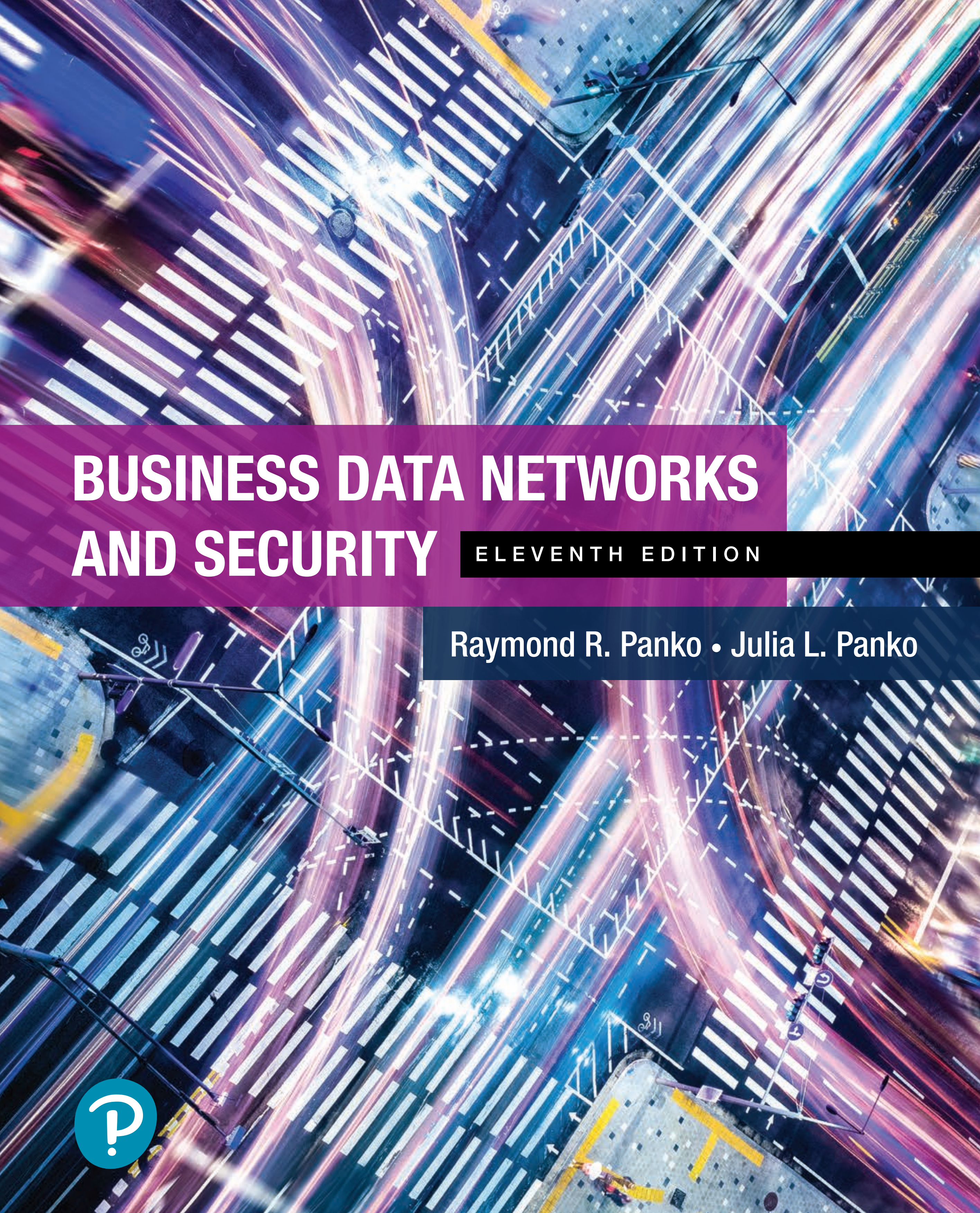

BUSINESS DATA NETWORKS AND SECURITY

ELEVENTH EDITION

Raymond R. Panko • Julia L. Panko

ELEVENTH EDITION

BUSINESS DATA NETWORKS AND SECURITY

Raymond R. Panko

University of Hawai`i at Mānoa

Julia L. Panko

Weber State University

Pearson

330 Hudson Street, NY NY 10013

Vice President, IT & Careers: Andrew Gilfillan
Senior Portfolio Manager: Samantha Lewis
Managing Producer: Laura Burgess
Associate Content Producer: Stephany Harrington
Portfolio Management Assistant: Madeline Houpt
Director of Product Marketing: Brad Parkins
Product Marketing Manager: Heather Taylor
Product Marketing Assistant: Jesika Bethea
Field Marketing Manager: Molly Schmidt
Field Marketing Assistant: Kelli Fisher
Cover Image: uschools/E+/Getty Images

Vice President, Product Model Management: Jason Fournier
Senior Product Model Manager: Eric Hakanson
Lead, Production and Digital Studio: Heather Darby
Digital Studio Course Producer: Jaimie Noy
Program Monitor: Christopher Rualizo, SPi Global
Project Manager: Neha Bhargava, Cenveo® Publisher Services
Composition: Cenveo Publisher Services
Printer/Binder: LSC Communications
Cover Printer: Phoenix Color
Text Font: Palatino LT Pro

Credits and acknowledgments borrowed from other sources and reproduced, with permission, in this textbook appear on the appropriate page within text or at the end of book.

Microsoft and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose. All such documents and related graphics are provided “as is“ without warranty of any kind. Microsoft and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall Microsoft and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services.

The documents and related graphics contained herein could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Microsoft and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time. Partial screen shots may be viewed in full within the software version specified.

Trademarks
Microsoft® Windows®, and Microsoft Office® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

Library of Congress Cataloging-in-Publication Data

Names: Panko, Raymond R., author. | Panko, Julia L., author.
Title: Business data networks and security / Raymond R. Panko, University of
Hawai’i at Mānoa, Julia L. Panko, Weber State University.
Description: Tenth edition. | Boston : Pearson, [2018] | Includes
bibliographical references and index.
Identifiers: LCCN 2017048586| ISBN 9780134817125 (alk. paper) | ISBN
0134817125 (alk. paper)
Subjects: LCSH: Business enterprises–Computer networks–Security measures. |
Computer networks–Management. | Computer networks–Security measures. |
Computer security.
Classification: LCC HD30.37 .P36 2018 | DDC 658.4/78–dc23 LC record available at
https://lccn.loc.gov/2017048586

Pearson

ISBN 10: 0134817125
ISBN 13: 9780134817125

To Sal Aurigemma. A great partner in crime in research and teaching.

This page intentionally left blank

BRIEF CONTENTS

Online Modules

This page intentionally left blank

CONTENTS

Online Modules

This page intentionally left blank

PREFACE FOR ADOPTERS

SIX QUESTIONS

This preface begins with six questions that adopters have when considering a textbook.

- What courses is this book used in?
- Why all the security?
- Does this book have the content your students need on the job market?
- Why does it have four principles chapters followed by chapters on specific technologies?
- Does this book have the support you need?
- Does this book have the support your students need?

What Courses use this Book?

- Introductory networking courses in information systems that prepare graduates to work in corporate IT departments use this book. It has the kind of knowledge they need to manage networking in corporations.
- It is used at both the undergraduate and graduate levels.
- Due to its extensive security content, some schools use it in a combined networking and security course. This requires covering the Appendix. Compared to the last edition, the Appendix considerably expands security content. Ideally, schools will have separate introductory network and security courses. Unfortunately, not all schools have that luxury.
- It *does not* focus on the very different needs of computer science students, who will build routers and switches in companies such as Cisco Systems. Instead, it focuses on how to manage and secure them, which is what networking professionals actually do in corporate IT departments. This still requires a lot of technical knowledge but not at the expense of job-required content.

Why all the Security?

In the last two decades, the need for network security knowledge has grown enormously in networking departments. It must be covered pervasively in networking courses. General security courses do not cover network-specific security, such as protecting access points with 802.11i security and knowing ways in which 802.11i security is bypassed in the real world.

Too many IS programs have had to choose between offering an introductory security course and an introductory networking course. This book lets the networking course serve as a decent introduction to security.

Does this Book have the Content your Students need?

This book is based on discussions with networking professionals and focuses on their current and emerging needs. We are especially concerned with potentially disruptive trends such as software-defined networking and high-density Wi-Fi networks. Here is a sampling of this type of job-ready content.

