Prepare. Practice. Pass the Test!

CompTIA® NETWORK+®

GET CERTIFIED!

EXAM N10-008

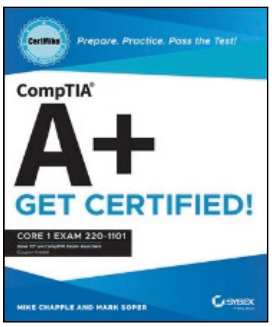
Save 10% on CompTIA Exam Vouchers
Coupon Inside!

MIKE CHAPPLE AND CRAIG ZACKER

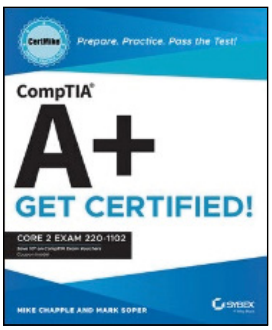
SYBEX®
A Wiley Brand

Wiley Books in the CertMike Series

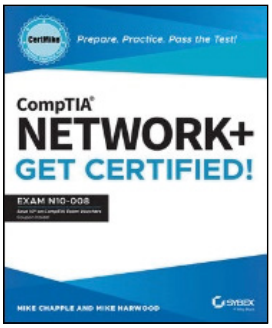
CompTIA ITF+ CertMike: *Prepare. Practice. Pass the Test! Get Certified! Exam FC0-U61*
by Mike Chapple
(ISBN 9781119897811)



CompTIA A+ CertMike: *Prepare. Practice. Pass the Test! Get Certified! Core 1 Exam 220-1101*
by Mike Chapple and Mark Soper
(ISBN 9781119898092)



CompTIA A+ CertMike: *Prepare. Practice. Pass the Test! Get Certified! Core 2 Exam 220-1102*
by Mike Chapple and Mark Soper
(ISBN 9781119898122)



CompTIA Network+ CertMike: *Prepare. Practice. Pass the Test! Get Certified! Exam N10-008*
by Mike Chapple and Craig Zacker
(ISBN 9781119898153)

CompTIA® Network+® CertMike

Prepare. Practice. Pass the Test! Get Certified!

CompTIA® Network+® CertMike

Prepare. Practice. Pass the Test! Get Certified!

Exam N10-008

Mike Chapple
Craig Zacker

SYBEX®
A Wiley Brand

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada and the United Kingdom.

ISBN: 978-1-119-89815-3
ISBN: 978-1-119-89817-7 (ebk.)
ISBN: 978-1-119-89816-0 (ebk.)

Library of Congress Control Number: 2023933804

Cover design: Wiley

Acknowledgments

From Mike Chapple:

This book marks the start of a new series of CertMike Test Prep books, and I'd first like to thank the people who helped shape the vision for this series. The original idea was hatched over breakfast with two very supportive editors from the Wiley team: Ken Brown and Jim Minatel. I've worked with both Jim and Ken on many books over many years, and they're both insightful industry experts who know what it takes to produce a great book.

Craig Zacker did the heavy lifting of putting this book together, and I am grateful to him for lending this series his expertise on end-user support and the Network+ exam.

I'd also like to extend a special thank-you to my agent, Carole Jelen of Waterside Productions. Carole is also an experienced industry pro who can deftly navigate the murky waters of publishing. Carole is the one who pushed me to create my own series.

Of course, the creation of any book involves a tremendous amount of effort from many people other than the authors. I truly appreciate the work of Adaobi Obi Tulton, the project editor. Adaobi and I have now worked together on many books and she keeps the train on the tracks! I'd also like to thank Buzz Murphy, the technical editor, who provided insightful advice and gave wonderful feedback throughout the book, and Saravanan Dakshinamurthy, production editor, who guided me through layouts, formatting, and final cleanup to produce a great book. I would also like to thank the many behind-the-scenes contributors, including the graphics, production, and technical teams who make the book and companion materials into a finished product.

Finally, I would like to thank my family, who supported me through the late evenings, busy weekends, and long hours that a book like this requires to write, edit, and get to press.

About the Authors

Mike Chapple, PhD, is the author of the best-selling *CISSP (ISC)² Certified Information Systems Security Professional Official Study Guide* (Sybex, 2021) and the *CISSP (ISC)² Official Practice Tests* (Sybex, 2021). He is an information technology professional with two decades of experience in higher education, the private sector, and government.

Mike currently serves as Teaching Professor in the IT, Analytics, and Operations department at the University of Notre Dame's Mendoza College of Business, where he teaches undergraduate and graduate courses on cybersecurity, cloud computing, data management, and business analytics.

Before returning to Notre Dame, Mike served as executive vice president and chief information officer of the Brand Institute, a Miami-based marketing consultancy. Mike also spent four years in the information security research group at the National Security Agency and served as an active duty intelligence officer in the U.S. Air Force.

Mike has written more than 25 books. He earned both his B.S. and Ph.D. degrees from Notre Dame in computer science and engineering. Mike also holds an M.S. in computer science from the University of Idaho and an MBA from Auburn University. Mike holds the IT Fundamentals (ITF+), Cybersecurity Analyst+ (CySA+), Data+, Security+, Certified Information Security Manager (CISM), Certified Cloud Security Professional (CCSP), and Certified Information Systems Security Professional (CISSP) certifications.

Learn more about Mike and his other security certification materials at his website, `CertMike.com`.

Craig Zacker is the author or co-author of dozens of books, manuals, articles, and websites on computer and networking topics. He has also been an English professor, a technical and copy editor, a network administrator, a webmaster, a corporate trainer, a technical support engineer, a minicomputer operator, a literature and philosophy student, a library clerk, a photographic darkroom technician, a shipping clerk, and a newspaper boy.

