



Interconnecting Cisco Network Devices, Part 1 (ICND1) Foundation Learning Guide



ciscopress.com

Anthony Sequeira

FREE SAMPLE CHAPTER



SHARE WITH OTHERS

Interconnecting Cisco Network Devices Part I (ICND1) Foundation Learning Guide

Anthony Sequeira CCIE #15626

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

Interconnecting Cisco Network Devices Part I (ICND1) Foundation Learning Guide

Anthony Sequeira

Copyright© 2013 Cisco Systems, Inc.

Published by:

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

First Printing June 2013

Library of Congress Cataloging-in-Publication Number: 2013938764

ISBN-13: 978-1-58714-376-2

ISBN-10: 1-58714-376-3

Warning and Disclaimer

This book is designed to provide information about network security. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The author, 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 author and are not necessarily those of Cisco Systems, Inc.

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.

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 of the U.S., 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 from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding 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 make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Business Operation Manager, Cisco Press: Jan Cornelssen

Executive Editor: Brett Bartow

Development Editor: Eleanor C. Bru

Copy Editor: John Edwards

Technical Editors: Narbik Kocharians, Ryan Lindfield

Editorial Assistant: Vanessa Evans

Managing Editor: Sandra Schroeder

Project Editor: Mandie Frank

Proofreader: Sheri Cain

Indexer: Erika Millen

Cover Designer: Mark Shirar

Composition: Trina Wurst



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCEI, CCOI, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

About the Author

Anthony Sequeira, CCIE No. 15626, is a seasoned trainer and author regarding all levels and tracks of Cisco certification. Anthony formally began his career in the information technology industry in 1994 with IBM in Tampa, Florida. He quickly formed his own computer consultancy, Computer Solutions, and then discovered his true passion—teaching and writing about Microsoft and Cisco technologies.

Anthony joined Mastering Computers in 1996 and lectured to massive audiences around the world about the latest in computer technologies. Mastering Computers became the revolutionary online training company, KnowledgeNet, and Anthony trained there for many years.

Anthony is currently pursuing his second CCIE in the area of security and then his third Cisco Data Center! When not writing for Cisco Press, Anthony is a full-time instructor for the next-generation of KnowledgeNet, StormWind.com.

Anthony is an avid tennis player, is a private pilot, and enjoys getting beaten up by women and children at his and his daughter's martial arts school, www.sparta.fm.

About the Technical Reviewers

Narbik Kocharians, CCSI, CCIE No. 12410, (R&S, Security, SP) who has over 36 years of experience in the industry, is a Triple CCIE. He has designed, implemented, and supported numerous enterprise networks. Some of the international companies that Narbik has worked for are IBM, Carlton United Breweries, Australian Cable and Wireless, BP, and AMOCO. In the United States, he has worked for 20th Century Insurance, Home Savings of America, Verizon, TTI, Trinet Inc, Andersen Networking and Consulting, and many more. Narbik has been a dedicated CCIE instructor for over 12 years. In 2012, he was awarded the Sirius Top Quality Instructor Award.

Narbik Kocharians established his own school, Micronics Networking & Training, Inc. (www.micronicstraining.com) in 2006, where he teaches Cisco authorized courses from CCNA to CCIE in R&S, Security, SP, and Data Center.

Ryan Lindfield is a Certified Cisco Systems Instructor (CCSI) and consultant, based in Tampa, FL. His first position in 1996 was the systems administrator of Gorilla, a video game developer for Mattel and Disney. In 2001, he became an independent contractor, handling system, network, and security contracts for a wide range of customers, including commercial business (IBM), service providers (Verizon), government contractors (L3), and government entities (TSA). In 2003, he became associated with Boson as technical instructor and developer. Topics of expertise include routing and switching, offensive and defensive security, data center technologies, and IPv6. In 2008, with the help of his wife and fellow Cisco instructor, Desiree Lindfield, he launched Westchase Technologies, providing consulting and educational services for clients globally. On a typical day, he can be found providing authorized training for Computer Data, Global Knowledge, and Boson. When not in the classroom, he spends time designing, troubleshooting, and securing customer networks. He is a frequent attendee of Cisco Live, Blackhat, and Defcon conferences. Ryan holds the following certifications: CCNP, CCNP-Data Center, CCNP-Security, HP MASE Networking, VCP, CISSP, CEH, CHFI, GCFA, OSWP, CPTE, LPI-2, and a variety of Microsoft and CompTIA certifications.

Dedication

This book is dedicated to my amazingly talented daughter, Bella Joy Sequeira. Remember that you can do and become anything that you really put your mind to!

Acknowledgments

As always, thanks to my friend, fantasy baseball nemesis, and tequila-drinking partner, Brett Bartow of Cisco Press. Thanks also to Ellie Bru and everyone else at Cisco Press who worked so tirelessly to make this book a reality!

Thanks also to my friends Ryan Lindfield and Narbik Kocharians, who were kind enough to lend their technical editing services to this text. You guys helped this product tremendously!

Finally, thanks to everyone at StormWind.com for the time and the resources to make this book, and the videos for each chapter, a reality.

Contents at a Glance

	Introduction	xxi
Chapter 1	The Functions of Networking	1
Chapter 2	The OSI and TCP/IP Models	25
Chapter 3	LANs and Ethernet	43
Chapter 4	Operating Cisco IOS Software	69
Chapter 5	Switch Technologies	89
Chapter 6	VLANs and Trunks	111
Chapter 7	The TCP/IP Internet Layer	139
Chapter 8	IP Addressing and Subnets	161
Chapter 9	The TCP/IP Transport Layer	195
Chapter 10	The Functions of Routing	219
Chapter 11	The Packet Delivery Process	233
Chapter 12	Configuring a Cisco Router	255
Chapter 13	Static Routing	285
Chapter 14	Dynamic Routing Protocols	293
Chapter 15	OSPF	311
Chapter 16	DHCP and NAT	343
Chapter 17	Securing the Network	371
Chapter 18	Managing Traffic with Access Control Lists	391
Chapter 19	Introducing WAN Technologies	433
Chapter 20	Introducing IPv6	441
Appendix A	Answers to Chapter Review Questions	457
Appendix B	Acronyms and Abbreviations	471
	Glossary	477
	Index	501

Contents

	Introduction	xxi
Chapter 1	The Functions of Networking	1
	Chapter Objectives	2
	What Is a Network?	2
	Physical Components of a Network	4
	Interpreting a Network Diagram	5
	Network User Applications	7
	Impact of User Applications on the Network	8
	Characteristics of a Network	10
	Physical Versus Logical Topologies	11
	Physical Topologies	11
	Logical Topologies	12
	Bus Topology	13
	Star and Extended-Star Topologies	14
	<i>Star Topology</i>	14
	<i>Extended-Star Topology</i>	15
	Ring Topologies	16
	<i>Single-Ring Topology</i>	16
	<i>Dual-Ring Topology</i>	17
	Mesh and Partial-Mesh Topologies	17
	<i>Full-Mesh Topology</i>	17
	<i>Partial-Mesh Topology</i>	18
	Connections to the Internet	18
Chapter 2	The OSI and TCP/IP Models	25
	Chapter Objectives	26
	Understanding the Host-to-Host Communications Model	26
	The OSI Reference Model	27
	Layer 7: The Application Layer	29
	Layer 6: The Presentation Layer	29
	Layer 5: The Session Layer	29
	Layer 4: The Transport Layer	30
	Layer 3: The Network Layer	30
	Layer 2: The Data Link Layer	31
	Layer 1: The Physical Layer	31

The Data Communications Process	31
Encapsulation	32
Deencapsulation	33
Peer-to-Peer Communication	34
The TCP/IP Protocol Stack	35
OSI Model Versus TCP/IP Stack	36

Chapter 3 LANs and Ethernet 43

Chapter Objectives	44
Understanding LANs	44
The Definition of a LAN	44
Components of a LAN	45
Functions of a LAN	46
How Big Is a LAN?	47
Ethernet	48
Ethernet LAN Standards	48
<i>LLC Sublayer</i>	49
<i>MAC Sublayer</i>	49
The Role of CSMA/CD in Ethernet	49
Ethernet Frames	50
Ethernet Frame Addressing	52
Ethernet Addresses	52
MAC Addresses and Binary-Hexadecimal Numbers	53
Connecting to an Ethernet LAN	54
Ethernet Network Interface Cards	54
Ethernet Media and Connection Requirements	55
Connection Media	55
Unshielded Twisted-Pair Cable	57
UTP Implementation	58
Auto-MDIX	62
Optical Fiber	62

Chapter 4 Operating Cisco IOS Software 69

Chapter Objectives	70
Cisco IOS Software Features and Functions	70
Cisco IOS CLI Functions	71
Configuring Network Devices	72
External Configuration Sources	73
Entering the EXEC Modes	75

Help in the CLI	77
Enhanced Editing Commands	79
Command History	81
Managing Cisco IOS Configuration	81
Improving the User Experience in the CLI	84

Chapter 5 Switch Technologies 89

Chapter Objectives	90
The Need for Switches	90
Switch Characteristics	92
Starting and Configuring a Switch	93
Switch Installation	93
Switch LED Indicators	93
Connecting to the Console Port	94
Basic Switch Configuration	95
Verifying the Switch Initial Startup Status	97
Switching Operation	99
Duplex Communication	100
Troubleshooting Common Switch Media Issues	102
Media Issues	102
Port Issues	106

Chapter 6 VLANs and Trunks 111

Chapter Objectives	112
Implementing VLANs and Trunks	112
Issues in a Poorly Designed Network	112
VLAN Overview	114
Understanding Trunking with 802.1Q	115
802.1Q Frame	116
802.1Q Native VLAN	117
Understanding VLAN Trunking Protocol	118
VTP Modes	118
VTP Operation	119
VTP Pruning	120
Configuring VLANs and Trunks	121
VTP Configuration	122
Example: VTP Configuration	122
802.1Q Trunking Configuration	123
VLAN Creation	126

- VLAN Port Assignment* 128
- Adds, Moves, and Changes for VLANs* 129
- Adding VLANs and Port Membership* 129
- Changing VLANs and Port Membership* 130
- Deleting VLANs and Port Membership* 130
- VLAN Design Considerations 130
- Physical Redundancy in a LAN 131
- Routing Between VLANs 133
 - Understanding Inter-VLAN Routing 133
 - Example: Router on a Stick* 134
 - Example: Subinterfaces* 135
 - Configuring Inter-VLAN Routing Using Router on a Stick 135
 - Using Multilayer (Layer 3) Switches 136

Chapter 7 The TCP/IP Internet Layer 139

- Chapter Objectives 140
- Understanding TCP/IP's Internet Layer 140
 - IP Network Addressing 140
 - IP Address Classes 143
 - Network and Broadcast Addresses 145
 - Public and Private IP Addresses 149
 - Address Exhaustion 150
- Addressing Services 153
 - Dynamic Host Configuration Protocol 154
 - Domain Name System 155
 - Using Common Host Tools to Determine the IP Address of a Host 155

Chapter 8 IP Addressing and Subnets 161

- Chapter Objectives 161
- Understanding Binary Numbering 162
 - Decimal and Binary Systems 162
 - Least Significant Bit and Most Significant Bit* 163
 - Base 2 Conversion System* 164
 - Powers of 2 164
 - Decimal-to-Binary Conversion 165
 - Binary-to-Decimal Conversion 166
- Constructing a Network Addressing Scheme 167
 - Subnetworks 167
 - Two-Level and Three-Level Addresses* 169
 - Subnet Creation* 170

	Computing Usable Subnetworks and Hosts	170
	<i>Computing Hosts for a Class C Subnetwork</i>	170
	<i>Computing Hosts for a Class B Subnetwork</i>	171
	<i>Computing Hosts for a Class A Subnetwork</i>	172
	How End Systems Use Subnet Masks	173
	How Routers Use Subnet Masks	174
	Mechanics of Subnet Mask Operation	176
	Applying Subnet Mask Operation	178
	Determining the Network Addressing Scheme	179
	Class C Example	180
	Class B Example	181
	Class A Example	183
	Implementing Variable-Length Subnet Masks	184
	Introducing VLSMs	184
	Route Summarization with VLSM	187
Chapter 9	The TCP/IP Transport Layer	195
	Chapter Objectives	195
	Understanding TCP/IP's Transport Layer	196
	The Transport Layer	196
	TCP/IP Applications	199
	Transport Layer Functionality	200
	<i>TCP/UDP Header Format</i>	202
	<i>How TCP and UDP Use Port Numbers</i>	204
	<i>Establishing a TCP Connection: The Three-Way Handshake</i>	205
	<i>Session Multiplexing</i>	208
	<i>Segmentation</i>	209
	<i>Flow Control for TCP/UDP</i>	209
	<i>Acknowledgment</i>	210
	<i>Windowing</i>	211
	<i>Fixed Windowing</i>	211
	<i>Example: Throwing a Ball</i>	212
	<i>TCP Sliding Windowing</i>	213
	<i>Maximize Throughput</i>	214
	<i>Global Synchronization</i>	214
Chapter 10	The Functions of Routing	219
	Chapter Objectives	220
	Exploring the Functions of Routing	220

Routers	220
Path Determination	222
Routing Tables	223
<i>Routing Table Information</i>	223
<i>Routing Update Messages</i>	224
Static, Dynamic, Directly Connected, and Default Routes	224
Dynamic Routing Protocols	225
<i>Routing Metrics</i>	225
<i>Routing Methods</i>	226

Chapter 11 The Packet Delivery Process 233

Chapter Objectives	233
Exploring the Packet Delivery Process	234
Layer 1 Devices and Their Functions	234
Layer 2 Devices and Their Functions	234
Layer 2 Addressing	235
Layer 3 Devices and Their Functions	236
Layer 3 Addressing	236
Mapping Layer 2 Addressing to Layer 3 Addressing	237
ARP Table	238
Host-to-Host Packet Delivery	238
Function of the Default Gateway	247
Using Common Host Tools to Determine the Path Between Two Hosts Across a Network	248

Chapter 12 Configuring a Cisco Router 255

Chapter Objectives	255
Starting a Cisco Router	256
Initial Startup of a Cisco Router	256
Initial Setup of a Cisco Router	257
Logging In to the Cisco Router	263
Showing the Router Initial Startup Status	266
Summary of Starting a Cisco Router	267
Configuring a Cisco Router	267
Cisco Router Configuration Modes	268
Configuring a Cisco Router from the CLI	269
Configuring Cisco Router Interfaces	271
Configuring the Cisco Router IP Address	272
Verifying the Interface Configuration	273
Verifying the Interface Configuration	277

Chapter 13 Static Routing 285

- Chapter Objectives 285
- Enabling Static Routing 286
 - Routing Overview 286
 - Static and Dynamic Route Comparison 287
 - Static Route Configuration 288
 - Example: Understanding Static Routes* 288
 - Example: Configuring Static Routes* 289
 - Default Route Forwarding Configuration 290
 - Static Route Verification 290

Chapter 14 Dynamic Routing Protocols 293

- Chapter Objectives 294
- Dynamic Routing Protocol Overview 294
- Features of Dynamic Routing Protocols* 296
 - Example: Administrative Distance* 296
- Classful Routing Versus Classless Routing Protocols 297
- Distance Vector Route Selection 299
 - Example: Distance Vector Routing Protocols* 299
 - Example: Sources of Information and Discovering Routes* 300
- Understanding Link-State Routing Protocols 300
 - Link-State Routing Protocol Algorithms* 304

Chapter 15 OSPF 311

- Chapter Objectives 311
- Introducing OSPF 312
 - Establishing OSPF Neighbor Adjacencies 313
 - SPF Algorithm 315
 - Configuring and Verifying OSPF 316
 - Loopback Interfaces 317
 - Verifying the OSPF Configuration 318
 - Load Balancing with OSPF 326
 - OSPF Authentication 328
 - Types of Authentication* 328
 - Configuring Plaintext Password Authentication* 329
 - Example: Plaintext Password Authentication Configuration* 330
 - Verifying Plaintext Password Authentication* 331
- Troubleshooting OSPF 332
 - Components of Troubleshooting OSPF 332
 - Troubleshooting OSPF Neighbor Adjacencies 333

Troubleshooting OSPF Routing Tables	336
Troubleshooting Plaintext Password Authentication	337

Chapter 16 DHCP and NAT 343

Chapter Objectives	343
Using a Cisco Router as a DHCP Server	344
Understanding DHCP	344
<i>DHCPDISCOVER</i>	344
<i>DHCPOFFER</i>	345
<i>DHCPREQUEST</i>	345
<i>DHCPACK</i>	345
Configuring a Cisco Router as a DHCP Client	345
Using a Cisco Router as a DHCP Server	345
Using a Cisco Router as a DHCP Relay Agent	347
Scaling the Network with NAT and PAT	347
Introducing NAT and PAT	348
Translating Inside Source Addresses	350
<i>Static NAT Address Mapping</i>	353
<i>Dynamic Address Translation</i>	354
Overloading an Inside Global Address	355
Resolving Translation Table Issues	359
Resolving Issues by Using the Correct Translation Entry	362

Chapter 17 Securing the Network 371

Chapter Objectives	372
Securing the Network	372
Need for Network Security	372
Balancing Network Security Requirements	375
Adversaries, Hacker Motivations, and Classes of Attack	376
<i>Classes of Attack</i>	376
Mitigating Common Threats	377
<i>Physical Installations</i>	377
<i>Reconnaissance Attacks</i>	378
<i>Access Attacks</i>	379
<i>Password Attacks</i>	379
Understanding Cisco Device Security	380
Physical and Environmental Threats	380
Configuring Password Security	380
Configuring the Login Banner	382

Telnet Versus SSH Access	383
Port Security Configuration on Switches	384
Securing Unused Ports	387

Chapter 18 Managing Traffic with Access Control Lists 391

Chapter Objectives	392
Access Control List Operation	392
Understanding ACLs	392
ACL Operation	395
Types of ACLs	398
ACL Identification	398
Additional Types of ACLs	401
<i>Dynamic ACLs</i>	401
<i>Reflexive ACLs</i>	402
<i>Time-Based ACLs</i>	404
ACL Wildcard Masking	405
Configuring ACLs	408
Configuring Numbered Standard IPv4 ACLs	408
<i>Example: Numbered Standard IPv4 ACL—Permit My Network Only</i>	409
<i>Example: Numbered Standard IPv4 ACL—Deny a Specific Host</i>	410
<i>Example: Numbered Standard IPv4 ACL—Deny a Specific Subnet</i>	411
Controlling Access to the Router Using ACLs	413
Configuring Numbered Extended IPv4 ACLs	413
<i>Extended ACL with the established Parameter</i>	416
<i>Numbered Extended IP ACL: Deny FTP from Subnets</i>	417
<i>Numbered Extended ACL: Deny Only Telnet from Subnet</i>	418
Configuring Named ACLs	419
<i>Creating Named Standard IP ACLs</i>	420
<i>Creating Named Extended IP ACLs</i>	421
<i>Named Extended ACL: Deny a Single Host from a Given Subnet</i>	422
<i>Named Extended ACL—Deny a Telnet from a Subnet</i>	424
Adding Comments to Named or Numbered ACLs	425
Troubleshooting ACLs	425
Problem: Host Connectivity	427

Chapter 19 Introducing WAN Technologies 433

Chapter Objectives	433
Introducing WANs	434

- WANs Versus LANs 435
- The Role of Routers in the WAN 437
- WAN Communication Link Options 437
- Point-to-Point Connectivity 438
- Configuring a Point-to-Point Link 438

Chapter 20 Introducing IPv6 441

- Chapter Objectives 441
- Overview of IPv6 442
 - IPv6 Features and Addresses 443
 - IPv6 Address Types 444
 - IPv6 Address Allocation Options 446
 - IPv6 Header Changes and Benefits 447
- Other IPv6 Features 449
 - ICMPv6 449
 - Neighbor Discovery 449
 - Stateless Autoconfiguration 449
- IPv6 Routing 450
 - Basic IPv6 Connectivity 451
 - Configuring IPv6 Routing 452
 - Static Routing 452
 - OSPFv3 452

Appendix A Answers to Chapter Review Questions 457

Appendix B Acronyms and Abbreviations 471

Glossary 477

Index 501

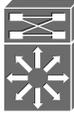
Icons



Router



Switch



Multilayer Switch



Cisco ASA



Database



Cisco CallManager



IP Phone



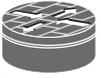
Access Server



VPN Concentrator



PIX Firewall



Router with Firewall



ATM Switch



CSU/DSU



Web Server



Server



Hub



Mac



PC



Laptop



100BaseT Hub



Repeater



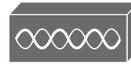
Bridge



IP Telephony Router



uBR910 Cable DSU



Access Point



Modem



Host



Printer



Headquarters



Branch Office



Home Office



Ethernet Connection



Serial Line Connection



Network Cloud

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:

- Boldface indicates commands and keywords that are entered literally, as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a show command).
- Italics indicate arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets [] indicate optional elements.
- Braces { } indicate a required choice.
- Braces within brackets [{ }] indicate a required choice within an optional element.

