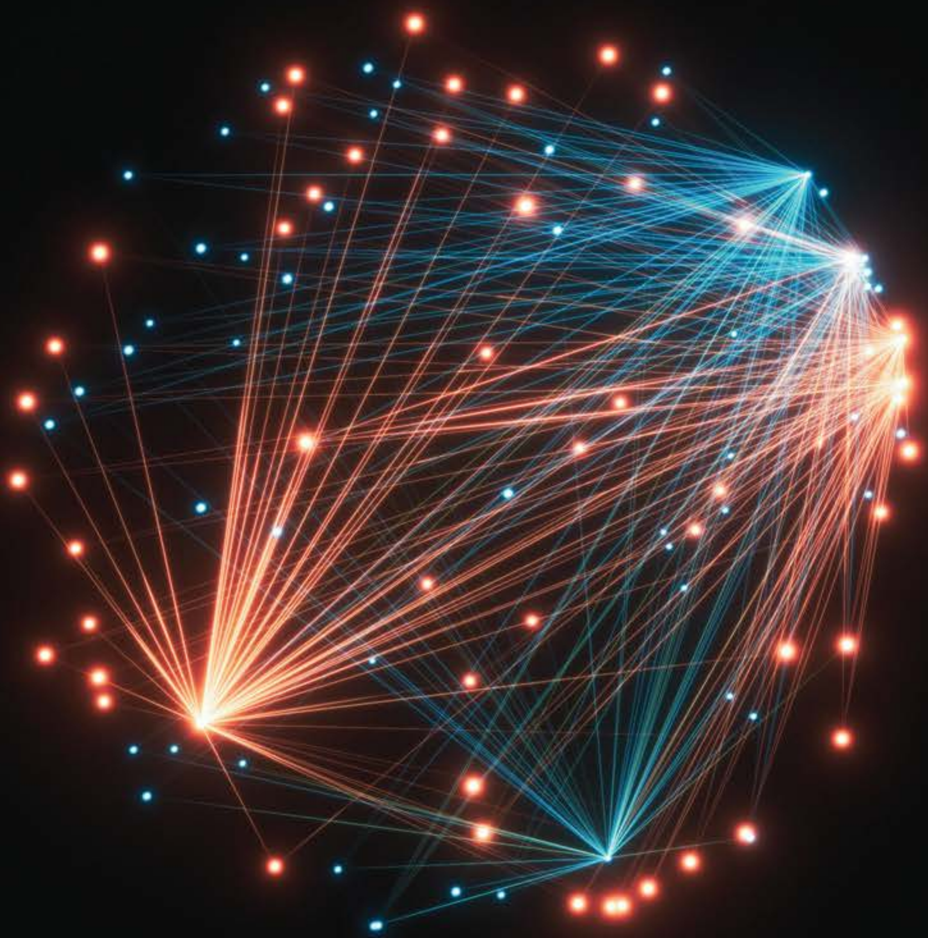
CENGAGE

Ninth Edition

Data Communications and Computer Networks

A Business User's Approach



Jill West
Curt M. White

Data Communications & Computer Networks

A Business User's Approach

Ninth Edition

Jill West

Curt M. White

CENGAGE

Australia • Brazil • Canada • Mexico • Singapore • United Kingdom • United States

Data Communications & Computer Networks: A Business User's Approach, **Ninth Edition**

Jill West and Curt M. White

SVP, Higher Education Product Management: Erin Joyner

VP, Product Management, Learning Experiences: Thais Alencar

Product Director: Jason Fremder

Product Manager: Natalie Onderdonk

Product Assistant: Tom Benedetto

Content Manager: Arul Joseph Raj, Lumina Datamatics, Inc.

Digital Delivery Quality Partner: Jim Vaughey

VP, Product Marketing: Jason Sakos

IP Analyst: Ann Hoffman

IP Project Manager: Anjali Kambli, Lumina Datamatics, Inc.

Production Service: Lumina Datamatics, Inc.

Designer: Erin Griffin

Cover Image Source: Xuanyu Han/Getty Images

For product information and technology assistance, contact us at **Cengage Customer & Sales Support, 1-800-354-9706 or support.cengage.com.**

For permission to use material from this text or product, submit all requests online at **www.copyright.com**.

Library of Congress Control Number: 2021925306

ISBN: 978-0-357-50440-6

Cengage
200 Pier 4 Boulevard
Boston, MA 02210
USA

Cengage is a leading provider of customized learning solutions with employees residing in nearly 40 different countries and sales in more than 125 countries around the world. Find your local representative at **www.cengage.com.**

To learn more about Cengage platforms and services, register or access your online learning solution, or purchase materials for your course, visit **www.cengage.com.**

Notice to the Reader

Publisher does not warrant or guarantee any of the products described herein or perform any independent analysis in connection with any of the product information contained herein. Publisher does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instructions contained herein, the reader willingly assumes all risks in connection with such instructions. The publisher makes no representations or warranties of any kind, including but not limited to, the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and the publisher takes no responsibility with respect to such material. The publisher shall not be liable for any special, consequential, or exemplary damages resulting, in whole or part, from the readers' use of, or reliance upon, this material.

Printed in the United States of America
Print Number: 01 Print Year: 2022

Brief Contents

Contents

Chapter 1

Chapter 2

Chapter 7

Chapter 8

Chapter 9

Chapter 11

Chapter 12

Appendix A

Dedication

In memory of Curt M. White

Preface

Today's business world could not function without data communications and computer networks. Most people cannot make it through an average day without encountering or using some form of computer network. In the past, this field of study occupied the time of only engineers and technicians, but it now involves business managers, end users, programmers, and just about anyone who might use a phone or computer! Thus, *Data Communications & Computer Networks: A Business User's Approach*, Ninth Edition maintains a business user's perspective on this vast and increasingly significant subject.

In a generic sense, this book serves as an owner's manual for the individual computer user. In a world in which computer networks are involved in nearly every facet of business and personal life, it is paramount that each person understands the basic features, operations, and limitations of different types of computer networks. This understanding helps people become better managers, better employees, and simply better computer users. As a computer network *user*, you will probably not be the one who designs, installs, and maintains the network. Instead, you will have interactions—either direct or indirect—with the individuals who do. Taking this course should give you a strong foundation in computer network concepts, which will enable you to work effectively with network administrators, network installers, and network designers. Here are some of the many scenarios in which the knowledge contained in this book would be particularly useful:

- You work for a company and must deal directly with a network specialist. To better understand the specialist and be able to conduct a meaningful dialog with them, you need a basic understanding of the many aspects of computer networks.
- You are a manager within a company and depend on network specialists to provide you with recommendations for the company's network. To ensure that you can make intelligent decisions regarding network resources, you need to know the basic concepts of data communications and computer networks.
- You work in a small company, in which each employee wears many hats. Thus, you may need to perform some level of network assessment, administration, or support.
- You have your own business and need to fully understand the advantages of using computer networks to support your operations. To optimize those advantages, you should have a good grasp of the basic characteristics of a computer network.
- You have a computer at home or at work, and you simply wish to learn more about computer networks.
- You have realized that, to keep your job skills current and remain a key player in the information technology arena, you must understand how different computer networks work and become familiar with their advantages and shortcomings.

Audience

Data Communications & Computer Networks: A Business User's Approach, Ninth Edition is intended for a one-semester course in business data communications for students majoring in business, information systems, management information systems, and other applied fields of computer science. Computer science departments will also find the book valuable, particularly if the students read the Details sections accompanying most chapters. It is a readable resource for computer network users that draws on examples from business environments. In a university setting, this book can be used at practically any level above the first year.

Defining Characteristics of This Book

The major goal of this ninth edition is the same as that of the first edition: to go beyond simply providing readers with a handful of new definitions, and instead introduce them to the next level of details found within the fields of computer networks and data communications. This higher level of detail, framed within the context of real-world scenarios, includes the network technologies and standards necessary to support computer network systems and their applications. This book is more than just an introduction to advanced terminology. It involves introducing concepts that will help the reader achieve a more in-depth understanding of the often-complex topic of data communications. Hands-on projects provide memorable insights into the concepts, and pedagogical features help readers assess their own learning and progress. It is hoped that once readers attain this in-depth understanding, the topic of networks and data communications will become engaging in the pursuit of business objectives. To facilitate this understanding, the book strives to maintain high standards in three major areas: readability, a balance between the technical and the practical, and currency.

Readability

Great care has been taken to provide the technical material in as readable a fashion as possible. Each new edition has received a complete rewrite, in which every sentence has been reexamined to convey the concepts as clearly as possible. Given the nature of this book's subject matter, the use of terminology is unavoidable. However, every effort has been made to present terms in a clear fashion, with minimal use of acronyms and even less use of jargon.

Balance between the Technical and the Practical

As in the very successful first edition, a major objective in writing *Data Communications & Computer Networks*, Ninth Edition was to achieve a balance between the more technical aspects of data communications and its everyday practical aspects. Throughout each chapter, there are sections entitled "Details," which delve into the more specialized aspects of the topic at hand. Should readers not have time to explore this technical information, they can skip these Details sections without missing out on the basic concepts of covered topics.

Current Technology

Because of the fast pace of change in virtually all computer-related fields, every attempt has been made to present the most current trends in data communications and computer networks. Some of these topics include:

- Integral coverage of cloud computing, especially from a business perspective
- An introduction to many new terms and concepts such as: IoT (Internet of Things), 5G (5th generation) cellular, SDN (software-defined networking), SD-WAN (software-defined wide area networking), data analytics, and AI (artificial intelligence)
- The most recent Wi-Fi standards of 802.11ac and 802.11ax
- Technologies to support remote workers
- Industry standards for cloud security

It is also important to remember the many older technologies still in prevalent use today. Discussions of these older technologies can be found, when appropriate, in each chapter of this book.

Organization

The organization of *Data Communications & Computer Networks*, Ninth Edition roughly follows that of the TCP/IP protocol suite, from the physical layer to the upper layers. In addition, the book has been carefully designed to consist of twelve, well-balanced chapters to fit into a typical 15- or 16-week semester (along with any required exams). The intent was to design a versatile introduction to the study of computer networks by creating a set of chapters that is cohesive but at the same time allows for flexibility in the week-to-week curriculum. Thus, instructors may choose to emphasize or de-emphasize certain topics, depending on the focus of their curriculums.

Coverage of CompTIA's Cloud Essentials+ exam objectives are deeply integrated into the material so that every objective is covered to or beyond the level required by the exam. Students who are taking this course and who engage in final exam preparation activities (such as review and practice testing) will be qualified to attempt the CompTIA Cloud Essentials+ certification exam. This exam sits at the crossroads of business and technology in cloud computing and encourages a common language for professionals from both areas of expertise.

Students who have taken other cloud computing courses, such as a course that covers CompTIA's more technical Cloud+ exam, can study Chapters 11 and 12 in preparation for the Cloud Essentials+ exam. These chapters focus on addressing the business-based language and concerns of cloud computing.

Features

To assist readers in better understanding the technical nature of data communications and computer networks, each chapter contains several significant features. These features are based on established, well-tested pedagogical techniques as well as some newer techniques.

Learning Objectives

The chapter opens with a list of learning objectives that should be accomplished by the end of the chapter. Each objective is tied to the main sections of the chapter. Readers can use the objectives to grasp the scope and intent of the chapter's content. The objectives also work in conjunction with the end-of-chapter summary and review questions, so that readers can assess whether they have adequately mastered the material.

Section Reviews

Each major section in each chapter concludes with a brief review of the main points students should remember from that section. This frequent review process helps students reflect on the material they've learned before moving on to the next section.

Self-Check Questions

Following the section review, self-check questions encourage students to practice recalling the information they've learned. This practice testing is proven in learning science research as one of the most effective methods to retain new information. Answers and explanations are provided for students at the end of each chapter so they can check themselves and identify gaps in their learning before moving forward.

Thought Experiments

Thought experiment boxes sprinkled throughout the reading invite students to consider a personal or business application of the concepts being discussed. These activities sometimes require outside research, and other times students draw upon their personal experiences and opinions.

Details

Most chapters contain one or more Details sections, which dig deeper into a particular topic. Readers who are interested in more technical details will find these sections valuable. Since the Details sections are physically separate from the main text, they can be skipped if the reader does not have time to explore this level of technical detail. Skipping these sections will not affect the reader's overall understanding of a chapter's material.

CompTIA Cloud Essentials+ Objectives Mapping

Where relevant, covered exam objectives are referenced within a section to support self-study efforts. All the exam objectives for the CompTIA Cloud Essentials+ certification are covered within this book at or beyond the level required by the exam.

End-of-Chapter Material

The end-of-chapter material is designed to help readers review the content of the chapter and assess whether they have adequately mastered the concepts. It includes:

- A bulleted summary that readers can use as a review of the key topics of the chapter and as a study guide.
- A list of the key terms used within the chapter.
- Review questions that readers can use to quickly check whether they understand the chapter's key concepts.
- A discussion starter designed to encourage readers to reflect on what they've learned in the chapter and how these topics might affect daily life, businesses and markets, and work processes in various industries.
- A Hands-On Project that gives students concrete experience with concepts from the chapter. These projects are carefully designed to work as effectively for a distance-learning student as for a student in the classroom. None of the projects require significant preparation beforehand for the instructor, hardware beyond a typical workstation or laptop, or paid subscriptions to any other service.

Glossary

At the end of the book, you will find a glossary that includes the key terms from each chapter.

New to This Edition

Just as networking technology continues to evolve, so does learning science and the insights available to course designers. In the interest of providing you with the most effective and durable learning experience, this latest edition is packed with improvements and enriched features.

- **Fully updated—**Content maps completely to CompTIA's Cloud Essentials+ CLO-002 exam for productive exam preparation.
- **"Remember this…" feature—**Section-specific learning objectives blend the Cloud Essentials+ exam objectives with the material covered in each section to help students focus on the most important points of that section.
- **Self-check questions—**Periodic multiple-choice questions placed throughout the readings help students mentally complete the "learning cycle" as they practice recalling the information to increase the durability of what they learn. With answers and thorough explanations at the end of each chapter, students can check their own learning and assess their progress toward mastering each chapter's objectives.
- **Flexible learning environment—**New skills-based projects encourage hands-on exploration of chapter concepts. These projects include thought-provoking questions that encourage critical thinking and in-depth evaluation of the material. The software tools used in the projects are included in Windows or freely available online, and hardware requirements are kept to a minimum, making these projects accessible to more students in a wide variety of learning environments.
- **Cloud, virtualization, and emulation technologies—**Projects at the end of each chapter challenge readers to explore concepts and apply skills with real-world tools. Some projects employ Cisco's network simulator, Packet Tracer, so learners can practice setting up a network from start to finish. Other projects guide students in accessing AWS so they can "get their hands dirty in the cloud" and discover why IT as an industry is becoming cloud-centric.
- **Certification preparation—**All exam objectives for the CompTIA Cloud Essentials+ certification are covered to or beyond the depth required by the exam. The CompTIA Cloud Essentials+ certification addresses the crossroads of business and technology in cloud computing. Training for the exam provides experts on both sides with a common language to encourage partnership and collaboration as companies increasingly migrate to the cloud.

Chapter Descriptions

To keep up with new technology in computer networks and data communications, this Ninth Edition has incorporated many updates and additions in every chapter, as well as some reorganization of sections within chapters. Here's a summary of the major concepts that can be found in each of the following chapters:

Chapter 1, Introduction to Data Communications and Computer Networks, introduces different types of computer networks, along with many of the major concepts that will be discussed in the following chapters, with an emphasis on the TCP/IP protocol suite followed by the OSI model. Cloud computing is introduced in this first chapter and is revisited in-depth in subsequent chapters.

Chapter 2, Conducted and Radiated Media, introduces the different types of wired and wireless media for transmitting data on personal and local area networks. Coverage of Wi-Fi, Bluetooth, and wireless IoT (Internet of Things) technologies reflects updated standards and evolution of wireless media.

Chapter 3, Fundamentals of Data and Signals, covers basic concepts describing how data is converted to signals for transmission on a network. Later chapters build on these concepts so students understand how to increase network performance and efficiency.

Chapter 4, Frames and Errors, discusses how a connection or interface is created between a computer and a peripheral device. The chapter explores types of noise and the errors they cause, how these errors are detected, and the actions that can take place in response to errors.

