



Network Basics

CCNA Companion Guide



Cisco | Networking Academy®
Mind Wide Open™

FREE SAMPLE CHAPTER



SHARE WITH OTHERS

Network Basics Companion Guide

Cisco Networking Academy

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

Network Basics Companion Guide

Copyright© 2014 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

First Printing November 2013

Library of Congress Cataloging-in-Publication data is on file.

ISBN-13: 978-1-58713-317-6

ISBN-10: 1-58713-317-2

Warning and Disclaimer

This book is designed to provide information about the Cisco Networking Academy Network Basics course. 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 authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

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

Publisher

Paul Boger

Associate Publisher

Dave Dusthimer

Business Operation Manager, Cisco Press

Jan Cornelissen

Executive Editor

Mary Beth Ray

Managing Editor

Sandra Schroeder

Development Editor

Ellie C. Bru

Project Editor

Mandie Frank

Copy Editor

Bill McManus

Technical Editor

Tony Chen

Editorial Assistant

Vanessa Evans

Designer

Mark Shirar

Composition

Trina Wurst

Indexer

Ken Johnson

Proofreader

Charlotte Kughen

This book is part of the Cisco Networking Academy® series from Cisco Press. The products in this series support and complement the Cisco Networking Academy curriculum. If you are using this book outside the Networking Academy, then you are not preparing with a Cisco trained and authorized Networking Academy provider.

For more information on the Cisco Networking Academy or to locate a Networking Academy, Please visit www.cisco.com/edu.



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 the United States, please contact:

International Sales

international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members 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 email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.



Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, IQ Expertise, the IQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0609R)

About the Contributing Authors

Antoon (Tony) W. Ruffi is Campus Director of Academic Affairs, ECPI University, Newport News, Virginia. Tony is a networking professional who retired from the U.S. Air Force in June 2000 after 29 years. He worked on communication systems. Since retirement, Tony has worked for ECPI University teaching a variety of networking courses. The courses he has led include CCNA, CCNP, and Fundamentals of Network Security in the Cisco Academy at ECPI University, as well as numerous courses in the university's Cloud Computing program. Tony is a PhD candidate, Applied Management and Decision Science, with an Information Systems Management specialty at Walden University.

Rick McDonald is an Associate Professor in the Information Systems department at the University of Alaska Southeast, in Ketchikan, Alaska, where he teaches computer and networking courses. He specializes in developing and delivering networking courses via e-learning. Rick worked in the airline industry for several years before returning to full-time teaching. He taught CCNA and CCNP courses in North Carolina before moving to Alaska in 2003.

Contents at a Glance

Introduction	xxiv
Chapter 1	Exploring the Network 1
Chapter 2	Configuring a Network Operating System 55
Chapter 3	Network Protocols and Communications 101
Chapter 4	Application Layer 139
Chapter 5	Transport Layer 169
Chapter 6	Network Layer 211
Chapter 7	IP Addressing 265
Chapter 8	Subnetting IP Networks 355
Chapter 9	Network Access 409
Chapter 10	Ethernet 485
Chapter 11	It's a Network 545
Appendix A	Answers to the "Check Your Understanding" Questions 613
Glossary	625
Index	653

Contents

Introduction xxiv

Chapter 1 Exploring the Network 1

Objectives 1

Key Terms 1

Introduction (1.0.1.1) 3

Communicating in a Network-Centric World (1.1) 4

Interconnecting Our Lives (1.1.1) 4

Networks in Our Daily Lives (1.1.1.1) 4

Technology Then and Now (1.1.1.2) 5

The Global Community (1.1.1.3) 6

Networks Support the Way We Learn (1.1.1.4) 6

Networks Support the Way We Communicate (1.1.1.5) 7

Networks Support the Way We Work (1.1.1.6) 9

Networks Support the Way We Play (1.1.1.7) 9

Supporting Communication (1.1.2) 10

What Is Communication? (1.1.2.1) 10

Quality of Communication (1.1.2.2) 12

The Network as a Platform (1.2) 13

Converged Networks (1.2.1) 13

Traditional Service Networks (1.2.1.1) 13

Planning for the Future (1.2.1.2) 14

Reliable Network (1.2.2) 15

The Supporting Network Architecture (1.2.2.1) 15

Fault Tolerance in Circuit-Switched Networks (1.2.2.2) 15

Packet-Switched Networks (1.2.2.3) 17

Scalable Networks (1.2.2.4) 18

Providing QoS (1.2.2.5) 20

Providing Network Security (1.2.2.6) 21

LANs, WANs, and the Internet (1.3) 23

Components of a Network (1.3.1) 23

Components of the Network (1.3.1.1) 23

End Devices (1.3.1.2) 24

Intermediary Devices (1.3.1.3) 25

Network Media (1.3.1.4) 25

Network Representations (1.3.1.5) 26

Topology Diagrams (1.3.1.6) 28

LANs and WANs (1.3.2) 28

Types of Networks (1.3.2.1) 28

Local-Area Networks (1.3.2.2) 29

Wide-Area Networks (1.3.2.3) 30

The Internet (1.3.3)	30
<i>The Internet (1.3.3.1)</i>	30
<i>Intranet and Extranet (1.3.3.2)</i>	31
Connecting to the Internet (1.3.4)	32
<i>Internet Access Technologies (1.3.4.1)</i>	32
<i>Connecting Remote Users to the Internet (1.3.4.2)</i>	33
<i>Connecting Businesses to the Internet (1.3.4.3)</i>	34

The Expanding Network (1.4) 35

Network Trends (1.4.1)	36
<i>New Trends (1.4.1.1)</i>	36
<i>Bring Your Own Device (BYOD) (1.4.1.2)</i>	36
<i>BYOD Considerations (1.4.1.3)</i>	37
<i>Online Collaboration (1.4.1.4)</i>	38
<i>Collaboration Considerations (1.4.1.5)</i>	38
<i>Video Communication (1.4.1.6)</i>	39
<i>Cloud Computing (1.4.1.7)</i>	40
<i>Types of Clouds (1.4.1.8)</i>	41
<i>Data Centers (1.4.1.9)</i>	41
Network Security (1.4.2)	42
<i>Security Threats (1.4.2.1)</i>	42
<i>Security Solutions (1.4.2.2)</i>	44
Network Architectures (1.4.3)	45
<i>Cisco Network Architectures (1.4.3.1)</i>	45
<i>Cisco Borderless Network (1.4.3.2)</i>	46
<i>Collaboration Architecture (1.4.3.3)</i>	46
<i>Data Center Architecture (1.4.3.4)</i>	47
<i>CCNA (1.4.3.5)</i>	47

Summary (1.5) 49

Practice 50

Class Activities	50
Labs	50
Packet Tracer Activity	50

Check Your Understanding 50

Chapter 2 Configuring a Network Operating System 55

Objectives 55

Key Terms 55

Introduction (2.0.1.1) 56

IOS Bootcamp (2.1) 56

Cisco IOS (2.1.1)	56
<i>Purpose of OS (2.1.1.1)</i>	56
<i>Location of the Cisco IOS (2.1.1.2)</i>	57
<i>IOS Functions (2.1.1.3)</i>	58

Accessing a Cisco IOS Device (2.1.2)	59
<i>Console Access Method (2.1.2.1)</i>	59
<i>Telnet, SSH, and AUX Access Methods (2.1.2.2)</i>	60
<i>Terminal Emulation Programs (2.1.2.3)</i>	61
Navigating the IOS (2.1.3)	61
<i>Cisco IOS Modes of Operation (2.1.3.1)</i>	62
<i>Primary Modes (2.1.3.2)</i>	63
<i>Global Configuration Mode and Submodes (2.1.3.3)</i>	64
<i>Navigating Between IOS Modes (2.1.3.4, 2.1.3.5)</i>	65
The Command Structure (2.1.4)	66
<i>IOS Command Structure (2.1.4.1)</i>	67
<i>Cisco IOS Command Reference (2.1.4.2)</i>	68
<i>Context-Sensitive Help (2.1.4.3)</i>	70
<i>Command Syntax Check (2.1.4.4)</i>	71
<i>Hot Keys and Shortcuts (2.1.4.5)</i>	72
<i>IOS Examination Commands (2.1.4.6)</i>	74
<i>The show version Command (2.1.4.7)</i>	75
Getting Basic (2.2)	76
Hostnames (2.2.1)	76
<i>Why the Switch (2.2.1.1)</i>	76
<i>Device Names (2.2.1.2)</i>	76
<i>Hostnames (2.2.1.3)</i>	78
<i>Configuring Hostnames (2.2.1.4)</i>	78
Limiting Access to Device Configurations (2.2.2)	79
<i>Securing Device Access (2.2.2.1)</i>	79
<i>Securing Privileged EXEC Access (2.2.2.2)</i>	80
<i>Securing User EXEC Access (2.2.2.3)</i>	81
<i>Encrypting Password Display (2.2.2.4)</i>	82
<i>Banner Messages (2.2.2.5)</i>	83
Saving Configurations (2.2.3)	84
<i>Configuration Files (2.2.3.1)</i>	84
<i>Capturing Text (2.2.3.2)</i>	87
Address Schemes (2.3)	88
Ports and Addresses (2.3.1)	88
<i>IP Addressing of Devices (2.3.1.1)</i>	88
<i>Interfaces and Ports (2.3.1.2)</i>	89
Addressing Devices (2.3.2)	90
<i>Configuring a Switch Virtual Interface (2.3.2.1)</i>	90
<i>Manual IP Address Configuration for End Devices (2.3.2.2)</i>	91
<i>Automatic IP Address Configuration for End Devices (2.3.2.3)</i>	91
<i>IP Address Conflicts (2.3.2.4)</i>	92

	Verifying Connectivity (2.3.3)	93
	<i>Test the Loopback Address on an End Device (2.3.3.1)</i>	93
	<i>Testing the Interface Assignment (2.3.3.2)</i>	94
	<i>Testing End-to-End Connectivity (2.3.3.3)</i>	94
	Summary (2.4)	96
	Practice	97
	Class Activities	97
	Labs	97
	Packet Tracer Activities	97
	Check Your Understanding	97
Chapter 3	Network Protocols and Communications	101
	Objectives	101
	Key Terms	101
	Introduction (3.0.1.1)	103
	Network Protocols and Standards (3.1)	103
	Protocols (3.1.1)	103
	<i>Protocols: Rules that Govern Communications (3.1.1.1)</i>	103
	<i>Network Protocols (3.1.1.2)</i>	105
	<i>Interaction of Protocols (3.1.1.3)</i>	105
	Protocol Suites (3.1.2)	106
	<i>Protocol Suites and Industry Standards (3.1.2.1)</i>	106
	<i>Creation of the Internet and Development of TCP/IP (3.1.2.2)</i>	107
	<i>TCP/IP Protocol Suite and Communication Process (3.1.2.3)</i>	108
	Standards Organizations (3.1.3)	109
	<i>Open Standards (3.1.3.1)</i>	109
	<i>ISOC, IAB, and IETF (3.1.3.2)</i>	110
	<i>IEEE (3.1.3.3)</i>	111
	<i>ISO (3.1.3.4)</i>	112
	<i>Other Standards Organizations (3.1.3.5)</i>	112
	Reference Models (3.1.4)	113
	<i>The Benefits of Using a Layered Model (3.1.4.1)</i>	113
	<i>The OSI Reference Model (3.1.4.2)</i>	115
	<i>The TCP/IP Protocol Model (3.1.4.3)</i>	116
	<i>Comparing the OSI Model with the TCP/IP Model (3.1.4.4)</i>	116
	Using Requests for Comments (3.2)	118
	Why RFCs (3.2.1)	118
	<i>Request for Comments (RFC) (3.2.1.1)</i>	118
	<i>History of RFCs (3.2.1.2)</i>	119
	<i>Sample RFC (3.2.1.3)</i>	119

RFC Processes (3.2.2) 120

RFC Process (3.2.2.1) 120

RFC Types (3.2.2.2) 121

Moving Data in the Network (3.3) 123

Data Encapsulation (3.3.1) 123

Elements of Communication (3.3.1.1) 123

Communicating the Messages (3.3.1.2) 124

Protocol Data Units (PDUs) (3.3.1.3) 125

Encapsulation (3.3.1.4) 126

De-encapsulation (3.3.1.5) 127

Accessing Local Resources (3.3.2) 127

Network Addresses and Data Link Addresses (3.3.2.1) 127

*Communicating with a Device on the Same Network
(3.3.2.2) 128*

MAC and IP Addresses (3.3.2.3) 129

Accessing Remote Resources (3.3.3) 130

Default Gateway (3.3.3.1) 130

*Communicating with a Device on a Remote Network
(3.3.3.2) 131*

Summary (3.4) 134

Practice 135

Class Activities 135

Labs 135

Packet Tracer Activities 135

Check Your Understanding 135

Chapter 4

Application Layer 139

Objectives 139

Key Terms 139

Introduction (4.0.1.1) 140

Application Layer Protocols (4.1) 140

Application, Session, and Presentation (4.1.1) 140

OSI and TCP/IP Models Revisited (4.1.1.1) 140

Application Layer (4.1.1.2) 141

Presentation and Session Layers (4.1.1.3) 141

TCP/IP Application Layer Protocols (4.1.1.4) 143

Services at the Application Layer (4.1.1.5; 4.1.1.6) 144

*Applications Interface with People and Other Applications
(4.1.1.7) 145*

How Application Protocols Interact with End-User Applications
(4.1.2) 145

Peer-to-Peer Networks (4.1.2.1) 145

Peer-to-Peer Applications (4.1.2.2) 146

	<i>Common P2P Applications (4.1.2.3)</i>	147
	<i>Client-Server Model (4.1.2.5)</i>	148
	Well-Known Application Layer Protocols and Services (4.2)	149
	Everyday Application Layer Protocols (4.2.1)	149
	<i>Application Layer Protocols Revisited (4.2.1.1)</i>	149
	<i>Hypertext Transfer Protocol and Hypertext Markup Language (4.2.1.2)</i>	150
	<i>HTTP and HTTPS (4.2.1.3)</i>	151
	<i>SMTP and POP (4.2.1.4–4.2.1.7)</i>	152
	Providing IP Addressing Services (4.2.2)	154
	<i>Domain Name Service (4.2.2.1)</i>	154
	<i>DNS Message Format (4.2.2.2)</i>	155
	<i>DNS Hierarchy (4.2.2.3)</i>	156
	<i>nslookup (4.2.2.4)</i>	157
	<i>Dynamic Host Configuration Protocol (4.2.2.6)</i>	158
	<i>DHCP Operation (4.2.2.7)</i>	159
	Providing File Sharing Services (4.2.3)	161
	<i>File Transfer Protocol (4.2.3.1)</i>	161
	<i>Server Message Block (4.2.3.4)</i>	162
	Summary (4.3)	164
	Practice	165
	Class Activities	165
	Labs	165
	Packet Tracer Activities	165
	Check Your Understanding	166
Chapter 5	Transport Layer	169
	Objectives	169
	Key Terms	169
	Introduction (5.0.1.1)	170
	Transport Layer Protocols (5.1)	170
	Transportation of Data (5.1.1)	170
	<i>Role of the Transport Layer (5.1.1.1, 5.1.1.2)</i>	170
	<i>Conversation Multiplexing (5.1.1.3)</i>	173
	<i>Transport Layer Reliability (5.1.1.4)</i>	174
	<i>TCP (5.1.1.5)</i>	175
	<i>UDP (5.1.1.6)</i>	176
	<i>The Right Transport Layer Protocol for the Right Application (5.1.1.7)</i>	176
	Introducing TCP and UDP (5.1.2)	178
	<i>Introducing TCP (5.1.2.1)</i>	178
	<i>Role of TCP (5.1.2.2)</i>	179
	<i>Introducing UDP (5.1.2.3)</i>	180
	<i>Role of UDP (5.1.2.4)</i>	181

<i>Separating Multiple Communications (5.1.2.5)</i>	181
<i>TCP and UDP Port Addressing (5.1.2.6–5.1.2.9)</i>	183
<i>TCP and UDP Segmentation (5.1.2.10)</i>	187

TCP and UDP (5.2) 188

TCP Communication (5.2.1)	188
<i>TCP Reliable Delivery (5.2.1.1)</i>	188
<i>TCP Server Processes (5.2.1.2)</i>	189
<i>TCP Connection Establishment (5.2.1.3)</i>	189
<i>TCP Three-way Handshake Analysis: Step 1 (5.2.1.4)</i>	191
<i>TCP Three-way Handshake Analysis: Step 2 (5.2.1.5)</i>	192
<i>TCP Three-way Handshake Analysis: Step 3 (5.2.1.6)</i>	193
<i>TCP Session Termination Analysis (5.2.1.7)</i>	194
Protocol Data Units (5.2.2)	195
<i>TCP Reliability—Ordered Delivery (5.2.2.1)</i>	195
<i>TCP Reliability—Acknowledgement and Window Size (5.2.2.2)</i>	196
<i>TCP Reliability—Data Loss and Retransmission (5.2.2.3)</i>	197
<i>TCP Flow Control—Window Size and Acknowledgements (5.2.2.4)</i>	198
<i>TCP Flow Control—Congestion Avoidance (5.2.2.5)</i>	199
UDP Communication (5.2.3)	201
<i>UDP Low Overhead Versus Reliability (5.2.3.1)</i>	201
<i>UDP Datagram Reassembly (5.2.3.2)</i>	201
<i>UDP Server Processes and Requests (5.2.3.3)</i>	202
<i>UDP Client Processes (5.2.3.4)</i>	202
TCP or UDP—That Is the Question (5.2.4)	203
<i>Applications That Use TCP (5.2.4.1)</i>	203
<i>Applications That Use UDP (5.2.4.2)</i>	203

Summary (5.3) 205

Practice 206

Class Activities	206
Labs	206
Packet Tracer Activity	206

Check Your Understanding 206

Chapter 6

Network Layer 211

Objectives 211

Key Terms 211

Introduction (6.0.1.1) 213

Network Layer Protocols (6.1) 213

Network Layer in Communication (6.1.1)	213
<i>The Network Layer (6.1.1.1)</i>	213
<i>Network Layer Protocols (6.1.1.2)</i>	214

Characteristics of the IP Protocol (6.1.2)	215
<i>Characteristics of IP (6.1.2.1)</i>	215
<i>IP – Connectionless (6.1.2.2)</i>	215
<i>IP – Best-Effort Delivery (6.1.2.3)</i>	216
<i>IP – Media Independent (6.1.2.4)</i>	217
<i>Encapsulating IP (6.1.2.5)</i>	217
IPv4 Packet (6.1.3)	218
<i>IPv4 Packet Header (6.1.3.1)</i>	218
<i>IPv4 Header Fields (6.1.3.2)</i>	220
<i>Sample IPv4 Headers (6.1.3.3)</i>	221
IPv6 Packet (6.1.4)	221
<i>Limitations of IPv4 (6.1.4.1)</i>	221
<i>Introducing IPv6 (6.1.4.2)</i>	222
<i>Encapsulating IPv6 (6.1.4.3)</i>	223
<i>IPv6 Packet Header (6.1.4.4)</i>	224
<i>Sample IPv6 Headers (6.1.4.5)</i>	225
Routing (6.2)	226
Host Routing Tables (6.2.1)	226
<i>Host Packet Forwarding Decision (6.2.1.1)</i>	226
<i>IPv4 Host Routing Table (6.2.1.2)</i>	227
<i>IPv4 Host Routing Entries (6.2.1.3)</i>	228
<i>Sample IPv4 Host Routing Table (6.2.1.4)</i>	229
<i>Sample IPv6 Host Routing Table (6.2.1.5)</i>	231
Router Routing Tables (6.2.2)	232
<i>Router Packet Forwarding Decision (6.2.2.1)</i>	232
<i>IPv4 Router Routing Table (6.2.2.2)</i>	233
<i>Directly Connected Routing Table Entries (6.2.2.3)</i>	234
<i>Remote Network Routing Table Entries (6.2.2.4)</i>	235
<i>Next-Hop Address (6.2.2.5)</i>	236
<i>Sample Router IPv4 Routing Table (6.2.2.6)</i>	236
Routers (6.3)	240
Anatomy of a Router (6.3.1)	240
<i>A Router Is a Computer (6.3.1.1)</i>	240
<i>Router CPU and OS (6.3.1.2)</i>	241
<i>Router Memory (6.3.1.3)</i>	241
<i>Inside a Router (6.3.1.4)</i>	243
<i>Router Backplane (6.3.1.5)</i>	244
<i>Connecting to a Router (6.3.1.6)</i>	245
<i>LAN and WAN Interfaces (6.3.1.7)</i>	245
Router Bootup (6.3.2)	247
<i>Cisco IOS (6.3.2.1)</i>	247
<i>Bootset Files (6.3.2.2)</i>	247
<i>Router Bootup Process (6.3.2.3)</i>	248
<i>Show Version Output (6.3.2.4)</i>	249

Configuring a Cisco Router (6.4) 251

- Configure Initial Settings (6.4.1) 251
 - Router Configuration Steps (6.4.1.1) 251*
- Configure Interfaces (6.4.2) 252
 - Configure LAN Interfaces (6.4.2.1) 252*
 - Verify Interface Configuration (6.4.2.2) 253*
- Configuring the Default Gateway (6.4.3) 254
 - Default Gateway on a Host (6.4.3.1) 254*
 - Default Gateway on a Switch (6.4.3.2) 255*

Summary (6.5) 258**Practice 259**

- Class Activities 259
- Labs 259
- Packet Tracer Activities 259

Check Your Understanding 260**Chapter 7****IP Addressing 265****Objectives 265****Key Terms 265****Introduction (7.0.1.1) 267****IPv4 Network Addresses (7.1) 267**

- IPv4 Address Structure (7.1.1) 267
 - Binary Notation (7.1.1.1) 267*
 - Binary Number System (7.1.1.2) 269*
 - Converting a Binary Address to Decimal (7.1.1.3) 271*
 - Converting from Decimal to Binary (7.1.1.5, 7.1.1.6) 272*
- IPv4 Subnet Mask (7.1.2) 278
 - Network Portion and Host Portion of an IPv4 Address (7.1.2.1) 278*
 - Examining the Prefix Length (7.1.2.2) 279*
 - IPv4 Network, Host, and Broadcast Addresses (7.1.2.3) 281*
 - First Host and Last Host Addresses (7.1.2.4) 284*
 - Bitwise AND Operation (7.1.2.5) 286*
 - Importance of ANDing (7.1.2.6) 288*
- IPv4 Unicast, Broadcast, and Multicast (7.1.3) 290
 - Assigning a Static IPv4 Address to a Host (7.1.3.1) 290*
 - Assigning a Dynamic IPv4 Address to a Host (7.1.3.2) 292*
 - Unicast Transmission (7.1.3.3) 293*
 - Broadcast Transmission (7.1.3.4) 294*
 - Multicast Transmission (7.1.3.5) 296*

Types of IPv4 Addresses (7.1.4)	298
<i>Public and Private IPv4 Addresses (7.1.4.1)</i>	298
<i>Special-Use IPv4 Addresses (7.1.4.3)</i>	299
<i>Legacy Classful Addressing (7.1.4.4)</i>	301
<i>Assignment of IP Addresses (7.1.4.5, 7.1.4.6)</i>	304
IPv6 Network Addresses (7.2)	307
IPv4 Issues (7.2.1)	307
<i>The Need for IPv6 (7.2.1.1)</i>	307
<i>IPv4 and IPv6 Coexistence (7.2.1.2)</i>	309
IPv6 Addressing (7.2.2)	310
<i>Hexadecimal Number System (7.2.2.1)</i>	310
<i>IPv6 Address Representation (7.2.2.2)</i>	312
<i>Rule 1: Omitting Leading 0s (7.2.2.3)</i>	313
<i>Rule 2: Omitting All 0 Segments (7.2.2.4)</i>	315
Types of IPv6 Addresses (7.2.3)	317
<i>IPv6 Address Types (7.2.3.1)</i>	317
<i>IPv6 Prefix Length (7.2.3.2)</i>	318
<i>IPv6 Unicast Addresses (7.2.3.3)</i>	319
<i>IPv6 Link-Local Unicast Addresses (7.2.3.4)</i>	321
IPv6 Unicast Addresses (7.2.4)	322
<i>Structure of an IPv6 Global Unicast Address (7.2.4.1)</i>	322
<i>Static Configuration of a Global Unicast Address (7.2.4.2)</i>	324
<i>Dynamic Configuration of a Global Unicast Address Using SLAAC (7.2.4.3)</i>	326
<i>Dynamic Configuration of a Global Unicast Address Using DHCPv6 (7.2.4.4)</i>	329
<i>EUI-64 Process or Randomly Generated (7.2.4.5)</i>	330
<i>Dynamic Link-Local Addresses (7.2.4.6)</i>	332
<i>Static Link-Local Addresses (7.2.4.7)</i>	333
<i>Verifying IPv6 Address Configuration (7.2.4.8)</i>	334
IPv6 Multicast Addresses (7.2.5)	337
<i>Solicited-Node IPv6 Multicast Addresses (7.2.5.2)</i>	338
Connectivity Verification (7.3)	340
ICMP (7.3.1)	340
<i>ICMPv4 and ICMPv6 Messages (7.3.1.1)</i>	340
<i>ICMPv6 Router Solicitation and Router Advertisement Messages (7.3.1.2)</i>	342
<i>ICMPv6 Neighbor Solicitation and Neighbor Advertisement Messages (7.3.1.3)</i>	343
Testing and Verification (7.3.2)	344
<i>Ping: Testing the Local Stack (7.3.2.1)</i>	344
<i>Ping: Testing Connectivity to the Local LAN (7.3.2.2)</i>	345

	<i>Ping: Testing Connectivity to Remote Device (7.3.2.3)</i>	346
	<i>Traceroute: Testing the Path (7.3.2.4)</i>	347
	Summary (7.4)	349
	Practice	350
	Class Activities	350
	Labs	350
	Packet Tracer Activities	350
	Check Your Understanding	351
Chapter 8	Subnetting IP Networks	355
	Objectives	355
	Key Terms	355
	Introduction (8.0.1.1)	356
	Subnetting an IPv4 Network (8.1)	357
	Network Segmentation (8.1.1)	357
	<i>Reasons for Subnetting (8.1.1.1)</i>	357
	<i>Communication Between Subnets (8.1.1.2)</i>	358
	Subnetting an IPv4 Network (8.1.2)	359
	<i>Basic Subnetting (8.1.2.1)</i>	359
	<i>Subnets in Use (8.1.2.2)</i>	361
	<i>Subnetting Formulas (8.1.2.3)</i>	364
	<i>Creating 4 Subnets (8.1.2.4)</i>	365
	<i>Creating 8 Subnets (8.1.2.5)</i>	368
	<i>Creating 100 Subnets with a /16 Prefix (8.1.2.10)</i>	372
	<i>Calculating the Hosts (8.1.2.11)</i>	374
	<i>Creating 1000 Subnets with a /8 Prefix (8.1.2.12)</i>	375
	Determining the Subnet Mask (8.1.3)	378
	<i>Subnetting Based on Host Requirements (8.1.3.1)</i>	378
	<i>Subnetting Network-Based Requirements (8.1.3.2)</i>	379
	<i>Subnetting to Meet Network Requirements (8.1.3.3, 8.1.3.4)</i>	380
	Benefits of Variable Length Subnet Masking (8.1.4)	384
	<i>Traditional Subnetting Wastes Addresses (8.1.4.1)</i>	384
	VLSM (8.1.4.2)	386
	Basic VLSM (8.1.4.3)	387
	VLSM in Practice (8.1.4.4)	389
	VLSM Chart (8.1.4.5)	391
	Addressing Schemes (8.2)	393
	Structured Design (8.2.1)	393
	<i>Planning to Address the Network (8.2.1.1)</i>	393
	<i>Assigning Addresses to Devices (8.2.1.2)</i>	394