Introduction

This book was written to allow students to gain a comprehensive foundation in the many different technologies that are found in modern internetworks today. From the most critical network devices to their configuration and troubleshooting, this text provides students with numerous examples, illustrations, and real-world scenarios to gain confidence in the vast world of computer networking.

Goals and Methods

The goal of this book is simple: to provide the reader with a strong foundation in each aspect of computer networking covered in the ICND1 Version 2 blueprint from Cisco Systems.

To accomplish this goal, great pains were taken to reorganize, simplify, and elaborate on specific content from previous editions of this text. Review questions were added for each technology to endure mastery. In addition, two new sections were added to each chapter: Additional Resources and Production Network Simulation Questions. The Additional Resources sections each contain a link to a video created by the author. These videos both complement and supplement the material from the chapter. We hope you enjoy them! The Production Network Simulation Questions help bring the material to life and also challenge the reader with a more “real-world” review.

Who Should Read This Book

Three primary audiences were identified for this text:

- The network engineer needing to review key technologies that are important in today’s networks.
- The reader who is interested in learning about computer networking and who might lack any previous experience in the subject.
- The reader who is interested in obtaining the Cisco CCNA Certification.

How This Book Is Organized

Although you could read this book from cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover only the material you need. If you intend to read all the chapters, the order in which they are presented is an excellent sequence.

Chapters 1 through 20 cover the following topics:

- Chapter 1, “The Functions of Networking”: What are the key devices that make up a network today? And for that matter, what is so important about a computer network anyway? These questions and more are explored in this first chapter.
- Chapter 2, “The OSI and TCP/IP Models”: While most students shudder at the thought of learning these important networking models, this chapter makes this pursuit simple—and perhaps even enjoyable!
- Chapter 3, “LANs and Ethernet”: The local-area network and the Ethernet connections that help build it are some of the most important aspects to learn in modern networking. This chapter details these important technologies for the reader.
- Chapter 4, “Operating Cisco IOS Software”: This chapter covers the basics of using the software that powers the majority of Cisco devices today.
- Chapter 5, “Switch Technologies”: Switch technologies replaced the need for hubs in our network environments and, as such, are a critical component in the modern network. This chapter explores the inner workings of these important devices.
- Chapter 6, “VLANs and Trunks”: VLANs permit the creation of broadcast domains (IP subnets) in the local-area network and are of critical importance. So are the trunk links that carry VLAN traffic from Cisco device to Cisco device. This chapter ensures that the reader is well versed in these important technologies.
- Chapter 7, “The TCP/IP Internet Layer”: One of the key layers in the OSI model for any network engineer to master is the Internet layer. This chapter is dedicated to this important concept.
- Chapter 8, “IP Addressing and Subnets”: What is one topic that many fear in the CCNA curriculum? The mastery of IP addressing—including subnetting. This chapter dispels these fears and provides simple instructions for creating the best IP addressing schemes for your small network.
- Chapter 9, “The TCP/IP Transport Layer”: The transport layer of the OSI model is often misunderstood. This chapter ensures that readers can describe the importance and operation of this key layer.
- Chapter 10, “The Functions of Routing”: Why is routing so important? How does it work? This chapter is a must-read for anyone who requires more information about these critical network devices called routers.
- Chapter 11, “The Packet Delivery Process”: Everything that must occur when you type `www.ciscopress.com` in your web browser and press Enter is absolutely amazing. This chapter details the processes that occur when two systems communicate on a typical network today.

- Chapter 12, “Configuring a Cisco Router”: In Chapter 10, you learn all about the functions that a router must perform, and how the device does it. In this chapter, you learn the basics of configuring a Cisco router to perform its important jobs!
- Chapter 13, “Static Routing”: Static routes are extremely important in your network infrastructure. This chapter ensures that you can create them with accuracy and ease in your Cisco-based network.
- Chapter 14, “Dynamic Routing Protocols”: There are many different implementations of routing protocols. This chapter sheds light on the different protocols and their differences.
- Chapter 15, “OSPF”: OSPF is the most popular interior gateway protocol in use on the planet today. This chapter is dedicated to this important protocol and provides the reader with a strong foundation in this complex routing protocol.
- Chapter 16, “DHCP and NAT”: How can we dynamically provide our workstations with their correct IP address information? What are we to do about the exhaustion of TCP/IP addresses today? These critical questions are answered in this chapter.
- Chapter 17, “Securing the Network”: To be a CCNA, you must understand the basic concepts involved with network security. This chapter provides that knowledge!
- Chapter 18, “Managing Traffic with Access Control Lists”: Access control lists are fundamental constructs in Cisco devices. If you want to master Cisco networking, you must be knowledgeable about these components.
- Chapter 19, “Introducing WAN Technologies”: There are a wide variety of methods in use today for sending data long distances in the network. This chapter is dedicated to these various options and provides an overview of WANs for further more in-depth study.
- Chapter 20, “Introducing IPv6”: The future of the TCP/IP protocol is here! And it is here to stay (at least for a while). This chapter educates the reader on IP version 6 and even gets him or her configuring this protocol in a dynamically routed network environment!

This page intentionally left blank

LANs and Ethernet

This chapter includes the following sections:

- Chapter Objectives
- Understanding LANs
- Connecting to an Ethernet LAN
- Chapter Summary
- Additional Resources
- Review Questions
- Production Network Simulation Question 3-1

Local-area networks (LAN) tend to spoil us as network users. These collections of high-speed network equipment allow us to achieve remarkable speeds in accessing network data and information. LANs are a relatively low-cost means of sharing expensive resources. LANs allow multiple users in a relatively small geographic area to exchange files and messages and to access shared resources such as file servers. LANs have rapidly evolved into support systems that are critical to communications within an organization. This chapter will ensure that you are comfortable describing these important network structures.

This chapter also describes different Ethernet media options (copper and fiber), which are presented together with a description of the most common connectors and cable types. Ethernet frame structure is introduced, and important fields are described. MAC addresses and their function are also elaborated on.

Chapter Objectives

Upon completing this chapter, you will be able to describe LAN networks. You will also be able to describe common Ethernet technologies typically found within these important areas of the overall network. These abilities include meeting these objectives:

- Define a LAN
- Identify the components of a LAN
- Describe the types of Ethernet LAN connection media
- Describe the fields of an Ethernet frame
- Define the structure and function of MAC addresses

Understanding LANs

A local-area network is a common type of network found in home offices, small businesses, and large enterprises. Understanding how a LAN functions, including network components, frames, Ethernet addresses, and operational characteristics, is important for an overall knowledge of networking technologies.

This section describes LANs and provides fundamental knowledge about LAN characteristics, components, and functions. It also describes the basic operations of an Ethernet LAN and how frames are transmitted over it.

The Definition of a LAN

A LAN is a network of computers and other components located relatively close together in a limited area. LANs can vary widely in their size. A LAN might consist of only two computers in a home office or small business, or it might include hundreds of computers in a large corporate office or multiple buildings. Figure 3-1 shows some examples of LANs.

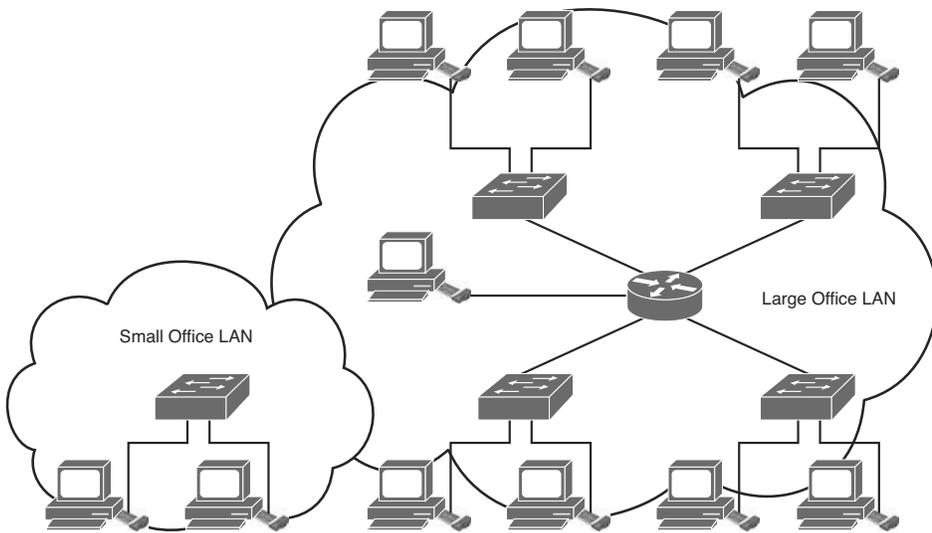


Figure 3-1 *Examples of LANs*

A small home business or a small office environment could use a small LAN to connect two or more computers and to connect the computers to one or more shared peripheral devices such as printers. A large corporate office could use multiple LANs to accommodate hundreds of computers and shared peripheral devices, for departments such as finance or operations, spanning many floors in an office complex.

Components of a LAN

Every LAN has specific components, including hardware, interconnections, and software. Figure 3-2 highlights some typical hardware components of a LAN.

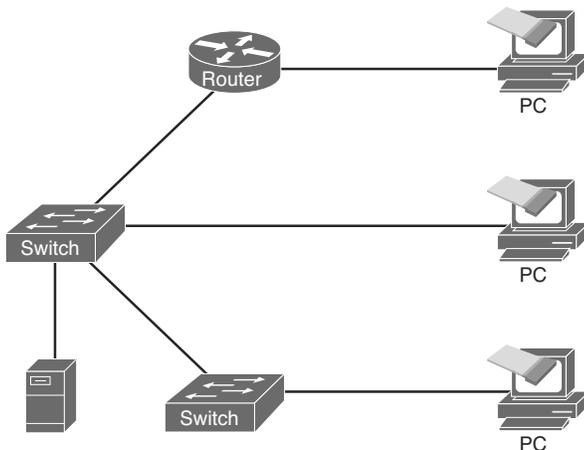


Figure 3-2 *Typical Components of a LAN*

Regardless of the size of the LAN, it requires these fundamental components for its operation:

- **Computers:** Computers serve as the endpoints in the network, sending and receiving data.
- **Interconnections:** Interconnections enable data to travel from one point to another in the network. Interconnections include these components:
 - **NICs:** Network interface cards (NIC) translate the data produced by the computer into a format that can be transmitted over the LAN.
 - **Network media:** Network media, such as cables or wireless media, transmit signals from one device on the LAN to another.
- **Network devices:** A LAN requires the following network devices:
 - **Hubs:** Hubs provide aggregation devices operating at Layer 1 of the OSI reference model. However, hubs have been replaced in this function by switches, and it is very rare to see hubs in any LAN these days.
 - **Ethernet switches:** Ethernet switches form the aggregation point for LANs. Ethernet switches operate at Layer 2 of the OSI reference model and provide intelligent distribution of frames within the LAN.
 - **Routers:** Routers, sometimes called gateways, provide a means to connect LAN segments. Routers operate at Layer 3 of the OSI reference model.
- **Protocols:** Protocols govern the way data is transmitted over a LAN and include the following:
 - Ethernet protocols
 - Internet Protocol (IP)
 - Internet Protocol version 6 (IPv6)
 - Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP)
 - Dynamic Host Configuration Protocol (DHCP)

Functions of a LAN

LANs provide network users with communication and resource-sharing functions, including the following:

- **Data and applications:** When users are connected through a network, they can share files and even software application programs. This makes data more easily available and promotes more efficient collaboration on work projects.
- **Resources:** The resources that can be shared include both input devices, such as cameras, and output devices, such as printers.

- **Communication path to other networks:** If a resource is not available locally, the LAN, through a gateway, can provide connectivity to remote resources—for example, access to the web.

How Big Is a LAN?

A LAN can be configured in a variety of sizes, depending on the requirements of the environment in which it operates.

LANs can be of various sizes to fit different work requirements, including the following:

- **Small office/home office (SOHO):** The SOHO environment typically has only a few computers and some peripherals such as printers.
- **Enterprise:** The enterprise environment might include many separate LANs in a large office building or in different buildings on a corporate campus. In the enterprise environment, each LAN might contain hundreds of computers and peripherals..

Figure 3-3 demonstrates the dramatic differences that can exist with the size of LANs.

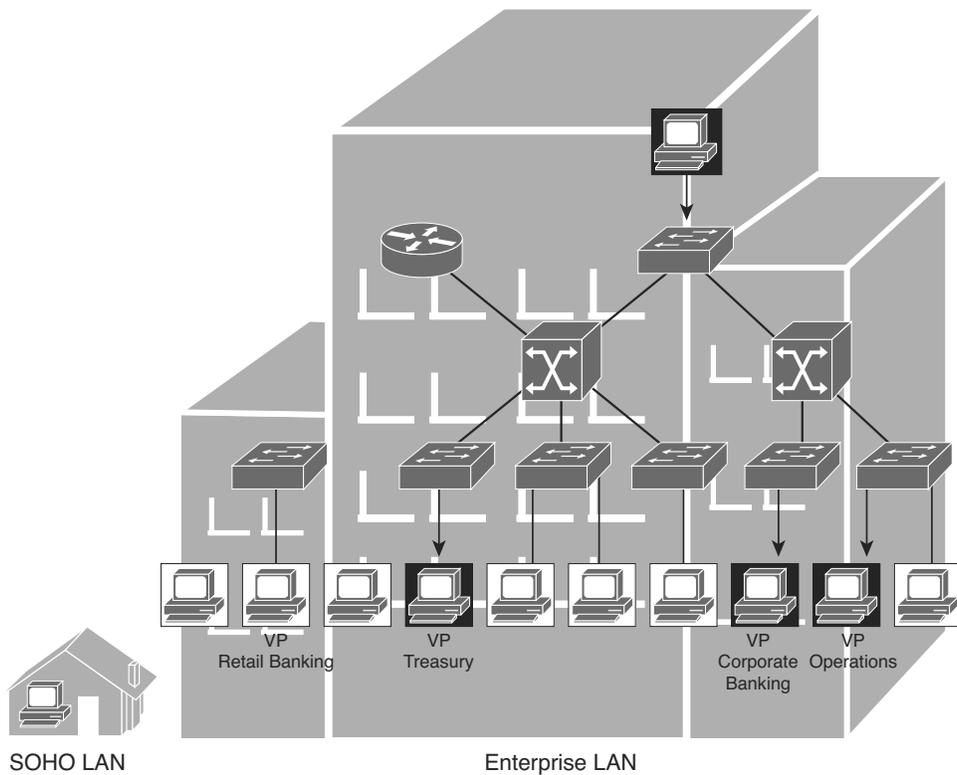


Figure 3-3 *Different LAN Sizes*

Ethernet

Ethernet is the most common type of LAN. It was originally developed in the 1970s by Digital Equipment Corporation (DEC), Intel, and Xerox (DIX) and was called DIX Ethernet. It later came to be called thick Ethernet (because of the thickness of the cable used in this type of network), and it transmitted data at 10 megabits per second (Mbps). The standard for Ethernet was updated in the 1980s to add more capability, and the new version of Ethernet was referred to as Ethernet Version 2 (also called Ethernet II).

The Institute of Electrical and Electronics Engineers (IEEE) is a professional organization that defines network standards. IEEE standards are the predominant LAN standards in the world today. In the mid-1980s, an IEEE workgroup defined new standards for Ethernet-like networks. The set of standards they created was called Ethernet 802.3 and was based on the carrier sense multiple access with collision detection (CSMA/CD) process. Ethernet 802.3 specified the physical layer (Layer 1) and the MAC portion of the data link layer (Layer 2). Today, this set of standards is most often referred to as simply “Ethernet.”

Ethernet LAN Standards

Ethernet LAN standards specify cabling and signaling at both the physical and data link layers of the OSI reference model. This topic describes Ethernet LAN standards at the data link layer.

Figure 3-4 shows how LAN protocols map to the OSI reference model.