Chapter 5, Wired and Wireless Local Area Networks, explains the evolution of topology and Ethernet standards in wired local area networks, emphasizing the role a switch plays in modern networks. The chapter then describes standards used to handle collisions on wireless networks.

Chapter 6, Network Systems and Software, discusses various network services and the network operating systems that support them. New content discusses how to configure network devices and explains the concept and role of virtualization. The chapter concludes with new content explaining cloud computing services and pricing strategies.

Chapter 7, The Internet, is devoted to technologies that make the Internet work. The chapter covers IPv4 and IPv6 protocols and addressing as well as TCP, UDP, and a brief discussion of MPLS. It also discusses Internet services, such as DNS, SSH, and VoIP, and it presents new content on the IoT (Internet of Things) and data analytics.

Chapter 8, Risk, Security, and Compliance, addresses common network vulnerabilities and attack types, including updated information on ransomware and phishing emails. The chapter explains network security technologies, from physical security and anti-malware to firewalls and IDS/IPS. Encryption processes and uses are explained along with an updated discussion of authentication measures. The chapter concludes with a section devoted to wireless security.

Chapter 9, Wide Area Networks, introduces the basic terminology and concepts of campus area networks, metropolitan area networks, and wide area networks. Routing processes and common routing protocols are explored, followed by discussions on multiplexing and compression in wide area networks.

Chapter 10, Connecting Networks and Resources, delves into the details of how local networks connect to the Internet. The chapter includes DSL, cable modems, fiber, satellite, and cellular connections for consumer-level services and MPLS, Ethernet, VPN, and cloud connectivity for enterprise-grade connections. New content on SD-WAN, SD-Branch, and SASE helps prepare students for the CompTIA Cloud Essentials+ certification exam. And coverage of digital marketing, edge computing, and supporting remote workers prepares students for working in today's Internet-based businesses.

Chapter 11, Network Design and Management, introduces application lifecycle management, change management, and project management. In the context of creating or improving networks, the chapter explores network modeling, gap analysis, feasibility studies, capacity planning, and testing environments. A section on network monitoring covers monitoring tools and the importance of baseline studies. The chapter concludes with new content on cloud deployment and migration concepts, including migration strategies, automation/orchestration, and cloud monitoring.

Chapter 12, Business Principles in IT, offers new content addressing a network's human resources, including the need for administrative and training skills in addition to ongoing professional development. The next section focuses on relationships with vendors, important vendor documentation, and methods for evaluating proposed projects with vendors. New content covers financial aspects of the cloud, including a comparison of CapEx versus OpEx and a discussion of cloud cost optimization. The final section addresses business continuity and disaster recovery planning.

Instructor Resources

Additional instructor resources for this product are available online. Instructor assets include an Instructor's Manual, PowerPoint® slides, and a test bank powered by Cognero®. Sign up or sign in at www.cengage.com to search for and access this product and its online resources.

Acknowledgments

This book has been a long time coming. Through delays, multiple schedule rearrangements, the 2020 quarantines, and team members being promoted to other responsibilities, this edition has now come to fruition. I believe this is good timing—as the demand for cloud skills increases so does the perception of cloud as an integral part of IT.

Many people contributed to the production of this book, and many more helped move it along before the official drafting process began. I'd like to thank Emily Pope for her vision of blending this book's network instruction in a business context with CompTIA's business-centered cloud computing certification. I'm grateful for Staci Eckenroth's high standards in editing the drafts and ensuring inclusive language that shows the inherent value of people in all walks of life. And thank you to Jennifer Ziegler for picking up the reins of this project from others to see it through.

The work I do is only possible through the support and encouragement of my husband, Mike, and our four kids: Winn, Sarah, Daniel, and Zack. Thank you to each of you for the unique ways you each contribute. And finally, a special thanks to each of my students—your curiosity, struggles, dreams, and hard work fuel my passion for teaching and for writing. I'm grateful to play a part in your journey.

Chapter 1

Introduction to Data Communications and Computer Networks

Objectives

After reading this chapter, you should be able to:

- Use common networking terms
- Identify basic networking devices
- Describe common types of networks
- Describe the purpose of each layer of the TCP/IP protocol suite and the OSI model
- Explain the significance of cloud computing

Introduction

Making predications is a difficult task, and predicting the future of computing is no exception. History is filled with computer-related predictions so inaccurate that today they are amusing. For example, consider the following predictions:

> "I think there is a world market for maybe five computers."
> *Thomas Watson, chairman of IBM, 1943*

> "I have traveled the length and breadth of this country, and talked with the best people, and I can assure you that data processing is a fad that won't last out the year."
> *Editor in charge of business books for Prentice Hall, 1957*

> "There is no reason anyone would want a computer in their home."
> *Ken Olsen, president and founder of Digital Equipment Corporation, 1977*

Apparently, no matter how famous you are or how influential your position, it is very easy to make very bad predictions. Nevertheless, it's hard to imagine that anyone can make a prediction worse than any of those above. Buoyed by this false sense of optimism, consider these forecasts:

> Someday your home's heating and cooling system will automatically turn off when it detects you leaving home, turn on when it detects you're heading back, adjust its settings according to your daily activities and current energy prices, and shut down completely if it detects smoke in the house.

At some point, a hacker manages to steal your banking password and log into your online bank account, but the attack is detected and booted from your account before any damage is done because he didn't move his mouse the same way you do.

Someday your car battery will be capable of detecting when the power gets too weak to start the car, and it will call to inform you that you need a replacement or a charge.

One day you will use an app on your phone to request personal transportation. The app will show you the car's photo, provide a map of the car's current location, and you'll be notified when the car arrives at your location. However, when you enter the car, there will be no driver because the car drives itself.

Someday while driving in a big city, your car will navigate you to the nearest empty parking spot and allow you to pay the parking fee with your phone.

Do these predictions sound far-fetched and filled with mysterious technologies that only scientists and engineers can understand? They shouldn't because these scenarios are happening today with technologies that already exist. What's more, none of these advances would be possible today were it not for computer networks and data communications.

The world of computer networks and data communications is a surprisingly vast and increasingly significant field of study. Once considered primarily the domain of network engineers and technicians, computer networks now involve business managers, computer programmers, system designers, office managers, home computer users, and everyday citizens.

It is virtually impossible for the average person on the street to spend 24 hours without directly or indirectly using some form of computer network. Consider all the ways you might interact with computer networks when you're literally on the street: Most transportation systems use extensive communication networks to monitor the flow of vehicles and trains. Expressways and highways have computerized systems for controlling traffic signals and limiting access during peak traffic times. Some major cities are placing the appropriate hardware inside city buses and trains so that the precise location of each bus and train is known. This information enables transportation systems to keep buses evenly spaced and more punctual, and it allows riders to know when the next bus or train will arrive.

In addition, more people are using satellite-based GPS devices in their cars and on smartphones to provide driving directions and avoid traffic hotspots. Similar systems can unlock your car doors if you leave your keys in the ignition or can locate your car in a crowded parking lot by beeping the horn and flashing the headlights if you cannot remember where you parked.

Even if you didn't use public transportation today or a GPS device in your car to commute to work, school, or the store, there are many other ways to use a computer network. Businesses can order parts and inventory on demand and build products to customer-designed specifications electronically, without the need for paper. Online retail outlets can track every item you click on or purchase. Using this data, they can make recommendations of similar products and inform you in the future when a new product becomes available. ATMs can verify a user's identity by taking their thumbprint. Plus, many employees and students now work from home, relying heavily on data networks to access remote resources for work, school, and socializing.

To support current demands for network connectivity, cable television continues to expand, offering extensive programming, pay-per-view options, video recording, digital television and music, and (in some markets) gigabit connectivity to the Internet. The telephone system, the oldest and most extensive network of communication devices, continues to become more of a computer network every day. The most recent "telephone" networks can now deliver voice, Internet, and television over a single connection. Cellular telephone systems cover virtually the entire North American continent and include systems that allow users to upload and download data to and from the Internet, send and receive images, and upload or download streaming video such as television programs, movies, web conferences, and social media videos. Your smartphone can play music, make phone calls (even video calls), take pictures, browse the web, and let you play games while you wait for the next train, class, or appointment.

Welcome to the amazing world of computer networks! As you can see, it is nearly impossible to not have used some form of computer network and data communication. Because of this growing integration of computer networks and data communications into business and daily life, everyone—particularly those considering careers in information systems, business, or computer science—needs to understand the basic concepts. Armed with this knowledge, you not only will be better at communicating with network specialists and engineers, but also will become better students, managers, and employees.

Section 1-1: The Language of Computer Networking

Over the years, numerous terms and definitions relating to computer networks and data communications have emerged. To gain insight into the many subfields of study, and to become familiar with the emphasis of this textbook, take a moment to examine the more common terms and their definitions:

- A **computer network** is an interconnected group of computers and computing equipment using either wires or radio waves that can share data and computing resources.
- **Wireless** computer networks use different kinds of low energy radiation below the visible light spectrum and can involve broadcast radio, microwaves, or infrared transmissions.
- Networks spanning an area of a few centimeters to several meters around an individual are called **PANs (personal area networks)**. PANs include devices such as laptop computers, smartphones, personal printers, and wireless peripheral devices (like a keyboard or speakers) that are typically used by one person at a time. A PAN can also include wearable devices, such as a smartwatch or smart glasses, although sometimes these devices are considered to be part of a BAN (body area network).
- Networks that are a little larger in geographic size—spanning a room, a floor within a building, or an entire building—are **LANs (local area networks)**. Figure 1-1 shows the relative sizes of PANs, LANs, and other common network types described here.
- Collections of local area networks that cover a campus (such as a college campus or a business campus) are often called **CANs (campus area networks)**.
- Networks that serve an area up to roughly 50 kilometers—approximately the area of a typical city—are called **MANs (metropolitan area networks)**. Metropolitan area networks are high-speed networks that interconnect businesses with other businesses and the Internet.
- Large networks encompassing parts of states, multiple states, countries, and the world are **WANs (wide area networks)**.

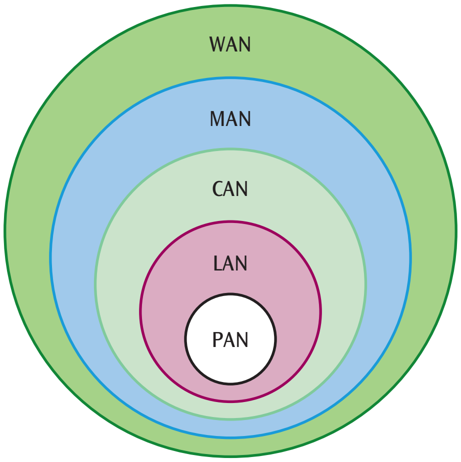


Figure 1-1 Relative sizes of common network types

There are many other terms you'll see repeatedly throughout this course. To put these terms in context, let's peruse the highlights of the coming chapters. It helps to think of the progression of these chapters in terms of how each chapter relates to a company's LAN, either internal to the LAN or external to it. For example, Chapters 2 through 6 concentrate on technologies used on LANs. Chapter 7 expands the discussion to see how networks function outside of the LAN environment, and Chapter 8 covers key security concepts when considering threats from outside the LAN. As you move away from the LAN, you find that several technologies can connect your network with other networks or with extensions to your own network. You'll learn about how WANs work in Chapter 9, and you'll discover many of the more common WAN connection types in Chapter 10. Let's take a more detailed look at what you can expect to learn during this course and some of the core vocabulary you'll be using.

The study of computer networks would be inadequate without the introduction of two important building blocks: data and signals. Data is information that has been translated into a form conducive to storage, transmission, and calculation. **Data communications** is the transfer of digital or analog data using digital or analog signals. Analog and digital signals are transmitted over conducted media or wireless (also called radiated) media, both of which are discussed in Chapter 2. These media are the foundational component of every network. Next, Chapter 3 evaluates how data is transformed into signals that can be transmitted on various network media.

Signals transmitted on a network must be formatted according to certain sets of rules, called **protocols**, a topic covered in Chapter 4. When the signals transmitted between computing devices are corrupted and errors result, error detection and error control are necessary. These topics are also discussed in detail in Chapter 4.

Many kinds of devices are needed to support network -based communications, such as switches and routers. Chapter 5 describes the different ways these *networking* devices (i.e., devices used to support the network) can be arranged to allow *networked* devices (i.e., devices using the network) to talk to each other. Then Chapter 6 evaluates the services and software used to manage the network, such as a NOS (network operating system), and Chapter 7 shows how you can connect your network to other networks using specialized networking protocols that enable communication across the Internet. As you open your network to the world, you need to keep it safe. Chapter 8 surveys common risks to your network and network security best practices that protect your network and your data when you're connected to the Internet.

Because sending only one signal over a medium at one time can be an inefficient way to use the transmission medium, many systems perform multiplexing. **Multiplexing** is the transmission of multiple signals on one medium, which is necessary with high-traffic connections like those that make up the Internet. For a medium to transmit multiple signals simultaneously, the signals must be altered so that they do not interfere with one another. **Compression** is another technique that can maximize the amount of data sent over a medium. Compression involves squeezing data into a smaller package, thus reducing the amount of time (as well as storage space) needed to transmit the data. Multiplexing and compression are covered in Chapter 9. Next, Chapter 10 shows how these techniques are used in different WAN technologies that connect your local network to the Internet and other remote networks.

Network management is the design, installation, and support of a network and its hardware and software. Chapter 11 discusses many of the basic concepts necessary to properly support the design and improvement of network hardware and software, as well as the more common management techniques used to optimize a network's performance.

A very common expression you may have heard is something like "back up your photos and documents to the cloud" or "the application is in the cloud." The key concept here is **cloud** and the way this term is currently used. Similar words or phrases that are commonly used today are **cloud computing** or ***Anything* as a Service (XaaS)**, where the *X* can be replaced with other letters to refer to a particular service, such as SaaS (Software as a Service) or NaaS (Networking as a Service). Very often "the cloud" simply refers to the Internet or to some other remote network. When a company places data or applications on some website on the Internet and allows people to access them, you might say the application is cloud-based. One of the more visible examples of cloud computing is storing one's music and files at a remote location on the Internet rather than on a local device. Major corporations such as Amazon and Apple allow users to store personal data and recent media purchases on their clouds. Companies such as Microsoft and Google (as well as many others) offer cloud-based applications (called **web apps**) such as word processors and spreadsheets. The actual code that runs the web app does not exist on the user's computer but runs on the cloud provider's servers and is typically accessed across the Internet through the user's browser. This way, users don't have to download and install the application to an individual machine. You will examine cloud concepts in more detail throughout this course and specifically from a business perspective in Chapter 12.

Cloud Essentials+ Exam Tip

This course covers all the objectives for the CompTIA Cloud Essentials+ CLO-002 certification. Look for these Cloud Essentials+ Exam Tips to indicate which objectives are addressed in a section.

Remember this…

- Networks are often categorized according to their size and the types of devices connected to them.
- The study of data communications includes digital and analog signals that can be transmitted over conducted or wireless (radiated) media.
- Cloud computing often relies on the Internet in some way for access to resources at a remote location.

Self-check

1. You plug your new printer into a USB port on your computer. What kind of network supports this connection?
   a. CAN
   b. LAN
   c. WAN
   d. PAN

2. You connect your home network to your Internet provider using a single fiber cable. What technology allows you to download and upload data over this connection at the same time?
   a. Network management
   b. Multiplexing
   c. Compression
   d. Cloud computing

Check your answers at the end of this chapter.

Section 1-2: The Big Picture of Networks

If you could create one picture that tries to give an overview of a typical computer network, what might this picture include? Figure 1-2 shows one possibility. Note that this figure shows two wide area networks (WAN 1 and WAN 2), two local area networks (LAN 1 and LAN 2), and a personal area network. Although a full description of the different components constituting wide area and local area networks is not necessary quite yet, it is important to note that most LANs often include the following hardware:

- **Workstations**—Personal computers (such as desktops, laptops, or tablets) or smartphones
- **Servers**—The computers that store network software and shared or private user files
- **Switches**—The collection points for the wires that interconnect the workstations on a LAN
- **Routers**—The connecting devices between LANs and WANs, such as the Internet

There are also many types of wide area networks. Although many different technologies are used to support WANs, all WANs include the following components:

- **Nodes**—Devices connected to the network, including endpoint devices (such as servers) and networking devices (such as routers) that make the decisions about where to route a piece of data
- Connecting media—Some type of wired or wireless high-speed transmission infrastructure (such as cables or radio signals) that connects one node to another
- A **subnetwork**—Collection of nodes and transmission media working together in a cohesive unit

To see how LANs and WANs work together, consider User A (in the upper-left corner of Figure 1-2), who wishes to retrieve a web page from the web server shown in the lower-right corner. To do this, User A's computer must have both the necessary hardware and software required to communicate with the first WAN it encounters, WAN 1 (User A's Internet service provider).