	Design Considerations for IPv6 (8.3)	397
	Subnetting an IPv6 Network (8.3.1)	397
	<i>Subnetting Using the Subnet ID (8.3.1.1)</i>	397
	<i>IPv6 Subnet Allocation (8.3.1.2)</i>	399
	<i>Subnetting into the Interface ID (8.3.1.3)</i>	400
	Summary (8.4)	402
	Practice	404
	Class Activities	404
	Labs	404
	Packet Tracer Activities	404
	Check Your Understanding	405
Chapter 9	Network Access	409
	Objectives	409
	Key Terms	409
	Introduction (9.0.1.1)	411
	Data Link Layer (9.1)	412
	<i>The Data Link Layer (9.1.1.1)</i>	412
	<i>Data Link Sublayers (9.1.1.2)</i>	413
	<i>Media Access Control (9.1.1.3)</i>	414
	<i>Providing Access to Media (9.1.1.4)</i>	415
	Layer 2 Frame Structure (9.1.2)	416
	<i>Formatting Data for Transmission (9.1.2.1)</i>	416
	<i>Creating a Frame (9.1.2.2)</i>	417
	Layer 2 Standards (9.1.3)	418
	<i>Data Link Layer Standards (9.1.3.1)</i>	418
	Media Access Control (9.2)	419
	Topologies (9.2.1)	419
	<i>Controlling Access to the Media (9.2.1.1)</i>	419
	<i>Physical and Logical Topologies (9.2.1.2)</i>	420
	WAN Topologies (9.2.2)	421
	<i>Common Physical WAN Topologies (9.2.2.1)</i>	421
	<i>Physical Point-to-Point Topology (9.2.2.2)</i>	422
	<i>Logical Point-to-Point Topology (9.2.2.3)</i>	423
	<i>Half and Full Duplex (9.2.2.4)</i>	424
	LAN Topologies (9.2.3)	425
	<i>Physical LAN Topologies (9.2.3.1)</i>	425
	<i>Logical Topology for Shared Media (9.2.3.2)</i>	426
	<i>Contention-Based Access (9.2.3.3)</i>	427
	<i>Multi-Access Topology (9.2.3.4)</i>	429
	<i>Controlled Access (9.2.3.5)</i>	429
	<i>Ring Topology (9.2.3.6)</i>	431

Data Link Frame (9.2.4)	431
<i>The Frame (9.2.4.1)</i>	431
<i>The Header (9.2.4.2)</i>	433
<i>Layer 2 Address (9.2.4.3)</i>	433
<i>The Trailer (9.2.4.4)</i>	435
<i>LAN and WAN Frames (9.2.4.5)</i>	435
<i>Ethernet Frame (9.2.4.6)</i>	436
<i>Point-to-Point (PPP) Frame (9.2.4.7)</i>	437
<i>802.11 Wireless Frame (9.2.4.8)</i>	438

Physical Layer (9.3) 441

Purpose of the Physical Layer (9.3.1)	441
<i>The Physical Layer (9.3.1.1)</i>	441
<i>Physical Layer Media (9.3.1.2)</i>	442
<i>Physical Layer Standards (9.3.1.3)</i>	443
Characteristics of the Physical Layer (9.3.2)	444
<i>Physical Layer Functions (9.3.2.1)</i>	445
<i>Physical Components (9.3.2.2)</i>	445
<i>Frame Encoding Techniques (9.3.2.3)</i>	446
<i>Signaling Method (9.3.2.4)</i>	447
<i>Bandwidth (9.3.2.5)</i>	449
<i>Throughput (9.3.2.6)</i>	450

Network Media (9.4) 451

Copper Cabling (9.4.1)	452
<i>Characteristics of Copper Media (9.4.1.1)</i>	452
<i>Copper Media (9.4.1.2)</i>	453
<i>UTP Cable (9.4.1.3)</i>	454
<i>STP Cable (9.4.1.4)</i>	454
<i>Coaxial Cable (9.4.1.5)</i>	455
<i>Copper Media Safety (9.4.1.6)</i>	457
UTP Cabling (9.4.2)	458
<i>Properties of UTP Cabling (9.4.2.1)</i>	458
<i>UTP Cabling Standards (9.4.2.2)</i>	459
<i>UTP Connectors (9.4.2.3)</i>	460
<i>Types of UTP Cable (9.4.2.4)</i>	461
<i>LAN Cabling Areas (9.4.2.5)</i>	462
<i>Testing UTP Cables (9.4.2.6)</i>	464
Fiber Optic Cabling (9.4.3)	465
<i>Properties of Fiber Optic Cabling (9.4.3.1)</i>	465
<i>Fiber Media Cable Design (9.4.3.2)</i>	466
<i>Types of Fiber Media (9.4.3.3)</i>	466
<i>Network Fiber Connectors (9.4.3.4)</i>	468
<i>Testing Fiber Cables (9.4.3.5)</i>	470
<i>Fiber Versus Copper (9.4.3.6)</i>	471

	Wireless Media (9.4.4)	472
	<i>Properties of Wireless Media (9.4.4.1)</i>	472
	<i>Types of Wireless Media (9.4.4.2)</i>	473
	Wireless LAN (9.4.4.3)	475
	802.11 Wi-Fi Standards (9.4.4.4)	476
	Summary (9.5)	478
	Practice	480
	Class Activities	480
	Labs	480
	Packet Tracer Activity	480
	Check Your Understanding	481
Chapter 10	Ethernet	485
	Objectives	485
	Key Terms	485
	Introduction (10.0.1.1)	486
	Ethernet Protocol (10.1)	487
	Ethernet Operation (10.1.1)	487
	<i>LLC and MAC Sublayers (10.1.1.1)</i>	487
	<i>MAC Sublayer (10.1.1.2)</i>	489
	<i>Media Access Control (10.1.1.3)</i>	490
	<i>MAC Address: Ethernet Identity (10.1.1.4)</i>	492
	<i>Frame Processing (10.1.1.5)</i>	493
	Ethernet Frame Attributes (10.1.2)	494
	<i>Ethernet Encapsulation (10.1.2.1)</i>	494
	<i>Ethernet Frame Size (10.1.2.2)</i>	495
	<i>Introduction to the Ethernet Frame (10.1.2.3)</i>	496
	Ethernet MAC (10.1.3)	497
	<i>MAC Addresses and Hexadecimal (10.1.3.1)</i>	497
	<i>MAC Address Representations (10.1.3.2)</i>	500
	<i>Unicast MAC Address (10.1.3.3)</i>	500
	<i>Broadcast MAC Address (10.1.3.4)</i>	501
	<i>Multicast MAC Address (10.1.3.5)</i>	501
	Mac and IP (10.1.4)	502
	<i>MAC and IP (10.1.4.1)</i>	502
	<i>End-to-End Connectivity, MAC, and IP (10.1.4.2)</i>	503
	Address Resolution Protocol (10.2)	504
	<i>Introduction to ARP (10.2.1.1)</i>	504
	<i>ARP Functions (10.2.1.2)</i>	504
	<i>ARP Operation (10.2.1.3)</i>	505
	<i>ARP Role in Remote Communication (10.2.1.4)</i>	508
	<i>Removing Entries from an ARP Table (10.2.1.5)</i>	512
	<i>ARP Tables on Networking Devices (10.2.1.6)</i>	512

ARP Issues (10.2.2)	514
<i>How ARP Can Create Problems (10.2.2.1)</i>	514
<i>Mitigating ARP Problems (10.2.2.2)</i>	515

LAN Switches (10.3) 516

Switching (10.3.1)	516
<i>Switch Port Fundamentals (10.3.1.1)</i>	516
<i>Switch MAC Address Table (10.3.1.2)</i>	517
<i>Duplex Settings (10.3.1.3)</i>	521
<i>Auto-MDIX (10.3.1.4)</i>	522
<i>Frame Forwarding Methods on Cisco Switches (10.3.1.5)</i>	523
<i>Cut-Through Switching (10.3.1.6)</i>	524
<i>Memory Buffering on Switches (10.3.1.8)</i>	525
Fixed or Modular (10.3.2)	526
<i>Fixed Versus Modular Configuration (10.3.2.1)</i>	526
<i>Fixed Configuration Cisco Switches (10.3.2.2)</i>	528
<i>Modular Configuration Cisco Switches (10.3.2.3)</i>	531
<i>Module Options for Cisco Switch Slots (10.3.2.4)</i>	533
Layer 3 Switching (10.3.3)	535
<i>Layer 2 Versus Layer 3 Switching (10.3.3.1)</i>	535
<i>Cisco Express Forwarding (10.3.3.2)</i>	536
<i>Types of Layer 3 Interfaces (10.3.3.3)</i>	537
<i>Configuring a Routed Port on a Layer 3 Switch (10.3.3.4)</i>	538

Summary (10.4) 540

Practice 541

Class Activities	542
Labs	542
Packet Tracer Activities	542

Check Your Understanding 542

Chapter 11 It's a Network 545

Objectives 545

Key Terms 545

Introduction (11.0.1.1) 547

Create and Grow (11.1) 547

Devices in a Small Network (11.1.1)	547
<i>Small Network Topologies (11.1.1.1)</i>	547
<i>Device Selection for a Small Network (11.1.1.2)</i>	548
<i>IP Addressing for a Small Network (11.1.1.3)</i>	550
<i>Redundancy in a Small Network (11.1.1.4)</i>	551
<i>Design Considerations for a Small Network (11.1.1.5)</i>	552

Protocols in a Small Network (11.1.2)	553
<i>Common Applications in a Small Network (11.1.2.1)</i>	554
<i>Common Protocols in a Small Network (11.1.2.2)</i>	555
<i>Real-Time Applications for a Small Network (11.1.2.3)</i>	556
Growing to Larger Networks (11.1.3)	557
<i>Scaling a Small Network (11.1.3.1)</i>	557
<i>Protocol Analysis of a Small Network (11.1.3.2)</i>	558
<i>Evolving Protocol Requirements (11.1.3.3)</i>	559
Keeping the Network Safe (11.2)	560
Network Device Security Measures (11.2.1)	560
<i>Categories of Threats to Network Security (11.2.1.1)</i>	560
<i>Physical Security (11.2.1.2)</i>	561
<i>Types of Security Vulnerabilities (11.2.1.3)</i>	562
Vulnerabilities and Network Attacks (11.2.2)	564
<i>Viruses, Worms, and Trojan Horses (11.2.2.1)</i>	564
<i>Network Attacks (11.2.2.2)</i>	565
Mitigating Network Attacks (11.2.3)	567
<i>Backup, Upgrade, Update, and Patch (11.2.3.1)</i>	567
<i>Authentication, Authorization, and Accounting (11.2.3.2)</i>	568
<i>Firewalls (11.2.3.3)</i>	570
<i>Endpoint Security (11.2.3.4)</i>	571
Securing Devices (11.2.4)	572
<i>Introduction to Securing Devices (11.2.4.1)</i>	572
<i>Passwords (11.2.4.2)</i>	573
<i>Basic Security Practices (11.2.4.3)</i>	574
<i>Enable SSH (11.2.4.4)</i>	576
Basic Network Performance (11.3)	578
Ping (11.3.1)	578
<i>Interpreting Ping Results (11.3.1.1)</i>	578
<i>Extended Ping (11.3.1.2)</i>	580
<i>Network Baseline (11.3.1.3)</i>	581
Tracert (11.3.2)	583
<i>Interpreting Tracert Messages (11.3.2.1)</i>	583
show Commands (11.3.3)	585
<i>Common show Commands Revisited (11.3.3.1)</i>	585
<i>Viewing Router Settings with the show version Command (11.3.3.2)</i>	588
<i>Viewing Switch Settings with the show version Command (11.3.3.3)</i>	589

Host and IOS Commands (11.3.4)	590
<i>ipconfig Command Options (11.3.4.1)</i>	590
<i>arp Command Options (11.3.4.2)</i>	591
<i>show cdp neighbors Command Options (11.3.4.3)</i>	592
<i>Using the show ip interface brief Command (11.3.4.4)</i>	594

Managing IOS Configuration Files (11.4) 596

Router and Switch File Systems (11.4.1)	596
<i>Router File Systems (11.4.1.1)</i>	596
<i>Switch File Systems (11.4.1.2)</i>	598
Back Up and Restore Configuration Files (11.4.2)	599
<i>Backing Up and Restoring Using Text Files (11.4.2.1)</i>	600
<i>Backing Up and Restoring Using TFTP (11.4.2.2)</i>	601
<i>Using USB Ports on a Cisco Router (11.4.2.3)</i>	602
<i>Backing Up and Restoring Using a USB (11.4.2.4)</i>	603

Summary (11.5) 607

Practice 608

Class Activities	609
Labs	609
Packet Tracer Activities	609

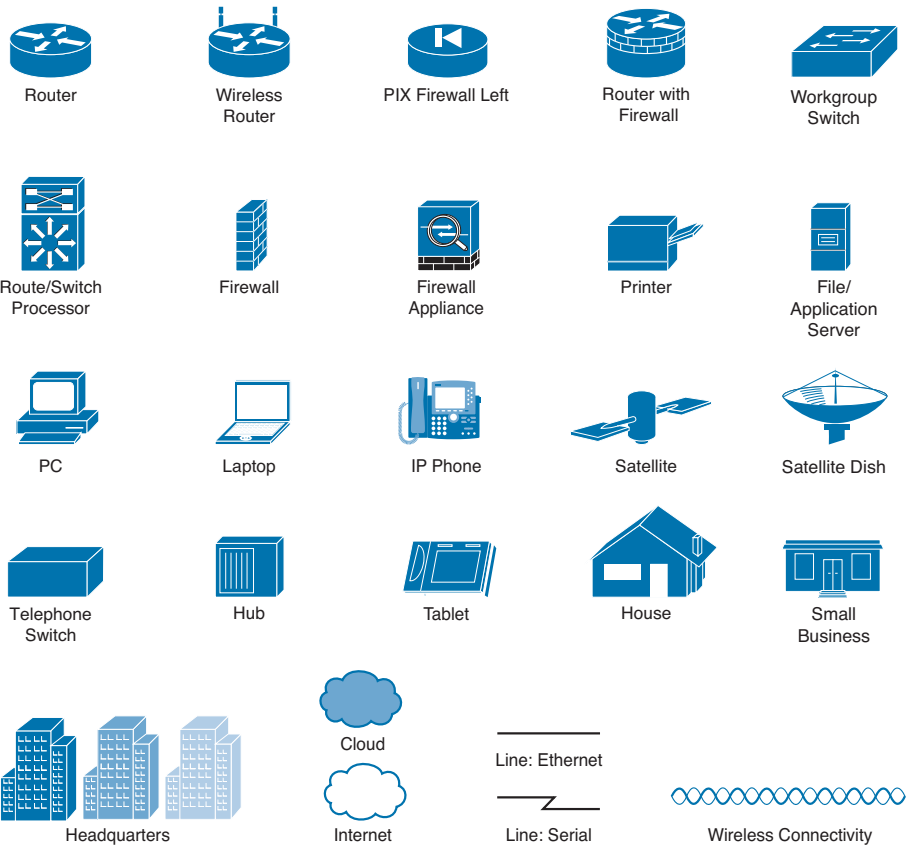
Check Your Understanding 609

Appendix A Answers to the “Check Your Understanding” Questions 613

Glossary 625

Index 653

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).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

Network Basics Companion Guide is the official supplemental textbook for the CCNA Routing and Switching Network Basics course in the Cisco Networking Academy Program.

As a textbook, this book provides a ready reference to explain the same networking concepts, technologies, protocols, and devices that are covered in the online course. This book emphasizes key topics, terms, and activities and provides some alternate explanations and examples as compared with the online course. You can use the online curriculum as directed by your instructor and then use this *Companion Guide*'s study tools to help solidify your understanding of all the topics.

Who Should Read This Book

This book is intended for students in the Cisco Networking Academy CCNA Routing and Switching Network Basics course. The goal of this book is to introduce you to fundamental networking concepts and technologies. In conjunction with the online course materials, this book will assist you in developing the skills necessary to plan and implement small networks across a range of applications. The specific skills covered in each chapter are described at the start of each chapter.

Book Features

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

Topic Coverage

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

- **Objectives:** Listed at the beginning of each chapter, the objectives reference the core concepts covered in the chapter. The objectives match the objectives stated in the corresponding chapters of the online curriculum; however, the question format in the *Companion Guide* encourages you to think about finding the answers as you read the chapter.
- **“How-to” feature:** When this book covers a set of steps that you need to perform for certain tasks, the text lists the steps as a how-to list. When you are studying, the icon helps you easily refer to this feature as you skim through the book.

- **Chapter summaries:** Each chapter includes a summary of the chapter's key concepts. It provides a synopsis of the chapter and serves as a study aid.
- **“Practice” section:** The end of each chapter includes a full list of all the Labs, Class Activities, and Packet Tracer Activities covered in that chapter.

Readability

The following features have been updated to assist your understanding of the networking vocabulary:

- **Key terms:** Each chapter begins with a list of key terms, along with a page-number reference for each key term. The key terms are listed in the order in which they are explained in the chapter. This handy reference allows you to find a term, flip to the page where the term appears, and see the term used in context. The Glossary defines all the key terms.
- **Glossary:** This book contains an all-new Glossary with more than 250 terms.

Practice

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

- **Check Your Understanding questions and answer key:** Updated review questions are presented at the end of each chapter as a self-assessment tool. These questions match the style of questions that you see in the online course. Appendix A, “Check Your Understanding Answer Key,” provides an answer key to all the questions and includes an explanation of each answer.
- **Labs and Activities:** Throughout each chapter you will be directed to the online course to take advantage of the activities created to reinforce concepts. In addition, the end of each chapter includes a “Practice” section that collects a list of all the labs and activities to provide practice with the topics introduced in the chapter. The Labs and Class Activities are available in the companion *Network Basics Lab Manual* (978-158713-313-8). The Packet Tracer Activities PKA files are found in the online course.
- **Page references to online course:** After each heading you will see, for example, (1.1.2.3). This number refers to the page number in the online course so that you can easily jump to that spot online to view a video, practice an activity, perform a lab, or review a topic.

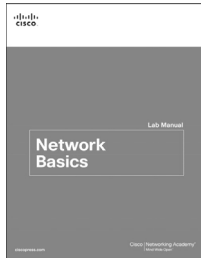


Packet Tracer
□ Activity

Video

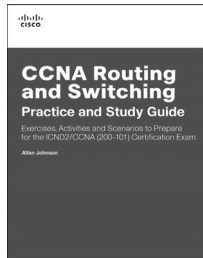
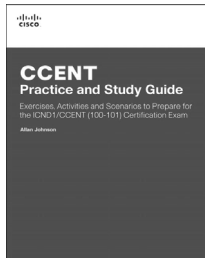
Lab Manual

The supplementary book *Network Basics Lab Manual* (978-158713-313-8), contains all the Labs and Class Activities from the course.



Practice and Study Guide

Additional study exercises, activities, and scenarios are available in the new *CCENT Practice and Study Guide* (978-158713-345-9) and *CCNA Routing and Switching Practice and Study Guide* (978-158713-344-2) books by Allan Johnson. Each Practice and Study Guide coordinates with the recommended curriculum sequence—one focusing on courses 1 and 2 (ICND1/CCENT topics) and the second focusing on courses 3 and 4 (ICND2/CCNA topics).



About Packet Tracer Software and Activities



Interspersed throughout the chapters you'll find many activities to work with the Cisco Packet Tracer tool. Packet Tracer enables you to create networks, visualize how packets flow in the network, and use basic testing tools to determine whether the network would work. When you see the Packet Tracer Activity icon, you can use Packet Tracer with the listed file to perform a task suggested in this book. The activity files are available in the course. Packet Tracer software is available only through the Cisco Networking Academy website. Ask your instructor for access to Packet Tracer.

How This Book Is Organized

This book corresponds closely to the Cisco Networking Academy Network Basics course and is divided into 11 chapters, one appendix, and a glossary of key terms:

- **Chapter 1, “Exploring the Network”:** This chapter introduces the platform of data networks upon which our social and business relationships increasingly depend. The material lays the groundwork for exploring the services, technologies, and issues encountered by network professionals as they design, build, and maintain the modern network.
- **Chapter 2, “Configuring a Network Operating System”:** This chapter references a basic network topology, consisting of two switches and two PCs, to demonstrate the use of Cisco IOS.
- **Chapter 3, “Network Protocols and Communications”:** In this chapter you will learn about two layered models that describe network rules and functions. These models, as well as the standards that make the networks work, are discussed here to give context to detailed study of the model layers in the following chapters.
- **Chapter 4, “Application Layer”:** This chapter explores the role of the application layer and how the applications, services, and protocols within the application layer make robust communication across data networks possible.
- **Chapter 5, “Transport Layer”:** This chapter examines the role of the transport layer in encapsulating application data for use by the network layer. The concepts of reliable data delivery and multiple application conversations are also introduced.
- **Chapter 6, “Network Layer”:** This chapter focuses on the role of the network layer. It examines how it divides networks into groups of hosts to manage the flow of data packets within a network. It also covers how communication between networks is facilitated through routing processes.
- **Chapter 7, “IP Addressing”:** This chapter describes the structure of IP addresses and their application to the construction and testing of IP networks and subnetworks.
- **Chapter 8, “Subnetting IP Networks”:** This chapter examines the creation and assignment of IP network and subnetwork addresses through the use of the subnet mask.
- **Chapter 9, “Network Access”:** This chapter introduces the general functions of the data link layer and the protocols associated with it. It also covers the general functions of the physical layer and the standards and protocols that manage the transmission of data across local media.

- **Chapter 10, “Ethernet”:** This chapter examines the characteristics and operation of Ethernet as it has evolved from a shared-media, contention-based data communications technology to today’s high-bandwidth, full-duplex technology.
- **Chapter 11, “It’s A Network”:** Having considered the services that a data network can provide to the human network, examined the features of each layer of the OSI model and the operations of TCP/IP protocols, and looked in detail at Ethernet, a universal LAN technology, this chapter discusses how to assemble these elements together in a functioning network that can be maintained
- **Appendix A, “Check Your Understanding Answer Key”:** This appendix lists the answers to the “Check Your Understanding” review questions included at the end of each chapter.
- **Glossary:** The Glossary provides you with definitions for all the key terms identified in each chapter.

Exploring the Network

Objectives

Upon completion of this chapter, you will be able to answer the following questions:

- How do networks affect the way we interact when we learn, work, and play?
- How do networks support communication?
- What is a converged network?
- What are the four requirements for a reliable network?
- How are network devices used?
- How do local-area network (LAN) devices compare to wide-area network (WAN) devices?
- What is the basic structure of the Internet?
- How do LANs and WANs interconnect the Internet?
- What is the effect of Bring Your Own Device (BYOD) use, online collaboration, video, and cloud computing on a business network?
- How do expanding networking trends affect security considerations?
- What are the three Cisco enterprise architectures and how do they meet the needs of an evolving network environment?

Key Terms

This chapter uses the following key terms. You can find the definitions in the Glossary.

Internet page 4

instant messaging (IM) page 7

social media page 8

collaboration tools page 8

weblogs (blogs) page 8

wikis page 8

podcasting page 8

peer-to-peer (P2P) file sharing page 8

quality of service (QoS) page 12

converged network page 13

fault tolerant page 15

packets page 17

scalable page 19

security page 21

network service page 24

end devices page 24

host device page 24

intermediary devices page 25

medium (media) page 25

local-area network (LAN) page 29

wide-area network (WAN) page 29

wireless LAN (WLAN) page 29

storage-area network (SAN) page 29

intranet page 32

extranet page 32

cable page 33

DSL page 33

cellular page 33

satellite page 33

dial-up page 34

dedicated leased line page 34

Metro Ethernet page 35

Bring Your Own Device (BYOD) page 36

cloud computing page 40

Introduction (1.0.1.1)

We now stand at a critical turning point in the use of technology to extend and empower our ability to communicate. The globalization of the Internet has succeeded faster than anyone could have imagined. The manner in which social, commercial, political, and personal interactions occur is rapidly changing to keep up with the evolution of this global network. In the next stage of our development, innovators will use the Internet as a starting point for their efforts as they create new products and services specifically designed to take advantage of the network capabilities. As developers push the limits of what is possible, the capabilities of the interconnected networks that form the Internet will play an increasing role in the success of these projects.

This chapter introduces the platform of data networks upon which our social and business relationships increasingly depend. The material lays the groundwork for exploring the services, technologies, and issues encountered by network professionals as they design, build, and maintain the modern network.



Class Activity 1.0.1.2: Draw Your Concept of the Internet

The Networking Academy curriculum has a new component called Modeling Activities. You will find them at the beginning and end of each chapter. Some activities can be completed individually (at home or in class), and some will require group or learning-community interaction. Your instructor will be facilitating so that you can obtain the most from these introductory activities. These activities will help you enhance your understanding by providing an opportunity to visualize some of the abstract concepts that you will be learning in this course. Be creative and enjoy these activities!

The Network Basics Lab Manual (ISBN 978-1-58713-313-8) contains all the Labs and Class Activities from the course. You can access the full instructions in the course itself or in this printed Lab Manual.

Here is your first modeling activity:

Draw Your Concept of the Internet

In this activity you will draw and label a map of the Internet as you interpret it now. Include your home or school/university location and its respective cabling, equipment, devices, etc. The following are some items you may want to include:

- Devices/Equipment
- Media (cabling)
- Link Addresses or Names
- Sources & Destinations
- Internet Service Providers

Upon completion, be sure to save your work in a hard-copy format, as it will be used for future reference at the end of this chapter. If it is an electronic document, save it to a server location provided by your instructor. Be prepared to share and explain your work in class.

For an example to get you started, please visit <http://www.kk.org/internet-mapping/>.

Communicating in a Network-Centric World (1.1)

Communication methods are constantly evolving, and the changes affect the way we interact with family, friends, and society. This chapter explores how we came to communicate over computer networks.

Interconnecting Our Lives (1.1.1)

In this section we will look at how people use networked computers to learn, work, and play.

Networks in Our Daily Lives (1.1.1.1)

Among all of the essentials for human existence, the need to interact with others ranks just below our need to sustain life. Communication is almost as important to us as our reliance on air, water, food, and shelter.

The methods that we use to communicate are constantly changing and evolving. Whereas we were once limited to face-to-face interactions, breakthroughs in technology have significantly extended the reach of our communications. From cave paintings to the printing press to radio and television, each new development has improved and enhanced our ability to connect and communicate with others.

The creation and interconnection of robust data networks has had a profound effect on communication, and has become the new platform on which modern communications occur.

Networks connect people and promote unregulated communication. Networks are the platforms on which to run businesses, to address emergencies, to inform individuals, and to support education, science, and government. The Internet is the largest network in existence. In fact, the term *Internet* means a network of networks. It is actually a collection of interconnected private and public networks. It is incredible how quickly the Internet has become an integral part of our daily routines.

Technology Then and Now (1.1.1.2)

Imagine a world without the Internet. No more Google, YouTube, instant messaging, Facebook, Wikipedia, online gaming, Netflix, iTunes, and easy access to current information. No more price comparison websites, avoiding lines by shopping online, or quickly looking up phone numbers and map directions to various locations at the click of a finger. How different would our lives be without all of this? That was the world we lived in just 15 to 20 years ago. But over the years, data networks have slowly expanded and been repurposed to improve the quality of life for people everywhere.