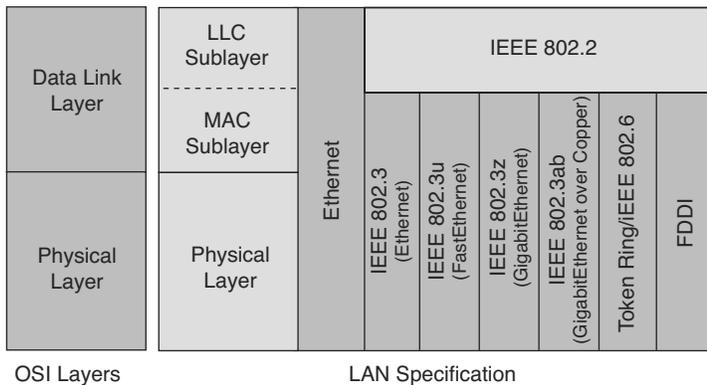


Figure 3-4 *Ethernet and the OSI Model*

The IEEE divides the OSI data link layer into two separate sublayers:

- **Logical link control (LLC):** Transitions up to the network layer
- **MAC:** Transitions down to the physical layer

LLC Sublayer

The IEEE created the LLC sublayer to allow part of the data link layer to function independently from existing technologies. This layer provides versatility in services to the network layer protocols that are above it, while communicating effectively with the variety of MAC and Layer 1 technologies below it. The LLC, as a sublayer, participates in the encapsulation process.

An LLC header tells the data link layer what to do with a packet when it receives a frame. For example, a host receives a frame and then looks in the LLC header to understand that the packet is destined for the IP protocol at the network layer.

The original Ethernet header (prior to IEEE 802.2 and 802.3) did not use an LLC header. Instead, it used a type field in the Ethernet header to identify the Layer 3 protocol being carried in the Ethernet frame.

MAC Sublayer

The MAC sublayer deals with physical media access. The IEEE 802.3 MAC specification defines MAC addresses, which uniquely identify multiple devices at the data link layer. The MAC sublayer maintains a table of MAC addresses (physical addresses) of devices. To participate on the network, each device must have a unique MAC address.

The Role of CSMA/CD in Ethernet

Ethernet signals are transmitted to every station connected to the LAN, using a special set of rules to determine which station can “talk” at any particular time. This topic describes that set of rules.

Ethernet LANs manage the signals on a network by CSMA/CD, which is an important aspect of Ethernet. Figure 3-5 illustrates the CSMA/CD process.

In an Ethernet LAN, before transmitting, a computer first listens to the network media. If the media is idle, the computer sends its data. After a transmission has been sent, the computers on the network compete for the next available idle time to send another frame. This competition for idle time means that no one station has an advantage over another on the network.

Stations on a CSMA/CD LAN can access the network at any time. Before sending data, CSMA/CD stations listen to the network to determine whether it is already in use. If it is, the CSMA/CD stations wait. If the network is not in use, the stations transmit. A collision occurs when two stations listen for network traffic, hear none, and transmit simultaneously (see Figure 3-5). In this case, both transmissions are damaged, and the stations must retransmit at some later time. CSMA/CD stations must be able to detect collisions to know that they must retransmit.

When a station transmits, the signal is referred to as a carrier. The NIC senses the carrier and consequently refrains from broadcasting a signal. If no carrier exists, a waiting station knows that it is free to transmit. This is the “carrier sense” part of the protocol.

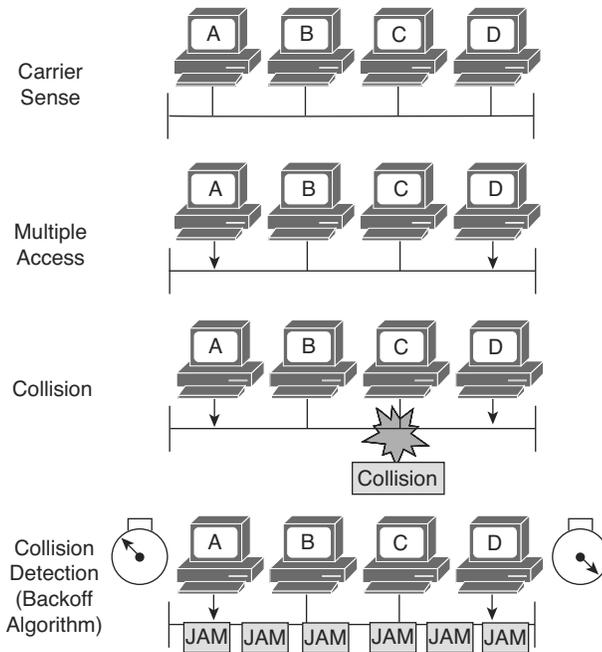


Figure 3-5 CSMA/CD Process

The extent of the network segment over which collisions occur is referred to as the collision domain. The size of the collision domain has an impact on efficiency and therefore on data throughput. In today's LANs, switches have replaced hubs. The reason this occurs is that switches create tiny collision domains containing just one device. This eliminates the potential for collisions. This process is often called "microsegmentation" of the network.

In the CSMA/CD process, priorities are not assigned to particular stations, so all stations on the network have equal access. This is the "multiple access" part of the protocol. If two or more stations attempt a transmission simultaneously, a collision occurs. The stations are alerted of the collision, and they execute a backoff algorithm that randomly schedules retransmission of the frame. This scenario prevents the machines from repeatedly attempting to transmit at the same time. Collisions are normally resolved in microseconds. This is the "collision detection" part of the protocol.

While collisions are resolved quickly, it is still advantageous to eliminate them entirely from the network. This allows much more efficient communications. This is accomplished through the use of switches as described earlier.

Ethernet Frames

Bits that are transmitted over an Ethernet LAN are organized into frames. In Ethernet terminology, the "container" into which data is placed for transmission is called a *frame*. The frame contains header information, trailer information, and the actual data that is being transmitted.

Figure 3-6 illustrates all the fields that are in a MAC layer of the Ethernet frame, which include the following:

- **Preamble:** This field consists of 7 bytes of alternating 1s and 0s, which synchronize the signals of the communicating computers.
- **Start-of-frame (SOF) delimiter:** This field contains bits that signal the receiving computer that the transmission of the actual frame is about to start and that any data following is part of the packet.
- **Destination address:** This field contains the address of the NIC on the local network to which the packet is being sent.
- **Source address:** This field contains the address of the NIC of the sending computer.
- **Type/length:** In Ethernet II, this field contains a code that identifies the network layer protocol. In 802.3, this field specifies the length of the data field. The protocol information is contained in 802.2 fields, which are at the LLC layer. The newer 802.3 specifications have allowed the use of Ethertype protocol identifiers when not using the 802.2 field.
- **Data and pad:** This field contains the data that is received from the network layer on the transmitting computer. This data is then sent to the same protocol on the destination computer. If the data is too short, an adapter adds a string of extraneous bits to “pad” the field to its minimum length of 46 bytes.
- **Frame check sequence (FCS):** This field includes a checking mechanism to ensure that the packet of data has been transmitted without corruption.

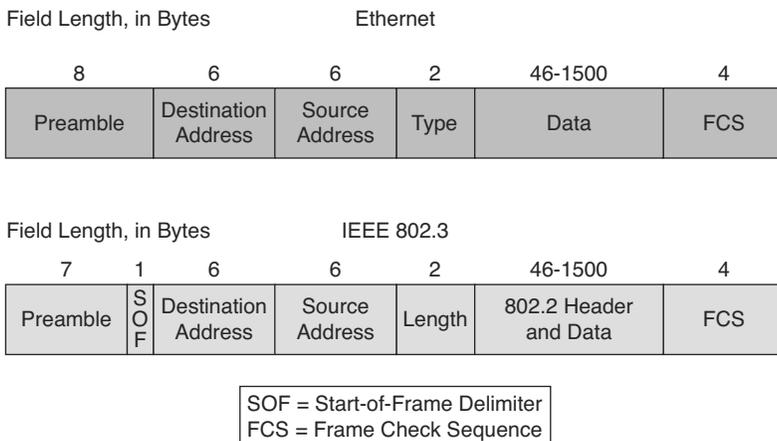


Figure 3-6 *Ethernet Frames*

Ethernet Frame Addressing

Communications in a network occur in three ways: unicast, broadcast, and multicast. Ethernet frames are addressed accordingly. Figure 3-7 shows forms of Ethernet communications.

The three major types of network communications are as follows:

- **Unicast:** Communication in which a frame is sent from one host and addressed to one specific destination. In a unicast transmission, you have just one sender and one receiver. Unicast transmission is the predominant form of transmission on LANs and within the Internet.
- **Broadcast:** Communication in which a frame is sent from one address to all other addresses. In this case, you have just one sender, but the information is sent to all connected receivers. Broadcast transmission is essential when sending the same message to all devices on the LAN.
- **Multicast:** Communication in which information is sent to a specific group of devices or clients. Unlike broadcast transmission, in multicast transmission, clients must be members of a multicast group to receive the information.

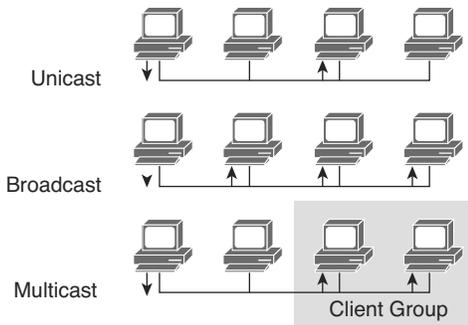


Figure 3-7 *Ethernet Communications*

Ethernet Addresses

The address used in an Ethernet LAN, which is associated with the network adapter, is the means by which data is directed to the proper receiving location. Figure 3-8 shows the format of an Ethernet MAC address.

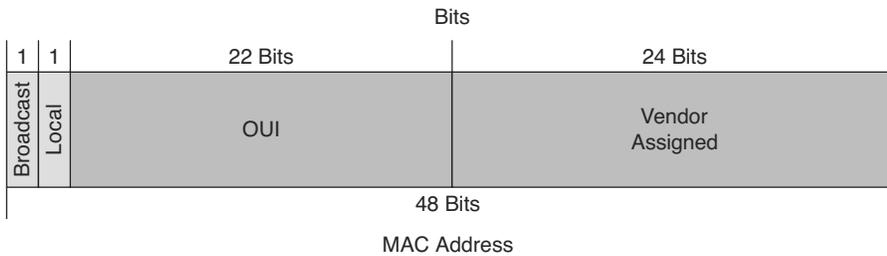


Figure 3-8 *Ethernet MAC Address*

The address that is on the NIC is the MAC address, often referred to as the burned-in address (BIA), and some vendors allow the modification of this address to meet local needs. A 48-bit Ethernet MAC address has two components:

- **24-bit Organizational Unique Identifier (OUI):** The letter *O* identifies the manufacturer of the NIC. The IEEE regulates the assignment of OUI numbers. Within the OUI, the two following bits have meaning only when used in the destination address:
 - **Broadcast or multicast bit:** This indicates to the receiving interface that the frame is destined for all or a group of end stations on the LAN segment.
 - **Locally administered address bit:** Normally the combination of OUI and a 24-bit station address is universally unique; however, if the address is modified locally, this bit should be set.
- **24-bit vendor-assigned end station address:** This uniquely identifies the Ethernet hardware.

MAC Addresses and Binary-Hexadecimal Numbers

The MAC address plays a specific role in the function of an Ethernet LAN. The MAC sublayer of the OSI data link layer handles physical addressing issues, and the physical address is a number in hexadecimal format that is actually burned into the NIC. This address is referred to as the MAC address, and it is expressed as groups of hexadecimal digits that are organized in pairs or quads, such as the following: 00:00:0c:43:2e:08 or 0000:0c43:2e08. Figure 3-9 shows the MAC address format compared to the MAC frame.

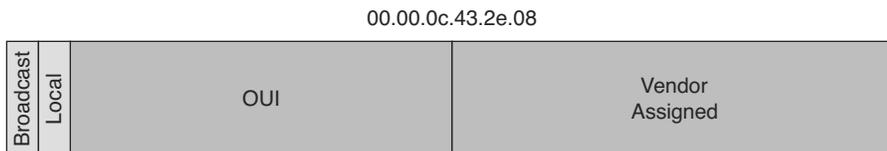


Figure 3-9 *Hexadecimal MAC Address*

Each device on a LAN must have a unique MAC address to participate in the network. The MAC address identifies the location of a specific computer on a LAN. Unlike other kinds of addresses used in networks, the MAC address should *not* be changed unless you have some specific need.

Connecting to an Ethernet LAN

In addition to understanding the components of an Ethernet LAN and the standards that govern its architecture, you need to understand the connection components of an Ethernet LAN. This section describes the connection components of an Ethernet LAN, including network interface cards (NIC) and cable.

Ethernet Network Interface Cards

A NIC is a printed circuit board that provides network communication capabilities to and from a personal computer on a network. Figure 3-10 shows an example of a NIC.

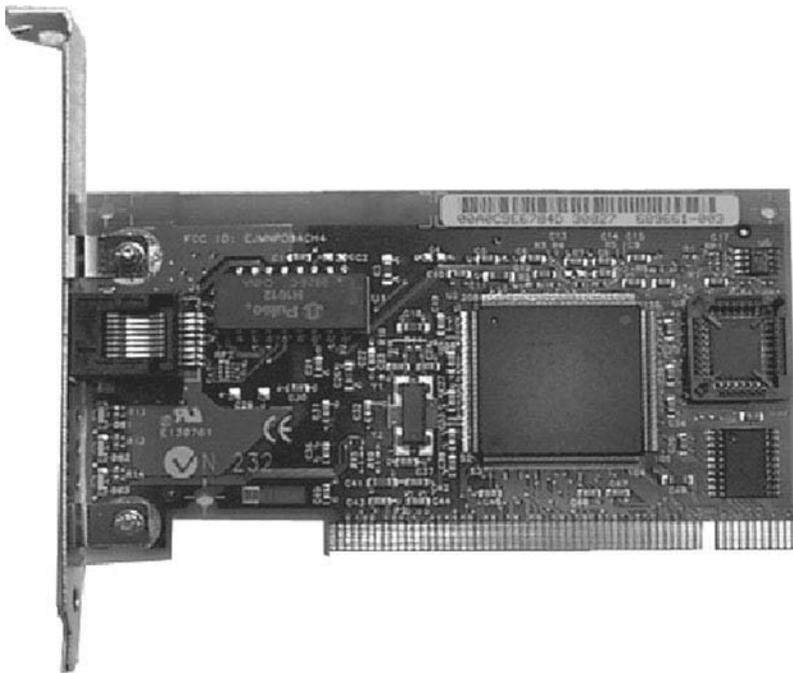


Figure 3-10 Network Interface Card

Also called a LAN adapter, the NIC plugs into a motherboard and provides a port for connecting to the network. The NIC constitutes the computer interface with the LAN.

The NIC communicates with the network through a serial connection, and with the computer through a parallel connection. When a NIC is installed in a computer, it requires an interrupt request line (IRQ), an input/output (I/O) address, a memory space within the operating system (such as DOS or Windows), and drivers (software) that allow it to perform its function. An IRQ is a signal that informs a central processing unit (CPU) that an event needing its attention has occurred. An IRQ is sent over a hardware line to the microprocessor. An example of an interrupt request being issued is when a key is pressed on a keyboard, and the CPU must move the character from the keyboard to RAM. An I/O address is a location in memory used by an auxiliary device to enter data into or retrieve data from a computer.

The MAC address is burned onto each NIC by the manufacturer, providing a unique, physical network address.

Ethernet Media and Connection Requirements

Distance and time dictate the type of Ethernet connections required. This section describes the cable and connector specifications used to support Ethernet implementations.

The cable and connector specifications used to support Ethernet implementations are derived from the EIA/TIA standards body. The categories of cabling defined for Ethernet are derived from the EIA/TIA-568 (SP-2840) Commercial Building Telecommunications Wiring Standards. EIA/TIA specifies an RJ-45 connector for unshielded twisted-pair (UTP) cable.

The important difference to note is the media used for 10-Mbps Ethernet versus 100-Mbps Fast Ethernet. In networks today, where you see a mix of 10- and 100-Mbps requirements, you must be aware of the need to change over to UTP Category 5 to support Fast Ethernet.

Connection Media

Several types of connection media can be used in an Ethernet LAN implementation. Figure 3-11 shows typical connection types.

The most common type of connection media is the RJ-45 connector and jack illustrated in Figure 3-11. The letters RJ stand for registered jack, and the number “45” refers to a specific physical connector that has eight conductors.

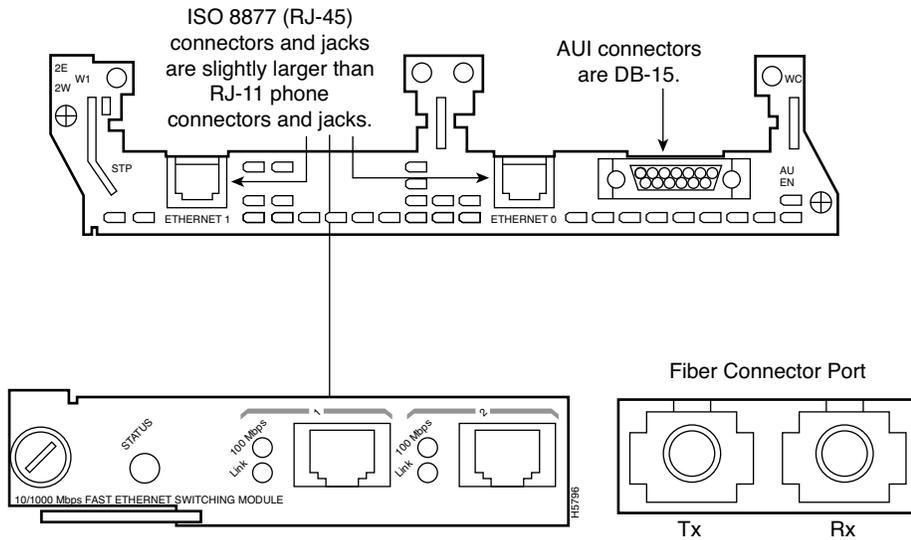


Figure 3-11 *Connection Types*

A Gigabit Interface Converter (GBIC), shown in Figure 3-12, is a hot-swappable I/O device that plugs into a Gigabit Ethernet port. A key benefit of using a GBIC is that it is interchangeable, allowing you the flexibility to deploy other 1000BASE-X technology without having to change the physical interface or model on the router or switch. GBICs support UTP (copper) and fiber-optic media for Gigabit Ethernet transmission.

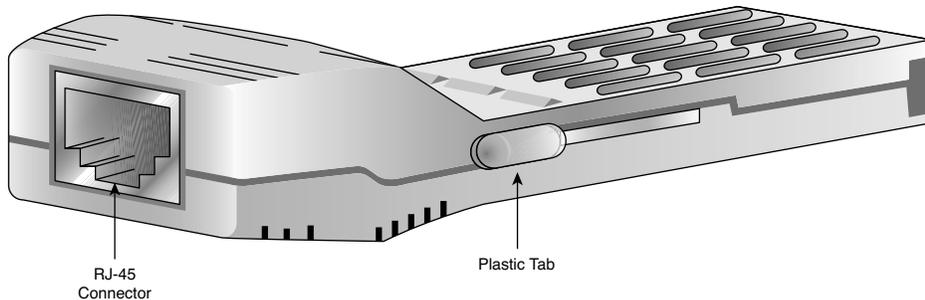


Figure 3-12 *1000BASE-T GBIC*

Typically, GBICs are used in the LAN for uplinks and are normally used for the backbone. GBICs are also seen in remote networks.