About the Technical Editor

George B. Murphy (Buzz), CISSP, CCSP, SSCP, CASP, CDWA, CISM, CRISC, CIPT, PCSA, ITIL, is a public speaker, corporate trainer, author, and CEO of CyberSpace Intelligence International who has consulted with cybersecurity professionals around the world over the past 25 years with training courses, seminars, and consulting presentations on a variety of technical and cybersecurity topics. A former Dell technology executive, he has addressed audiences at RSA, COMDEX, SecureWorld Conference, World Security Conference, NetWorld, and the National Computer Conference as well as major corporations and educational institutions such as Princeton University, Oak Ridge, CERN, and major U.S. government agencies. Buzz has earned more than 29 IT and cybersecurity certifications from such prestigious organizations as (ISC)^2, CompTIA, PMI, and Microsoft, and other industry certification organizations, and has authored 12 Cyber Security textbooks. He is an (ISC)^2 Authorized Instructor.

Contents at a Glance

Contents

Introduction

If you're preparing to take the Network+ exam, you might find yourself overwhelmed with information. This exam covers a very broad range of topics, and it's possible to spend weeks studying each one of them. Fortunately, that's not necessary!

As part of the CertMike Test Prep series, this book is designed to help you focus on the specific knowledge that you'll need to pass the exam. CompTIA publishes a detailed list of exam objectives, and this book is organized around those objectives. Each chapter clearly states the single objective that it covers and then concisely covers the material you need to know about that objective.

You'll find two important things at the end of each chapter: Exam Essentials and Practice Questions. The CertMike Exam Essentials distill the major points from the chapter into just a few bullet points. Reviewing the Exam Essentials is a great way to prepare yourself right before the exam. We've also recorded a free audio version of the Exam Essentials that you'll find on the book's companion website at `www.wiley.com/go/sybextestprep`. They're great listening when you're in the car, at the gym, or mowing the lawn!

Each chapter concludes with two Practice Questions that are designed to give you a taste of what it's like to take the exam. You'll find that they're written in the same style as the Network+ exam questions and have detailed explanations to help you understand the correct answer. Be sure to take your time and thoroughly read these questions.

Finally, the book's website includes a full-length practice exam that you can use to assess your knowledge when you're ready to take the test. Good luck on the Network+ exam!

NOTE

Don't just study the questions and answers! The questions on the actual exam will be different from the Practice Questions included in this book. The exam is designed to test your knowledge of a concept or objective, so use this book to learn the objectives behind the questions.

THE NETWORK+ CERTIFICATION

Network+ is designed to be a vendor-neutral certification for those seeking to demonstrate their networking expertise. CompTIA recommends this certification for individuals who want to develop careers in IT infrastructure, specifically in the areas of troubleshooting, configuring, and managing networks. Common job roles held by Network+ certified individuals include the following:

- Junior network administrator
- Network engineer
- NOC technician

- Cable technician
- Data center support technician
- System administrator
- Telecommunications technician

The exam covers five major domains of knowledge:

1. Networking Fundamentals
2. Network Implementations
3. Network Operations
4. Network Security
5. Network Troubleshooting

These five areas include a range of topics, from securing networks to configuring subnets, while focusing heavily on the core knowledge expected of all networking professionals.

The Network+ exam uses a combination of standard multiple-choice questions and performance-based questions that require you to manipulate objects on the screen. This exam is designed to be straightforward and not to trick you. If you know the material in this book, you will pass the exam.

The exam costs $348 in the United States, with roughly equivalent prices in other locations around the globe. You can find more details about the Network+ exam and how to take it at

`www.comptia.org/certifications/network#examdetails`

You'll have 90 minutes to take the exam and will be asked to answer up to 90 questions during that time period. Your exam will be scored on a scale ranging from 100 to 900, with a passing score of 720.

NOTE

CompTIA frequently does what is called *item seeding*, which is the practice of including unscored questions on exams. It does so to gather psychometric data, which is then used when developing new versions of the exam. Before you take the exam, you will be told that your exam may include these unscored questions. So, if you come across a question that does not appear to map to any of the exam objectives—or for that matter, does not appear to belong in the exam—it is likely a seeded question. You never really know whether or not a question is seeded, however, so always make your best effort to answer every question.

Taking the Exam

Once you are fully prepared to take the exam, you can visit the CompTIA website to purchase your exam voucher:

`https://store.comptia.org`

Currently, CompTIA offers two options for taking the exam: an in-person exam at a testing center and an at-home exam that you take on your own computer.

TIP

This book includes a coupon that you may use to save 10 percent on your CompTIA exam registration.

In-Person Exams

CompTIA partners with Pearson VUE's testing centers, so your next step will be to locate a testing center near you. In the United States, you can do this based on your address or your zip code, while non-U.S. test takers may find it easier to enter their city and country. You can search for a test center near you at the Pearson Vue website, where you will need to navigate to "Find a test center."

`www.pearsonvue.com/comptia`

Now that you know where you'd like to take the exam, simply set up a Pearson VUE testing account and schedule an exam on their site.

On the day of the test, take two forms of identification, and be sure to show up with plenty of time before the exam starts. Remember that you will not be able to take your notes, electronic devices (including smartphones and watches), or other materials in with you.

At-Home Exams

CompTIA began offering online exam proctoring in 2020 in response to the coronavirus pandemic. As of this writing, the at-home testing option was still available and appears likely to continue. Candidates using this approach will take the exam at their home or office and be proctored over a webcam by a remote proctor.

Due to the rapidly changing nature of the at-home testing experience, candidates wishing to pursue this option should check the CompTIA website for the latest details.

After the Exam

Once you have taken the exam, you will be notified of your score immediately, so you'll know if you passed the test right away. You should keep track of your score report with your exam registration records and the email address you used to register for the exam.