- The Internet of Things. The IoT will keep networking professionals very busy. Obviously, connecting lots and lots of small devices that talk to each other is going to require a lot of work. More broadly, IoT transmission standards and security are pretty raw, requiring even more effort to manage them. Chapter 7 deals with the standards and technologies competing for dominance (or at least survival) in the new market for the Internet of Things.
- Network management. Networking, like security, is more about management than it is about technology. Chapter 3 focuses on network management principles that must be applied in all networking projects. It also focuses on the pervasive importance of SNMP and the potentially disruptive impacts of SDN.
- Security threats and protections. Sun Tzu, in *The Art of War*, exhorted military leaders to know their enemies and to also know themselves. Chapter 4 covers the threat environment facing firms today and the countermeasures that companies can put into place to protect themselves. However, security begins with the first paragraph of the first chapter and continues throughout the book.
- Ethernet is covered in Chapter 5 with a holistic approach. The chapter covers the explosion in Ethernet standards, including those driven by Wi-Fi trends.
- Chapter 6 and much of Chapter 7 deal with Wi-Fi. They again cover technology, which is multifaceted and complex, and they cover wireless management and security. They deal with the current explosion in emerging standards, such as the potentially disruptive 802.11ax standard. Importantly, they show how 802.11i security can be broken.
- Chapter 7 also covers Internet of Things transmission protocols. IoT transmission turns many networking ideas on their heads, such as the desirability of high speed and long transmission distance.
- Chapters 8 and 9 deal with the Internet in context. A special focus is IPv6, which has now gone well beyond its infancy in both technology and use. This material is considerably updated from the previous edition. The material on IPsec is considerably stronger.
- Chapter 10 deals with networking beyond the customer premises. It focuses first on access technologies, then on WAN technologies that must be used beyond the Internet with its limited QoS abilities. The WAN technologies section focuses on leased lines, carrier Ethernet, and MPLS.
- Chapter 11 deals with networked applications—applications that need networks to operate. It focuses on management and security. In the past, some schools skipped this chapter because the material was covered in introductory courses. Actually, intro courses did not focus on the needs of networking professionals, and that is even more true today. This chapter brings the student into the worlds of cloud computing, HTTP/HTML, email, VoIP, and peer-to-peer applications, and it does so in terms of the knowledge that IT professionals need.

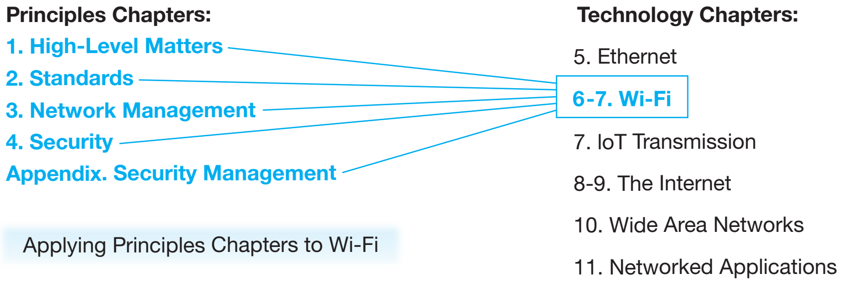

FIGURE P-1 Principles and Applications

Why have four Principles Chapters followed by Chapters on Specific Technologies?

Networking professionals want students to be able to *apply principles* to *real networking situations*. The book begins with four chapters that cover core network principles. It then applies these principles in a series of chapters that deal with Ethernet, Wi-Fi, Internet of Things transmission, the Internet, wide area networks, and networked applications. Figure P-1 illustrates this logical flow for Wi-Fi in Chapters 6 and 7. These chapters deal with how 802.11 Wi-Fi is used in business, how Wi-Fi operates at the physical and data link layers, Wi-Fi security threats and countermeasures, and key points in network management. This approach not only has students deal with technologies holistically. It also reinforces difficult core concepts such as layering.

Traditionally, networking books go “up through the layers.“ At the end of the course, students have all the knowledge of concepts and principles they need. However, they have limited experience in applying them, which is the whole point of the networking job.

Does this Book have the Support you need?

Teaching is hard. Teaching networking is harder. This book tries to make it a little easier.

PowerPoint Presentations and the Centrality of Figures The PowerPoint presentations are full lectures, not “a few significant figures.“ A core design principle of this book is that all key concepts are expressed in figures. Most of these figures are Illustrations. Some are “Study Figures,“ which essentially take notes for the student in areas that do not lend themselves to illustrations.

A core design principle of this book is that all key concepts are expressed in figures.

In line with this focus, the PowerPoint presentations are created directly from the figures. Figures are designed for this. Font size is larger in the PowerPoint slides, and several slide builds are often used to cover a figure well, but making them consistent with the figures has proven to be a great help for both teachers and students.

Adopters get an annotated version of each PowerPoint presentation. This can help you present the material in the slide. Sometimes we even add a little extra information for you to present.

The Instructor's Manual: The Usual Suspects with a Twist Of course, there is an Instructor's Manual with chapter teaching hints and answer keys for chapter questions. There is also a multiple-choice test item file and a test generator for exams.

Test Your Understanding Questions Now for the twist. Each chapter is broken into fairly small and highly targeted sections that end in a handful of Test Your Understanding questions. The Test Item File questions are linked to specific Test Your Understanding Questions. This means that you can assign certain questions for study and exclude others from exams. This lets you tailor exams to exactly the content points you wish your students to be responsible for.

Chapter-Opening Caselets Most chapters begin with brief caselets that students find interesting. In Chapter 1, for example, the caselet deals with how KrebsOnSecurity.com was hit with a denial-of-service attack that used small Internet of Things devices. Try assigning them for reading before the class and go over them as an interaction starter.

Does this Book have the Support your Students Need?

Let's face it. Networking and security are tough. They are highly conceptual. It is not primarily a matter of building cumulative skills as in programming courses. There are a lot of concepts, and they are often abstract or require the student to understand multiple steps. Networking professionals know that their careers are governed by the few things they need to know but don't in particular situations. Students must understand a lot just to be minimally competent.

Guided Reading One way the book helps students is by guided reading. There usually is a chapter-opening caselet to get the juices flowing. The flow that follows is broken up into fairly small pieces, with many headings. This helps the student focus on specific points. Figures show them how they fit together in a broader framework. Important concepts are displayed as key words. The index and glossary are linked to these key words. In addition, critically important concepts are often shown as callouts:

Students quickly learn to pay special attention to these callouts.

Fun Footnotes? Then there are fun footnotes. No, that is not an oxymoron. We limit chapter content to what all students should be able to master in an introduction to networking course. Sometimes, it is useful for some students if a bit more information is available to satisfy their curiosity. We put them in footnotes. They are not required reading, so they are not deadly detailed. Sometimes, footnotes are used for illustrative (semisnarky) comments.

Test Your Understanding Test Your Understanding questions help students stop after a section and see if they understood it. The best students learn that this is the best way to learn because networking is so cumulative, and moving on too fast is a capital mistake. At the end of the chapter are integrative questions that provide exercises for putting the things the student has learned together.

Exam Study These and other design elements help students prepare for exams as well.

- It is good for students to begin their exam prep by skimming for callouts and key words and being sure that they know them.
- Importantly, they should look at all of the figures and see if they can explain them. Again, figures include nearly all major content in the book.
- With this grounding, they should go over the test our understanding questions to see if they understand the detail. If they aren't sure, the text is right there to reread.

CONTENT FLOW

This section describes the flow of content in the book. It discusses each chapter briefly, giving its role in the book. It also describes changes from the previous edition. Overall, this edition is a 70% rewrite.

Chapter 1

This is the first of four "principles chapters" that give the student broad grounding in core concepts and principles needed to understand and deal with specific networking technologies such as Ethernet, Wi-Fi, and the Internet of Things.

Chapter 1 covers basic Internet terminology, concepts, and architectural principles. It begins with a broad introduction to the Internet. It then looks at the Internet from the outside by focusing on what hosts do to send and receive packets. It then looks inside the Internet to show how packets are delivered. On the Internet, routers are connected by data links, which may be single networks. The chapter ends with the distinction between Internet routers, personal access routers, and wireless access points. Students tend to confuse these terms. The Internet of Things is a major theme of the chapter.

Caselet The chapter begins with a caselet to show how KrebsOnSecurity.com was the victim of a distributed denial-of-service attack that used IoT devices.

Objectives After mastering the chapter, the student should be able to . . .

- Discuss how the Internet is changing and the security challenges these changes are creating.
- Explain basic concepts and terminology for the hosts (devices) that connect to the Internet.
- Explain basic concepts and terminology for the Internet itself.
- Explain basic concepts and terminology for single networks and their role on the Internet.
- Explain the distinctions between Internet routers and personal access routers; explain the differences between personal access routers and wireless access points.