The fiber-optic GBIC, shown in Figure 3-13, is a transceiver that converts serial electric currents to optical signals and converts optical signals to digital electric currents.

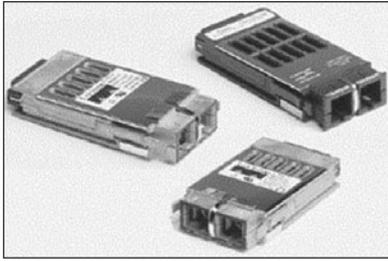


Figure 3-13 *Fiber GBIC*

Optical GBICs include these types:

- Short wavelength (1000BASE-SX)
- Long wavelength/long haul (1000BASE-LX/LH)
- Extended distance (1000BASE-ZX)

Unshielded Twisted-Pair Cable

Twisted-pair is a copper wire–based cable that can be either shielded or unshielded. UTP cable is frequently used in LANs. Figure 3-14 shows an example of a UTP cable.

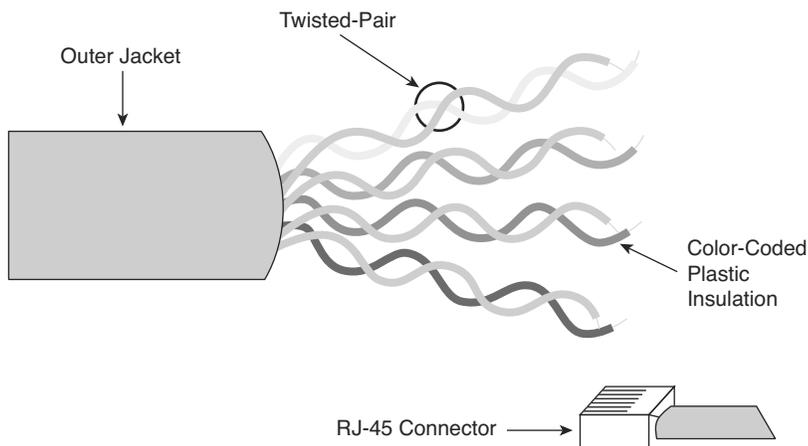


Figure 3-14 *UTP Cable*

UTP cable is a four-pair wire. Each of the eight individual copper wires in UTP cable is covered by an insulating material. In addition, the wires in each pair are twisted around each other. The advantage of UTP cable is its ability to cancel interference, because the twisted wire pairs limit signal degradation from electromagnetic interference (EMI) and

radio frequency interference (RFI). To further reduce crosstalk between the pairs in UTP cable, the number of twists in the wire pairs varies. Both UTP and shielded twisted-pair (STP) cable must follow precise specifications regarding how many twists or braids are permitted per meter.

UTP cable is used in a variety of types of networks. When used as a network medium, UTP cable has four pairs of either 22- or 24-gauge copper wire. UTP used as a network medium has an impedance of 100 ohms, differentiating it from other types of twisted-pair wiring, such as that used for telephone wiring. Because UTP cable has an external diameter of approximately 0.43 cm, or 0.17 inches, its small size can be advantageous during installation. Also, because UTP can be used with most major network architectures, it continues to grow in popularity.

Here are the categories of UTP cable:

- **Category 1:** Used for telephone communications; not suitable for transmitting data
- **Category 2:** Capable of transmitting data at speeds of up to 4 Mbps
- **Category 3:** Used in 10BASE-T networks; can transmit data at speeds up to 10 Mbps
- **Category 4:** Used in Token Ring networks; can transmit data at speeds up to 16 Mbps
- **Category 5:** Capable of transmitting data at speeds up to 100 Mbps
- **Category 5e:** Used in networks running at speeds up to 1000 Mbps (1 Gbps)
- **Category 6:** Consists of four pairs of 24-gauge copper wires, which can transmit data at speeds of up to 1000 Mbps
- **Category 6a:** Used in networks running at speeds up to 10 Gbps

The most commonly used categories in LAN environments today are Categories 1 (used primarily for telephony), 5, 5e, and 6.

UTP Implementation

For a UTP implementation in a LAN, you must determine the EIA/TIA type of cable needed and also whether to use a straight-through or crossover cable. This topic describes the characteristics and uses of straight-through and crossover cables, as well as the types of connectors used when UTP is implemented in a LAN. Figure 3-15 shows an RJ-45 connector.

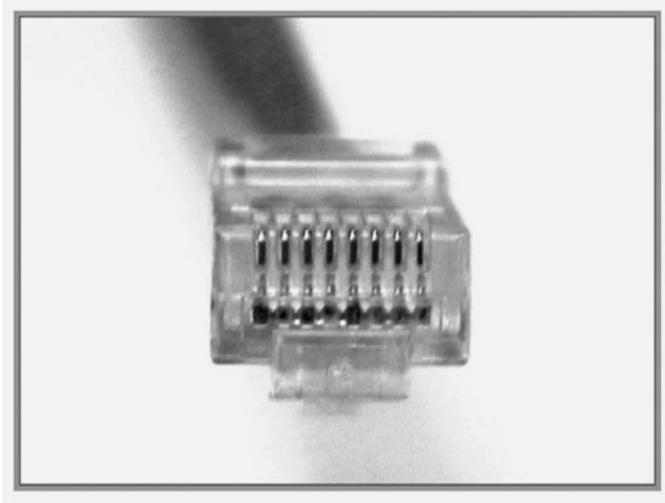


Figure 3-15 *RJ-45 Connector*

If you look at the RJ-45 transparent-end connector, you can see eight colored wires, twisted into four pairs. Four of the wires (two pairs) carry the positive or true voltage and are considered “tip” (T1 through T4); the other four wires carry the inverse of false voltage grounded and are called “ring” (R1 through R4). *Tip* and *ring* are terms that originated in the early days of the telephone. Today, these terms refer to the positive and negative wires in a pair. The wires in the first pair in a cable or a connector are designated as T1 and R1, the second pair as T2 and R2, and so on.

The RJ-45 plug is the male component, crimped at the end of the cable. As you look at the male connector from the front, the pin locations are numbered from 8 on the left to 1 on the right.

The jack is the female component in a network device, wall, cubicle partition outlet, or patch panel.

In addition to identifying the correct EIA/TIA category of cable to use for a connecting device (depending on which standard is being used by the jack on the network device), you need to determine which of the following to use:

- A straight-through cable (either T568A or T568B at each end)
- A crossover cable (T568A at one end; T568B at the other)

In Figure 3-16, the RJ-45 connectors on both ends of the cable show all the wires in the same order. If the two RJ-45 ends of a cable are held side by side in the same orientation, the colored wires (or strips or pins) can be seen at each connector end. If the order of the colored wires is the same at each end, the cable type is straight-through.

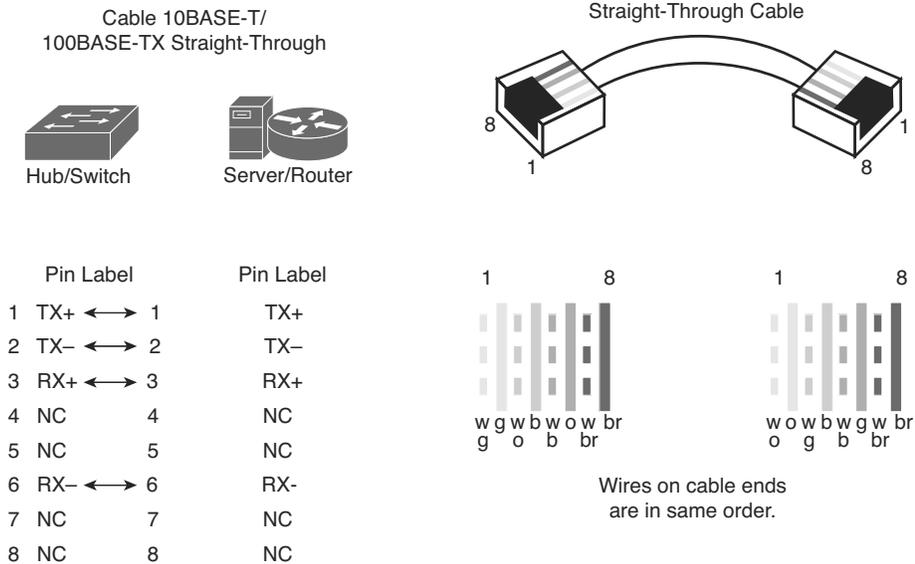


Figure 3-16 *Straight-Through Cable*

With crossover cables, the RJ-45 connectors on both ends show that some of the wires on one side of the cable are crossed to a different pin on the other side of the cable. Specifically, for Ethernet, pin 1 at one RJ-45 end should be connected to pin 3 at the other end. Pin 2 at one end should be connected to pin 6 at the other end, as shown in the Figure 3-17.

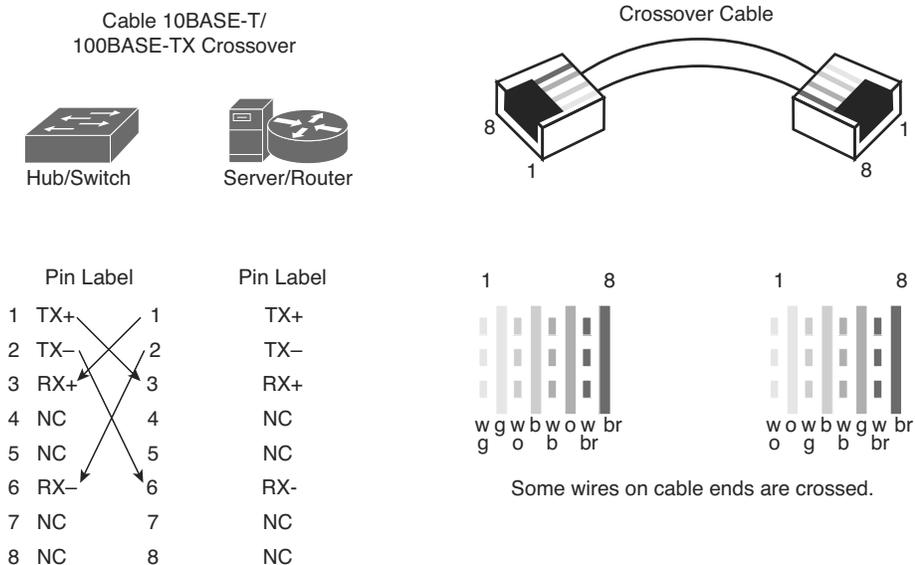


Figure 3-17 *Crossover Cable*

Figure 3-18 shows the guidelines for choosing which type of cable to use when interconnecting Cisco devices. In addition to verifying the category specification on the cable, you must determine when to use a straight-through or crossover cable.

Use straight-through cables for the following cabling:

- Switch to router
- Switch to PC or server
- Hub to PC or server

Use crossover cables for the following cabling:

- Switch to switch
- Switch to hub
- Hub to hub
- Router to router
- Router Ethernet port to PC NIC
- PC to PC

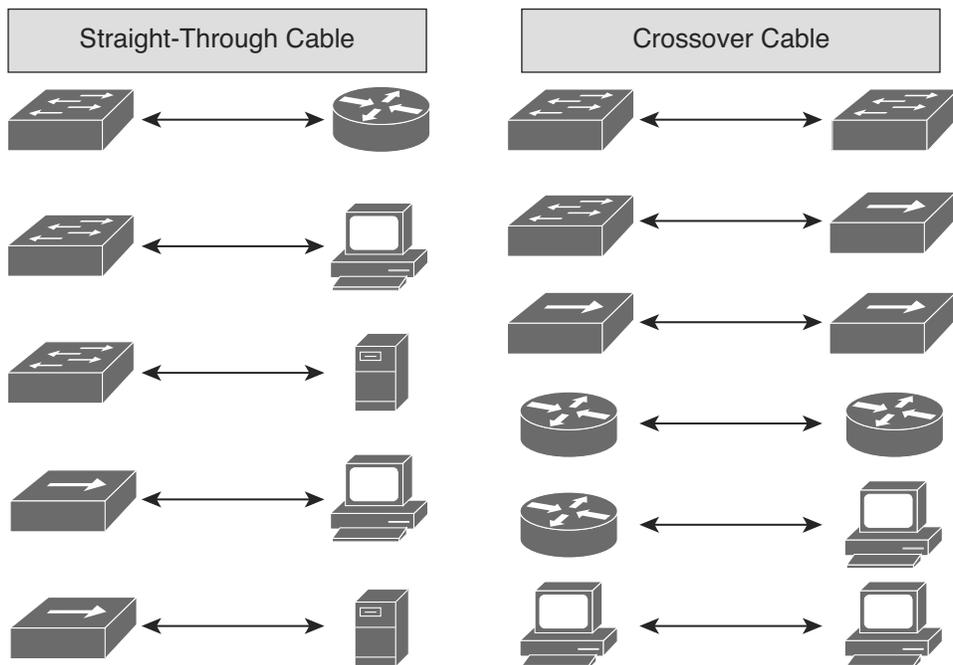


Figure 3-18 *When to Use a Straight-Through Cable Versus a Crossover Cable*

Auto-MDIX

After reading the previous section, you might be concerned about when you are cabling your network, you might make a critical mistake! Imagine, just one wrong type of cable, and your entire LAN might fail to access key resources. Fortunately, there is great news because of a new technology called Auto-MDIX. Auto-MDIX stands for automatic medium-dependent interface crossover, a feature that lets the interface automatically discover whether the wrong cable is installed. A switch that supports the Auto-MDIX feature detects the wrong cable and causes the switch to swap the pair it uses for transmitting and receiving. This solves the cabling problem, and the switch is able to communicate just fine regardless of the fact that you connected the “wrong” cable. Obviously, this new technology is very desirable and is making its way to more and more Cisco devices all the time.

Optical Fiber

An optical fiber is a flexible, transparent fiber that is made of very pure glass (silica) and is not much bigger in diameter than a human hair. It acts as a waveguide, or “light pipe,” to transmit light between the two ends of the fiber. Optical fibers are widely used in fiber-optic communications, which permit transmission over longer distances and at higher bandwidths (data rates) than other forms of communication. Fibers are used instead of metal wires because signals travel along them with less loss and with immunity to electromagnetic interference. Figure 3-19 shows an example of optical fiber.

Optical Fiber (Single Mode)

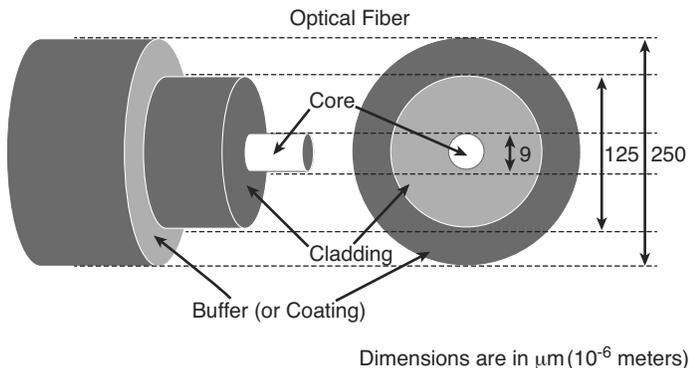


Figure 3-19 *Optical Fiber*

The two fundamental components that allow a fiber to confine light are the core and the cladding. Most of the light travels from the beginning to the end inside the core. The cladding around the core provides confinement. The diameters of the core and cladding are shown in this illustration, but the core diameter can vary for different fiber types. In this case, the core diameter of 9 μm is very small—the diameter of a human hair is about 50 μm . The outer diameter of the cladding is a standard size of 125 μm . Standardizing the size means that component manufacturers can make connectors for all fiber-optic cables.

The third element in this picture is the buffer (coating), which has nothing to do with the confinement of the light in the fiber. Its purpose is to protect the glass from scratches and moisture. The fiber-optic cable can be easily scratched and broken, like a glass pane. If the fiber is scratched, the scratch could propagate and break the fiber. Another important aspect is the need to keep the fiber dry.

The most significant difference between single-mode fiber (SMF) and multimode fiber (MMF) is in the ability of the fiber to send light for a long distance at high bit rates. In general, MMF is used for shorter distances at a lower bit rate than SMF. For long-distance communications, SMF is preferred. There are many variations of fiber for both MMF and SMF. Figure 3-20 shows the two fiber types.

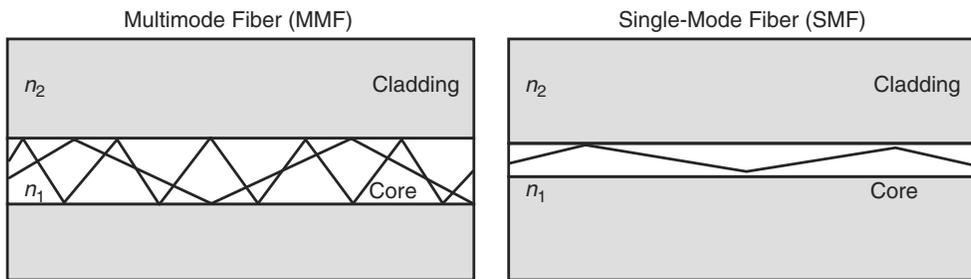


Figure 3-20 *Fiber-Optic Types*

The most significant physical difference is in the size of the core. The glass in the two fibers is the same, and the index of refraction change is similar. The core diameter can make a major difference. The diameter of the fiber cladding is universal for matching fiber ends.

The effect of having different-size cores in fiber is that the two fiber types will support different ways for the light to get through the fiber. The left image illustrates MMF. MMF supports multiple ways for the light from one source to travel through the fiber (the source of the designation “multimode”). Each path can be thought of as a mode.

For SMF, the possible ways for light to get through the fiber have been reduced to one, a “single mode.” It is not exactly one, but that is a useful approximation. Table 3-1 summarizes the characteristics of MMF and SMF.

Table 3-1 *Summarizing MMF and SMF Characteristics*

MMF Characteristics	SMF Characteristics
LED transmitter usually used	Larger transmitter usually used
Lower bandwidth and speed	Higher bandwidth and speed
Shorter distances	Longer distances
Less expensive	More expensive

An optical fiber connector terminates the end of an optical fiber. A variety of optical fiber connectors are available. The main differences among the types of connectors are dimensions and methods of mechanical coupling. Generally, organizations standardize on one kind of connector, depending on the equipment that they commonly use, or they standardize per type of fiber (one for MMF, one for SMF). Taking into account all the generations of connectors, about 70 connector types are in use today. Figure 3-21 shows some common connector types.