After you earn the Network+ certification, you're required to renew your certification every three years by either earning an advanced certification, completing a CertMaster continuing education program, or earning 20 continuing education units over a three-year period.

Many people who earn the Network+ credential use it as a stepping stone to earning other certifications in their areas of interest. Those interested in end-user support work toward the A+ credential, data analytics professionals might go on to earn the Data+ certification, and the Security+ program is a gateway to a career in cybersecurity.

WHAT DOES THIS BOOK COVER?

This book covers everything you need to know to pass the Network+ exam. It is organized into five parts, each corresponding to one of the five Network+ domains.

Part I: Domain 1.0: Networking Fundamentals

Chapter 1: OSI Model
Chapter 2: Network Topologies
Chapter 3: Cables and Connectors
Chapter 4: IP Addressing
Chapter 5: Ports and Protocols
Chapter 6: Network Services
Chapter 7: Network Architecture
Chapter 8: Cloud Computing

Part II: Domain 2.0: Network Implementations

Chapter 9: Network Devices
Chapter 10: Routing and Bandwidth Management
Chapter 11: Switching
Chapter 12: Wireless Standards

Part III: Domain 3.0: Network Operations

Chapter 13: Network Availability
Chapter 14: Organizational Documents and Policies
Chapter 15: High Availability and Disaster Recovery

Part IV: Domain 4.0: Network Security

Chapter 16: Security Concepts
Chapter 17: Network Attacks
Chapter 18: Network Hardening
Chapter 19: Remote Access
Chapter 20: Physical Security

Part V: Domain 5.0: Network Troubleshooting

Chapter 21: Network Troubleshooting Methodology
Chapter 22: Troubleshooting Cable Connectivity
Chapter 23: Network Software Tools and Commands
Chapter 24: Troubleshooting Wireless Connectivity
Chapter 25: Troubleshooting Network Issues

Study Guide Elements

This study guide uses a number of common elements to help you prepare. These include the following:

Exam Tips Throughout each chapter, we've sprinkled practical exam tips that help focus your reading on items that are particularly confusing or important for the exam.

CertMike Exam Essentials The Exam Essentials focus on major exam topics and critical knowledge that you should take into the test. The Exam Essentials focus on the exam objectives provided by CompTIA.

Practice Questions Two questions at the end of each chapter will help you assess your knowledge and if you are ready to take the exam based on your knowledge of that chapter's topics.

Additional Study Tools

This book comes with a number of additional study tools to help you prepare for the exam. They include the following:

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

Sybex Test Preparation Software

Sybex's test preparation software lets you prepare with electronic test versions of the Practice Questions from each chapter and the Practice Exam that is included in this book. You can build and take tests on specific domains or by chapter, or cover the entire set of Network+ exam objectives using randomized tests.

Audio Review

I've (Mike) recorded an audio review where I read each of the sets of chapter Exam Essentials. This provides a helpful recap of the main material covered on the exam that you can use while you're commuting, working out, or relaxing.

> **NOTE**
>
> Like all exams, the Network+ certification from CompTIA is updated periodically and may eventually be retired or replaced. At some point after CompTIA is no longer offering this exam, the old editions of our books and online tools will be retired. If you have purchased this book after the exam was retired, or are attempting to register in the Sybex online learning environment after the exam was retired, please know that we make no guarantees that this exam's online Sybex tools will be available once the exam is no longer available.

EXAM N10-008 EXAM OBJECTIVES

CompTIA goes to great lengths to ensure that its certification programs accurately reflect the IT industry's best practices. They do this by establishing committees for each of its exam programs. Each committee consists of a small group of IT professionals, training providers, and publishers who are responsible for establishing the exam's baseline competency level and who determine the appropriate target-audience level.

Once these factors are determined, CompTIA shares this information with a group of hand-selected subject matter experts (SMEs). These folks are the true brainpower behind the certification program. The SMEs review the committee's findings, refine them, and shape them into the objectives that follow this section. CompTIA calls this process a job-task analysis.

Finally, CompTIA conducts a survey to ensure that the objectives and weightings truly reflect job requirements. Only then can the SMEs go to work writing the hundreds of questions needed for the exam. Even so, they have to go back to the drawing board for further refinements in many cases before the exam is ready to go live in its final state. Rest assured that the content you're about to learn will serve you long after you take the exam.

CompTIA also publishes relative weightings for each of the exam's objectives. The following table lists the five Network+ objective domains and the extent to which they are represented on the exam.

Domain	% of Exam
1.0 Networking Fundamentals	24%
2.0 Network Implementations	19%
3.0 Network Operations	16%
4.0 Network Security	19%
5.0 Network Troubleshooting	22%

N10-008 CERTIFICATION EXAM OBJECTIVE MAP

Objective	Chapter
1.0 Networking Fundamentals	
1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts	1
1.2 Explain the characteristics of network topologies and network types	2
1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution	3
1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes	4
1.5 Explain common ports and protocols, their application, and encrypted alternatives	5
1.6 Explain the use and purpose of network services	6
1.7 Explain basic corporate and datacenter network architecture	7
1.8 Summarize cloud concepts and connectivity options	8
2.0 Network Implementations	
2.1 Compare and contrast various devices, their features, and their appropriate placement on the network	9
2.2 Compare and contrast routing technologies and bandwidth management concepts	10
2.3 Given a scenario, configure and deploy common Ethernet switching features	11
2.4 Given a scenario, install and configure the appropriate wireless standards and technologies	12

Objective	Chapter
3.0 Network Operations	
3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability	13
3.2 Explain the purpose of organizational documents and policies	14
3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution	15
4.0 Network Security	
4.1 Explain common security concepts	16
4.2 Compare and contrast common types of attacks	17
4.3 Given a scenario, apply network hardening techniques	18
4.4 Compare and contrast remote access methods and security implications	19
4.5 Explain the importance of physical security	20
5.0 Network Troubleshooting	
5.1 Explain the network troubleshooting methodology	21
5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools	22
5.3 Given a scenario, use the appropriate network software tools and commands	23
5.4 Given a scenario, troubleshoot common wireless connectivity issues	24
5.5 Given a scenario, troubleshoot general networking issues	25

NOTE

Exam objectives are subject to change at any time without prior notice and at CompTIA's discretion. Please visit CompTIA's website (`www.comptia.org`) for the most current listing of exam objectives.