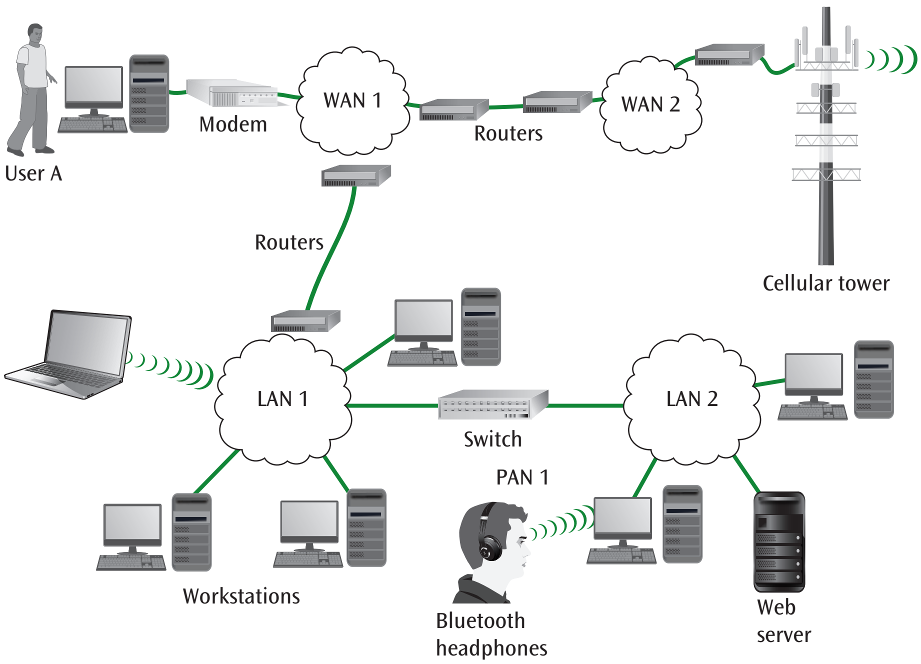


Figure 1-2 An overall view of the interconnection between different types of networks

Assuming that User A's computer is connected to this WAN through a DSL telephone line, User A needs some type of modem. Furthermore, if this WAN is part of the Internet, User A's computer requires software that speaks the language of the Internet: TCP/IP (Transmission Control Protocol/Internet Protocol).

Notice that no direct connection exists between WAN 1, where User A resides, and LAN 2, where the web server resides. To ensure that User A's web page request reaches its intended receiver (the web server), User A's software attaches the appropriate address information that WAN 1 needs to send User A's request to the router that connects WAN 1 to LAN 1. Once the request is on LAN 1, the node connecting LAN 1 and LAN 2 uses address information to pass the request to LAN 2. Additional address information then routes User A's web page request to the web server, whose software accepts the request.

Under normal traffic and conditions, this procedure might take only a fraction of a second. When you begin to understand all the steps involved and the great number of transformations that a simple web page request must undergo, the fact that it takes *only* a fraction of a second to deliver is amazing.

Remember this...

- LANs connect devices to each other using switches and connect to other networks using routers.
- WANs connect networks to each other using routing devices and are organized into groups of nodes called subnetworks.
- Specialized hardware and software are required for a workstation to communicate over a network such as the Internet.
- Addressing information is used to route information across a network.

Self-check

3. You plug your laptop into your local network's router and use your browser to visit a website. What type of device allows your router to communicate with your Internet provider's network?
   a. Switch
   b. Modem
   c. Server
   d. Subnetwork
4. You need to make some changes to a file stored on your office's network. On which device is the file located?
   a. Router
   b. Server
   c. Workstation
   d. Switch

Check your answers at the end of this chapter.

Section 1-3: Common Network Examples

The introduction of this chapter described a few applications of computer networks and data communications in everyday life. Think about the basic communications networks that you might encounter on any typical day while at school, at work, or living life in general. This will help you see how extensively you rely on data communications and computer networks. In Figure 1-3, Katrina is sitting at a desk at her college library. On the desk are two computers: a desktop PC (provided by the school) and her personal laptop. She is holding her smartphone. Try to identify each of the communications networks that Katrina might encounter in this scenario.

The Desktop Computer and the Internet

The desktop computer sitting on Katrina's desk is "connected" to the Internet via a cable at the back. ("Connected" was placed in quotations because, as this book will hopefully demonstrate, it is an intricate process to enable a device to communicate with other devices across the Internet and involves much more than simply plugging a cable into the computer's Internet port.) This is perhaps the most common network connection today and is found in virtually every business, every academic environment, and in many homes. The desktop computer—which is commonly known as the personal computer, PC, microcomputer, or workstation, and could also be a laptop or notebook—began to emerge in the late 1970s and early 1980s.

In a business or education environment, the Ethernet cable plugging the desktop into a wall jack travels through the walls to some collection point, such as a network switch. This network switch, as you will learn in Chapter 5, is part of a local area network. This LAN is possibly connected to other LANs, but eventually

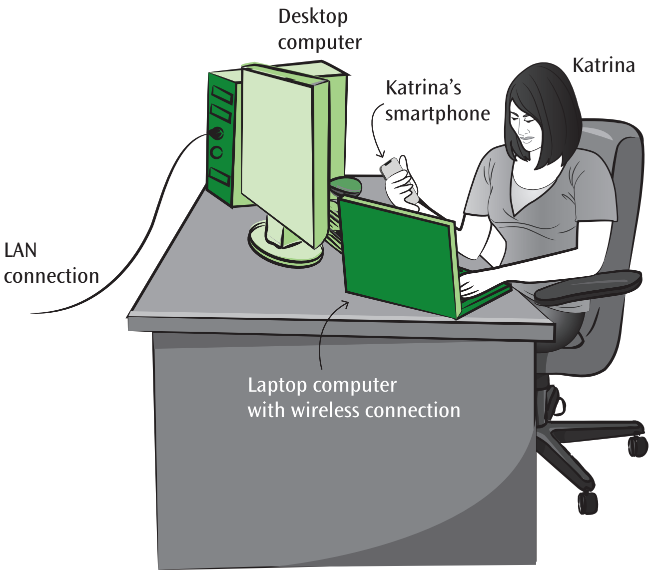


Figure 1-3 Katrina sitting at a desk at school, surrounded by networks and their connections

connects to a router. From the router, there is some form of high-speed connection to a site which specializes in high-speed connections to the Internet.

The LAN, as you'll see in Chapter 6, is an excellent tool for providing a connection to the Internet, as well as to other networks, software, and peripheral devices. In the business and education world, this network is called an **enterprise network** or a corporate network. The connection between workstations and the Internet in an enterprise network is handled by a client/server system. In a **client/server system**, a user at a computer, called the client machine, issues a request for some form of data or service. This could be a request for a database record from a database server, a request for a web page from a web server, a request for a file from a file server, or a request to retrieve an email message from an email server. If the requested data is stored locally, the request travels across the local system to a local server. If the requested data is stored remotely, the request travels across the local system and then onto an external network, such as the Internet, to a remote server that contains a potentially large repository of data and/or applications. The remote server fills the request and returns the results to the client, displaying the results on the client's monitor. If users wish to print documents on a high-quality network printer, the LAN contains the network software necessary (a print server) to route their print requests to the appropriate printer. If users wish to access their email, the LAN provides a fast, stable connection between user workstations and the email server. If a user wishes to access the Internet, the LAN provides an effective gateway to the outside world. Figure 1-4 shows a diagram of this type of desktop-to-Internet connection.

Earlier, you met Katrina studying at her school library. What about connecting her personal computer to the Internet when she studies at home? Many years ago, most home users connected their computer to the Internet via a dial-up telephone line and a modem. Today, most home users either connect to the Internet using DSL (digital subscriber line) or a cable modem service, which is connected to a home router. DSL and cable modems can achieve much higher connection speeds (or data transfer rates) than dial-up connections, which are rarely used anymore. The home router functions as both a router and a switch, and it allows multiple devices to connect to the Internet at one time.

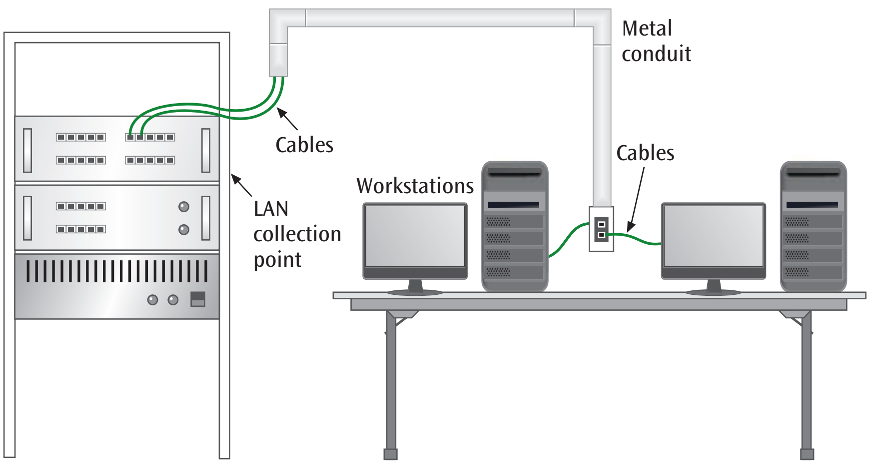


Figure 1-4 A desktop computer (or microcomputer) at a business or school connected from the user's desk to the company's local area network

To communicate with the Internet using a DSL or cable modem connection, a user's computer must connect to another device already communicating with the Internet. The easiest way to establish this connection is through the services of an ISP (Internet service provider). In this case, the user's computer needs to have the necessary software to communicate with the Internet. The Internet "talks" only in TCP/IP, so computers must have software that supports the TCP and IP protocols. Once the user's computer is talking TCP/IP, a connection to the Internet can be established. Figure 1-5 shows a typical home computer-to-Internet connection.

A Laptop Computer and a Wireless Connection

Back at the library, Katrina also has her laptop sitting on the desk. Many laptops do not connect to a network using a fixed wire but instead connect via a wireless connection. This type of network connection continues to grow in popularity. A user working with a laptop, tablet, or even a smartphone uses wireless communications (often called Wi-Fi) to send and receive data to and from a wireless access point (also called a wireless router). This access point is usually connected to a wired LAN and basically serves as the "bridge" between the wireless user device and the wired network. As you'll see in later chapters, there are different data communication protocols for wireless and wired LANs. While the flexibility of not having to physically cable your device to a wall jack is nice, you'll see there are also limitations as to how far the wireless signals can travel and how fast they can carry data.

Because both wireless and wired LANs are standard in business, academic, and many home environments, it should come as no surprise that having just one LAN is not going to get the job done. Many organizations need the services of multiple LANs, and it may be necessary for these networks to communicate with each other. For example, the school that Katrina attends may want the LAN that supports its chemistry department to share an expensive color laser printer with its biology department's LAN. Fortunately, it is possible to connect two LANs so that they can share peripherals (such as the printer) as well as software and files. Depending on the situation, you might use a switch or a router to connect two or more LANs or segments of LANs.

In some cases, it may be more important to *prevent* data from flowing between LANs than to allow data to flow from one network to another. For instance, some businesses have political reasons for supporting multiple networks—each division may want its own network to run as it wishes. Additionally, there may be security reasons for limiting traffic flow between networks; or allowing data destined for one network to traverse other networks simply may generate too much network traffic. The switches that connect LANs can help manage these types of services as well. For example, the switch can filter out traffic not intended for the neighboring network, thus minimizing the overall amount of traffic flow. This process of separating network traffic is called **segmentation**. Figure 1-6 provides an example of two LANs connected by two switches.

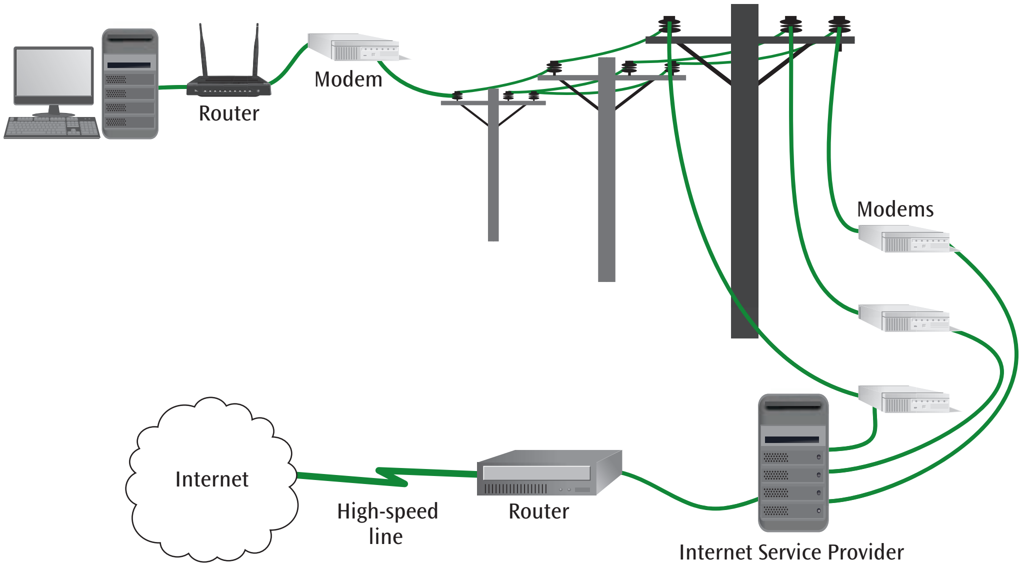


Figure 1-5 A computer sending data over a DSL line to an Internet service provider and onto the Internet

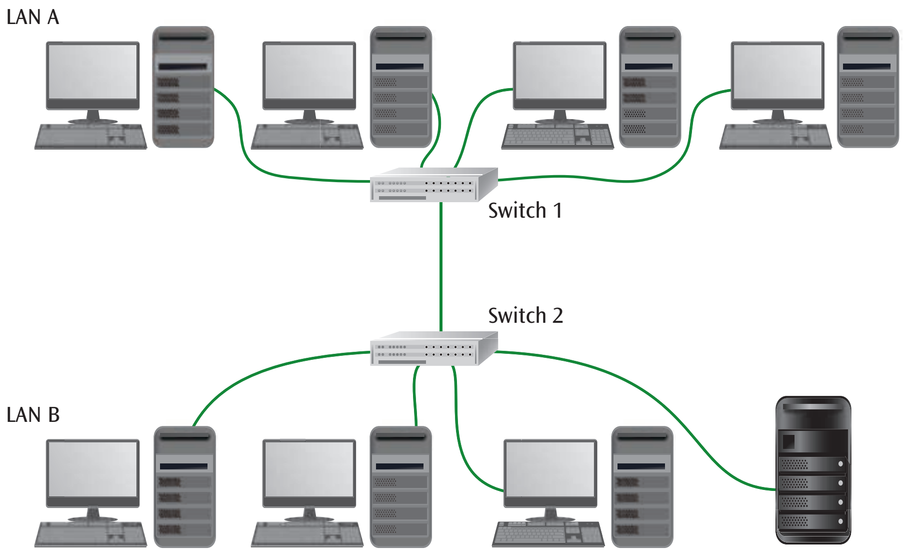


Figure 1-6 Two local area networks connected by switches

Cellular Network

While sitting in the library, Katrina can connect her smartphone to the Internet using Wi-Fi, but what if she needs to access her school email or assignments in a place where there is no Wi-Fi signal available? In this case, she can instead use a cell phone network, or cellular network.

One of the most explosive areas of growth in recent years has been cell phone systems. Originally, cell phones could only perform voice calls, but now your smartphone can send text messages, download pictures and videos from the Internet, stream music and video, and take high resolution photos and videos. The processing power built into modern smartphones rivals the mainframe computers of generations ago.

The network infrastructure that is needed to support modern smartphones has also increased in dramatic fashion. Large numbers of cell towers cover the face of North America and elsewhere throughout the globe. These cell towers are tied together into some form of network, allowing a user to send a text message all the way around the world. The data encoding technologies that support smartphones continue to increase in complexity so that users can access these networks at ever-increasing speeds.

