLAN)	208
Section	Zero Trust Architecture (ZTA)	209
List	Key components for IaC	213
List	Steps for shorthand with IPv6 addresses	217
List	Functions of NDP	218
List	Types of IPv6 data flows	219

Define Key Terms

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

application awareness, authorization, automation, branching, central policy management, central repository, compliance, configuration drift, conflict identification, data center interconnect (DCI), dual stack, dynamic inventories, infrastructure as code (IaC), IPv6 addressing, Layer 2 encapsulation, least privilege access, NAT64, playbooks, policy-based authentication, reusable tasks, Secure Access Secure Edge (SASE), Security Service Edge (SSE), source control, software-defined networking (SDN), software-defined wide area network (SD-WAN), templates, transport agnostic, tunneling, upgrades, version control, Virtual Extensible Local Area Network (VXLAN), zero-touch provisioning (ZTP), zero trust architecture (ZTA)

Additional Resources

Software Defined Networking (SDN) Demystified: https://www.youtube.com/watch?v=lVcUZCVvBjw

VXLAN Simple Explanation: https://www.youtube.com/watch?v=7Shfu9BrJP8

Review Questions

The answers to these review questions appear in Appendix A, "Answers to Review Questions."

1. BGP is an example of a technology found in what layer/plane of operation in a software-defined network?
   a. Management
   b. Control
   c. Data
   d. Application

2. What feature of the SD-WAN allows the network to seamlessly route and manage traffic over diverse transport media without dependency on the underlying physical connections?
   a. Central policy management
   b. Application awareness
   c. Zero-touch provisioning
   d. Transport agnostic

3. What protocol serves as the transport protocol for encapsulating Layer 2 Ethernet frames with Layer 3 packets in the VXLAN solution?
   a. UDP
   b. TCP
   c. ARP
   d. FHRP

4. What is the term given to the difference in the actual state of your infrastructure compared to the state defined in an IaC implementation?
   a. Version control
   b. Configuration drift
   c. Source control
   d. Conflict identification

5. How can the following IPv6 address be condensed?

   2009:0123:4040:0000:0000:000:000A:100B
   a. 2009::123:404:A:100B
   b. 2009::123:404:A:1B
   c. 2009:123:4040::A:100B
   d. 2009:0123:4040::0::000A:100B

6. What technology allows for the automatic assignment of the host portion of an IPv6 address?
   a. Dual stack
   b. EUI-64
   c. Neighbor discovery
   d. Anycast

7. What can IPv6 networks use to assign IP addresses?
   a. SLAAC
   b. CIDR
   c. Port address translation
   d. Classless inter-domain routing notation

8. Which of the following is a network architecture that integrates wide area networking (WAN) capabilities with comprehensive network security functions such as Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall as a Service (FWaaS), and Zero Trust Network Access (ZTNA)?
   a. SD-WAN
   b. VXLAN
   c. SSE
   d. SASE

9. Which of the following involves connecting multiple data centers to provide a unified infrastructure, allowing for efficient resource sharing, workload mobility, and disaster recovery?
   a. NAT64
   b. SASE
   c. DCI
   d. SSE

10. Which of the following is a technology that facilitates communication between IPv6-only clients and IPv4-only servers, bridging the gap between the two distinct IP address families?
   a. NAT64
   b. Dual stack
   c. Conflict identification
   d. Branching

This page intentionally left blank

Index

B

C

D

E

F

G

H

J

K

L

M

N

O

P

Q-R

T

U

V

W

X-Y-Z