HOW TO CONTACT THE PUBLISHER

If you believe you have found a mistake in this book, please bring it to our attention. At John Wiley & Sons, we understand how important it is to provide our customers with accurate content, but even with our best efforts an error may occur.

In order to submit your possible errata, please email it to our Customer Service Team at `wileysupport@wiley.com` with the subject line "Possible Book Errata Submission."

CompTIA® Network+® CertMike

Prepare. Practice. Pass the Test! Get Certified!

PART I

Domain 1.0: Networking Fundamentals

Networking Fundamentals is the first domain of CompTIA's Network+ exam. It provides the foundational knowledge that IT professionals need to work with common network devices and technologies. This domain has eight objectives:

1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.
1.2 Explain the characteristics of network topologies and network types.
1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.
1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes.
1.5 Explain common ports and protocols, their application, and encrypted alternatives.
1.6 Explain the use and purpose of network services.
1.7 Explain basic corporate and datacenter network architecture.
1.8 Summarize cloud concepts and connectivity options.

Questions from this domain make up 24% of the questions on the Network+ exam, so you should expect to see approximately 22 questions on your test covering the material in this part.

CHAPTER 1

OSI Model

Objective 1.1: Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.

The OSI reference model can serve as a roadmap to many of the other concepts covered on the Network+ exam, providing a common lexicon that enables people working with these processes to communicate more easily.

In this chapter, you'll learn everything you need to know about Network+ Objective 1.1, including the following topics:

- **OSI model**
- **Data encapsulation and decapsulation within the OSI model context**

OSI MODEL

The *Open Systems Interconnection (OSI) reference model* is an architectural diagram of network communications. The model defines a highly complex process by dividing it into its component elements, in this case seven discrete layers, as shown in Figure 1.1.

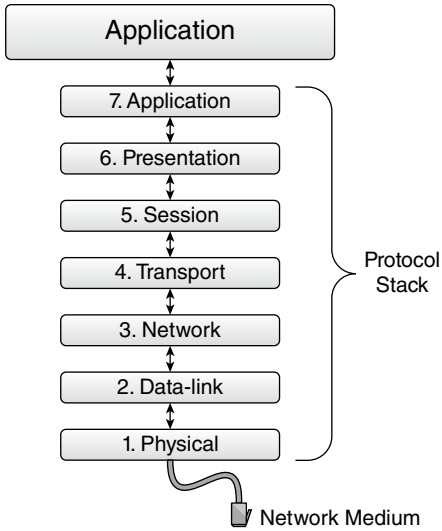


FIGURE 1.1 The seven layers of the OSI reference model

The seven layers of the model correspond to various network communications processes (called protocols) running on a computer. Table 1.1 lists the model layers, their functions, and the protocols that implement them. These protocols are covered in more detail throughout this book.

EXAM TIP

Memorizing this table is a good idea, as many Network+ exam questions reference the various layers of the OSI model, their functions, and their protocols. An easy way to remember the order of the layers is with the mnemonic "Please Do Not Throw Sausage Pizza Away."

TABLE 1.1 OSI reference model layers

Number	Layer	Main functions	Protocols
7	Application	File, print, messaging, and other services	DNS, FTP, HTTP, POP3, SMTP, SNMP, DHCP
6	Presentation	Syntax translation	
5	Session	Dialog control, dialog separation	

Number	Layer	Main functions	Protocols
4	Transport	Data segmentation, packet acknowledgment, error detection and correction, flow control, port identification	TCP, UDP
3	Network	Addressing, routing, error detection, protocol identification	IP, IPv4, IPv6, ICMP
2	Data Link	Framing, media access control, protocol identification	IEEE 802.3 (Ethernet), IEEE 802.11 (Wi-Fi)
1	Physical	Network interface hardware, binary signaling	Twisted pair, fiber-optic, Wi-Fi

EXAM TIP

The layers of the OSI model are numbered from the bottom of the stack to the top. The physical layer at the bottom is designated as layer 1 and the application layer at the top as layer 7. In some reference works and product documentation, the model layers are referenced by number instead of name.

A *protocol* is a language that computers use to communicate with each other. Collectively, the processes running on the seven layers of the model are called the *protocol stack*. The network medium (whether a copper cable, fiber-optic cable, or wireless) connects to the physical layer at the bottom of the stack, and the signals entering at this layer travel up through the layers of the stack to the top. In the same way, data being sent over the network by software running at the top of the stack travel down through the layers and out to the network using the connected medium.

This vertical communication between the layers of the protocol stack takes the form of services that each layer provides for the layer above and requests from the layer below. For example, when an email client application sends a message, it typically generates a request for the services of the Simple Mail Transfer Protocol (SMTP), running at the application layer. SMTP then passes the request down to the next lower layer, which hands it off to the next layer, and so forth, until it reaches the bottom layer and is transmitted over the network.

The server receiving the transmission over the network then begins the same process in reverse, passing the message up through the layers of its own protocol stack until it reaches a mail server application running on the computer. The protocols running at specific layers of the OSI model have complementary functions that make network communication possible. The protocols at the individual layers of the model can therefore be said to communicate virtually with their counterparts on other systems.