In the course of a day, resources that are available through the Internet can help you

- Post and share your photographs, home videos, and experiences with friends or with the world
- Access and submit school work
- Communicate with friends, family, and peers using email, instant messaging, or video applications
- Watch videos, movies, or television episodes on demand
- Play online games with friends
- Decide what to wear using online current weather conditions
- Find the least congested route to your destination by displaying weather and traffic video from webcams
- Check your bank balance and pay bills electronically

Innovators are figuring out new ways to use the Internet more every day. As developers push the limits of what is possible, the capabilities of the Internet and the role the Internet plays in our lives will expand broader and broader. Consider the changes that have happened within the last couple of decades, as depicted in Figure 1-1. Now consider what changes will happen within the next decade. What else do you think we will be able to do using the network as the platform?

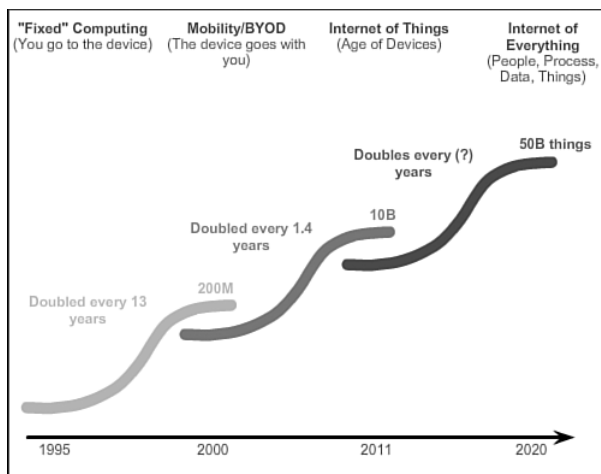


Figure 1-1 Computing Timeline

The Global Community (1.1.1.3)

Advancements in networking technologies are perhaps the most significant change agent in the world today. They are helping to create a world in which national borders, geographic distances, and physical limitations become less relevant, and present ever-diminishing obstacles.

The Internet has changed the manner in which social, commercial, political, and personal interactions occur. The immediate nature of communications over the Internet encourages the creation of global communities. Global communities allow for social interaction that is independent of location or time zone. The creation of online communities for the exchange of ideas and information has the potential to increase productivity opportunities across the globe.

Cisco refers to this as the *human network*. The human network centers on the impact of the Internet and networks on people and businesses.

How has the human network affected you?

Networks Support the Way We Learn (1.1.1.4)

Networks and the Internet have changed everything we do—the way we learn, the way we communicate, how we work, and even how we play.

Changing the Way We Learn

Communication, collaboration, and engagement are fundamental building blocks of education. Institutions are continually striving to enhance these processes to maximize the dissemination of knowledge. Traditional learning methods provide primarily two

sources of expertise from which the student can obtain information: the textbook and the instructor. These two sources are limited, both in the format and the timing of the presentation.

Networks have changed the way we learn. Robust and reliable networks support and enrich student learning experiences. They deliver learning material in a wide range of formats, including interactive activities, assessments, and feedback. Networks now

- Support the creation of virtual classrooms
- Provide on-demand video
- Enable collaborative learning spaces
- Enable mobile learning

Access to high-quality instruction is no longer restricted to students living in proximity to where that instruction is being delivered. Online distance learning has removed geographic barriers and improved student opportunity. Online (e-learning) courses can now be delivered over a network. These courses can contain data (text, links), voice, and video available to the students at any time from any place. Online discussion groups and message boards enable a student to collaborate with the instructor, with other students in the class, or even with students across the world. Blended courses can combine instructor-led classes with online courseware to provide the best of both delivery methods.

In addition to the benefits for the student, networks have improved the management and administration of courses as well. Some of these online functions include student enrollment, assessment delivery, and progress tracking.

Networks Support the Way We Communicate (1.1.1.5)

Changes in network communications have enabled friends, families, and businesses to communicate in ways that could only be imagined by previous generations.

Changing the Way We Communicate

The globalization of the Internet has ushered in new forms of communication that empower individuals to create information that can be accessed by a global audience.

Some forms of communications include

- **Instant messaging (IM) and texting:** IM and texting both enable instant, real-time communication between two or more people. Many IM and texting applications incorporate features such as file transfer. IM applications can offer additional features such as voice and video communication.

- **Social media:** Social media consists of interactive websites where people and communities create and share user-generated content with friends, family, peers, and the world.
- **Collaboration tools:** Collaboration tools give people the opportunity to work together on shared documents. Without the constraints of location or time zone, individuals connected to a shared system can speak to each other, often across real-time, interactive video. Across the network, they can share text and graphics, and edit documents together. With collaboration tools always available, organizations can move quickly to share information and pursue goals. The broad distribution of data networks means that people in remote locations can contribute on an equal basis with people at the heart of large population centers.
- **Weblogs (blogs):** Weblogs are web pages that are easy to update and edit. Unlike commercial websites, which are created by professional communications experts, blogs give anyone, including those without technical knowledge of web design, a means to communicate their thoughts to a global audience. There are blogs on nearly every topic one can think of, and communities of people often form around popular blog authors.
- **Wikis:** Wikis are web pages that groups of people can edit and view together. Whereas a blog is more of an individual, personal journal, a wiki is a group creation. As such, it may be subject to more extensive review and editing. Like blogs, wikis can be created in stages, and by anyone, without the sponsorship of a major commercial enterprise. Wikipedia has become a comprehensive resource—an online encyclopedia—of publicly contributed topics. Private organizations and individuals can also build their own wikis to capture collected knowledge on a particular subject. Many businesses use wikis as their internal collaboration tool. With the global Internet, people of all walks of life can participate in wikis and add their own perspectives and knowledge to a shared resource.
- **Podcasting:** Podcasting is an audio-based medium that originally enabled people to record audio and convert it for use. Podcasting allows people to deliver their recordings to a wide audience. The audio file is placed on a website (or blog or wiki) where others can download it and play the recording on their computers, laptops, and other mobile devices.
- **Peer-to-peer (P2P) file sharing:** Peer-to-peer file sharing enables people to share files with each other without having to store the files on and download them from a central server. The user joins the P2P network by simply installing the P2P software. This lets them locate and share files with others in the P2P network. The widespread digitization of media files, such as music and video files, has increased the interest in P2P file sharing. P2P file sharing has not been embraced by everyone. Many people are concerned that widespread use of P2P has enabled many to violate the laws of copyrighted materials.

What other sites or tools do you use to share your thoughts?

Networks Support the Way We Work (1.1.1.6)

Businesses, whether a small family business or a multinational corporation, have changed the way they operate to reap the benefits of network communications.

Changing the Way We Work

In the business world, data networks were initially used by businesses to internally record and manage financial information, customer information, and employee payroll systems. These business networks evolved to enable the transmission of many different types of information services, including email, video, messaging, and telephony.

The use of networks to provide efficient and cost-effective employee training is increasing in acceptance. Online learning opportunities can decrease time-consuming and costly travel yet still ensure that all employees are adequately trained to perform their jobs in a safe and productive manner.

There are many success stories illustrating innovative ways networks are being used to make us more successful in the workplace. Some of these scenarios are available through the Cisco website at <http://www.cisco.com>.

Networks Support the Way We Play (1.1.1.7)

Games, music, and TV are all enjoyed in significantly different ways than a decade ago due to changes in network communications.

Changing the Way We Play

The widespread adoption of the Internet by the entertainment and travel industries enhances the ability to enjoy and share many forms of recreation, regardless of location. It is possible to explore places interactively that previously we could only dream of visiting, as well as preview the actual destinations before making a trip. Travelers can post the details and photographs from their adventures online for others to view.

In addition, the Internet is used for traditional forms of entertainment. We listen to recording artists, preview or view motion pictures, read entire books, and download material for future offline access. Live sporting events and concerts can be experienced as they are happening, or recorded and viewed on demand.

Networks enable the creation of new forms of entertainment, such as online games. Players participate in any kind of online competition that game designers can imagine. We compete with friends and foes around the world in the same manner as if they were in the same room.

Even offline activities are enhanced using network collaboration services. Global communities of interest have grown rapidly. We share common experiences and hobbies well beyond our local neighborhood, city, or region. Sports fans share opinions and facts about their favorite teams. Collectors display prized collections and get expert feedback about them.

Online markets and auction sites provide the opportunity to buy, sell, and trade all types of merchandise.

Whatever form of recreation we enjoy in the human network, networks are improving our experience.

How do you play on the Internet?



Lab 1.1.1.8: Researching Network Collaboration Tools

In this lab you will use collaboration tools, share documents with Google Drive, explore conferencing and web meetings, and create wiki pages.

Supporting Communication (1.1.2)

This section discusses the various forms of communication, expected communication behaviors, and communication styles.

What Is Communication? (1.1.2.1)

Communication in our daily lives takes many forms and occurs in many environments. We have different expectations depending on whether we are chatting via the Internet or participating in a job interview. Each situation has its corresponding expected behaviors and styles.

Establishing the Rules

Before beginning to communicate with each other, we establish rules or agreements to govern the conversation. These rules, or protocols, must be followed in order for the message to be successfully delivered and understood. Figures 1-2, 1-3, and 1-4 depict a few of these rules. Among the protocols that govern successful human communication are the following:

- Identified sender and receiver
- Agreed-upon method of communicating (face-to-face, telephone, letter, photograph; see Figure 1-2)
- Common language and grammar (see Figure 1-3)

- Speed and timing of delivery
- Confirmation or acknowledgement requirements (see Figure 1-4)

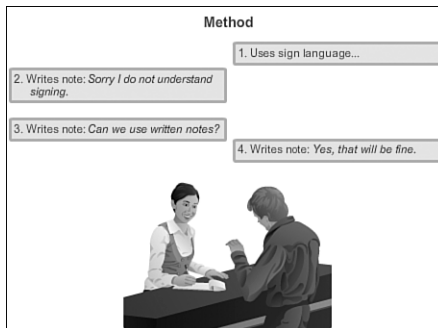


Figure 1-2 Agreeing on a Communication Method

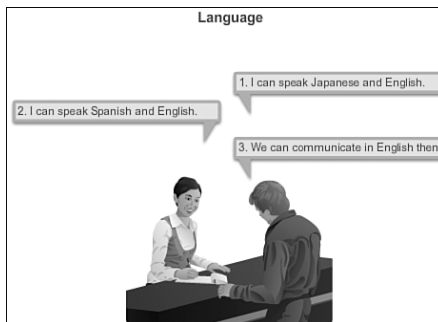


Figure 1-3 Agreeing on a Common Language

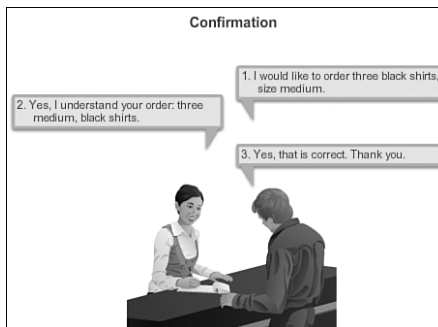


Figure 1-4 Confirming a Message

Communication rules may vary according to the context. If a message conveys an important fact or concept, a confirmation that the message has been received and understood is necessary. Less important messages may not require an acknowledgement from the recipient.

The techniques that are used in network communications share these fundamentals with human conversations.

Quality of Communication (1.1.2.2)

Communication between individuals is determined to be successful when the meaning of the message understood by the recipient matches the meaning intended by the sender. For data networks, we use the same basic criteria to judge success. However, as a message moves through the network, many factors can prevent the message from reaching the recipient or distort its intended meaning. These factors can be either external or internal.

External QoS Factors

The external *quality of service (QoS)* factors affecting data communications are related to the complexity of the network and the number of devices a message must pass through on its route to its final destination.

External QoS factors affecting the success of communication include

- The quality of the pathway between the sender and the recipient
- The number of times the message has to change form
- The number of times the message has to be redirected or readdressed
- The number of other messages being transmitted simultaneously on the communication network
- The amount of time allotted for successful communication

QoS will be discussed in greater detail throughout the course.

Internal QoS Factors

Internal QoS factors that interfere with network communications are related to the nature of the message itself. Different types of messages may vary in complexity and importance. Clear and concise messages are usually easier to understand than complex messages. Important communications require more care to ensure that they are delivered and understood by the recipient.

Internal factors affecting successful communications across the network include

- The size of the message
- The complexity of the message
- The importance of the message

Large messages may be interrupted or delayed at different points within the network. A message with a low importance or priority could be dropped if the network becomes overloaded.

Both the internal and external factors that affect the receipt of a message must be anticipated and controlled for network communications to be successful. New innovations in network hardware and software are being implemented to ensure the quality and reliability of network communications.

The Network as a Platform (1.2)

In the past, traditional networks such as television, telephone, and computer networks worked in very different ways. This chapter explores how those differences are rapidly shrinking.

Converged Networks (1.2.1)

In this section you will learn how different types of networks are becoming increasingly alike as network technologies change.

Traditional Service Networks (1.2.1.1)

Modern networks are constantly evolving to meet user demands. Early data networks were limited to exchanging character-based information between connected computer systems. Traditional telephone and television networks were maintained separately from data networks. In the past, every one of these services required a dedicated network, with different communications channels and different technologies to carry a particular communication signal. Each service had its own set of rules and standards to ensure successful communication.

Consider a hospital built 40 years ago. Back then, hospital rooms were cabled for the data network, telephone network, and video network for televisions. These separate networks were disparate, meaning that they could not communicate with each other, as shown on the left in Figure 1-5.

Advances in technology are enabling us to consolidate these different kinds of networks onto one platform, referred to as the *converged network*. Unlike dedicated networks, converged networks are capable of delivering voice, video streams, text, and graphics between many different types of devices over the same communications channel and network structure, as shown on the right in Figure 1-5. Previously separate and distinct communication forms have converged onto a common platform. This platform provides access to a wide range of alternative and new communication methods that enable people to interact directly with each other almost instantaneously.

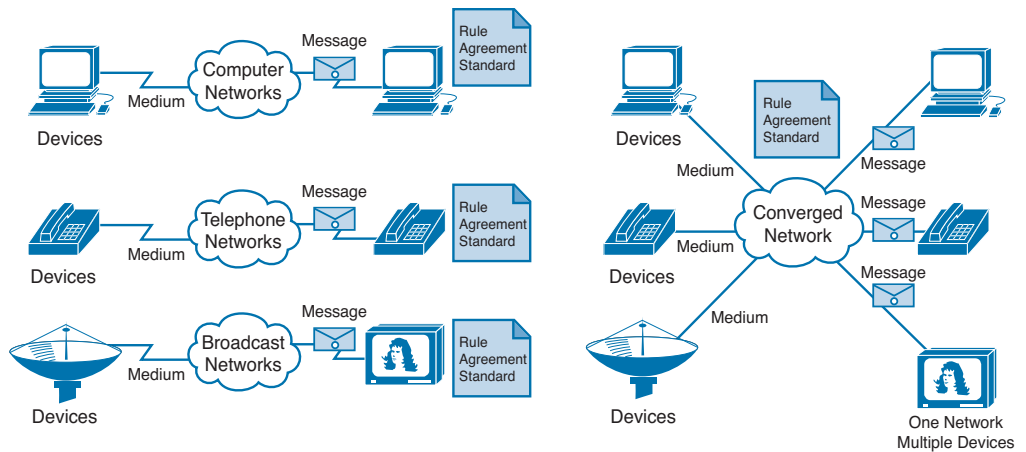


Figure 1-5 Traditional Networks (Left) and Converged Network (Right)

On a converged network, there are still many points of contact and many specialized devices, such as personal computers, phones, TVs, and tablet computers, but there is one common network infrastructure. This network infrastructure uses the same set of rules, agreements, and implementation standards.

Planning for the Future (1.2.1.2)

The convergence of the different types of communications networks onto one platform represents the first phase in building the intelligent information network. We are currently in this phase of network evolution. The next phase will be to not only consolidate the different types of messages onto a single network, but also consolidate the applications that generate, transmit, and secure the messages onto integrated network devices.

Not only will voice and video be transmitted over the same network, the devices that perform the telephone switching and video broadcasting will be the same devices that route the messages through the network. The resulting communications platform will provide high-quality application functionality at a reduced cost.

The pace at which the development of exciting new converged network applications is occurring can be attributed to the rapid growth and expansion of the Internet. This expansion has created a wider audience for whatever message, product, or service can be delivered. The underlying mechanics and processes that drive this explosive growth have resulted in a network architecture that is both capable of supporting changes and able to grow. As the supporting technology platform for living, learning, working, and playing in the human network, the network architecture of the Internet must adapt to constantly changing requirements for a high quality of service and security.



Lab 1.2.1.3: Researching Converged Network Services

In this lab you will explore converged services offered by local ISPs and research how converged networks are in use by institutions.

Reliable Network (1.2.2)

In this section you will learn about characteristics of a reliable network.

The Supporting Network Architecture (1.2.2.1)

Networks must support a wide range of applications and services, as well as operate over many different types of cables and devices that make up the physical infrastructure. The term *network architecture*, in this context, refers to the technologies that support the infrastructure and the programmed services and rules, or protocols, that move messages across the network.

As networks evolve, we are discovering that there are four basic characteristics that the underlying architectures need to address in order to meet user expectations:

- Fault tolerance
- Scalability
- QoS
- Security

Fault Tolerance in Circuit-Switched Networks (1.2.2.2)

Designing for unforeseen problems is an essential element of network design. This section explains how networks can manage unexpected equipment failure.

Fault Tolerance

The expectation is that the Internet is always available to the millions of users who rely on it. This requires a network architecture that is built to be *fault tolerant*. A fault-tolerant network is one that limits the effect of a failure, so that the fewest number of devices are affected by it. It is also built in a way that enables quick recovery when such a failure occurs. Fault-tolerant networks depend on multiple paths between the source and destination of a message. If one path fails, the messages can be instantly sent over a different link. Having multiple paths to a destination is known as redundancy, as shown in Figure 1-6.

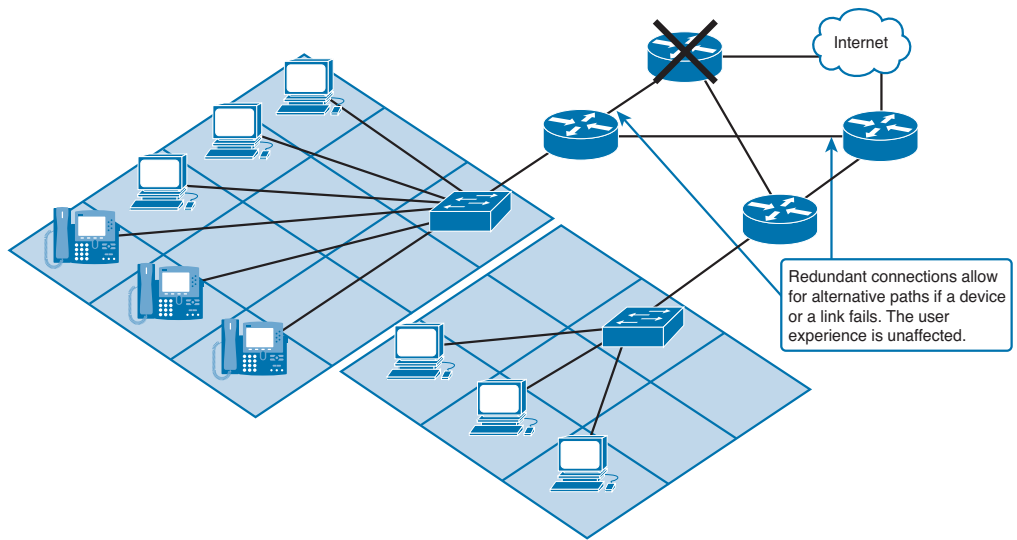


Figure 1-6 Fault Tolerance

Circuit-Switched, Connection-Oriented Networks

To understand the need for redundancy, we can look at how early telephone systems worked. When a person made a call using a traditional telephone set, the call first went through a setup process. This process identified the telephone switching locations between the person making the call (the source) and the phone set receiving the call (the destination). A temporary path, or *circuit*, was created for the duration of the telephone call. If any link or device in the circuit failed, the call was dropped. To reconnect, a new call had to be made, with a new circuit. This connection process is referred to as a circuit-switched process and is illustrated in Figure 1-7.

Many circuit-switched networks give priority to existing circuit connections at the expense of new circuit requests. After a circuit is established, even if no communication is occurring between the persons on either end of the call, the circuit remains connected and resources are used until one of the parties disconnects the call. Because there are only so many circuits that can be created, it is possible to get a message that all circuits are busy and a call cannot be placed. The cost to create many alternative paths with enough capacity to support a large number of simultaneous circuits, and the technologies necessary to dynamically re-create dropped circuits in the event of a failure, are why circuit-switched technology was not optimal for the Internet.

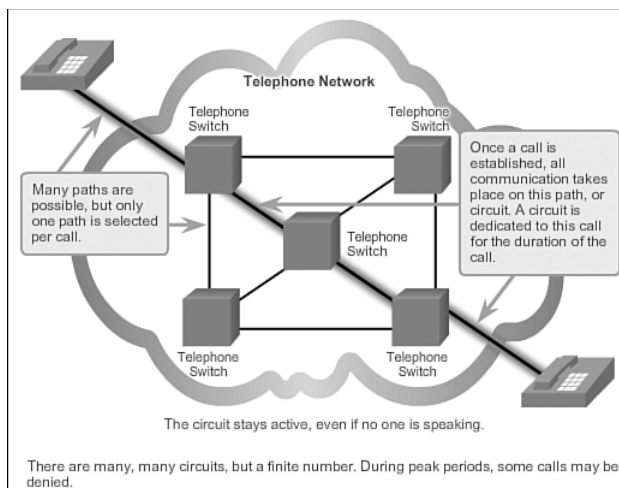


Figure 1-7 Circuit-Switched Network

Packet-Switched Networks (1.2.2.3)

In the search for a network that was more fault tolerant, the early Internet designers researched packet-switched networks. The premise for this type of network is that a single message can be broken into multiple message blocks, with each message block containing addressing information to indicate the origination point and final destination. Using this embedded information, these message blocks, called *packets*, can be sent through the network along various paths, and can be reassembled into the original message when they reach their destination. Figure 1-8 demonstrates how packets can travel different paths and arrive at the correct destination for sorting.

The devices within the network itself are typically unaware of the content of the individual packets. The only packet information used by intermediate devices is the original source address and the final destination address. These addresses are often referred to as *IP addresses*, represented in a dotted decimal format such as 10.10.10.10. Each packet is sent independently from one location to another. At each location, a routing decision is made as to which path to use to forward the packet toward its final destination. If a previously used path is no longer available, the routing function can dynamically choose the next best available path. Because the messages are sent in pieces, rather than as a single complete message, the few packets that may be lost can be retransmitted to the destination along a different path. In many cases, the destination device is unaware that any failure or rerouting occurred.

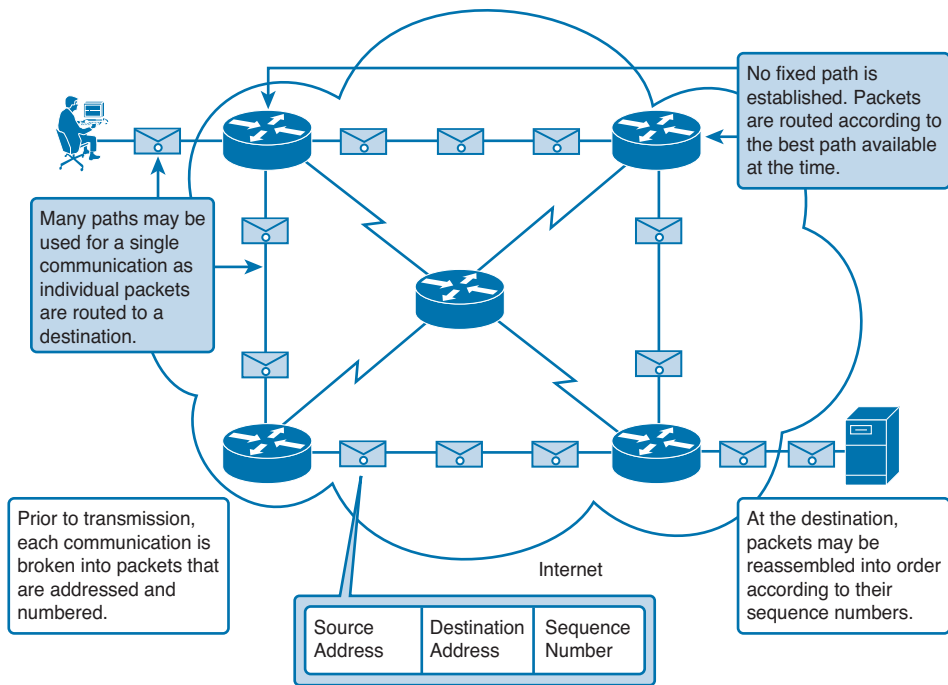


Figure 1-8 Packet-Switched Network

The need for a single, reserved circuit from end to end does not exist in a packet-switched network. Any piece of a message can be sent through the network using any available path. Additionally, packets containing pieces of messages from different sources can travel the network at the same time. By providing a method to dynamically use redundant paths, without intervention by the user, the Internet has become a fault-tolerant method of communication.

Although packet-switched, connectionless networks are the primary infrastructure for today's Internet, there are some benefits to a connection-oriented system like the circuit-switched telephone system. Because resources at the various switching locations are dedicated to providing a finite number of circuits, the quality and consistency of messages transmitted across a connection-oriented network can be guaranteed. Another benefit is that the provider of the service can charge the users of the network for the period of time that the connection is active. The ability to charge users for active connections through the network is a fundamental premise of the telecommunication service industry.

Scalable Networks (1.2.2.4)

Designing a network that will be able to efficiently expand is an important network design consideration.

Scalability

Thousands of new users and service providers connect to the Internet each week. In order for the Internet to support this rapid amount of growth, it must be scalable. A *scalable* network can expand quickly to support new users and applications without affecting the performance of the service being delivered to existing users. Figure 1-9 depicts a scalable network accepting additional users.

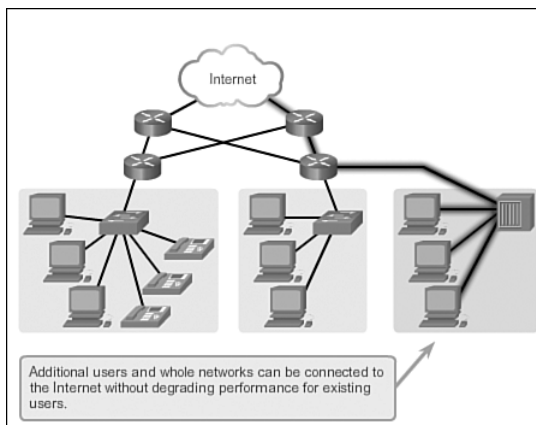


Figure 1-9 Scalability

The fact that the Internet is able to expand at the rate that it is, without seriously impacting the performance experienced by individual users, is a function of the design of the protocols and underlying technologies on which it is built. The Internet has a hierarchical, layered structure for addressing, for naming, and for connectivity services. As a result, network traffic that is destined for local or regional services does not need to traverse to a central point for distribution. Common services can be duplicated in different regions, thereby keeping traffic off the higher-level backbone networks.

Scalability also refers to the ability to accept new products and applications. Although there is no single organization that regulates the Internet, the many individual networks that provide Internet connectivity cooperate to follow accepted standards and protocols. The adherence to standards enables the manufacturers of hardware and software to concentrate on product development and improvements in the areas of performance and capacity, knowing that the new products can integrate with and enhance the existing infrastructure.

The current Internet architecture, while highly scalable, may not always be able to keep up with the pace of user demand. New protocols and addressing structures are under development to meet the increasing rate at which Internet applications and services are being added.

Providing QoS (1.2.2.5)

A well-designed network can prioritize network traffic to provide users with reliable quality of service, or QoS.