Changes In the previous edition, Chapter 1 began with single networks and then showed how they are connected to the Internet. Students said that they wanted to know about the Internet first, so that is how we wrote it. Speed details were moved to Chapter 3 to give a cleaner flow. Students already know speed basics enough to put off details. Cloud computing was moved to Chapter 11 because it primarily deals with application architecture, which deals with the locus of processing. Application architecture is a major theme of that chapter. Standards architectures were moved to Chapter 2, although the first chapter introduces terminology that readies students for standards architectures.

Chapter 2

Chapter 2 presents standards principles and patterns that the student will see throughout networking. This chapter also introduces the main syntax elements of IP, TCP, UDP, and Ethernet.

The chapter, like the rest of the book, is based on the hybrid standards architecture that companies use in real life. They use OSI standards at the physical and data link layer. They primarily use TCP standards at the internet and transport layers. They use standards from a variety of sources for applications. TCP/IP have no problem working with OSI standards at lower layers, and nearly all applications can interface with TCP or UDP. Focusing only on OSI standards makes no sense in terms of corporate realities.

Caselet The chapter opens with a caselet on how Internet standards came to be and why they are sometimes weird.

Objectives After mastering the chapter, the student should be able to . . .

- Explain how Internet standards are made and why this approach is valuable.
- Provide the definitions of network standards and protocols and articulate their importance.
- Explain the OSI, TCP/IP, and Hybrid TCP/IP-OSI architectures and their standards agencies.
- Explain the purpose of each standards layer in the hybrid TCP/IP-OSI architecture, what is standardized at each layer, and which standards agency dominates standards at each layer.
- Explain message ordering in general and in HTTP and TCP.
- Explain message syntax in general and in IP packets, TCP segments, and UDP datagrams, and Ethernet frames.
- Demonstrate how application programs encode alphanumeric, decimal, and alternative data into bits (1s and 0s) before passing their messages to the transport layer.

Changes Compared to the previous edition, standards architectures have been moved entirely from Chapter 1 to this chapter. The syntax of HTTP has been moved entirely to Chapter 11, the Networked Applications chapter.

A specific significant change is that the chapter discusses the Ethernet II frame, not the 802.3 MAC Layer frame. The Internet Protocol standards call for IP packets to be carried inside Ethernet II frames, and this practice appears to be general. Now that IP dominates at the Internet layer, it is Ethernet II frames that students have to understand. Conveniently, the Ethernet II frame is simpler.

Chapter 3

Chapter 3 covers core concepts and principles in network management. It introduces students to the importance of centralized management and to software-defined networking (SDN), which is potentially a fundamentally disruptive technology for changing how we manage networks.

Objectives After mastering the chapter, the student should be able to . . .

- Discuss network quality of service (QoS) and specify service level agreement (SLA) guarantees.
- Design a network layout based on required traffic volumes between pairs of sites.
- Describe options for dealing with momentary traffic peaks.
- Describe the benefits and importance of centralized network management; discuss and compare three tools for centralizing network management: Ping, traceroute, and the Simple Network Management Protocol (SNMP).
- Describe Software-Defined Networking (SDN), including why it is potentially revolutionary.

Changes In the previous edition, Chapter 4 covered both network and security management. That was too much to cover well. Chapter 3 in this edition has the network management information. It also centralizes SDN information, which was spread across multiple chapters in the previous edition. The section on network design has additional examples and exercises and introduces a new tabular approach. Redundancy is shown, but no computations are made because that is for an advanced course.

Chapter 4

Chapter 4 is primarily Chapter 3 in the previous edition. It introduces security threats and countermeasures. It may seem odd to put off security to the end of the principles chapters, but the material in the chapter requires full knowledge of core networking principles and concepts.

Caselet This chapter's caselet is the Target Breach, which was a complex hack. It takes several years before the details of such hacks are understood.

Objectives After mastering the chapter, the student should be able to . . .

- Describe the threat environment, including categories of attacks and attackers.
- Explain how to protect dialogues by cryptography, including encryption for confidentiality, electronic signatures, and host-to-host virtual private networks (VPNs).
- Evaluate alternative authentication mechanisms, including passwords, smart cards, biometrics, digital certificate authentication, and two-factor authentication.
- Describe firewall protection, including stateful packet inspection, next-generation firewalls, and related intrusion prevention systems.
- Describe the role of antivirus protection.

Changes Everything has been updated. The stateful inspection and next-generation firewall sections have been considerably redone.

Appendix

Most teachers who cover the Appendix cover it after Chapter 4, although some will wait until the end because it is a fun read. It includes much of the material from Chapter 4 on security management. It goes into more depth on planning principles and adds a discussion of the response phase. Covering the Appendix after Chapter 4 allows teachers to talk about defense in depth, weakest link thinking, and other principles throughout the discussion of security for specific technologies.

Caselet This caselet builds on the Target Breach discussed at the beginning of Chapter 4. It describes how critical security policies were violated, making the breach possible.

Objectives After mastering the chapter, the student should be able to . . .

- Describe the threat environment, including types of attacks and types of attackers.
- Explain how to protect dialogues by cryptography, including encryption for confidentiality, electronic signatures, and host-to-host virtual private networks (VPNs).
- Evaluate alternative authentication mechanisms, including passwords, smart cards, biometrics, digital certificate authentication, and two-factor authentication.
- Describe firewall protection, including stateful packet inspection, next-generation firewalls, and related intrusion prevention systems.
- Describe the role of antivirus protection.

Chapter 5

Now that the student has mastered basic principles and concepts regarding the Internet, standards, network management, and security, they are ready to apply this knowledge to key network technologies. In Chapter 5, this is Ethernet. Ethernet is covered before Wi-Fi because it is impossible to talk about Wi-Fi management without understanding Ethernet.

Objectives After mastering the chapter, the student should be able to . . .

- Explain basic Ethernet terminology and how Ethernet is standardized.
- Describe basic physical propagation concepts: digital and binary signaling, full-duplex transmission, and parallel transmission.
- Explain the technologies of 4-pair UTP and optical fiber. Compare their relative strengths and weaknesses, including cost and transmission distances.
- Design an Ethernet network based on knowledge of transmission requirements and Ethernet physical link standards, including link aggregation.
- Describe the Ethernet II frame. Explain basic Ethernet data link layer switch operation.
- Describe security threats to Ethernet and ways to deal with them.

Changes Compared to the last edition, this chapter relegates some nice to know but advanced features to footnotes. Power Over Ethernet is one of them. There is just too much stuff to learn about Ethernet to cover everything in an introductory course. The discussion of UTP and fiber media has also been streamlined, and single-mode fiber is moved to a box for additional information. As in Chapter 2, the focus is on Ethernet II frames.

Chapter 6

This chapter and most of the next deal with 802.11 Wi-Fi. This chapter focuses on what students need to know about the core technologies of Wi-Fi. The box at the end deals with the ongoing explosion of new physical layer standards and their relative strengths and issues.

Objectives After mastering the chapter, the student should be able to . . .

- Explain basic Wi-Fi 802.11 terminology and the role of access points.
- Explain basic radio signal propagation concepts, including frequencies, antennas, and wireless propagation problems. These are physical layer concepts.
- Explain the frequency spectrum, service bands, channels, bandwidth, licensed versus unlicensed service bands, and spread spectrum transmission used in 802.11 Wi-Fi LANs. These are also physical layer concepts.
- Describe 802.11 Wi-Fi WLAN operation with access points and a switched Ethernet distribution system to link the access points. Distinguish between BSSs, ESSs, and SSIDs. Discuss communication between access points. These are data link layer concepts.
- If you read the box “Media Access Control (MAC),“ compare CSMA/CA+ACK and RTS/CTS for media access control. These are data link layer concepts.
- Compare and contrast the 802.11n and 802.11ac transmission standards. Discuss emerging trends in 802.11 operation, including channels with much wider bandwidth, MIMO, beamforming, and multiuser MIMO. These are physical layer concepts.
- If you read the box “802.11/Wi-Fi Notes,“ be able to know what happens when devices follow different Wi-Fi standards, explain how devices that follow new Wi-Fi standards get released in profile waves, and describe emerging 802.11 standards and what they will bring.

Changes Compared to the previous edition, a number of topics have been streamlined. The material in the closing box is new. It deals more specifically with the current standards explosion and how products implement standards in profile waves.

Chapter 7

This chapter deals heavily with Wi-Fi security. A key point is that 802.11i security is mandatory but can be defeated by evil twin and rogue access point attacks. Centralized wireless LAN (WLAN) management is critical because access points are so widely dispersed. There is a boxed section on decibel calculations. You can decide how much, if anything, to cover. The chapter ends with a section on the wireless technologies that underpin Internet of Things transmission, including Bluetooth Low Energy, ZigBee, Wi-Fi Direct, and near-field communication (including radio frequency IDs).