One of the objectives of the OSI model was to define a networking architecture that enables manufacturers to create products that communicate readily with those of other manufacturers. As long as two computers are running compatible protocols at each layer of the OSI model, communication between them is theoretically possible, even if they are using different hardware and software.

While there have been other protocols over the years, LANs today nearly always run Ethernet or Wi-Fi at the physical and data link layers, *Internet Protocol (IP)* at the network layer, *Transmission Control Protocol (TCP)* and *User Datagram Protocol (UDP)* at the transport layer, and a collection of *Transmission Control Protocol/Internet Protocol (TCP/IP)* protocols and services at the application layer.

This TCP/IP protocol suite has a layered architecture similar to that of the OSI model, but it has only four layers, as shown in Table 1.2, and the layers do not correspond exactly to those of the OSI model. Some documents, such as the Requests for Comments (RFCs) that define the various TCP/IP protocols, reference the layers of the TCP/IP model instead of the OSI model layers.

TABLE 1.2 Corresponding OSI model and TCP/IP layers

OSI model layers	TCP/IP layers
Application	Application
Presentation	
Session	
Transport	Transport
Network	Internet
Data Link	Link
Physical	

The seven layers of the OSI reference model are described in more detail in the following sections.

Layer 1: The Physical Layer

The physical layer, as the name implies, provides the actual physical connection between the computer and the network. The hardware implementing the physical layer in a computer—called a *network interface adapter*—typically includes either a connector for a network cable or a transceiver that provides wireless connectivity. In the network

communications architecture, the physical layer specification is responsible for providing the following elements:

Network Medium The technology that carries signals from one computer to another, such as copper-based cable, fiber-optic cable, or radio transmissions

Network Interface The connection between the computer and the network medium, such as a cable connector or a radio transceiver

Network Topology The arrangement of the network medium in the work site, such as the star topology typically used by cabled networks today

Network Installation The guidelines for the installation of the network medium, such as radio frequencies, maximum cable lengths, number of devices permitted, and proximity to other equipment

Network Signaling Specifies the nature of the signals: electrical, optical, or radio, which the devices use to transmit binary data over the network medium.

Computers communicate at the physical layer by generating signals and transmitting them over a network medium. For outgoing communications, the physical layer receives data from a protocol running on the layer above it (the data link layer), converts the data into a binary code appropriate for the medium, and transmits it over the network. In the same way, the physical layer receives incoming signals from the network and converts them into an appropriate form for the data link layer protocol.

These elements—the network medium, interface, topology, installation, and signaling scheme—are all typically defined by a single protocol specification. For example, a typical Ethernet physical layer specification might call for unshielded twisted pair (UTP) cable, installed in a star topology, with a maximum segment length of 100 meters, using RJ-45 connectors and an encoding scheme called Differential Manchester. Other Ethernet specifications call for fiber-optic or other network media, each with its own interface, topology, installation, and signaling characteristics. For more information on physical layer hardware, see Chapter 2, "Network Topologies and Types," and Chapter 3, "Cables and Connectors."

EXAM TIP

When preparing for the Network+ exam, it can be easy to get lost in details that are unlikely to appear in exam questions. It's only important to know the basic functions associated with each layer of the model and how those functions fit into the network communications process.

Layer 2: The Data Link Layer

The data link layer, layer 2 of the OSI model, is closely associated with the physical layer. The two together implement the computer's connection to and communication with the local area network (LAN) to which the device is attached. Selecting a protocol for the data

link layer also dictates the network medium options that are available at the physical layer. For more information on Ethernet variants and their supported cable types, see Chapter 3.

The functions that data link layer protocols typically perform include the following:

Frame Format The data link layer protocol packages the data passed down to it from the network layer in a protocol data unit called a frame. A *frame* consists of a header and a footer generated by the data link layer protocol, with the network layer data as the payload in between.

Addressing Every network interface adapter has a unique 6-byte identifier assigned to it by the manufacturer called a *media access control (MAC) address*. Data link layer frames use these addresses in their headers to identify the sender and recipient of each packet.

Protocol Identification Data link layer headers include a code that indicates which network layer protocol generated the data in each packet. This enables the data link layer protocol on the receiving system to pass incoming traffic up to the correct network layer process.

Error Detection The frame footer contains the result of a cyclical redundancy check (CRC) calculation performed on the frame's data payload by the sending system. The receiving system performs the same calculation and, if the results do not match, discards the packet.

Media Access Control (MAC) When a LAN has devices connected to a shared network medium, the data link layer protocol uses a media access control mechanism to prevent two devices from transmitting simultaneously and causing a data collision.

Physical Layer Specifications The data link layer protocol also includes specifications for the physical layer options associated with the protocol.

Most cabled LANs run the Ethernet protocol at the data link layer, the actual name for which is IEEE 802.3, after the standards published by the Institute of Electrical and Electronics Engineers. The functions just listed are all implemented as part of the Ethernet frame.

Layer 3: The Network Layer

The protocols running at the physical and data link layers of the OSI model are dedicated to local network communications only. For example, Ethernet is capable of transmitting frames to another computer or router on the LAN; it is not concerned with the delivery of the data to its final destination. That is the responsibility of the network layer protocol.

Network layer devices called routers connect individual networks together, forming an *internetwork*, or network of networks. A *router* is an intermediate system that only processes incoming packets as high as the network layer, as shown in Figure 1.2.