For a more precise view, examine Figure 1-7. When a user talks into their smartphone, sends a text message or email, or interacts with a website, the data is transmitted across the cellular network to a telephone company building. The telephone company then transfers the smartphone's data over the public telephone network or through another high-speed connection onto the Internet.

All Things Considered

Thought Experiment

You've just taken a picture of your best friend with your smartphone. You decide to email it to a mutual friend across the country. List all the different networks possibly involved in this operation.

Other Common Network Systems

Cloud Essentials+ Exam Tip

This section discusses cloud deployment models, which is required by

- Part of Objective 1.1: Explain cloud principles.

The three sample networks you just viewed—a desktop computer connected to the Internet via a wired LAN, a laptop computer connected to the Internet via a wireless LAN, and a cellular network—are only a few of the many

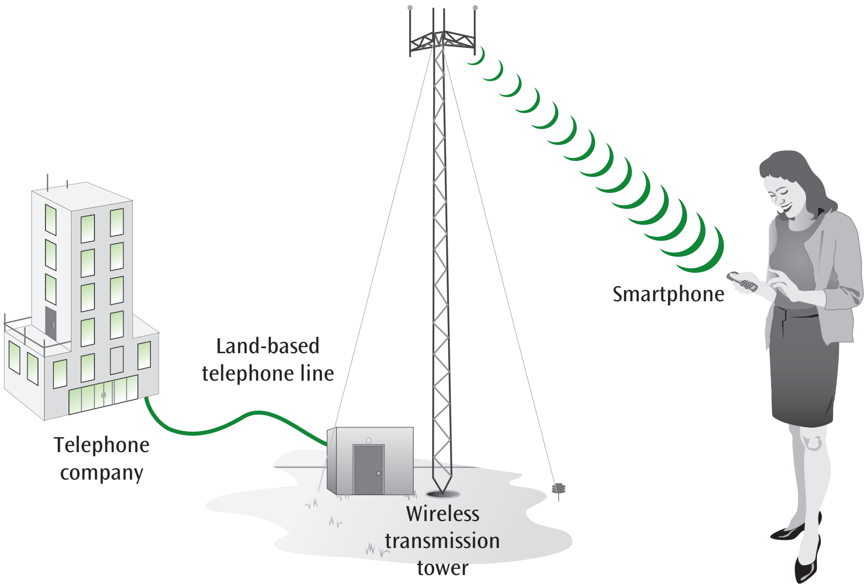


Figure 1-7 An example of a user with a smartphone transmitting and receiving data

examples of communication networks. Others that you will examine in more detail in later chapters include sensor networks, business mainframe networks, satellite networks, and cloud networks.

Sensor Networks

Sensor networks are often found in industrial and real-world settings. In this type of network, the action of a person or object triggers a sensor that is connected to a network. For example, in many left-turn lanes, a separate left-turn signal will appear if and only if one or more vehicles enter in the left-turn lane. A sensor embedded in the roadway detects the movement of a vehicle in the lane and triggers the left-turn mechanism in the traffic signal control box at the side of the road. If this traffic signal control box is connected to a larger traffic control system, the sensor is connected to a LAN.

Another example of a sensor network is found within manufacturing environments. Assembly lines, robotic control devices, oven temperature controls, moisture detection or water level controls, and chemical analysis equipment, often use sensors connected to data-gathering computers that control movements and operations, sound alarms, and compute experimental or quality control results. These sensors are often interconnected via one or more LANs. Figure 1-8 shows a diagram of a typical sensor network in a manufacturing environment.

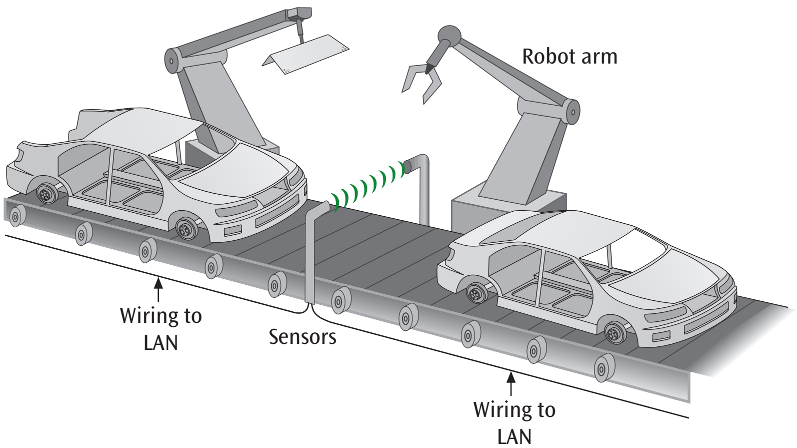


Figure 1-8 Automobiles move down an assembly line and trigger a sensor

Finally, don't forget all the sensor systems in people's homes and vehicles. Home appliances, such as washing machines, dryers, and dishwashers, include sensors to monitor water and air temperatures as well as water levels. Modern vehicles contain a myriad of sensors, monitoring fuel mixtures, oxygen levels, proximity detection, and wheel rotations (to trigger anti-lock brakes and anti-skid controls). Sensors and controllers have also been added to appliances such as refrigerators and thermostats so users can control these devices remotely through apps on their smartphones or through smart speakers. These speaker devices provide voice interaction with a digital assistant, such as Siri, Alexa, or Google. Smart appliances and other smart devices are part of the **IoT (Internet of Things).** While there is some debate on exactly what is included in the IoT, this textbook will refer to IoT specifically as devices that would not normally be considered computing devices (like kitchen appliances or door locks) but are connected to the Internet to allow for remote and/or voice activated control.

Business Mainframe Network

Another fairly common network system is the business mainframe network. Many businesses still use mainframe computers to support their day-to-day operations. To "connect" to a mainframe, a user employs hardware and software that makes their computer act as a computer terminal. A **computer terminal**, or terminal, consists of essentially a keyboard and screen with no large hard drives, no gigabytes of memory, and little, if any, processing power. Computer terminals are used for entering data into a system, such as a mainframe computer, and then displaying results from the mainframe. Because the terminal does not possess a lot of computing power, it's considered "dumb" and relies on the mainframe computer to control the sending and receiving of data to and from each terminal. This requires special types of protocols.

Business mainframe networks are still being used for inquiry/response applications, interactive applications, and data-entry applications. One example is the system that your bank might use to record ATM transactions from thousands of locations, as seen in Figure 1-9.

Satellite Networks

Satellite networks are continuously evolving technologies used in a variety of applications. If the distance between two networks is great and running a wire between them would be difficult, if not impossible, satellite transmission systems can be an effective way to connect the two networks or computer systems. Examples of these applications include digital satellite TV, meteorology, intelligence operations, mobile maritime telephony, GPS navigation systems, worldwide mobile telephone systems, and video conferencing. Figure 1-10 shows a diagram of a typical satellite system. You will examine these networks in more detail in Chapter 10.

Cloud Networks

Cloud networks connect resources that are said to reside "in the cloud." In reality, the cloud is essentially remote access to virtualized resources hosted in a software-defined environment. Let's break this down a little. **Virtualization** means that software is used

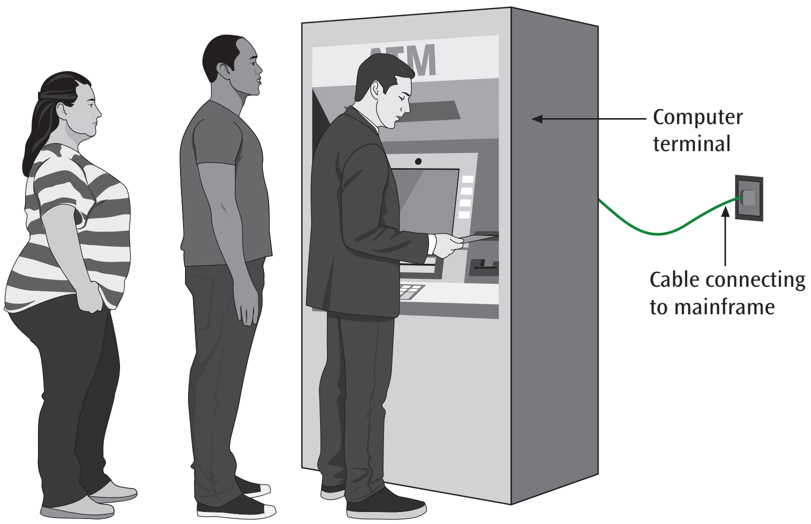


Figure 1-9 Using an ATM terminal (or thin-client workstation) to perform a financial transaction

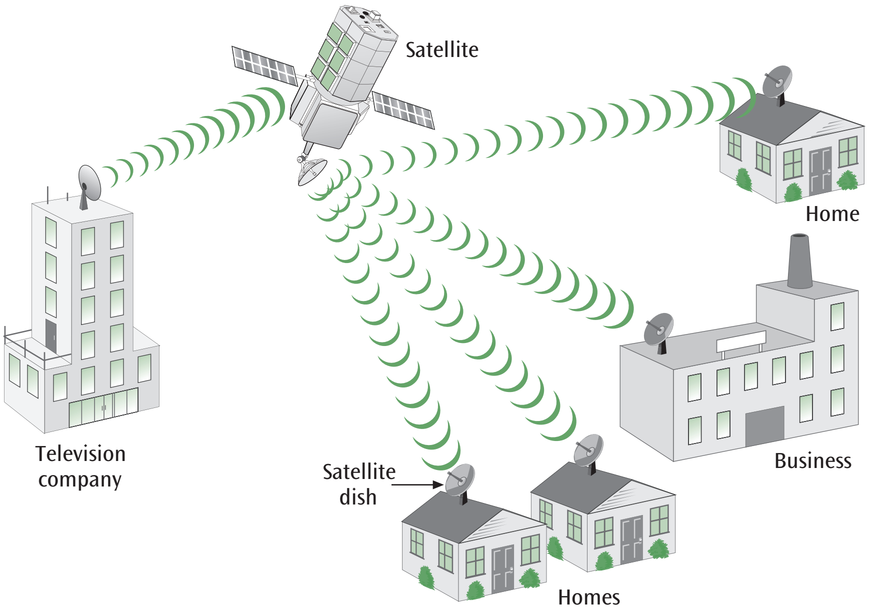


Figure 1-10 Example of a television company using a satellite system to broadcast television services into homes and businesses

to replicate the functions of hardware. For example, suppose you have a Windows computer like the one in Figure 1-11. You install virtualization software called a **hypervisor** on the Windows computer, and then you create a **virtual machine (VM)** in the hypervisor that functions as its own computer in a virtual environment. It needs its own OS (operating system), like Windows, or you can install a different OS, such as Linux. Figure 1-11 shows a Linux VM on the right where it's running on the Windows host computer. The hypervisor makes the Linux VM think it's the only computer running on the available hardware. The hypervisor allocates hardware resources to both the Linux VM and the Windows host.

A cloud network relies on a similar type of virtualization. A cloud hypervisor runs on top of a large collection of datacenter hardware, such as servers, routers, switches, and other devices. However, none of those physical devices are accessed directly by the cloud customer. The hypervisor abstracts the cloud network functions away from the physical devices so the customer only interacts with virtual resources, such as a virtual server. The cloud customer can create a new server VM, a process which is called "spinning up" a VM. From the customer's perspective, they're creating a new server that might run Linux or Windows or some other operating system. But the server is not an actual computer in

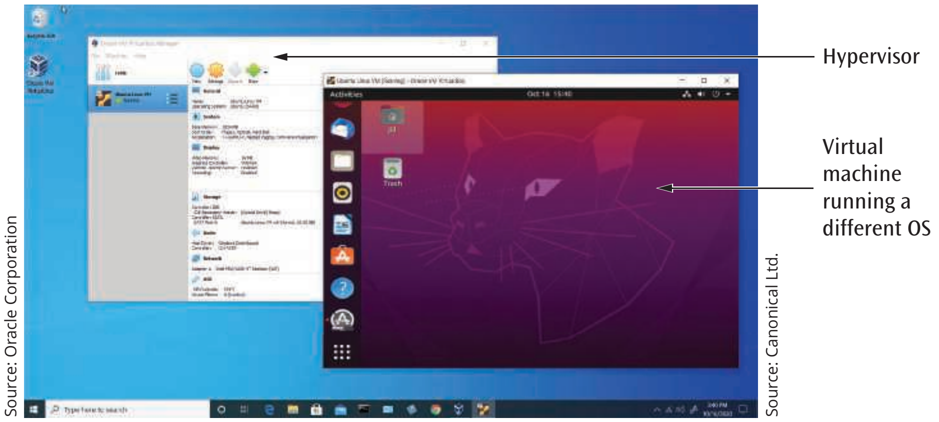


Figure 1-11 A Linux VM running in a hypervisor on a Windows computer

a rack—it's a virtual machine running in the hypervisor. The cloud network can run many other virtualized resources in the hypervisor, such as routing services or file storage services. You'll learn more about these service types later in this chapter.
Three primary types of cloud computing are as follows:

- **Public cloud**—These virtualized resources are hosted by a CSP (cloud service provider) at a remote location. While access control restrictions can protect these resources from unauthorized access, the hosting services can be used by anyone. For example, you might have files saved in a cloud storage service and only you can access them. However, thousands of other customers might use the same cloud storage service, and their files might be stored on the same physical server where your files are stored.
- **Private cloud**—These virtualized resources are hosted by the owner of the resources either in its own datacenter or at a remote location. The resources and the hosting services can only be accessed by the owner.
- **Hybrid cloud**—In a hybrid cloud, virtualized resources at a remote location and physical or virtual resources in the local datacenter are connected and interact at a functional level that is invisible to users. For example, you might sign into your computer at your desk, you open an application, and then you create and save a file. However, the application might be running on a server in your company's datacenter, and the file might be stored on a cloud-based server.

Cloud resources are collectively referred to as cloud computing, as you read earlier in this chapter. You'll learn more about cloud computing throughout this textbook.

Remember this…

- Many kinds of networks exist, depending on the connection technologies used, the types of communications the network supports, and the kinds of devices connected to the network.
- A client/server system provides client computers with a variety of services, such as a database, a web page, email, files, or printing.
- Protocols define the rules used by devices to communicate with each other over a network.
- Routers and switches can be used to connect devices across multiple LANs or segment traffic for security or traffic management purposes.
- Smartphones often rely on cellular networks to connect to the Internet and to provide calling and texting services.
- Other kinds of networks include sensor networks, wireless networks that use satellite technologies, and cloud networks that rely on virtualization.

Self-check

5. What kind of protocols support addressing and communication over the Internet?
   a. DSL
   b. TCP/IP
   c. LAN
   d. PC
6. You're setting up a small office network with a few desktop computers and a file server. You want to make sure only certain network users have access to the file server. What device will you need to configure to segment the network?
   a. Switch
   b. Cell phone tower
   c. Mainframe
   d. Router
7. Your school hosts its own cloud to provide students with virtual desktops. These desktops give students access to expensive software that most students couldn't afford to purchase on their own. Your school also stores student files in a cloud service that requires an Internet connection for students to access their files, even when they're on campus. What kind of cloud architecture is your school using?
   a. Public
   b. Enterprise
   c. Hybrid
   d. Private

Check your answers at the end of this chapter.

Section 1-4: Network Architectures

Now that you know the different types of networks, you need a framework to understand how all the various components of a network interoperate. When someone uses a computer network to perform a task, many pieces come together to assist in the operation. A **network architecture**, or communications model, places the appropriate network pieces in layers. The layers define a *model* for the functions or services that need to be performed. Each layer in the model defines what services either the hardware or software (or both) provides. The two most common architectures known today are the **TCP/IP protocol suite** and the **OSI (Open Systems Interconnection) model**. The TCP/IP protocol suite is a working model (currently used on the Internet), while the OSI model (originally designed to be a working model) has been relegated to a theoretical model. You will learn about these two architectures in more detail throughout the rest of this section. But first you should know a bit more about the components of a network and how a network architecture helps organize those components.

Consider that a typical computer network within a business contains the following components that must interact in various ways:

- Wires
- Printed circuit boards
- Wiring connectors and jacks
- Computers
- Centrally located wiring concentrators
- Storage drives
- Computer applications such as word processors, email programs, and software for accounting, marketing, and ecommerce
- Computer software that supports the transfer of data, checks for errors when the data is transferred, allows access to the network, and protects user transactions from unauthorized viewing

This large number of network components and their possible interactions inspires two questions. First, how do all these pieces work together harmoniously? You do not want two pieces performing the same function, or no pieces performing a necessary function. Like the elements of a well-oiled machine, all components of a computer network must work together to produce a product.

