Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

This book is designed to provide information about the Accessing the WAN course of the Cisco Networking Academy CCNA Exploration curriculum. Every effort has been made to make this book as complete and accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the authors and are not necessarily those of Cisco Systems, Inc.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact:

U.S. Corporate and Government Sales
1-800-382-3419
corpsales@pearsontechgroup.com

For sales outside the United States please contact:

International Sales
international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members of the professional technical community.

Reader feedback is a natural continuation of this process. If you have any comments about how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please be sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.
About the Authors

**Bob Vachon** is the coordinator of the Computer Systems Technology program at Cambrian College in Sudbury, Ontario, Canada, where he teaches networking infrastructure courses. He has worked and taught in the computer networking and information technology field since 1984. He is a scholar graduate of Cambrian College, and he received the prestigious Teaching Excellence Award in 1997. Vachon has been a Cisco Networking Academy instructor since 1999 and has been CCNP certified since 2002. He has worked with Cisco as team lead, author, CCNP certification assessment developer, and subject matter expert on a variety of projects, including CCNA, CCNP, and global partner training courses. He enjoys playing the guitar and being outdoors, either working in his gardens or white-water canoe tripping.

**Rick Graziani** teaches computer science and computer networking courses at Cabrillo College in Aptos, California. He has worked and taught in the computer networking and information technology fields for almost 30 years. Before that, he worked in IT for various companies, including Santa Cruz Operation, Tandem Computers, and Lockheed Missiles and Space Corporation. He holds an M.A. in computer science and systems theory from California State University Monterey Bay. Graziani also does consulting work for Cisco and other companies. When he is not working, he is most likely surfing. He is an avid surfer who enjoys longboarding at his favorite Santa Cruz surf breaks.
About the Technical Reviewers

Nolan Fretz is a college professor in network and telecommunications engineering technology at Okanagan College in Kelowna, British Columbia. He has almost 20 years of experience in implementing and maintaining IP networks and has been sharing his experiences by educating students in computer networking for the past nine years. He holds a master’s degree in information technology.

Charles Hannon is an assistant professor of network design and administration at Southwestern Illinois College. He has been a Cisco Certified Academy instructor since 1998. He has a master of arts degree in education from Maryville University in St. Louis. He holds a valid CCNA certification and has eight years of experience in managing information systems. His priority is to empower students to become successful and compassionate lifelong learners.

Snezhy Neshkova, CCIE No. 11931, is a technical manager with the Cisco Networking Academy. She has more than 20 years of networking experience including field services and support, management, and networking education. She has developed and taught a number of different courses in the networking field including Cisco Networking Academy curricula. Snezhy holds a master of science degree in computer science from the Technical University of Sofia, Bulgaria.

Matt Swinford, associate professor of network design and administration at Southwestern Illinois College, has been an active Cisco Certified Academy instructor since 1999. He is dedicated to fostering a learning environment that produces certified students and quality IT professionals. He has a master of business administration degree from Southern Illinois University at Edwardsville and holds valid CCNP, A+, and Microsoft certifications.
Dedications

For my wife, Teri. Without your patience and understanding, I would not have been able to participate in this project. Thank you for your love and support throughout the countless hours it took me to complete this book and for your understanding that I still needed time to surf.
—Rick Graziani

To my wife, Judy, who, through good times and hard times, helped me keep body and soul together. Without her support and encouragement, I would not have been involved with this project.
—Bob Vachon
Acknowledgments

From Rick Graziani:
First of all, I want to thank my good friend Bob Vachon for the pleasure of writing this book with him. Bob’s expertise with and commitment to the Cisco Networking Academy have always been extraordinary. His work in the creation of this book has been another example of his exceptional talents.

This book was not the work of any one or two individuals but literally was a team effort. Jeremy Creech headed a team that included Gail Behrend, Koksal Cengiz, Don Chipman, Sonya Coker, Allan Johnson, David Kotfila, Jeff Luman, Bob Vachon, Alan Weiler, and me. My sincere gratitude and thanks to Jeremy and the team for letting me be part of such an outstanding team. I am honored and humbled to work with such a fine group of dedicated people.

Special thanks to Mary Beth Ray for her patience and understanding throughout this long process. Mary Beth always provided that voice of calm reassurance and guidance whenever needed.

Thank you, Chris Cleveland, for your help in the editing and production stages. I am amazed at the level of cooperation and teamwork required to produce a technical book, and I am grateful for all your help.

Thanks to all the technical editors for providing feedback and suggestions. Nolan Fretz, Charles Hannon, Snezhy Neshkova, and Matt Swinford did more than just technical editing; they helped take these topics and made sure that they were understandable and accurate.

Finally, I want to thank all my students over the years. For some reason, I always get the best students. You make my job fun and are the reason why I love teaching.

From Bob Vachon:
I would first like to thank Rick Graziani for providing guidance and assistance when I needed it most. They say you can measure a man by the amount of respect he gets. Rick, you are a giant. Thank you. It has been a pleasure writing this book with you.

I would also like to thank my friends Jeremy Creech and John Behrens of Cisco for their continued support and for asking me to be part of a great development team. My sincere gratitude to the entire development team for their outstanding contribution. I am honored to work with such a fine group of dedicated people.

Special thanks to the folks at Cisco Press. A big thank-you goes to Mary Beth Ray for providing me the opportunity to be part of this project and to Chris Cleveland for your editing insight and patience. Thanks to the technical editors for providing a fresh set of eyes when reviewing the book.

A great big thanks to the folks at Cambrian College—specifically, Liz Moratz, Geoff Dalton, Sonia Del Missier, and Sylvia Barnard for your encouragement and support. I would also like to thank Betty Freelandt for providing me with the opportunity to discover the Cisco Networking Academy.

Finally, thanks to all my students. You’re the reason why we’re here. I learn so much from you, and you make me thankful for having the best job in the world!
## Contents at a Glance

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction to WANs</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>PPP</td>
<td>55</td>
</tr>
<tr>
<td>3</td>
<td>Frame Relay</td>
<td>127</td>
</tr>
<tr>
<td>4</td>
<td>Network Security</td>
<td>189</td>
</tr>
<tr>
<td>5</td>
<td>ACLs</td>
<td>309</td>
</tr>
<tr>
<td>6</td>
<td>Teleworker Services</td>
<td>377</td>
</tr>
<tr>
<td>7</td>
<td>IP Addressing Services</td>
<td>429</td>
</tr>
<tr>
<td>8</td>
<td>Network Troubleshooting</td>
<td>525</td>
</tr>
<tr>
<td>Appendix</td>
<td></td>
<td>601</td>
</tr>
<tr>
<td>Glossary</td>
<td></td>
<td>637</td>
</tr>
<tr>
<td>Index</td>
<td></td>
<td>655</td>
</tr>
</tbody>
</table>
Contents

Chapter 1 Introduction to WANs  1
  Objectives  1
  Key Terms  1
  Introducing Wide-Area Networks (WANs)  3
    What Is a WAN?  3
    Why Are WANs Necessary?  5
  The Evolving Enterprise  5
    Businesses and Their Networks  5
    Small Office (Single LAN)  6
    Campus (Multiple LANs)  6
    Branch (WAN)  8
    Distributed (Global)  9
  The Evolving Network Model  11
    The Hierarchical Design Model  11
    The Enterprise Architecture  13
  WAN Technology Concepts  17
    WAN Technology Overview  17
    WAN Physical Layer Concepts  18
    WAN Data Link Layer Concepts  23
    WAN Switching Concepts  26
  WAN Connection Options  29
    WAN Link Connection Options  29
    Dedicated Connection Link Options  31
    Circuit-Switched Connection Options  32
    Packet-Switched Connection Options  35
    Internet Connection Options  38
    Choosing a WAN Link Connection  44
  Summary  48
  Labs  49
  Check Your Understanding  50
  Challenge Questions and Activities  54
Chapter 3  Frame Relay  127

Objectives  127

Key Terms  127

Introduction  128

Basic Frame Relay Concepts  128
   Introducing Frame Relay  128
   Virtual Circuits  134
   Frame Relay Encapsulation  140
   Frame Relay Topologies  141
   Frame Relay Address Mapping  145

Configuring Frame Relay  152
   Enabling Frame Relay Encapsulation  153
   Configuring Static Frame Relay Maps  156

Advanced Frame Relay Concepts  159
   Solving Reachability Issues  159
   Frame Relay Subinterfaces  161
   Paying for Frame Relay  162
   Frame Relay Flow Control  166

Configuring Advanced Frame Relay  168
   Configuring Frame Relay Subinterfaces  168
   Verifying Frame Relay Operation  171
   Troubleshooting Frame Relay Configuration  178

Summary  180

Labs  181

Check Your Understanding  182

Challenge Questions and Activities  188

To Learn More  188

Chapter 4  Network Security  189

Objectives  189

Key Terms  189

Introduction to Network Security  190
   Why Is Network Security Important?  190
   Common Security Threats  199
   Types of Network Attacks  206
Using ACLs to Secure Networks  310
  A TCP Conversation  310
  Packet Filtering  313
  What Is an ACL?  316
  ACL Operation  318
  Types of Cisco ACLs  322
  How a Standard ACL Works  323
  Numbering and Naming ACLs  323
  Where to Place ACLs  324
  General Guidelines for Creating ACLs  327

Configuring Standard ACLs  327
  Entering Criteria Statements  327
  Configuring a Standard ACL  328
  ACL Wildcard Masking  332
  Applying Standard ACLs to Interfaces  339
  Editing Numbered ACLs  343
  Creating Standard Named ACLs  345
  Monitoring and Verifying ACLs  346
  Editing Named ACLs  347

Configuring an Extended ACL  348
  Extended ACLs  349
  Configuring Extended ACLs  351
  Applying Extended ACLs to the Interfaces  353
  Creating Named Extended ACLs  355

Configure Complex ACLs  357
  What Are Complex ACLs?  357
  Dynamic ACLs  358
  Reflexive ACLs  360
  Time-Based ACLs  363
  Troubleshooting Common ACL Errors  364

Summary  368

Labs  368

Check Your Understanding  369

Challenge Questions and Activities  375
Chapter 6  Teleworker Services  377

Objectives  377

Key Terms  377

Business Requirements for Teleworker Services  379

The Business Requirements for Teleworker Services  379

The Teleworker Solution  380

Broadband Services  384

Connecting Teleworkers to the WAN  384

Cable  385

DSL  391

Broadband Wireless  396

VPN Technology  401

VPNs and Their Benefits  402

Types of VPNs  405

VPN Components  407

Characteristics of Secure VPNs  408

VPN Tunneling  409

VPN Data Confidentiality and Integrity  410

IPsec Security Protocols  416

Summary  419

Labs  419

Check Your Understanding  419

Challenge Questions and Activities  423

Chapter 7  IP Addressing Services  429

Objectives  429

Key Terms  429

Introduction  431

DHCP  431

Introduction to DHCP  432

DHCP Operation  432

BOOTP and DHCP  435
<table>
<thead>
<tr>
<th>Chapter 8</th>
<th>Network Troubleshooting</th>
<th>525</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Objectives</strong></td>
<td>525</td>
<td></td>
</tr>
<tr>
<td><strong>Key Terms</strong></td>
<td>525</td>
<td></td>
</tr>
<tr>
<td><strong>Establishing the Network Performance Baseline</strong></td>
<td>526</td>
<td></td>
</tr>
<tr>
<td>Documenting Your Network</td>
<td>526</td>
<td></td>
</tr>
<tr>
<td>Network Documentation Process</td>
<td>533</td>
<td></td>
</tr>
<tr>
<td>Why Is Establishing a Network Baseline Important?</td>
<td>535</td>
<td></td>
</tr>
<tr>
<td>Steps for Establishing a Network Baseline</td>
<td>535</td>
<td></td>
</tr>
<tr>
<td><strong>Troubleshooting Methodologies and Tools</strong></td>
<td>541</td>
<td></td>
</tr>
<tr>
<td>A General Approach to Troubleshooting</td>
<td>541</td>
<td></td>
</tr>
<tr>
<td>Using Layered Models for Troubleshooting</td>
<td>541</td>
<td></td>
</tr>
<tr>
<td>General Troubleshooting Procedures</td>
<td>544</td>
<td></td>
</tr>
<tr>
<td>Troubleshooting Methods</td>
<td>545</td>
<td></td>
</tr>
<tr>
<td>Gathering Symptoms</td>
<td>548</td>
<td></td>
</tr>
<tr>
<td>Troubleshooting Tools</td>
<td>551</td>
<td></td>
</tr>
<tr>
<td><strong>Review of WAN Communications</strong></td>
<td>560</td>
<td></td>
</tr>
<tr>
<td>WAN Communications</td>
<td>560</td>
<td></td>
</tr>
<tr>
<td>Steps in WAN Design</td>
<td>561</td>
<td></td>
</tr>
<tr>
<td>WAN Traffic Considerations</td>
<td>562</td>
<td></td>
</tr>
<tr>
<td>WAN Topology Considerations</td>
<td>564</td>
<td></td>
</tr>
<tr>
<td>WAN Connection Technologies</td>
<td>567</td>
<td></td>
</tr>
<tr>
<td>WAN Bandwidth Considerations</td>
<td>568</td>
<td></td>
</tr>
<tr>
<td>Common WAN Implementations Issues</td>
<td>569</td>
<td></td>
</tr>
<tr>
<td>WAN Troubleshooting from an ISP’s Perspective</td>
<td>570</td>
<td></td>
</tr>
<tr>
<td><strong>Network Troubleshooting</strong></td>
<td>571</td>
<td></td>
</tr>
<tr>
<td>Physical Layer Troubleshooting</td>
<td>573</td>
<td></td>
</tr>
<tr>
<td>Data Link Layer Troubleshooting</td>
<td>577</td>
<td></td>
</tr>
<tr>
<td>Network Layer Troubleshooting</td>
<td>584</td>
<td></td>
</tr>
<tr>
<td>Transport Layer Troubleshooting</td>
<td>586</td>
<td></td>
</tr>
<tr>
<td>Application Layer Troubleshooting</td>
<td>589</td>
<td></td>
</tr>
</tbody>
</table>
Icons Used in This Book

Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Bold** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), bold indicates commands that the user enters (such as a `show` command).

- **Italic** indicates arguments for which you supply actual values.

- Vertical bars (|) separate alternative, mutually exclusive elements.

- Square brackets ([ ]) indicate an optional element.

- Braces ({ }) indicate a required choice.

- Braces within brackets ({{ } }) indicate a required choice within an optional element.
Introduction

The Cisco Networking Academy is a comprehensive e-learning program that provides students with Internet technology skills. A Networking Academy delivers web-based content, online assessment, student performance tracking, and hands-on labs to prepare students for industry-standard certifications. The CCNA curriculum includes four courses oriented around the topics on the Cisco Certified Network Associate (CCNA) certification.

Accessing the WAN, CCNA Exploration Companion Guide is the official supplement textbook to be used with version 4 of the CCNA Exploration Accessing the WAN online curriculum of the Networking Academy.

This book goes beyond earlier editions of the Cisco Press Companion Guides by providing many alternative explanations and examples as compared with the course. You can use the online curriculum as normal and use this Companion Guide to help solidify your understanding of all the topics through the alternative examples.