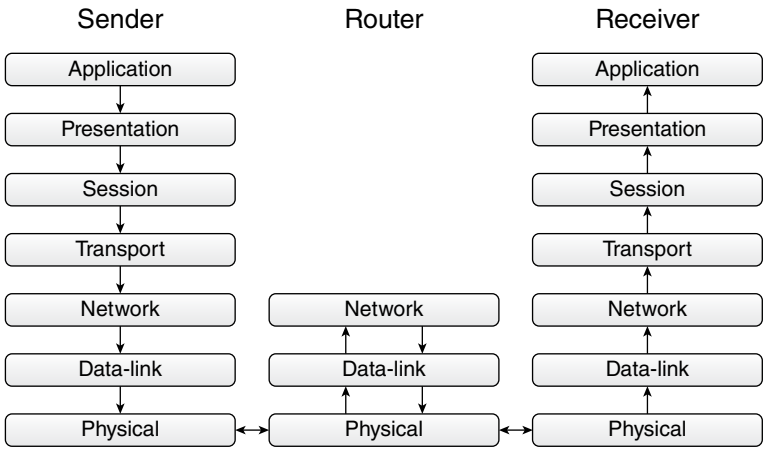


FIGURE 1.2 **Network traffic processed by an intermediate router**

The functions of a network layer protocol are as follows:

End-to-End Addressing The network layer protocol header contains the addresses of both the sending system and its final destination. Data link layer MAC addresses change for each leg of an internetwork journey, but network layer addresses always reflect a packet's starting point and its final destination.

Routing Routers are intermediate network layer devices that forward packets to other networks. Network layer protocols use routing tables to look up the addresses of other networks, so the router can forward packets to the correct destinations.

Fragmentation Networks can have different frame size limits, based on their *maximum transmission unit (MTU)* values, so if a single frame is too large to transmit over another network, the network layer protocol splits it into smaller fragments and transmits each fragment in a separate frame. The network layer protocol reassembles the fragments when they reach their final destination.

Protocol Identification Just as a data link layer protocol header contains a code to identify the network layer protocol that generated the data in the packet, the network layer protocol contains a code identifying the transport layer protocol that generated the data.

On TCP/IP networks, the primary protocol at the network layer is the *Internet Protocol (IP)*. IP exists in two versions: *IPv4*, with a 32-bit address space, which is the standard Internet protocol at the network layer, and *IPv6*, which is a newer version with a 128-bit address space. IPv6 has not yet been widely adopted for public Internet communications. For more information on the Internet Protocol, see Chapter 4, "IP Addressing."

IP functions are implemented in the header, which the protocol applies to the data it receives from the transport layer. This forms a unit called a *datagram*.

Layer 4: The Transport Layer

The term *TCP/IP* refers to the two protocols operating at the transport and network layers. The protocols at these two layers function together to provide a unified quality of service. IP, as noted earlier, provides addressing and routing services. The protocols at the transport layer of the OSI model provide additional end-to-end communication services, such as guaranteed delivery and flow control, to the adjacent layers, as needed.

Connection-Oriented and Connectionless Protocols

The OSI model standard recognizes two basic types of end-to-end protocol at the transport layer:

Connection-Oriented A connection-oriented protocol always establishes a connection between the sending and receiving systems before it transmits any application data. The systems do this by exchanging messages (called a *handshake*) containing *TCP flags* that confirm that both systems are available to send and receive data. After the transmission, another handshake terminates the connection. These additional messages (and a connection-oriented protocol's larger header) cause a significant increase in bandwidth overhead for this type of protocol. On most networks, the primary connection-oriented protocol at the transport layer is the *Transmission Control Protocol (TCP)*.

Connectionless A connectionless protocol provides no additional services other than the basic transmission of data, so there is no need for handshake messages and the header can be much smaller. This reduces the protocol's bandwidth overhead significantly. On most networks the primary connectionless protocol at the transport layer is the *User Datagram Protocol (UDP)*. The Internet Protocol (IP) running at the network layer is also connectionless.

Transport Layer Functions

The transport layer provides a variety of services for data transmissions. Most of the functions in the following list are provided by connection-oriented protocols such as TCP only. Only the protocol identification function is required for all protocols at the transport layer.

Data Segmentation A connection-oriented protocol accepts data from upper-layer application processes and splits it into segments of appropriate size for the network. Each segment is numbered so that they can be reassembled by the receiving system, even if they arrive out of order.

Packet Acknowledgment Connection-oriented protocols provide a *guaranteed delivery* service. The receiving system generates messages that acknowledge the successful receipt of packets from the sender.

Flow Control A connection-oriented mechanism to regulate the speed at which a sending system transmits data. The responses returned to the sender by the receiving system specify the size of a *sliding window*—that is, a buffer that holds incoming data. When the sliding window gets smaller, the sending system reduces its transmission speed to avoid overwhelming the receiver.

Signaled Error Correction A *signaled error* is a packet that has been discarded by the network layer protocol due to a CRC failure. The network layer protocol cannot correct errors, so it signals the transport layer protocol to retransmit the lost packets.

Unsignaled Error Detection and Correction The transport layer provides the only end-to-end error detection and correction mechanism for the entire packet. The transport layer protocol on the sending system performs a CRC calculation and includes the results in its header. The receiving system then performs the same calculation and compares the results. For any lost packets, the receiver alters the packet acknowledgment value in its header, causing the sender to retransmit the unacknowledged packets.

Port Identification Transport layer protocol headers always contain a code (called a *port*) identifying the application layer protocol that generated or will receive the packet's data.

The transport layer functions are implemented in headers applied by each protocol. Because it is a connection-oriented protocol with many functions, TCP has a large 20-byte header. UDP is connectionless and therefore needs only a comparatively small 8-byte header.

Layer 5: The Session Layer

The boundary between the transport layer and the session layer marks an important change in the functioning of the protocol stack. All of the communication functions, both end-to-end and local, that are needed to transmit data from one system to another over a TCP/IP network are handled by the bottom four layers of the OSI model. The session, presentation, and application layers assume that the communication services are functional and that any messages they need to send or receive will be handled correctly.