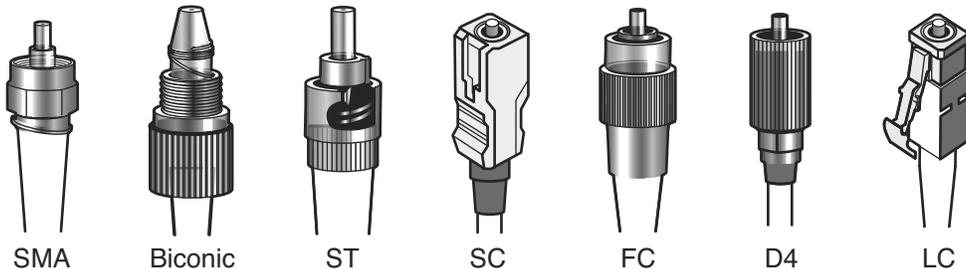


Figure 3-21 *Common Fiber-Optic Connector Types*

There are three types of connectors:

- Threaded
- Bayonet
- Push-pull

These materials are used for connectors:

- Metal
- Plastic sleeve

Most common connectors are classified as these types:

- **ST:** Typical for patch panels (for their durability)
- **FC:** Typical used by service providers for patch panels
- **SC:** Typical for enterprise equipment
- **LC:** Typical for enterprise equipment, commonly used on Small Form-Factor Pluggable (SFP) modules

In data communications and telecommunications applications today, small-form-factor connectors (for example, LCs) are replacing the traditional connectors (for example, SCs), mainly to pack more connectors on the faceplate and thus reduce system footprints.

Chapter Summary

LANs are a critical component in computer networks today. While these structures come in many different sizes, they are always used to carry data at speeds as fast as possible over short geographic distances.

Ethernet is the most common type of LAN used today. Standards unique to Ethernet specify Ethernet LAN cabling and signaling at both the physical and data link layers of the OSI reference model. Bits that are transmitted over an Ethernet LAN are organized into frames. Ethernet LANs manage the signals on a network using a process called CSMA/CD.

A NIC or LAN adapter plugs into a motherboard and provides an interface for connecting to the network. The MAC address is burned onto each NIC by the manufacturer, providing a unique, physical network address that permits the device to participate in the network.

The cable and connector specifications used to support Ethernet implementations are derived from the EIA/TIA standards body. The categories of cabling defined for Ethernet are derived from the EIA/TIA-568 (SP2840) Commercial Building Telecommunications Wiring Standards. Several connection media are used for Ethernet, with RJ-45 and GBIC being the most common.

A GBIC is a hot-swappable I/O device that plugs into a Gigabit Ethernet port on a network device to provide a physical interface.

UTP cable is a four-pair wire. Each of the eight individual copper wires in UTP cable is covered by an insulating material, and the wires in each pair are twisted around each other. A crossover cable connects between similar devices like router to router, PC to PC, or switch to switch. A straight-through cable connects between dissimilar devices like switch to router or PC to switch.

This chapter also examined fiber-optic media. Optical fiber is a flexible, transparent fiber that is made of very pure glass (silica) and is not much bigger than a human hair. It acts as a waveguide, or “light pipe,” to transmit light between the two ends of the fiber. Optical fibers are widely used in fiber-optic communications, which permit transmission over longer distances and at higher bandwidths (data rates) than other forms of communication.

Additional Resources

- Gigabit Ethernet, Wikipedia: http://en.wikipedia.org/wiki/Gigabit_Ethernet
- How Fiber Optics Work, How Stuff Works: <http://computer.howstuffworks.com/fiber-optic.htm>

Review Questions

Use the questions here to review what you learned in this chapter. The correct answers and solutions are found in Appendix A, “Answers to Chapter Review Questions.”

- 1.** What organization is responsible for Ethernet standards?
 - a.** ISO
 - b.** IEEE
 - c.** EIA
 - d.** IEC

- 2.** What are the characteristics of Ethernet 802.3? (Choose three.)
 - a.** Based on the CSMA/CD process
 - b.** Is a standard that has been replaced by Ethernet II
 - c.** Specifies the physical layer (Layer 1)
 - d.** Developed in the mid-1970s
 - e.** Specifies the MAC portion of the data link layer (Layer 2)
 - f.** Also referred to as thick Ethernet

- 3.** Which statement about an Ethernet address is accurate?
 - a.** The address used in an Ethernet LAN directs data to the proper receiving location.
 - b.** The source address is the 4-byte hexadecimal address of the NIC on the computer that is generating the data packet.
 - c.** The destination address is the 8-byte hexadecimal address of the NIC on the LAN to which a data packet is being sent.
 - d.** Both the destination and source addresses consist of a 6-byte hexadecimal number.

- 4.** Which statement about MAC addresses is accurate?
 - a.** A MAC address is a number in hexadecimal format that is physically located on the NIC.
 - b.** A MAC address is represented by binary digits that are organized in pairs.
 - c.** It is not necessary for a device to have a unique MAC address to participate in the network.
 - d.** The MAC address can never be changed.

- 5.** Which statement about NICs is accurate?
 - a.** The NIC plugs into a USB port and provides a port for connecting to the network.
 - b.** The NIC communicates with the network through a serial connection and communicates with the computer through a parallel connection.
 - c.** The NIC communicates with the network through a parallel connection and communicates with the computer through a serial connection.
 - d.** A NIC is also referred to as a switch adapter.

6. Which minimum category of UTP is required for Ethernet 1000BASE-T?
- a. Category 3
 - b. Category 4
 - c. Category 5
 - d. Category 5e
7. Match the UTP categories to the environments in which they are most commonly used.
- ___ 1. Category 1
 - ___ 2. Category 2
 - ___ 3. Category 3
 - ___ 4. Category 4
 - ___ 5. Category 5
 - ___ 6. Category 5e
 - ___ 7. Category 6
 - ___ 8. Category 6e
- a. Capable of transmitting data at speeds up to 100 Mbps
 - b. Used in networks running at speeds up to 1000 Mbps (1 Gbps)
 - c. Consists of four pairs of 24-gauge copper wires, which can transmit data at speeds up to 1000 Mbps
 - d. Used for telephone communications; not suitable for transmitting data
 - e. Used in Token Ring networks; can transmit data at speeds up to 16 Mbps
 - f. Capable of transmitting data at speeds up to 4 Mbps
 - g. Used in 10BASE-T networks; can transmit data at speeds up to 10 Mbps
 - h. Used in networks running at speeds up to 10 Gbps
8. Which type of UTP cable would you use to connect a router to a PC to have the devices pass user data?
- a. Straight-through
 - b. Crossover
 - c. Rollover
 - d. None of these options are correct.
9. Which type of UTP cable would you use to connect a switch to another switch?
- a. Straight-through
 - b. Crossover
 - c. Rollover
 - d. None of these options are correct.

- 10.** What type of optical fiber provides higher speeds and bandwidths?
- a.** MMF
 - b.** SMF
 - c.** MNF
 - d.** GMF

Production Network Simulation Question 3-1

Your colleague has come to you desperate for help. He needs to know what type of Ethernet cable he needs to use in each of these segments he is responsible for:

- 1.** The PC to the switch
- 2.** The switch to another switch
- 3.** The switch to a router
- 4.** The router to another router

None of these devices support the Auto-MDIX feature, so provide him with the correct cable type for each instance.

Index

Symbols

^ (caret symbol), 79

\$ (dollar sign), 80

(pound sign), 270

? command, 75-76, 79

/? parameter

arp command, 250

ipconfig command, 157

ping command, 249

" (quotation marks), 382

> (right-facing arrow), 75

802.1Q technology, 115-117

configuration, 123-126

frames, 116

native VLAN, 117

A

-a flag

arp command, 250

ping command, 248

abbreviations, 471-476

access attacks, 379

access control lists. *See* ACLs (access control lists)

access parameter (switchport mode command), 124

access-list access-list-number command, 357

access-list command, 409-412, 415-419, 423-424

accessing CLI (command-line interface), 71

acknowledgment (TCP), 210-211

ACLs (access control lists)

access control to routers, 413

classification and filtering, 392-394

comments, 425

dynamic ACLs, 401-402

explained, 391-394

extended ACLs, 398

identification, 398-400

named ACLs, 419-424

numbered extended IPv4 ACLs, 413-419

numbered standard IPv4 ACLs, 408-413

operation, 395-397

reflexive ACLs, 402-404

standard ACLs, 398

- time-based ACLs, 404-405
- troubleshooting, 425-429
- wildcard masking, 405-407

acronyms, 471-476

active attacks, 376

adding VLANs (virtual local-area networks), 129

address exhaustion, 150-153

address parameter

- ip route command, 288
- network command, 317
- show port-security command, 386

Address Resolution Protocol.
See ARP (Address Resolution Protocol)

address translation. *See* NAT (Network Address Translation)

addressing

- addressing services
 - DHCP (Dynamic Host Configuration Protocol), 154-155*
 - DNS (Domain Name System), 155-157*
- frame addressing, 52
- IP addresses
 - address classes, 143-145*
 - address exhaustion, 150-153*
 - assigning to switches, 96*
 - broadcast addresses, 145-149*
 - CIDR (classless interdomain routing), 152-153*
 - configuring for Cisco routers, 272-273*
 - determining, 155-157*
 - dotted-decimal notation, 142*
 - explained, 140-142*
 - IANA (Internet Assigned Numbers Authority), 149*

- network addressing scheme determination, 179-180*
- obtaining, 149*
- private IP addresses, 149-150*
- public IP addresses, 149-150*
- subnets. *See* subnets*
- two-level and three-level addresses, 169*

IPv6

- address allocation, 446-447*
- address types, 444-445*
- explained, 151-152, 441-443*
- features, 443-444*
- headers, 447-448*
- ICMPv6, 449*
- neighbor discovery, 449*
- routing, 450-453*
- stateless autoconfiguration, 449-450*

Layer 2 addressing

- explained, 235-236*
- mapping Layer 2 addressing to Layer 3 addressing, 237-238*

Layer 3 addressing

- explained, 236-237*
- mapping to Layer 2 addressing, 237-238*

MAC addresses, 52-54, 235-236

NAT (Network Address Translation), 442-443

- benefits of, 349*
- dynamic NAT (Network Address Translation), 349*
- explained, 343, 347-350*
- inside source address translation, 350-354*
- overloading, 349, 355-359*

- PAT (Port Address Translation)*, 349-350
 - static NAT*, 349, 353-354
 - translation table issues, resolving*, 359-362
 - verifying translation*, 361-367
 - administrative distance**, 296-297
 - adversaries**, 376
 - /all parameter (ipconfig)**, 156
 - allocating IPv6 addresses**, 446-447
 - % Ambiguous command (error message)**, 78
 - anycast addresses**, 444
 - application layer**
 - OSI (Open Systems Interconnection) model, 29
 - TCP/IP protocol stack, 36
 - applications**
 - batch applications, 8
 - collaboration, 8
 - databases, 8
 - email, 7
 - impact of, 8-9
 - instant messaging, 8
 - interactive applications, 8-9
 - real-time applications, 9
 - web browsers, 7
 - applying subnet masks**, 178
 - area**, 303
 - area ID**, 314
 - area-id parameter (network)**, 317
 - areas**, 313
 - ARP (Address Resolution Protocol)**
 - ARP table, 238
 - host-to-host packet delivery, 238-247
 - mapping Layer 2 addressing to Layer 3 addressing, 237-238
 - arp command**, 250
 - AS (autonomous system)**, 303, 313
 - assigning**
 - IP addresses to switches, 96
 - names to Cisco routers, 269-270
 - VLAN ports, 128-130
 - attacks**, 376-377
 - access attacks, 379
 - active attacks, 376
 - close-in attacks, 377
 - distributed attacks, 377
 - insider attacks, 377
 - passive attacks, 376
 - reconnaissance attacks, 378-379
 - authentication (OSPF)**
 - explained, 328
 - MD5 authentication, 329
 - plaintext password authentication, 329-332, 337-338
 - Auto-MDIX**, 62
 - automatic IP address allocation**, 344
 - autonegotiation**, 101-102
 - autonomous system (AS)**, 303, 313
 - AutoSecure**, 260-262
 - availability**, 10
- ## B
-
- balanced hybrid routing**, 296
 - balancing**
 - load via OSPF (Open Shortest Path First), 326-328
 - network security requirements, 375-376
 - bandwidth as routing metric**, 226
 - banner motd command**, 270

banners, login, 382-383
 base 2 conversion system, 164
 basic IPv6 connectivity, 451-452
 batch applications, 8
 begin parameter
 show command, 85
 show port-security command, 386
 binary numbering
 base 2 conversion system, 164
 binary-hexadecimal numbers, 53-54
 binary-to-decimal conversion,
 166-167
 decimal versus binary numbering, 162
 decimal-to-binary conversion,
 165-166
 explained, 162
 LSB (least significant bit), 163
 MSB (most significant bit), 163
 powers of 2, 164-165
 binary-to-decimal conversion,
 166-167
 bit spitters, 89
 BOOTP (Bootstrap Protocol), 155
 Bootstrap Protocol (BOOTP), 155
 branch offices, 3
 Bring Your Own Device (BYOD), 3
 broadcast addresses, 145-149
 broadcast domains, 113
 broadcast storms, 132
 broadcast transmission, 52
 bus topology, 13
 BYOD (Bring Your Own Device), 3

C

calculating VLSM (variable-length
 subnet masks), 186
 caret symbol (^), 79
 carrier sense multiple access with
 collision detection (CSMA/CD),
 49-50
 Catalyst switches. *See* switches
 categories of UTC (unshielded
 twisted-pair) cable, 58
 CDP (Cisco Discovery Protocol),
 273-280
 channel service unit (CSU), 19
 CIDR (classless interdomain routing),
 149, 152-153, 442
 Cisco AutoSecure, 260-262
 Cisco device security
 password security, 380-382
 physical and environmental
 threats, 380
 port security, 384-387
 Telnet versus SSH access, 383
 Cisco Discovery Protocol (CDP),
 273-280
 Cisco IOS Software, 75
 Cisco IOS configuration manage-
 ment, 81-84
 CLI (command-line interface). *See*
 also commands
 accessing, 71
 command history, 81
 enhanced editing commands,
 79-80
 entering commands into, 71
 error messages, 78
 functions, 71-72
 help, 77-79
 improving user experience in,
 84-85
 shortcut keys, 80

cable Internet connections, 18-19
 cables, UTP (unshielded twisted-pair),
 58-61

- EXEC modes
 - entering*, 75-77
 - explained*, 72
 - privileged EXEC mode*, 72
 - user EXEC mode*, 72
- external configuration sources, 73-75
- features and functions, 70-71
- network device configuration, 72-73
- Cisco routers**
 - configuration
 - from CLI (command-line interface)*, 269-270
 - configuration modes*, 268-269
 - interfaces*, 271-272
 - IP addresses*, 272-273
 - MOTD (message-of-the-day) banner*, 270
 - verifying interface configuration*, 273-277
 - verifying neighbor device configuration*, 277-280
 - as DHCP clients, 345
 - as DHCP relay agents, 347
 - as DHCP servers, 345-346
 - initial setup, 257-263
 - additional configuration prompts*, 259
 - Cisco AutoSecure*, 260-262
 - configuration command script*, 262-263
 - default settings and global parameters*, 258-259
 - FastEthernet 0/0*, 259
 - interface statuses*, 258
 - setup mode, entering*, 257-258
 - initial startup, 256
 - initial status, verifying, 266-267
 - logging in to, 263-265
 - naming, 269-270
- Cisco Switch Hardware Installation Guide**, 93
- Class A addresses (IP)**, 143-145
- Class A subnets**
 - computing hosts for, 172-173
 - example, 183-184
- Class B addresses (IP)**, 143-145
- Class B subnets**
 - computing hosts for, 171-172
 - example, 181-182
- Class C addresses (IP)**, 144-145
- Class C subnets**
 - computing hosts for, 170-171
 - example, 180-181
- Class D addresses (IP)**, 144
- Class E addresses (IP)**, 144
- classes of attack, 376-377
- classful routing, 297-298
- classless interdomain routing (CIDR), 149, 152-153, 297-298, 442
- clear ip nat translation command**, 359
- CLI (command-line interface)**. *See also* **commands**
 - accessing, 71
 - Cisco router configuration, 269-270
 - command history, 81
 - enhanced editing commands, 79-80
 - entering commands into, 71
 - error messages, 78
 - EXEC modes
 - entering*, 75-77
 - explained*, 72

- privileged EXEC mode*, 72
- user EXEC mode*, 72
- external configuration sources, 73-75
- functions, 71-72
- help, 77-79
- improving user experience in, 84-85
- network device configuration, 72-73
- shortcut keys, 80
- client mode (VTP)**, 119
- clients, Cisco routers as DHCP clients**, 345
- close-in attacks**, 377
- collaboration**, 8
- collisions**, 103-105
- Collisions parameter (show interface comma)**, 106
- command history**, 81
- command-line interface (CLI)**. *See* CLI (command-line interface)
- commands**
 - ? command, 75-76, 79
 - access-list, 409-412, 415-419, 423-424
 - access-list access-list-number, 357
 - arp, 250
 - banner motd, 270
 - clear ip nat translation, 359
 - command history, 81
 - configure terminal, 272
 - copy, 83
 - copy running-config startup-config, 83
 - copy running-config tftp, 83
 - debug ip nat, 360
 - debug ip ospf adj, 338
 - debug ip ospf events, 323-325
 - debug ip ospf packet, 325
 - description, 271
 - enhanced editing commands, 79-80
 - entering into CLI (command-line interface), 71
 - exec-timeout, 270
 - exit, 270, 273
 - global commands, 268
 - hostname, 270
 - interface, 409, 417
 - ip access-group, 408-409, 416-417, 420
 - ip access-list extended, 421
 - ip access-list standard, 420
 - ip address, 273
 - ip nat inside source, 354, 357
 - ip nat inside source static, 352
 - ip nat pool, 353
 - ip ospf authentication, 329-330
 - ip ospf authentication command, 329
 - ip route, 288-289
 - ipconfig, 155-157
 - logging synchronous, 270
 - major commands, 269
 - name vlan-name, 126
 - no access-list, 409
 - no access-list access-list-number, 357
 - no description, 271
 - no ip access-group, 408-409
 - no ip nat inside source, 354
 - no ip nat inside source static, 352
 - no ip nat pool, 353
 - no no ip nat inside source, 357
 - no shutdown, 273
 - ping, 248-249