The basis for this book as well as the online curriculum is to help you understand several WAN technologies, including PPP and Frame Relay, and related topics, such as access control lists and Network Address Translation. This book also introduces other WAN technologies, such as DSL, cable modems, and Virtual Private Networks (VPNs).

Goals of This Book

First and foremost, by providing a fresh, complementary perspective on the topics, this book is intended to help you learn all the required materials of the Exploration Accessing the WAN course in the Networking Academy CCNA curriculum. As a secondary goal, the text is intended as a mobile replacement for the online curriculum for individuals who do not always have Internet access. In those cases, you can instead read the appropriate sections of the book, as directed by your instructor, and learn the same material that is covered in the online curriculum. Another secondary goal is to serve as your offline study material and help you prepare for the CCNA exam.

Audience for This Book

This book’s main audience is anyone taking the CCNA Exploration Accessing the WAN course of the Cisco Networking Academy curriculum. Many Academies use this textbook as a required tool in the course, and other Academies recommend the Companion Guides as an additional source of study and practice materials.

The secondary audience for this book includes people taking CCNA-related classes from professional training organizations. This book can also be used for college- and university-level networking courses, as well as by anyone who wants to gain a detailed understanding of wide-area networks.
Book Features

The educational features of this book focus on supporting topic coverage, readability, and practice of the course material to facilitate your full understanding of the course material.

Topic Coverage

The following features give you a thorough overview of the topics covered in each chapter so that you can make constructive use of your study time:

- **Objectives**: Listed at the beginning of each chapter, the objectives reference the core concepts covered in the chapter. The objectives match the objectives stated in the corresponding chapters of the online curriculum. However, the question format in the Companion Guide encourages you to think about finding the answers as you read the chapter.

- **“How-to” feature**: When this book covers a set of steps that you need to perform for certain tasks, this book lists the steps as a how-to list. When you are studying, the How To icon helps you easily find this feature as you skim through the book.

- **Notes, tips, cautions, and warnings**: These are sidebars that point out interesting facts, time-saving methods, and important safety issues.

- **Chapter summaries**: At the end of each chapter is a summary of the chapter’s key concepts. It provides a synopsis of the chapter and serves as a study aid.

Readability

The authors have compiled, edited, and in some cases rewritten the material so that it has a more conversational tone that follows a consistent and accessible reading level. In addition, the following features have been updated to aid your understanding of the networking vocabulary:

- **Key terms**: Each chapter begins with a list of key terms, along with a page number reference. The terms are listed in the order in which they are explained in the chapter. This handy reference allows you to see a term, flip to the page where it appears, and see it used in context. The glossary defines all the key terms.

- **Glossary**: This book contains an all-new glossary with more than 240 terms.
Practice

Practice makes perfect. This new Companion Guide offers you ample opportunities to put what you learn into practice. You will find the following features valuable and effective in reinforcing the instruction that you receive:

- **Check Your Understanding questions and answer key**: Updated review questions are presented at the end of each chapter as a self-assessment tool. These questions match the style of questions that you see in the online course. The appendix, “Check Your Understanding and Challenge Questions Answer Key,” provides the answers to all the questions and includes an explanation of each answer.

- **(New) Challenge questions and activities**: Additional—and more challenging—review questions and activities are presented at the end of each chapter. These questions are designed to be similar to the more complex styles of questions you might see on the CCNA exam. This section might also include activities to help prepare you for the exams. Appendix A provides the answers.

- **Packet Tracer activities**: Interspersed throughout the chapters, you’ll find many opportunities to work with the Cisco Packet Tracer tool. Packet Tracer allows you to create networks, visualize how packets flow in the network, and use basic testing tools to determine whether the network would work. When you see this icon, you can use Packet Tracer with the listed file to perform a task suggested in this book. The activity files are available on this book’s CD-ROM; Packet Tracer software is available through the Academy Connection website. Ask your instructor for access to Packet Tracer.

Labs and Study Guide

The supplementary book Accessing the WAN, CCNA Exploration Labs and Study Guide by Cisco Press (ISBN: 1-58713-201-x) contains all the labs from the curriculum plus additional challenge labs and study guide material. The end of each chapter of this Companion Guide indicates with icons what labs, activities, and Packet Tracer activities are available in the Labs and Study Guide.

- **Lab references**: This icon notes the hands-on labs created for this chapter in the online curriculum. In Accessing the WAN, CCNA Exploration Labs and Study Guide you will also find additional labs and study guide material created by the author of that book.

- **(New) Packet Tracer Companion activities**: Many of the hands-on labs include Packet Tracer Companion activities, where you can use Packet Tracer to complete a simulation of the lab. Look for this icon in Accessing the WAN, CCNA Exploration Labs and Study Guide for hands-on labs that have a Packet Tracer Companion.
- **(New) Packet Tracer Skills Integration Challenge activities**: These activities require you to pull together several skills you learned from the chapter to successfully complete one comprehensive exercise. Look for this icon in *Accessing the WAN, CCNA Exploration Labs and Study Guide* for instructions on how to perform the Packet Tracer Skills Integration Challenge for this chapter.

### A Word About Packet Tracer Software and Activities

Packet Tracer is a self-paced, visual, interactive teaching and learning tool developed by Cisco. Lab activities are an important part of networking education. However, lab equipment can be a scarce resource. Packet Tracer provides a visual simulation of equipment and network processes to offset the challenge of limited equipment. Students can spend as much time as they like completing standard lab exercises through Packet Tracer, and they have the option to work from home. Although Packet Tracer is not a substitute for real equipment, it allows students to practice using a command-line interface. This “e-doing” capability is a fundamental component of learning how to configure routers and switches from the command line.

Packet Tracer version 4.x is available only to Cisco Networking Academies through the Academy Connection website. Ask your instructor for access to Packet Tracer.

The course essentially includes three different types of Packet Tracer activities. This book uses icons to indicate which type of Packet Tracer activity is available. The icons are intended to give you a sense of the activity’s purpose and the amount of time you’ll need to complete it. The three types of Packet Tracer activities are as follows:

- **Packet Tracer Activity**: This icon identifies straightforward exercises interspersed throughout the chapters, where you can practice or visualize a specific topic. The activity files for these exercises are available on the book’s CD-ROM. These activities take less time to complete than the Packet Tracer Companion and Challenge activities.

- **Packet Tracer Companion**: This icon identifies exercises that correspond to the course’s hands-on labs. You can use Packet Tracer to complete a simulation of the hands-on lab or complete a similar “lab.” The *Companion Guide* points these out at the end of each chapter, but look for this icon and the associated exercise file in *Accessing the WAN, CCNA Exploration Labs and Study Guide* for hands-on labs that have a Packet Tracer Companion.

- **Packet Tracer Skills Integration Challenge**: This icon identifies activities that require you to pull together several skills you learned from the chapter to successfully complete one comprehensive exercise. The *Companion Guide* points these out at the end of each chapter, but look for this icon in *Accessing the WAN, CCNA Exploration Labs and Study Guide* for instructions on how to perform the Packet Tracer Skills Integration Challenge for this chapter.
How This Book Is Organized

The book covers the major topic headings in the same sequence as the online curriculum for the CCNA Exploration Accessing the WAN course. This book has eight chapters, with the same numbers and similar names as the online course chapters.

If you’re reading this book without being in the CCNA Accessing the WAN class, or if you’re just using this book for self-study, the sequence of topics in each chapter provides a logical sequence for learning the material presented.

- **Chapter 1, “Introduction to WANs,”** provides an overview of the options available for designing enterprise WANs, the technologies available to implement them, and the terminology used to discuss them. You will learn about selecting the appropriate WAN technologies, services, and devices to meet the changing business requirements of an evolving enterprise.

- **Chapter 2, “PPP,”** examines PPP, including its roots in HDLC, PPP concepts, PPP layered architecture, and configuring PPP. Configuring PPP with authentication using PAP and CHAP are also discussed.

- **Chapter 3, “Frame Relay,”** examines the Frame Relay protocol. Basic Frame Relay concepts are discussed, including encapsulation, topologies, and address mapping. Various Frame Relay configuration techniques are examined, including the use of static Frame Relay maps, the use of inverse ARP, and configuring Frame Relay on subinterfaces.

- **Chapter 4, “Network Security,”** covers the threats and attacks that face many of today’s networks. Security policies and mitigation techniques are discussed. Securing networks and devices is examined, including an introduction to Cisco SDM. Managing Cisco IOS images is also discussed in this chapter, including password recovery and restoring IOS images.

- **Chapter 5, “ACLs,”** discusses ACL operation and guidelines using standard, extended, and named ACLs. Configuring ACLs is examined, including using wildcard masks, monitoring ACLs, and applying ACLs to interfaces. Dynamic ACLs, reflexive ACLs, and time-based ACLs are introduced.

- **Chapter 6, “Teleworker Services,”** discusses how organizations can provide secure, fast, and reliable remote network connections for teleworkers. This chapter introduces DSL, cable modem, and broadband wireless. VPNs and IPsec also are discussed.

- **Chapter 7, “IP Addressing Services,”** discusses DHCP, NAT, and IPv6. This chapter includes both the concepts and configurations needed to implement these technologies.

- **Chapter 8, “Network Troubleshooting,”** discusses documenting your network, creating a baseline, and the troubleshooting tools and methodologies used in diagnosing network issues.
The appendix, “Check Your Understanding and Challenge Questions Answer Key,” provides the answers to the Check Your Understanding questions at the end of each chapter. It also includes answers for the Challenge Questions and Activities that conclude most chapters.

The glossary defines all the key terms that appear throughout this book.

About the CD-ROM

The CD-ROM included with this book provides many useful tools and information to support your education:

- **Packet Tracer Activity files**: These are files to work through the Packet Tracer Activities referenced throughout the book, as indicated by the Packet Tracer Activity icon.

- **Taking Notes**: This section includes a .txt file of the chapter objectives to serve as a general outline of the key topics of which you need to take note. The practice of taking clear, consistent notes is an important skill not only for learning and studying the material but for on-the-job success as well. Also included in this section is “A Guide to Using a Networker’s Journal” PDF booklet providing important insight into the value of the practice of using a journal, how to organize a professional journal, and some best practices on what, and what not, to take note of in your journal.

- **IT Career Information**: This section includes a student guide to applying the toolkit approach to your career development. Learn more about entering the world of information technology as a career by reading two informational chapters excerpted from The IT Career Builder’s Toolkit: “The Job Search” and “The Interview.”

- **Lifelong Learning in Networking**: As you embark on a technology career, you will notice that it is ever-changing and evolving. This career path provides new and exciting opportunities to learn new technologies and their applications. Cisco Press is one of the key resources to plug into on your quest for knowledge. This section of the CD-ROM provides an orientation to the information available to you and tips on how to tap into these resources for lifelong learning.

About the Cisco Press Website for This Book

Cisco Press may provide additional content that you can access by registering your book at the ciscopress.com website. Becoming a member and registering is free, and you then gain access to exclusive deals on other resources from Cisco Press.

To register this book, go to [http://www.ciscopress.com/bookstore/register.asp](http://www.ciscopress.com/bookstore/register.asp) and enter the book’s ISBN, located on the back cover. You’ll then be prompted to log in or to join ciscopress.com to continue the registration.

After you register this book, a link to the supplemental content will be listed on your My Registered Books page.
CHAPTER 1

Introduction to WANs

Objectives

After completing this chapter, you should be able to answer the following questions:

■ How does the Cisco enterprise architecture provide integrated services over an enterprise network?
■ What are the key WAN technology concepts?
■ What appropriate WAN technologies are used to meet different enterprise business requirements?

Key Terms

This chapter uses the following key terms. You can find the definitions in the glossary at the end of the book.

wide-area network (WAN) page 3
enterprise network page 3
data communications page 3
transactions page 5
voice over IP (VoIP) page 6
broadband page 6
teleworkers page 11
wiring closets page 11
backbone page 12
metropolitan-area network (MAN) page 15
Frame Relay page 18
Asynchronous Transfer Mode (ATM) page 18
High-Level Data Link Control (HDLC) page 18
Customer Premises Equipment (CPE) page 19
channel page 19
Data Communications Equipment (DCE) page 19
Data Terminal Equipment (DTE) page 19
local loop page 19
cable page 19
demarcation point page 19
central office (CO) page 19
communications lines page 19
modem page 20
T1 page 20
T3 page 20
channel service unit (CSU) page 20
data service unit (DSU) page 20
T-carrier page 20
access server page 21
X.25 page 21
public switched telephone network (PSTN) page 21
Integrated Services Digital Network (ISDN)  page 21
point of presence (POP)  page 21
core router  page 21
High-Speed Serial Interface (HSSI)  page 22
Point-to-Point Protocol (PPP)  page 24
circuit  page 26
time-division multiplexing (TDM)  page 26
circuit-switching  page 27
packet switching  page 27
packet-switched network  page 27
connectionless  page 27
connection-oriented  page 27
Data Link Connection Identifiers (DLCI)  page 27
virtual circuit (VC)  page 27
permanent virtual circuit (PVC)  page 28
switched virtual circuit (SVC)  page 28
leased line  page 29
telephony  page 33
bearer (B) channels  page 33
signaling  page 33
delta channel  page 33
Basic Rate Interface (BRI)  page 33
Primary Rate Interface (PRI)  page 34
synchronization  page 34
E1  page 34
J1  page 34
call setup time  page 34
cell  page 38
cable television  page 39
headend 39
Microwave 40
firewall 42
When an enterprise grows to include branch offices, e-commerce services, or global operations, a single local-area network (LAN) is no longer sufficient to meet its business requirements. **Wide-area network (WAN)** access has become essential for larger businesses today.

A variety of WAN technologies meet the different needs of businesses, and there are many ways to scale the network. Adding WAN access introduces other considerations, such as network security and address management. Consequently, designing a WAN and choosing the correct carrier network services is not a simple matter.

In this chapter, you will begin exploring some of the options available for designing enterprise WANs, the technologies available to implement them, and the terminology used to discuss them. You will learn about selecting the appropriate WAN technologies, services, and devices to meet the changing business requirements of an evolving enterprise. The activities and labs confirm and reinforce your learning.

After completing this chapter, you will be able to identify and describe the appropriate WAN technologies to enable integrated WAN services over a multilocation enterprise network.

---

**Introducing Wide-Area Networks (WANs)**

One way to categorize networks is to divide them into local-area networks (LAN) and wide-area networks (WAN). LANs typically are connected workstations, printers, and other devices within a limited geographic area such as a building. All the devices in the LAN are under the common administration of the owner of that LAN, such as a company or an educational institution. Most LANs today are Ethernet LANs.

WANs are networks that span a larger geographic area and usually require the services of a common carrier. Examples of WAN technologies and protocols include Frame Relay, ATM, and DSL.

**What Is a WAN?**

A WAN is a *data communications* network that operates beyond the geographic scope of a LAN. Figure 1-1 shows the relative location of a LAN and WAN.
WANs differ from LANs in several ways. Whereas a LAN connects computers, peripherals, and other devices in a single building or other small geographic area, a WAN allows the transmission of data across greater geographic distances. In addition, an enterprise must subscribe to a WAN service provider to use WAN carrier network services. LANs typically are owned by the company or organization that uses them.