The top three layers of the OSI model do not have separate protocols to implement their functions in the TCP/IP suite. Instead, the session layer functions as something of a toolbox; the OSI model standard lists 22 functions performed at the session layer, but on a TCP/IP network, those functions are usually integrated into an application layer protocol. It is for this reason that the session, presentation, and application layers are often referenced collectively as the *upper layers*.

The functions associated with the session layer are mostly concerned with the establishment, maintenance, and termination of communications during a connection between two end systems, called a *session*. The maintenance of a session can be a complicated business requiring various session layer functions to initiate the dialog, maintain orderly communication, and then terminate it.

Two of the important functions used to manage a session include the following:

- **Dialog control:** Specifies the mode in which the systems communicate. *Simplex* mode is when only one of the computers is transmitting. In *half duplex*, also called *two-way alternate (TWA)* mode, the systems exchange a token, and only the computer with the token can transmit. In *full duplex*, also called *two-way simultaneous (TWS)* mode, there is no token, and the computers can transmit any time.
- **Dialog separation:** Calls for the creation of checkpoints in the data stream to separate functions.

Layer 6: The Presentation Layer

As noted earlier, each OSI model layer provides services to the layer above and requests services from the layer below. In the case of the presentation layer, its primary function is to provide pass-through services that enable application layer protocols to request session layer services. For each of the services at the session layer, there is a corresponding pass-through service at the presentation layer. This enables the upper layers to function as a single entity.

The presentation layer also includes a syntax translation service that enables two end systems to communicate, despite their use of data compression, encryption, or different bit-encoding algorithms.

Layer 7: The Application Layer

The application layer is the entrance point to the protocol stack for applications running on the computer. In some cases, the application is separate from the application layer protocol, but in others, the application and the application layer protocol are the same.

There are hundreds of application layer protocols, many more than at any of the other layers. This is because there are so many applications that require a variety of highly specific networking services.

DATA ENCAPSULATION

As outgoing data travels down through the protocol stack to the network medium, it undergoes a process called *data encapsulation*, which is the functional equivalent of putting a letter into an envelope for mailing. When an application produces data that needs to be transmitted over the network, it generates a request for one of the application layer protocols. This protocol generates a message, properly formatted for the application, and passes it down through the layers of the stack. The protocols at the lower layers then add their own data, such as addresses and codes, to implement their functions.

For example, when the application layer data reaches the transport layer, the protocol there generates a *Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) header* and adds it to the data. The TCP header includes *TCP flags* that the protocol uses to establish a connection between the sending and receiving systems and then break down the connection after the data transmission. The application layer request then becomes the *payload* in the transport layer segment or datagram, as shown in Figure 1.3.

The transport layer protocol then passes the data down to the network layer, which adds its own *Internet Protocol (IP) header*. The *maximum transmission unit (MTU)* value for the interface specifies the size of the largest IP datagram that can be transmitted over the network. Datagrams that are larger than the MTU are split into fragments for transmission. Finally, at the data link layer, all of the data from the layers above becomes the payload in a data link layer frame. The data link layer protocol typically adds both an *Ethernet header* and a footer to the payload, resulting in a packet that is ready for transmission.

For packets arriving at the destination system, the process occurs in reverse, with the data passed up through the OSI model layers, a process called *decapsulation*. Each layer processes the incoming packet by reading and stripping off the header and then passing the payload up to the correct protocol at the next higher layer.

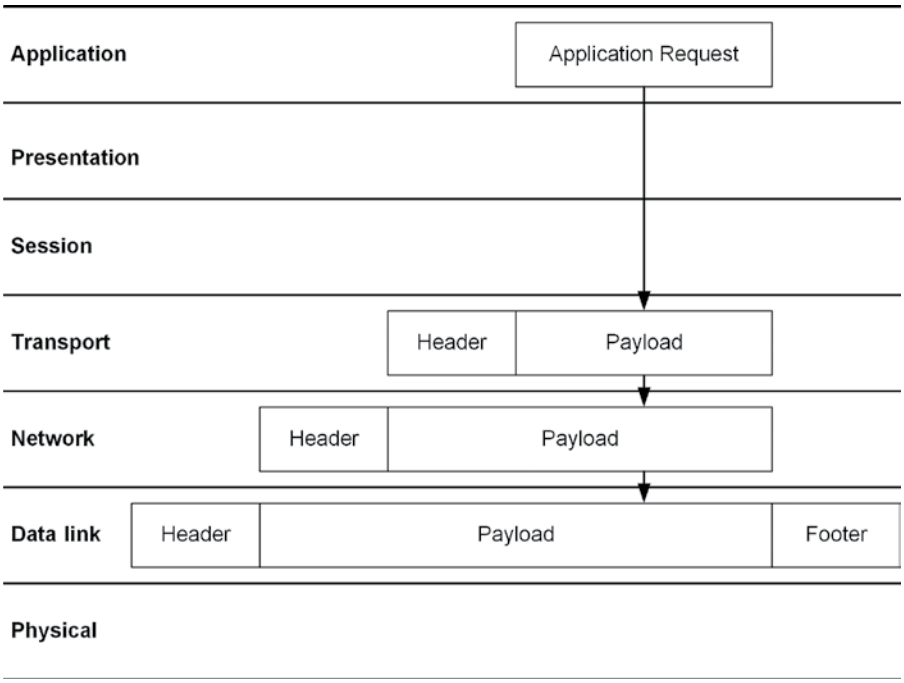


FIGURE 1.3 The data encapsulation process

CERTMIKE EXAM ESSENTIALS

- The OSI reference model divides the network communications process into seven layers. In order from the first layer to the seventh layer, these are the physical layer, the data link layer, the network layer, the transport layer, the session layer, the presentation layer, and the application layer. You can remember them in order using the mnemonic "Please Do Not Throw Sausage Pizza Away."
- Data encapsulation is the process by which the data generated by an application is packaged for transmission over the network through the application of headers by the protocols at the transport, network, and data link layers. When packets arrive at their destination, a decapsulation process occurs in which the protocols at each layer strip off their respective headers and pass the payload data up to the next layer.