- setup, 263
- show, 84-85
- show access-list, 365
- show access-lists, 416
- show cdp entry, 279
- show cdp neighbors detail, 279
- show interface, 103-106
- show interfaces, 98, 129, 273-277
- show ip access-list, 425
- show ip interface, 426
- show ip nat statistics, 360-363
- show ip nat translation, 357-358, 364-365
- show ip ospf, 319-321
- show ip ospf interface, 321-322
- show ip ospf neighbor, 322-324
- show ip protocol, 366
- show ip route, 290, 318-320, 328, 365-366
- show port-security interface, 385-386
- show running-config, 82
- show startup-config, 82
- show version, 266-267
- show vlan, 128
- show vlan brief, 128
- show vlan id vlan_number, 127
- show vlan name vlan-name, 127
- shutdown, 271
- switchport access, 128
- switchport mode, 124
- traceroute, 251
- vlan vlan-id, 126
- comments, adding to ACLs, 425**
- communication link options (WANs), 437-438**
- Computer Security Institute (CSI), 372**

computing subnet hosts

- Class A subnets, 172-173
- Class B subnets, 171-172
- Class C subnets, 170-171

configuration

- ACLs (access control lists), 408
 - access control to routers, 413*
 - comments, 425*
 - dynamic ACLs, 401-402*
 - named ACLs, 419-424*
 - numbered extended IPv4 ACLs, 413-419*
 - numbered standard IPv4 ACLs, 408-413*
 - reflexive ACLs, 402-404*
 - time-based ACLs, 404-405*
 - wildcard masking, 405-407*
- binary-to-decimal conversion, 166-167
- Cisco IOS configuration management, 81-84
- Cisco routers, 257-263
 - additional configuration prompts, 259*
 - Cisco AutoSecure, 260-262*
 - from CLI (command-line interface), 269-270*
 - configuration command script, 262-263*
 - configuration modes, 268-269*
 - default settings and global parameters, 258-259*
 - as DHCP clients, 345*
 - as DHCP relay agents, 347*
 - as DHCP servers, 345-346*
 - FastEthernet 0/0, 259*
 - interface statuses, 258*

- interfaces*, 271-272
- IP addresses*, 272-273
- MOTD (message-of-the-day) banner*, 270
- setup mode, entering*, 257-258
- verifying interface configuration*, 273-277
- verifying neighbor device configuration*, 277-280
- default gateways, 96
- default route forwarding, 290
- external configuration sources, 73-75
- IPv6 routing, 449-450
 - OSPFv3*, 452-453
 - static routing*, 452
- login banner, 382-383
- network devices, 72-73
- OSPF (Open Shortest Path First), 316-317
- password security, 380-382
- plaintext password authentication, 329-332
- point-to-point links, 438-439
- port security, 384-387
- router on a stick, 135
- static routing, 288-289
- switches, 95-97
- VLANs (virtual local-area networks)
 - 802.1Q technology*, 123-126
 - port assignment*, 128-130
 - VLAN creation*, 126-128
 - VTP (VLAN Trunking Protocol)*, 122
- VTP (VLAN Trunking Protocol), 122
- configuration files**
 - copying, 82-83
 - saving to NVRAM, 269
- configure terminal command**, 272
- connection components for Ethernet LANs**
 - Auto-MDIX, 62
 - connection media, 55-57
 - media and connection requirements, 55
 - NICs (network interface cards), 54-55
 - optical fiber, 62-64
 - UTP (unshielded twisted-pair) cable, 58-61
- console port**, 221
 - connecting switches to, 94-95
- console terminals, configuring devices with**, 74
- convergence time**, 224
- conversions, decimal-to-binary**, 165-166
- copy command**, 83
- copy running-config startup-config command**, 83
- copy running-config tftp: command**, 83
- copying configuration files**, 82-83
- cost**
 - of networks, 10
 - as routing metric, 226
- CPE (customer premises equipment)**, 19
- CRC (cyclic redundancy check) errors**, 103
- CRC parameter (show interface comma)**, 106
- CSI (Computer Security Institute)**, 372
- CSMA/CD (carrier sense multiple access with collision detection)**, 49-50

CSU (channel service unit), 19
 customer premises equipment (CPE), 19
 cyclic redundancy check (CRC) errors, 103

D

-d flag

arp command, 250
 traceroute command, 251

data and pad field (Ethernet frames), 51

data communications process

deencapsulation, 33-34
 encapsulation, 32
 explained, 31-32

data containers (TCP/IP), 201-202

Data Link Connection Identifier (DLCI), 236

data link layer (OSI), 31

databases, 8

datagrams, 201

dead intervals, 314

debug commands (OSPF), 323-325

debug ip nat command, 360

debug ip ospf adj command, 338

debug ip ospf events command, 323-325

debug ip ospf packet command, 325

DEC (Digital Equipment Corporation), 48

decimal versus binary numbering, 162

decimal-to-binary conversion, 165-166

dedicated communication links, 437

deencapsulation, 33-34

default gateways, 247

configuring, 96
 verifying, 363-364

default route forwarding, 290

default routing, 222, 225

default settings for Cisco routers, 258-259

delay, 226

deleting VLANs (virtual local-area networks), 130

description command, 271

design considerations for VLANs (virtual local-area networks), 130-131

destination address field (Ethernetframes), 51

Destination Address field (IPv6 header), 448

determining IP addresses, 155-157

device security

password security, 380-382
 physical and environmental threats, 380
 port security, 384-387
 Telnet versus SSH access, 383

DHCP (Dynamic Host Configuration Protocol), 154-155

automatic allocation, 344
 Cisco routers as DHCP clients, 345
 Cisco routers as DHCP relay agents, 347
 Cisco routers as DHCP servers, 345-346

DHCPACK message, 345

DHCPDISCOVER message, 344

DHCPOFFER message, 345

DHCPREQUEST message, 345

- dynamic allocation, 344
- explained, 343-345
- manual allocation, 344
- DHCPACK message, 345
- DHCPDISCOVER message, 344
- DHCPOFFER message, 345
- DHCPREQUEST message, 345
- diagrams, network, 5-7
- Digital Equipment Corporation (DEC), 48
- digital service unit (DSU), 19
- digital subscriber line (DSL), 18-19
- Dijkstra, Edsger, 302
- directly connected routes, 224
- /displaydns parameter (ipconfig), 156
- displaying VTP (VLAN Trunking Protocol) status, 123
- distance parameter (ip route), 288
- distance vector routing, 226-227, 295, 299-300
- distributed attacks, 377
- DIX Ethernet, 48
- DLCI (Data Link Connection Identifier), 236
- DNS (Domain Name System), 155-157
- dns-timeout parameter (ip nat translation), 362
- dollar sign (\$), 80
- Domain Name System (DNS), 155-157
- dotted-decimal notation, 142
- DSL (digital subscriber line), 18-19
- DSU (digital service unit), 19
- dual-ring topology, 17
- duplex communication, 100-102
- dynamic ACLs, 401-402
- dynamic address translation, 354

- dynamic auto parameter (switchport mode command), 124
- dynamic desirable parameter (switchport mode command), 124
- Dynamic Host Configuration Protocol. *See* DHCP (Dynamic Host Configuration Protocol)
- dynamic IP address allocation, 344
- dynamic NAT (Network Address Translation), 349
- dynamic routing, 224
 - balanced hybrid routing, 296
 - classful versus classless routing, 297-298
 - compared to static routing, 287
 - distance vector routing, 226-227, 295, 299-300
 - example: administrative distance, 296-297
 - explained, 293-296
 - IGP (interior gateway protocols), 295
 - link-state routing, 227, 296, 300-307
 - advantages of*, 302, 306, 307
 - IS-IS (Intermediate System-to-Intermediate System)*, 301
 - limitations*, 307
 - LSA (link-state advertisements)*, 301
 - network hierarchy*, 302-304
 - OSFP (Open Shortest Path First)*, 301
 - SPF (shortest path first) algorithms*, 302-306
 - routing metrics, 225-226

E

- echo request packets, 248
- echo response replies, 248

EGP (exterior gateway protocols), 295
 EIGRP (Enhanced Interior Gateway Routing Protocol), 223, 228
 email, 7
 encapsulation, 32
 endpoints, 4
 enhanced editing commands, 79-80
 Enhanced Interior Gateway Routing Protocol (EIGRP), 223, 228
 entering EXEC modes, 75-77, 263-264
 enterprise environment, 47
 environmental security, 380
 equal-cost load balancing, 326-328
 errors

- cyclic redundancy check (CRC) errors, 103
- error messages in CLI (command-line interface), 78

 Ethernet LANs, 47

- Auto-MDIX, 62
- connection media, 55-57
- CSMA/CD (carrier sense multiple access with collision detection), 49-50
- development of, 48
- frame addressing, 52
- frames, 50-51
- MAC addresses, 52-54
- media and connection requirements, 55
- NICs (network interface cards), 54-55
- optical fiber, 62-64
- standards, 48-49
- UTP (unshielded twisted-pair) cable, 58-61

EUI-64 standard, 445
 evanescent wave, 102
 exclude parameter

- show command, 85
- show port-security command, 386

 EXEC modes

- entering, 75-77
- explained, 72
- privileged EXEC mode
 - entering*, 263-264
 - explained*, 72, 263
 - help*, 265
- user EXEC mode
 - entering*, 264
 - explained*, 72, 263
 - help*, 264

 exec-timeout command, 270
 exit command, 270, 273
 expression parameter (show port-security command), 386
 extended ACLs, 398
 extended-star topology, 15-16
 exterior gateway protocols (EGP), 295
 external configuration sources, 73-75

F

-f flag (ping), 249
 failure domains, 113
 FastEthernet 0/0, 259
 FCS (frame check sequence), 51
 fiber-optic GBIC, 56-57
 File Transfer Protocol (FTP), 199
 files, configuration

- copying, 82-83
- saving to NVRAM, 269

filtering show command outputs, 84-85
 finrst-timeout parameter (ip nat translation), 358
 fixed windowing, 211-213
 Flash memory, 81
 flow control (TCP/UDP), 209-210
 Flow Label field (IPv6 header), 448
 /flushdns parameter (ipconfig), 156
 forwarding, default route forwarding, 290
 frames, 50-51, 201

- 802.1Q technology, 116
- frame addressing, 52
- frame buffers (switches), 92
- frame check sequence (FCS), 51
- multiple frame transmission, 132

 FTP (File Transfer Protocol), 199
 full duplex communication, 101
 full-mesh topology, 17

G

-g flag (arp), 250
 gateways

- default gateways, 247
 - configuring*, 96
 - verifying*, 363-364
- gateway IP address (GIADDR), 347

 GBIC (Gigabit Interface Converter), 56
 GIADDR (gateway IP address), 347
 Giants parameter (show interface comma), 106
 Gigabit Interface Converter (GBIC), 56
 global commands, 268

global parameters for Cisco routers, 258-259
 global synchronization, 214
 global unicast addresses, 444

H

-h flag (traceroute), 251
 hacker motivations, 376
 half-duplex communication, 100-101
 HDLC (High-Level Data Link Control), 439
 headers

- IP headers, 141
- IPv6, 447-448
- TCP/UDP header formats, 202-204

 hello intervals, 314
 help

- in CLI (command-line interface), 77-79
- in privileged EXEC mode, 265
- in user EXEC mode, 264

 hierarchy, OSPF (Open Shortest Path First), 312
 High-Level Data Link Control (HDLC), 439
 history (command), 81
 home offices, 3
 hop count, 226
 Hop Limit field (IPv6 header), 448
 host connectivity, troubleshooting, 427-429
 host ID, 141
 host-to-host communications model, 26-27
 host-to-host packet delivery, 238-247

- hostname command, 270
 - hostname> prompt, 76
 - hosts, computing for subnets
 - Class A subnets, 172-173
 - Class B subnets, 171-172
 - Class C subnets, 170-171
 - hubs, 46
-
- I**
 - i flag (ping), 249
 - IANA (Internet Assigned Numbers Authority), 149, 295
 - ICMP (Internet Control Message Protocol), 248
 - ICMPv6, 449
 - icmp-timeout parameter (ip nat translation), 358
 - ICMPv6, 449
 - identification of ACLs (access control lists), 398-400
 - IEEE (Institute of Electrical and Electronics Engineers), 48
 - IETF (Internet Engineering Task Force), 144. *See also* OSPF (Open Shortest Path First)
 - IGP (interior gateway protocols), 295. *See also* OSPF (Open Shortest Path First)
 - incomplete command (error message), 78
 - impact of user applications, 8-9
 - include parameter
 - show command, 85
 - show port-security command, 386
 - initial sequence numbers (ISN), 205
 - initial startup status, verifying
 - Cisco routers, 266-267
 - switches, 97-99
 - Input Errors parameter (show interface comma), 106
 - inside global addresses
 - definition of, 349
 - overloading, 355-359
 - inside local addresses, 349
 - inside source address translation, 350-354
 - dynamic address translation, 354
 - static NAT address mapping, 353-354
 - insider attacks, 377
 - installing switches, 93
 - instant messaging, 8
 - Institute of Electrical and Electronics Engineers (IEEE), 48
 - Intel, 48
 - Inter-Switch Link (ISL) trunks, 115
 - interactive applications, 8-9
 - interconnections, 5
 - interface command, 409, 417
 - interface interface-id parameter (show port-security command), 386
 - interface parameter (ip route), 288
 - interfaces, configuring for Cisco routers, 271-272
 - interior gateway protocols (IGP), 295. *See also* OSPF (Open Shortest Path First)
 - Intermediate System-to-Intermediate System (IS-IS), 227, 301
 - internal switching, 92
 - Internet Assigned Numbers Authority (IANA), 149, 295
 - Internet connections, 18-19

Internet Control Message Protocol (ICMP), 248

ICMPv6, 449

Internet Engineering Task Force (IETF), 144. *See also* OSPF (Open Shortest Path First)

Internet layer (TCP/IP), 36

address classes, 143-145

address exhaustion, 150-153

address format, 140-142

broadcast addresses, 145-149

CIDR (classless interdomain routing), 152-153

determining IP addresses, 155-157

DHCP (Dynamic Host Configuration Protocol), 154-155

DNS (Domain Name System), 155-157

dotted-decimal notation, 142

explained, 140

IANA (Internet Assigned Numbers Authority), 149

IPv6 addresses, 151-152

network addresses, 145-149

obtaining IP addresses, 149

private IP addresses, 149-150

public IP addresses, 149-150

Internet Layer Video, 158

interpreting network diagrams, 5-7

invalid input detected at '^' marker (error message), 78

IOS Software. *See* Cisco IOS Software

ip access-group command, 408-409, 416-417, 420

ip access-list extended command, 421

ip access-list standard command, 420

ip address command, 273

IP addresses

address classes, 143-145

address exhaustion, 150-153

address format, 140-142

addressing services

DHCP (Dynamic Host Configuration Protocol), 154-155

DNS (Domain Name System), 155-157

assigning to switches, 96

broadcast addresses, 145-149

CIDR (classless interdomain routing), 152-153

configuring for Cisco routers, 272-273

determining, 155-157

dotted-decimal notation, 142

IANA (Internet Assigned Numbers Authority), 149

IPv6

address allocation, 446-447

address types, 444-445

explained, 151-152, 441-443

features, 443-444

headers, 447-448

ICMPv6, 449

neighbor discovery, 449

routing, 450-453

stateless autoconfiguration, 449-450

NAT (Network Address Translation), 442-443

benefits of, 349

dynamic NAT (Network Address Translation), 349

- explained*, 343, 347-350
- inside source address translation*, 350-354
- overloading*, 349, 355-359
- PAT (Port Address Translation)*, 349-350
- static NAT*, 349, 353-354
- translation table issues, resolving*, 359-362
- verifying translation*, 361-367
- network addresses, 145-149
- obtaining, 149
- private IP addresses, 149-150
- public IP addresses, 149-150
- subnets, 161
 - advantages of*, 167-169
 - binary numbering*, 162-167
 - Class A example*, 183-184
 - Class B example*, 181-182
 - Class C example*, 180-181
 - computing hosts for*, 170-173
 - creating*, 170
 - network addressing scheme determination*, 179-180
 - subnet masks*, 173-178
 - two-level and three-level addresses*, 169
 - VLSM (variable-length subnet masks)*, 184-191
- ip nat inside source command**, 354, 357
- ip nat inside source static command**, 352
- ip nat pool command**, 353
- ip ospf authentication command**, 329-330
- ip route command**, 288-289

- ipconfig command**, 155-157
- IPv6**
 - address allocation, 446-447
 - address types, 444-445
 - explained, 151-152, 441-443
 - features, 443-444
 - headers, 447-448
 - ICMPv6, 449
 - neighbor discovery, 449
 - routing, 450-451
 - basic IPv6 connectivity*, 451-452
 - OSPFv3*, 452-453
 - static routing*, 452
 - stateless autoconfiguration, 449-450
- IS-IS (Intermediate System-to-Intermediate System)**, 227, 301
- ISL (Inter-Switch Link) trunks**, 115
- ISN (initial sequence numbers)**, 205

J-K

- j flag**
 - ping command, 249
 - traceroute command, 251
- jitter**, 9
- k flag (ping)**, 249

L

- l flag (ping)**, 248
- LANs (local area networks)**
 - communication and resource-sharing functions, 46-47
 - compared to WANs (wide area networks), 435-436

- components, 45-46
- definition of, 44-45
- Ethernet LANs, 47
 - Auto-MDIX*, 62
 - connection media*, 55-57
 - CSMA/CD (carrier sense multiple access with collision detection)*, 49-50
 - development of*, 48
 - frame addressing*, 52
 - frames*, 50-51
 - MAC addresses*, 52-54
 - media and connection requirements*, 55
 - NICs (network interface cards)*, 54-55
 - optical fiber*, 62-64
 - standards*, 48-49
 - UTP (unshielded twisted-pair) cable*, 58-61
- physical redundancy, 131-133
- size, 47
- VLANs (virtual local-area networks)
 - 802.1Q technology*, 115-117
 - adding*, 129
 - configuration*, 122
 - creating*, 126-128
 - deleting*, 130
 - design considerations*, 130-131
 - modifying*, 130
 - overview*, 111-115
 - poorly designed networks*, 112-113
 - routing between*, 133-136
 - VID (VLAN ID)*, 116
 - VTP (VLAN Trunking Protocol)*, 117-121
- late collisions, 105
- Late Collisions parameter (show interface comma), 106
- latency, 9
- Layer 1 devices, 234
- Layer 2 addressing
 - explained, 235-236
 - mapping to Layer 3 addressing, 237-238
- Layer 2 devices, 234
- Layer 3 addressing
 - explained, 236-237
 - mapping to Layer 2 addressing, 237-238
- Layer 3 devices, 236
- layers (OSI)
 - application layer, 29
 - data link layer, 31
 - explained, 27-29
 - network layer, 30
 - physical layer, 31
 - presentation layer, 29
 - session layer, 29-30
 - transport layer, 30
- layers (TCP/IP), 35-36
- least significant bit (LSB), 163
- LED indicators (switches), 93-94
- Link Layer Discovery Protocol (LLDP), 278
- link-state advertisements (LSA), 301
- link-state packets (LSPs), 304-306
- link-state routing, 227, 296, 300-307
 - additional resources, SPF (shortest path first) algorithms, 339
 - advantages of, 302, 306-307
 - IS-IS (Intermediate System-to-Intermediate System), 301
 - limitations, 307