WANs use facilities provided by a service provider, or carrier, such as a telephone or cable company, to connect the locations of an organization to each other, to locations of other organizations, to external services, and to remote users. WANs provide network capabilities to support a variety of mission-critical traffic such as voice, video, and data.

Here are the three major characteristics of WANs:

- WANs generally connect devices that are separated by a broader geographic area than can be served by a LAN.
- WANs use the services of carriers, such as telephone companies, cable companies, satellite systems, and network providers.
- WANs use serial connections of various types to provide access to bandwidth over large geographic areas.
Why Are WANs Necessary?

LAN technologies provide both speed and cost efficiency for the transmission of data in organizations over relatively small geographic areas. However, other business needs require communication among remote sites, including the following:

- People in the regional or branch offices of an organization need to be able to communicate and share resources with the central site.
- Organizations often want to share information with other organizations across large distances. For example, software manufacturers routinely communicate product and promotion information to distributors that sell their products to end users.
- Employees who frequently travel on company business need to access information that resides on their corporate networks.

In addition, home computer users need to send and receive data across increasingly larger distances. Here are some examples:

- It is now common in many households for consumers to communicate with banks, stores, and a variety of providers of goods and services via computers.
- Students do research for classes by accessing library catalogs and publications located in other parts of their country and in other parts of the world.

Because it is obviously not feasible to connect computers across a country or around the world in the same way that they are connected in a LAN with cables, different technologies have evolved to support this need. The Internet has become and continues to be an inexpensive alternative for WAN connectivity. New technologies are available to businesses to provide security and privacy for their Internet communications and transactions. WANs used by themselves, or in concert with the Internet, allow organizations and individuals to meet their wide-area communication needs.

The Evolving Enterprise

As companies grow, they hire more employees, open branch offices, and expand into global markets. These changes also influence companies’ requirements for integrated services and drive their network requirements. This section explores how company networks evolve to accommodate companies’ changing business requirements.

Businesses and Their Networks

Every business is unique. How an organization grows depends on many factors, such as the type of products or services the business sells, the owners’ management philosophy, and the economic climate of the country in which the business operates.
In slow economic times, many businesses focus on increasing their profitability by improving the efficiency of the existing operations, increasing employee productivity, and lowering operating costs. Establishing and managing networks can represent significant installation and operating expenses. To justify such a large expense, companies expect their networks to perform optimally and to be able to deliver an ever-increasing array of services and applications to support productivity and profitability.

To illustrate, we’ll use a fictitious company called Span Engineering as an example. You’ll watch how its network requirements change as the company grows from a small local business into a global enterprise.

**Small Office (Single LAN)**

Span Engineering, an environmental consulting firm, has developed a special process for converting household waste into electricity. It is developing a small pilot project for a municipal government in its local area. The company, which has been in business for four years, has grown to include 15 employees: six engineers, four computer-aided drawing (CAD) designers, two senior partners, a receptionist, and two office assistants.

Span Engineering’s management is hoping that the company will have full-scale projects after the pilot project successfully demonstrates the feasibility of its process. Until then, the company must manage its costs carefully.

For its small office, shown in Figure 1-2, Span Engineering uses a single LAN to share information between computers and to share peripherals, such as a printer, a large-scale plotter (to print engineering drawings), and fax equipment. The company recently upgraded its LAN to provide inexpensive voice over IP (VoIP) service to save on the costs of separate phone lines for its employees.

The company connects to the Internet through a common broadband service called Digital Subscriber Line (DSL), which is supplied by the local telephone service provider. With so few employees, bandwidth is not a significant problem.

The company cannot afford in-house information technology (IT) support staff, so it uses support services purchased from the same service provider. The company also uses a hosting service rather than purchasing and operating its own FTP and e-mail servers.

**Campus (Multiple LANs)**

Five years later, Span Engineering has grown rapidly. As the owners had hoped, the company was contracted to design and implement a full-sized waste conversion facility soon after the successful implementation of their first pilot plant. Since then, other projects have also been won in neighboring municipalities and in other parts of the country.
To handle the additional workload, the business has hired more staff and leased more office space. It is now a small to medium-sized business with several hundred employees. Many projects are being developed at the same time, and each requires a project manager and support staff. The company has organized itself into functional departments, with each department having its own organizational team. To meet its growing needs, the company has moved into several floors of a larger office building.

As the business has expanded, the network has also grown. Instead of a single small LAN, the network now consists of several subnetworks, each devoted to a different department. For example, all the engineering staff are on one LAN, and the marketing staff is on another LAN. These multiple LANs are joined to create a company-wide network, or campus, which spans several floors of the building. Figure 1-3 shows Span Engineering’s expanded campus LAN.

The business now has in-house IT staff to support and maintain the network. The network includes servers for e-mail, data transfer and file storage, web-based productivity tools, and applications. The network includes a company intranet to provide in-house documents and information to employees. In addition, the company has an extranet that provides project information only to designated customers.
Another five years later, Span Engineering has been so successful with its patented process that demand for its services has skyrocketed. New projects are now being built in other cities. To manage those projects, the company has opened small branch offices closer to the project sites.

This situation presents new challenges to the IT team. To manage the delivery of information and services throughout the company, Span Engineering now has a data center, which houses the company’s various databases and servers. To ensure that all parts of the business can access the same services and applications regardless of where the offices are located, the company now needs to implement a WAN.

For its branch and regional offices that are in nearby cities, the company decides to use private dedicated lines through its local service provider, as shown in Figure 1-4. However, for the offices that are located in other countries, the Internet is now an attractive WAN connection option. Although connecting offices through the Internet is economical, it introduces security and privacy issues that the IT team must address.
Span Engineering has now been in business for 20 years and has grown to thousands of employees distributed in offices worldwide. The cost of the network and its related services is a significant expense. The company is looking to provide its employees with the best network services at the lowest cost. Optimized network services would allow each employee to work at high efficiency.

To increase profitability, Span Engineering needs to reduce its operating expenses. It has relocated some of its office facilities to less expensive areas. The company is also encouraging teleworking and virtual teams. Web-based applications—including web conferencing, e-learning, and online collaboration tools—are being used to increase productivity and reduce costs. Site-to-site and remote-access Virtual Private Networks (VPN) enable the company to use the Internet to connect easily and securely with employees and facilities around the world. To meet these requirements, the network must provide the necessary converged services and secure Internet WAN connectivity to remote offices and individuals. Figure 1-5 shows SPAN Engineering’s new distributed or global network.
As you can see from this example, a company’s network requirements can change dramatically as the company grows over time. Distributing employees saves costs in many ways, but it puts increased demands on the network. Not only must a network meet the business’s day-to-day operational needs, but it also needs to be able to adapt and grow as the company changes. Network designers and administrators meet these challenges by carefully choosing network technologies, protocols, and service providers, and by optimizing their networks using many of the techniques we teach in this series of courses. The next sections describe a model for designing networks that can accommodate the changing needs of today’s evolving businesses.
The Evolving Network Model

The hierarchical network model is a framework that helps you visualize and design networks. Several variations of this model exist, and it can be adapted for specific implementations.

The Hierarchical Design Model

Figure 1-6 shows the hierarchical network model, which is a useful high-level tool for designing a reliable network infrastructure. It provides a modular view of a network, making it easier to design and build a scalable network. The figure conceptually displays the model and identifies its major responsibilities.

Figure 1-6  Hierarchical Network Model

The Hierarchical Network Model

As you may recall from CCNA Exploration: LAN Switching and Wireless, the hierarchical network model divides a network into three layers:

- The access layer grants user access to network devices. In a network campus, the access layer generally incorporates switched LAN devices with ports that provide connectivity to workstations and servers. In the WAN environment, it may give teleworkers or remote sites access to the corporate network across WAN technology.

- The distribution layer aggregates the wiring closets, using switches to segment workgroups and isolate network problems in a campus environment. Similarly, the distribution layer aggregates WAN connections at the edge of the campus and provides policy-based connectivity.
The core layer (also called the backbone) is a high-speed backbone that is designed to switch packets as fast as possible. Because the core is critical for connectivity, it must provide a high level of availability and adapt to changes very quickly. It also provides scalability and fast convergence.

Figure 1-7 represents the Hierarchical Network Model in campus environments. The Hierarchical Network Model provides a modular framework that allows flexibility in network design and facilitates ease of implementation and troubleshooting in the infrastructure. However, it is important to understand that the network infrastructure is only the foundation of a comprehensive architecture.

![Hierarchical Network Model in Campus Environments](image)

Networking technologies have advanced considerably in recent years, resulting in networks that are increasingly intelligent. The current network elements are more aware of traffic characteristics and can be configured to deliver specialized services based on such things as the types of data they carry, the data’s priority, and even the security needs. Although most of these various infrastructure services are outside the scope of this course, it is important to understand that they influence network design. The next sections explore the Cisco Enterprise Architecture, which expands on the hierarchical model by making use of network intelligence to address the network infrastructure.
The Enterprise Architecture

As described earlier, different businesses need different types of networks, depending on how the business is organized and its business goals. Unfortunately, all too often networks grow in a haphazard way as new components are added in response to immediate needs. Over time, those networks become complex and expensive to manage. Because the network is a mixture of newer and older technologies, it can be difficult to support and maintain. Outages and poor performance are a constant source of trouble for network administrators.

To help prevent this situation, Cisco has developed a recommended architecture called the Cisco Enterprise Architecture. It has relevance to the different stages of a business’s growth, as shown in Figure 1-8. This architecture is designed to give network planners a road map for network growth as the business moves through different stages. By following the suggested road map, IT managers can plan for future network upgrades that will integrate seamlessly into the existing network and support the ever-growing need for services.

Figure 1-8 Cisco Enterprise Architecture
The Cisco Enterprise Architecture consists of modules representing focused views that target each place in the network. Each module has a distinct network infrastructure with services and network applications that extend across the modules. The following are some of the modules within the architecture that are relevant to the Span Engineering scenario described earlier:

- Enterprise Campus Architecture
- Enterprise Branch Architecture
- Enterprise Data Center Architecture
- Enterprise Teleworker Architecture

Figure 1-9 shows the Cisco Enterprise Architecture, which consists of modules representing focused views that target each place in the network. Each module has a distinct network infrastructure with services and network applications that extend across the modules.

**Figure 1-9   Modules of the Enterprise Architecture**

The Cisco Enterprise Architecture includes the following modules, each of which is described in greater detail in the following sections:

- Enterprise Campus Architecture
Enterprise Campus Architecture

A campus network is a building or group of buildings connected into one enterprise network that consists of many LANs. A campus generally is limited to a fixed geographic area, but it can span several neighboring buildings, such as an industrial complex or business park environment. In the Span Engineering example, the campus spans multiple floors of the same building.

The Enterprise Campus Architecture describes the recommended methods to create a scalable network while addressing the needs of campus-style business operations. The architecture is modular and can easily expand to include additional campus buildings or floors as the enterprise grows. The Enterprise Campus Architecture, as illustrated in Figure 1-9, is composed of four submodules:

- The building access contains end-user workstations, IP phones, and Layer 2 access switches that connect devices to the building distribution submodule.
- The building distribution provides aggregation of building access devices, often using Layer 3 switching. This submodule performs routing, quality control, and access control.
- The campus core provides redundant and fast-converging connectivity between buildings and the server farm and enterprise edge.
- The server farm contains e-mail and corporate servers providing application, file, print, e-mail, and Domain Name System (DNS) services to internal users.

The enterprise campus module describes the connections between users, the campus network, the server farm, and the Enterprise Edge modules.

Enterprise Edge Architecture

This module, as illustrated in Figure 1-9, often functions as a liaison between the campus module and the other modules in the Enterprise Architecture. It offers connectivity to voice, video, and data services outside the enterprise. It enables the enterprise to use Internet and partner resources and provide resources for its customers. The Enterprise WAN and metropolitan-area network (MAN) Architecture, which the technologies covered later in this course are relevant to, are considered part of this module.
The enterprise edge aggregates the connectivity from the various functional areas at the enterprise edge (e-commerce, Internet connectivity, and VPNs) and routes the traffic into the campus core submodule.

**Enterprise Branch Architecture**
This module, as illustrated in Figure 1-9, allows businesses to extend the applications and services found at the campus to thousands of remote locations and users or to a small group of branches. Much of this course focuses on the technologies that are often implemented in this module.

**Enterprise Data Center Architecture**
Data centers provide management for many data systems that are vital to modern business operations. Employees, partners, and customers rely on data and resources in the data center to effectively create, collaborate, and interact. Over the last decade, the rise of Internet and web-based technologies has made the data center more important than ever, improving productivity, enhancing business processes, and accelerating change.

The enterprise data center, as illustrated in Figure 1-9, manages and maintains centralized data systems for the entire enterprise.

**Enterprise Teleworker Architecture**
Many businesses today offer a flexible work environment to their employees, allowing them to telecommute from home offices. To telecommute is to leverage the network resources of the enterprise from home. The teleworker module, as illustrated in Figure 1-9, recommends that connections from home using broadband services such as cable modem or DSL connect to the Internet and from there to the corporate network. Because the Internet introduces significant security risks to businesses, special measures need to be taken to ensure that teleworker communications are secure and private.

The enterprise teleworker module connects individual employees to network resources remotely, typically from their homes.

Figure 1-10 shows how all the Enterprise Architecture modules can be used to build a business network topology.
This section discusses the physical and data link layer concepts of wide-area networks, including an introduction to some of the standards and protocols.

**WAN Technology Concepts**

A variety of protocols and technologies are used in wide-area networks. Some of these services, such as HDLC and Frame Relay, are explained in more detail later in this book.

As described in relation to the OSI reference model, WAN operations focus primarily on Layer 1 and Layer 2, as shown in Figure 1-11. WAN access standards typically describe both physical layer delivery methods and data link layer requirements, including physical addressing, flow control, and encapsulation. WAN access standards are defined and managed by a number of recognized authorities, including the International Organization for Standardization (ISO), the Telecommunication Industry Association (TIA), and the Electronic Industries Alliance (EIA).
As highlighted in Figure 1-11, the physical layer (OSI Layer 1) protocols describe how to provide electrical, mechanical, operational, and functional connections to the services of a communications service provider.

The data link layer (OSI Layer 2) protocols define how data is encapsulated for transmission toward a remote location and the mechanisms for transferring the resulting frames. A variety of technologies are used, such as Frame Relay and Asynchronous Transfer Mode (ATM). Some of these protocols use the same basic framing mechanism, High-Level Data Link Control (HDLC), an ISO standard, or one of its subsets or variants.

**WAN Physical Layer Concepts**

The WAN physical layer includes several devices and terms specific to wide-area networks, as described in the following sections.

**WAN Physical Layer Terminology**

One primary difference between a WAN and a LAN is that for a company or organization to use WAN carrier network services, it must subscribe to an outside WAN service provider. A WAN uses data links provided by carrier services to access or connect the locations of an
organization to each other, to locations of other organizations, to external services, and to remote users. The WAN access physical layer describes the physical connection between the company network and the service provider network.

Figure 1-12 illustrates the terminology commonly used to describe physical WAN connections, as described in further detail in the following list:

- **Customer Premises Equipment (CPE):** The devices and inside wiring located at the premises of the subscriber, connected with a telecommunication channel of a carrier. The subscriber either owns or leases the CPE. A subscriber, in this context, is a company that arranges for WAN services from a service provider or carrier.