Second, does the choice of one piece depend on the choice of another piece? To make the pieces as modular as possible, you do not want the selection of one piece to constrain the options for another piece. For example, if you create a network and originally plan to use one type of wiring but later change your mind and use a different type of wiring, will that decision affect your choice of word processor? Such an interaction would seem highly unlikely. In contrast, can the choice of wiring affect the options for the protocol that checks for errors in the data sent over the wires? The answer to this question is not as obvious.

To keep the pieces of a computer network working together harmoniously, and to allow modularity between the pieces, national and international organizations developed network architectures, which are cohesive layers of protocols defining a set of communication services. Consider the following noncomputer example. Most organizations that produce some type of product or perform a service have a division of labor. Office assistants do the administrative work, accountants keep the books, laborers perform manual duties, scientists design products, engineers test the products, and managers control operations. Rarely is one person capable of performing all these duties. Large software applications operate the same way. Different procedures perform different tasks, and the whole system would not function without the proper operation of each of its parts. Computer network applications are no exception. As the size of the applications grows, the need for a division of labor becomes increasingly important. Computer network applications also have a similar delineation of job functions. This delineation is the network architecture. Now you're ready to examine the two network architectures or models in more detail: the TCP/IP protocol suite, followed by the OSI model.

The TCP/IP Protocol Suite

The TCP/IP protocol suite was created by a group of computer scientists to support a new type of network (the ARPANET) being installed across the United States in the 1960s and 1970s. The goal was to create an open architecture that would allow virtually all networks to inter-communicate. The design was based on several layers in which the user would connect at the uppermost layer and would be isolated from the details of the electrical signals found at the lowest layer.

The number of layers in the suite is not static. In fact, some books present the TCP/IP protocol suite as four layers, while others present it as five. Even then, different sources use different names for each of the layers. This textbook defines five layers, as shown in Figure 1-12: application, transport, network, data link, and physical.

Note that the layers do not specify precise protocols or exact services. In other words, the TCP/IP protocol suite does not tell you, for example, what kind of wire or what kind of connector to use to connect the devices of a network. That choice is left to the designer or implementer of the system. Instead, the suite simply says that if you specify a type of wire or a specific connector, you do that in a particular layer. In addition, each layer of the TCP/IP protocol suite provides a service for the next layer. For example, the transport layer makes sure the data received at the very end of a transmission is exactly the same as the data originally transmitted, but it relies upon the network layer to find the best path for the data to take from one point to the next within the network. With each layer performing its designated function, the layers work together to allow an application to send its data over a network of computers.

Application
Transport
Network
Data link
Physical

Figure 1-12 The five layers of the TCP/IP protocol suite

A common network application is email. An email communication that sends and accepts the message, "Blake, how about lunch? Najma," has many steps. Let's look at a simple analogy, as illustrated in Figure 1-13, to understand how the layers of the TCP/IP protocol suite work together to support this email message. Think of each layer of the TCP/IP suite as a worker. Each worker has its own job function, and Figure 1-13 shows how these workers cooperate to create a single package for transmission. Using the TCP/IP protocol suite, the steps might look like the following:

- The email "application worker" prompts the user to enter a message and specify an intended receiver. The application worker would create the appropriate data package with message contents and addresses, and send it to a "transport worker," who is responsible for providing overall transport integrity.
- The transport worker might establish a connection with the intended receiver, monitor the flow between sender and receiver, and perform the necessary operations to recover lost data in case some data disappears or becomes unreadable.
- The network worker would then take the data package from the transport worker and might add routing information so that the data package can find its way through the network.
- Next to get the data package would be the data link worker, who would insert error-checking information and prepare the data package for transmission.
- Finally, the physical worker would transmit the data package over some form of wire or through the air using radio waves.

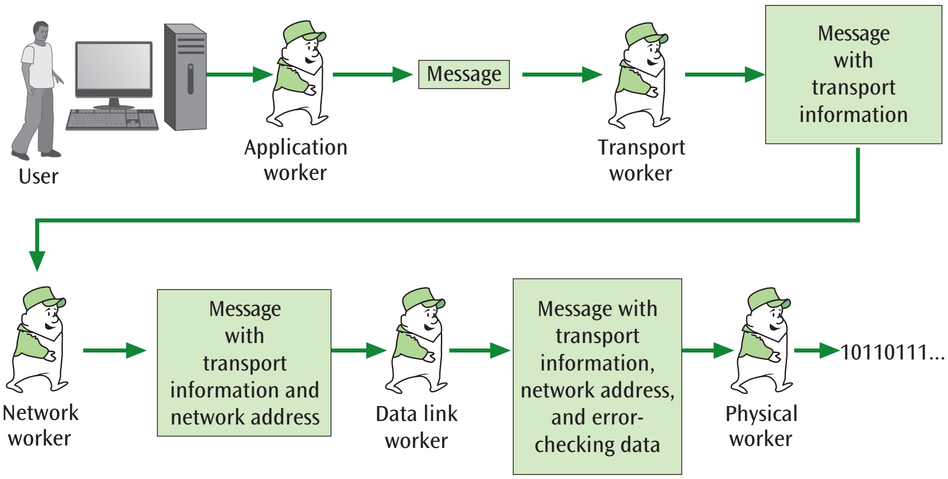


Figure 1-13 Several kinds of workers perform their job duties at each layer in the model

Application Layer

Now that you understand the big picture, let's examine each layer in more detail. The top layer of the TCP/IP protocol suite, the **application layer**, supports applications and might in some cases include additional services such as encryption or compression. Note that user applications, such as a browser or word processing application, don't reside in the application layer themselves. These applications rely directly on support provided by protocols that function within the application layer. The TCP/IP application layer includes several frequently used protocols:

- **HTTP (Hypertext Transfer Protocol)** allows web browsers and servers to send and receive web pages.
- **SMTP (Simple Mail Transfer Protocol)** allows users to send and receive email.
- **FTP (File Transfer Protocol)** transfers files from one computer system to another.
- **SSH (Secure Shell)** allows a remote user to securely log in to another computer system.
- **SNMP (Simple Network Management Protocol)** allows the numerous elements within a computer network to be managed from a single point.

Transport Layer

The TCP/IP **transport layer** commonly uses TCP (Transmission Control Protocol) to maintain an error-free end-to-end connection. To maintain this connection, TCP includes error control information in case one packet from a sequence of packets does not arrive at the final destination, and packet sequencing information so that all the packets can be sorted into the proper order as they're received. The transport layer performs *end-to-end* error control and *end-to-end* flow control, which ensures that the rate of transmitted packets does not overwhelm the device at the receiving end. This means the transport layer is not in use while the data packet is hopping from point to point within the network—it is used *only* at the two endpoints of the connection.

TCP is not the only possible protocol found at the TCP/IP transport layer. UDP (User Datagram Protocol) is an alternative also used, though less frequently, in the TCP/IP protocol suite. UDP does not provide the same kind of error control that TCP does and is most often used with streaming data, such as music or videos.

The two layers described so far are called end-to-end layers. They are responsible for the data transmitted between the endpoints of a network connection. In other words, these layers perform their operations *only* at the beginning point and ending point of the network connection. The remaining three layers of the TCP/IP protocol suite—the network, data link, and physical layers—are not end-to-end layers. They perform their operations at each node (or device) along the network path, not just at the endpoints.

Network Layer

TCP/IP's **network layer**, sometimes called the Internet layer or IP layer, is used to transfer data within and between networks. **IP (Internet Protocol)** is the software that prepares a packet of data so that it can move from one network to another on the Internet or within a set of corporate networks. As this layer sends the packet from node to node, it generates the network addressing necessary for the system to recognize the next intended receiver. IPv4 (version 4) uses a 32-bit IP address, while IPv6 uses a 128-bit IP address. To choose a path through the network, the network layer determines routing information and applies it to each packet or group of packets.

Data Link Layer

The next lower layer of the TCP/IP protocol suite is the **data link layer**, which is also sometimes referred to as the network access layer or the link layer. Where the network layer deals with passing packets across the Internet, the data link layer is the layer that gets the data from the user workstation to the router connected to the Internet. In most cases, the connection that gets the data from the user workstation to the Internet is a LAN. Thus, the data link layer prepares a **frame**, or data packet, for transmission from the user workstation to a router sitting between the LAN and the Internet. This frame contains an identifier that signals the beginning and end of the frame, as well as spaces for control information and address information. In addition, the data link layer can incorporate some form of error detection software. If an error occurs during transmission, the data link layer is responsible for error control, which it does by informing the sender of the error. The data link layer might also perform flow control. In a large network where the data hops from node to node as it makes its way across the network, flow control ensures that one node does not overwhelm the next node with too much data. Note that these data link operations are quite similar to some of the transport layer operations. The primary difference is that the transport layer performs its operations only at the endpoints, while the data link layer performs its operations at every stop (node) along the path. This is also the last layer before the data is handed off for transmission across the medium.

All Things Considered

Thought Experiment

If the data link layer provides error checking and the transport layer provides error checking, isn't this redundant? Why or why not? Explain your answer.

Physical Layer

The bottom-most layer in the TCP/IP protocol suite (according to the layers as defined in this discussion) is the physical layer. The **physical layer** is where the actual transmission of data occurs. As noted earlier, this transmission can be over a physical wire, or it can be a radio signal transmitted through the air. To perform this transmission of bits, the physical layer handles voltage levels, plug and connector dimensions, pin configurations, and other electrical and mechanical issues. Furthermore, because the digital or analog data is encoded or modulated onto a digital or analog signal at this point in the process, the physical layer also determines the encoding or modulation technique to be used in the network. Note that some people combine the data link layer and physical layer into one layer.

Having distinctly defined layers enables you to "pull out" a technology used at one layer and insert an equivalent technology into that layer without affecting the other layers. For example, assume a network was designed for copper-based wire. Later, the system owners decide to replace the copper-based wire with fiber-optic cable. Even though a change is being made at the physical layer, it should not be necessary to make any changes at any other layers. In reality, however, a few relationships exist between the layers of a communication system that cannot be ignored. For example, if the physical organization of a LAN is changed (say from a wired network to a wireless network), it is likely that the frame description at the data link layer also will need to be changed. (You will examine this phenomenon in Chapter 4.) The TCP/IP protocol suite recognizes these relationships and merges many of the services of the physical and data link layers into one layer.

The OSI Model

Although the TCP/IP protocol suite is the model of choice for almost all installed networks, it is important to study both this architecture and the OSI model. Many books and articles, when describing a product or a protocol, often refer to the OSI model with a statement such as, "This product is compliant with OSI layer *x*." If you do not become familiar with the various layers of the OSI model and the TCP/IP protocol suite, you will struggle to understand more advanced concepts in the future.

The OSI model defines seven layers, as shown in Figure 1-14. Note further the relationship between the five layers of the TCP/IP protocol suite and the seven layers of the OSI model. As you examine descriptions of each of the OSI layers next, consider how their functions compare to the corresponding TCP/IP layer:

- The top layer in the OSI model is the application layer, which provides protocols to support applications using the network. Notice again that these protocols provide a support function—they are not the applications themselves, which do not reside on the network model. This OSI layer is similar to the application layer in the TCP/IP protocol suite.
- The next layer in the OSI model, the **presentation layer**, performs a series of miscellaneous functions necessary for presenting the data package properly to the sender or receiver. For example, the presentation layer might perform ASCII-to-non-ASCII character conversions, encryption and decryption of secure documents, and the compression of data into smaller units. There is no separate presentation layer in the TCP/IP protocol suite, as these functions are wrapped into the TCP/IP application layer.
- The **session layer** is another layer that does not exist separately in the TCP/IP protocol suite and is responsible for establishing sessions between users. It also can support token management, a service that controls which user's computer talks during the current session by passing a software

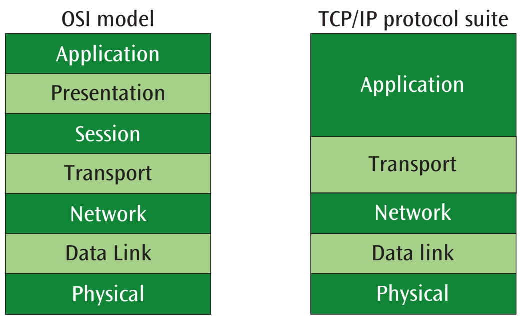


Figure 1-14 The seven layers of the OSI model compared to the five layers of the TCP/IP protocol suite

token back and forth. Additionally, the session layer establishes synchronization points, which are backup points used in case of errors or failures. For example, while transmitting a large document such as an ebook, the session layer might insert a synchronization point at the end of each chapter. If an error occurs during transmission, both sender and receiver can back up to the last synchronization point (to the beginning of a previously transmitted chapter) and start retransmission from there. Many network applications do not include a specific session layer and do not use tokens to manage a conversation. If they do, the "token" is inserted by the application layer, or possibly the transport layer, instead of the session layer. Likewise, if network applications use synchronization points, these points often are inserted by the application layer.

- The fourth layer in the OSI model, the transport layer, operates in the same way as the transport layer of the TCP/IP protocol suite. It ensures that the data packet arriving at the final destination is identical to the data packet that left the originating station.
- The network layer of the OSI model is similar to the network layer of the TCP/IP protocol suite and is responsible for getting the data packets from router to router through the network.
- The data link layer, similar to TCP/IP's data link layer, is responsible for taking data from the network layer and transforming it into a frame. It also handles addressing between devices within a LAN.
- The bottom layer in the OSI model—the physical layer—handles the transmission of bits over a communications channel. This layer is essentially identical to the physical layer of the TCP/IP protocol suite.

Logical and Physical Connections

An important concept to understand with regard to the layers of a communication model is the lines of communication between a sender and a receiver. Consider Figure 1-15, which shows the sender and receiver using a network application designed on the TCP/IP protocol suite.

Notice the dashed lines between the sender's and receiver's application layers, transport layers, network layers,

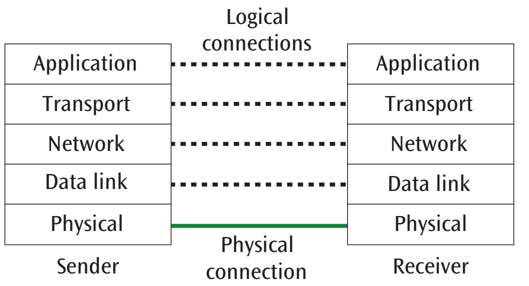


Figure 1-15 Sender and receiver communicating using the TCP/IP protocol suite

and data link layers. No data flows over these dashed lines. Each dashed line indicates a logical connection. A **logical connection** is a nonphysical connection between sender and receiver that allows an exchange of commands and responses. The sender's and receiver's transport layers, for example, share a set of commands used to perform transport-type functions, but the actual information or data must be passed through the lower layers of the sender and receiver, as there is no direct connection between the two transport layers. Without a logical connection, the sender and receiver would not be able to coordinate their functions. The **physical connection** is the only direct connection between sender and receiver, and is at the physical layer, where actual 1s and 0s—the digital content of the message—are transmitted over wires or airwaves.

For an example of logical and physical connections, consider what happens when you want to buy a house. Typically, you won't call homeowners directly. You'll first contact a real estate agent, who will show you several houses. Once you pick your favorite, you still won't communicate directly with the homeowner—your real estate agent will call the homeowner's agent. To negotiate the sales price, you and the homeowner will communicate through your respective agents as representatives of the best interests for each party. Figure 1-16 shows how this communication relies on layers of people and technology to send messages back and forth during the negotiation.

Note that the data did not flow directly between you and the homeowner; nor are the real estate agents likely to see each other face-to-face for the majority of these communications. Instead, the data had to flow down to the physical layer (in this case, the agents' smartphones) and then back up the other side. At each layer in the process, information that might be useful to the "peer" layer on the other side was added

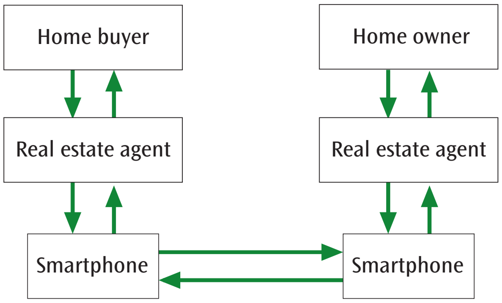


Figure 1-16 Flow of data through the layers of bureaucracy

(such as information about the house's address or information about the other agent's phone number). While this example illustrates the concept of layered communications, it is a bit overly simplified. Therefore, let's examine a more realistic example in which a person using a web browser requests a web page from somewhere on the Internet.