Caselet How easy is it to crack an unprotected Wi-Fi hot spot? This caselet shows how seven-year-old Betsy Davies did it in just under 11 minutes. Including reading a tutorial on how to do it.While drinking a milkshake.

Objectives After mastering the chapter, the student should be able to . . .

- Explain 802.11i Wi-Fi security.
- Explain why 802.11i security is not enough for WLANs.
- Discuss 802.11 WLAN management.
- Work with decibel representations of power ratios (if he or she reads the box on decibels).
- Compare peer-to-peer local wireless technologies that will be important for the Internet of Things.

Changes The challenging evil twin section has been broken into more pieces and simplified to the extent possible. The decibel section has been heavily rewritten. The section on IoT transmission technologies is expanded considerably to reflect today's explosion in IoT transmission standards and technology.

Chapter 8

Chapters 5 through 7 dealt with single-network technologies that use standards at the physical and data link layers. With this as a basis, we can now move into TCP/IP at the Internet and transport layers. This chapter looks at how routers make their routing decisions and looks at the syntax of IPv6 main headers, extension headers, and higher-layer content. IPv6 is an important topic in networking today because IPv6 is no longer just a percent or less of all IP traffic. Students need to know how to write IPv6 addresses for human reading.

Some have asked why the book waits so long to move into TCP/IP. The answer is that TCP/IP is substantially more complex than Ethernet and Wi-Fi technology. Learning simpler technologies first makes it easier to learn TCP/IP and its many standards.

Objectives After mastering the chapter, the student should be able to . . .

- Define hierarchical IPv4 addresses, networks and subnets, border and internal routers, and masks.
- Given an arriving packet's destination IPv4 address, explain what the router will do with the packet based on its routing table.
- Explain the IPv4 packet header fields we did not see in earlier chapters.
- Explain the IPv6 packet's main header fields and IPv6's use of extension headers.
- Convert a 128-bit IPv6 address into canonical text notation consistent with RFC 5952.

- Explain TCP segment fields, UDP datagram fields, and TCP session closings.
- Explain why application message fragmentation is not possible with UDP.

Changes Relatively little is new to this edition, although almost all topics have been rewritten to help student comprehension.

Chapter 9

This chapter takes the TCP/IP discussion into management and security. TCP/IP uses many supervisory protocols beyond TCP, UDP, and IP. This chapter discusses a few of them.

Objectives After mastering the chapter, the student should be able to . . .

- Explain IPv4 subnet planning and do the calculations needed for working with subnet and host parts and deciding on part lengths.
- Do the same for IPv6.
- Explain the purposes of Network Address Translation (NAT) and how NAT operates.
- Explain in more detail than you learned in Chapter 1 about how the Domain Name System (DNS) and the Dynamic Host Configuration Protocol (DHCP) operate.
- Describe the object model in the Simple Network Management Protocol (SNMP) and describe the enabling value of good security in the use of Set commands.
- Describe how the DNS was modified to deal with IPv6 addresses for host names.
- Describe how dynamic routing protocols work and how to select among alternative dynamic routing protocols.
- Describe the Internet Control Message Protocol (ICMP).
- Explain central concepts in IPsec (IP security), including its strategic importance, transport versus tunnel mode operation, ESP versus AH protection, security associations, important cryptographic methods and options, session initiation with IKE, and how IPsec compares to SSL.

Changes Again, relatively few things were changed, but there was a good deal of rewriting and streamlining. One specific change is that subnetting for IPv6 now follows immediately after subnetting for IPv4. Another is that the section on IPsec has been expanded to include such things as how session initiation is done. More IPv6 material is an obvious need.

Chapter 10

This chapter deals specifically with wide area networking. In WANs, companies must deal with carriers instead of doing things themselves. They also face much higher costs per bit transmitted, so efficiency is critical. Isn't wide area networking just the Internet? No, it isn't. Companies must have quality of service guarantees for some of their site-to-site traffic, and the Internet does not provide that. Carrier WAN services for corporations today are dominated by lease lines, carrier Ethernet, and MPLS.

Most carriers have moved all of their Frame Relay and other customers to carrier Ethernet or MPLS. The chapter looks at cellular data communication, ADSL, and cable modem services as well as the carriers' local loop, which serves the premises of home and business users.

Changes After mastering the chapter, the student should be able to . . .

- Contrast LANs and WANs in terms of technology, diversity, economics, speed, and need for optimization.
- Describe the three carrier WAN components and the two typical business uses for carrier WANs.
- Describe how the telephone system is organized, including its hierarchy of switches. (Most carrier WAN networks use the public switched telephone network for some or all of their communication.)
- Explain and compare the ADSL and cable modem residential Internet access services and how fiber to the home is changing the residential access market.
- Discuss trends in cellular data transmission speeds.
- Distinguish between access lines and leased lines. Select a leased line for a given application speed requirement. Explain how companies use leased lines in Internet access.
- Explain how networks of leased lines, carrier Ethernet, and MPLS can be used for site-to-site communication within a firm. Discuss the relative advantages and disadvantages of each.
- Explain the capabilities of WAN optimization devices.

Changes This chapter mostly covers the same topics that Chapter 10 did in the previous edition. However, rewriting and streamlining is very heavy. There is more clarity on why the Internet does not meet the quality of service levels needed in most firms, requiring them to used technologies beyond the Internet for their much of their long-distance communication

Chapter 11

This chapter is about application architectures—where application processing is done and why it is done there. Falling prices for both computers and transmission have taken us from stand-alone mainframes to mainframes with dumb terminals, to client/server processing, cloud computing, and peer-to-peer computing. The chapter begins by noting that most computer hacks today involve taking over an application and receiving its permissions. The chapter looks at cloud computing and P2P computing. In between, it looks at the behavior of today's most central networked applications.

Objectives After mastering the chapter, the student should be able to . . .

- Explain core concepts in networked applications and application architectures.
- Describe how taking over an application can give an attacker the ability to control the computer.

- Describe how Netflix uses cloud computing and how this illustrates the importance of host technology (and cloud computing specifically) as a driving force for networking.
- Describe the World Wide Web in terms of standards and explain how a webpage with text, graphics, and other elements is downloaded.
- Describe electronic mail standards and security.
- Describe voice over IP (VoIP) operation and standards.
- Explain why peer-to-peer (P2P) computing is both desirable and dangerous.

Changes This chapter brings cloud computing from Chapter 1. The treatment of the "Big Three" business applications—the WWW, e-mail, and VoIP—is somewhat expanded. Peer-to-peer computing is reduced. It focuses on traditional VoIP versus P2P VoIP to show what peer-to-peer computing changes. It also discusses Tor, which is a P2P tool for anonymizing IP transmission. Tor is used both by people seeking anonymity and by cybercriminals.

The "a" Chapters

Several chapters are followed by an "a" chapter (1a, 3a, etc.) that provides some hands-on experience for students.

Chapter 1a. Hands-On: A Few Internet Tools This "a chapter" gives the student a bit of basic hands-on experience to help them make the concepts in Chapter 1 more concrete while learning a few useful tools. After mastering the chapter, the student should be able to . . .

- Test his or her Internet connection speed.
- Look up a host's IP address by querying a DNS server.
- Use Ping and traceroute to diagnose an Internet connection.

Chapter 3a. Hands-On: Microsoft Office Visio As the name suggests, this is a quick tutorial on Visio basics. Visio is widely used in network representation. Some schools have free versions for students. For those that do, Visio is useful in doing some homework questions.

Chapter 5a. Hands-On: Cutting and Connectorizing UTP If students are still cutting and connectorizing wire on a regular basis three or four years into their careers, they have probably made a wrong turn somewhere. However, learning how to do it is a good skill, and it makes 4-pair UTP less abstract. It is also fun, and it gives students something to take home to show their parents. After mastering the chapter, the student should be able to . . .

- Cut, connectorize, and test 4-pair UTP cabling.
- Explain the difference between solid wire and stranded-wire UTP.
- Know when to use patch cables.

Chapter 8a. Hands-On: Wireshark Packet Capture This chapter has the student capture a stream of IP packets and then analyze their headers in some detail. This exercise makes the syntax of IP, TCP, and UDP far more real to the student.

Chapter 9a. Hands-On: Cisco's IOS Command Line Interface (CLI) This chapter addition introduces the student to the flavor of Cisco's command line interface used in switches, routers, and other devices. It walks the student through a few sample interactions. After the class, some students may wish to master IOS in detail to help them pass valued Cisco certifications. This chapter was not in the previous edition.