- **Data Communications Equipment (DCE):** Also called data circuit-terminating equipment, the DCE consists of devices that put data on the local loop. The DCE primarily provides an interface to connect subscribers to a communication link on the WAN cloud.

- **Data Terminal Equipment (DTE):** The customer devices that pass the data from a customer network or host computer for transmission over the WAN. The DTE connects to the local loop through the DCE.

- **Local loop:** The copper or fiber cable that connects the CPE at the subscriber site to the central office (CO) of the service provider. The local loop is sometimes called the “last mile.”

- **Demarcation point:** A point established in a building or complex to separate customer equipment from service provider equipment. Physically, the demarcation point is the cabling junction box, located on the customer premises, that connects the CPE wiring to the local loop. It is usually placed for easy access by a technician. The demarcation point is the place where the responsibility for the connection changes from the user to the service provider. This is very important, because when problems arise, it is necessary to determine whether the user or the service provider is responsible for troubleshooting or repair.

- **Central office (CO):** A local service provider facility or building where local cables link to long-haul, all-digital, fiber-optic communications lines through a system of switches and other equipment.
WAN Devices

WANs use numerous types of devices that are specific to WAN environments:

- **Modem**: Modulates an analog carrier signal to encode digital information, and also demodulates the carrier signal to decode the transmitted information. A voiceband modem converts the digital signals produced by a computer into voice frequencies that can be transmitted over the analog lines of the public telephone network. On the other side of the connection, another modem converts the sounds back into a digital signal for input to a computer or network connection. Faster modems, such as cable modems and DSL modems, transmit using higher broadband frequencies.

- **CSU/DSU**: Digital lines, such as T1 and T3 carrier lines, require a **channel service unit (CSU)** and a **data service unit (DSU)**. The two are often combined into a single piece of equipment, called the CSU/DSU. The CSU provides termination for the digital signal and ensures connection integrity through error correction and line monitoring. The DSU converts the T-carrier line frames into frames that the LAN can interpret and vice versa.
- **Access server**: Concentrates dial-in and dial-out user communications. An access server may have a mixture of analog and digital interfaces and support hundreds of simultaneous users.

- **WAN switch**: A multiport internetworking device used in carrier networks. These devices typically switch traffic such as Frame Relay, ATM, or X.25 and operate at the data link layer of the OSI reference model. *Public switched telephone network (PSTN)* switches may also be used within the cloud for circuit-switched connections such as *Integrated Services Digital Network (ISDN)* or analog dialup.

- **Router**: Provides internetworking and WAN access interface ports that are used to connect to the service provider network. These interfaces may be serial connections or other WAN interfaces. With some types of WAN interfaces, an external device such as a DSU/CSU or modem (analog, cable, or DSL) is required to connect the router to the service provider’s local **point of presence (POP)**.

- **Core router**: A router that resides within the middle or backbone of the WAN rather than at its periphery. To fulfill this role, a router must be able to support multiple telecommunications interfaces of the highest speed in use in the WAN core, and it must be able to forward IP packets at full speed on all those interfaces. The router must also support the routing protocols being used in the core.

Figure 1-13 shows the location of each device.

**Figure 1-13  WAN Devices**
**WAN Physical Layer Standards**

WAN physical-layer protocols describe how to provide electrical, mechanical, operational, and functional connections for WAN services. The WAN physical layer also describes the interface between the DTE and DCE.

The DTE/DCE interface uses various physical layer protocols:

- **EIA/TIA-232**: This protocol allows signal speeds of up to 64 kbps on a 25-pin D-connector over short distances. It was formerly known as RS-232. The ITU-T V.24 specification is effectively the same.

- **EIA/TIA-449/530**: This protocol is a faster (up to 2 Mbps) version of EIA/TIA-232. It uses a 36-pin D-connector and is capable of longer cable runs. Several versions exist. This standard is also known as RS-422 and RS-423.

- **EIA/TIA-612/613**: This standard describes the **High-Speed Serial Interface (HSSI)** protocol, which provides access to services up to 52 Mbps on a 60-pin D-connector.

- **V.35**: This is the ITU-T standard for synchronous communications between a network access device and a packet network. Originally specified to support data rates of 48 kbps, it now supports speeds of up to 2.048 Mbps using a 34-pin rectangular connector.

- **X.21**: This protocol is an ITU-T standard for synchronous digital communications. It uses a 15-pin D-connector.

These protocols establish the codes and electrical parameters the devices use to communicate with each other. Choosing a protocol is largely determined by the service provider’s method of facilitation.

Figure 1-14 illustrates the types of cable connectors associated with each physical layer protocol.

**Figure 1-14  WAN Cable Connectors**
WAN Data Link Layer Concepts

In addition to physical layer devices, WANs require data link layer protocols to establish the link across the communication line from the sending to the receiving device. This section describes the common data link protocols that are used in today’s enterprise networks to implement WAN connections.

Data Link Protocols

Data link layer protocols define how data is encapsulated for transmission to remote sites and the mechanisms for transferring the resulting frames. A variety of technologies are used, such as ISDN, Frame Relay, or ATM, as shown in Figure 1-15. Many of these protocols use the same basic framing mechanism, HDLC, an ISO standard, or one of its subsets or variants. ATM is different from the others, because it uses small fixed-size cells of 53 bytes (48 bytes for data), unlike the other packet-switched technologies, which use variable-sized packets.

Figure 1-15  Data Link Layer Protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Access Procedure Balanced (LAPB)</td>
<td>X.25</td>
</tr>
<tr>
<td>Link Access Procedure D Channel (LAPD)</td>
<td>ISDN D Channel</td>
</tr>
<tr>
<td>Link Access Procedure Frame (LAPF)</td>
<td>Frame Relay</td>
</tr>
<tr>
<td>High-Level Data Link Control (HDLC)</td>
<td>Cisco Default</td>
</tr>
<tr>
<td>Point-to-Point Protocol (PPP)</td>
<td>Serial WAN Switched Connections</td>
</tr>
</tbody>
</table>
The most common WAN data-link protocols are as follows:

- **HDLC**
- **Point-to-Point Protocol (PPP)**
- **Frame Relay**
- **ATM**

ISDN and X.25 are older data-link protocols that are less frequently used today. However, ISDN is still covered in this course because of its use when provisioning a VoIP network using PRI links. X.25 is mentioned to help explain the relevance of Frame Relay. As well, X.25 is still in use in developing countries where packet data networks (PDN) are used to transmit credit card and debit card transactions from retailers.

**Note**

Another data link layer protocol is Multiprotocol Label Switching (MPLS). MPLS is increasingly being deployed by service providers as an economical solution to carry circuit-switched as well as packet-switched network traffic. It can operate over any existing infrastructure, such as IP, Frame Relay, ATM, or Ethernet. It sits between Layer 2 and Layer 3 and is sometimes referred to as a Layer 2.5 protocol. MPLS is beyond the scope of this course, but it is covered on the CCNP: Implementing Secure Converged Wide Area Networks course.

**WAN Encapsulation**

Data from the network layer is passed to the data link layer for delivery on a physical link, which normally is point-to-point on a WAN connection. The data link layer builds a frame around the network layer data so that the necessary checks and controls can be applied. Each WAN connection type uses a Layer 2 protocol to encapsulate a packet while it is crossing the WAN link. To ensure that the correct encapsulation protocol is used, the Layer 2 encapsulation type used for each router serial interface must be configured. The choice of encapsulation protocols depends on the WAN technology and the equipment. HDLC was first proposed in 1979; for this reason, most framing protocols that were developed afterwards are based on it.

Figure 1-16 shows how WAN data link protocols encapsulate traffic.

Examining the header portion of an HDLC frame, shown in Figure 1-17, helps you identify common fields used by many WAN encapsulation protocols. The frame always starts and ends with an 8-bit Flag field. The bit pattern is 01111110. The Address field is not needed for WAN links, which are almost always point-to-point. The Address field is still present and may be 1 or 2 bytes long. The Control field is protocol-dependent, but it usually indicates whether the data is control information or network layer data. The Control field normally is 1 byte.
The Address and Control fields, as illustrated in Figure 1-17, are called the frame header. The encapsulated data follows the Control field. Then a frame check sequence (FCS) uses the cyclic redundancy check (CRC) mechanism to establish a 2- or 4-byte field.

Several types of WAN encapsulation formats exist, including subsets and proprietary versions of HDLC. Both PPP and the Cisco version of HDLC have an extra field in the header to identify the network layer protocol of the encapsulated data.
**WAN Switching Concepts**

WAN switched networks are categorized as either circuit-switched or packet-switched, as described in greater detail in the following sections.

**Circuit Switching**

A circuit-switched network is one that establishes a dedicated *circuit* (or channel) between nodes and terminals before the users may communicate.

As an example, Figure 1-18 shows that when a subscriber makes a telephone call, the dialed number is used to set switches in the exchanges along the call’s route so that a continuous circuit exists from the caller to the called party. Because of the switching operation used to establish the circuit, the telephone system is called a circuit-switched network. If the telephones are replaced with modems, the switched circuit can carry computer data.

**Figure 1-18  Circuit Switching**

The internal path taken by the circuit between exchanges is shared by a number of conversations. *Time-division multiplexing (TDM)* gives each conversation a share of the connection in turn. TDM ensures that a fixed-capacity connection is made available to the subscriber.
If the circuit carries computer data, the usage of this fixed capacity may be inefficient. For example, if the circuit is used to access the Internet, a burst of activity occurs on the circuit while a web page is transferred. This could be followed by no activity while the user reads the page, and then another burst of activity while the next page is transferred. This variation in usage between none and maximum is typical of computer network traffic. Because the subscriber has sole use of the fixed-capacity allocation, switched circuits generally are an expensive way of moving data.

PSTN and ISDN are two types of circuit-switching technology that may be used to implement a WAN in an enterprise setting.

Packet Switching

In contrast to circuit switching, packet switching splits traffic data into packets that are routed over a shared network. Packet-switching networks do not require a circuit to be established, and they allow many pairs of nodes to communicate over the same channel.

The switches in a packet-switched network determine which link the packet must be sent on next from the addressing information in each packet. There are two approaches to this link determination:

- **Connectionless** systems, such as the Internet, carry full addressing information in each packet. Each switch must evaluate the address to determine where to send the packet.

- **Connection-oriented** systems predetermine a packet’s route, and each packet only has to carry an identifier. In the case of Frame Relay, these are called *Data Link Connection Identifiers (DLCI)*. The switch determines the onward route by looking up the identifier in tables held in memory. The set of entries in the tables identifies a particular route or circuit through the system. If this circuit exists only while a packet travels through it, it is called a *virtual circuit (VC)*. A virtual circuit is a logical circuit between two network devices to help ensure reliable communications.

Because the internal links between the switches are shared between many users, the costs of packet switching are lower than those of circuit switching. Delays (latency) and variability of delay (jitter) are greater in packet-switched networks than in circuit-switched networks. This is because the links are shared, and packets must be entirely received at one switch before moving to the next. Despite the latency and jitter inherent in shared networks, modern technology allows satisfactory transport of voice and even video communications on these networks.

In Figure 1-19, Server A is sending data to Server B. Packets may not necessarily always take the same path to reach the destination. Each packet may take different routes to reach Server B.
Packet-switched networks may establish routes through the switches for particular end-to-end connections. These routes are called virtual circuits (VC). A VC is a logical circuit created within a shared network between two network devices. Two types of VCs exist:

- **Permanent virtual circuit (PVC):** A permanently established virtual circuit that consists of one mode: data transfer. PVCs are used in situations in which data transfer between devices is constant. PVCs decrease the bandwidth use associated with establishing and terminating VCs, but they increase costs because of constant virtual circuit availability. PVCs generally are configured by the service provider when an order is placed for service.

- **Switched virtual circuit (SVC):** A VC that is dynamically established on demand and terminated when transmission is complete. Communication over an SVC consists of three phases: circuit establishment, data transfer, and circuit termination. The establishment phase involves creating the VC between the source and destination devices, with SVC entries stored in lookup tables held in memory. Data transfer involves transmitting data between the devices over the VC, and the circuit termination phase involves tearing down the VC between the source and destination devices. SVCs are used in situations in which data transmission between devices is intermittent, largely to save costs. SVCs release the circuit when transmission is complete, which results in less expensive connection charges than those incurred by PVCs, which maintain constant virtual circuit availability.
Connecting to a Packet-Switched Network

To connect to a packet-switched network, a subscriber needs a local loop to the nearest location where the provider makes the service available. This is called the service’s point of presence (POP). Normally this is a dedicated leased line. This line is much shorter than a leased line connected directly between the subscriber locations. In addition, this one line to the POP can carry several VCs, allowing it to provide connections to multiple destinations. Because it is likely that not all the VCs require maximum demand simultaneously, the capacity of the leased line can be smaller than the sum of the individual VCs. Examples of packet- or cell-switched connections include:

- X.25
- Frame Relay
- ATM

WAN Connection Options

This section covers various WAN connection options, including private dedicated links, private switched links, and public connection options using the Internet.

WAN Link Connection Options

Many options for implementing WAN solutions are currently available. They differ in technology, speed, and cost. Familiarity with these technologies is an important part of network design and evaluation:

Figure 1-20 provides a high-level view of the various WAN link connection options:

- **Private WAN connection options**: Private WAN connections include both dedicated and switched communication link options:
  - **Dedicated communication links**: When permanent dedicated connections are required, point-to-point lines are used with various capacities that are limited only by the underlying physical facilities and the willingness of users to pay for these dedicated lines. A point-to-point link provides a preestablished WAN communications path from the customer premises through the provider network to a remote destination. Point-to-point lines usually are leased from a carrier and are also called leased lines.
Switched communication links: Switched communication links can be either circuit-switched or packet-switched:

Circuit-switched communication links: Circuit switching dynamically establishes a dedicated connection for voice or data between a sender and a receiver. Before communication can start, it is necessary to establish the connection through the service provider’s network. Examples of circuit-switched communication links are analog dialup (PSTN) and ISDN.

Packet-switched communication links: Many WAN users do not make efficient use of the fixed bandwidth that is available with dedicated, switched, or permanent circuits, because the data flow fluctuates. Communications providers have data networks available to more appropriately service these users. In packet-switched networks, the data is transmitted in labeled frames, cells, or packets. Packet-switched communication links include Frame Relay, ATM, X.25, and Metro Ethernet.

Public WAN connection options: Public connections use the global Internet infrastructure. Until recently, the Internet was not a viable networking option for many businesses because of the significant security risks and lack of adequate performance guarantees in an end-to-end Internet connection. With the development of VPN technology, however, the Internet is now an inexpensive and secure option for connecting to teleworkers and remote offices where performance guarantees are not critical. Internet WAN connection links are through broadband services such as DSL, cable modem, and broadband wireless, and they are combined with VPN technology to provide privacy across the Internet.

Figure 1-20 WAN Link Connection Options
Dedicated Connection Link Options

When permanent dedicated connections are required, a point-to-point link is used to provide a preestablished WAN communications path from the customer premises through the provider network to a remote destination.

Point-to-point lines usually are leased from a carrier and are called leased lines. Figure 1-21 shows a T3 and E3 circuit. This section describes how enterprises use leased lines to provide a dedicated WAN connection.

Figure 1-21  Leased Lines

Leased lines are available in different capacities. They generally are priced based on the bandwidth required and the distance between the two connected points.