All Things Considered

Thought Experiment

Recall a job you have had or still have. Was a chain of command in place for getting tasks done? If so, draw that chain of command on paper or using a drawing app. How does this chain of command compare to either the OSI model or the TCP/IP protocol suite?

The TCP/IP Protocol Suite in Action

A more detailed and more challenging example of a request for a service moving through the layers of a communications model will help make the involved concepts clearer. Consider Figure 1-17, in which a user browsing the Internet on a personal computer requests a web page to be downloaded and then displayed on their screen.

Beginning in the upper-left corner of the figure, the process is initiated when the user clicks a link on the current web page. In response, the browser software (the application) creates a *Get web page* command that is given to the browser's transport layer, TCP. TCP adds a variety of header information to be used by the TCP software on the receiving end. Added to the front of the packet, this information will be used to control the transfer of data. This information assists with end-to-end error control and end-to-end flow control, and it provides the transport-layer address of the receiving application on the web server (which likely is running several applications, and so each application has its own address called a port).

The enlarged packet is now sent to the network layer, where IP adds its header. The information contained within the IP header assists the IP software on the receiving end, and it assists the IP software at each intermediate node (router) during the data's progress through the Internet. This assistance includes providing the Internet address of the web server that contains the requested web page.

The packet is now given to the data link layer. Because the user's computer is connected to a LAN, the appropriate LAN headers are added. Note that sometimes, in addition to headers, control information is added to the end of the data packet as a trailer. One of the most important pieces of information included in the data link header is the address of the device (the router) that connects the LAN to the Internet.

Eventually, the binary 1s and 0s of the data packet are transmitted across the user's LAN via the physical layer, where they encounter a router. The router serves as the gateway to the Internet. The router removes the data link header and trailer. The information in the IP header is examined, and the router determines that the data packet must go out to the Internet. New data link header information, which is necessary for the data packet to traverse the Internet to the next router, is applied, and the binary 1s and 0s of the data packet are placed onto the WAN connection.

As the data packet moves across the Internet, it will eventually arrive at the router connected to the LAN that contains the desired web server. This remote router removes the WAN information, sees that the packet must be placed on its LAN, and inserts the LAN header and trailer information. The packet is placed onto the LAN; using the address information in the data link header, it travels to the computer holding the web server application. As the data packet moves up the layers of the web server's computer, the data link, IP, and TCP headers are removed. The web server application receives the *Get web page* command, retrieves the requested web page, and creates a new data packet with the requested information. This new data packet now moves down the layers and back through the routers to the user's network and workstation. Finally, the web page is displayed on the user's monitor.

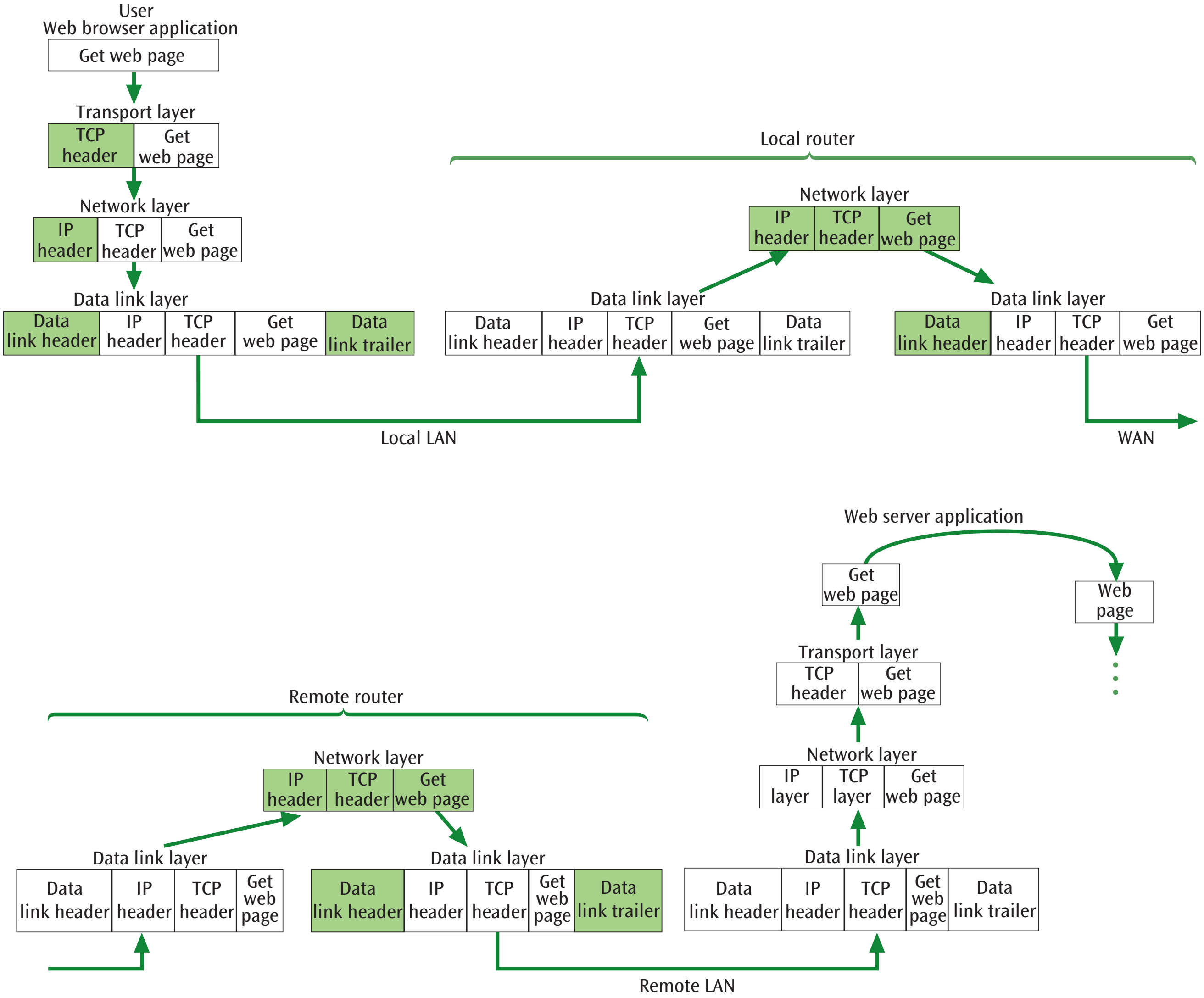


Figure 1-17 Path of a web page request as it flows from browser to Internet web server and back

It is interesting to note that, as a packet of data flows down through a model and passes through each layer of the system, the data packet grows in size. This growth is attributable to the fact that each layer adds more information to the original data. Some of this layer-added information is needed by the nodes in the data packet's path, and some is required by the data packet's final destination. This information aids in providing services such as error detection, error control, flow control, and network addressing. The addition of control information to a packet as it moves through the layers is called **encapsulation**. Note also that, as the packet moves up through the layers, the data packet shrinks in size as each layer removes the header it needs to perform its job. Once the job is complete, the header information is discarded and the smaller packet is handed to the next highest layer.

Details | The Internet's Request for Comment (RFC)

Network models, like communications protocols, computer hardware, and application software, continue to evolve daily. The TCP/IP protocol suite is a good example of a large set of protocols and standards constantly being revised and improved. An Internet standard is a tested specification that is both useful and adhered to by users who work with the Internet. Consider the path a proposal must follow on the way to becoming an Internet standard.

All Internet standards start as an Internet draft, which is a preliminary work in progress. One or more internal Internet committees work on a draft, improving it until it is in an acceptable form. When Internet authorities feel the draft is ready for the public, it is published as an RFC (Request for Comment), a document open to all interested parties. The RFC is assigned a number, and it enters its first phase: proposed standard. A proposed standard is a proposal that is stable, of interest to the Internet community, and fairly well understood. The specification is tested and implemented by different groups, and the results are published. If the proposal passes at least two independent and interoperable implementations, the proposed standard is elevated to draft standard. If, after feedback from test implementations is considered, the draft standard experiences no further problems, the proposal is finally elevated to Internet standard.

If, however, the proposed standard is deemed inappropriate at any point along the way, it becomes an historic RFC and is kept for historical perspective. (Internet standards that are replaced or superseded also become historic.) An RFC also can be categorized as experimental or informational. In these cases, the RFC in question probably was not meant to be an Internet standard, but it was created either for experimental reasons or to provide information. Figure 1-18 shows the levels of progression for an RFC.

It is possible to obtain a printed listing of each RFC. See the IETF's (Internet Engineering Task Force) website at *ietf.org/rfc/* for the best way to access RFCs.

The Internet is managed by the work of several committees, as described next:

- The topmost committee is the ISOC (Internet Society). ISOC is a nonprofit, international committee that provides support for the entire Internet standards-making process.

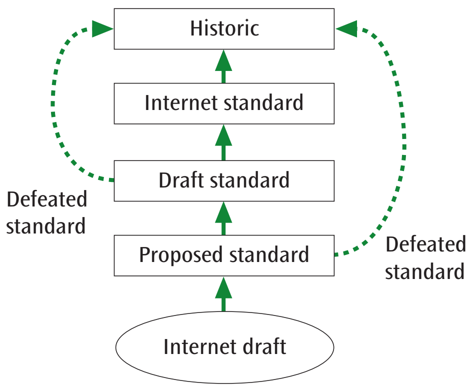


Figure 1-18 Levels of progression as an RFC moves toward becoming a standard

- Associated with ISOC is the IAB (Internet Architecture Board), which is the technical advisor to ISOC. Under the IAB are two major committees:
  - The IETF (Internet Engineering Task Force) manages the working groups that create and support functions such as Internet protocols, security, user services, operations, routing, and network management.
  - The IRTF (Internet Research Task Force) manages the working groups that focus on the long-range goals of the Internet, such as architecture, technology, applications, and protocols.

Internet committees are not the only groups that create protocols or approve standards for computer networks, data communications, and telecommunications. Another organization that creates and approves network standards is the **ISO (International Organization for Standardization)**, which is a multinational group composed of volunteers from the standards-making committees of various governments throughout the world. ISO is involved in developing standards in the field of information technology and created the OSI (Open Systems Interconnection) model for a network architecture.

Note

The shortened name for the International Organization for Standardization, *ISO*, is derived from a Greek word meaning *equal* and is not an acronym of the longer name.

Other standards-making organizations include the following:

- **ANSI (American National Standards Institute)**—A private, nonprofit organization not associated with the U.S. government, ANSI strives to support the U.S. economy and protect the interests of the public by encouraging the adoption of various standards.
- **ITU-T (International Telecommunication Union-Telecommunication Standardization Sector)**—Formerly the Consultative Committee on International Telegraphy and Telephony (CCITT), ITU-T is devoted to the research and creation of standards for telecommunications in general, and telephone and data systems in particular.

- **IEEE (Institute of Electrical and Electronics Engineers)**—The largest professional engineering society in the world, IEEE strives to promote the standardization of the fields of electrical engineering, electronics, and radio. Of particular interest is the work IEEE has performed on standardizing local area networks.

Remember this…

- Networks rely on a modular design based on various levels of functionality so that changes can be made at one layer without greatly affecting any other layer.
- The TCP/IP protocol suite defines four or five layers, the names of which can vary depending on the source. This text labels five layers: application, transport, network, data link, and physical.
- The OSI model defines seven layers: application, presentation, session, transport, network, data link, and physical.
- A logical connection identifies a conversation between the sender and receiver at each layer of communication, while a physical connection shows a direct connection between sender and receiver at the layer where actual 1s and 0s are transmitted over wires or airwaves.
- A message moves up and down the TCP/IP layers as it interacts with each protocol to carry information from one hop to the next across one or more networks.

Self-check

8. Which of these protocols do network admins use to help them identify problems on a network?

- **a.** HTTP
- **b.** SMTP
- **c.** FTP
- **d.** SNMP

9. Which OSI layer provides address information for a message to travel from a workstation to a router?

- **a.** Physical
- **b.** Data link
- **c.** Network
- **d.** Transport

10. A rat chews through a cable connecting two switches on your network. What layer of the OSI model has been compromised?

- **a.** Application
- **b.** Transport
- **c.** Network
- **d.** Physical

Check your answers at the end of this chapter.

Section 1-5: Cloud Computing

Throughout this course, you'll learn about cloud computing systems in the context of networking and data communications. While cloud computing is a relatively recent technological innovation, it's touching nearly every area of IT and, in many ways, revolutionizing the way datacenters and networks function. Why is this the case? Essentially, cloud computing provides a new way of running a company's IT resources. Cloud computing relies on the abstraction of compute, network, security, and storage functions away from the underlying physical hardware in ways that give network admins and other IT professionals almost unlimited resources at affordable prices. Let's start to break this concept down into bite-size pieces so you can see the significance of what cloud computing offers.

Cloud Computing Characteristics

Cloud Essentials+ Exam Tip

This section discusses cloud characteristics, which is required by

- Part of Objective 1.1: Explain cloud principles.
- Part of Objective 1.4: Summarize important aspects of cloud design.
- Part of Objective 2.4: Identify the benefits or solutions of utilizing cloud services.

To begin, you need a solid understanding of what characteristics define cloud computing and distinguish these technologies from more traditional options. NIST (National Institute of Standards and Technology) and similar organizations refer to the following characteristics to differentiate cloud computing from other types of IT resources:

- **Scalability** refers to the ability of resources to be adjusted over time in response to changing needs. Scalable resources can be increased or decreased either vertically or horizontally. For example, suppose a new doctor's office buys one server to hold their patient database. As their customer base grows, the database will continue to increase in size. Figure 1-19 illustrates two options for how to handle the growing demand. Vertical scaling would add more resources to the server, such as storage and memory, to increase its capacity, while horizontal scaling would add more servers to help host the database. With physical servers, this scaling up or scaling out is time-consuming and costly; cloud services are designed with scalability as a primary feature that can be performed quickly and even automatically, with little to no interruption in service.
- **Elasticity** means that resources can be increased or decreased quickly in response to changing needs, and in many cases, these shifts can be configured to occur automatically. Suppose you anticipate a huge increase in website traffic during a weekend advertising campaign. With traditional computing, you would have to purchase additional servers many months ahead of time, and then spend hours installing and configuring the servers in preparation for a temporary traffic spike. After the campaign, the servers would no longer be needed, thereby wasting a lot of money. Elastic cloud resources can be temporarily increased only for the few days you need them, and then decreased as the traffic volume declines.

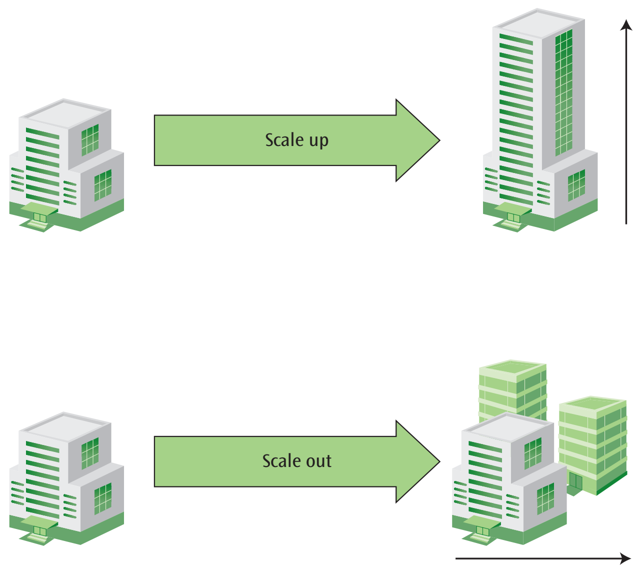


Figure 1-19 Resources can be scaled vertically by increasing an existing resource's capacity or horizontally by increasing the number of resources available

- **Pay-as-you-go** means the customer only pays for the resources they use. For example, when the customer no longer needs extra servers to handle increased traffic from the weekend advertising campaign, those extra servers are terminated and no longer accrue charges. The cloud customer does not have to pay for resources they're not using.
- **Self-service** resources can be increased, decreased, or otherwise altered by the customer without having to involve the cloud service provider. In many cases, the customer can configure these processes to happen automatically.
- **Broad network access** refers to a customer's ability to access and configure cloud resources from any Internet-connected computer. In other words, a technician or administrator does not have to be onsite at the cloud datacenter to make changes to their company's cloud resources. A company's IT team can access and control their cloud resources from home, from the company's own location, or from anywhere else where they have Internet access.