Practice Question 1

There are several OSI model layers that provide error detection services, but only one that provides error correction as well. At which layer of the OSI model is there a protocol that provides both end-to-end error detection and correction?

A. Physical
B. Data link
C. Network
D. Transport

Practice Question 2

Which of the following OSI model layers specifies the address of each packet's sender and its ultimate recipient?

A. Data link
B. Network
C. Transport
D. Session

Practice Question 1 Explanation

A. is incorrect because the physical layer provides the connection to the network and implements the signaling algorithm that converts the packet data into the electrical, optical, or radio signals necessary for transmission. This layer does not manipulate or evaluate the data in any way, so it performs no error correction.

B. is incorrect because the data link layer is concerned only with local network communication. The data link layer performs a CRC calculation on each frame and includes the results in a frame check sequence field, but it cannot perform end-to-end error detection and has no error correction capability.

C. is incorrect because as a connectionless protocol, it has no packet acknowledgment capability and therefore no means of error correction. The network layer performs error detection by including a CRC code in its header. If a packet fails the CRC test, the network layer discards it and signals the loss to the transport layer.

D. is correct because TCP, a connection-oriented transport layer protocol, performs its own error detection, but it also includes a packet acknowledgment service. The segments transmitted during a TCP connection are numbered, so the acknowledgment messages generated by the receiver can specify the number of the last packet received correctly. The sender processes these messages and automatically retransmits any unacknowledged packets.

Correct Answer: D, Transport

Practice Question 2 Explanation

A. is incorrect because the data link layer is only concerned with local network communications. The frame's destination address does not identify the ultimate recipient of the packet, only the next recipient on the LAN.

B. is correct because IP, at the network layer, is the protocol responsible for end-to-end transmissions between the packet's sender and its ultimate recipient. The IP header therefore contains IP addresses that identify the two end systems.

C. is incorrect because the transport layer headers do not contain addresses for the end systems. The transport layer protocols, TCP and UDP, provide services that support the end-to-end network communication process, but they rely on the network layer for addressing.

D. is incorrect because the session layer provides functions that manage connections between end systems once they are established, but it does not have a dedicated protocol and has no addressing functionality.

Correct Answer: B, Network

CHAPTER 2

Network Topologies

Objective 1.2: Explain the characteristics of network topologies and network types.

This chapter examines the various types of networks that technicians encounter in their work, as well as the basic physical topologies that these networks use. These are fundamental networking concepts mentioned in many questions on the Network+ exam.

In this chapter, you'll learn everything you need to know about Network+ Objective 1.2, including the following topics:

- **Mesh**
- **Star/hub-and-spoke**
- **Bus**
- **Ring**
- **Hybrid**
- **Network types and characteristics**
- **Service-related entry points**
- **Virtual network concepts**
- **Provider links**

NETWORK TOPOLOGIES

In networking terminology, a *topology* is a definition of the manner in which a network medium is installed. Originally coined to describe cable installations, the topology of a

network specifies how the cables are installed and how the computers and other devices are connected to each other.

For example, the most commonly used topology in cabled local area networks (LANs) today is the *star topology* (see Figure 2.1), sometimes called a *hub-and-spoke topology* because of the diagram's resemblance to a wheel.

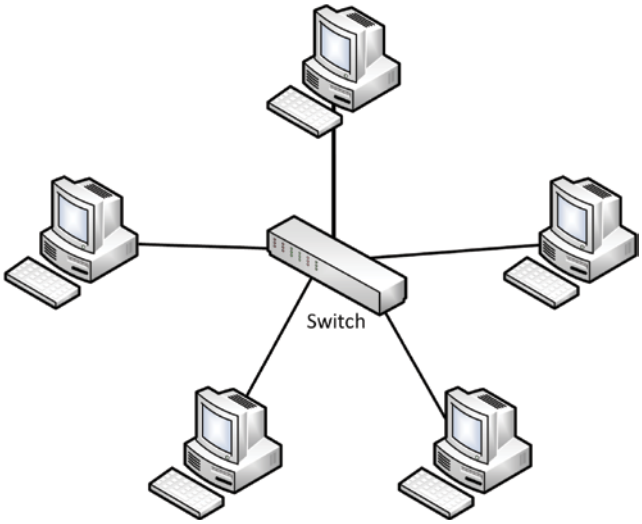


FIGURE 2.1 **A cabled local area network using a star topology**

In a star topology, each computer or other device has its own dedicated connection to a central cabling nexus called a *switch*. The switch relays the traffic it receives from each computer to the appropriate recipient on the network by transmitting it out through one of its other ports. Older star networks might use a hub instead of a switch. A hub is a physical layer device that forwards incoming traffic out through all of its ports instead of just one, forming a true shared network medium.

Virtually all cabled LANs installed today use the Ethernet protocol with unshielded twisted pair cable in a star topology. To build larger networks, it is possible to cable switches together, forming a hierarchical star topology in which the computers on all of the switches can communicate with each other.

Before the star topology became ubiquitous for cabled LANs, there were other topologies in use, including the following:

Bus Early Ethernet networks used coaxial cable in a *bus topology*, in which each device is connected to the next device, forming a chain. The bus topology is no longer used primarily because of its lack of fault tolerance. A cable break or a malfunctioning network interface adapter in one of the computers splits the network in two, with the devices on one segment unable to communicate with the other segment.