Online Modules

Teachers who want to cover material not in the text may find it useful to look at online modules that cover additional matters. These are available for both teacher and student download. The purpose is to allow you to cover certain additional topics without having to do more preparation. A word of caution. There is a lot of material. Only small amounts of the material in the online modules are likely to fit into courses.

Module A: More on TCP This module is for teachers who wish to cover TCP sequence and acknowledge numbering and flow control using the Windows Size field. It comes most naturally after Chapter 8.

Module B: More on Modulation The main text does not deal with modulation. Covering this short module will help your students understand how the most advanced 802.11 physical layer standards can transmit data more efficiently by sending more bits per clock cycle.

Module C: More on Telecommunications Some courses have titles that include Telecommunications. This normally means telephony. This chapter has material for these courses.

Module D: Directory Servers Directory servers are a big thing in the corporate world. This module looks at directory servers in more detail, including Microsoft's Active Directory and authentication using directory servers. The latter is covered briefly in the Appendix. This module adds metadirectory servers.

PREFACE FOR STUDENTS

THIS BOOK

Most textbooks start by trying to convince you that the subject matter is important. This one doesn't need to do so. Everybody knows that the Internet is important. Ditto on security.

Networking and Security Why *both* networking and security? The reason is that security pervades professional networking today. There is no way to separate them. Every network project has a sizeable security content. The traditional view that networking is the moving of bits and packets is no longer sufficient. Nor is it enough to slap a security chapter at the end of the book. Security must be deeply integrated into your knowledge of Ethernet, Wi-Fi, TCP/IP, applications, and everything else. Some teachers cover the Appendix to give you an even deeper view of security planning and response when security failures happen.

Principles and Their Application Figure 1 shows how this book will help you learn networking and security. First, you will learn concepts and principles. You will learn core ideas such as how the Internet operates, the nature and idiosyncrasies of network standards, keys to managing networking projects, and core security concepts. Why does security come last among these core chapters? The answer is simply that you can't learn network security without understanding core networking ideas first.

The rest of the book takes you through a series of technologies. For each, you will apply the concepts and principles you mastered in the first four chapters. For instance, when you learn about Wi-Fi in Chapters 6 and 7, you will understand its basic operation, physical transmission, switch operation, standards, management, and, of course, security. You will do the same for the other technologies and applications shown in Figure 1.

Job-Relevant Knowledge We have done everything we could to fill this book with job-relevant knowledge. You will not have to learn about technologies that haven't been seen in this century. There simply isn't time to cover history when companies need

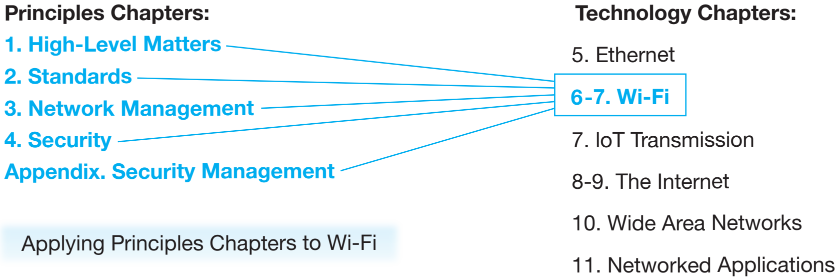

FIGURE 1 Learning and Applying Security Concepts and Principles

students who understand IPv6, IPsec, the current explosion in Ethernet standards, the current explosion in Wi-Fi standards, Internet of Things transmission protocols, and many other recent developments. You will learn all the general principles that all networking books cover, but you will learn about them in the context of today's important technologies. If you can, work through the hands-on "a" chapters that follow several main chapters. These things are kind of fun, and they will make concepts a lot more concrete.

Information Systems versus Computer Science How does an information systems book differ from computer science books? Our friends in computer science teach students how to design routers in networking and how to create ciphers in security. Our students will work in IT departments. They will never build a router, but they will buy them and need to understand how to manage and secure them. Would it help to teach you how to build a router? Perhaps. But that would mean not teaching you how to use them in real organizations because there wouldn't be time. Design your own cipher? We teach our students that doing that is stupid. You do not have to know how to design a cipher to know how to select a cipher to use in a project, and 99.9% of all developed ciphers are broken quickly.

STUDYING NETWORKING

Although networking and security are exciting, many find them hard to learn. It is not that they are terribly difficult inherently. The main problem is that you do not have a mental framework when you start, so it is hard to absorb individual pieces of knowledge. You need to learn frameworks and individual pieces at the same time.

Frameworks and Individual Pieces Unfortunately, this means that you need to jump back and forth between frameworks and individual pieces until both settles into place. Once you master that discipline, you will be able to grasp major constellations of concepts. If you do not, this course is going to be very hard.

Intelligent Choices This class requires upper-level college thinking. In the first years of college, you are learning individual facts. In your final years, you need to master comparisons between concepts so that you know which to apply. This is exactly what networking professionals need to do. To design a network, you need to make complex decisions requiring you to evaluate alternatives. You also need a complex mental model to troubleshoot problems, which takes up a surprising amount of professional work time. It has been said that artists are known for their best moments but engineers are known for their worst. Any piece you do not master comes back to haunt you.

TLAs and FLAs Then there is the problem of TLAs and FLAs (three-letter acronyms and four-letter acronyms). You will see a lot of them. Why not just avoid acronyms? The problem again is the environment in which network professionals work. If you pick up any trade magazine, you will see that few acronyms are ever spelled out. You will have to learn a lot of them. Think of them as abbreviations when you text people on your phone.

There is a comprehensive Glossary at the back of the book. If you aren't sure what a term means, go to it for a quick definition. If that isn't enough, the index will tell you what pages to read. If a page number in the Index is boldfaced, look at that page first.

No Escape By this point, you may have decided that networking and security are rather challenging and that programming and database are beginning to seem attractive. Unfortunately, they won't get you away from networking and security. Today, most programs in industry are written to work with other programs on other machines; and all of their interactions take place over networks. Database management systems and systems analysis also require solid networking knowledge. So learn networking as much as you can. We have cute kittens to watch and alien ships to destroy. For security, we have fascinating stories, and you are not just going up against hardware reliability and software bugs. You will find yourself matched against determined attackers who will respond to whatever you do.

STRUCTURE OF THE MATERIAL

If you page through the book, you will see that it is set up a little differently than other textbooks you have seen.

Fun Footnotes Fun Footnotes? Footnotes are dry and academic. Ours are little bits of knowledge that take you beyond the book. Some students are really turned on by them. No, honestly. In any case, they are never required reading. If you find them interesting, enjoy them.[1] If not, ignore them. Some are different; they take a swipe or two at what standards agencies do.

Small Sections Long blocks of text are daunting to read. This book breaks things into a lot of small digestible sections with a lot of headings.

Short Sections with Level Three Headings (Like This One) If you just read a title, you often can get the gist of what follows. This will make it easier to know what the section does. Learning small chunks of information also increases comprehension.

Key Terms Key concepts and their acronyms are shown in **boldface**. That alerts you to their importance. If you forget this key term, you can always go to the Glossary to refresh your memory. The index also lets you see where a key term appears. If a page number is shown in boldface, that is where the concept is defined or characterized.

Callouts As you read a section, pay attention to callouts like the one below. They emphasize an important fact or idea and often things that are points of frequent confusion. Before exams, first go over the callouts until you have them cold.

[1] This is our way to put in some material that is good to know but that is more than an introductory course should include and that generally has proven difficult for even well-prepared undergraduates to master.

As you read a section, pay attention to callouts like this one. They emphasize an important fact or idea.

Comprehensive Figures Nearly every important concept in the book is covered in a figure. The figures are very carefully designed to show the flow of actions or ideas. As you read a section, look at the figures carefully. See if you can teach each to an imaginary friend. First set the stage. What are the pieces? Then step through the various parts of the figure.

Some figures end with (Study Figure). These are essentially notes on what the section covers. It gives you a view of a block of material from 10,000 feet and helps link frameworks with individual facts.

Test Your Understanding Questions The material in networking is highly cumulative, so you want to master the material in a section before going on. Each section ends with Test Your Understanding questions designed to help you see if you have understood what you just read. When you reach them, you want to go on instead of testing yourself. If can get yourself to go over the questions immediately, it will help you learn whether you understand the material you just read. If you aren't comfortable, go back and learn the material again.[2]

STUDYING FOR EXAMS

If you think you won't have to study for exams, it will probably end in tears. Given this reality, some advice about how to study for exams is in order.