LSA (link-state advertisements), 301
network hierarchy, 302-304
OSPF (Open Shortest Path First), 301
areas, 313
authentication, 328-332
autonomous system (AS), 313
configuration, 316-317
debug commands, 323-325
explained, 311-313
hierarchy, 312
load balancing, 326-328
loopback interfaces, 317-318
neighbor adjacencies, 313-315
SPF (shortest path first) algorithms, 302-306, 315-316
troubleshooting, 329-338
verifying configuration of, 318

lists, access control. *See* ACLs
(access control lists)

LLC (logical link control) sublayer, 49

LLDP (Link Layer Discovery Protocol), 278

load balancing (OSPF), 326-328

local area networks. *See* LANs (local area networks)

local-link addresses, 445

logging in to Cisco routers, 263-265

logging synchronous command, 270

logical link control (LLC) sublayer, 49

logical topologies, 12

login banner, 382-383

loop resolution, 132

loopback addresses, 445

LSA (link-state advertisements), 301

LSB (least significant bit), 163

LSPs (link-state packets), 304-306

M

MAC addresses, 52-54, 235-236

MAC database instability, 132

MAC sublayer, 49

MAC tables, 91

macrobends, 102

main offices, 3

major commands, 269

management of Cisco IO
configuration, 81-84

manual IP address allocation, 344

mapping Layer 2 addressing to
Layer 3 addressing, 237-238

mask parameter (ip route), 288

maximum transmission unit
(MTU), 209

MD5 authentication, 329

media, 46
for Ethernet LANs, 55-57
media and connection requirements
for for Ethernet LANs, 55
troubleshooting, 102-106

memory
Flash memory, 81
NVRAM, 81
RAM, 81
ROM, 81

mesh topologies
full-mesh topology, 17
partial-mesh topology, 18

message-of-the-day (MOTD)
banner, 270

messages
DHCPACK, 345
DHCPDISCOVER, 344
DHCPOFFER, 345

- DHCPREQUEST, 345
- IPv6, 449
- TCP/IP messages, 201
- metrics (routing), 225-226
- mitigating threats. *See* threat mitigation
- MMF (multimode fiber), 63
- mobile users, 3
- modifying VLANs (virtual local-area networks), 130
- most significant bit (MSB), 163
- MOTD (message-of-the-day) banner, 270
- MSB (most significant bit), 163
- MTU (maximum transmission unit), 209
- multicast addresses, 144, 444
- multicast transmission, 52
- multilayer switches, 136
- multimode fiber (MMF), 63
- multiple frame transmission, 132
- multiplexing (session), 208-209

N

- n flag (ping), 248
- name vlan-name command, 126
- named ACLs, 419-424
- naming Cisco routers, 269-270
- NAT (Network Address Translation), 442-443
 - benefits of, 349
 - dynamic NAT (Network Address Translation), 349
 - explained, 343, 347-350
 - inside source address translation, 350-354
 - dynamic address translation*, 354
 - static NAT address mapping*, 353-354
 - overloading, 349, 355-359
 - PAT (Port Address Translation), 349-350
 - static NAT, 349, 353-354
 - translation table issues, resolving, 359-362
 - verifying translation, 361-367
- native 802.1Q VLAN (virtual local-area network), 117
- neighbor adjacencies
 - establishing, 313-315
 - troubleshooting, 333-335
- neighbor device configuration, verifying, 277-280
- neighbor discovery (IPv6), 449
- network access layer (TCP/IP), 36
- Network Address Translation. *See* NAT (Network Address Translation)
- network addresses, 145-149
- network command, 316-317
- network diagrams, interpreting, 5-7
- network ID, 141
- network interface cards (NICs), 5, 46, 54-55
- network layer (OSI), 30
- network media, 46
- network operating systems (NOS), 235
- network parameter (ip route), 288
- network service access point (NSAP), 236

networks

- ACLs (access control lists), 398-400
 - access control to routers*, 413
 - classification and filtering*, 392-394
 - comments*, 425
 - dynamic ACLs*, 401-402
 - explained*, 391-394
 - extended ACLs*, 398
 - identification*, 398-400
 - named ACLs*, 419-424
 - numbered extended IPv4 ACLs*, 413-419
 - numbered standard IPv4 ACLs*, 408-413
 - operation*, 395-397
 - reflexive ACLs*, 402-404
 - standard ACLs*, 398
 - time-based ACLs*, 404-405
 - troubleshooting*, 425-429
 - wildcard masking*, 405-407
- addressing. *See* addressing
- addressing services
 - DHCP (Dynamic Host Configuration Protocol)*, 154-155
 - DNS (Domain Name System)*, 155-157
- availability, 10
- characteristics of, 10-11
- cost, 10
- definition of, 2-4
- endpoints, 4
- interconnections, 5
- Internet connections, 18-19

IP addresses

- address classes*, 143-145
 - address exhaustion*, 150-153
 - address format*, 140-142
 - assigning to switches*, 96
 - broadcast addresses*, 145-149
 - CIDR (classless interdomain routing)*, 152-153
 - determining*, 155-157
 - dotted-decimal notation*, 142
 - IANA (Internet Assigned Numbers Authority)*, 149
 - IPv6 addresses*, 151-152
 - NAT (Network Address Translation)*. *See* NAT (Network Address Translation)
 - network addresses*, 145-149
 - obtaining*, 149
 - private IP addresses*, 149-150
 - public IP addresses*, 149-150
- LANs (local area networks)
- communication and resource-sharing functions*, 46-47
 - compared to WANs (wide area networks)*, 435-436
 - components*, 45-46
 - definition of*, 44-45
 - Ethernet*. *See* Ethernet LANs
 - physical redundancy*, 131-133
 - size*, 47
 - VLANs (virtual local-area networks)*. *See* VLANs (virtual local-area networks)
- network device configuration, 72-73
 - network diagrams, interpreting, 5-7
 - open networks, 373

OSI (Open Systems Interconnection) model

- application layer*, 29
- compared to TCP/IP protocol stack*, 36-37
- data communications process*, 31-34
- data link layer*, 31
- explained*, 27-29
- host-to-host communications model*, 26-27
- LLC (logical link control) sub-layer, 49
- MAC sublayer, 49
- network layer*, 30
- peer-to-peer communication*, 34-35
- physical layer*, 31
- presentation layer*, 29
- session layer*, 29-30
- transport layer*, 30

packet delivery process

- arp command*, 250
- ARP table*, 238
- default gateways*, 247
- host-to-host packet delivery*, 238-247
- Layer 1 devices*, 234
- Layer 2 addressing*, 235-236
- Layer 2 devices*, 234
- Layer 3 addressing*, 236-237
- Layer 3 devices*, 236
- mapping Layer 2 addressing to Layer 3 addressing*, 237-238
- ping command*, 248-249
- traceroute command*, 251
- TRACERT, 250-251

protocols. *See* protocols

reliability, 11

routers

- Cisco routers. See Cisco routers*
- controlling access to via ACLs*, 413
- definition of*, 5
- explained*, 220-222
- priority*, 315
- router ID*, 314
- router on a stick*, 134-135
- use of subnet masks*, 174-176
- in WANs (wide area networks)*, 437

routing, 219

- default routing*, 225
- directly connected routes*, 224
- distance vector routing*, 226-227
- dynamic routing. See dynamic routing*
- explained*, 219
- link-state routing*, 227
- path determination*, 221-223
- route summarization*, 187-191
- routers*, 220-222
- routing metrics*, 225-226
- routing tables*, 223-224
- static routing. See static routing*
- between VLANs (virtual local-area networks)*, 133-136

scalability, 10

security

- access attacks*, 379
- adversaries*, 376
- balancing network security requirements*, 375-376
- classes of attack*, 376-377

- explained*, 371-372
- hacker motivations*, 376
- need for*, 372-375
- overview*, 10
- password attacks*, 379-380
- password security*, 380-382
- physical and environmental threats*, 380
- physical installations*, 377-378
- port security*, 384-387
- reconnaissance attacks*, 378-379
- Telnet versus SSH access*, 383
- speed, 10
- subnets, 161
 - advantages of*, 167-169
 - binary numbering*, 162-167
 - Class A example*, 183-184
 - Class B example*, 181-182
 - Class C example*, 180-181
 - computing hosts for*, 170-173
 - creating*, 170
 - network addressing scheme determination*, 179-180
 - subnet masks*, 173-178
 - two-level and three-level addresses*, 169
 - VLSM (variable-length subnet masks)*, 184-191, 442
- switches, 46
 - assigning IP addresses to*, 96
 - characteristics of*, 92
 - configuring*, 95-97
 - connecting to console port*, 94-95
 - definition of*, 5
 - duplex communication*, 100-102
 - initial startup status, verifying*, 97-99
 - installing*, 93
 - LED indicators*, 93-94
 - multilayer switches*, 136
 - need for*, 90-92
 - switching operation*, 99
 - troubleshooting*, 102-107
- TCP/IP protocol stack. *See* TCP/IP protocol stack
- topology
 - bus topology*, 13
 - dual-ring topology*, 17
 - explained*, 11
 - extended-star topology*, 15-16
 - full-mesh topology*, 17
 - logical topologies*, 12
 - partial-mesh topology*, 18
 - physical topologies*, 11-12
 - single-ring topology*, 16
 - star topology*, 14
- user applications
 - collaboration*, 8
 - databases*, 8
 - email*, 7
 - impact of*, 8-9
 - instant messaging*, 8
 - web browsers*, 7
- VPN (Virtual Private Network), 437-438
- WANs (wide area networks)
 - communication link options*, 437-438
 - compared to LANs (local area networks)*, 435-436
 - explained*, 433-434
 - point-to-point connectivity*, 438

point-to-point link configuration, 438-439
routers, 437
 never parameter (ip nat translation), 358
 Next Header field (IPv6 header), 448
 NICs (network interface cards), 5, 46, 54-55
 no access-list access-list-number command, 357
 no access-list command, 409
 no description command, 271
 no ip access-group command, 408-409
 no ip nat inside source command, 354, 357
 no ip nat inside source static command, 352
 no ip nat pool command, 353
 no shutdown command, 273
 NOS (network operating systems), 235
 not-so-stubby area (NSSA), 303
 NSAP (network service access point), 236
 NSSA (not-so-stubby area), 303
 numbered extended IPv4 ACLs, 413-419
 numbered standard IPv4 ACLs, 408-413
 numbers
 ACL numbers, 398-400
 binary numbering
 base 2 conversion system, 164
 binary-hexadecimal numbers, 53-54
 binary-to-decimal conversion, 166-167

decimal versus binary numbering, 162
decimal-to-binary conversion, 165-166
explained, 162
LSB (least significant bit), 163
MSB (most significant bit), 163
powers of 2, 164-165
 ISN (initial sequence numbers), 205
 port numbers, 204-205
 NVRAM, 81
 saving configuration files to, 269

O

obtaining IP addresses, 149
 offices
 branch offices, 3
 home offices, 3
 main offices, 3
 mobile users, 3
 remote locations, 3
 open networks, 373
 Open Shortest Path First (OSPF). *See* OSPF (Open Shortest Path First)
 Open Systems Interconnection model. *See* OSI (Open Systems Interconnection) model
 optical fiber, 62-64
 Organizational Unique Identifier (OUI), 53
 OSFP (Open Shortest Path First), 301
 OSI (Open Systems Interconnection) model
 application layer, 29
 compared to TCP/IP protocol stack, 36-37

- data communications process
 - deencapsulation*, 33-34
 - encapsulation*, 32
 - explained*, 31-32
 - data link layer, 31
 - explained, 27-29
 - host-to-host communications model, 26-27
 - LLC (logical link control) sublayer, 49
 - MAC sublayer, 49
 - network layer, 30
 - peer-to-peer communication, 34-35
 - physical layer, 31
 - presentation layer, 29
 - session layer, 29-30
 - transport layer, 30
 - OSPF (Open Shortest Path First), 223**
 - additional resources, 339
 - areas, 313
 - authentication
 - explained*, 328
 - MD5 authentication*, 329
 - plaintext password authentication*, 329-332
 - autonomous system (AS), 313
 - configuration, 316-317
 - debug commands, 323-325
 - explained, 311-313
 - hierarchy, 312
 - load balancing, 326-328
 - loopback interfaces, 317-318
 - neighbor adjacencies
 - establishing*, 313-315
 - troubleshooting*, 333-335
 - OSPFv3, 452-453
 - SPF (shortest path first) algorithms, 315-316
 - troubleshooting, 329-338
 - components*, 332
 - neighbor adjacencies*, 333-335
 - plaintext password authentication*, 337-338
 - routing tables*, 336-337
 - verifying configuration of, 318
 - show ip ospf command*, 318-320
 - show ip ospf interface command*, 321-322
 - show ip ospf neighbor command*, 322-324
 - show ip route command*, 318-320
 - OSPFv3, 452-453
 - OUI (Organizational Unique Identifier), 53
 - Output Errors parameter (show interface comma), 106
 - output modifiers (show command), 84-85
 - outside global addresses, 349
 - outside local addresses, 349
 - overloading
 - inside global addresses, 355-359
 - NAT (Network Address Translation), 349
- ## P
-
- packet delivery process**
 - arp command, 250
 - default gateways, 247
 - host-to-host packet delivery, 238-247
 - Layer 1 devices, 234

- Layer 1 devices and functions, 234
- Layer 2 addressing, 235-236
- Layer 2 devices, 234
- Layer 3 addressing, 236-237
- Layer 3 devices, 236
- mapping Layer 2 addressing to
 - Layer 3 addressing, 237-238
- ping command, 248-249
- traceroute command, 251
- TRACERT, 250-251
- packet forwarding, 222**
- packets, 201**
- partial-mesh topology, 18**
- passive attacks, 376**
- password attacks, 379-380**
- password security, 380-382**
- passwords**
 - password attacks, 379-380
 - password security, 380-382
 - plaintext password authentication, 329-332
 - configuration, 329-332*
 - troubleshooting, 337-338*
 - verifying, 331-332*
- PAT (Port Address Translation), 349-350**
- path determination, 221**
- Payload Length field (IPv6 header), 448**
- PDU (protocol data units), 34-35**
- peer-to-peer communication, 34-35**
- permanent parameter (ip route), 288**
- per-port cost (switches), 92**
- physical layer (OSI), 31**
- physical redundancy (LANs), 131-133**
- physical security, 377-380**
- physical topologies, 11-12**
 - bus topology, 13
 - dual-ring topology, 17
 - extended-star topology, 15-16
 - full-mesh topology, 17
 - partial-mesh topology, 18
 - single-ring topology, 16
 - star topology, 14
- ping command, 248-249**
- plaintext password authentication, 329-332**
 - configuration, 329-332
 - troubleshooting, 337-338
 - verifying, 331-332
- point-to-point connectivity, 438**
- point-to-point link configuration, 438-439**
- Port Address Translation (PAT), 349-350**
- port-timeout parameter (ip nat translation), 358**
- ports**
 - port density (switches), 92
 - port numbers, 204-205
 - port security, 384-387
 - port speed (switches), 92
 - router ports, 221
 - troubleshooting, 105-107
 - VLAN port assignment, 128-130
 - well-known port numbers, 414
- pound sign (#), 270**
- powers of 2, 164-165**
- pptp-timeout parameter (ip nat translation), 358**
- preamble field (Ethernet frames), 51**
- presentation layer (OSI), 29**
- priority of routers, 315**

private IP addresses, 149-150

privileged EXEC mode

entering, 75-77, 263-264

explained, 72, 263

help, 265

protocol data units (PDU), 34-35

protocols, 46

ARP (Address Resolution Protocol)