Quality of Service

Quality of service is also an ever-increasing requirement of networks today. New applications available to users over internetworks, such as voice and live video transmissions, as shown in Figure 1-10, create higher expectations for the quality of the delivered services. Have you ever tried to watch a video with constant breaks and pauses?

Networks must provide predictable, measurable, and, at times, guaranteed services. The packet-switched network architecture does not guarantee that all packets that comprise a particular message will arrive on time and in their correct order, or even that they will arrive at all.

Networks also need mechanisms to manage congested network traffic. Network bandwidth is the measure of the data-carrying capacity of the network. In other words, how much information can be transmitted within a specific amount of time? Network bandwidth is measured in the number of bits that can be transmitted in a single second, or bits per second (bps). When simultaneous communications are attempted across the network, the demand for network bandwidth can exceed its availability, creating network congestion. The network simply has more bits to transmit than what the bandwidth of the communications channel can deliver.

In most cases, when the volume of packets is greater than what can be transported across the network, devices *queue*, or hold, the packets in memory until resources become available to transmit them, as shown in Figure 1-10. Queuing packets causes delay because new packets cannot be transmitted until previous packets have been processed. If the number of packets to be queued continues to increase, the memory queues fill up and packets are dropped.

Achieving the required QoS by managing the delay and packet loss parameters on a network becomes the secret to providing a successful solution for end-to-end application quality. One way this can be accomplished is through classification. To create QoS classifications of data, we use a combination of communication characteristics and the relative importance assigned to the application. We then treat all data within the same classification according to the same rules. For example, communication that is time-sensitive, such as voice transmissions, would be classified differently from communication that can tolerate delay, such as file transfers.

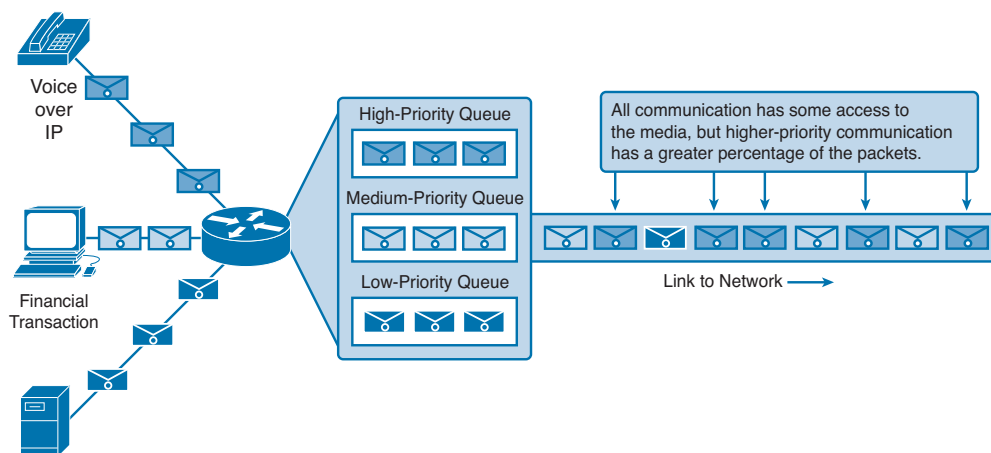


Figure 1-10 Priority Queuing

Examples of priority decisions for an organization might include

- **Time-sensitive communication:** Increase priority for services like telephony or video distribution
- **Non-time-sensitive communication:** Decrease priority for web page retrieval or email
- **High importance to organization:** Increase priority for production control or business transaction data
- **Undesirable communication:** Decrease priority or block unwanted activity, like peer-to-peer file sharing or live entertainment

Providing Network Security (1.2.2.6)

Security is one of the most important design elements in a computer network.

Security

The Internet has evolved from a tightly controlled internetwork of educational and government organizations to a widely accessible means for transmission of business and personal communications. As a result, the security requirements of the network have changed. The network infrastructure, the network services, and the data contained on network-attached devices are crucial personal and business assets. Compromising the integrity of these assets could have serious consequences, such as

- Network outages that prevent communications and transactions from occurring, with consequent loss of business
- Intellectual property (research ideas, patents, or designs) that is stolen and used by a competitor

- Personal or private information that is compromised or made public without the user's consent
- Misdirection and loss of personal or business funds
- Loss of important data that takes a significant labor to replace, or is irreplaceable

There are two types of network security concerns that must be addressed: network infrastructure security and information security.

Securing a network infrastructure includes physically securing devices that provide network connectivity, and preventing unauthorized access to the management software that resides on those devices.

Information security refers to protecting the information contained within the packets being transmitted over the network and the information stored on network-attached devices. Security measures taken in a network should prevent the following:

- Unauthorized disclosure
- Theft of information (see Figure 1-11)
- Unauthorized modification of information
- Denial of service (DoS)

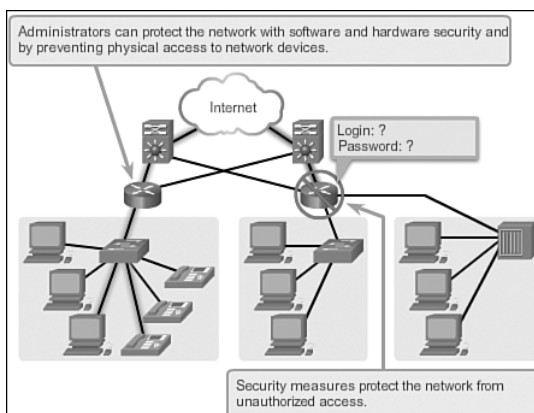


Figure 1-11 Security in a Computer Network.

In order to achieve the goals of network security, there are three primary requirements:

- **Ensuring confidentiality:** Data confidentiality means that only the intended and authorized recipients—individuals, processes, or devices—can access and read data. This is accomplished by having a strong system for user authentication, enforcing passwords that are difficult to guess, and requiring users to change their passwords frequently. Encrypting data, so that only the intended recipient can read it, is also part of confidentiality.

- **Maintaining communication integrity:** Data integrity means having the assurance that the information has not been altered in transmission, from origin to destination. Data integrity can be compromised when information has been corrupted—willfully or accidentally. Data integrity is made possible by requiring validation of the sender and by using mechanisms to validate that the packet has not changed during transmission.
- **Ensuring availability:** *Availability* means having the assurance of timely and reliable access to data services for authorized users. Network firewall devices, along with desktop and server antivirus software, can ensure system reliability and the robustness to detect, repel, and cope with such attacks. Building fully redundant network infrastructures, with few single points of failure, can reduce the impact of these threats.

**Interactive
Graphic****Activity 1.2.2.7: Reliable Networks**

Go to the online course to perform this practice activity.

LANs, WANs, and the Internet (1.3)

Most web users never consider how the Internet works. In this section you will begin to explore the pieces that come together to enable network communications.

Components of a Network (1.3.1)

In this section you will begin to learn about the devices and equipment that work together in networks.

Components of the Network (1.3.1.1)

The path that a message takes from source to destination can be as simple as a single cable connecting one computer to another or as complex as a network that literally spans the globe. This network infrastructure is the platform that supports the network. It provides the stable and reliable channel over which our communications can occur.

The network infrastructure contains three categories of network components:

- End devices
- Intermediary devices
- Network media

Devices and media are the physical elements, or *hardware*, of the network. Hardware comprises the components of the network platform that typically are visible, such as a laptop, PC, switch, router, wireless access point, or the cabling used to connect the devices. Occasionally, some network components may not be visible. In the case of wireless media, for example, messages are transmitted through the air using invisible radio frequency or infrared waves.

Network components are used to provide services and processes. These services and processes are the communication programs, called *software*, that run on the networked devices. A *network service* provides information in response to a request. Services include many of the common network applications people use every day, like email hosting services and web hosting services. Processes provide the functionality that directs and moves the messages through the network. Processes are less obvious to us but are critical to the operation of networks.

End Devices (1.3.1.2)

The network devices that people are most familiar with are called *end devices*, or hosts. These devices form the interface between users and the underlying communication network.

Some examples of end devices are

- Computers (work stations, laptops, file servers, web servers)
- Network printers
- VoIP phones
- TelePresence endpoints
- Security cameras
- Mobile handheld devices (such as smartphones, tablets, PDAs, and wireless debit/credit card readers and barcode scanners)

A *host device* is either the source or destination of a message transmitted over the network. In order to distinguish one host from another, each host on a network is identified by an address. When a host initiates communication, it uses the address of the destination host to specify where the message should be sent.

In modern networks, a host can act as a client, a server, or both. Software installed on the host determines which role it plays on the network. *Servers* are hosts that have software installed that enables them to provide information and services, like email or web pages, to other hosts on the network. *Clients* are hosts that have software installed that enables them to request and display the information obtained from the server.

Intermediary Devices (1.3.1.3)

Intermediary devices interconnect end devices. These devices provide connectivity and work behind the scenes to ensure that data flows across the network. Intermediary devices connect the individual hosts to the network and can connect multiple individual networks to form an internetwork.

Interactive Graphic

Activity 1.3.1.3: Internetworks

Go to the online course and view the animation.

Examples of intermediary network devices are

- Network access devices (switches and wireless access points)
- Internetworking devices (routers)
- Security devices (firewalls)

The management of data as it flows through the network is also a role of the intermediary devices. These devices use the destination host address, in conjunction with information about the network interconnections, to determine the path that messages should take through the network.

Processes running on the intermediary network devices perform these functions:

- Regenerate and retransmit data signals
- Maintain information about which pathways exist through the network and internetwork
- Notify other devices of errors and communication failures
- Direct data along alternate pathways when there is a link failure
- Classify and direct messages according to QoS priorities
- Permit or deny the flow of data, based on security settings

Network Media (1.3.1.4)

Communication across a network is carried on a *medium*. The medium provides the channel over which the message travels from source to destination.

Modern networks primarily use the following three types of media to interconnect devices and to provide the pathway over which data can be transmitted:

- Metallic wires within cables
- Glass or plastic fibers (fiber-optic cable)
- Wireless transmission

Figure 1-12 shows examples of the three types of physical media.

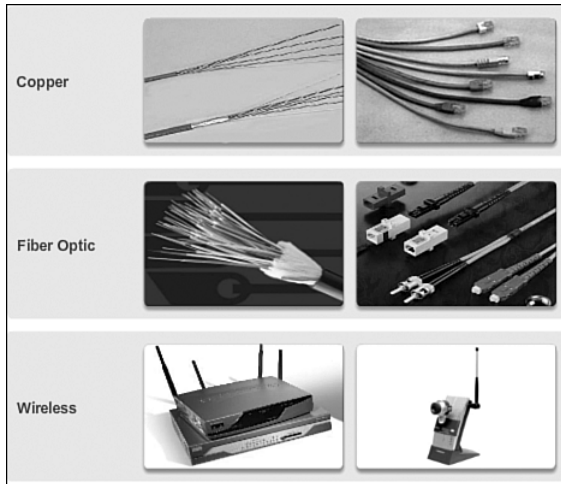


Figure 1-12 Network Media

The signal encoding that must occur for the message to be transmitted is different for each media type. On metallic wires, the data is encoded into electrical impulses that match specific patterns. Fiber-optic transmissions rely on pulses of light, within either infrared or visible light ranges. In wireless transmission, patterns of electromagnetic waves depict the various bit values.

Different types of network media have different features and benefits. Not all network media types have the same characteristics or are appropriate for the same purpose. The criteria for choosing network media are

- The distance the media can successfully carry a signal
- The environment in which the media is to be installed
- The amount of data and the speed at which it must be transmitted
- The cost of the media and installation

Network Representations (1.3.1.5)

When conveying complex information, such as displaying all the devices and media in a large internetwork, it is helpful to use visual representations. A diagram provides an

easy way to understand the way the devices in a large network are connected. Such a diagram uses symbols to represent the different devices and connections that make up a network. This type of “picture” of a network is known as a *topology diagram*.

Like any other language, the language of networking uses a common set of symbols to represent the different end devices, network devices, and media, as shown in Figure 1-13. The ability to recognize the logical representations of the physical networking components is critical to being able to visualize the organization and operation of a network. Throughout this course and its accompanying labs, you will learn both how these devices operate and how to perform basic configuration tasks on these devices.

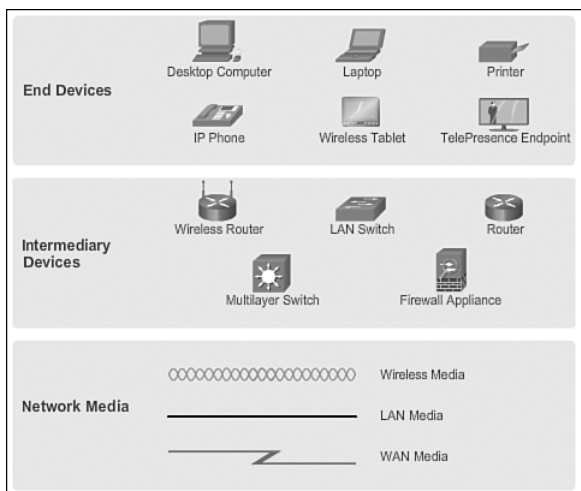


Figure 1-13 Network Representations

In addition to being able to recognize these representations, you need to understand the specialized terminology that is used when discussing how each of these devices and media connect to each other. Important terms to remember are

- **Network interface card (NIC):** Provides the physical connection to the network at the PC or other host device. The media connecting the PC to the networking device plugs directly into the NIC (also known as a LAN adapter).
- **Physical port:** A connector or outlet on a networking device where the media is connected to a host or other networking device.
- **Interface:** Specialized ports on an internetworking device that connect to individual networks. Because routers are used to interconnect networks, the ports on a router are referred to as network interfaces.

Topology Diagrams (1.3.1.6)

Topology diagrams are mandatory for anyone working with a network. A topology diagram provides a visual map of how the network is connected.

There are two types of topology diagrams:

- **Physical topology diagram:** Identifies the physical location of intermediary devices, configured ports, and cable installation, as shown on the left in Figure 1-14.
- **Logical topology diagram:** Identifies devices, ports, and the IP addressing scheme, as shown on the right in Figure 1-14.

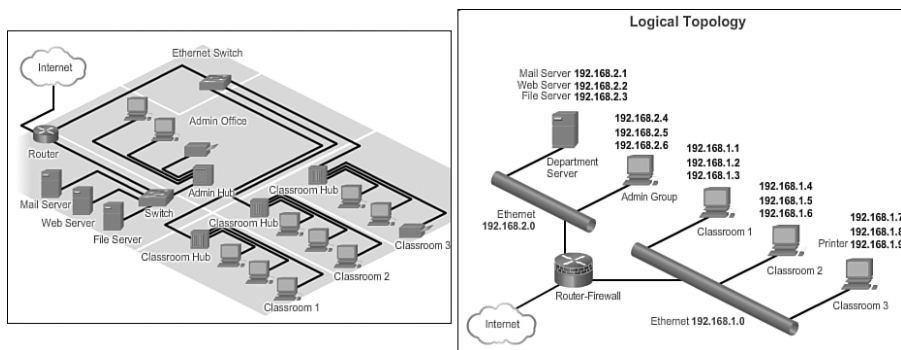


Figure 1-14 Physical Topology (Left) and Logical Topology (Right)

Interactive Graphic

Activity 1.3.1.7: Network Component Representations and Functions

Go to the online course to perform this practice activity.

LANs and WANs (1.3.2)

This section explains how LANs and WANs form computer networks.

Types of Networks (1.3.2.1)

Network infrastructures can vary greatly in terms of

- Size of the area covered
- Number of users connected
- Number and types of services available

Figure 1-15 illustrates the two most common types of network infrastructures:

- **Local-area network (LAN):** A network infrastructure that provides access to users and end devices in a small geographical area.
- **Wide-area network (WAN):** A network infrastructure that provides access to other networks over a wide geographical area.

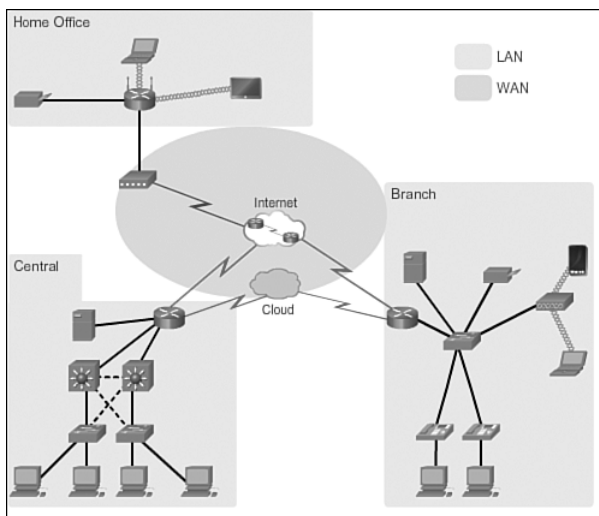


Figure 1-15 LANs Separated by Geographic Distance Connected by a WAN

Other types of networks include

- **Metropolitan-area network (MAN):** A network infrastructure that spans a physical area larger than a LAN but smaller than a WAN (e.g., a city). MANs are typically operated by a single entity, such as a large organization.
- **Wireless LAN (WLAN):** Similar to a LAN but wirelessly interconnects users and endpoints in a small geographical area.
- **Storage-area network (SAN):** A network infrastructure designed to support file servers and provide data storage, retrieval, and replication. It involves high-end servers, multiple disk arrays (called *blocks*), and Fibre Channel interconnection technology.

Local-Area Networks (1.3.2.2)

LANs are a network infrastructure that spans a small geographical area. Specific features of LANs include

- LANs interconnect end devices in a limited area such as a home, school, office building, or campus.

- A LAN is usually administered by a single organization or individual. The administrative control that governs the security and access control policies is enforced on the network level.
- LANs provide high-speed bandwidth to internal end devices and intermediary devices.

Wide-Area Networks (1.3.2.3)

WANs are a network infrastructure that spans a wide geographical area. WANs are typically managed by service providers (SPs) or Internet service providers (ISPs).

Specific features of WANs include

- WANs interconnect LANs over wide geographical areas such as between cities, states, provinces, countries, or continents.
- WANs are usually administered by multiple service providers.
- WANs typically provide slower-speed links between LANs.

The Internet (1.3.3)

This section explains how the Internet consists of many connected LANs and WANs.

The Internet (1.3.3.1)

Although there are benefits to using a LAN or WAN, most individuals need to communicate with a resource on another network, outside of the local network within the home, campus, or organization. This is done using the Internet.

As shown in Figure 1-16, the Internet is a worldwide collection of interconnected networks (internetworks or the Internet for short), cooperating with each other to exchange information using common standards. Through telephone wires, fiber-optic cables, wireless transmissions, and satellite links, Internet users can exchange information in a variety of forms.

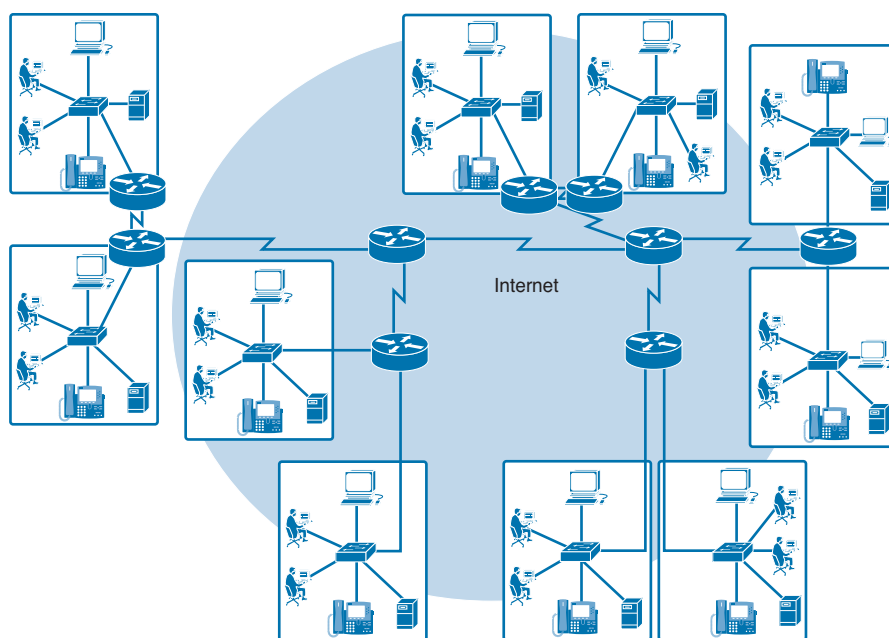


Figure 1-16 Internetworks Made Up of LANs and WANs

The Internet is a conglomerate of networks and is not actually owned by any individual or group. Ensuring effective communication across this diverse infrastructure requires the application of consistent and commonly recognized technologies and standards as well as the cooperation of many network administration agencies. There are organizations that have been developed for the purpose of helping to maintain structure and standardization of Internet protocols and processes. These organizations include the Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN), and the Internet Architecture Board (IAB), plus many others.

Note

The term *internet* (with a lower case “i”) is used to describe multiple networks interconnected. When referring to the global system of interconnected computer networks or the World Wide Web, the term *Internet* (with a capital “I”) is used.

Intranet and Extranet (1.3.3.2)

Two other terms are similar to the term Internet:

- Intranet
- Extranet

Intranet is a term often used to refer to a private connection of LANs and WANs that belongs to an organization, and is designed to be accessible only by the organization's members, employees, or others who have authorization. An intranet is basically an internet that is usually only accessible from within the organization.

An organization may publish on its intranet web pages about internal events, health and safety policies, staff newsletters, and staff phone directories. For example, a school may have an intranet that includes class schedule information, online curriculum, and discussion forums. Intranets usually help eliminate paperwork and speed up workflows. An organization's intranet may be accessible to staff working outside of the organization by using secure connections to the internal network.

An organization may use an *extranet* to provide secure and safe access to individuals who work for different organizations but require company data. Examples of extranets include

- A company providing access to outside suppliers/contractors
- A hospital providing a booking system to doctors so they can make appointments for their patients
- A local office of education providing budget and personnel information to the schools in its district



Lab 1.3.3.3: Mapping the Internet

In this lab you will test network connectivity, trace network routes using different tools, and compare the results provided by those tools.

Connecting to the Internet (1.3.4)

This section explores the different ways to access the Internet.

Internet Access Technologies (1.3.4.1)

There are many different ways to connect users and organizations to the Internet.

Home users, teleworkers (remote workers), and small offices typically require a connection to an Internet service provider (ISP) to access the Internet. Connection options vary greatly depending on the ISP and the geographical location. However, popular choices include broadband cable, broadband digital subscriber line (DSL), wireless WANs, and mobile services.

Organizations typically require access to other corporate sites and the Internet. Fast connections are required to support business services, including IP phones, video conferencing, and data center storage.

Business-class interconnections are usually provided by service providers (SPs). Popular business-class services include business DSL, leased lines, and Metro Ethernet.

Connecting Remote Users to the Internet (1.3.4.2)

Figure 1-17 illustrates common Internet connection options for small office and home office users, which include

- **Cable:** Typically offered by cable television service providers, the Internet data signal is carried on the same coaxial cable that delivers cable television. It provides a high-bandwidth, always-on connection to the Internet. A special cable modem separates the Internet data signal from the other signals carried on the cable and provides an Ethernet connection to a host computer or LAN.
- **DSL:** Provides a high-bandwidth, always-on connection to the Internet. It requires a special high-speed modem that separates the DSL signal from the telephone signal and provides an Ethernet connection to a host computer or LAN. DSL runs over a telephone line, with the line split into three channels. One channel is used for voice telephone calls. This channel allows an individual to receive phone calls without disconnecting from the Internet. A second channel is a faster download channel, used to receive information from the Internet. The third channel is used for sending or uploading information. This channel is usually slightly slower than the download channel. The quality and speed of the DSL connection depends mainly on the quality of the phone line and the distance from your phone company's central office. The farther you are from the central office, the slower the connection.
- **Cellular:** Cellular Internet access uses a cell phone network to connect. Wherever you can get a cellular signal, you can get cellular Internet access. Performance will be limited by the capabilities of the phone and the cell tower to which it is connected. The availability of cellular Internet access is a real benefit in those areas that would otherwise have no Internet connectivity at all, and for people who are constantly on the go.
- **Satellite:** Satellite service is a good option for homes or offices that do not have access to DSL or cable. Satellite dishes require a clear line of sight to the satellite, so satellite service might not be an option in heavily wooded areas or places with other overhead obstructions. Speeds will vary depending on the contract, though they are generally good. Equipment and installation costs can be high (although check the provider for special deals), with a moderate monthly fee thereafter. The availability of satellite Internet access is a real benefit in those areas that would otherwise have no Internet connectivity at all.

- **Dial-up telephone:** An inexpensive option that uses any phone line and a modem. To connect to the ISP, a user calls the ISP access phone number. The low bandwidth provided by a dial-up modem connection is usually not sufficient for large data transfer, although it is useful for mobile access while traveling. A modem dial-up connection should only be considered when higher-speed connection options are not available.

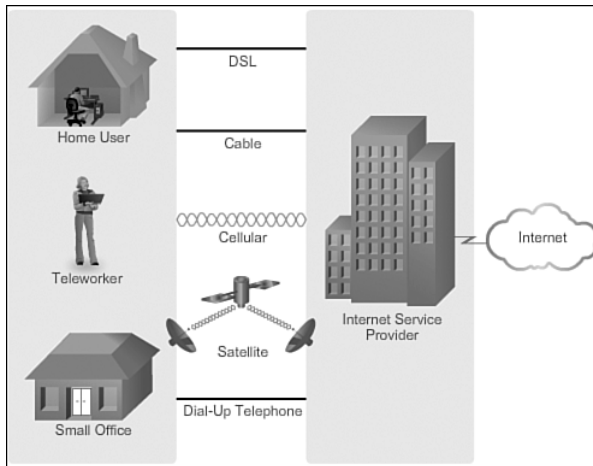


Figure 1-17 Internet Connection Options

Many homes and small offices are more commonly being connected directly with fiber-optic cables. This enables an ISP to provide higher bandwidth speeds and support more services such as Internet, phone, and TV.

The choice of connection varies depending on geographical location and service provider availability.

What are your options for connecting to the Internet?

Connecting Businesses to the Internet (1.3.4.3)

Corporate connection options differ from home-user options. Businesses may require higher bandwidth, dedicated bandwidth, and managed services. Connection options available differ depending on the number of service providers located nearby.

Common connection options for organizations include

- **Dedicated leased line:** This is a dedicated connection from the service provider to the customer premises. Leased lines are actually reserved circuits that connect geographically separated offices for private voice and/or data networking. The circuits are typically rented at a monthly or yearly rate, which tends to make it expensive. In North America, common leased-line circuits include T1 (1.54

Mbps) and T3 (44.7 Mbps), whereas in other parts of the world they are available in E1 (2 Mbps) and E3 (34 Mbps).

- **Metro Ethernet:** Metro Ethernet is typically available from a provider to the customer premises over a dedicated copper or fiber connection providing bandwidth speeds of 10 Mbps to 10 Gbps. Ethernet over Copper (EoC) is more economical than fiber-optic Ethernet service in many cases, is quite widely available, and reaches speeds of up to 40 Mbps. However, EoC is limited by distance. Fiber-optic Ethernet service delivers the fastest connections available at an economical price per megabit. Unfortunately, there are still many areas where this service is unavailable.
- **DSL:** Business DSL is available in various formats. A popular choice is symmetric DSL (SDSL), which is similar to asymmetric DSL (ADSL) but provides the same upload and download speeds. ADSL is designed to deliver bandwidth at different rates downstream than upstream. For example, a customer getting Internet access may have downstream rates that range from 1.5 to 9 Mbps, whereas upstream bandwidth ranges are from 16 to 640 kbps. ADSL transmissions work at distances up to 18,000 feet (5,488 meters) over a single copper twisted pair.
- **Satellite:** Satellite service can provide a connection when a wired solution is not available. Satellite dishes require a clear line of sight to the satellite. Equipment and installation costs can be high, with a moderate monthly fee thereafter. Connections tend to be slower and less reliable than terrestrial competition, which makes satellite less attractive than other alternatives.