- Again, a good place to begin is the callouts. Go through them and make sure you understand them all. They include a lot of the chapter's important content in little chunks.
- A good place to go next is the figures. Go through them one at a time, teaching them to your imaginary friend. This again packs a lot of material in small packages. Let the study figures help you understand the structure of the relevant section and its key points. To tell a story, first set the stage. What is the problem being solved or presented in the figure? What are the devices and programs involved? Then walk through the rest of the figure. Often, steps to do so are numbered. If you understand all the figures, you should do well.
- After you have done these things, go over your Test Your Understanding answers. If you did them from homework, don't just study your original answers. When you wrote them, your knowledge was less mature than it will be just before exams, and many of your early answers will be science fiction. One helpful trick is to ask yourself why each question is important. Why do you have to know it?

[2] A key idea in answering Test Your Understanding questions is to maximize what you learn, ask yourself, "Why is this question important?" Each question has a reason for being there. See if you can understand what it is and why it is important.

- Yes, you are going to have to reread much of the text. This is especially important for parts of the chapter that deals with complex frameworks with multiple parts. As discussed previously, you will learn them, forget them, learn them again, and so forth.

CERTIFICATIONS

In high school, you may have taken advanced placement exams. Passing AP exams impress college admissions committees. Analogously, IT certification exams let you demonstrate some in-depth knowledge and also tell companies that you are serious and proactive. The problem is that there are many certifications, and they offer different levels of knowledge about different topics. Many require hands-on expertise in working with networking technology. Most require two to five years of work experience for full certification, although some of these allow you to receive associate status if you pass but have not yet acquired the work experience. All of them cost money, in some cases thousands of dollars.

Network+ and Security+ The least ambitious certifications are CompTIA's Network+ and Security+ certifications. Both are quite doable with some extra study. Neither impresses IT departments highly. However, they are achievable with reasonable effort. A major practical problem with these certifications is that they spend far too much time on technologies and concepts that have been irrelevant for thirty years or more.

Vendor Certifications Vendors offer certification exams that are prized by IT departments. The introductory certifications show that the bearer has the knowledge to do entry-level tasks in the exam's area.

The problem with vendor certification is that they see things only from that particular vendor's point of view. For example, Cisco will cover a great deal about Cisco routers, switches, and other network devices. In contrast, Microsoft will focus on networking from the client and server point of view, including various types of network servers such as DNS servers.

Passing a vendor certification will require you to learn more than an introductory network course will cover. You will need to buy a book to study. Many of the concepts will be the ones you learned in this course. You will also see quite a few topics in depth. Sadly, in our opinion, you will also have to master quite a few legacy technologies that have not been seen in this century. We understand that businesses must support some obsolete network technologies, so learning about them in a vendor certification course makes sense. Given that only some students go on to networking makes it silly to cover these topics in introductory networking courses, however. It takes too much time away from job-relevant material.

For new graduates, Cisco now offers the Cisco Certified Entry Network Technician certification. A CCENT certification validates skills for entry-level work. Those who pass have the skills to install and manage a small branch office network in an enterprise. This includes relevant network security. To be attractive to corporations, students should achieve the next-level Cisco certification, Cisco Certified Network Associate (CCNA).

Professional Association Security Certifications Security has professional associations for people working in security. They generally offer certification programs.

- For broad security professionals, (ISC)^2 offers certifications in a number of security domains. Passing most or all of them will validate a good level of mastery of security. For new graduates, there is the Associate of (ISC)^2 certification, which allows a student with no work experience to demonstrate a good level of knowledge before obtaining the experience requirements for more advanced certifications. In turn, the Systems Security Certified Practitioner (SSCP) certification requires one year of experience in one of eight content domains. The most important initial certification is the Certified Information Systems Security Professional (CISSP). This requires five years in two or more of the eight domains.
- For information systems auditors, there are more focused certifications. These are offered by ISACA, the Information Systems Auditing and Control Association. ISACA offers the Certified Information Systems Auditor (CISA) and Certified Information Systems Manager (CISM) certifications.

Advanced Certification Programs and Master's Degrees At a higher level of knowledge and skills, there are advanced certification programs and master's degrees. The predominant advanced certification program in security is offered by SANS, which offers advanced courses in specific areas leading to a broad level of knowledge. These courses are quite expensive. Most SANS participants are sponsored by their employers. The first author has found them to be great courses.

ABOUT THE AUTHORS

Ray Panko is a professor of IT management and a Shidler Fellow at the University of Hawai'i's Shidler College of Business. His main courses are networking and security. Before coming to the university, he was a project manager at Stanford Research Institute (now SRI International), where he worked for Doug Englebart, the inventor of the mouse and creator of the first operational hypertext system. He received his B.S. in physics and his M.B.A. from Seattle University. He received his doctorate from Stanford University, where his dissertation was conducted under contract to the Office of the President of the United States. He has been awarded the Shidler College of Business's Dennis Ching award as the outstanding teacher among senior faculty. His e-mail is Ray@Panko.com.

Julia Panko is an assistant professor on the faculty at Weber State University. She received her doctorate from the University of California, Santa Barbara. Her research interests include the twentieth- and twenty-first-century novel, the history and theory of information technology, and the digital humanities. Her dissertation focused on the relationship between information culture and modern and contemporary novels.

This page intentionally left blank

Chapter 1

Core Network Concepts and Terminology

LEARNING OBJECTIVES

By the end of this chapter, you should be able to:

- Discuss how the Internet is changing and the security challenges these changes are creating.
- Explain basic concepts and terminology for the hosts (devices) that connect to the Internet.
- Explain basic concepts and terminology for the Internet itself.
- Explain basic concepts and terminology for single networks and their role on the Internet.
- Explain the distinctions between Internet routers and personal access routers; explain the differences between personal access routers and wireless access points.

A STATE OF SIEGE[1]

On September 15, 2016, criminals launched a massive cyberattack on KrebsOnSecurity .com. This is the blogsite of Brian Krebs, whose posts are often the first analyses of major cybercrime incidents (such as the Target breach we will see in Chapter 4).

[1] Kyle York, "Dyn Statement on 10/22/2016 DDoS Attack," Dyn, April 19, 2017, https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/; Brian Krebs, "KrebsOnSecurity Hit With Record DDoS," KrebsOnSecurity.com, September 16, 2016, https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/; Brian Krebs, "Source Code for IoT Botnet 'Mirai' Released," KrebsOnSecurity.com, October 16, 2016, https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/; Brian Krebs, "Who Makes the IoT Things Under Attack?" KrebsOnSecurity.com, October 16, 2016, https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/; Brian Krebs, "Hacked Cameras, DVRs Powered Today's Massive Internet Outage," KrebsOnSecurity.com, October 16, 2016, https://krebsonsecurity .com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/; Brian Krebs, "Akamai on the Record KrebsOnSecurity Attack," KrebsOnSecurity.com, November 16, 2016, https://krebsonsecurity .com/2016/11/akamai-on-the-record-krebsonsecurity-attack/.

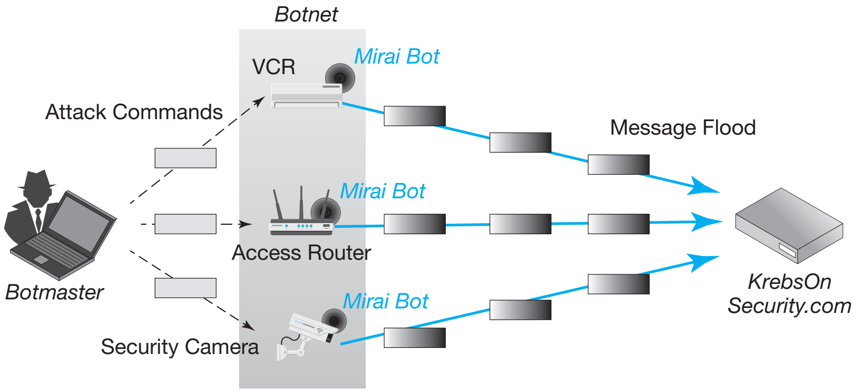

FIGURE 1-1 Simplified Depiction of Mirai Distributed Denial-of-Service Attack

Cybercriminals hate him, and they had attacked his site 269 times in the previous four years.[2] (This was about one attack every five days.) The attacks that began on September 15, 2016, however, were unprecedented.

DDoS Attack These attacks were distributed denial-of-service (DDoS) attacks. Figure 1-1 shows a simplified view of a DDoS attack.[3] In advance, a cybercriminal called a botmaster installs malware on hundreds or thousands of computers without the owners' knowledge. This malware is called a bot. Like a physical robot, a malware bot can be given goals, which it will then execute in detail. In Figure 1-1, the botmaster commands the bots to attack a certain target site. Each bot then sends a flood of packets at the target host. The traffic overwhelms transmission lines to the target. The particular botnet malware that attacked Krebs' site was called Mirai.