Table 1-1 lists the available leased-line types and their bit-rate capacities.

Table 1-1  Leased-Line Types and Capacities

<table>
<thead>
<tr>
<th>Line Type</th>
<th>Bit Rate Capacity</th>
<th>Line Type</th>
<th>Bit Rate Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>56</td>
<td>56 kbps</td>
<td>OC-9</td>
<td>466.56 Mbps</td>
</tr>
<tr>
<td>64</td>
<td>64 kbps</td>
<td>OC-12</td>
<td>622.08 Mbps</td>
</tr>
<tr>
<td>T1</td>
<td>1.544 Mbps</td>
<td>OC-18</td>
<td>933.12 Mbps</td>
</tr>
<tr>
<td>E1</td>
<td>2.048 Mbps</td>
<td>OC-24</td>
<td>1244.16 Mbps</td>
</tr>
<tr>
<td>J1</td>
<td>2.048 Mbps</td>
<td>OC-36</td>
<td>1866.24 Mbps</td>
</tr>
<tr>
<td>E3</td>
<td>34.064 Mbps</td>
<td>OC-48</td>
<td>2488.32 Mbps</td>
</tr>
<tr>
<td>T3</td>
<td>44.736 Mbps</td>
<td>OC-96</td>
<td>4976.64 Mbps</td>
</tr>
<tr>
<td>OC-1</td>
<td>51.84 Mbps</td>
<td>OC-192</td>
<td>9953.28 Mbps</td>
</tr>
<tr>
<td>OC-3</td>
<td>155.54 Mbps</td>
<td>OC-768</td>
<td>39,813.12 Mbps</td>
</tr>
</tbody>
</table>
Point-to-point links usually are more expensive than shared services such as Frame Relay. The cost of leased-line solutions can become significant when they are used to connect many sites over increasing distances. However, sometimes the benefits outweigh the cost of the leased line. The dedicated capacity removes latency and jitter between the endpoints. Constant availability is essential for some applications, such as VoIP and video over IP.

A router serial port is required for each leased-line connection. A CSU/DSU and the actual circuit from the service provider are also required.

Leased lines provide permanent dedicated capacity and are used extensively to build WANs. They have been the traditional connection of choice but have a number of disadvantages. Leased lines have a fixed capacity; however, WAN traffic is often variable, leaving some of the capacity unused. In addition, each endpoint needs a separate physical interface on the router, which increases equipment costs. Any changes to the leased line generally require a site visit by the carrier.

**Circuit-Switched Connection Options**

Circuit-switched networks establish a dedicated connection for voice or data between a sender and a receiver. Before any communications can begin, it is necessary to establish the connection through the service provider’s network.

**Analog Dialup**

When intermittent, low-volume data transfers are needed, modems and analog dialed telephone lines provide low capacity and dedicated switched connections.

This section describes the pros and cons of using analog dialup connection options and describes the types of business scenarios that benefit most from this type of option. Figure 1-22 shows an analog dialup connection.

**Figure 1-22** WAN Built with an Intermittent Connection Using a Modem and the Voice Telephone Network

![Figure 1-22](image_url)
Traditional telephony uses a copper cable, called the local loop, to connect the telephone handset in the subscriber premises to the CO. The signal on the local loop during a call is a continuously varying electronic signal that is a translation of the subscriber analog voice signal.

Traditional local loops can transport binary computer data through the voice telephone network using a modem. The modem modulates the binary data into an analog signal at the source and demodulates the analog signal into binary data at the destination. The physical characteristics of the local loop and its connection to the PSTN limit the signal’s rate to less than 56 kbps.

For small businesses, these relatively low-speed dialup connections are adequate for the exchange of sales figures, prices, routine reports, and e-mail. Using automatic dialup at night or on weekends for large file transfers and data backup can take advantage of lower off-peak tariffs (line charges). Tariffs are based on the distance between the endpoints, time of day, and the call’s duration.

The advantages of modem and analog lines are simplicity, availability, and low implementation cost. The disadvantages are the low data rates and a relatively long connection time. The dedicated circuit has little delay or jitter for point-to-point traffic, but voice or video traffic does not operate adequately at these low bit rates.

Integrated Services Digital Network

Integrated Services Digital Network (ISDN) is a circuit-switching technology that enables the local loop of a PSTN to carry digital signals, resulting in higher-capacity switched connections. ISDN changes the internal connections of the PSTN from carrying analog signals to time-division multiplexed (TDM) digital signals. TDM allows two or more signals or bit streams to be transferred as subchannels in one communication channel. The signals appear to transfer simultaneously, but physically they take turns on the channel. A data block of subchannel 1 is transmitted during time slot 1, subchannel 2 during time slot 2, and so on. One TDM frame consists of one time slot per subchannel. TDM is described in more detail in Chapter 2, “PPP.”

ISDN turns the local loop into a TDM digital connection. This change enables the local loop to carry digital signals that result in higher-capacity switched connections. The connection uses 64-kbps bearer (B) channels to carry voice or data and a signaling, delta channel for call setup and other purposes.

There are two types of ISDN interfaces:

- **Basic Rate Interface (BRI):** ISDN is intended for the home and small enterprise and provides two 64-kbps B channels and a 16-kbps D channel. The BRI D channel is designed for control and often is underused, because it has only two B channels to control. Therefore, some providers allow the D channel to carry data at low bit rates, such as X.25 connections at 9.6 kbps.
Primary Rate Interface (PRI): ISDN is also available for larger installations. PRI delivers 23 B channels with 64 kbps and one D channel with 64 kbps in North America, for a total bit rate of up to 1.544 Mbps. This includes some additional overhead for synchronization. In Europe, Australia, and other parts of the world, ISDN PRI provides 30 B channels and one D channel, for a total bit rate of up to 2.048 Mbps, including synchronization overhead. In North America, PRI corresponds to a T1 connection. The PRI rate of lines outside North America corresponds to an E1 or J1 connection.

Figure 1-23 illustrates the various differences between ISDN BRI and PRI lines.

For WAN links, which require low bandwidth, the BRI ISDN can provide an ideal connection mechanism. BRI has a call setup time that is less than a second, and the 64-kbps B channel provides greater capacity than an analog modem link. If greater capacity is required, a second B channel can be activated to provide a total of 128 kbps. Although this is inadequate for video, it permits several simultaneous voice conversations in addition to data traffic.

Another common application of ISDN is to provide additional capacity as needed on a leased-line connection. The leased line is sized to carry average traffic loads, and ISDN is added during peak demand periods. ISDN is also used as a backup if the leased line fails. ISDN tariffs are based on a per-B-channel basis and are similar to those of analog voice connections.
With PRI ISDN, multiple B channels can be connected between two endpoints. This allows for videoconferencing and high-bandwidth data connections with no latency or jitter. However, multiple connections can be very expensive over long distances.

**Note**

Although ISDN is still an important technology for telephone service provider networks, it is declining in popularity as an Internet connection option with the introduction of high-speed DSL and other broadband services. The “Consumer and Industry Perspectives” section at http://en.wikipedia.org/wiki/ISDN provides a good discussion of ISDN worldwide trends.

### Packet-Switched Connection Options

The most common packet-switching technologies used in today’s enterprise WANs include legacy X.25, Frame Relay, and ATM, as described in the following sections.

**X.25**

Figure 1-24 shows an X.25 network. X.25 is a legacy network-layer protocol that provides subscribers with a network address. Virtual circuits can be established through the network with call request packets to the target address. The resulting SVC is identified by a channel number. Data packets labeled with the channel number are delivered to the corresponding address. Multiple channels can be active on a single connection.

**Figure 1-24**  X.25 Network
Typical X.25 applications are point-of-sale card readers. These readers use X.25 in dialup mode to validate transactions on a central computer. For these applications, the low bandwidth and high latency are not a concern, and the low cost makes X.25 affordable.

X.25 link speeds vary from 2400 bps up to 2 Mbps. However, public networks usually are low-capacity, with speeds rarely exceeding 64 kbps.

X.25 networks are now in dramatic decline, being replaced by newer Layer 2 technologies such as Frame Relay, ATM, and ADSL. However, they are still in use in many portions of the developing world, which have limited access to newer technologies.

Frame Relay

Figure 1-25 shows a Frame Relay network. Although the network layout appears similar to X.25, Frame Relay differs from X.25 in several ways. Most importantly, it is a much simpler protocol, operating strictly at Layer 2, whereas X.25 additionally provides Layer 3 services. Frame Relay implements no error or flow control. The simplified handling of frames leads to reduced latency, and measures taken to avoid frame buildup at intermediate switches help reduce jitter. Frame Relay offers data rates up to 4 Mbps, with some providers offering even higher rates.

**Figure 1-25** Frame Relay Network
Frame Relay VCs are uniquely identified by a DLCI, which ensures bidirectional communication from one DTE device to another. Most Frame Relay connections are PVCs rather than SVCs.

Frame Relay provides permanent, shared, medium-bandwidth connectivity that carries both voice and data traffic. Frame Relay is ideal for connecting enterprise LANs. The router on the LAN needs only a single interface, even when multiple VCs are used. The short-leased line to the Frame Relay network edge allows cost-effective connections between widely scattered LANs.

Frame Relay is described in more detail in Chapter 3.

**ATM**

Figure 1-26 shows an ATM network. Asynchronous Transfer Mode (ATM) technology can transfer voice, video, and data through private and public networks. It is built on a cell-based architecture rather than on a frame-based architecture. ATM cells are always a fixed length of 53 bytes. The ATM cell contains a 5-byte ATM header followed by 48 bytes of ATM payload. Small, fixed-length cells are well suited for carrying voice and video traffic, because this traffic is intolerant of delay. Video and voice traffic do not have to wait for a larger data packet to be transmitted.
The 53-byte ATM cell is less efficient than the bigger frames and packets of Frame Relay and X.25. Furthermore, the ATM cell has at least 5 bytes of overhead for each 48-byte payload. When the cell is carrying segmented network layer packets, the overhead is higher, because the ATM switch must be able to reassemble the packets at the destination. A typical ATM line needs almost 20 percent more bandwidth than Frame Relay to carry the same volume of network layer data.

ATM was designed to be extremely scalable. It can support link speeds of T1/E1 to OC-12 (622 Mbps) and higher.

ATM offers both PVCs and SVCs, although PVCs are more common with WANs. And as with other shared technologies, ATM allows multiple VCs on a single leased-line connection to the network edge.

**Internet Connection Options**

The Internet is an inexpensive and secure option for connecting to teleworkers and remote offices where performance guarantees are not critical.

Broadband connection options typically are used to connect telecommuting employees to a corporate site over the Internet. These options include DSL, cable, and wireless.

**DSL**

DSL technology, shown in Figure 1-27, is an always-on connection technology that uses existing twisted-pair telephone lines to transport high-bandwidth data and provides IP services to subscribers. A DSL modem converts an Ethernet signal from the user device into a DSL signal, which is transmitted to the central office.

*Figure 1-27  DSL*
Multiple DSL subscriber lines are multiplexed into a single high-capacity link using a DSL access multiplexer (DSLAM) at the provider location. DSLAMs incorporate TDM technology to aggregate many subscriber lines into a single medium, generally a T3 (DS3) connection. Current DSL technologies use sophisticated coding and modulation techniques to achieve data rates of up to 8.192 Mbps.

A wide variety of DSL types, standards, and emerging technologies exist. DSL is now a popular choice for enterprise IT departments to support home workers. Generally, a subscriber cannot choose to connect to an enterprise network directly. The subscriber must first connect to an ISP, and then an IP connection is made through the Internet to the enterprise. Security risks are incurred in this process, but they can be mediated with security measures.

Cable Modem

Coaxial cable is widely used in urban areas to distribute television signals. Network access is available from some cable television networks. This allows for greater bandwidth than the conventional telephone local loop.

Cable modems provide an always-on connection and a simple installation. Figure 1-28 shows how a subscriber connects a computer or LAN router to the cable modem, which translates the digital signals into the broadband frequencies used for transmitting on a cable television network. The local cable TV office, which is called the cable headend, contains the computer system and databases needed to provide Internet access. The most important component located at the headend is the cable modem termination system (CMTS). It sends and receives digital cable modem signals on a cable network and is necessary for providing Internet services to cable subscribers.

Figure 1-28  Cable Modem
Cable modem subscribers must use the ISP associated with the service provider. All the local subscribers share the same cable bandwidth. As more users join the service, available bandwidth may be below the expected rate.

**Broadband Wireless**

Wireless technology uses the unlicensed radio spectrum to send and receive data. The unlicensed spectrum is accessible to anyone who has a wireless router and wireless technology in the device he or she is using.

Until recently, one limitation of wireless access has been the need to be within the local transmission range (typically less than 100 feet) of a wireless router or a wireless modem that has a wired connection to the Internet. The following new developments in broadband wireless technology are changing this situation:

- **Municipal Wi-Fi**: Many cities have begun setting up municipal wireless networks. Some of these networks provide high-speed Internet access for free or for substantially less than the price of other broadband services. Others are for city use only, allowing police and fire departments and other city employees to do certain aspects of their jobs remotely. To connect to a municipal Wi-Fi, a subscriber typically needs a wireless modem, which provides a stronger radio and directional antenna than conventional wireless adapters. Most service providers provide the necessary equipment for free or for a fee, much like they do with DSL or cable modems.

- **WiMAX**: Worldwide Interoperability for Microwave Access (WiMAX) is a new technology that is just beginning to come into use. It is described in IEEE standard 802.16. WiMAX provides high-speed broadband service with wireless access and provides broad coverage like a cell phone network rather than through small Wi-Fi hotspots. WiMAX operates in a similar way to Wi-Fi, but at higher speeds, over greater distances, and for a greater number of users. It uses a network of WiMAX towers that are similar to cell phone towers, as shown in Figure 1-29. To access a WiMAX network, subscribers must subscribe to an ISP that has a WiMAX tower within 10 miles of their location. They also need a WiMAX-enabled computer and a special encryption code to get access to the base station.

- **Satellite Internet**: This is typically used by rural users where cable and DSL are unavailable. A satellite dish provides two-way (upload and download) data communications. The upload speed is about one-tenth of the 500-kbps download speed. Cable and DSL have higher download speeds, but satellite systems are about ten times faster than an analog modem. To access satellite Internet services, subscribers need a satellite dish, two modems (uplink and downlink), and coaxial cables between the dish and the modem.
DSL, cable, and wireless broadband services are described in more detail in Chapter 6, “Teleworker Services.”

**VPN Technology**

Security risks are incurred when a teleworker or remote office uses broadband services to access the corporate WAN over the Internet. To address security concerns, broadband services provide capabilities for using Virtual Private Network (VPN) connections to a VPN server, which typically is located at the corporate site.

A VPN is an encrypted connection between private networks over a public network such as the Internet. Instead of using a dedicated Layer 2 connection such as a leased line, a VPN uses virtual connections called VPN tunnels, which are routed through the Internet from the company’s private network to the remote site or employee host.

**VPN Benefits**

Benefits of VPN include the following:

- **Cost savings**: VPNs enable organizations to use the global Internet to connect remote offices and remote users to the main corporate site, thus eliminating expensive dedicated WAN links and modem banks.
- **Security**: VPNs provide the highest level of security by using advanced encryption and authentication protocols that protect data from unauthorized access.
Scalability: Because VPNs use the Internet infrastructure within ISPs and devices, it is easy to add new users. Corporations can add large amounts of capacity without adding significant infrastructure.