The choice of connection varies depending on geographical location and service provider availability.

Packet Tracer
□ Activity

Packet Tracer Activity 1.3.4.4: Network Representation

In this activity you will learn the essentials of using Packet Tracer. Packet Tracer is a downloadable software program that will help you with your Cisco Certified Network Associate (CCNA) studies. You will explore a relatively complex network that highlights a few of Packet Tracer's features. While doing so, you will learn how to access Help and the tutorials. Finally, you will explore how Packet Tracer serves as a modeling tool for network representations.

The Expanding Network (1.4)

The Internet has continuously expanded in the last two decades, and there is no indication that the expansion is slowing.

Network Trends (1.4.1)

In this section you will learn about emerging Internet trends.

New Trends (1.4.1.1)

When you look at how the Internet has changed so many of the things people do daily, it is hard to believe that it has only been around for most people for about 20 years. It has truly transformed the way individuals and organizations communicate. For example, before the Internet became so widely available, organizations and small businesses largely relied on print marketing to make consumers aware of their products. It was difficult for businesses to determine which households were potential customers, so businesses relied on mass print marketing programs. These programs were expensive and varied in effectiveness. Compare that to how consumers are reached today. Most businesses have an Internet presence where consumers can learn about their products, read reviews from other customers, and order products directly from the website. Social networking sites partner with businesses to promote products and services. Bloggers partner with businesses to highlight and endorse products and services. Most of this product placement is targeted to the potential consumer, rather than to the masses.

As new technologies and end-user devices come to market, businesses and consumers must continue to adjust to this ever-changing environment. The role of the network is transforming to enable the connections of people, devices, and information. There are several new networking trends that will affect organizations and consumers. Some of the top trends include

- Bring Your Own Device (BYOD)
- Online collaboration
- Video communication
- Cloud computing

These trends are interconnected and will continue to build off of one another in the coming years. The next couple of topics will cover these trends in more detail.

But keep in mind, new trends are being dreamed up and engineered every day. How do you think the Internet will change in the next 10 years? 20 years?

Bring Your Own Device (BYOD) (1.4.1.2)

The concept of any device, to any content, in any way is a major global trend occurring in business IT environments that requires significant changes to the way devices are used. This trend is known as *Bring Your Own Device (BYOD)*.

In the past, an employee who needed access to the corporate network would be issued a company-provided device, such as a laptop or PC. These devices were typically expensive and were seen as tools for work. With the growth of consumer devices, and the related drop in cost, employees can be expected to have some of the most advanced tools for personal use. These personal tools include laptops, netbooks, tablets, smartphones, and e-readers. BYOD is about end users having the freedom to use these personal tools to access information and communicate across the corporate network. These can be devices purchased by the employer, devices purchased by the employee, or both. BYOD means any device, with any ownership, used anywhere. Extended connectivity through mobile and remote access to the corporate network gives employees tremendous flexibility and increased productivity.

BYOD is an influential trend that has or will touch every IT organization. There are many effects and considerations when providing for a BYOD environment.

BYOD Considerations (1.4.1.3)

In a BYOD environment, individuals are likely to have multiple devices connected to the network, possibly simultaneously. This leads to a large increase in the overall number of connected devices. The network must be designed in a way to support these additional devices and their traffic.

Additionally, a complete BYOD solution must consider how to extend the full services of the organization seamlessly, providing the same types of services to a user on a BYOD as are available to a user on a corporate PC. This includes collaboration tools such as integrated voice, video, IM, conferencing, and application sharing.

Finally, the network and applications must be able to offer quality of service regardless of whether the connectivity to those applications or collaboration tools occurs in the main campus, branch office, home office, or mobile teleworker location. Any solution must consider not only the employee using their own device, but also the individuals and applications that they are connecting and communicating with.

Security is a major consideration in a BYOD environment; therefore, any solution must be a highly secure mobile solution. Mobile and remote-access devices are typically not under the same strict control and scrutiny as employer-provided desktop and laptop computers. Therefore, appropriate security and user policies need to be applied to protect corporate data when employees connect with these devices. The range of those policies may vary depending on the spectrum of BYOD access that an organization wants.

Depending on the needs of the organization, a range of BYOD policies may be in place, from limited access to advanced BYOD implementation. Each of these implementations must include end-user agreements that outline the use of personal devices on corporate networks, policies for how and what those devices can access, and

guidelines for how lost or stolen devices will be handled. Organizations may also need an agreement about when and if data can be accessed from the personal device of an employee. There have been several legal challenges recently for cases involving an employer who remotely “wiped” an employee-owned device, including both the corporate and personal data it contained. Imagine your surprise as an employee when you discover that by using your new tablet to access the corporate network, you unknowingly agreed to let IT delete your favorite family photos remotely.

Online Collaboration (1.4.1.4)

Employees want to connect to the network not only for access to data applications, but also to collaborate with one another. Collaboration is defined as “the act of working with another or others on a joint project.”

For businesses, collaboration is a critical and strategic priority. To remain competitive, organizations must answer three primary collaboration questions:

- How can they get everyone on the same page?
- With decreased budgets and personnel, how can they balance resources to be in more places at once?
- How can they maintain face-to-face relationships with a growing network of colleagues, customers, partners, and peers in an environment that is more dependent on 24-hour connectivity?

One way to answer these questions in today’s environment is through online collaboration tools. In traditional workspaces, and with BYOD environments alike, employees are taking advantage of voice, video, and conferencing services in collaboration efforts.

The ability to collaborate online is changing business processes. New and expanding collaboration tools allow individuals to quickly and easily collaborate, regardless of physical location. Organizations have much more flexibility in the way they are organized. Employees are no longer restricted to physical locations. Expert knowledge is easier to access than ever before. Expansions in collaboration allow organizations to improve their information gathering, innovation, and productivity

Collaboration tools give employees, customers, and partners a way to instantly connect, interact, and conduct business, through whatever communications channels they prefer, and achieve business objectives.

Collaboration Considerations (1.4.1.5)

The ability to work together to solve a common problem has proven to be one of mankind’s greatest accomplishments. Great things can happen when we all work

together. However, implementing a collaboration strategy is not always easy and there can be many challenges to overcome.

End users have high expectations that application performance will be maintained, regardless of time, location, and end device. Users also want to be able to have collaboration capabilities regardless of service provider, meaning they want those capabilities to be available whether they are connecting with collaboration tools across a corporate-maintained network or connecting via their home or hotel Internet connection.

For an organization to be successful in its collaboration strategy, it must determine its collaboration needs and establish which tools effectively meet those needs. Additionally, an organization must be able to prioritize traffic and effectively monitor and manage the performance of those collaboration tools. Finally, an organization must consider security requirements for collaboration and establish proper-use policies to ensure corporate data remains secure.

There's a wide range of collaboration tools available on the market today, including mobile applications, telePresence, and online web-conferencing tools, just to name a few.

Video Communication (1.4.1.6)

Another trend in networking that is critical in the communication and collaboration effort is the use of video. Video conferencing and person-to-person video calling are already proving particularly powerful for sales processes and for doing business at a distance, both locally and globally. Today, businesses are using video to transform key business processes to create competitive advantage, lower costs, and reduce environmental impact, particularly by avoiding the need for travel. Figure 1-18 shows the trend of video in communication.

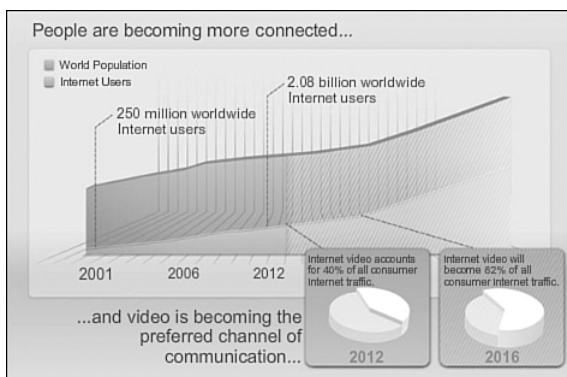


Figure 1-18 Use of Video on the Internet Is Growing.

Both consumers and businesses are driving this change. Video is becoming a key requirement for effective collaboration as organizations extend across geographical and cultural boundaries. Video users now demand the ability to view any content, on any device, anywhere.

Businesses are also recognizing the role of video to enhance the human network. The growth of media, and the new uses to which it is being put, is driving the need to integrate audio and video into many forms of communication. The audio conference will coexist with the video conference. Collaboration tools designed to link distributed employees will integrate desktop video to bring teams closer together.

There are many drivers and benefits for including a strategy for using video. Each organization is unique. The exact mix, and the nature of the drivers for adopting video, will vary from organization to organization, and by business function. Marketing, for example, may focus on globalization and fast-changing consumer tastes, while the focus of the Chief Information Officer (CIO) may be on cost savings by reducing travel costs of employees who need to meet face-to-face.

Cloud Computing (1.4.1.7)

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network. A company uses the hardware and software in the cloud and pays a service fee to the cloud provider.

Local computers no longer have to do all the “heavy lifting” when it comes to running network applications. The network of computers that make up the cloud handles them instead. The hardware and software requirements of the user are decreased. The user’s computer must interface with the cloud using software, which may be a web browser, and the cloud’s network takes care of the rest.

Cloud computing is another global trend changing the way organizations access and store data. Cloud computing uses cloud-based services to reduce costs and improve business processes. Cloud computing encompasses any subscription-based or pay-per-use service, in real time over the Internet, that extends the capabilities of IT without requiring investment in new infrastructure, training new personnel, or licensing new software. These services are available on demand and delivered economically to any device anywhere in the world without compromising security or function.

Cloud computing helps enterprise IT shift spending from large, one-time capital expenditures to ongoing operating expenses. It also allows enterprise IT to share cloud solution assets and provide dynamic, on-demand delivery of services to the enterprise as a whole.

Cloud computing offers the following potential benefits:

- **Organizational flexibility:** Users can access the information anytime and anyplace using a web browser.
- **Agility and rapid deployment:** The IT department can focus on delivering the tools to mine, analyze, and share the information and knowledge from databases, files, and people.
- **Reduced cost of infrastructure:** Technology is moved from on site to a cloud provider, eliminating the cost of hardware and applications.
- **Refocus of IT resources:** Cost savings of hardware and applications can be applied elsewhere.
- **Creation of new business models:** Applications and resources are easily accessible, so companies can react quickly to customer needs. This helps them set strategies to promote innovation while potentially entering new markets.

Types of Clouds (1.4.1.8)

There are four primary types of clouds:

- **Public clouds:** Cloud-based applications and services offered in a public cloud are made available to the general population. Services may be free or may be offered on a pay-per-use model, such as paying for online storage. A public cloud uses the Internet to provide services.
- **Private clouds:** Cloud-based applications and services offered in a private cloud are intended for a specific organization or entity, such as the government. A private cloud can be set up using the organization's private network, though this can be expensive to build and maintain. A private cloud can also be managed by an outside organization with strict access security.
- **Custom clouds:** These are clouds built to meet the needs of a specific industry, such as healthcare or media. Custom clouds can be private or public.
- **Hybrid clouds:** A hybrid cloud is made up of two or more clouds (for example, part custom and part public), where each part remains a distinctive object but both parts are connected using a single architecture. Individuals on a hybrid cloud would be able to have degrees of access to various services based on user access rights.

Data Centers (1.4.1.9)

Cloud computing is possible because of data centers. A *data center* is a facility used to house computer systems and associated components, including

- Redundant data communications connections
- High-speed virtual servers (sometimes referred to as server farms or server clusters)
- Redundant storage systems (typically use SAN technology)
- Redundant or backup power supplies
- Environmental controls (e.g., air conditioning, fire suppression)
- Security devices

A data center can occupy one room of a building, one or more floors, or an entire building. Modern data centers make use of cloud computing and virtualization to efficiently handle large data transactions. Virtualization is the creation of a virtual version of something, such as a hardware platform, operating system (OS), storage device, or network resources. Whereas a physical computer is an actual discrete device, a virtual machine consists of a set of files and programs running on an actual physical system. Unlike multitasking, which involves running several programs on the same OS, virtualization runs several different OSs in parallel on a single CPU. This drastically reduces administrative and cost overheads.

Data centers are typically very expensive to build and maintain. For this reason, only large organizations use privately built data centers to house their data and provide services to users. For example, a large hospital may own a separate data center where patient records are maintained electronically. Smaller organizations that cannot afford to maintain their own private data center can reduce the overall cost of ownership by leasing server and storage services from a larger data center organization in the cloud.

Network Security (1.4.2)

This section explores how securing a network is becoming an increasingly complex task.

Security Threats (1.4.2.1)

Network security is an integral part of computer networking. As new technologies and trends emerge, so too must the protections that organizations use. Network security requirements must take into account the BYOD environment, the collaboration applications, video requirements, and cloud computing needs. Network security must be able to secure the corporate data while still allowing for the quality of service that is expected of each technology.

Securing a network involves protocols, technologies, devices, tools, and techniques to secure data and mitigate threats. Many external network security threats today are spread over the Internet. The most common external threats to networks include

- **Viruses, worms, and Trojan horses:** Malicious software and arbitrary code running on a user device
- **Spyware and adware:** Software installed on a user device that secretly collects information about the user
- **Zero-day attack, also called zero-hour attack:** An attack that occurs on the first day that a vulnerability becomes known
- **Hacker attack:** An attack by a knowledgeable person using software or network vulnerabilities to exploit devices or network resources
- **Denial of service attack:** An attack designed to slow or crash applications and processes on a network device
- **Data interception and theft:** An attack to capture private information from an organization's network
- **Identity theft:** An attack to steal the login credentials of a user in order to access private data

It is equally important to consider internal threats. There have been many studies that show that the most common data breaches happen because of employees. This can be attributed to lost or stolen devices, accidental misuse by employees, and even malicious insiders. With the evolving BYOD strategies, corporate data is much more vulnerable. Therefore, when developing a security policy, it is important to address both external and internal security threats. Figure 1-19 depicts threats from internal and external sources.

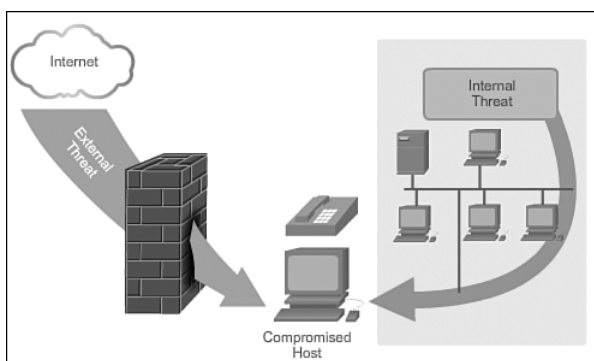


Figure 1-19 Network Threats

Security Solutions (1.4.2.2)

No single solution can protect the network from the variety of threats that exist. For this reason, security should be implemented in multiple layers, using more than one security solution. If one security component fails to identify and protect the network, others still stand.

The network security implementation for a corporate network usually consists of many components built into the network to monitor and filter traffic. Ideally, all components work together, which minimizes maintenance and improves security.

Network security components for a home or small office network should include, at a minimum, the following:

- **Antivirus and antispyware:** To protect user devices from malicious software.
- **Firewall filtering:** To block unauthorized access to the network. This may include a host-based firewall system that is implemented to prevent unauthorized access to the host device, or a basic filtering service on the home router to prevent unauthorized access from the outside world into the network.

Larger networks and corporate networks often have additional security requirements:

- **Dedicated firewall system:** To provide more advanced firewall capability that can filter large amounts of traffic with more granularity
- **Access control lists (ACL):** To further filter access and traffic forwarding
- **Intrusion prevention system (IPS):** To identify fast-spreading threats, such as zero-day or zero-hour attacks
- **Virtual private network (VPN):** To provide secure access to remote workers

Network security requirements must take into account the network environment, as well as the various applications and the computing requirements. Both home environments and businesses must be able to secure their data, while still allowing for the quality of service that is expected of each technology. Additionally, the security solution implemented must be adaptable to the growing and changing trends of the network.

The study of network security threats and mitigation techniques starts with a clear understanding of the underlying switching and routing infrastructure used to organize network services.

Activity 1.4.2.3: Network Security Terminology

Go to the online course to perform this practice activity.

Network Architectures (1.4.3)

This section explores network architectures and how they evolve to handle new technologies.

Cisco Network Architectures (1.4.3.1)

The role of the network has changed from a data-only network to a system that enables the connections of people, devices, and information in a media-rich, converged network environment.

In order for networks to function efficiently and grow, the network must be built upon a standard architecture. The *network architecture* refers to the devices, connections, and products that are integrated to support the necessary technologies and applications. A well-planned network technology architecture helps to ensure that any device can be connected across any combination of network, increases cost efficiency by integrating network security and management, and improves business processes.

With the constant evolution of networks, Cisco has updated its enterprise architectures and frameworks and has created the following three enterprise architectures to address the new network trends, as shown in Figure 1-20:

- Borderless networks architecture
- Collaboration architecture
- Data center and virtualization architecture

These three enterprise technology architectures can be implemented separately, or combined.

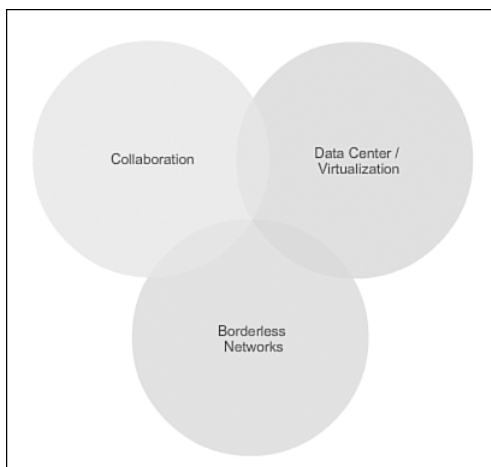


Figure 1-20 Three Cisco Network Architectures

Cisco Borderless Network (1.4.3.2)

The Cisco Borderless Network Architecture is a network solution that enables organizations and individuals to connect securely, reliably, and seamlessly to the corporate network in a BYOD environment.

This architecture separates the network functions into four areas of responsibility:

- **Cisco Borderless End Point/User Services:** Connects the various devices to provide access to network services. Devices that can connect to the borderless network can range from PCs to tablets and smartphones.
- **Cisco Borderless Network Services:** Optimizes the network connection and includes wireless access, secure access to corporate assets, and video performance optimization.
- **Cisco Borderless Network Systems:** Spans an organization from initial device network access to connecting devices to the cloud.
- **Cisco Borderless Infrastructure:** Supports services and systems with an infrastructure of scalable and resilient hardware and software.

The borderless network architecture supports a highly secure, high-performing network that is accessible to a wide range of devices. It needs to be flexible enough to scale in its support for future growth in terms of business expansion, including BYOD, mobility, and cloud computing, and must be able to support the growing requirements for online voice and video.

Collaboration Architecture (1.4.3.3)

To help organizations meet expanding collaboration needs, Cisco provides a collaboration architecture consisting of four categories of collaboration products:

- **TelePresence:** Provides next-generation video conferencing, where everyone, everywhere can be face-to-face and more effective through the most natural and lifelike communications experience available.
- **Collaboration Applications:** Stay connected and productive with voice, video, and web conferencing; messaging; mobile applications; and enterprise social software. For example, Cisco WebEx Meetings enables users to create and attend web conference calls. Users can meet to present ideas, share desktops, work on files together, and collaborate with others. Callers can see one another using webcams, and meetings can be recorded for people who are unable to attend.
- **Customer Collaboration:** Creates the foundation for positive customer service, a primary factor in building a stronger business. An example of this is the Cisco SocialMiner social media customer care solution. It can help companies proactively respond to customers and prospects communicating through public social media networks such as Twitter, Facebook, and other public forums or blogging sites.

- **Unified Communications:** View, optimize, and manage the entire communications system from one screen. With Cisco Unified Communications, organizations can seamlessly manage voice, video, mobility, and presence services between IP endpoints, media-processing devices, Voice over IP (VoIP) gateways, mobile devices, and multimedia applications.

Data Center Architecture (1.4.3.4)

The Cisco Unified Data Center is a complete data center infrastructure architecture that combines computing, networking, security, virtualization, and management solutions in a framework that delivers outstanding performance for physical and virtualized business applications. It is uniquely capable of providing the kind of simplicity, performance, and security that IT departments demand as they transition from physical to virtual to cloud environments.

The Cisco Unified Data Center incorporates three main data center technologies:

- **Cisco Unified Computing:** Integrates computing, networking, and storage resources to provide a unique, open, managed system that can scale to hundreds of server blades and thousands of desktops on virtual machines. Cisco Unified Computing reduces infrastructure costs, and can be deployed nearly 90 percent more quickly than traditional server platforms.
- **Cisco Unified Fabric:** Flexible network solutions deliver network services to servers, storage, and applications, providing transparent convergence, scalability, and sophisticated intelligence using Cisco Nexus and Catalyst switches.
- **Cisco Unified Management:** Provides the framework for IT service-creation and self-service capabilities, enabling IT to operate more efficiently and to more quickly offer new services to the business.

CCNA (1.4.3.5)

The three Cisco architectures previously discussed are built on an infrastructure of scalable and resilient hardware and software. Components of the architectures come together to build network systems that span your organization from network access to the cloud, and provide organizations with the services they need.

At the foundation of all three of these architectures, and in fact, at the foundation of the Internet itself, are routers and switches. Routers and switches transport data, voice, and video communications, allow for wireless access, and provide for security. After a basic network infrastructure with routing and switching is built, organizations can grow their network over time, adding features and functionality in an integrated solution.

As the use of these integrated, expanding networks increases, so does the need for training for individuals who implement and manage network solutions. This training must begin with the routing and switching foundation. Achieving Cisco Certified Network Associate (CCNA) certification is the first step in helping an individual prepare for a career in networking.

CCNA certification validates an individual's ability to install, configure, operate, and troubleshoot medium-size routed and switched networks, including implementation and verification of connections to remote sites in a WAN. This CCNA curriculum includes lessons that address the basic mitigation of security threats, introduction to wireless networking concepts and terminology, and performance-based skills. This CCNA curriculum also includes the use of various protocols, such as Internet Protocol (IP), Open Shortest Path First (OSPF), Serial Line Interface Protocol (SLIP), Frame Relay, VLANs, Ethernet, access control lists (ACLs), and others.

This course helps set the stage for networking concepts and basic routing and switching configurations and is a start on your path for CCNA certification.



Lab 1.4.3.6: Researching IT and Networking Job Opportunities

In this lab you will research job opportunities and reflect on that research.

Summary (1.5)

This section reviews the key networking concepts explained in this chapter.



Class Activity 1.5.1.1: Draw Your Concept of the Internet Now

In this activity you will use the knowledge you have acquired throughout Chapter 1, and the modeling activity document that you prepared at the beginning of this chapter.

Networks and the Internet have changed the way we communicate, learn, work, and even play.

Networks come in all sizes. They can range from simple networks consisting of two computers, to networks connecting millions of devices.

The Internet is the largest network in existence. In fact, the term *Internet* means a network of networks. The Internet provides the services that enable us to connect and communicate with our families, friends, and coworkers.

The network infrastructure is the platform that supports the network. It provides the stable and reliable channel over which communication can occur. It is made up of network components, including end devices, intermediate devices, and network media.

Networks must be reliable. This means the network must be fault tolerant and scalable, provide quality of service, and ensure security of the information and resources on the network. Network security is an integral part of computer networking, regardless of whether the network is limited to a home environment with a single connection to the Internet or is as large as a corporation with thousands of users. No single solution can protect the network from the variety of threats that exist. For this reason, security should be implemented in multiple layers, using more than one security solution.

The network infrastructure can vary greatly in terms of size, number of users, and number and types of services that are supported on it. The network infrastructure must grow and adjust to support the way the network is used. The routing and switching platform is the foundation of any network infrastructure.

This chapter focused on networking as a primary platform for supporting communication. The next chapter will introduce you to the Cisco Internetwork Operating System (IOS) used to enable routing and switching in a Cisco network environment.

Practice

The following activities provide practice with the topics introduced in this chapter. The Labs and Class Activities are available in the companion *Network Basics Lab Manual* (978-1-58713-313-8). The Packet Tracer Activities PKA files are found in the online course.



Class Activities

Class Activity 1.0.1.2: Draw Your Concept of the Internet

Class Activity 1.5.1.1: Draw Your Concept of the Internet Now



Labs

Lab 1.2.1.3: Researching Converged Network Services

Lab 1.1.1.8: Researching Network Collaboration Tools

Lab 1.3.3.3: Mapping the Internet

Lab 1.4.3.6: Researching IT and Networking Job Opportunities



Packet Tracer Activity

Packet Tracer Activity 1.3.4.4: Network Representation

Check Your Understanding

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. The appendix, “Answers to the ‘Check Your Understanding’ Questions,” lists the answers.

1. Which of the following is an example of QoS?
 - A. Data arrives via different physical media.
 - B. Intermediate devices deliver all packets along the same physical route.
 - C. Different types of traffic are delivered according to planned priority.
 - D. An intermediate device fails and traffic is rerouted and delivered reliably.

2. Fill in the blanks of the sentence with the best terms from the following list (not all of which will be used): *fault tolerance*, *security*, *QoS*, *data integrity*, and *scalability*.

The network designer for the small bank needed to plan for the network to double in size over 5 years, requiring her to allow for _____. Of course, all information needed to be kept confidential and safe, so she incorporated _____ into the design. She accounted for _____ when she ensured packets arrived with minimal loss or delay, and accounted for _____ by making sure the network would recover quickly if there was a hardware failure.