Note

Access to a customer's cloud console can be restricted to one or more specific locations based on IP address. However, this is a security measure, not a limitation of cloud capabilities.

- **Availability** refers to a cloud resource's ability to withstand losses or outages while minimizing disruption of service. **High availability (HA)** is the expectation that a service will be accessible for a certain percentage of time over the course of a year or a month and is usually listed by the number of 9s, such as 99.9% ("three nines") or 99.9999%

("six nines"). For example, if a service is down for less than 5.26 minutes per year, that service is said to have 99.999%, or five nines, availability. HA is achieved by providing **redundancy** within a system, which means that single points of failure (SPOFs), such as a network connection or a server, are duplicated. If one of these resources goes down, the other can take over and keep the system functioning.

Note

Various cloud services and ISPs offer three nines, four nines, five nines, or better availability, depending on what's defined in their **SLAs (Service-Level Agreements)**, which is a legally binding contract or part of a contract that defines certain aspects of a service. When shopping for cloud services, examine the SLA carefully so you'll know what parts of a service are guaranteed to be available.

However, be aware there's a difference between availability (the ability to access a resource) and **durability** (the resource's ongoing existence). For example, AWS lists its storage service, S3, at 99.999999999% durability (that's 11 nines!), but S3's *availability* is 99.99% for its Standard storage class. Why the discrepancy?

That 11 nines durability means you could store 10,000,000 objects in S3 and expect to lose one of those objects every 10,000 years on average (okay, not bad). This is because S3 stores each object on multiple devices in multiple, physical datacenters. The four nines availability means that, each year on average, there should only be 52.6 minutes when you can't get to your objects in S3—this is also pretty good, considering you can relax in knowing that your stored data isn't lost during that 52 minutes, even if you can't get to it for a bit.

Similar terms include **reliability**, which refers to how well a resource functions without errors, and **resiliency**, which refers to a resource's ability to recover from errors even if it becomes unavailable during the outage.

Cloud Service Models

Cloud Essentials+ Exam Tip

This section discusses cloud service models, which is required by

- Part of Objective 1.1: Explain cloud principles.

Now that you've read about the characteristics that are common to all cloud deployments, you're ready to learn about ways to differentiate various types of cloud services. You can think about each cloud service as a building block where you select the types of blocks that you need for your structure and connect them to work together. It helps to first think about these services in high-level categories, as described next:

- **SaaS (Software-as-a-Service)**, pronounced *sass*, is the type of cloud service most users are familiar with and provides access to an application that runs in the cloud environment. SaaS solutions tend to be highly scalable and require little to no understanding of the underlying architecture. SaaS applications also can be accessed from almost any kind of computer or mobile device. If you've used Google Docs or Dropbox, you've used SaaS. These cloud-based applications offer some level of configurability for the user or the administrator but provide no access to the underlying hardware, software, or virtualized resources supporting the application.
- **PaaS (Platform-as-a-Service)**, pronounced *pass*, requires more technical skill and often serves professional or hobbyist application developers or website developers. PaaS allows some underlying configurability, but developers can mostly focus on their development work without having to devote time to managing a network infrastructure. Imagine if you could develop an application without having to manage and update a server's operating system. This is one of the primary advantages of PaaS.

- **IaaS (Infrastructure-as-a-Service)**, pronounced *i-as*, requires the most technical skill for configuring cloud resources. While the customer cannot access the underlying hardware, IaaS allows the cloud customer to perform deep configurations to the cloud environment where they can most closely replicate a physical datacenter in the cloud, complete with virtual servers, firewalls, routers, and load balancers.

Notice that each of these categories varies on the type of person who would use a solution from that category. Figure 1-20 shows how each of these service models varies in the type of user the service is targeted to, and Figure 1-21 shows the different levels of technical skill required for each service model.

The progression of these categories reveals the fact that cloud customers and cloud providers each take part of the responsibility for managing and configuring cloud resources. As you can see in Figure 1-22, the placement of that dividing line determining who is responsible for what varies with the type of cloud service. In fact, this is one of the points that must be carefully studied and understood by cloud professionals for each service they use. It's important for cloud customers to know and consider what kinds of management tasks they must perform on their cloud services, what security precautions they must take, and what kinds of customization changes they can make. This reality is complicated by the fact that each cloud service provider handles the division of labor a little differently. For this reason, cloud professionals often specialize in one or a handful of cloud providers and service types.

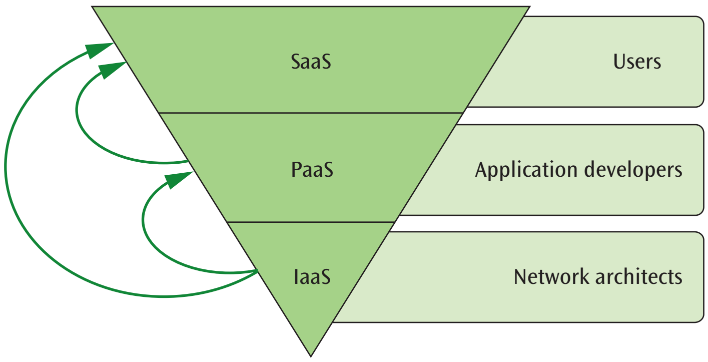


Figure 1-20 SaaS services are more immediately accessible to a wide market of users than other categories of cloud services

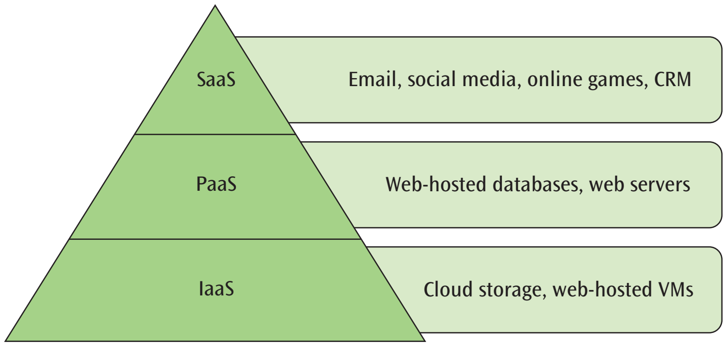


Figure 1-21 IaaS customers must understand more about configuring their cloud infrastructure—and they have more control—than do SaaS customers

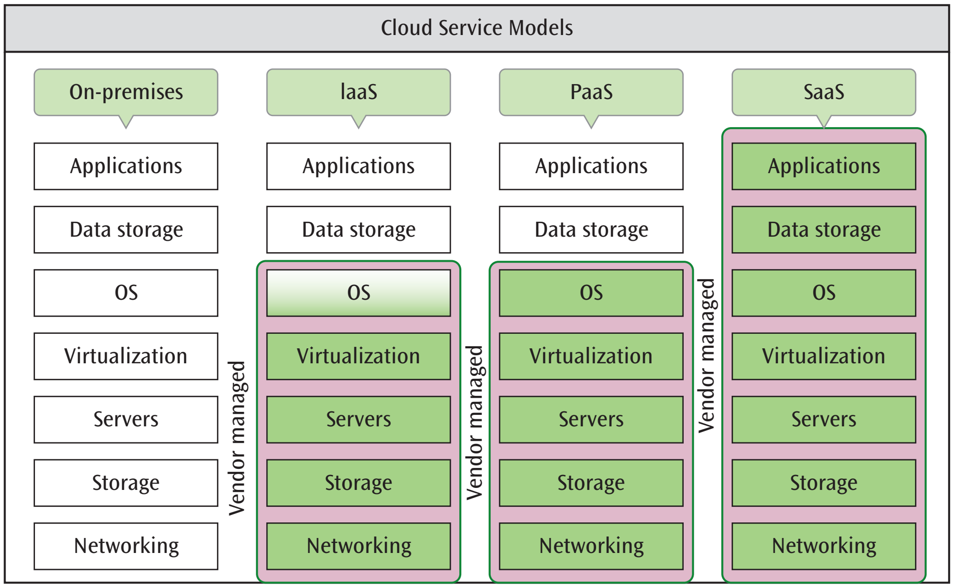


Figure 1-22 At each progressive level of these cloud service models, the vendor takes over more computing responsibility for the organization

In this chapter, you've laid a solid foundation of terminology and basic networking concepts to serve as the launching point for the remainder of this book.

Remember this...

- Cloud computing relies on the abstraction of compute, network, security, and storage functions away from the underlying physical hardware in ways that give network admins and other IT professionals almost unlimited resources at affordable prices.
- Characteristics that differentiate cloud computing from other types of IT resources include built-in scalability and availability, elastic resources, pay-as-you-go and self-service services, and broad network access.
- The three primary cloud service models are SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service), and IaaS (Infrastructure-as-a-Service), which differ by how much access the cloud customer has to configure the underlying virtual infrastructure and by how much cloud management technical skill is required.
- It's important for cloud customers to know and consider what kinds of management tasks they must perform on their cloud services, what security precautions they must take, and what kinds of customization changes they can make.

Self-check

11. When schools suddenly closed and classes were held over the Internet instead, your company's video conferencing software suddenly needed to host five times more traffic than usual. What feature of your cloud-hosted web app allowed your service to automatically adapt to the changing demand?

a. Accessibility
b. Elasticity
c. Self-service
d. Broad network access

12. What kind of cloud service model is web-based email?

a. SaaS
b. PaaS
c. IaaS
d. XaaS

Check your answers at the end of this chapter.

Summary

Section 1-1: The Language of Computer Networking

- Networks are often categorized according to their size and the types of devices connected to them.
- The study of data communications includes digital and analog signals that can be transmitted over conducted or wireless (radiated) media.
- Cloud computing typically relies on the Internet in some way for access to resources at a remote location.

Section 1-2: The Big Picture of Networks

- LANs connect devices to each other using switches and connect to other networks using routers.
- WANs connect networks to each other using routing devices and are organized into groups of nodes called subnetworks.
- Specialized hardware and software are required for a workstation to communicate over a network such as the Internet.
- Addressing information is used to route information across a network.

Section 1-3: Common Network Examples

- Many kinds of networks exist, depending on the connection technologies used, the types of communications the network supports, and the kinds of devices connected to the network.
- A client/server system provides client computers with a variety of services, such as a database, a web page, email, files, or printing.
- Protocols define the rules used by devices to communicate with each other over a network.
- Routers and switches can be used to connect devices across multiple LANs or segment traffic for security or traffic management purposes.
- Smartphones often rely on cellular networks to connect to the Internet and to provide calling and texting services.
- Other kinds of networks include sensor networks, wireless networks that use satellite technologies, and cloud networks that rely on virtualization.

Section 1-4: Network Architectures

- Networks rely on a modular design based on various levels of functionality so that changes can be made at one layer without greatly affecting any other layer.
- The TCP/IP protocol suite defines four or five layers, the names of which can vary depending on the source. This text labels five layers: application, transport, network, data link, and physical.
- The OSI model defines seven layers: application, presentation, session, transport, network, data link, and physical.
- A logical connection identifies a conversation between the sender and receiver at each layer of communication, while a physical connection shows a direct connection between sender and receiver at the layer where actual 1s and 0s are transmitted over wires or airwaves.
- A message moves up and down the TCP/IP layers as it interacts with each protocol to carry information from one hop to the next across one or more networks.

Section 1-5: Cloud Computing

- Cloud computing relies on the abstraction of compute, network, security, and storage functions away from the underlying physical hardware in ways that give network admins and other IT professionals almost unlimited resources at affordable prices.
- Characteristics that differentiate cloud computing from other types of IT resources include built-in scalability and availability, elastic resources, pay-as-you-go and self-service services, and broad network access.
- The three primary cloud service models are SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service), and IaaS (Infrastructure-as-a-Service), which differ by how much access the cloud customer has to configure the underlying virtual infrastructure and by how much cloud management technical skill is required.
- It's important for cloud customers to know and consider what kinds of management tasks they must perform on their cloud services, what security precautions they must take, and what kinds of customization changes they can make.

Key Terms

For definitions of key terms, see the Glossary near the end of the book.

application layer
availability
broad network access
CAN (campus area network)
client/server system
cloud
cloud computing
compression
computer network
computer terminal
data communication
data link layer
durability
elasticity
encapsulation
enterprise network
frame
FTP (File Transfer Protocol)
HA (high availability)
HTTP (Hypertext Transfer Protocol)
hybrid cloud
hypervisor
IaaS (Infrastructure-as-a-Service)
IEEE (Institute of Electrical and Electronics Engineers)
IoT (Internet of Things)
IP (Internet Protocol)
ISO (International Organization for Standardization)
LAN (local area network)
logical connection
MAN (metropolitan area network)
multiplexing
network architecture
network layer
network management
node
OSI (Open Systems Interconnection) model
PaaS (Platform-as-a-Service)
PAN (personal area network)
pay-as-you-go
physical connection
physical layer
presentation layer
private cloud
protocol
public cloud
redundancy
reliability
resiliency
router
SaaS (Software-as-a-Service)
scalability
segmentation
self-service
server
session layer
SLA (Service-Level Agreement)
SMTP (Simple Mail Transfer Protocol)
SNMP (Simple Network Management Protocol)
SSH (Secure Shell)
subnetwork
switch
TCP/IP protocol suite
transport layer
virtualization
VM (virtual machine)
WAN (wide area network)
web app
wireless
workstation
XaaS (Anything as a Service)

Review Questions

1. You are sitting at the local coffee shop, enjoying your favorite latte. You pull out your laptop and, using the wireless network available at the coffee shop, access your email. Which portion of the electromagnetic spectrum is your laptop most likely using?
   a. Ultraviolet waves
   b. Visible light waves
   c. Radio waves
   d. X-rays
2. Which of the following characteristics distinguishes a PAN from other types of networks?
   a. A printer is connected to the network.
   b. The network is intended to be used by one person at a time.
   c. The network supports wearable devices.
   d. The network is small in geographical coverage.
3. When you set up a network at your home with a home router, a few computers, a printer, multimedia devices, and your smartphone, which of the following statements is true?
   a. You can have several PANs, you have one LAN, and you probably have one WAN connection.
   b. You can have several LANs, you have one PAN, and you probably have one WAN connection.
   c. You can have several WANs, you have one MAN, and you probably have one LAN connection.
   d. You can have several PANs, you have one MAN, and you probably have one LAN connection.
4. Your company's network administrator mentions during a meeting that she has migrated your company's database to a DBaaS. What can you deduce about the database, given just this information?
   a. The database has been backed up.
   b. The database is now more secure than it was.
   c. The database is stored on a cloud provider's servers.
   d. The database has been archived.
5. When your work computer requests a web page, which device does the computer communicate with *first*?
   a. Web server
   b. Local server
   c. Router
   d. Switch
6. As you're setting up your home network, you connect one desktop and two laptops to your home router. You then connect your home router to your cable modem. When you test the connection with your desktop, the computer can access websites on the Internet. What functions is your home router providing for your home network?
   a. Web server and file server
   b. Web server and router
   c. Switch and web server
   d. Router and switch
7. What computer "language" is spoken over the Internet?
   a. WAN
   b. NaaS
   c. TCP/IP
   d. DSL
8. Using a laptop computer with a wireless connection to your company's LAN, you download a web page from the Internet. Which of the following statements can you know is true, given this information?
   a. Your web page request crossed at least two LANs.
   b. Your web page request crossed exactly one LAN.
   c. Your web page request was handled by exactly one router.
   d. Your web page request was handled by exactly one switch.
9. Your coworker, Raul, has stored a few documents on his workstation that you and several others in your office access regularly as you're writing emails to customers. What function is Raul's computer filling?
   a. Web server
   b. Switch
   c. Email server
   d. File server

10. Your family-owned business is growing and has just added a few new employees. The owners decide, for security purposes, that the network needs to be segmented so that only certain people can get to sensitive data. Which of these changes will accomplish this goal most effectively?
    a. Add a new WAN.
    b. Divide the network into two LANs.
    c. Divide the network into two WANs.
    d. Add a new PAN.