Compatibility with broadband technology: VPN technology is supported by broadband service providers such as DSL and cable, so mobile workers and telecommuters can take advantage of their home high-speed Internet service to access their corporate networks. Business-grade, high-speed broadband connections can also provide a cost-effective solution for connecting remote offices.

Types of VPN Access

Two types of VPN access exist:

Site-to-site VPNs: Site-to-site VPNs connect entire networks to each other. For example, they can connect a branch office network to a company headquarters network, as shown in Figure 1-30. Each site is equipped with a VPN gateway, such as a router, firewall, VPN concentrator, or security appliance. In the figure, a remote branch office uses a site-to-site VPN to connect with the corporate head office.

Remote-access VPNs: Remote-access VPNs enable individual hosts, such as telecommuters, mobile users, and extranet consumers, to access a company network securely over the Internet, as shown in Figure 1-31. Each host typically has VPN client software loaded or uses a web-based client.

Figure 1-30 Site-to-Site VPNs
Metro Ethernet

Metro Ethernet is a rapidly maturing networking technology that broadens Ethernet to the public networks run by telecommunications companies. IP-aware Ethernet switches enable service providers to offer enterprises converged voice, data, and video services such as IP telephony, video streaming, imaging, and data storage. Figure 1-32 shows that by extending Ethernet to the metropolitan area, companies can provide their remote offices with reliable access to applications and data on the corporate headquarters LAN.

Here are some benefits of Metro Ethernet:

- **Reduced expenses and administration**: Metro Ethernet provides a switched, high-bandwidth Layer 2 network that can manage data, voice, and video all on the same infrastructure. This characteristic increases bandwidth and eliminates expensive conversions to ATM and Frame Relay. The technology enables businesses to inexpensively connect numerous sites in a metropolitan area to each other and to the Internet.

- **Easy integration with existing networks**: Metro Ethernet connects easily to existing Ethernet LANs, reducing installation costs and time.

- **Enhanced business productivity**: Metro Ethernet enables businesses to take advantage of productivity-enhancing IP applications that are difficult to implement on TDM or Frame Relay networks, such as hosted IP communications, VoIP, and streaming and broadcast video.
Choosing a WAN Link Connection

Now that you have looked at the variety of WAN connection options, how do you choose the best technology to meet the requirements of a specific business? Table 1-2 compares the advantages and disadvantages of the WAN connection options that we have discussed in this chapter.
Table 1-2  Choosing a WAN Link Connection

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Advantages</th>
<th>Disadvantages</th>
<th>Sample Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leased line</td>
<td>Point-to-point connection between two computers’ LANs.</td>
<td>Most secure</td>
<td>Expensive</td>
<td>PPP, HDLC, SDLC</td>
</tr>
<tr>
<td>Circuit switching</td>
<td>A dedicated circuit path is created between endpoints. Best example is dialup connections.</td>
<td>Less expensive</td>
<td>Call setup</td>
<td>PPP, ISDN</td>
</tr>
<tr>
<td>Packet switching</td>
<td>Devices transport packets via a shared single point-to-point or point-to-multipoint link across a carrier inter network. Variable-length packets are transmitted over PVCs or SVCs.</td>
<td>Highly efficient use of bandwidth</td>
<td>Shared media across link</td>
<td>X.25, Frame Relay</td>
</tr>
<tr>
<td>Cell relay</td>
<td>Similar to packet switching, but uses fixed-length cells instead of variable-length packets. Data is divided into fixed-length cells and then transported across virtual circuits.</td>
<td>Best for simultaneous use of voice and data</td>
<td>Overhead can be considerable</td>
<td>ATM</td>
</tr>
<tr>
<td>Internet</td>
<td>Connectionless packet switching using the Internet as the WAN infrastructure. Uses network addressing to deliver packets. Because of security issues, VPN technology must be used.</td>
<td>Least expensive, globally available</td>
<td>Least secure</td>
<td>VPN, DSL, cable modem, wireless</td>
</tr>
</tbody>
</table>

This information is a good start. In addition, to help you in the decision-making process, the following sections list some questions to ask yourself when choosing a WAN connection option.
What Is the Purpose of the WAN?

Do you want to connect local branches in the same city area, connect remote branches, connect to a single branch, connect to customers, connect to business partners, or some combination of these? If the WAN is for providing authorized customers or business partners limited access to the company intranet, what is the best option?

What Is the Geographic Scope?

Is it local, regional, global, one-to-one (single branch), one-to-many branches, many-to-many (distributed)? Depending on the range, some WAN connection options may be better than others.

What Are the Traffic Requirements?

Traffic requirements to consider include the following:

- Traffic type (data only, VoIP, video, large files, streaming files) determines the quality and performance requirements. For example, if you are sending a lot of voice or streaming video traffic, ATM may be the best choice.

- Traffic volumes depending on type (voice, video, or data) for each destination determine the bandwidth capacity required for the WAN connection to the ISP.

- Quality requirements may limit your choices. If your traffic is highly sensitive to latency and jitter, you can eliminate any WAN connection options that cannot provide the required quality.

- Security requirements (data integrity, confidentiality, and security) are an important factor if the traffic is of a highly confidential nature or if provides essential services, such as emergency response.

Should the WAN Use a Private or Public Infrastructure?

A private infrastructure offers the best security and confidentiality, whereas the public Internet infrastructure offers the most flexibility and lowest ongoing expense. Your choice depends on the purpose of the WAN, the types of traffic it carries, and the available operating budget. For example, if the purpose is to provide a nearby branch with high-speed secure services, a private dedicated or switched connection may be best. If the purpose is to connect many remote offices, a public WAN using the Internet may be the best choice. For distributed operations, a combination of options may be the best solution.

For a Private WAN, Should It Be Dedicated or Switched?

Real-time, high-volume transactions have special requirements that could favor a dedicated line, such as traffic flowing between the data center and the corporate head office. If you are connecting to a local single branch, you could use a dedicated leased line. However, that
option would become very expensive for a WAN connecting multiple offices. In that case, a switched connection might be better.

**For a Public WAN, What Type of VPN Access Do You Need?**

If the purpose of the WAN is to connect a remote office, a site-to-site VPN may be the best choice. To connect teleworkers or customers, remote-access VPNs are a better option. If the WAN is serving a mixture of remote offices, teleworkers, and authorized customers, such as a global company with distributed operations, a combination of VPN options may be required.

**Which Connection Options Are Available Locally?**

In some areas, not all WAN connection options are available. In this case, your selection process is simplified, although the resulting WAN may provide less-than-optimal performance. For example, in a rural or remote area, the only option may be broadband satellite Internet access.

**What Is the Cost of the Available Connection Options?**

Depending on the option you choose, the WAN can be a significant ongoing expense. The cost of a particular option must be weighed against how well it meets your other requirements. For example, a dedicated leased line is the most expensive option, but the expense may be justified if it is critical to ensure secure transmission of high volumes of real-time data. For less-demanding applications, a cheaper switched or Internet connection option may be more suitable. Also, wireless point-to-point bridges are becoming a potential alternative to leased lines.

As you can see, you must consider many important factors when choosing an appropriate WAN connection. Following the guidelines just described, as well as those described by the Cisco Enterprise Architecture, you should now be able to choose an appropriate WAN connection to meet the requirements of different business scenarios.
Summary

A WAN is a data communications network that operates beyond the geographic scope of a LAN.

As companies grow, adding more employees, opening branch offices, and expanding into global markets, their requirements for integrated services change. These business requirements drive companies' network requirements.

The Cisco Enterprise Architecture expands on the Hierarchical Network Model by further dividing the enterprise network into physical, logical, and functional areas.

Implementing a Cisco Enterprise Architecture provides a secure, robust network with high availability that facilitates the deployment of converged networks.

WANs operate in relation to the OSI reference model, primarily on Layers 1 and 2.

Devices that put data on the local loop are called data circuit-terminating equipment or data communications equipment (DCE). The customer devices that pass the data to the DCE are called data terminal equipment (DTE). The DCE primarily provides an interface for the DTE into the communication link on the WAN cloud.

The physical demarcation point is the place where the responsibility for the connection changes from the enterprise to the service provider.

Data link layer protocols define how data is encapsulated for transmission to remote sites and the mechanisms for transferring the resulting frames.

A circuit-switching network establishes a dedicated circuit (or channel) between nodes and terminals before the users may communicate.

A packet-switching network splits traffic data into packets that are routed over a shared network. Packet-switching networks do not require a circuit to be established and allow many pairs of nodes to communicate over the same channel.

A point-to-point link provides a preestablished WAN communications path from the customer premises through the provider network to a remote destination. Point-to-point links use leased lines to provide a dedicated connection.

Circuit-switching WAN options include analog dialup and ISDN. Packet-switching WAN options include X.25, Frame Relay, and ATM. ATM transmits data in 53-byte cells rather than frames. ATM is best suited to video traffic.

Internet WAN connection options include broadband services, such as DSL, cable modem or broadband wireless, and Metro Ethernet. VPN technology enables businesses to provide secure teleworker access through the Internet over broadband services.
Labs

The activities and labs available in the companion *Accessing the WAN, CCNA Exploration Labs and Study Guide* (ISBN 1-58713-212-5) provide hands-on practice with the following topic introduced in this chapter:

**Lab 1-1: Challenge Review (1.4.1)**

In this lab, you review basic routing and switching concepts. Try to do as much on your own as possible. Refer to previous material when you cannot proceed on your own.

**Note**

Configuring three separate routing protocols—RIP, OSPF, and EIGRP—to route the same network definitely is not a best practice. It should be considered a *worst* practice and is not something that would be done in a production network. It is done here so that you can review the major routing protocols before proceeding and see a dramatic illustration of the concept of administrative distance.

Many of the Hands-on Labs include Packet Tracer Companion Activities, where you can use Packet Tracer to complete a simulation of the lab. Look for this icon in *Accessing the WAN, CCNA Exploration Labs and Study Guide* for Hands-on Labs that have a Packet Tracer Companion.
Check Your Understanding

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. Answers are listed in Appendix, “Check Your Understanding and Challenge Questions Answer Key.”

1. Which of the following items are considered WAN devices? (Choose three.)
   A. Bridge
   B. Modem
   C. Router
   D. Ethernet switch
   E. Access server
   F. Repeater

2. Which layer of the hierarchical network design model is often called the backbone?
   A. Access
   B. Distribution
   C. Network
   D. Core
   E. Workgroup
   F. WAN

3. Match each term with its definition:
   - Circuit switching
   - Packet switching
   - Connection-oriented packet switching
   - Connectionless packet switching

   A. A switching technology in which each switch must evaluate the packet’s address to determine where to send it.
   B. A switching technology in which a virtual circuit exists only while a packet travels through it.
   C. A switching technology that establishes routes through the switches for particular end-to-end connections.
   D. A switching technology that has a preestablished dedicated circuit (or channel) between nodes and terminals.
4. Match each term with its packet-switched technology definition:

Metro Ethernet
X.25
ATM
Frame Relay

A. Provides a high-bandwidth Layer 2 network that can manage data, voice, and video all on the same infrastructure.
B. Built on a cell-based architecture in which the cell has a fixed length of 53 bytes.
C. Operates at the data link layer, and the PVC is identified by a Data Link Control Identifier.
D. Operates at the network layer, and the SVC is identified by a channel number.

5. Which device is commonly used as Data Terminal Equipment?

A. ISDN
B. Modem
C. Router
D. CSU/DSU

6. Which type of WAN connection should you choose when a dedicated point-to-point WAN communications path from the customer premises through the provider network to a remote destination is required?

A. ISDN
B. Analog dialup
C. ATM
D. Frame Relay
E. Leased line

7. How are Frame Relay virtual circuits identified?

A. CIR
B. DLCI
C. VPI
D. MAC
E. SPI
8. What WAN technology is designed to deliver data, voice, and video simultaneously built on a cell-based architecture?
   A. ATM
   B. Cable
   C. Frame Relay
   D. ISDN

9. Which architecture enables enterprises to offer important network services—such as security, new communication services, and improved application performance—to every office, regardless of its size or proximity to headquarters?
   A. Cisco Enterprise Campus Architecture
   B. Cisco Enterprise Data Center Architecture
   C. Cisco Enterprise Branch Architecture
   D. Cisco Enterprise Teleworker Architecture

10. At which layer of the hierarchical network model do users connect to the network?
    A. Application
    B. Access
    C. Distribution
    D. Network
    E. Core

11. ISDN PRI is composed of how many B channels in North America?
    A. 2
    B. 16
    C. 23
    D. 30
    E. 64

12. The ability to connect securely to a private network over a public network is provided by which WAN technology?
    A. DSL
    B. Frame Relay
    C. ISDN
    D. PSTN
    E. VPN
13. Which hierarchical network model layer is responsible for containing network problems to the workgroups in which they occur?
   A. Application
   B. Access
   C. Distribution
   D. Network
   E. Core

14. What term describes the cabling that connects the customer site to the nearest exchange of the WAN service provider?
   A. CPE
   B. CO
   C. Local loop
   D. DCE
   E. DTE

15. Which goal can be accomplished by implementing the Cisco Enterprise Teleworker Architecture?
   A. It allows the enterprise to add large branch sites that span geographic areas.
   B. It allows the enterprise to deliver secure voice and data services to workers no matter where or when they work.
   C. To reduce remote security threats, it forces users who are located at main sites to log on to resources.
   D. It satisfies telephony requirements for users who are located at medium to large enterprise sites.