3. Which type of communications allows for dynamic routing over multiple paths and adaptation to failures in a network?
- A. Circuit switching
 - B. QoS
 - C. Leased fiber lines for packet delivery
 - D. Packet-switched, connectionless data communications
4. Employees of an insurance company accessing company data on restricted local-area and wide-area networks is an example of using a(n)
- A. Internet
 - B. Extranet
 - C. Intranet
 - D. BYOD nets
5. An organization that allows employees to use their own tablets and notebook computers in a secure environment has implemented which type of network?
- A. WAN
 - B. BYOD
 - C. QoS
 - D. Intranet
6. A group of movie critics posting a recording of their weekly radio show about movies is an example of
- A. Podcasting
 - B. Webhosting
 - C. Blogging
 - D. A wiki

7. When instructors provide common space on a computer to create and share documents they can access on their mobile devices or desktops, they are using:
 - A. Podcasts
 - B. Instant messaging
 - C. Social media
 - D. Collaboration tools
8. The complexity of a message can affect successful communication across a network. The level of complexity in a message is considered a(n):
 - A. Switching factor
 - B. External factor
 - C. Internal factor
 - D. Routing factor
9. Which of the following describes a converged network?
 - A. A network that enables people in different countries to work together in the cloud
 - B. A network that allows songs and videos to be shared peer to peer
 - C. A network that carries voice, video, and data traffic at the same time
 - D. A network that allows secure access to the Internet from inside a firewall
10. A system that allows communications between local networks around the world is a/the
 - A. BYOD
 - B. Internet
 - C. LANs
 - D. SAN
11. Which of the following is an intermediary device?
 - A. Router
 - B. Hand-held device
 - C. Security camera
 - D. Laptop

- 12.** A group of computers connected to store data is which type of network?
- A. LAN
 - B. SAN
 - C. BYOD
 - D. WAN
- 13.** What is the function of a WLAN?
- A. Wireless connection in a small geographical area
 - B. Wired connections in a local-area network
 - C. Worldwide communications between local-area networks
 - D. Wireless communications across the Internet
- 14.** If there are two DSL customers with consistent line quality, which will have the faster connection speed?
- A. The one closest to the cable company
 - B. They will have the same connection speed
 - C. The one closest to the central office
 - D. The one whose cable modem is on the last mile
- 15.** Which items can be associated with network availability? (Choose three.)
- A. Firewall devices
 - B. Antivirus software
 - C. Collaboration software
 - D. Redundant devices

This page intentionally left blank

Symbols

3COM, Ethernet development, 107
 10-Gigabit Ethernet SFP modules, 534
 802.11 Wireless frames, 438-440

A

A records, 155
 AAA network security services, 568-569
 abbreviated commands/keywords and IOS, 73-74
 access attacks (security), 565
 access networks, FTTH, 465
 access technologies (Internet), 32
 business access
 dedicated leased line, 34
 DSL, 35
 Metro Ethernet, 35
 satellite, 35
 remote access
 cable, 33
 cellular, 33
 dial-up (telephone), 34
 DSL, 33
 satellite, 33
 accessing
 CLI
 AUX ports, 61
 console port, 60
 console ports, 59
 SSH protocol, 60
 Telnet, 60
 terminal emulation programs, 61
 devices, security, 79-80
 IOS
 AUX ports, 61
 console ports, 59-60
 SSH protocol, 60
 Telnet, 60
 local resources (data delivery)
 communicating with devices on the same network, 128-129
 data link addresses, 128
 network addresses, 127-128
 out-of-band access, defining, 59
 privileged EXEC access, securing, 80
 remote resources (data delivery)
 communicating with devices on remote networks, 131-132
 data link addresses, 132
 default gateways, 130
 network addresses, 131
 user EXEC access, securing, 81-82
 accounting, network security, 569
 ACK (acknowledgement) control flags, TCP three-way handshakes, 192-193
 ACK (acknowledgement) numbers, confirming receipt of TCP segments, 196-197
 acknowledgements
 expectational acknowledgement, 196
 SACK, 198
 TCP flow control, 198-199
 TCP reliability, 196-199
 ACL (Access Control Lists), 44
 address pools and DHCP, 293
 addressing. *See* IPv4 addressing, IPv6 addressing
 administration (Internet), 31
 administrative distance, remote network routes, 235
 ADSL (Asymmetric Digital Subscriber Line) Internet connections, 35
 adware, 43
 AM (Amplitude Modulation), 448
 ANDing (AND operation), IPv4 addressing, 287-290
 ANSI (American National Standards Institute), data link layer standards, 418
 antispyware, 44
 antivirus software, 44
 anycast IPv6 addresses, 318

AP (Access Points), 475

appliance-based firewalls, 570

application filtering (firewalls), network security, 570

application layer

client/server model and application protocols, 148

defining, 141

network-aware applications, 144

OSI reference model, 140

P2P networks and application protocols, 145-147

protocols, 105, 141, 145

services

defining, 144

small networks, 554

TCP/IP protocol suite, 141

BOOTP, 143

DHCP, 143, 158-160

DNS, 143, 155-157

FTP, 143

HTTP, 143, 149-150

IMAP, 143

POP, 143, 152

SMTP, 143, 152-154

Telnet, 143

TFTP, 143

application layer protocol, 105

application interfaces and OSI reference model, 145

architectures (network)

CCNA certification, 47-48

Cisco Borderless Network Architectures, 46

Cisco Unified Data Center, 47

collaboration architectures, 46-47

defining, 15, 45

arguments, defining, 67

ARP (Address Resolution Protocol)

ARP caches and RAM, 242

arp command, 591-592

ARP poisoning, 515

ARP spoofing, 515

frames, creating, 505-508

IP addresses, resolving, 504

MAC addresses, 130

operation of, 505-508

problems with

mitigating, 515

overhead, 514

security, 515

remote communication and, 508-510

tables

arp -a command, 513

maintaining, 505

networking devices, 512

removing entries from, 512

show ip arp command, 512

ARPANET (Advanced Research Projects Agency Network)

Internet development, 107

RFC development, 119

Arrows and IOS, 73

ASCII (American Standard Code for Information Interchange)

binary notation, IPv4 addressing, 267

Digital Translator, 268

assigned multicast IPv6 addresses, 337

assigning interfaces, testing assignments, 94

asynchronous data signals, 448

attacks (security), 564

access attacks, 565

defining, 562

DoS attacks, 565-566

reconnaissance attacks, 565

attenuation (signal), 452

audio files and podcasting, 8

authentication

IPv6 packets, 222

network security, 568-569

authorization, network security, 569

Auto-MDIX, LAN switches, 522

AUX (auxiliary) ports

CLI environments, accessing via routers, 245

IOS access, 61

routers and, 244

availability (data), network security, 23

B

backbone cabling, 463

backups

IOS configuration files

backing up via text capture (Tera Term), 87, 600

backing up via text files, 600

backing up via TFTP, 601-602

backing up via USB flash drives, 603
restoring via USB flash drives, 605
 network security, 567
bandwidth, physical layer (OSI reference model), 449-450
banners
 banner motd command, 83, 251
 device security, 575
 messages, 83-84
 MOTD, 83-84
base (positional notation), 268
baselines (networks), determining, 581-582
BCP (Best Current Practices), 121
best effort (unreliable) delivery, IP, 215-216
BIA (burned-in addresses). See MAC addresses
binary notation
 binary number system, 269-270
 converting
 binary notation to decimal addressing, 271
 decimal addressing to binary notation, 272, 275-277, 290
 IPv4 addressing, 267-268
 binary notation conversion to decimal addressing, 271
 binary number system, 269-270
 decimal address conversion to binary notation, 272, 275-277, 290
 octets, 269-272, 275-277
 positional notation, 268
BIND (Berkeley Internet Name Domain) and DNS, 155-156
bitwise AND operation, IPv4 addressing, 287-290
blocks, SAN, 29. See also disk arrays
blogs (weblogs), 10
BOOTP (Bootstrap Protocol), application layer, 143
bootset files, router bootups, 247
Borderless Network Architectures, 46
branches and routers, 241
broadcast addresses
 IPv4 addresses, 283, 297
 directed broadcast addressing, 295
 limited broadcast addressing, 295
 MAC addresses, 501
broadcast domains, 295

businesses
 business Internet connections
 dedicated leased line, 34
 DSL, 35
 Metro Ethernet, 35
 satellite, 35
 employees and security breaches, 43
 Internet's changes to, 9
bus topologies, 426
BYOD (Bring Your Own Device), 38
 accessibility, 37
 collaboration tools, 37
 defining, 36
 QoS, 37
 security, 37
bytes, hexadecimal numbering, 311

C

cable
 backbone cabling, 463
 central equipment rooms, 463
 coaxial cable, 453-457
 copper cable, 452
 coaxial cable, 453-456
 electrical hazards, 457
 fiber optic cable versus, 471-472
 fire hazards, 457
 physical layer (OSI reference model), 442, 445
 safety, 457
 STP, 453-455
 UTP, 453-454, 458-464
 entrance facilities, 463
 fiber optic cable, 442
 components of, 466
 copper cable versus, 471-472
 end finish errors, 470
 end gap errors, 470
 misalignment errors, 470
 MMF, 467-468
 network fiber-optic connectors, 468-469
 properties of, 465
 SMF, 467
 testing, 470
 types of, 466-468

- horizontal cabling, 462
- STP, 453-455
- telecommunications rooms, 463
- UTP, 453-454
 - connectors*, 460-461
 - Ethernet crossover cable*, 461
 - Ethernet straight through cable*, 461
 - LAN cabling*, 462-463
 - properties of*, 458-459
 - rollover cable*, 462
 - standards*, 459-460
 - testing*, 464
 - types of*, 461
- work areas, 462
- cable Internet connections**, 33, 457
- capturing text, configuration backups**, 87
- Catalyst 2960 switches, fixed LAN switch configurations**, 529-530
- Catalyst 3560 switches, fixed LAN switch configurations**, 530
- Catalyst 3750 switches, fixed LAN switch configurations**, 530
- Catalyst 4500 switches, modular LAN switch configurations**, 531-532
- Catalyst 4900 switches, modular LAN switch configurations**, 532
- Catalyst 6500 switches, modular LAN switch configurations**, 532
- Catalyst Express 500 switches, fixed LAN switch configurations**, 528
- CCNA (Cisco Certified Network Associate) certification**, 47-48
- cellular Internet connections**, 33
- central equipment rooms, LAN cabling**, 463
- Cerf, Vinton, TCP protocol suite development**, 107
- certifications, CCNA**, 47, 48
- CIDR (Classless Inter-Domain Routing)**, 303
- circuit-switched networks**, 15-16
- Cisco Borderless Network Architectures**, 46
- Cisco Catalyst switches**, 61
- Cisco Express Forwarding, Layer 3 LAN switches**, 536-537
- Cisco routers and USB ports**, 602-603
- Cisco Unified Data Center**, 47
- classful addressing**
 - class A address space, 301
 - class B address space, 301
 - class C address space, 302
 - limits of, 303
- classless addressing (CIDR)**, 303
- CLI (Command-Line Interface)**
 - accessing**
 - AUX ports*, 61
 - console ports*, 59-60
 - SSH protocol*, 60
 - Telnet*, 60
 - terminal emulation programs*, 61
 - CLI prompt, user EXEC mode, 63
 - hostnames, 76-78
 - modes of operation, 62
 - command prompts*, 64
 - global configuration mode*, 64-66
 - interface mode*, 64
 - line mode*, 64
 - navigating between*, 65-66
 - privileged EXEC mode*, 63-66, 80
 - subconfiguration modes*, 64-66
 - user EXEC mode*, 63-66, 81-82
- clients**
 - defining, 24
 - client/server model and application protocols, 148
- cloud computing, 40**
 - benefits of, 41
 - custom clouds, 41
 - data centers, 41-42
 - hybrid clouds, 41
 - private clouds, 41
 - public clouds, 41
- CNAME records**, 155
- coaxial cable, 453-456**
- collaboration**
 - collaboration architectures, 46-47
 - collaboration tools
 - BYOD solutions*, 37
 - defining*, 8
 - online collaboration, 38-39
- commands**
 - abbreviated commands/keywords, 73-74
 - Command Reference, 68-69
 - context-sensitive help, 70

- Ctrl-C and, 73
- Ctrl-R and, 72-73
- Ctrl-Shift-6 and, 73
- Ctrl-Z and, 73
- defining, 67
- examination commands, 74
- finding, 69
- hot keys, 72
- IOS command structure
 - abbreviated commands/keywords*, 73-74
 - arguments*, 67
 - Command Reference*, 68-69
 - command syntax check*, 71
 - context-sensitive help*, 70
 - Ctrl-C*, 73
 - Ctrl-R*, 72-73
 - Ctrl-Shift-6*, 73
 - Ctrl-Z*, 73
 - examination commands*, 74
 - hot keys*, 72
 - keyboard shortcuts*, 72
 - More prompt*, 75
 - syntax*, 68
 - Tab key*, 72
 - Up/Down arrows*, 73
- keyboard shortcuts, 72
- prompts
 - IOS operation*, 64
 - More command prompt*, 75
- syntax
 - error messages*, 71
 - syntax checks*, 71
- Tab key and, 72
- undoing effects of, 79
- Up/Down arrows and, 73
- communication**
 - defining, 10
 - elements of, 123-124
 - messages
 - multiplexing*, 124
 - segmenting*, 124
 - networks
 - business, changes to*, 9
 - communication, changes to*, 7-8
 - computing, evolution of*, 5
 - daily applications*, 4-5
 - entertainment, changes to*, 9-10
 - global communities, development of*, 6, 10
 - learning, changes to*, 6-7
 - non-time sensitive communication (QoS data classifications), 21
 - protocol suites, defining, 104
 - protocols, defining, 103
 - quality of, 12-13
 - remote communication, ARP, 508-510
 - rules of, establishing, 10-12
 - TCP/IP protocol suite communication process, 108-109
 - time sensitive communication (QoS data classifications), 21
 - undesirable communication (QoS data classifications), 21
 - unified communications, collaboration architectures, 47
 - video communication, 39, 40
- computing, evolution of**, 5
- conceptualizing the Internet**, 3, 27-28, 49
- conferencing (video)**, 39-40
- confidentiality (data), network security**, 22
- configuring**
 - default gateways
 - hosts*, 254-255
 - switches*, 255-256
 - hosts, static configuration of global unicast addresses, 325
 - routers
 - initial settings*, 251
 - interface command*, 324
 - LAN interfaces*, 252-253
 - static configuration of global unicast addresses*, 324
 - verifying configurations*, 253-254
 - saving configurations, 84-87
 - terminals, configure terminal command, 78
 - text configurations, restoring, 87-88
- confirming receipt of segments (TCP)**, 196-197
- connection-based access, LAN topologies**, 427
- connection-oriented protocols, TCP**, 178
- connectionless communication, IP**, 215
- connectionless sessions, UDP**, 201

connections (Internet), 32

business Internet connections

*dedicated leased line, 34**DSL, 35**Metro Ethernet, 35**satellite, 35*

remote Internet connections

*cable, 33**cellular, 33**dial-up (telephone), 34**DSL, 33**satellite, 33***connectivity**

testing via ping command

*LAN, 345**local stacks, 344**loopbacks, 345**remote devices, 346*

verifying

*DAD, 343**ICMP, 340-341**NDP, 342-343**testing end-to-end connectivity, 94**testing interface assignments, 94**testing loopback addresses, 93**testing PC-to-switch connectivity, 94***consoles**

CLI environments, accessing via routers, 245

console ports

*IOS access, 59-60**out-of-band access, 59**routers and, 244***controlled access, LAN topologies, 427-429****converged networks**

developing, 14

planning, 14

traditional networks, 13

copper cable, 452

coaxial cable, 453-456

electrical hazards, 457

fiber optic cable versus, 471-472

fire hazards, 457

physical layer (OSI reference model), 442, 445

safety, 457

STP, 453-455

UTP, 453-454

*connectors, 460-461**Ethernet crossover cable, 461**Ethernet straight through cable, 461**LAN cabling, 462-463**properties of, 458-459**rollover cable, 462**standards, 459-460**testing, 464**types of, 461*

copy run start command, router configuration, 251

copy running-config startup-config command,

85, 254

coverage areas (wireless media), 473

Crocker, Steve, RFC development, 119

crosstalk, 452

crypto key generate rsa general-keys modulus command, SSH and remote access, 576

CSMA (Carrier Sense Multiple Access), data collisions, 490

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)

data collisions, 492

media contention, 428

CSMA/CD (Carrier Sense Multiple Access/Collision Detection)

data collisions, 491

media contention, 428

Ctrl-C and IOS, 73

Ctrl-N, 73

Ctrl-P, 73

Ctrl-R and IOS, 72-73

Ctrl-Shift-6 and IOS, 73

Ctrl-Z and IOS, 73

custom clouds (cloud computing), 41

customer collaboration architectures, 46

cut-through switching, 524

D

DAD (Duplicate Address Detection), 343

data

availability, network security, 23

collisions, 490

confidentiality, network security, 22

data centers, 41-42, 47

- encapsulation, 123
 - de-encapsulation process*, 127
 - encapsulation process*, 126
 - Ethernet MAC sublayer*, 489
 - PDU*, 125
- integrity, network security, 23
- interception/theft, 43
- Layer 2 frames, 416
- loss of
 - network security*, 560
 - TCP segments*, 197
- transmission
 - crosstalk*, 452
 - EMI*, 452
 - RFI*, 452
- Data field (Ethernet frames), 497**
- data link addresses**
 - local resources (data delivery), accessing, 128
 - remote resources (data delivery), accessing, 132
- data link layer (OSI reference model), 411-414**
 - addressing, Ethernet MAC sublayer data
 - encapsulation, 489
 - frames, 109, 431
 - 802.11 Wireless frames*, 438-440
 - creating*, 417
 - data*, 416
 - Ethernet frames*, 436-437, 440
 - formatting data for transmission*, 416
 - headers*, 416, 433-434
 - LAN frames*, 435-436
 - PPP frames*, 437-438
 - trailers*, 416, 435
 - WAN frames*, 435-436
- LLC, 413
- MAC, 413-414
 - bus LAN topologies*, 426
 - connection-based access*, LAN topologies, 427
 - controlled access*, LAN topologies, 427-429
 - CSMA/CA*, 428
 - CSMA/CD*, 428
 - extended star (hybrid) LAN topologies*, 426
 - hub and spoke WAN topologies*, 422
 - logical topologies*, 420
 - media sharing*, 420
 - mesh WAN topologies*, 422
 - multi-access LAN topologies*, 429
 - physical topologies*, 420
 - point-to-point WAN topologies*, 422-424
 - ring LAN topologies*, 426, 431
 - star LAN topologies*, 425
 - topologies*, 420
 - media access, 415
 - standards, 418-419
- datagrams and UDP, 181, 201-202**
- decimal addressing, converting**
 - binary notation to decimal addressing*, 271
 - decimal addressing to binary notation*, 272, 275-277, 290
- decimal notation, positional notation, 268**
- dedicated leased line Internet connections, 34**
- de-encapsulation, 127, 214**
- default gateways, 91, 130, 226**
 - configuring
 - hosts*, 254-255
 - switches*, 255-256
 - troubleshooting, 257
- delete vlan.dat command, 86**
- delimiting frames, Ethernet MAC sublayer data**
 - encapsulation, 489
- description command, syntax of, 68**
- description text, configuring LAN interfaces, 253**
- Destination Address field (Ethernet frames), 497**
- destination data link addresses, IP packets, 128**
- destination IP addresses**
 - destination IP address field (IPv4 packet headers), 220
 - IP packets, 127-128, 131, 225
- destination MAC addresses, IP packets, 129, 132**
- destination networks, remote network routes, 235**
- destination ports, 183**
- Destination Unreachable messages (ICMP), 341**
- devices**
 - accessing, security, 79-80
 - connectivity, verifying
 - testing interface assignments*, 94
 - testing loopback addresses*, 93
 - identifiers and EUI-64, 330
 - IP addresses
 - automatic configuration for end devices*, 91-92
 - defining*, 88
 - manual configuration for end devices*, 91
 - names. *See* hostnames

- security, 572
 - banners*, 575
 - best practices*, 574-576
 - exec timeouts*, 575-576
 - pass phrases*, 574
 - passwords*, 573-574
 - SSH*, 576
 - DHCP (Dynamic Host Configuration Protocol)**
 - address pools, 293
 - application layer, 143, 158-160
 - automatic IP address configuration for end devices, 91
 - DHCPACK messages, 160
 - DHCPDISCOVER messages, 159-160
 - DHCNACK messages, 160
 - DHCPOFFER messages, 160
 - DHCPREQUEST messages, 160
 - dynamic IPv4 addresses, assigning to hosts, 292
 - IP address conflicts, 92
 - ipconfig command, 293
 - DHCPv6 (Dynamic Host Configuration Protocol version 6)**
 - global unicast addresses, 328-330
 - Interface ID, 330
 - stateless DHCPv6, 328
 - diagrams (topologies)**, 27
 - logical topology diagrams, 28
 - physical topology diagrams, 28
 - dial-up (telephone) Internet connections**, 34
 - DIMM (dual in-line memory modules), DRAM**, 242
 - direct connections, host packet forwarding**, 226
 - directed broadcast IPv4 addressing**, 295
 - directly connected routes**
 - router packet forwarding, 232
 - routing table entries, 234, 235
 - disable command, navigating CLI between modes of operation**, 65-66
 - disk arrays**, 29. *See also* blocks
 - dispersion**, 467
 - disruption of service and network security**, 560
 - DIZ Ethernet standard**, 107
 - DNS (Domain Name Service) protocol**
 - application layer, 143, 155-157
 - BIND and, 155-156
 - message format, 155-156
 - nslookup command, 157
 - scalability, 157
 - server hierarchy, 156-157
 - DNS servers**, 91
 - domain names, defining**, 155
 - DoS (denial of service) attacks (security)**, 43, 565-566
 - dotted decimal addressing, converting**
 - binary notation to decimal addressing, 271
 - decimal addressing to binary notation, 272, 275-277, 290
 - Down/Up arrows and IOS**, 73
 - DRAM (Dynamic Random Access Memory)**, 242
 - drawing the Internet**, 3, 27-28, 49
 - DS (Differentiated Services) field (IPv4 packet headers)**, 219
 - DSL (Digital Subscriber Line) Internet connections**
 - ADSL, 35
 - business DSL, 35
 - remote user connections, 33
 - SDSL, 35
 - dual stacks**, 309
 - duplex connectors**, 469
 - duplex settings, LAN switches**, 521-522
 - dynamic addressing**
 - defining, 158
 - dynamic link-local addresses, 332-333
 - hosts, assigning to, 292-293
 - dynamic (private) ports and port addressing**, 186
 - dynamic window sizes**, 200
-
- ## E
- education, Internet's changes to**, 6-7
 - EH (Extension Headers), IPv6 packets**, 225
 - EHWIC (Enhanced High-Speed WAN Interface Card) slots and routers**, 244
 - EIA (Electronic Industries Alliance)**, 112
 - EIGRP (Enhanced Interior Gateway Routing Protocol)**, 107
 - electrical hazards, copper cable**, 457
 - email**
 - MDA, 152
 - MTA, 152
 - MUA, 152
 - POP and, 152
 - SMTP and, 152, 154

- embedded IPv4 addresses, 320
- EMI (Electromagnetic Interference), 452
- employees, security breaches, 43
- enable command, navigating CLI between modes of operation, 65
- enable password command, 80
- enable secret command, router configuration, 251
- enable secret password command, 80
- encapsulation
 - data, 123
 - de-encapsulation process*, 127
 - encapsulation process*, 126
 - PDU*, 125
 - Ethernet frames, 494-495
 - IP, 217-218
 - IPv6 packets, 223
 - network layer (OSI reference model), 214
- encoding
 - frames (physical layer), 446-447
 - Manchester encoding, 447
 - NRZ, 447
- encryption, 82
- end devices
 - addressing, 213
 - clients, defining, 24
 - examples of, 24
 - host devices, 24
 - servers, 24
- end finish errors, fiber optic cable, 470
- end gap errors, fiber optic cable, 470
- endpoint security, 571-572
- end-to-end connectivity, testing, 94
- enterprise networks, 465
- entertainment, Internet's changes to, 9-10
- entrance facilities, LAN cabling, 463
- EoC (Ethernet over Copper), 35
- ephemeral ports. *See* dynamic (private) ports and port addressing
- erase command, 86
- erase startup-config command, 86
- errors
 - detecting, Ethernet MAC sublayer data encapsulation, 489
 - messages, command syntax, 71
 - RFC errata, 122
- Ethernet, 486
 - ARP, 504
 - arp -a command*, 513
 - ARP poisoning*, 515
 - ARP spoofing*, 515
 - creating frames*, 505-508
 - maintaining ARP tables*, 505
 - networking devices and ARP tables*, 512
 - operation of*, 505-508
 - overhead*, 514
 - problems with*, 514-515
 - remote communication and*, 508-510
 - removing entries from ARP tables*, 512
 - resolving IP addresses*, 504
 - security*, 515
 - show ip arp command*, 512
 - development of, 107
 - DIX standard, 107
 - EoC, 35
 - Ethernet crossover cable, 461
 - Ethernet II, 495
 - Ethernet straight through cable, 461
 - fiber-optic Ethernet, 35
 - frames, 436-437
 - ARP frame creation*, 505-508
 - Data field*, 497
 - Destination Address field*, 497
 - encapsulation*, 494-495
 - Ethernet II*, 495
 - FCS field*, 497
 - forwarding*, 523-525
 - frame size*, 495-496
 - Length field*, 497
 - Preamble field*, 496
 - processing*, 493-494
 - SFD field*, 496
 - Source Address field*, 497
 - GigabitEthernet interfaces, subnetting IPv4 networks, 361
 - IEEE Ethernet standards, 488
 - LAN interfaces and routers, 246
 - LAN switches
 - Auto-MDIX*, 522
 - cut-through switching*, 524
 - duplex settings*, 521-522
 - fast-forward switching*, 524

- fixed configurations*, 526-530
- fragment-free switching*, 524
- frame forwarding*, 523-525
- full-duplex communication*, 521-522
- half-duplex communication*, 521
- Layer 2 LAN switches*, 535
- Layer 3 LAN switches*, 535-537
- MAC address tables*, 517-520
- mdix auto interface command*, 522
- memory buffering*, 525
- modular configurations*, 526-527, 531-534
- ports*, 516
- store-and-forward switching*, 523
- LLC sublayer, 487, 494
- MAC addresses, 128, 492, 497
 - ARP, 130
 - broadcast MAC addresses, 501
 - EUI-64, 330-331
 - frame processing, 493-494
 - hexadecimal, 498-499
 - identifying, 500
 - IP addresses and, 502-503
 - ipconfig/all command, 500
 - IP packets, 129, 132
 - LAN switches, 517-520
 - MAC address structures, 492
 - multicast MAC addresses, 501
 - resolving via ARP, 504
 - unicast MAC addresses, 500
- MAC sublayer, 488
 - data encapsulation, 489
 - MAC, 490-492
- Metro Ethernet Internet connections, 35
- ports, 89
- TCP/IP communication process, 109
- EUI-64 (Extended Unique Identifier 64), unicast IPv6 addresses, 330-331
- examination commands, 74
- exec timeouts, device security, 575-576
- exit command, navigating CLI from global configuration mode and submodes, 66
- expandability (networks), 550
- expectational acknowledgement, 196
- experimental IPv4 addresses, 301
- experimental RFC (Request for Comments), 122
- extended ping command, 580-581

- extended star (hybrid) topologies, 426
- external QoS (Quality of Service), communication and, 12-13
- extranet, defining, 32. *See also* Internet, intranet

F

- Fast Ethernet SFP modules, 534
- fast-forward switching, 524
- fault tolerance, circuit-switched networks, 15
- FCS (Frame Check Sequence) field, Ethernet frames, 497
- fiber optic cable
 - components of, 466
 - copper cable versus, 471-472
 - end finish errors, 470
 - end gap errors, 470
 - misalignment errors, 470
 - MMF, 467-468
 - network fiber-optic connectors, 468-469
 - physical layer (OSI reference model), 442
 - properties of, 465
 - SMF, 467
 - testing, 470
 - types of, 466-468
- fiber optic Ethernet, 35
- file sharing
 - file sharing protocols
 - FTP, 161-162
 - SAMBA, 163
 - SMB, 162
 - P2P, 8
- finding commands, 69
- FIN (finish) control flags, TCP three-way handshakes, 194
- fire hazards, copper cable, 457
- firewalls
 - dedicated firewall systems, 44
 - filtering, 44
 - network security, 570
- first host addresses, IPv4 addressing, 284
- fixed LAN switch configurations, 526-527
 - Catalyst 2960, 529-530
 - Catalyst 3560, 530
 - Catalyst 3750, 530
 - Catalyst Express 500, 528

Flash, 606

- flash drives (USB), backing up/restoring IOS configuration files, 603-605
- file systems, 598
- memory, 57, 243

flat network design, 357**flow control**

- TCP, 179
 - congestion, avoiding, 200*
 - window size, 198-199*
- UDP, 180

flow label field, IPv6 packet headers, 224**FM (Frequency Modulation), 448****formatting IPv6 addresses**

- 0 segments, 315
- leading 0s, 313
- preferred format, 312

fragmentation, 217

- fragment-free switching, 524
- IPv4 packet header fields, 220

frames, 412

- delimiting, Ethernet MAC sublayer data encapsulation, 489
- encoding, physical layer (OSI reference model), 446-447