Enormous Traffic The September 2016 attack was remarkable for two reasons. The first was the deluge of traffic it threw at Krebs' site. The Mirai bots were able to flood the site with traffic at an astounding 620 Gbps[4] (billions of bits per second).[5] According to Akamai, which was protecting KrebsonSecurity.com at the time, this was almost twice the volume of any DDoS attack it had ever encountered.[6] Mitigating such an attack was daunting, and it took considerable time.

Internet of Things (IoT) Devices The second reason the attack was remarkable was the nature of the devices used in the attack. Normally, DDoS attacks use

[2] Krebs, "Akamai on the Record KrebsOnSecurity Attack."

[3] We will look at these attacks in more depth in Chapter 4.

[4] Speeds are measured in bits per second, kilobits per second (kbps), megabits per second (Mbps), and gigabits per second (Gbps).

[5] Krebs, "Source Code for IoT Botnet 'Mirai' Released."

[6] Krebs, "KrebsOnSecurity Hit With Record DDoS."

compromised desktop computers, laptops, and other traditional IT devices. In the attack on Krebs' site, however, the attacking computers were small nontraditional devices, including home access routers, home security cameras, and home VCRs. In a trend called the Internet of Things (IoT), we are seeing explosive growth in Internet connections by devices previously too lacking in power to use the internet. The size of the IoT is difficult to discuss because it is growing so explosively. However, Gartner, Inc. estimated the number of active IoT devices at 5 billion and forecasts that 2020 will see almost 21 billion.[7] Even if that forecast is highly optimistic, IoT devices are already about as widespread as humanly used computers and will soon be far more numerous.

Weak IoT Security The cybercriminals realized that IoT devices often have weak security. Many come with a login account paired with a well-known default password. If the default password is not changed, anyone can take over the device over the Internet. Users often fail to change them. In fact, some default passwords are hardcoded into IoT devices and cannot be changed by the user.[8] The Mirai malware jumped from one device to another by trying a mere 68 device-password combinations.[9] In many ways, this attack was a coming of age for the Internet of Things. IoT may still be in its infancy overall, but it is now mature as a destructive force.

Dyn There have been many other Mirai victims. On October 21, 2016, Dyn, Inc. was the target of a similar attack. In a postmortem on the attack, Dyn reported that it had been attacked by tens of millions of discrete IP addresses known to be part of the Mirai botnet.[10] Dyn is a Domain Name System (DNS) hosting service. We will see DNS later in this chapter. If you know the name of a site, such as panko.com, you cannot send it messages until you learn its official Internet Protocol (IP) address. (To give an analogy, if you know someone's name, you cannot call that person until you learn his or her telephone number.) A DNS server gives your computer a named site's IP address. If a DNS server that serves hundreds or thousands of popular sites is disabled, the result can be chaos. Among the sites at least temporarily disrupted in the Dyn attack were Amazon, Netflix, Twitter, Spotify, Reddit, and Tumblr.[11] This incident did not merely attack a site. It attacked a critical piece of the Internet infrastructure.

Perspective The great promise of the Internet has been to give access to "anything, anytime, anywhere." Unfortunately, criminals are quick to exploit new technologies. The Internet has evolved with breathtaking speed, bringing both new applications and new types of attacks. Networking people are involved in a protracted arms race with cybercriminals, and the cybercriminals have been winning too often.

[7] Ibid.

[8] Krebs, "Hacked Cameras, DVRs Powered Today's Massive Internet Outage."

[9] Krebs, "Who Makes the IoT Things Under Attack?"

[10] York, "Dyn Statement on 10/22/2016 DDoS Attack."

[11] Krebs, "Hacked Cameras, DVRs Powered Today's Massive Internet Outage."

All this does not mean that the Internet or other networks are bad. The very reason denial-of-service attacks are so damaging is that the Internet's benefits have become indispensable for people and organizations. However, every garden has snakes. Networking cannot be managed without understanding security, and security cannot be managed without understanding networks.

Test Your Understanding

1. a) What is a DDoS attack? b) In what two ways was the KrebsOnSecurity.com DDoS attack unusual? c) What do we mean by the "Internet of Things?" d) What happens when a host cannot reach a Domain Name System server? e) What specific security weakness did the Mirai malware use to propagate from machine to machine?

ANYTHING, ANYTIME, ANYWHERE

The Internet used to be the "*New Thing*." It caught fire in the public's imagination in 1995 when the Internet first became commercial. Before then, the Internet's Acceptable Use Policy explicitly prohibited most commercial activity. This was done because the Internet's transmission backbone was supplied by the National Science Foundation (NSF). Using the NSF to subsidize commercial activity was simply not in the cards. In 1995, however, the NSF pulled out. The rationale for the Acceptable Use Policy vanished. The Internet could be used commercially. It was, immediately.

Test Your Understanding

2. When was commercial activity on the Internet first allowed?

The Internet Reorganizes to Get Commercial

Internet Service Providers In 1995, commercial **Internet service providers (ISPs)** took over the backbone of the Internet. They also became the onramps to the Internet. Anyone wanting to use the Internet must go through an ISP. The Internet today is simply a collection of ISPs that collectively deliver traffic from source to destination computers. Figure 1-2 illustrates this situation.

Internet transmission is handled by commercial Internet service providers (ISPs).

Hosts Figure 1-2 notes that all devices connected to the Internet are called **hosts**. You will encounter this term throughout this book. A laptop is a host when it connects to the Internet. So is a mobile phone. So are the webservers and other servers that provide the services you use when you use the Internet.

Devices that connect to the Internet are called hosts.

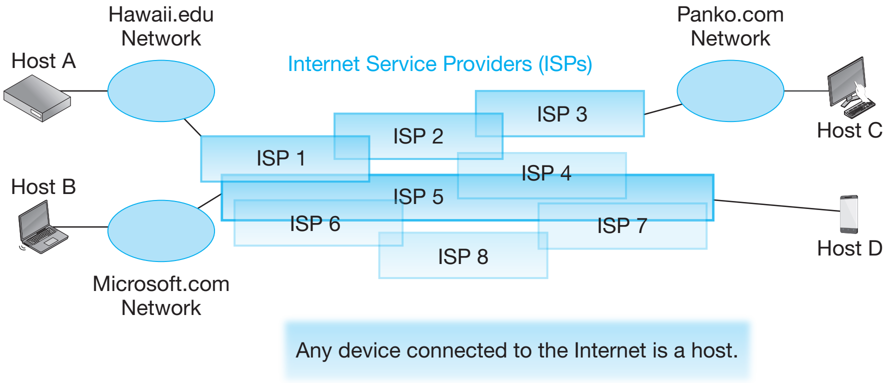

FIGURE 1-2 The Internet: Internet Service Providers, Organizational Networks, and Hosts

E-Commerce The year 1995 saw an immediate rush of commercial companies to ply their businesses over the Internet. Companies with such familiar names as Amazon and eBay were ready and waiting. Amazon's entry was especially interesting. Jeff Bezos wanted to create a company that would sell everything over the Internet, not just books. He chose the name of the company to indicate that it would be a very wide torrent for delivering goods and services. When you look at the Amazon logo, note the arrow at the bottom. It points from A to Z.

Why start with books? Bezos realized that the book industry had almost everything needed for online sales. Publishers and distributors had huge warehouses of books and the ability to do single-item packaging. More importantly, everything was on their computers. Amazon could reach into those databases and provide an online sales front end, complete with the company's innovative one-click ordering. Many organizations and individuals developed simpler non-interactive informational websites to provide information. Soon the Internet became the first place to go for information, some of it correct.

Test Your Understanding

3. a) What services do Internet service providers provide? b) In Figure 1-2, through which ISP(s) will traffic pass if a packet from Hawaii.edu goes to Panko.com? (Answer: ISP 1, ISP 2, and ISP 3) c) Through which ISP(s) will traffic pass if a packet from Microsoft.com goes to the mobile phone in the lower right of Figure 1-2? d) Through which ISP(s) may traffic pass if a packet from Microsoft .com goes to Panko.com? (Hint: There are multiple possible answers.)
4. a) What do we call any device connected to the Internet? b) When you use a laptop to connect to the Internet, is it a host? Explain in terms of the definition of *host*. c) When you use the Internet, are *you* a host? Explain in terms of the definition.