16. Describe the three layers of the hierarchical network model.

17. Describe the five modules of the Cisco Enterprise Architecture.

18. Compare and contrast the following WAN terms: CPE, CO, local loop, DCE, DTE, and demarcation point.

19. Compare and contrast the following WAN devices: modem, CSU/DSU, access server, WAN switch, and router.

20. Compare and contrast X.25, Frame Relay, and ATM.
**Challenge Questions and Activities**

1. Explain the advantages and disadvantages of circuit-switched networks.
2. What are the differences between a site-to-site VPN and a remote-access VPN?
### Numerics

3DES, 411

### A

- access attacks, 208
- access rates, 162
- access servers, 21
- access-class command, 342-343
- access-list command, parameters, 329-330

#### ACLs, 310, 316-317

- applying to interfaces, 339-342
- creating, 327
- dynamic ACLs, 358-360
- extended ACLs, 322
- applying to interfaces, 353, 355
- configuring, 351-353
- packets, testing, 349
- placing, 325-326
  - port number lists, generating, 350-351
- functions performed by, 318
- implicit “deny” behavior, 322
- inbound, 319-320
- named ACLs, 324
  - creating, 345-346
  - editing, 347-348
- named extended ACLs, creating, 355-357
- numbered ACLs, 324
  - editing, 343-345
- outbound, 319-320
- placing, 324
- reflexive ACLs, 360, 363
- remarks, 331-332
- removing, 330-331
- router processing logic, 321
- standard, 322-323
  - configuring, 327-329
  - placing, 325
- time-based ACLs, 363-364
- troubleshooting, 365-367
- verifying, 346-347
- VTY access, controlling, 342-343
- wildcard masks, 332
  - bit keywords, 337-339
  - calculating, 336-337
  - IP subnets, matching, 334-337
- activity logging on routers, 249-250

#### address mapping

- Frame Relay
  - dynamic mapping, 145-146
  - Inverse ARP, 145
  - LMI, 150, 152
  - static mapping, 146
- static mapping, 156-158

#### addressing, IPv6, 493

- IPv6 global unicast address, 494
- loopback addresses, 496
- private addresses, 496
- reserved addresses, 496
- unspecified addresses, 497

#### ADSL (asynchronous DSL), 391-395

#### AES (Advanced Encryption Standard), 412

#### AH (Authentication Header), 416

#### analog dialup, 32-33

#### antenna site, 386

#### antivirus software, 220

#### any option (wildcard masking), 337, 339

#### APIPA (Automatic Private IP Addressing), 451

#### application layer, troubleshooting, 589-594

#### applications, security, 224

#### applying ACLs to interfaces, 339-342

- extended ACLs, 353-355

#### asymmetric encryption, 412-413

#### ATM (Asynchronous Transfer Mode), 37, 73, 567

#### attacks

- access attacks, 208
- DDoS, 214-217
- DoS, 212
- malicious code, 217-219
mitigation techniques
  antivirus software, 220
  device hardening, 220
  HIPS, 223
  IDS, 223
  IPS, 223
  operating system patches, 222-223
  personal firewalls, 221
MITM, 211
port redirection, 210
reconnaissance, 206-207
seven-step process, 193
social engineering, 205
trust exploitation, 209-210
types of, 193-194
authentication, 415
  PPP, 112
    CHAP, 110
    configuring, 115-118
    PAP, 109-110
    troubleshooting, 118-119
AutoSecure, implementing on routers, 263-264
AUX ports, securing remote administration of routers, 243

B
backbone, 12
backing up software images, 284
bandwidth, 568–569
BE (excess burst), 165
BECN (Backward Explicit Congestion Notification), 141
BECN bit, 167
bit keywords for wildcard masks, 337-339
black hats, 192
BOOTP (Bootstrap Protocol), 435
  comparing with DHCP, 435-436
  bottom-up troubleshooting method, 545
branch networks, 8
  Enterprise Branch Architecture, 16
BRI (Basic Rate Interface), 33
broadband, 382
  wireless, 40, 396
    meshed municipal Wi-Fi network, 397
    satellite Internet, 399
  single wireless router deployment, 397
  standards, 400
  WiMAX, 398
brute force attacks, 208
business networks, 5
  branch, 8
  campus, 6-7
  distributed, 9-10
  small office, 6
business requirements for teleworker services, 379
bursting, 164

C
cable, 385-386
  CMTS, 390-391
  DOCSIS, 388-389
  electromagnetic spectrum, 387
  headend, 386
cable analyzers, 557
cable modem, 39
cable taps, 386
cable testers, 556
calculating wildcard masks, 336-337
campus networks, 6-7
  Enterprise Campus Architecture, 15
carrier protocols, 409
CATV (community antenna television), 386
CBIR (committed burst information rate), 165
CDMA (code-division multiple access), 389
cells, 38
CHAP (Challenge Handshake Authentication Protocol), 110
  configuring, 115-118
CIR (committed information rate), 163
circuit-switched connections, 26, 32
  analog dialup, 32-33
  ISDN, 33-35
Cisco ASA (Adaptive Security Appliance), 225
Cisco Enterprise Architecture, 13-14
  Enterprise Branch Architecture, 16
  Enterprise Campus Architecture, 15
  Enterprise Data Center Architecture, 16
  Enterprise Edge Architecture, 15
  Enterprise Teleworker Architecture, 16
Cisco IOS dual stack, 500-502
Cisco IOS Software, 225
  configuration files, managing, 280
  enable passwords, protecting, 238
  file naming conventions, 282-283
  image management, 283-294
  lost passwords, recovering, 297-300
  security features, applying to routers, 235-250
  troubleshooting, 294-297
  username passwords, protecting, 239
Cisco IPS 4200 series sensors, 226
Cisco NAC appliance, 226
Cisco routers, configuring as DHCP server, 440-441
  clear frame-relay inarp command, 177
  clear ip nat translation command, 482
  clock skew, 57
closed networks, 194-197
CMTS (cable modem termination system), 390-391
CO (central office), 19
commands
  access-class, 342-343
  access-list, parameters, 329-330
  clear frame-relay inarp, 177
  clear ip nat translation, 482
d debug, 295-297
  debug frame-relay lmi, 178-179
d debug ip nat, 484
d debug ppp, 102
d debug ppp authentication, 118
d debug ppp error, 107-108
d debug ppp negotiation, 105-106
d debug ppp packet, 103-105
d dn-s-server, 441
d encapsulation hdlc, 76
d frame-relay interface dlci, 170
d interface serial, 169
d ip dhcp excluded-address, 440
d ip dhcp pool, 440
ip helper-address, 451
ip ppp authentication, 116
ip show, 294
ip show controllers, 81-82
ip show frame-relay lmi, 148, 174
show frame-relay map, 145, 158
show frame-relay pvc, 175-176
show interface, 507
show interfaces, 172
show interfaces serial, 76-81, 118, 155
show ip dhcp binding, 442
show ip dhcp conflict, 456
show ip dhcp server statistics, 443
show ip interface, 449
show ip nat statistics, 481
show ip nat translations, 480
show running-config, 343
troubleshooting-related, 295-297
d debug commands, 295-297
d show commands, 294
comments, adding to numbered ACLs, 344-345
cost effectiveness of Frame Relay and ISDN, 132
DHCP and BOOTP, 435-436
IPv6 and IPv4, 490-493
NAT and NAT overload, 468
complex ACLs
  dynamic ACLs, 358-360
  reflexive ACLs, 360-363
time-based ACLs, 363-364
compression (PPP), configuring, 99
counting (PPP), configuring, 99
counting files, managing, 285
counting
  ACLs
    extended ACLs, 351-353
data ACLs, 345-346
  named ACLs, 345-346
  standard, 327-329
  verifying configuration, 346-347
Cisco routers as DHCP server, 440-441
DHCP clients, 447-449
DHCP relay, 449-453
DHCP servers with SDM, 453-455
dynamic NAT, 471-473
Frame Relay, 152
d encapsulation type, 153-155
static mapping, 146
d static maps, 156-158
subinterfaces, 168-171
HDLC encapsulation, 75
IPv6, 506
  RIPng, 508-510
named extended ACLs, 355-357
D

DDoS attacks, 214-217
DE (Discard Eligible) bit, 141, 165-166
debug commands, 295-297
debug frame-relay lmi command, 178-179
debug ip nat command, 484
debug ppp authentication command, 118
debug ppp command, 102
debug ppp error command, 107-108
debug ppp negotiation command, 105-106
debug ppp packet command, 103-105
debugging DHCP, 459-460
decryption, 208
dedicated connection links, 31-32
dedicated lines, 130
demarc, 19, 66
DES (Data Encryption Standard), 411
designing WANs, 561-562
device hardening, 220
DH (Diffie-Hellman), 417
DHCP (Dynamic Host Configuration Protocol), 431-432
clients, configuring, 447, 449
comparing with BOOTP, 435-436
debugging, 459-460
disabling, 442
dynamic address assignment, 432, 435
Easy IP, 432
manual address assignment, 433
messages, 436-438
troubleshooting, 456-458
verifying configuration, 442-447
DHCP relay
configuring, 449-453
verifying configuration, 458
DHCP servers
Cisco routers, configuring, 440-441
configuring with SDM, 453-455
DHCPCPACK messages, 434
DHCPDISCOVER messages, 434, 438-440
DHCOFFER messages, 434, 438-440
DHCPREQUEST messages, 434
DHCPv6, 498
dictionary attacks, 208

data centers, Enterprise Data Center Architecture, 16
data link layer, 18, 23-24
capsulation, 24-25
troubleshooting, 578-580
Frame Relay, 581-583
PPP, 579-580
STP loops, 583-584
data plane (IPv6), 503-504
data streams, 62
DCE, 19

NAT overload, 473-475
  for multiple public IP addresses, 475-477
port forwarding, 477-479
PPP, 94-98
  authentication, 115-118
  compression, 99
  link quality monitoring, 99
  load balancing, 100
routers
  activity logging, 251-252
  network services, 252-264, 267
  security features, 236-241, 244-251
static NAT, 470-471
congestion notification mechanisms, Frame Relay, 166-167
connecting to packet-switched networks, 29
connection options, selecting, 44-47
control plane (IPv6), 503-504
controlling VTY access with ACLs, 342-343
core routers, 21
cost effectiveness of Frame Relay, 131
CPE (customer premises equipment), 19, 392
crackers, 192
creating
  ACLs, 327
  named ACLs, 345-346
  named extended ACLs, 355-357
CSA (Cisco Security Agent), 226
CSU/DSU, 20
CTS (Clear to Send) pin, 61
cycles per second, 388
disabling
  DHCP, 442
  router services, 253, 255
displaying Frame Relay traffic statistics, 175-176
distributed networks, 9-10, 386
divide and conquer troubleshooting method, 547
DLCI (data link connection identifiers), 27
  address mapping, 145-146
  local significance, 136
  verifying remote IP address-to-local translation, 177
DMM (digital multimeters), 556
DMZ (demilitarized zone), 210
DNS (Domain Name System), securing, 255
dns-server command, 441
DOCSIS (Data-over-Cable Service Interface Specification), 388
  Layer 2 requirements, 389
documenting the network, 526, 533-534
  end-system configuration table, 531-533
  network configuration table, 528-531
  network topology diagram, 527
DoS attacks, 212, 214
downstream RF signal transmission, 388
DS0, 64
DSL (digital subscriber line), 38, 391
  ADSL, 393, 395
  local loop, 392
DSLAM (DSL Access Multiplexer), 392
DSR (Data Set Ready), 61
DTE (Data Termination Equipment), 19
DTE-DCE (Data Termination Equipment-Data Communication Equipment), 22
  cable standard, 67, 70
  parallel-to-serial conversion, 71
DTR (Data Terminal Ready), 61
dual stacking, 499-502
dynamic 6to4 tunneling, 499
dynamic ACLs, 358-360
dynamic address mapping, 145-146
dynamic IP address assignment, 432, 435
dynamic NAT, 465
  configuring, 471-473

E
Easy IP, 432
editing
  named ACLs, 347-348
  numbered ACLs, 343
    comments, adding, 344-345
EIA standards, 17
EIGRP (Enhanced Interior Gateway Routing Protocol), securing, 261
electrical supply threats, mitigating, 203
electromagnetic spectrum, 387
enable passwords, protecting, 238
encapsulating protocols, 409
capsulation, 24-25
  Frame Relay, 140-141
encapsulation hdlc command, 76
capsulation type (Frame Relay), configuring, 153-155
cryption, 207, 410
  asymmetric, 413
  hashes, 414
  symmetric, 413
end-system configuration table, 531, 533
Enterprise Branch Architecture, 16
Enterprise Data Center Architecture, 16
Enterprise Edge Architecture, 15
Enterprise Teleworker Architecture, 16
environmental threats, mitigating, 203
ESP (Encapsulating Security Payload), 416
establishing
  network baseline, 535-541
  PPP link with LCP, 89-91
  PPP sessions, 88
EUI-64 interface ID assignment, 497
Euro-DOCSIS, 389
extended ACLs, 322
applying to interfaces, 353-355
configuring, 351-353
packets, testing, 349
placing, 325-326
port number lists, generating, 350-351
external threats, 204
F

FECN (Forward Explicit Congestion Notification), 141
FECN bit, 167
fields of DHCP messages, 436-438
flexibility of Frame Relay, 132
flow control, Frame Relay, 166-167
Frame Relay, 36, 73, 128, 567

  address mapping
    dynamic mapping, 145-146
    Inverse ARP, 145
    static mapping, 146
configuring, 152
cost effectiveness, 131
data link layer, 134
DLCIs
  local significance, 136
  verifying remote IP address-to-local translation, 177
encapsulation process, 140-141
encapsulation type, configuring, 153-155
flexibility of, 132
flow control, 166-167
interfaces, verifying configuration, 172
leased-line design, 130
LMI, 148-149
  address mapping, 150-152
  extensions, 149-150
  frame format, 150
  verifying statistics, 174
physical layer, 134
reachability issues, solving, 159
static maps, configuring, 156-158
subinterfaces, 161-162
  configuring, 168-171
topologies
  full-mesh topology, 143
  partial-mesh topology, 145
  star topology, 142
traffic statistics, displaying, 175-176
troubleshooting, 178-179, 581-583
VCs, 134, 137
  multiple VCs on single access line, 137-139
  versus X.25, 133
frame-relay interface-dlci command, 170
frames
  HDLC, 74-75
  PPP, 87

frequency, 388
full-mesh topology, 143, 564
functions performed by ACLs, 318

G-H

generating list of port numbers, 350-351
global networks, 9-10
GRE (Generic Route Encapsulation) packets, 409

hackers, 192
hardware threats, mitigating, 203
hardware troubleshooting tools, 555
hashes, 414
HDLC encapsulation, 72-73
  configuring, 75
  fields, 74-75
headend, 39, 386
header structure of IPv6, 492
HIDS (host-based intrusion detection system), 223
hierarchical network model, 11-12
hierarchical topology, 566
HIPS (host-based intrusion prevention system), 223
HMAC (hashed message authentication code), 415
host option (wildcard masking), 337, 339
HSSI (High-Speed Serial Interface), 60
hub-and-spoke topology, 142

I

IDS (intrusion detection system), 223
IEEE 802.11 standard, 400
IEEE 802.11b standard, 400
IEEE 802.11g standard, 400
IEEE 802.11n standard, 401
IFS (Cisco IOS Integrated File System), 276-280
implementation issues, 569
implicit “deny all” behavior (ACLs), 322
inbound ACLs, 319-320
inside networks, 463
interface serial command, 169
interfaces
   ACLs, applying, 339-342, 353-355
   Frame Relay, verifying configuration, 172
internal threats, 204
Internet connection options
   broadband wireless, 40
   cable modem, 39
   DSL, 38
   Metro Ethernet, 43
   VPN technology, 41
Inverse ARP, 145
   address mapping, 150-152
inverse masks, 333
ip dhcp excluded-address command, 440
ip dhcp ppol command, 440
ip helper-address command, 451
IP subnets, matching with wildcard masks, 334-337
IPS (intrusion prevention system), 223
IPsec, 416, 418
IPv6, 485, 489
   address management, 497
   addressing, 493
   IPv6 global unicast address, 494
   loopback addresses, 496
   private addresses, 496
   reserved addresses, 496
   unspecified addresses, 497
   comparing with IPv4, 490-493
   configuring, 506
   DHCPv6, 498
   dual stacking, 499
   enabling on router
       control plane operation, 504
       data plane operation, 504
   manual configuration, 502
   RIPng, 505
      configuring, 508-510
      troubleshooting, 510
   routing configurations, 503
   stateless autoconfiguration, 498
   transition mechanisms
       dual stacking, 500-502
       tunneling, 499, 502
ISATAP (Intrasite Automatic Tunnel Addressing Protocol), 500
ISDN, 33-35, 63
   cost effectiveness versus Frame Relay, 132
ISO standards, 17
ISO/IEC 27002, 198
isolating physical layer problems, 576
ISPs
   oversubscription, 163
   WANs, troubleshooting, 570