Ethernet frames

- ARP frame creation, 505-508*
- Data field, 497*
- Destination Address field, 497*
- encapsulation, 494-495*
- Ethernet II, 495*
- FCS field, 497*
- forwarding, 523-525*
- frame size, 495-496*
- Length field, 497*
- Preamble field, 496*
- processing, 493-494*
- SFD field, 496*
- Source Address field, 497*

Layer 2 frames, 431

- 802.11 Wireless frames, 438-440*
- addresses, 433-434*
- creating, 417*
- data, 416*

*Ethernet frames, 436-437, 440**formatting data for transmission, 416**headers, 416, 433**LAN frames, 435-436**PPP frames, 437-440**trailers, 416, 435**WAN frames, 435-436***FTP (File Transfer Protocol)**

- application layer, 143
- processes, 161

FTTH (Fiber To The Home), access networks, 465**full-duplex communication**

- LAN switches, 521-522
- point-to-point WAN topologies, 425

G**gateways**

- IPv4 host routing tables, 228
- IPv6 route tables, 231

GET messages (HTTP), 151**.GIF (Graphics Interchange Format) files, presentation layer, 142****Gigabit Ethernet SFP modules, 534****GigabitEthernet interfaces, subnetting IPv4 networks, 361****global communities, development of, 6, 10****global configuration mode**

- IOS operation, 64
- navigating from, 66

global routing prefixes, 323**global unicast addresses, 319, 322, 332****dynamic configuration**

- DHCPv6, 328-330*
- SLAAC, 327-328*

global routing prefixes, 323**Interface ID, 323, 330****reading, 324****static configuration**

- host configuration, 325*
- router configuration, 324*

Subnet ID, 323

H

hacker attacks, 43

half-duplex communication

- LAN switches, 521

- point-to-point WAN topologies, 424

handshakes (three-way), TCP, 190

- ACK control flags, 192-193

- SYN control flags, 191-193

- SYN segments, 192

hardware, defining, 24

header checksum field (IPv4 packet headers), 220

headers

- IPv4 packets, 218

 - destination IP address field, 220*

 - DS field, 219*

 - header checksum field, 220*

 - identification field, 220*

 - IHL field, 220*

 - protocol field, 219*

 - sample headers, 221*

 - source IP address field, 220*

 - total length field, 220*

 - TTL (Time to Live) field, 219*

 - version field, 219*

- IPv6 packets

 - destination IP field, 225*

 - EH, 225*

 - flow label field, 224*

 - hop limit field, 225*

 - next header field, 225*

 - payload length field, 225*

 - sample headers, 225*

 - source IP address field, 225*

 - traffic class field, 224*

 - version field, 224*

- Layer 2 frames, 416, 433

hexadecimal numbering

- Ethernet MAC addresses, 498

 - number conversions, 499*

 - value representation, 499*

- IPv6 addressing, 311-312

hextet, 312

high importance to organization (QoS data classifications), 21

historic RFC (Request for Comments), 122

hops, 214

- hop counts, 219

- IPv6 hop limits

 - packet headers, 225*

 - testing via traceroute command, 347-348*

- next-hop addressing, 235-236

horizontal cabling, LAN cabling, 462

hostnames, 76

- applying, example of, 78

- configuring, 78

- naming conventions, 77

hosts, 213

- configuring

 - default gateways, 254-255*

 - static configuration of global unicast addresses, 325*

- dynamic IPv4 addresses, assigning to hosts, 292-293

- host addresses, IPv4 addressing, 282, 297

 - first host addresses, 284*

 - last host addresses, 285*

- host commands, monitoring network performance

 - arp command, 591-592*

 - ipconfig command, 590*

 - show cdp neighbors command, 592-594*

 - show ip interface brief command, 594-595*

- Host Confirmation messages (ICMP), 340

- host devices, defining, 24

- host routing tables

 - host packet forwarding decisions, 226*

 - IPv4, 227-230*

 - IPv6 sample table, 231-232*

- static IPv4 addresses, assigning to hosts, 290-292

- subnetting

 - formulas, 365*

 - host calculations, 366-367, 371, 374, 377*

hot keys, 72

HTML (Hypertext Markup Language), 108, 150

HTTP (Hypertext Transfer Protocol)

- application layer, 143, 149-150

- GET messages, 151

- POST messages, 151

- PUT messages, 151

- segments, 105

- TCP/IP communication process, 108

HTTPS (HTTP Secure), 151

hub and spoke topologies, 422

human networks, development of, 6, 10
 hybrid (extended star) topologies, 426
 hybrid clouds (cloud computing), 41

I

IAB (Internet Architecture Board), 110
IANA (Internet Assigned Numbers Authority), 113
 IP address assignments, 304
 port number assignments, 184
ICANN (Internet Corporation for Assigned Names and Numbers), 113
ICMP (Internet Control Message Protocol)
 Destination Unreachable messages, 341
 Host Confirmation messages, 340
 Route Redirection messages, 341
 Service Unreachable messages, 341
 Time Exceeded messages, 341
I-D (Internet-Draft), RFC creation/validation process, 120
identification field (IPv4 packet headers), 220
identity theft, 43, 560
IEEE (Institute of Electrical and Electronics Engineers), 111-112
 data link layer standards, 418
 Ethernet standards, 488
IEEE 802.3 standard, 107
IEEE 802.11 (WLAN), 474
 AP, 475
 NIC adapters, 475
 standards, 476
 Wireless frames, 438-440
IEEE 802.15 (WPAN), 474
IEEE 802.16 (WiMAX), 474
IETF (Internet Engineering Task Force), 110, 303
If column (IPv6 route tables), 231
IHL (Internet Header Length) field (IPv4 packet headers), 220
IM (instant messaging), 7. *See also* texting
image files (IOS) and routers, 247-249
IMAP (Internet Message Access Protocol), application layer, 143
IMP (Interface Message Processors), RFC development, 119
impconfig/all command, identifying Ethernet MAC addresses, 500

inband router interfaces, router connections, 245
informational RFC (Request for Comments), 121
information theft and network security, 22, 560
infrastructures (network)
 components of, 23
 end devices, 24
 interfaces, 27
 intermediary devices, 25
 LAN, 29-30
 MAN, 29
 media, 25-27
 NIC, 27
 physical ports, 27
 SAN, 29
 small networks, 556
 topology diagrams, 27-28
 types of, 28-29
 WAN, 29-30
 WLAN, 29
integrated firewalls, 570
integrity (data), network security, 23
interception/theft (data), 43
interface command, router configuration, 324
Interface ID
 DHCPv6, 330
 global unicast addresses, 323, 330
 IPv6 subnetting, 400
 randomly generated Interface ID, 331-332
interface lists, IPv4 host routing tables, 227
interface mode, IOS operation, 64
interface type-and-number command, configuring LAN interfaces, 252
interfaces
 assigning, testing assignments, 94
 defining, 27
 IPv4 host routing tables, 228
 small networks, 549
 switch interfaces, verifying, 94
 virtual interfaces
 defining, 89
 switch virtual interfaces, 90-91
 VLAN interfaces, verifying assignments, 94
interference (wireless media), 473
intermediary devices. *See* network, devices
internal QoS (Quality of Service) and communication, 12-13

Internet. *See also* intranet, extranet

- access technologies, 32
 - business access*, 34-35
 - remote access*, 33-34
- business, changes to, 9
- BYOD, 38
 - accessibility*, 37
 - collaboration tools*, 37
 - defining*, 36
 - QoS*, 37
 - security*, 37
- cable Internet, coaxial cable, 457
- cloud computing, 40-41
- communication, changes to, 7-8
- conceptualizing, 3, 27-28, 49
- connections, 32
 - business connections*, 35
 - business Internet connections*, 34-35
 - cable*, 33
 - cellular*, 33
 - dedicated leased line*, 34
 - dial-up (telephone)*, 34
 - DSL*, 33-35
 - Metro Ethernet*, 35
 - remote Internet connections*, 33-34
 - satellite*, 33
- daily applications, 5
- data centers, 41-42
- defining, 4
- development of, 107-108
- drawing, 3, 49
- entertainment, changes to, 9-10
- evolution of, 5
- global communities, development of, 6, 10
- IANA, IP address assignments, 304
- IETF, classless addressing (CIDR), 303
- Internet of things, 308-309
- Internet standards and RFC creation/validation process, 121
- ISP, IP address assignments, 305-307
- LAN and, 30
- learning, changes to, 6-7
- mapping, 3, 49
- network administration organizations, 31

new trends

- BYOD*, 36-38
- cloud computing*, 40-41
- data centers*, 41-42
- online collaboration*, 38-39
- video communication*, 39-40

online collaboration, 38-39

RIR, IP address assignments, 304-305

video communication, 39-40

WAN and, 30

intranet, defining, 32. *See also* Internet, extranet**IOS (Internetwork Operating System), 56**

accessing

- AUX ports*, 61
- console ports*, 59-60
- SSH protocol*, 60
- Telnet*, 60
- terminal emulation programs*, 61

backups via

- text capture (Tera Term)*, 600
- text files*, 600
- TFTP*, 601-602
- USB flash drives*, 603

banner messages, 83-84

CLI

- accessing*, 59-61
- CLI prompt*, 63
- hostnames*, 76-78
- modes of operation*, 62-66

Command Reference, 68-69

command structure

- abbreviated commands/keywords*, 73-74
- arguments*, 67
- Command Reference*, 68-69
- command syntax check*, 71
- context-sensitive help*, 70
- Ctrl-C*, 73
- Ctrl-R*, 72-73
- Ctrl-Shift-6*, 73
- Ctrl-Z*, 73
- examination commands*, 74
- hot keys*, 72
- keyboard shortcuts*, 72
- More prompt*, 75
- syntax*, 68

- Tab key*, 72
- Up/Down arrows*, 73
- configurations
 - restoring text configurations*, 87-88
 - saving*, 84-87
 - text capture*, 87
- connectivity, verifying
 - testing end-to-end connectivity*, 94
 - testing interface assignments*, 94
 - testing loopback addresses*, 93
 - testing PC-to-switch connectivity*, 94
- context-sensitive help, 70
- devices, securing access, 79-80
- examination commands, 74
- Flash file systems, 598
- Flash memory, 57
- functions, 58
- hot keys, 72
- image files and routers, 247-249
- keyboard shortcuts, 72
- modes of operation
 - command prompts*, 64
 - global configuration mode*, 64-66
 - interface mode*, 64
 - line mode*, 64
 - navigating between*, 65-66
 - privileged EXEC mode*, 63-66, 80
 - subconfiguration modes*, 64-66
 - user EXEC mode*, 63-66, 81-82
- More prompt, 75
- network performance, monitoring
 - arp command*, 591-592
 - ipconfig command*, 590
 - show cdp neighbors command*, 592-594
 - show ip interface brief command*, 594-595
- NVRAM file systems, 598
- ping indicators, 578-579
- RAM, 57, 242
- restoring via
 - text capture (Tera Term)*, 600
 - text configurations*, 601
 - text files*, 600
 - TFTP, 602
 - USB flash drives, 605
- router file systems, 596-598
- routers, 57
 - bootups*, 247
 - functions*, 58
- security, passwords, 79
- switch file systems, 598
- switches, 57, 76
 - configuring management addresses*, 95
 - functions*, 58
 - testing PC-to-switch connectivity*, 94
 - virtual interfaces*, 90-91
- text capture, configuration backups, 87
- text configurations, restoring, 87-88
- variations of, 57
- virtual interfaces, switches, 90-91
- IP (Internet Protocol), 106**
 - characteristics of, 215
 - best effort (unreliable) delivery*, 215, 216
 - connectionless communication*, 215
 - encapsulation*, 217, 218
 - media independence*, 215, 217
 - IP addresses, 90
 - ARP, resolving IP addresses, 504
 - automatic configuration for end devices, 91, 92
 - conflicts, 92
 - default gateways, 91
 - defining, 17, 88
 - DNS servers, 91
 - hosts, 213
 - ip address command and subnetting*, 363
 - ip address subnet-mask command, configuring LAN interfaces*, 253
 - MAC addresses and, 502-503
 - manual configuration for end devices, 91
 - small networks, 550, 551
 - sockets, 184
 - testing end-to-end connectivity*, 94
 - Windows IP configuration, verifying, 92
 - IP packets
 - data link frames*, 109
 - destination data link addresses*, 128
 - destination IP addresses*, 127, 128, 131
 - destination MAC addresses*, 129, 132
 - source data link addresses*, 128
 - source IP addresses*, 127, 128, 131
 - source MAC addresses*, 129, 132
 - TCP/IP communication process, 109

- ipconfig command, 92, 293, 590
- ip domain-name command, SSH and remote access, 576
- IP protocol suite, 107
- IP telephony, small networks, 557
- private addresses, 120
- routing tables and RAM, 242
- IPS (Intrusion Prevention Systems), 44**
- IPv4 addressing**
 - address depletion, 307
 - binary notation, 267-268
 - binary number system, 269-270*
 - converting binary addresses to decimal, 271*
 - converting decimal addresses to binary notation, 272, 275-277, 290*
 - broadcast addresses, 283
 - broadcast addressing, 295
 - classful addressing
 - class A address space, 301*
 - class B address space, 301*
 - class C address space, 302*
 - limits of, 303*
 - classless addressing (CIDR), 303
 - dynamic addresses, assigning to hosts, 292-293
 - experimental addresses, 301
 - host addresses, 282
 - first host addresses, 284*
 - last host addresses, 285*
 - host portion, 278
 - host routing tables, 227
 - host routing entries, 228-229*
 - sample table, 229-230*
 - IANA address assignments, 304
 - Internet of things, 308-309
 - IPv6 addressing and
 - dual stacks, 309*
 - NAT64, 310*
 - tunneling, 309*
 - ISP address assignments, 305-307
 - issues with, 307-309
 - LAN interfaces, configuring, 253
 - link local addresses, 300
 - loopbacks, 299
 - multicast addressing, 296-297
 - network addresses, 281, 289
 - network portion, 278
 - packets
 - end-to-end connectivity, 222*
 - headers, 218-221*
 - hops, 214*
 - improvements to packet handling, 222*
 - Internet routing table expansion, 221*
 - IP address depletion, 221*
 - IP address space, 222*
 - limitations of, 221-222*
 - NAT, 222*
 - payloads, 218*
 - positional notation, 268
 - private addresses, 298-299
 - public addresses, 299
 - RIR address assignments, 304-305
 - router routing tables, 233, 236-239
 - static addresses, assigning to hosts, 290-292
 - subnet masks, 278
 - ANDing, 287-290*
 - broadcast addresses, 283*
 - first host addresses, 284*
 - host addresses, 282-285*
 - last host addresses, 285*
 - network addresses, 281, 289*
 - prefix length, 279*
 - subnetting
 - address assignments, 393-396*
 - addressing schemes, 393-396*
 - basic subnetting, 359-362*
 - creating 4 subnets, 365-367*
 - creating 8 subnets, 368-371*
 - creating 100 subnets with a /16 prefix, 372-374*
 - creating 1000 subnets with a /8 prefix, 375-376*
 - determining subnet masks, 378-384*
 - flat network design, 357*
 - GigabitEthernet interfaces, 361*
 - host calculation, 366-367, 371, 374, 377*
 - ip address command, 363*
 - network segmentation, 358-359*
 - reasons for subnetting, 357-358*
 - subnet communication, 358-359*
 - subnetting formulas, 364-365*
 - VLSM, 386-393, 397*
 - wasted addresses, 384-385*

testing

- connectivity via ping command, 344-346*

- paths via traceroute command, 347-348*

- TEST-NET addresses, 301*

TTL fields, testing via traceroute command, 347-348

unicast addresses, 293-294, 320

verifying connectivity

- address resolution, 343*

- DAD, 343*

- ICMP, 340-341*

- NDP, 342-343*

IPv6 addressing

anycast addresses, 318

formatting addresses

- 0 segments, 315*

- leading 0s, 313*

- preferred format, 312*

hexadecimal numbering, 311-312

hop limits, testing via traceroute command, 347-348

host routing tables

- If column, 231*

- sample table, 231-232*

IANA address assignments, 304

IPv4 addressing and,

- dual stacks, 309*

- NAT64, 310*

- tunneling, 309*

ipv6 unicast-routing command, assigned multicast

- IPv6 addresses, 337

ISP address assignments, 305-307

multicast addresses, 318

- assigned multicast addresses, 337*

- solicited-node multicast addresses, 338-339*

need for, 307

packets

- authentication, 222*

- benefits of, 222*

- encapsulation, 223*

- headers, 224-225*

- hops, 214*

- NAT, 222*

- privacy, 222*

- security, 222*

prefix length, 318

RIR address assignments, 304-305

subnetting

- Interface ID, 400*

- subnet allocation, 399-400*

- Subnet ID, 397-398*

testing

- connectivity via ping command, 344-346*

- paths via traceroute command, 347-348*

unicast addresses, 317

- embedded IPv4 addresses, 320*

- EUI-64, 330-331*

- global unicast addresses, 319, 322-332*

- link-local addresses, 320-321, 332-334*

- loopbacks, 320*

- randomly generated Interface ID, 331-332*

- unique local addresses, 320*

- unspecified addresses, 320*

verifying

- configurations, 334-337*

- connectivity, 340-343*

IRTF (Internet Research Task Force), 110**ISN (Initial Sequence Numbers)**

- TCP segments, resequencing, 196

- TCP three-way handshakes, 191

ISO (International Organization of Standards), 112, 418**ISOC (Internet Society), 110****ISP (Internet Service Providers), IP address assignments, 305-307****ITU (International Telecommunication Union), data link layer standards, 418****ITU-T (International Telecommunications Union-Telecommunication Standardization Sector), 113**

J - K

job opportunities, 48

.JPEG (Joint Photographics Experts Group) files, presentation layer, 142

Kahn, Robert, TCP protocol suite development, 107

keyboard shortcuts, 72

keywords, abbreviated keywords/commands, 73-74

L**LAN (Local-Area Networks), 29-30**

- bus topologies, 426
- connection-based access, 427
- connectivity, testing via ping command, 345
- controlled access, 427-429
- copper cable, 462-463
- Ethernet LAN interfaces and routers, 246
- extended star (hybrid) topologies, 426
- frames, 435-436
- IEEE 802.3 standard, 107
- interfaces, configuring, 252-253
- multi-access topologies, 429
- ring topologies, 426, 431
- routers and, 244-246
- star topologies, 425
- WLAN, 474
 - AP, 475
 - NIC adapters, 475
 - standards, 476

LAN adapters. See NIC**LAN switches**

- Auto-MDIX, 522
- cut-through switching, 524
- duplex settings, 521-522
- fast-forward switching, 524
- fixed configurations, 526-527
 - Catalyst 2960*, 529-530
 - Catalyst 3560*, 530
 - Catalyst 3750*, 530
 - Catalyst Express 500*, 528
- fragment-free switching, 524
- frame forwarding, 523-525
- full-duplex communication, 521-522
- half-duplex communication, 521
- Layer 2 LAN switches, 535
- Layer 3 LAN switches, 535
 - Cisco Express Forwarding*, 536-537
 - Layer 3 EtherChannel*, 538
 - routed port interfaces*, 538
 - SVI, 537
- MAC address tables, 517-520
- mdix auto interface command, 522
- memory buffering, 525

- modular configurations, 526-527

- Catalyst 4500*, 531-532

- Catalyst 4900*, 532

- Catalyst 6500*, 532

- SFP ports*, 533-534

- ports, 516

- store-and-forward switching, 523

last host addresses and IPv4 addressing, 285**latency, 450****Layer 2 frames, 431**

- 802.11 Wireless frames, 438-440

- addresses, 433-434

- creating, 417

- data, 416

- Ethernet frames, 436-437, 440

- formatting data for transmission, 416

- headers, 416, 433

- LAN frames, 435-436

- PPP frames, 437-440

- trailers, 416, 435

- WAN frames, 435-436

Layer 2 LAN switches, 535**Layer 3 LAN switches, 535**

- Cisco Express Forwarding, 536-537

- Layer 3 EtherChannel, 538

- routed port interfaces, 538

- SVI, 537

layered models, benefits of, 113**LC (Lucent Connectors), 468****learning, Internet's changes to, 6-7****leased line Internet connections, 34****LED indicators, router connections, 245****legacy classful addressing**

- class A address space, 301

- class B address space, 301

- class C address space, 302

- limits of, 303

Length field (Ethernet frames), 497**limited broadcast IPv4 addressing, 295****line mode, IOS operation, 64****link-local addresses, 300**

- dynamic link-local addresses, 332-333

- IPv6 addressing, 320-321

- dynamic link-local addresses*, 332-333

- static link-local addresses*, 333-334

- static link-local addresses, 333-334

LLC (Logical Link Control), 413
 LLC sublayer (Ethernet), 487, 494
 local default route, host packet forwarding, 226
 local hosts, host packet forwarding, 226
 local network route, host packet forwarding, 226
 local resources (data delivery), accessing
 communicating with devices on the same network,
 128-129
 data link addresses, 128
 network addresses, 127-128
 logical topologies
 diagrams, 28
 logical ring topologies, 431
 MAC, 420
 point-to-point topologies, 423
 login command, 82, 251
 login local command, SSH and remote access, 576
 long-haul networks, 465
 loopbacks, 299
 addresses, testing, 93
 direct connections, 226
 interfaces, 226
 IPv6 addressing, 320
 ping command, 345
 testing, 579-580
 losing segments (TCP), 197

M

MAC addresses, 128
 ARP, 130, 504
 Ethernet, 492-494
 frame processing, 493-494
 MAC address structures, 492
 Ethernet MAC addresses, 497
 broadcast MAC addresses, 501
 hexadecimal, 498, 499
 identifying, 500
 IP addresses and, 502, 503
 ipconfig/all command, 500
 multicast MAC addresses, 501
 unicast MAC addresses, 500
 EUI-64, 330, 331
 IP addresses and, 502
 end-to-end connectivity, 503
 IP packets
 destination MAC addresses, 129, 132
 source MAC addresses, 129, 132
 LAN switches, 517, 519-520
 MAC (Media Access Control), 413-414, 419
 CSMA/CA, 428
 CSMA/CD, 428
 Ethernet MAC sublayer, 488
 CSMA, 490
 CSMA/CA, 492
 CSMA/CD, 491
 data collisions, 490-492
 data encapsulation, 489
 MAC addresses, 128, 492
 ARP, 130, 504
 broadcast MAC addresses, 501
 destination MAC addresses, 129, 132
 EUI-64, 330-331
 frame processing, 493-494
 hexadecimal, 498-499
 identifying, 500
 IP addresses and, 502-503
 ipconfig/all command, 500
 LAN switches, 517-520
 multicast MAC addresses, 501
 source MAC addresses, 129, 132
 structures of, 492
 unicast MAC addresses, 500
 media sharing, 420
 topologies, 420
 bus LAN topologies, 426
 connection-based access, LAN topologies, 427
 controlled access, LAN topologies, 427-429
 extended star (hybrid) LAN topologies, 426
 hub and spoke WAN topologies, 422
 logical topologies, 420
 mesh WAN topologies, 422
 multi-access LAN topologies, 429
 physical topologies, 420
 point-to-point WAN topologies, 422-424
 ring LAN topologies, 426, 431
 star LAN topologies, 425
 MAN (Metropolitan-Area Networks), 29
 management addresses (switches), configuring, 95
 management ports, router connections, 245
 Manchester encoding, 447

mapping

- Internet, 3, 49, 27-28
- networks, 27-28

MDA (Mail Delivery Agents) and email, 152**mdix auto interface command, 522****media**

- contention
 - CSMA/CA, 428
 - CSMA/CD, 428
- defining, 25
- independence, IP, 215-217
- network media, defining, 89
- sharing, 420

memory

- buffering via LAN switches, 525
- DRAM
 - DIMM and*, 242
 - routers and*, 242
- Flash memory, 57, 243
- NVRAM
 - router bootups*, 249
 - routers and*, 242
- RAM
 - ARP caches and*, 242
 - DRAM, DIMM and*, 242
 - DRAM, routers and*, 242
 - IOS and*, 57, 242
 - IP routing tables and*, 242
 - NVRAM*, 242, 249
 - packet buffers and*, 242
 - routers and*, 241
 - running configuration (running-config) files and*, 242
 - saving running configurations*, 87
- ROM, 242
- routers and
 - Flash memory*, 243
 - NVRAM*, 242
 - RAM*, 241
 - ROM*, 242

mesh topologies, 422**messages**

- communication, elements of, 123-124
- DHCPACK messages, 160
- DHCPDISCOVER messages, 159-160

- DHCNPAK messages, 160
- DHCPOFFER messages, 160
- DHCPREQUEST messages, 160
- formats of, 155-156
- GET messages (HTTP), 151
- multiplexing, 124
- POST messages (HTTP), 151
- PUT messages (HTTP), 151
- segmenting, 124

Metcalf, Bob, Ethernet development, 107**metrics**

- IPv4 host routing tables, 228
- IPv6 route tables, 231
- remote network routes, 235

Metro Ethernet Internet connections, 35**misalignment errors, fiber optic cable, 470****MMF (Multimode Fiber), 467-468****modular LAN switch configurations, 526-527**

- Catalyst 4500, 531-532
- Catalyst 4900, 532
- Catalyst 6500, 532
- SFP ports, 533-534

modulation, 448-449**More prompt, 75****MOTD (Message Of The Day) banner, 83-84****moving data in networks**

- accessing
 - local resources*, 127-129
 - remote resources*, 130-132
- data encapsulation, 123-127
- multiplexing messages, 124
- segmenting messages, 124

.MPEG (Motion Picture Experts Group) files, presentation layer, 142**MTA (Mail Transfer Agents) and email, 152****MTU (Maximum Transmission Units), 217****MUAN (Mail User Agents), 152****multi-access topologies, 429****multicast addresses**

- IPv4 addressing, 296-297
- IPv6 addresses, 318
 - assigned multicast addresses*, 337
 - solicited-node multicast addresses*, 338-339
- MAC addresses, 501

multiplexing

- conversations, transport layer (OSI reference model), 173
- messages, 124

MX records, 155**N****naming devices. *See* hostnames****NAT (Network Address Translation)**

- IPv4 packets, 222
- IPv6 packets, 222

NAT64 (Network Address Translation 64), 310**NDP (Neighbor Discovery Protocol)**

- Neighbor Advertisement messages, 343
- Neighbor Solicitation messages, 343
- Router Advertisement messages, 342
- Router Solicitation messages, 342

netmasks, IPv4 host routing tables, 228**netstat command, TCP/UDP port addressing, 186****netstat -r command**

- IPv4 host routing tables, 227-228
- IPv6 host routing tables, 231

network access

- data link layer, 411-412
 - frames*, 416-417, 431-440
 - LAN topologies*, 425-431
 - LLC*, 413
 - MAC*, 413-414, 419-431
 - media access*, 415
 - standards*, 418-419
 - WAN topologies*, 422-424

network access protocols, 106**physical layer, 411, 441**

- bandwidth*, 449-450
- components of*, 445
- copper cable*, 442, 445
- fiber-optic cable*, 442
- frame encoding*, 446-447
- functions*, 445
- signaling method*, 447-449
- standards*, 443-444
- throughput*, 450
- wireless media*, 442

Network Basics Lab Manual, 3**network layer (OSI reference model)**

- de-encapsulation, 214
- encapsulation, 214
- end devices, addressing, 213
- IP, characteristics of
 - best effort (unreliable) delivery*, 215-216
 - connectionless communication*, 215
 - encapsulation*, 217-218
 - media independence*, 215-217

IPv4, 214

- end-to-end connectivity*, 222
- host routing tables*, 227-230
- improvements to packet handling*, 222
- Internet routing table expansion*, 221
- IP address depletion*, 221
- IP address space*, 222
- limitations of*, 221-222
- NAT*, 222
- packets*, 218-221
- router routing tables*, 233, 236-239