Old Yet Always New

No Longer New? The Internet today, more than a human generation after its creation, is no longer new. Many of the young pioneers who created it are no longer with us. Both e-commerce and informational websites that appeared only about twenty years ago are also old hat.

Commercial for More than Twenty Years

In 1995, the U.S. government pulled out transmission funding

Now, e-Commerce was possible

Yet Still New Applications, Even Entire Classes of Applications

Social Media, etc.

Growing Speed

High-definition and 4K video, large data transfers, full-computer backup, etc. are now possible

Companies can locate servers far from expensive city locations, even rent servers “in the cloud”

Back-end artificial intelligence processing for speech recognition, more

Growing Ubiquity and Reliability

Almost never out of touch with the Internet and your resources there

The Emerging Internet of Everything

Traditionally, there was a human user involved

Growing technology allows devices to talk to one another, without human involvement

These devices can now be very small, such as thermostats

These devices now communicate by low-cost radio directly with one another

FIGURE 1-3 The Ever-Changing Internet (Study Figure)

However, what the Internet offers to people and organizations who use it is constantly new. Social media are relatively recent developments, as are high-quality video streaming and teleconferencing. Now we are beginning to see augmented reality, and not just to find and fight Pokémons. What will come next? Based on what we know about the past, it will surprise us. Since the emergence of the Internet, we have always been shocked when new “killer app” categories emerge to create a whole new set of billionaires and addicted users.

Growing Speed How can the Internet change so frequently and so radically in the applications it supports? The answer is that the Internet itself is changing technically at an enormous rate and will continue to do so. Simple speed is the most obvious change. Today, wired Internet connections can bring multiple high-definition videos to homes. Increasing velocity also allows you to use programs like Box and Dropbox to back up your files in real time and use them immediately or later despite their sizes. At the corporate level, companies even back up their massive transaction databases in real time. If one corporate site fails, another site can pick up the computing load almost instantly. At a very broad level, many companies have decided to stop buying and running their own servers. They have turned to cloud computing, in which you rent just the number of servers you need. If your load varies, you can even rent servers by the hour. Netflix, which generates about a third of the Internet traffic going into American homes in the evening, varies the number of servers it uses throughout the day. It even has a self-service portal to add and drop servers instantly. These cloud servers are clustered in massive server farms that each has thousands of servers under one roof. Where are these server farms? It really doesn’t matter. The Internet can connect computers anywhere with minimal delay.

Growing Ubiquity and Reliability Another continuing disruptive change is the ubiquity of Internet access. Initially, you needed a desktop or at least a laptop computer. It was probably stationary in your home or office. When you were away from it, your access to the Internet depended on the presence of an Internet cafe or the kindness of friends. Mobile phones changed that, but only gradually. Early mobiles either could not access the Internet at all or were limited to a stupefying slow 10 kbps (10,000 bits per second). No mega, and certainly no giga. Today, speeds are far greater.

Of even greater importance, we can use the Internet everywhere. Our connection to the Internet is "always on." Our mobiles provide that to us nearly all the time, and we are increasingly able to plug into lower-cost (and higher-speed) Wi-Fi as we travel.

This always-on connectivity of mobile devices is used in ways we do not even realize. For example, the speed recognition processing needed for voice commands is usually done on a distant server with massive processing power, not on our puny little phones and tablets. This allows far richer and smarter interactions.

Along with this near ubiquity of Internet access is nearly perfect reliability. When the first author initially used the ARPANET (the forerunner of the Internet), he was astounded to see that he had new mail. It was from a colleague at MIT, welcoming him to the 'Net. A week later, he was still amazed, but like everybody else who was using networks, he also thought, "Too bad it doesn't work more often." Today, it does.

The Emerging Internet of Everything When the Internet was created in the late 1970s, computers were the size of rooms. Users worked at dumb terminals on their desks. These terminals were basically keyboards and low-quality displays. Microprocessors had just been invented, and they were too expensive for individuals to use. When the Internet was designed, it was widely assumed that only these large computers would connect to the Internet. However, Moore's Law forecast that microprocessor prices would soon fall dramatically and would continue doing so for many years. Personal computers (PCs) began to communicate. Then came smartphones.

Today, we increasingly have residential thermostats, air conditioners, and even coffee makers with enough processing power to run applications and communicate over the Internet. Furthermore, these devices increasingly talk to one another, with no human involvement. As noted at the beginning of this chapter, this trend is being called the **Internet of Things (IoT)**. In fact, the "devices" connected to the Internet may not even be physical. Today, a computer can run two or more virtual machines, which are programs and related data that act like full computers when they talk to real devices and humans on the Internet.

Test Your Understanding

5. a) What continuing changes in the Internet are contributing to its ability to support new applications constantly? b) What are the characteristics of the Internet of Things?

Owning and Managing the Internet

When the U.S. government pulled out of the Internet, the Internet needed a way to fund itself. This task was left to the ISPs. To use the Internet, you must connect through an ISP. Doing this is not free. As an individual or part of a family, you probably pay about

Commercial ISPs Handle Transmission

- You must have an ISP to use the Internet
- You pay the ISP money
- Corporations pay a lot more
- ISPs deliver packets across one another
- Settlements for sharing revenue from users
- Nobody owns the Internet. The ISPs do collectively

Nobody Controls the Internet, Either

- The Internet Engineering Task Force (IETF) sets standards, but compliance is voluntary
- A few things are centralized, including controlling Internet addresses to prevent duplication

FIGURE 1-4 Owning and Managing the Internet (Study Figure)

$50 per month to your ISP for Internet access. Organizations pay far more—often tens of thousands or even millions of dollars each year. Traffic must flow across ISPs, so the ISPs have financial settlement agreements among themselves to compensate for cross traffic.

Under these conditions, "Who owns the Internet?" The answer is, "nobody." Each ISP owns its own resources, and the Internet is the sum of these resources. This may seem like an odd situation, but this is exactly how the worldwide telephone network works. There are thousands of telephone companies around the world. Like ISPs, they exchange traffic and use financial settlements to balance costs and revenues.

An obvious related question is, "Who controls the Internet?" The answer, again, is, "nobody." A few things about the Internet are controlled. For example, the **Internet Assigned Numbers Authority (IANA)** controls internet addresses to avoid address duplication. However, remarkably little else is controlled.

What about standards? There is certainly a need for standards to govern how devices talk to one another. However, things are a little complicated. The organization that creates standards is the **Internet Engineering Task Force (IETF)**. This is a volunteer and sometimes rowdy organization that creates great standards. However, it has no power to impose these standards on ISPs and user organizations. In fact, quite a few of its standards have been ignored by ISPs. Keep this in mind when we talk about Internet standards created by the IETF.

The Internet Engineering Task Force (IETF) creates Internet standards.

Test Your Understanding

6. a) Who owns the Internet? b) Who is in charge of the Internet? c) What is the role of the IETF?

The Snake in the Garden

The Internet promises to give users access to almost everything, anytime, anywhere. Unfortunately, it does the same for criminals, national governments, and just plain jerks. As the Internet has grown in size and complexity, so have the adversaries and

Anything, Anytime, Anywhere

Works for Attackers As Well As Legitimate Users

Security Underlies Everything That Network Professionals Do

FIGURE 1-5 Security: The Snake in the Internet Garden (Study Figure)

the attacks they use. Networking practitioners are not the only professionals who are responsible for stopping security threats, but security underlies almost everything that networking professionals do. We will hold off looking more deeply into security until Chapter 4. This is not because security is unimportant but because you need a solid grasp of networking concepts, standards, and management before you can understand security threats and countermeasures.

Test Your Understanding

7. a) Why is the Internet's ability to give broad access a good thing? b) What danger does it bring?

Next Steps

So far, we have been looking at the Internet at a very high level. For the rest of this chapter (and this book in general), we look at the Internet and other networks in the detail that professionals in IT, networking, and security need to understand to enter the profession. In this chapter, we focus on the core Internet terms and concepts we will see throughout this term.

This introduction ends with a fundamental point. So far, we have been talking about the Internet. However, the Internet is not the only network. In fact, "Inter" means "between." The Internet was specifically created to link many individual networks together. We begin with the Internet, but later in the chapter we also look at two types of networks that can be standalone networks or parts of the Internet.

The Internet is not the only network.

Test Your Understanding

8. a) What does "Inter" in Internet mean. b) Why is this important?

OUTSIDE THE INTERNET

We will spend most of this term looking *inside the Internet* and other networks. However, we begin by looking at the Internet *from the outside*—focusing on the user devices attached to it. Figure 1-6 shows some devices attached to the Internet. However, it depicts the Internet itself as an opaque cloud. The **cloud** indicates that the average