J-K-L
jabber, 574
LAPB (Link Access Procedure, Balanced), 73
LAPF (Link Access Procedure for Frame Relay), 140
Layer 2 DOCSIS requirements, 389
Layer 2 WAN protocols, 73
layered models
   OSI reference model, 542
   TCP/IP model, 543
layered PPP architecture
   LCP, 85
   NCP, 86
LCP (Link Control Protocol), 85
   establishing link with PPP, 89-91
   packets, 92
lease command, 441
leased lines, 29-32
link connection options, 29-30
   choosing, 44-47
   circuit-switched connections, 32-35
   dedicated connection links, 31-32
   packet-switched connections, 35-37
link quality monitoring, configuring PPP, 99
link-local addresses (IPv6), 496
LMI (Local Management Interface), 148-149
   address mapping, 150-152
   extensions, 149-150
   frame format, 150
   statistics, verifying, 174
load balancing (PPP), configuring, 100
local loop, 19, 392
local significance of DLCIs, 136
lock-and-key ACLs, 358-360
logical network diagrams, 571-572
logical topologies, 571
loopback addresses (IPv6), 496
LOphtCrack, 208
lost passwords, recovering, 297, 299-300

M
MAC layer DOCSIS requirements, 389
maintenance threats, mitigating, 204
malicious code attacks, 217-219
MAN (metropolitan area network), 15
manual interface ID assignment, 497
manual IP address allocation, 432
manual IP address assignment, 433
manual IPv6-over-IPv4 tunneling, 499
MD5, 415
measuring performance data, 538-541
meshed municipal Wi-Fi networks, 397
messages, DHCP, 436-440
Metro Ethernet, 43
microfilters, 393
mitigating security threats
antivirus software, 220
device hardening, 220
HIPS, 223
IDS, 223
IPS, 223
Network Security Wheel, 226, 228
operating system patches, 223-224
personal firewalls, 221
MITM attacks, 211
Mitnick, Kevin, 204
modems, 20
monitoring ACLs, 346-347
MPLS (Multi-Protocol Label Switching), 24
Multilink PPP, configuring, 100
multiple LAN networks, 6-7
multipoint subinterfaces, 161
Municipal Wi-Fi, 40
MUX (multiplexer), 62

N
NAM (network analysis module), 555
named ACLs, 324
creating, 345-346
editing, 347-348
named extended ACLs, creating, 355-357
NAT (Network Address Translation), 431, 460-462
benefits of, 468-470
comparing with NAT overloading, 468
dynamic NAT, 465
configuring, 471-473
inside networks, 463
outside networks, 464
static NAT, 465
configuring, 470-471
troubleshooting, 483-485, 589-590
verifying configuration, 479, 483
NAT overload, 466-467
comparing with NAT, 468
configuring, 473-475
for multiple public IP addresses, 475-477
troubleshooting, 488-489
verifying configuration, 479, 483
NAT-PT (NAT-Protocol Translation), 500
NCP (Network Control Protocol), 86, 95
need for WANs, 5
networks, documenting, 526-534
network baseline, establishing, 535-541
network configuration table, 528-531
network diagrams, logical, 571-572
network layer, troubleshooting, 585-586
network security, routers, 232-235
activity logging, 249-250
AutoSecure, implementing, 263-264
Cisco IOS security features, applying, 235-248
network services, securing, 250-258, 260-263
SDM, implementing, 264, 266-267, 270, 272
software images maintenance, 275-280, 282-294
Network Security Wheel, 226, 228
network topology diagram, 527
NID (network interface device), 393
NMS tools, 551
North American IPv6 Task Force, 489
NTP (Network Time Protocol), securing, 255
null modem, 68
numbered ACLs, 324
  configuring, 329
  editing, 343
    comments, adding, 344-345

one-way satellite Internet systems, 399
open networks, 194, 197
operating system patches, 222-223
OSI model, 542
  data link layer protocols, 23-24
    encapsulation, 24-25
  physical layer, 18
    DTE/DCE interface, 22
OSPF (Open Shortest Path First), securing, 262, 263
OTDRs (optical time-domain reflectometers), 556
outbound ACLs, 319-320
outside networks, 464
oversubscription, 163

packet filtering, 313, 316. See also ACLs
packet-switched networks, 27
  ATM, 37
  connecting to, 29
  Frame Relay, 36
  VCs, 28
  X.25, 35
packets
  Frame Relay, encapsulation process, 140-141
  LCP, 92
  testing with extended ACLs, 349
PAP (Password Authentication Protocol), 109-110
  configuring, 115-118
  troubleshooting, 118-119
  authentication process, 112, 115
  authentication protocols
    CHAP, 110
    PAP, 109-110
  compression, configuring, 99
  configuring, 94-98
  frames, 87
  LCP, 85
    packets, 92
    link establishment, 89-91
  link quality monitoring, configuring, 99
  load balancing, configuring, 100
  NCP, 86, 95
  passwords, 236-237
    minimum length, 240
    recovering, 297, 299-300
  payload-only encryption, 208
  performance, measuring, 538-541
  personal firewalls, 221
  phishing, 192, 205
  phreakers, 192
  physical layer, 18
    DTE/DCE interface, 22
    troubleshooting, 574-577
  physical layer protocols, 18
  physical threats to security, 202, 204
  physical topologies, 571
  ping-of-death attacks, 213
  placing ACLs, 324
    extended ACLs, 325-326
    standard ACLs, 325
  point-to-point subinterfaces, 161
  POP (point of presence), 21
  port forwarding, configuring, 477-479
  port numbers, 311
    generating, 350-351
  port redirection, 210
  port speed, 162
  portable network analyzers, 558
  POTS, 391
  PPP (Point-to-Point Protocol), 56, 73, 83
    authentication
      configuring, 115-118
      troubleshooting, 118-119
    authentication process, 112, 115
    authentication protocols
      CHAP, 110
      PAP, 109-110
    compression, configuring, 99
    configuring, 94-98
    frames, 87
    LCP, 85
      packets, 92
      link establishment, 89-91
    link quality monitoring, configuring, 99
    load balancing, configuring, 100
    NCP, 86, 95
serial encapsulation
  troubleshooting, 102-108
verifying, 101-102
session establishment, 88
troubleshooting, 579-580
ppp authentication command, 116
PRI (primary rate interface), 34
private addresses (IPv6), 496
private IP addresses, 461
PSK (preshared key), 415
PVCs, 28, 135, 163
displaying statistics, 175-176

Q-R

QoS, 383

rainbow tables, 208
reachability, extending on Frame Relay networks, 159
reconnaissance attacks, 206-207
recovering lost passwords, 297, 299-300
reflexive ACLs, 360, 363
remarks, adding to ACLs, 331-332
  numbered ACLs, 344-345
remote access VPNs, 406
remote administration of routers, securing, 241, 243-248
remote connection options for teleworker services, 380
remote-access VPNs, 42
removing ACLs, 330-331
required telecommuting components, 383-384
required VPN components, 407
researching troubleshooting methods, 558
reserved addresses (IPv6), 496
restoring software images, 288, 290-292, 294
RIPng, 505
  configuring, 508-510
troubleshooting, 510
RIPv2, securing, 258, 260
RS-232, 59
RSA (Rivest, Shamir, and Adleman), 412, 415

S

S-CDMA (synchronous code-division multiple access), 389
SANS Institute, 230
satellite Internet, 40, 399
SDM (Cisco Router and Security Device Manager)
  DHCP servers, configuring, 453-455
  implementing on routers, 264, 266-267, 270, 272, 274
SDSL (synchronous DSL), 392
security
  attacks
    access attacks, 208
    DDoS, 214, 217
    DoS, 212
    malicious code attacks, 217-219
    mitigating, 220-223
    MITM, 211
    port redirection, 210
    reconnaissance attacks, 206-207
    seven-step process, 193
    trust exploitation, 209-210
types of, 193-194
closed networks, 19, 197
importance of, 191
Network Security Wheel, 226, 228
of VPNs, 408
open networks, 194, 197
demarc, 66
physical threats, 202, 204
social engineering, 205
vulnerabilities, 199
configuration weaknesses, 201
technological weaknesses, 200
security policies, 229
components of, 230-231
creating, 197, 199
functions of, 229
selecting troubleshooting technique, 547
selecting WAN link connections, 44-47
serial communication, 56-58
demarc, 66
DTE-DCE, 67
cable standards, 67, 70
parallel-to-serial conversion, 71
HDLC encapsulation, 72-73
configuring, 75
frame fields, 74-75
standards, 59-60
TDM, 61
DS0, 64
ISDN, 63
SONET, 64
STDM, 63
serial interfaces, troubleshooting, 76-82
serial PPP encapsulation
troubleshooting, 102-108
verifying, 101-102
SHA-1 (Secure Hash Algorithm 1), 415
shared networks, 567
show commands, 294
show controllers command, 81-82
show frame-relay lmi command, 148, 174
show frame-relay map command, 145, 158
show frame-relay pvc command, 175-176
show interface command, 507
show interfaces command, 172
show interfaces serial command, 76-81, 118, 155
show ip dhcp binding command, 442
show ip dhcp conflict command, 456
show ip dhcp server statistics command, 443
show ip interface command, 449
show ip nat translations command, 480
show running-config command, 343
single LAN networks, 6
site-local addresses (IPv6), 496
site-to-site VPNs, 42, 405
SLD (Synchronous Data Link Control), 73
SLIP (Serial Line Internet Protocol), 73
small office networks, 6
Smurf attacks, 214
SNMP (Simple Network Management Protocol), securing, 255
social engineering, 205
software image maintenance, 27-283
on Cisco IOS Software, 283-294
software troubleshooting tools
knowledge bases, 552
NMS tools, 551
SONET, 64
spammers, 192
split horizon, solving Frame Relay reachability issues, 159
splitters, 393
SSH (Secure Shell), securing remote administration of routers, 243, 245-248
standard ACLs, 322-323
configuring, 327-329
placing, 325
standards
for serial communication, 59-60
for wireless broadband, 400
star topology, 142, 564
stateless autoconfiguration (IPv6), 498
static address mapping, 146
static maps, configuring Frame Relay, 156-158
static NAT, 465
configuring, 470-471
STDM (statistical time division multiplexing), 63
STM (Spanning Tree Protocol) loops, troubleshooting, 583-584
structured threats, 204
subinterfaces
configuring, 168-171
Frame Relay, 161-162
subscriber drop, 387
SVCs (switched virtual circuits), 28
switches, 21
symmetric encryption, 412-413
symptoms
  of application layer problems, 591
  of data link layer problems, 577
  gathering for troubleshooting process, 548-551
  of physical layer problems, 574
SYN flood attacks, 213
systematic troubleshooting approach, 541

TCP, 310-311
TCP/IP model, 543
TDM (time-division multiplexing), 26, 33, 61
  DS0, 64
  ISDN, 63
  SONET, 64
  STDMA, 63
TDMA (time-division multiple access), 389
teleworker services
  business requirements, 379
  Enterprise Teleworker Architecture, 16
  remote connection options, 380
  required components, 383-384
VPNs, 402
  asymmetric encryption, 413
  authentication, 415
  benefits of, 404
  encryption, 410
  hashes, 414
  IPsec, 416-418
  island analogy, 403
  remote access, 406
  required components, 407
  security, characteristics, 408
  site-to-site, 405
  symmetric encryption, 413
  tunneling, 409
WAN connection options, 384
  broadband wireless, 396-400
  cable, 385-391
  DSL, 391-395
Teredo tunneling, 500
testing packets with extended ACLs, 349
threat control, 224
TIA standards, 17
time-based ACLs, 363-364
top-down troubleshooting method, 546
topologies, 564-567
  full-mesh topology, 143
  partial-mesh topology, 145
  star topology, 142
traffic, 562, 564
transceivers, 392
transport layer
  NAT, troubleshooting, 588-589
  troubleshooting, 586-587
transport protocols, TCP, 310-311
tree-and-branch cable system, distribution network, 386
Trojan horse attacks, 219
troubleshooting, 545. See also troubleshooting tools
  ACLs, 365-367
  application layer, 589-594
  bottom-up method, 545
  data link layer, 577-579
    Frame Relay, 581-583
    PPP, 579-580
    STP loops, 583-584
  DHCP, 456-458
  divide-and-conquer method, 547
  Frame Relay, 178-179
  from ISP perspective, 570
  IPv6, RIPng, 510
  method, selecting, 547
  NAT, 483-485
  NAT overload, 483-485
  network layer, 585-586
  physical layer, 573-576
  PPP authentication, 118-119
  serial interfaces, 76-82
  serial PPP encapsulation, 102-108
  symptoms, gathering, 548-551
  systematic approach, 541
top-down method, 546
transport layer, 586-587
  NAT, 588-589
troubleshooting commands, 294
  show commands, 294

troubleshooting tools
  hardware tools, 555
  research activity, 558
  software tools
    knowledge bases, 552
    NMS tools, 551

trust exploitation, 209-210

TTY lines, securing remote administration of routers, 243
tunneling, 383, 409, 477-479, 499, 502
two-way satellite Internet systems, 399

Type 5 encryption, 238
Type 7 encryption, 237

UDP port numbers, 311
unspeciﬁed addresses (IPv6), 497
unstructured threats, 204
upgrading software images, 285, 287-288
upstream RF signal transmission, 388
username passwords, protecting, 239

V

V.35 standard, 59
VCs, 27-28, 134
  multiple VCs on single access line, 137-139
verifying
  ACLs, 346-347
  DHCP, 442-447
  DHCP relay conﬁguration, 458
  Frame Relay conﬁguration
    DLCIs, 177
    interfaces, 172
    LMI statistics, 174
  NAT conﬁguration, 479, 483
  serial PPP encapsulation, 101-102
virus, 218

VPNs, 41, 402
  authentication, 415
  beneﬁts of, 404

encryption, 410
  asymmetric, 413
  hashes, 414
  symmetric, 413
IPsec, 416-418
island analogy, 403
remote access, 406
required components, 407
security, characteristics, 408
site-to-site, 405
tunneling, 409

VTY access
  controlling with ACLs, 342-343
  securing remote administration of routers, 243-245

vulnerabilities, 199
  conﬁguration weaknesses, 201
  of networks, 204
  technological weaknesses, 200

W

Walson, John, 386

WAN connection options for teleworker services, 384
See also WANs
  broadband wireless, 396
  mesh municipal Wi-Fi network, 397
  satellite Internet, 399
  single wireless router deployment, 397
  standards, 400
  WiMAX, 398
  cable, 385-386
    CMTS, 390-391
    DOCSIS, 388-389
  electromagnetic spectrum, 387
  DSL, 391
    ADSL, 393-395
    local loop, 392

WANs, 3, 8
  global networks, 9-10
  need for, 5
  purpose of, 46

white hats, 191

Wi-Fi Alliance, 400

wildcard masks, 332
  bit keywords, 337-339
  calculating, 336-337
  IP subnets, matching, 334-337
WiMAX (Worldwide Interoperability for Microwave Access) , 40, 398
wireless connections, 40
wiring closets, 11
worms, 217

X-Y-Z

X.25 networks, 35, 133
xmodem command, restoring software images,
291-292, 294