11. As you're riding the bus to work, you check your email on your smartphone. Your smartphone is using the cellular network to access the email server at your company's datacenter. What kind of network is this?
    a. Local area network
    b. Personal area network
    c. Body area network
    d. Wide area network

12. Which of the following is *not* an example of a sensor network?
    a. A doorbell sends an alert to the homeowner's smartphone when movement is detected.
    b. A security camera records some burglars robbing a gas station.
    c. A robot rejects a circuit board that does not meet manufacturing standards.
    d. An alarm sounds when water is detected on the datacenter floor.

13. Peggy owns a MacBook but needs to install and use an application that only works on the Windows operating system. How can she use the hardware she has to install and use the application?
    a. Wipe the macOS off her MacBook and install Windows instead.
    b. Spin up a macOS VM in the cloud and install the application on the VM.
    c. Create a VM on the MacBook and install Windows and the application on the VM.
    d. Change the hard drive on her MacBook and install Windows and the application on the new hard drive.

14. Which OSI layers does the TCP/IP architecture combine into one?
    a. Physical and network
    b. Network and application
    c. Application, transport, and physical
    d. Application, presentation, and session

15. Which of the following protocols functions at the transport layer?
    a. HTTP
    b. TCP
    c. IP
    d. SSH

16. Which of the following devices relies on IP addresses to send messages from network to network toward their destination?
    a. Routers
    b. Switches
    c. Servers
    d. Workstations

17. As you chat with a friend on social media, what type of connection maintains the immediacy of the conversation?
    a. Physical connection
    b. Logical connection
    c. Network connection
    d. Data link connection

18. In what part of a message on the Internet can a router find the destination IP address?
    a. Data link layer header
    b. Application layer header
    c. Transport layer header
    d. Network layer header

19. Mae sets up a database in the cloud for her new application, and she configures the database with automatic backups. The application runs on duplicate servers in her local area network. The local area network connects to the Internet through her router that was supplied by her Internet service provider. What is the single point of failure in Mae's architecture?
    a. The database
    b. The server
    c. The router
    d. The Internet

20. Kason creates a server in his private cloud where he will host his new website. Which cloud service model is Kason using for his VM?
    a. SaaS
    b. PaaS
    c. IaaS
    d. XaaS

Hands-On Project 1

Create a CloudWatch Alarm in AWS

Estimated time: 45 minutes

Resources:

› AWS account (instructions for free accounts and free credits are included below)

› Internet access

› **Context:**

Note

To Instructors: AWS Academy offers a plethora of helpful and free resources for schools, instructors, and students. At the time of this writing, students can only join AWS Academy when you post an invitation link in your LMS (learning management system) or when you send an email invite from the AWS Academy website, which provides students with free credits and tools for you to help them with their work in AWS. You can allocate free credits to your students for every class using a Learner Lab, and it does not count against their free credits in their own accounts. Creating an instructor's AWS Academy account is easy and free, and begins with a free AWS Academy application from your institution. Creating a Learner Lab in AWS Academy is even easier, and you can allocate free AWS credits for your students. For more information, visit **aws.amazon.com/training/awsacademy/**. If you have questions or need assistance, contact AWS Academy staff or email the author at *jillwestauthor@gmail.com*.

The Hands-on Projects in this course use the AWS (Amazon Web Services) public cloud platform. The steps below can help you create an AWS account if you don't have one already.

In this project, you'll create a CloudWatch alarm. Often, CloudWatch alarms are used to monitor availability and performance of cloud resources. In this case, you'll use CloudWatch to alert you if your cloud resources accumulate charges beyond a set maximum. While this shouldn't be necessary if you follow all project steps and properly delete all resources after you're finished with them, the alarm serves as a backup measure to help protect your liability. Note that these steps were accurate at the time of writing. You might need to do some research for updated information as things change. Search engines such as Google and documentation websites such as AWS and YouTube can be very helpful.

If you're using an AWS Academy account for this project, you'll be able to complete most of the steps and create the alarm; however, the alarm will not trigger because of a permissions limitation in AWS Academy. If you're using a standard AWS account, this alarm will help protect your liability for costs in AWS. Complete the following steps:

1. If you don't already have an AWS account, you'll need to create one. Choose one of the following options:
    a. Your instructor might have an AWS Academy course for you. In this case, your instructor should send you an invitation email to join the course, or your instructor might post a link in your LMS (learning management system). Follow the steps given in the email. No credit card is required.
    b. Alternatively, you can create a standard, free account with AWS directly. When you first create an AWS account, you get some Always Free services and 12 months Free Tier services that allow you to test-drive certain features within pre-defined limits. The AWS projects in this course can be completed within the limits of Free Tier services at the time of this writing, although that could change. Be sure to read and understand the terms and conditions of Free Tier services, which services are included, and what the defined limits are. To sign up, go to **aws.amazon.com/free/**. A credit card *is* required for this option.
2. After creating your AWS account, regardless of the approach you used, save your sign-in information in a safe place for future reference in later projects.

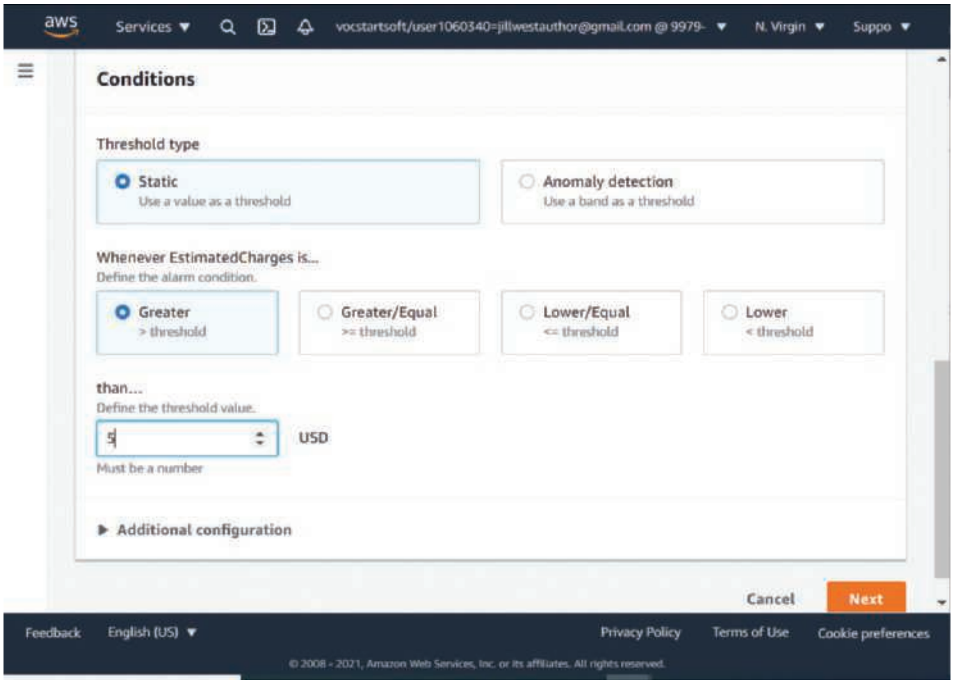
3. Sign into your AWS management console:
    a. If you're using an AWS Academy Learner Lab, you'll need to access your AWS management console through the AWS Academy website.
    b. If you're using a standard AWS account, sign in directly at **aws.amazon.com**.

Steps 4, 5, and 6 can only be completed using a standard AWS account. If you're using an account through AWS Academy, skip to Step 7. If you're using a standard AWS account, make sure you're signed in as the root user (this is the default) or as an IAM user with permission to view billing information, and then complete the following steps:

4. At the top of the console, make sure the **US East (N. Virginia)** region is selected.
5. At the top of the console, click the name of your account, and then click **My Billing Dashboard**.
6. In the navigation pane on the left, click **Billing preferences**. Select **Receive Billing Alerts**. Click **Save preferences**.

Regardless of the account type you're using, complete the following steps to create a billing alarm in CloudWatch:

7. At the top of the console, click **Services**. Services are grouped according to the kinds of resources they create. In the Management & Governance group, click **CloudWatch**.
8. In the navigation pane on the left, click **Alarms**. Click **Create alarm**. A CloudWatch alarm is a free resource in the CloudWatch service.
9. Click **Select metric**. On the Select metric page, you can drag up the two lines in the middle of the screen to resize the lower section, making it easier to see the available metrics. Under Metrics, click **Billing**. Click **Total Estimated Charge**. Check **USD**. Click **Select metric**.
10. By default, the Statistic field is set to Maximum, and the Period field is set to 6 hours. In the Conditions section, the Threshold type is set to **Static**, and the *Whenever Estimated Charge is…* field is set to **Greater**. Scroll to the bottom of the page to the *than…* field. Under *Define the threshold value*, type **5**. As shown in Figure 1-23, this metric will trigger the alarm if charges exceed $5 once within six hours. Click **Next**.



Source: Amazon Web Services, Inc.

Figure 1-23 This will trigger if estimated charges exceed $5

In AWS, an alarm is an event that is triggered when certain conditions are met (similar to a smoke detector identifying smoke in the air). In contrast, an SNS (Simple Notification Service) topic handles any notifications that should be sent if the alarm is triggered (such as the noise a smoke detector emits when smoke is detected). Basically, an alarm identifies that something occurred, and the SNS topic is the communications channel in response to that alarm. In AWS, that response might be an email or text message sent to an admin, among other possibilities. Therefore, as you're setting up your alarm, you also need to set up a topic, as follows:

11. Under *Select an SNS topic*, select **Create new topic**. Give the topic an informative name. What name did you use?
12. In the Email endpoints field, enter your email address (an account you monitor regularly—this email does *not* have to be the same address you use to access your AWS console). Click **Create topic**. Scroll down and click **Next**.
13. Give the alarm an informative name and description. What name and description did you use? Click **Next**.
14. Study the information on the Preview and create page to make sure you understand the alarm you're creating. In your own words, give an example of what could trigger this alarm.
15. Click **Create alarm**.

Your email address was listed as a subscription, or communication endpoint, to the topic, meaning a message should be sent to your address if the alarm is triggered. However, to reduce spamming, you must first confirm your email subscription before you'll receive notices:

16. To confirm your email subscription to the topic you created, go to your email account, open the email from AWS Notifications, and click **Confirm subscription**.
17. Return to your AWS console and click the **Refresh** button (it shows a circle arrow icon) above the list of alarms. What is the initial state of the alarm?
18. If your alarm is not currently in the OK state, continue refreshing the data until your alarm reaches the OK state.
19. Click the alarm's name to see more information about it. **Take a screenshot** of the Details section of your alarm; submit this visual with your answers to this project's questions.
20. Currently, only your email address is subscribed to the alarm's topic. To see all current subscriptions in SNS (Simple Notification Service), click **Services**. In the Application Integration group, click **Simple Notification Service**. In the navigation pane, click **Topics**. Click the topic you created. What is the status of your email subscription? If there are any problems indicated for the email subscription, troubleshoot those now.

Reflection Discussion 1

As you read about in this chapter, you use many kinds of networks nearly every day, such as when you check your email, post on social media, use your smartphone, make a payment at a store, or even just drive down the road. Perhaps you've had some experience working with networks, either setting up a network or troubleshooting problems. Did you set up your own home network? Have you had to troubleshoot a problem with your employer's network?

Consider the following questions:

› What did you notice about how devices communicate with each other?

› What solutions did you find to problems you encountered?

› What questions do you have now that warrant further research?

Go to the discussion forum in your school's LMS (learning management system). Write a post of at least 100 words discussing your thoughts about the kinds of experiences you've had with networks, what you learned in those experiences, and what more you would like to learn. Then respond to two of your classmates' threads with posts of at least 50 words discussing their comments and ideas. Use complete sentences and check your grammar and spelling. Try to ask open-ended questions that encourage discussion, and remember to respond to people who post on your thread. Use the rubric in Table 1-1 to help you understand what is expected of your work for this assignment.

Table 1-1 Grading rubric for Reflection Discussion 1

Task	Novice	Competent	Proficient	Earned
Initial post	Generalized statements about experiences working with networks **30 points**	Some specific statements with examples about experiences working with networks and learning from those experiences **40 points**	Self-reflective discussion with specific and thoughtful statements about experiences working with networks, learning from those experiences, and questions for further research **50 points**	
Initial post: Mechanics	• Length < 100 words • Several grammar and spelling errors **5 points**	• Length = 100 words • Occasional grammar and spelling errors **7 points**	• Length > 100 words • Appropriate grammar and spelling **10 points**	
Response 1	Brief response showing little engagement or critical thinking **5 points**	Detailed response with specific contributions to the discussion **10 points**	Thoughtful response with specific examples or details and open-ended questions that invite deeper discussion of the topic **15 points**	
Response 2	Brief response showing little engagement or critical thinking **5 points**	Detailed response with specific contributions to the discussion **10 points**	Thoughtful response with specific examples or details and open-ended questions that invite deeper discussion of the topic **15 points**	
Both responses: Mechanics	• Length < 50 words each • Several grammar and spelling errors **5 points**	• Length = 50 words each • Occasional grammar and spelling errors **7 points**	• Length > 50 words each • Appropriate grammar and spelling **10 points**	
			Total	

Solutions to Self-Check Questions

Section 1-1: The Language of Computer Networking

1. You plug your new printer into a USB port on your computer. What kind of network supports this connection?

Answer: d. PAN

Explanation: A PAN (personal area network) includes devices connected within an area of a few meters, such as smartphones, music players, wireless keyboard or speakers, and a USB-connected printer.

2. You connect your home network to your Internet provider using a single fiber cable. What technology allows you to download and upload data over this connection at the same time?

Answer: b. Multiplexing

Explanation: Multiplexing is the transmission of multiple signals on one medium at the same time by altering each signal slightly to keep them from interfering with one another.

Section 1-2: The Big Picture of Networks

3. You plug your laptop into your local network's router and use your browser to visit a website. What type of device allows your router to communicate with your Internet provider's network?

Answer: b. Modem

Explanation: A modem allows communication over a DSL or cable connection between a local network and a wide area network.

4. You need to make some changes to a file stored on your office's network. On which device is the file located?

Answer: b. Server

Explanation: Servers store shared or private user files that can be accessed remotely.

Section 1-3: Common Network Examples

5. What kind of protocols support addressing and communication over the Internet?

Answer: b. TCP/IP

Explanation: The Internet "talks" in TCP/IP to provide an addressing scheme and establish communication connections, and users must use software that supports the TCP and IP protocols.

6. You're setting up a small office network with a few desktop computers and a file server. You want to make sure only certain network users have access to the file server. What device will you need to configure to segment the network?

Answer: a. Switch

Explanation: The switches that connect local area networks can help manage network segmentation as well, such as when separating some traffic from other network traffic.

7. Your school hosts its own cloud to provide students with virtual desktops. These desktops give students access to expensive software that most students couldn't afford to purchase on their own. Your school also stores student files in a cloud service that requires an Internet connection for students to access their files, even when they're on campus. What kind of cloud architecture is your school using?

Answer: c. Hybrid

Explanation: In a hybrid cloud, virtualized resources at a remote location (such as the file storage accessed over the Internet) and physical or virtual resources in the local datacenter (such as servers hosting the virtual desktops) are connected and interact at a functional level that is invisible to users.

Section 1-4: Network Architectures

8. Which of these protocols do network admins use to help them identify problems on a network?

Answer: d. SNMP

Explanation: SNMP allows the numerous elements within a computer network to be managed from a single point, including receiving and processing error messages to identify problems.

9. Which OSI layer provides address information for a message to travel from a workstation to a router?

Answer: b. Data link

Explanation: The data link layer prepares a frame for transmission from the user workstation to a router sitting between the LAN and the Internet. The frame contains address information for this local transmission.

10. A rat chews through a cable connecting two switches on your network. What layer of the OSI model has been compromised?

Answer: d. Physical

Explanation: The physical layer is where the actual transmission of data occurs over a physical wire, such as a network cable, or by radio signal, such as with Wi-Fi. Problems at this layer usually involve physical equipment such as cables or access points.

Section 1-5: Cloud Computing

11. When schools suddenly closed and classes were held over the Internet instead, your company's video conferencing software suddenly needed to host five times more traffic than usual. What feature of your cloud-hosted web app allowed your service to adapt to the changing demand?

Answer: b. Elasticity

Explanation: Elasticity allows resources to scale up or down quickly in response to changing needs, and