ARP table, 238

host-to-host packet delivery, 238-247

mapping Layer 2 addressing to Layer 3 addressing, 237-238

CDP (Cisco Discovery Protocol), 273-280

DHCP (Dynamic Host Configuration Protocol), 154-155

automatic allocation, 344

Cisco routers as DHCP clients, 345

Cisco routers as DHCP servers, 345-346

DHCPACK message, 345

DHCPDISCOVER message, 344

DHCPOFFER message, 345

DHCPREQUEST message, 345

dynamic allocation, 344

explained, 343-345

manual allocation, 344

DNS (Domain Name System), 347

EGP (exterior gateway protocols), 295

EIGRP (Enhanced Interior Gateway Routing Protocol), 223, 228

FTP (File Transfer Protocol), 199

ICMP (Internet Control Message Protocol), 248

ICMPv6, 449

IGP (interior gateway protocols), 295

LLDP (Link Layer Discovery Protocol), 278

OSPF (Open Shortest Path First), 223, 301

additional resources, 339

areas, 313

authentication, 328-332

autonomous system (AS), 313

configuration, 316-317

debug commands, 323-325

explained, 311-313

hierarchy, 312

load balancing, 326-328

loopback interfaces, 317-318

neighbor adjacencies, 313-315

SPF (shortest path first) algorithms, 315-316

troubleshooting, 329-338

verifying configuration of, 318

OSPFv3, 452-453

SMTP (Simple Mail Transfer Protocol), 200

STP, 132-133

TCP (Transmission Control Protocol)

acknowledgment, 210-211

characteristics of, 198

explained, 197

fixed windowing, 211-213

flow control, 209-210

header format, 202-204

port number usage, 204-205

sliding windowing, 213-214

three-way handshake, 205-208

TCP/IP protocol stack. *See* TCP/IP protocol stack

Telnet, 200

TFTP (Trivial File Transfer Protocol), 199

UDP (User Datagram Protocol), 196
explained, 199

flow control, 209-210

header format, 202-204

port number usage, 204-205

VTP (VLAN Trunking Protocol), 117
configuration, 122

modes, 117-119

operation, 119-120

pruning, 120-121

pruning (VTP), 120-121

public IP addresses, 149-150

Q

QoS (quality of service), 9

question mark (?), 75-76, 79

quotation marks ("), 382

R

-r flag (ping), 249

RADIUS (Remote Authentication Dial-In User Service), 383

RAM, 81

real-time applications, 9

reconnaissance attacks, 378-379

redundancy in LANs (local-area networks), 131-133

reflexive ACLs, 402-404

/registerdns parameter (ipconfig), 156

relay agents, Cisco routers as, 347

/release parameter (ipconfig), 156

reliability, 11

Remote Authentication Dial-In User Service (RADIUS), 383

remote office locations, 3

remote terminals, configuring devices with, 74

/renew parameter (ipconfig), 156

replies (ARP), 242-243

requests (ARP), 240

resolving translation table issues, 359-362

right-facing arrow (>), 75

ring topologies, 16-17

dual-ring topology, 17

single-ring topology, 16

RJ-45 connector, 58-59

ROM, 81

round-trip time (RTT), 248

route aggregation, 187-191

router IDs, 314

routers, 46

Cisco routers

as DHCP clients, 345

as DHCP relay agents, 347

as DHCP servers, 345-346

initial setup, 257-263

initial startup, 256

initial startup status, verifying, 266-267

logging in to, 263-265

naming, 269-270

controlling access to via ACLs, 413

definition of, 5

explained, 220-222

priority, 315

router ID, 314

- router on a stick, 134-135
- use of subnet masks, 174-176
- in WANs (wide area networks), 437
- routing**
 - default routing, 222, 225
 - directly connected routes, 224
 - distance vector routing, 226-227, 295, 299-300
 - dynamic routing, 224
 - balanced hybrid routing*, 296
 - classful versus classless routing*, 297-298
 - compared to static routing*, 287
 - distance vector routing*, 295, 299-300
 - example: administrative distance*, 296-297
 - explained*, 293-296
 - IGP (interior gateway protocols)*, 295
 - link-state routing*, 296, 300-307
 - SPF (shortest path first) algorithms*, 302
 - explained, 219
 - IPv6, 450-451
 - basic IPv6 connectivity*, 451-452
 - OSPFv3*, 452-453
 - static routing*, 452
 - link-state routing, 227, 296, 300-307
 - advantages of*, 302, 306-307
 - IS-IS (Intermediate System-to-Intermediate System)*, 301
 - limitations*, 307
 - LSA (link-state advertisements)*, 301
 - network hierarchy*, 302-304
 - OSFP (Open Shortest Path First)*, 301
 - OSPF (Open Shortest Path First)*. *See* *OSPF (Open Shortest Path First)*
 - SPF (shortest path first) algorithms*, 302-306
 - OSPF (Open Shortest Path First). *See* *OSPF (Open Shortest Path First)*
 - path determination, 221-223
 - route summarization, 187-191
 - routers
 - Cisco routers*. *See* *Cisco routers*
 - controlling access to via ACLs*, 413
 - definition of*, 5
 - explained*, 220-222
 - priority*, 315
 - router ID*, 314
 - router on a stick*, 134-135
 - use of subnet masks*, 174-176
 - in WANs (wide area networks)*, 437
 - routing metrics, 225-226
 - routing tables, 223-224
 - static routing, 222, 224
 - compared to dynamic routing*, 287
 - configuration*, 288-289
 - default route forwarding*, 290
 - explained*, 285-287
 - verifying*, 290-291
 - between VLANs (virtual local-area networks), 133-136
 - explained*, 133-134
 - multilayer switches*, 136
 - router on a stick*, 134-135

routing metrics, 225-226
 routing tables, 223-224
 RTT (round-trip time), 248
 Runts parameter (show interface command), 106

S

-s flag

arp command, 250
 ping command, 249

saving configuration files to NVRAM, 269

scalability, 10

seconds parameter (ip nat translation), 358

section parameter (show command), 85

Secure Shell (SSH), 383

security

access attacks, 379
 ACLs (access control lists). *See*
 ACLs (access control lists)
 adversaries, 376
 balancing network security requirements, 375-376
 Cisco device security, 380
 classes of attack, 376-377
 explained, 371-372
 hacker motivations, 376
 need for, 372-375
 overview, 10
 password attacks, 379-380
 password security, 380-382
 physical installations, 377-378
 port security, 384-387
 reconnaissance attacks, 378-379
 Telnet versus SSH access, 383

segmentation, 201, 209

server mode (VTP), 117

servers

Cisco routers as DHCP servers, 345-346
 copying configuration files from, 82-83

session layer (OSI), 29-30

session multiplexing, 208-209

/setclassid parameter (ipconfig), 157

setup. *See* configuration

setup command, 263

setup mode (Cisco routers), entering, 257-258

shortcut keys, 80

shortest path first (SPF) algorithms, 302, 304-306, 315-316. *See also* link-state routing

show access-list command, 365

show access-lists command, 416

show cdp entry command, 279

show cdp neighbors command, 278

show cdp neighbors detail command, 279

show command, 84-85

show interface command, 103-106

show interfaces command, 98, 129, 273-277

show ip access-list command, 425

show ip interface command, 426

show ip nat statistics command, 360-363

show ip nat translation command, 357-358, 364-365

show ip ospf command, 319-321

show ip ospf interface command, 321-322

- show ip ospf neighbor command, 322-324
- show ip protocol command, 366
- show ip route command, 290, 318-320, 328, 365-366
- show port-security interface command, 385-386
- show running-config command, 82
- show startup-config command, 82
- show version command, 266-267
- show vlan brief command, 128
- show vlan command, 128
- show vlan id vlan_number command, 127
- show vlan name vlan-name command, 127
- /showclassid parameter (ipconfig), 157
- shutdown command, 271
- Simple Mail Transfer Protocol (SMTP), 200
- single-mode fiber (SMF), 63
- single-ring topology, 16
- size of LANs (local area networks), 47
- sliding windowing, 213-214
- small office/home office (SOHO), 47
- SMF (single-mode fiber), 63
- SMTP (Simple Mail Transfer Protocol), 200
- Sneakernet, 2
- SOF (start-of-frame) delimiter, 51
- software, Cisco IOS Software, 70-71
- SOHO (small office/home office), 47
- Source Address field
 - Ethernet frames, 51
 - IPv6 header, 448
- speed of networks, 10
- SPF (shortest path first) algorithms.
 - See* link-state routing
- splices, 103
- SSH (Secure Shell), 383
- standard ACLs, 398
- star topology, 14
- starting Cisco routers
 - initial setup, 257-263
 - initial startup, 256
 - initial startup status, verifying, 266-267
 - login, 263-265
- start-of-frame (SOF) delimiter, 51
- stateless autoconfiguration, 449-450
- static NAT (Network Address Translation), 349, 353-354
- static routing, 222-224, 452
 - compared to dynamic routing, 287
 - configuration, 288-289
 - default route forwarding, 290
 - explained, 285-287
 - verifying, 290-291
- Static Routing Video, 291
- status (VTP), displaying, 123
- STP, 132-133
- stub area, 303, 315
- subnet masks
 - applying, 178
 - end system use of, 173-174
 - mechanics of subnet mask operation, 176-177
 - router use of, 174-176
 - VLSM (variable-length subnet masks), 442
 - advantages of*, 185
 - calculating*, 186

- example*, 186-187
- explained*, 184-187
- route summarization*, 187-191
- subnets**, 161
 - advantages of, 167-169
 - binary numbering
 - base 2 conversion system*, 164
 - binary-to-decimal conversion*, 166-167
 - decimal versus binary numbering*, 162
 - decimal-to-binary conversion*, 165-166
 - explained*, 162
 - LSB (least significant bit)*, 163
 - MSB (most significant bit)*, 163
 - powers of 2*, 164-165
 - Class A subnets
 - computing hosts for*, 172-173
 - example*, 183-184
 - Class B subnets
 - computing hosts for*, 171-172
 - example*, 181-182
 - Class C subnets
 - computing hosts for*, 170-171
 - example*, 180-181
 - computing hosts for
 - Class A subnets*, 172-173
 - Class B subnets*, 171-172
 - Class C subnets*, 170-171
 - creating, 170
 - network addressing scheme
 - determination, 179-180
 - subnet masks
 - applying*, 178
 - end system use of*, 173-174
 - mechanics of subnet mask operation*, 176-177
 - router use of*, 174-176
 - VLSM (variable-length subnet masks)*, 442
 - two-level and three-level addresses, 169
 - VLSM (variable-length subnet masks)
 - advantages of*, 185
 - calculating*, 186
 - example*, 186-187
 - explained*, 184-187
 - route summarization*, 187-191
- supernetting**, 187-191
- switched communication links**, 437
- switches**, 5, 46
 - assigning IP addresses to, 96
 - characteristics of, 92
 - configuring, 95-97
 - connecting to console port, 94-95
 - duplex communication, 100-102
 - initial startup status, verifying, 97-99
 - installing, 93
 - LED indicators, 93-94
 - multilayer switches, 136
 - need for, 90-92
 - switching operation, 99
 - troubleshooting, 102-107
 - media issues*, 102-106
 - port issues*, 105-107
- switchport access command**, 128
- switchport mode command**, 124
- synchronization**, global, 214
- syntax help (CLI)**, 78
- syn-timeout parameter (ip nat translation)**, 358

T

-t flag (ping), 248

tables

ARP table, 238

MAC tables, 91

OSPF routing tables,
troubleshooting, 336-337

routing tables, 223-224

translation table issues, resolving,
359-362

**TACACS+ (Terminal Access
Controller Access Control System
Plus), 383**

target_host flag (traceroute), 251

TargetName flag (ping), 249

**TCP (Transmission Control
Protocol), 197**

acknowledgment, 210-211

characteristics of, 198

explained. *See also* TCP/IP protocol
stack

fixed windowing, 211-213

flow control, 209-210

header format, 202-204

port number usage, 204-205

sliding windowing, 213-214

three-way handshake, 205-208

TCP/IP protocol stack

addressing services

*DHCP (Dynamic Host
Configuration Protocol),
154-155*

*DNS (Domain Name System),
155-157*

compared to OSI (Open Systems
Interconnection) model, 36-37

explained, 35-36, 140

IANA (Internet Assigned Numbers
Authority), 149

Internet layer, 36

address classes, 143-145

address exhaustion, 150-153

address format, 140-142

broadcast addresses, 145-149

*CIDR (classless interdomain
routing), 152-153*

*determining IP addresses,
155-157*

*DHCP (Dynamic Host
Configuration Protocol),
154-155*

*DNS (Domain Name System),
155-157*

dotted-decimal notation, 142

explained, 140

*IANA (Internet Assigned
Numbers Authority), 149*

IPv6 addresses, 151-152

network addresses, 145-149

obtaining IP addresses, 149

private IP addresses, 149-150

public IP addresses, 149-150

IP addresses

address classes, 143-145

address exhaustion, 150-153

address format, 140-142

broadcast addresses, 145-149

*CIDR (classless interdomain
routing), 152-153*

*configuring for Cisco routers,
272-273*

determining, 155-157

dotted-decimal notation, 142

*IANA (Internet Assigned
Numbers Authority), 149*

- network addresses, 145-149*
- obtaining, 149*
- private IP addresses, 149-150*
- public IP addresses, 149-150*
- IPv6
 - address allocation, 446-447*
 - address types, 444-445*
 - explained, 151-152, 441-443*
 - features, 443-444*
 - headers, 447-448*
 - ICMPv6, 449*
 - neighbor discovery, 449*
 - routing, 450-453*
 - stateless autoconfiguration, 449-450*
- packet delivery process
 - arp command, 250*
 - ARP table, 238*
 - default gateways, 247*
 - host-to-host packet delivery, 238-247*
 - Layer 1 devices, 234*
 - Layer 2 addressing, 235-236*
 - Layer 2 devices, 234*
 - Layer 3 addressing, 236-237*
 - Layer 3 devices, 236*
 - mapping Layer 2 addressing to Layer 3 addressing, 237-238*
 - ping command, 248-249*
 - traceroute command, 251*
 - TRACERT, 250-251*
- routing. *See routing*
- subnets, 161
 - advantages of, 167-169*
 - binary numbering, 162-167*
 - Class A example, 183-184*
 - Class B example, 181-182*
 - Class C example, 180-181*
 - computing hosts for, 170-173*
 - creating, 170*
 - network addressing scheme determination, 179-180*
 - subnet masks, 173-178*
 - two-level and three-level addresses, 169*
 - VLSM (variable-length subnet masks), 184-191*
- TCP (Transmission Control Protocol)
 - acknowledgment, 210-211*
 - characteristics of, 198*
 - explained, 197*
 - fixed windowing, 211-213*
 - flow control, 209-210*
 - header format, 202-204*
 - port number usage, 204-205*
 - sliding windowing, 213-214*
 - three-way handshake, 205-208*
- Transport layer
 - acknowledgment, 210-211*
 - applications, 199-200*
 - connection initiation, 200-201*
 - data containers, 201-202*
 - explained, 195-199*
 - fixed windowing, 211-213*
 - flow control, 209-210*
 - global synchronization, 214*
 - port number usage, 204-205*
 - segmentation, 209*
 - session multiplexing, 208-209*
 - sliding windowing, 213-214*
 - TCP (Transmission Control Protocol), 197-198*
 - TCP/UDP header formats, 202-204*

- three-way handshake*, 205-208
- throughput maximization*, 214
- UDP (User Datagram Protocol), 197-199
 - UDP (User Datagram Protocol)
 - explained*, 197
 - flow control*, 209-210
 - header format*, 202-204
- tcp-timeout parameter (ip nat translation), 358
- Telnet, 75, 200, 383
- terminal (vty) sessions, 75
- Terminal Access Controller
 - Access Control System Plus (TACACS+), 383
- Terminal Emulation. *See* Telnet
- TFTP (Trivial File Transfer Protocol), 75, 199
- threat mitigation, 377-378
- three-level addresses, 169
- three-way handshake, 205-208
- throughput maximization, 214
- time-based ACLs, 404-405
- timeout parameter (ip nat translation), 358
- Time-To-Live (TTL), 132
- topology
 - bus topology, 13
 - dual-ring topology, 17
 - explained*, 11
 - extended-star topology, 15-16
 - full-mesh topology, 17
 - logical topologies, 12
 - partial-mesh topology, 18
 - physical topologies, 11-12
 - single-ring topology, 16
 - star topology, 14
- totally not-so-stubby area, 303
- totally stubby area, 303
- traceroute command, 251
- TRACERT utility, 250-251
- Traffic Class field (IPv6 header), 448
- translation
 - inside source address translation, 350-353
 - dynamic address translation*, 354
 - static NAT address mapping*, 353-354
 - translation table issues, resolving, 359-362
- Transmission Control Protocol (TCP). *See* TCP (Transmission Control Protocol)
- transparent mode (VTP), 119
- Transport layer (OSI), 30
- Transport layer (TCP/IP), 36
 - acknowledgment, 210-211
 - applications, 199-200
 - connection initiation, 200-201
 - data containers, 201-202
 - explained*, 195-199
 - fixed windowing, 211-213
 - flow control, 209-210
 - global synchronization, 214
 - port number usage, 204-205
 - segmentation, 209
 - session multiplexing, 208-209
 - sliding windowing, 213-214
 - TCP (Transmission Control Protocol), 197-198
 - TCP/UDP header formats, 202-204
 - three-way handshake, 205-208
 - throughput maximization, 214
 - UDP (User Datagram Protocol), 197-199

Trivial File Transfer Protocol (TFTP),
75, 199

troubleshooting

ACLs (access control lists), 425-429

OSPF (Open Shortest Path First),
329-338

components, 332

neighbor adjacencies, 333-335

plaintext password authentication, 337-338

routing tables, 336-337

ports, 105-107

switches, 102-107

media issues, 102-106

port issues, 105-107

trunk parameter (switchport mode command), 124

trunking

802.1Q technology, 115-117

configuration, 123-126

frames, 116

ISL (Inter-Switch Link) trunks, 115

native VLAN, 117

VTP (VLAN Trunking Protocol), 117

configuration, 122

modes, 117-119

operation, 119-120

pruning, 120-121

TTL (Time-To-Live), 132

two-level addresses, 169

type/length field (Ethernetframes), 51

U

UDP (User Datagram Protocol), 196

explained, 197-199

flow control, 209-210

header format, 202-204

port number usage, 204-205

udp-timeout parameter (ip nat translation), 358

unicast addresses, 444-445

unicast transmission, 52

unshielded twisted-pair (UTP) cables,
57-61

user applications

batch applications, 8

collaboration, 8

databases, 8

email, 7

impact of, 8-9

instant messaging, 8

interactive applications, 8-9

real-time applications, 9

web browsers, 7

User Datagram Protocol (UDP),
196-199

user EXEC mode

entering, 75-77, 264

explained, 72, 263

help, 264

users, mobile, 3

utilities, TRACERT, 250-251

UTP (unshielded twisted-pair) cable,
58-61

V

-v flag (ping), 249

variable-length subnet masks. *See* VLSM (variable-length subnet masks)

verifying

address translation, 361-367

Cisco router configuration

initial setup, 266-267

interface configuration, 273-277

neighbor device configuration, 277-280

default gateways, 363-364

initial switch startup status, 97-99

OSPF (Open Shortest Path First)

neighbor adjacencies, 333-335

show ip ospf interface command, 321-322

show ip ospf neighbor command, 322-324

OSPF (Open Shortest Path First)

configuration, 318

show ip ospf command, 318-320

show ip route command, 318-320

plaintext password authentication, 331-332

static route configuration, 290-291

Version field (IPv6 header), 448

VID (VLAN ID), 116

Virtual Private Network (VPN), 437-438

virtual type terminal (vty), 381

VLAN ID (VID), 116

VLAN Trunking Protocol. *See* VTP (VLAN Trunking Protocol)

vlan vlan-id command, 126

VLANs (virtual local-area networks)

802.1Q technology, 115-117

frames, 116

native VLAN, 117

adding, 129

configuration

802.1Q trunking, 123-126

port assignment, 128-130

VLAN creation, 126-128

VTP (VLAN Trunking Protocol), 122

creating, 126-128

deleting, 130

design considerations, 130-131

modifying, 130

overview, 111-115

poorly designed networks, 112-113

routing between, 133-136

explained, 133-134

multilayer switches, 136

router on a stick, 134-135

VID (VLAN ID), 116

VTP (VLAN Trunking Protocol)

configuration, 122

modes, 117-119

operation, 119-120

pruning, 120-121

VLSM (variable-length subnet masks), 442

advantages of, 185

calculating, 186

example, 186-187

explained, 184-187

route summarization, 187-191

VPN (Virtual Private Network),
437-438

VTP (VLAN Trunking Protocol), 117

configuration, 122

modes, 117-119

operation, 119-120

pruning, 120-121

VTY (Telnet) ports, 381-382

vty (virtual type terminal), 381

W-X-Y-Z

-w flag

ping command, 249

traceroute command, 251

WANs (wide area networks)

communication link options,
437-438

compared to LANs (local area
networks), 435-436

explained, 433-434

point-to-point connectivity, 438

point-to-point link configuration,
438-439

routers, role of, 437

web browsers, 7

well-known port numbers, 414

wide area networks. *See* WANs
(wide area networks)

wildcard masking, 405-407

wildcard-mask parameter (network), 317

windowing

explained, 211

fixed windowing, 211-213

sliding windowing, 213-214

Word help (CLI), 77

Xerox, 48