IPv6, 214

- authentication*, 222
- benefits of*, 222
- encapsulation*, 223
- headers*, 224-225
- host routing tables*, 231-232
- NAT*, 222
- privacy*, 222
- security*, 222

PDU, 217**routers**

- AUX ports*, 244
- backplane*, 244
- bootups*, 247-250
- branches*, 241
- computers, routers as*, 240-241
- configuring initial settings*, 251
- configuring LAN interfaces*, 252-253
- connecting to*, 245-246
- console ports*, 244
- CPU and OS*, 241
- default gateways*, 254-256
- EHWIC slots*, 244
- inside of*, 243
- LAN*, 244
- LAN interfaces*, 245-246

- memory*, 241-243
- service providers*, 241
- verifying configurations*, 253-254
- WAN, 241
 - WAN interfaces, 245-246
- routing, 214
 - host routing tables*, 226-232
 - router routing tables*, 232-240
- networks**
 - access networks, FTTH, 465
 - application layer
 - client/server model and application protocols*, 148
 - defining*, 141
 - network-aware applications*, 144
 - OSI reference model*, 140
 - P2P networks and application protocols*, 145-147
 - protocols*, 141, 145
 - services*, 144
 - TCP/IP protocol suite*, 141-143, 149-150
 - architectures
 - CCNA certification*, 47-48
 - Cisco Borderless Network Architectures*, 46
 - Cisco Unified Data Center*, 47
 - collaboration architectures*, 46-47
 - defining*, 45
 - baselines, determining, 581-582
 - business, changes to, 9
 - BYOD, 38
 - accessibility*, 37
 - collaboration tools*, 37
 - defining*, 36
 - QoS*, 37
 - security*, 37
 - CCNA certification, 47-48
 - circuit-switched networks, 15-16
 - Cisco Borderless Network Architectures, 46
 - Cisco Unified Data Center, 47
 - clients, defining, 24
 - cloud computing, 40-41
 - collaboration architectures, 46, 47
 - collaboration tools
 - BYOD solutions*, 37
 - defining*, 8
 - communication
 - business*, 9
 - changes in*, 7-8
 - daily applications*, 4-5
 - entertainment*, 9-10
 - evolution of computing*, 5
 - global communities*, 6, 10
 - learning*, 6-7
 - components of, 23
 - end devices*, 24
 - interfaces*, 27
 - intermediary devices*, 25
 - media*, 25
 - network representations*, 26-28
 - NIC*, 27
 - physical ports*, 27
 - topology diagrams*, 27-28
 - connectivity
 - testing via ping command*, 344-346
 - verifying*, 93-94
 - converged networks
 - developing*, 14
 - planning*, 14
 - traditional networks*, 13
 - data centers, 41-42
 - data encapsulation, 123
 - de-encapsulation process*, 127
 - encapsulation process*, 126
 - PDU*, 125
 - destinations
 - IPv6 route tables*, 231
 - remote network routes*, 235
 - devices
 - defining*, 56
 - end devices*, 24
 - securing access*, 79-80
 - security*, 572-576
 - endpoints, security, 571-572
 - enterprise networks, 465
 - entertainment, changes to, 9-10
 - expandability, 550
 - fiber-optic connectors, 468-469
 - hardware, defining, 24
 - host devices, defining, 24
 - hostnames, 76
 - applying*, 78
 - configuring*, 78
 - naming conventions*, 77
 - human networks, development of, 6, 10

infrastructures

- components of*, 23-28
- end devices*, 24
- interfaces*, 27
- intermediary devices*, 25
- LAN, 29-30
- MAN, 29
- media*, 25
- network representations*, 26-28
- NIC, 27
- physical ports*, 27
- SAN, 29
- topology diagrams*, 27-28
- types of*, 28-29
- WAN, 29-30
- WLAN, 29

interfaces, defining, 27

intermediary devices, defining, 25

Internet administration organizations, 31

IP addresses

- automatic configuration for end devices*, 91-92
- defining*, 88
- manual configuration for end devices*, 91
- sockets*, 184

LAN, 29

- configuring interfaces*, 252-253
- IEEE 802.3 standard*, 107
- Internet and*, 30
- routers and*, 244-246
- testing connectivity via ping command*, 345
- WLAN, 474-477

learning, changes to, 6-7

long-haul networks, 465

MAC addresses, 128

- ARP, 130
- IP packets*, 129, 132

MAN, 29

mapping, topology diagrams, 27-28

media, defining, 25, 89

moving data in

- accessing local resources*, 127-129
- accessing remote resources*, 130-132
- data encapsulation*, 123-127
- multiplexing messages*, 124
- segmenting messages*, 124

network architecture, defining, 15

network addresses

- IPv4 addressing*, 281, 289, 297
- local resources (data delivery)*, *accessing*, 127-128
- remote resources (data delivery)*, *accessing*, 131
- Windows Calculator*, 289

network applications

- network-aware applications*, *defining*, 144
- small networks*, 554

network protocols, 105

network representations, 26-28

network services, defining, 24

new trends

- BYOD, 36-38
- cloud computing*, 40-41
- data centers*, 41-42
- online collaboration*, 38-39
- video communication*, 39-40

NIC, defining, 27

online collaboration, 38-39

packet-switched networks

- IP addresses*, *defining*, 17
- queues*, 20

paths, testing via traceroute command, 347-348

performance, monitoring

- arp commands*, 591-592
- host commands*, 590-595
- IOS commands*, 590-595
- ipconfig commands*, 590
- ping command*, 578-582
- show cdp neighbors commands*, 592-594
- show commands*, 585, 588-589
- show ip interface brief command*, 594-595
- tracert command*, 583-585

physical ports, defining, 27

platforms, networks as

- converged networks*, 13-14
- reliable networks*, 15-23

presentation layer

- .GIF files*, 142
- .JPEG files*, 142
- .MPEG files*, 142
- OSI reference model*, 142
- .PNG files*, 142
- QuickTime*, 142

QoS, 20-21

reliable networks

- circuit-switched networks*, 15
- fault tolerance*, 15
- packet-switched networks*, 17, 20
- QoS, 20-21
- scalable networks*, 19
- security*, 21-23
- supporting network architectures*, 15

SAN, 29

scalable networks, 19, 557

security, 560

- AAA network security services*, 568-569
- ACL, 44
- adware*, 43
- antispyware*, 44
- antivirus software*, 44
- attacks*, 562-566
- availability (data)*, 23
- backups*, 567
- confidentiality (data)*, 22
- data interception/theft*, 43
- data loss/manipulation*, 560
- dedicated firewall systems*, 44
- defining*, 21
- denial of service attacks*, 43
- devices*, 572-576
- disruption of service*, 560
- employees and security breaches*, 43
- endpoint security*, 571-572
- firewall filtering*, 44
- firewalls*, 570
- hacker attacks*, 43
- identity theft*, 43, 560
- information theft*, 560
- integrity (data)*, 23
- IPS, 44
- patches*, 567
- physical security*, 561
- RADIUS, 569
- reliable networks*, 21-23
- solutions*, 44
- spyware*, 43
- TACACS+, 569
- threats*, 42-43, 562
- Trojan horses*, 43, 564
- updates*, 567

upgrades, 567*viruses*, 43, 564

VPN, 44

vulnerabilities, 562-564*worms*, 43, 564, 567*zero-day (zero-hour) attacks*, 43

segmenting messages, 124

servers, defining, 24

session layer (OSI reference model), 142

small networks

application layer services, 554*design considerations*, 552-553*growing*, 557-559*infrastructures*, 556*interfaces*, 549*IP addresses*, 550-551*IP telephony*, 557*network applications*, 554*ports*, 549*protocol analysis*, 558-559*protocol requirements*, 559*protocols*, 555*real-time applications*, 556-557*redundancy*, 551-552

RTCP, 557

RTP, 557

scaling, 557*selecting devices*, 548-550*topologies*, 547-548

VoIP, 557

software, defining, 24

submarine networks, 465

telephone networks, 13

television networks, 13

topologies, 27

logical topology diagrams, 28*physical topology diagrams*, 28*small networks*, 547-548

traditional networks, 13

transport layer

choosing protocols, 176*identifying applications*, 172*multiplexing conversations*, 173*OSI reference model*, 170*port numbers*, 172*reliability of*, 174

- role of*, 170
- segmenting/reassembling data*, 172
- separating multiple communications*, 181
- TCP, 171, 175-200, 203
- tracking individual conversations*, 171-172
- UDP, 171, 174-177, 180-187, 201-204
- types of, 28-29
- video communication, 39-40
- VLAN, verifying interface assignments, 94
- VPN, 44
- WAN, 29
 - Internet and*, 30
 - routers and*, 245-246
- WLAN, 29, 474
 - AP, 475
 - NIC adapters, 475
 - standards, 476
- WPAN, 474
- next header field, IPv6 packet headers, 225
- next-hop addressing, 235-236
- nibble boundaries, 401
- NIC (Network Interface Cards)
 - defining, 27
 - NIC adapters, 475
- no login command, 82
- non-time sensitive communication (QoS data classifications), 21
- no shutdown command, configuring LAN interfaces, 253
- no switchport command, routed port Layer 3 switch configurations, 539
- NRZ (Non-Return to Zero), 447
- NS records, 155
- nslookup command and DNS, 157
- NVRAM (Non-Volatile Random Access Memory)
 - file systems, 598
 - routers, 242, 249

O

- octets
 - binary notation, 269-272, 275-277
 - decimal conversion, 271
- online collaboration, 38-39
- open protocol standards, 109
- optical fiber cable

- components of, 466
- copper cable versus, 471-472
- end finish errors, 470
- end gap errors, 470
- misalignment errors, 470
- MMF, 467-468
- network fiber-optic connectors, 468-469
- properties of, 465
- SMF, 467
- testing, 470
- types of, 466-468
- OS (Operating Systems). *See* IOS
- OSI Layer 3. *See* network layer (OSI reference model)
- OSI (Open Systems Interconnection) reference model, 112-115
 - application interfaces, 145
 - application layer, 140
 - data link layer, 411-412
 - frames*, 416-417, 431-440
 - LAN topologies*, 425-431
 - LLC*, 413
 - MAC*, 413-414, 419-431
 - media access*, 415
 - standards*, 418-419
 - WAN topologies*, 422-424
- network layer
 - addressing end devices*, 213
 - de-encapsulation*, 214
 - encapsulation*, 214
 - IP, characteristics of*, 215-218
 - IPv4*, 214-222
 - IPv6*, 214, 222-225
 - PDU*, 217
 - routers*, 214
 - routers, anatomy of*, 240-244
 - routers, bootups*, 247-250
 - routers, configuring initial settings*, 251
 - routers, configuring LAN interfaces*, 252-253
 - routers, connecting to*, 245-246
 - routers, default gateways*, 254-256
 - routers, host routing tables*, 226-232
 - routers, LAN interfaces*, 245-246
 - routers, router routing tables*, 232-240
 - routers, verifying configurations*, 253-254
 - routers, WAN interfaces*, 245-246

- physical layer, 411, 441
 - bandwidth*, 449-450
 - components of*, 445
 - copper cable*, 442, 445
 - fiber-optic cable*, 442
 - frame encoding*, 446-447
 - functions*, 445
 - signaling method*, 447-449
 - standards*, 443-444
 - throughput*, 450
 - wireless media*, 442
- presentation layer, 142
- session layer, 142
- TCP/IP protocol model comparisons to, 116-117
- transport layer
 - choosing protocols*, 176
 - identifying applications*, 172
 - multiplexing conversations*, 173
 - port numbers*, 172
 - reliability of*, 174
 - role of*, 170
 - segmenting/reassembling data*, 172
 - separating multiple communications*, 181
 - TCP, 171, 175-200, 203
 - tracking individual conversations*, 171-172
 - UDP, 171, 174-177, 180-187, 201-204
- OUI (Organizationally Unique Identifiers) and EUI-64, 330
- outgoing interfaces, remote network routes, 236
- out-of-band access, defining, 59
- overhead
 - ARP problems, 514
 - TCP, 189
 - UDP, 201

P

P2P (Peer-to-Peer) networks

- application protocols and, 145-147
- file sharing, 8

packets

- best effort (unreliable) delivery, IP, 215-216
- filtering (firewalls), network security, 570
- fragmentation, 217, 220
- hops, 214
- host packet forwarding decisions, 226

IP packets

- destination data link addresses*, 128
- destination IP addresses*, 127-128, 131
- destination MAC addresses*, 129, 132
- source data link addresses*, 128
- source IP addresses*, 127-128, 131
- source MAC addresses*, 129, 132

IPv4 packets

- end-to-end connectivity*, 222
- headers*, 218-221
- improvements to packet handling*, 222
- Internet routing table expansion*, 221
- IP address depletion*, 221
- limitations of*, 221-222
- NAT, 222
- payloads*, 218

IPv6 packets

- authentication*, 222
- benefits of*, 222
- encapsulation*, 223
- headers*, 224-225
- IP address space*, 222
- NAT, 222
- privacy*, 222
- security*, 222

MTU, 217

- network security, 570
- next-hop addressing, 236
- packet buffers and RAM, 242
- packet-switched networks
 - IP addresses, defining*, 17
 - queues*, 20

- router packet forwarding decisions
 - directly connected routes*, 232-235
 - remote network routes*, 235
 - remote routes*, 232

routing

- host routing tables*, 226-232
- router routing tables*, 232-240

PARC (Palo Alto Research Center), Xerox, Ethernet development, 107

pass phrases, device security, 574

password command, router configuration, 251

passwords

- best practices, 79
- choosing, 80

- device security, 573-574
- enable password command, 80
- enable secret password command, 80
- encryption, 82
- service password-encryption command, 82
- vty, 81
- patches, network security, 567**
- paths, testing via traceroute command, 347-348**
- payloads**
 - IPv4 packets, 218
 - payload length field, IPv6 packet headers, 225
- PC connectivity, testing, 94**
- PCM (Pulse-Code Modulation), 449**
- PDU (Protocol Data Units)**
 - data encapsulation, 125
 - MTU, 217
 - network layer (OSI reference model), 217
 - TCP, 195
 - TCP/UDP segmentation, 187
 - UDP. *See* datagrams and UDP
- peer-to-peer file sharing. *See* P2P (Peer-to-Peer)**
- networks, file sharing**
- performance (networks), monitoring**
 - host commands
 - arp command*, 591-592
 - ipconfig command*, 590
 - show cdp neighbors command*, 592-594
 - show ip interface brief command*, 594-595
 - IOS commands
 - arp command*, 591-592
 - ipconfig command*, 590
 - show cdp neighbors command*, 592-594
 - show ip interface brief command*, 594-595
 - ping command
 - extended ping command*, 580-581
 - IOS ping indicators*, 578-579
 - loopback tests*, 579-580
 - network baselines*, 581-582
 - show commands, 585
 - viewing router settings*, 588-589
 - viewing switch settings*, 589
 - tracert command, 583-584
- personal firewalls, 570**
- person-to-person video, 39-40**
- physical addresses. *See* MAC addresses**
- physical layer (OSI reference model), 411, 441**
 - bandwidth, 449-450
 - components of, 445
 - copper cable, 442, 445, 452
 - coaxial cable*, 453-457
 - STP*, 453-455
 - UTP*, 453-454, 458-464
 - fiber-optic cable, 442
 - frames, encoding, 446-447
 - functions, 445
 - signaling method, 447-449
 - standards, 443-444
 - throughput, 450
 - wireless media, 442
- physical ports, defining, 27**
- physical security (networks), 561**
- physical topologies, 28**
 - MAC, 420
 - point-to-point topologies, 422-423
- ping command, 297**
 - connectivity, testing
 - LAN*, 345
 - local stacks*, 344
 - loopbacks*, 345
 - remote devices*, 346
 - loopback addresses, testing, 93
 - network performance, monitoring
 - extended ping command*, 580-581
 - IOS ping indicators*, 578-579
 - loopback tests*, 579-580
 - network baselines*, 581-582
 - syntax of, 68
 - testing PC-to-switch connectivity, 94
 - verifying
 - IPv6 address configuration*, 336
 - router configuration*, 253
- planning converged networks, 14**
- platforms, networks as**
 - converged networks
 - developing*, 14
 - planning*, 14
 - traditional networks*, 13
 - reliable networks
 - circuit-switched, connection-oriented networks*, 16
 - circuit-switched networks*, 15
 - fault tolerance*, 15
 - packet-switched networks*, 17, 20

- QoS, 20-21
- scalable networks, 19
- security, 21-23
- supporting network architectures, 15
- play (entertainment), Internet's changes to, 9-10
- .PNG (Portal Network Graphics) files, presentation layer, 142
- podcasting, defining, 8
- point-to-point topologies
 - full-duplex communication, 425
 - half-duplex communication, 424
 - logical topologies, 423
 - physical topologies, 422-423
- POP (Post Office Protocol)
 - application layer, 143, 152
 - email and, 152
- ports
 - addressing
 - destination ports, 183
 - dynamic (private) ports, 186
 - IANA port number assignments, 184
 - registered ports, 185-186
 - socket pairs, 184
 - sockets, 184
 - source ports, 183
 - TCP, 183-186
 - TCP/UDP common ports, 186
 - UDP, 183-186
 - well-known ports, 184
 - AUX ports
 - CLI environments, accessing via routers, 245
 - IOS access, 61
 - routers and, 244
 - console ports
 - IOS access, 59-60
 - out-of-band access, 59
 - routers and, 244
 - Ethernet ports, 89
 - LAN switches, 516
 - management ports, router connections, 245
 - physical ports, defining, 27
 - port-based memory buffering, 525
 - port numbers, 172
 - dynamic (private) ports, 186
 - IANA assignments, 184
 - registered ports, 185-186
 - sockets, 184
 - TCP, 182
 - UDP, 182
 - well-known ports, 184
 - private (dynamic) ports and port addressing, 186
 - SFP ports, modular LAN switch configurations, 533-534
 - small networks, 549
 - USB ports and Cisco routers, 602-603
- positional notation, 268
- POST (Power On Self Test)
 - POST messages (HTTP), 151
 - router bootup process, 248
- power cycles, defining, 57
- PPP (Point-to-Point Protocol), PPP frames, 437-438
- Preamble field (Ethernet frames), 496
- prefix length, 279, 318
- presentation layer
 - .GIF files, 142
 - .JPEG files, 142
 - .MPEG files, 142
 - OSI reference model, 142
 - .PNG files, 142
 - QuickTime, 142
- priority queuing, packet-switched networks, 20
- privacy, IPv6 packets, 222
- private clouds (cloud computing), 41
- private (dynamic) ports and port addressing, 186
- private IP addresses, 120
- private IPv4 addresses, 298-299
- privileged EXEC mode
 - defining, 63
 - IOS operation, 63
 - securing access, 80
 - user EXEC mode, moving between, 65-66
- processes
 - defining, 144
 - FTP processes, 161
- proposed standards, RFC creation/validation process, 120
- proprietary protocols, 107
- protocol suites
 - defining, 104
 - IP, 107

OSI reference model, 112
application interfaces, 145
application layer, 140
network layer, 213-256
presentation layer, 142
session layer, 142
TCP/IP protocol model comparisons to, 116-117
transport layer, 170-204

TCP/IP, 106, 114-116
application layer, 141-143, 149-150
communication process, 108-109
development of, 107
OSI reference model comparisons to, 117

protocols

analysis, small networks, 558-559
 application layer protocols, 105, 141
 BOOTP, 143
 client/server model and, 148
 P2P networks and, 145-147
 ARP, MAC addresses, 130
 BOOTP, 143
 connection-oriented protocols, 178
 defining, 103

DHCP
 application layer, 143, 158-160
 DHCPACK messages, 160
 DHCPDISCOVER messages, 159-160
 DHCPNAK messages, 160
 DHCPOFFER messages, 160
 DHCPREQUEST messages, 160

DNS
 application layer, 143, 155-157
 BIND and, 155-156
 message format, 155-156
 nslookup command, 157
 scalability, 157
 server hierarchy, 156-157

EIGRP, 107

Ethernet
 development of, 107
 TCP/IP communication process, 109

file sharing protocols
 FTP, 143, 161-162
 SAMBA, 163
 SMB, 162

HTTP
 application layer, 143, 149-150
 GET messages, 151
 HTML and, 150
 HTTPS and, 151
 POST messages, 151
 PUT messages, 151
 segments, 105
 TCP/IP communication process, 108

HTTPS, 151

IMAP, *application layer*, 143

interaction of, 105-106

IP, 106

IP packets
 defining, 109
 destination data link addresses, 128
 destination IP addresses, 127-128, 131
 destination MAC addresses, 129, 132
 source data link addresses, 128
 source IP addresses, 127-128, 131
 source MAC addresses, 129, 132

network access protocols, 106

network protocols, 105

open standards, 109

POP
 application layer, 143, 152
 email and, 152

proprietary protocols, 107

protocol field (IPv4 packet headers), 219

protocol models, 114-117

reference models, 113-114

requirements, small networks, 559

RFC, 118
 BCP, 121
 creation/validation process, 120-121
 development of, 119
 errors in, 122
 experimental RFC, 122
 historic RFC, 122
 informational RFC, 121
 Internet standards, 121
 private addresses, 120
 RFC 1918, 119
 sample of, 119
 types of, 121-122

SAMBA, 163

SMB, 162

SMTP

application layer, 143, 152-154

email and, 152-154

standards-based protocols, 106

standards organizations

EIA, 112

IAB, 110

IANA, 113

ICANN, 113

IEEE, 111, 112

IETF, 110

IRTF, 110

ISO, 112

ISOC, 110

ITU-T, 113

TIA, 112

stateful protocols, 179

stateless protocols, 181

TCP, 105, 171, 175

applications using TCP, 203

establishing connections, 189, 190, 191

establishing sessions, 178

flow control, 179, 198-200

overhead, 179, 189

PDU, 195

port addressing, 183-186

port numbers, 182

reliability, 178, 188, 195-200

role of, 179

SACK, 198

same-order delivery, 179

segmentation, 187

segments, 175, 180

server processes, 189

TCP/IP communication process, 108

terminating sessions, 194-195

three-way handshakes, 190-193

UDP versus, 177

Telnet, application layer, 143

TFTP, application layer, 143

transport layer protocol, 105

UDP, 171, 174-176

applications using TCP, 203-204

client requests, 202

connectionless sessions, 201

datagrams, 181

features of, 180

flow control, 180

overhead, 201

port addressing, 183-186

port numbers, 182

reassembling datagrams, 201-202

reliability, 201

role of, 181

segmentation, 187

segments, 181

server processes/requests, 202

TCP versus, 177

public clouds (cloud computing), 41

public IPv4 addresses, 299

PUT messages (HTTP), 151

Q

QoS (Quality of Service)

BYOD solutions, 37

communication and

external QoS, 12-13

internal QoS, 12-13

data classifications, 20-21

reliable networks, 20-21

queues (priority) and packet-switched networks, 20

QuickTime, presentation layer, 142

R

RADIUS (Remote Authentication Dial-In User Service), network security network security, 569

radix (positional notation), 268

RAM (Random Access Memory)

ARP caches and, 242

DRAM, 242

IOS and, 57, 242

IP routing tables and, 242

NVRAM, 242, 249

packet buffers and, 242

routers and, 241

running configuration (running-config) files and, 87, 242

randomly generated Interface ID, unicast IPv6 addresses, 331-332

- real-time applications, small networks, 556-557
- reassembling datagrams (UDP), 201-202
- receiving segments, TCP, 196-197
- reconnaissance attacks (security), 565
- recreation, Internet's changes to, 9-10
- reducing window sizes, 200
- redundancy, small networks, 551-552
- reference models
 - layered models, benefits of, 113
 - OSI, 112, 114, 115
 - application interfaces*, 145
 - application layer*, 140
 - network layer*, 213-256
 - presentation layer*, 142
 - session layer*, 142
 - TCP/IP protocol model comparisons to*, 116-117
 - transport layer*, 170-204
- registered ports, port addressing and, 185-186
- reliable networks
 - circuit-switched networks, 15-16
 - fault tolerance, 15
 - packet-switched networks
 - IP addresses, defining*, 17
 - queues*, 20
 - QoS, 20-21
 - scalable networks, 19
 - security, 21-23
 - support network architectures, 15
- reload command, 85
- remote communication, ARP, 508-510
- remote devices, testing connectivity via ping
 - command, 346
- remote hosts, host packet forwarding, 226
- remote Internet connections
 - cable, 33
 - cellular, 33
 - dial-up (telephone), 34
 - DSL, 33
 - satellite, 33
- remote network routes, routing table entries, 235
- remote resources (data delivery), accessing
 - communicating with devices on remote networks, 131-132
 - data link addresses, 132
 - default gateways, 130
 - network addresses, 131
- remote routes, router packet forwarding, 232
- representations (network), 26-28
- resequencing segments, TCP, 195
- restoring IOS configuration files
 - text capture (Tera Term), 600
 - text configurations, 601
 - text files, 600
 - TFTP, 602
- retransmitting TCP segments, 198
- RFC (Request for Comments), 118
 - BCP, 121
 - creation/validation process, 120-121
 - development of, 119
 - EIGRP, 107
 - errors in, 122
 - experimental RFC, 122
 - historic RFC, 122
 - informational RFC, 121
 - Internet standards, 121
 - private addresses, 120
 - RFC 1918, 119
 - sample of, 119
 - types of, 121-122
- RFI (Radio Frequency Interference), 452
- ring topologies, 426, 431
- RIR (Regional Internet Registries), IP address assignments, 304-305
- rollover cable, 462
- ROM (Read Only Memory) and routers, 242
- routers
 - AUX ports, 244
 - backpane, 244
 - bootups
 - bootset files*, 247
 - IOS*, 247-249
 - POST*, 248
 - show version output*, 249-250
 - startup configuration files*, 249
 - TFTP servers*, 249
 - branches, 241
 - Cisco routers and USB ports, 602-603
 - computers, routers as, 240-241
 - configuring
 - initial settings*, 251
 - interface command*, 324
 - LAN interfaces*, 252-253

- static configuration of global unicast addresses*, 324
 - verifying configurations*, 253-254
- connecting to, 245-246
- console ports, 244
- CPU and OS
 - Flash memory*, 243
 - NVRAM, 242
 - RAM, 241
 - ROM, 242
- default gateways, 130, 254-256
- EHWIC slots, 244
- file systems, 596-598
- hops, 214
- host routing tables
 - host packet forwarding decisions*, 226
 - IPv4, 227-230
 - IPv6, 231-232
- inside of, 243
- interfaces, verifying, 594-595
- IOS, 57
 - image files*, 247-249
 - router functions*, 58
- LAN, 244-246
- network layer (OSI reference model), 214
- reloading, 257
- route print command, IPv4 host routing tables, 227
- Route Redirection messages (ICMP), 341
- route sources, remote network routes, 235
- route timestamps, remote network routes, 236
- routed port interfaces, Layer 3 LAN switches, 538
- Router Advertisement messages (NDP), 342
- router routing tables, 240
 - directly connected routing table entries*, 234-235
 - IPv4, 233, 236-239
 - next-hop addressing*, 236
 - remote network routing table entries*, 235
 - router packet forwarding decisions*, 232
- Router Solicitation messages (NDP), 342
- security, 572
- service providers, 241
- settings, viewing, 588-589
- show version command, 75
- startup configuration files, 247-249
- subnet communication, 358-359
- WAN, 241, 245-246

- RTCP (Real-Time Transport Control Protocol), small networks, 557
- RTP (Real-Time Transport Protocol), small networks, 557
- RTT (Round-Trip Time), 347
- running configuration (running-config) files and RAM, 242

S

- SACK (Selective Acknowledgements), TCP segments, 198
- SAMBA protocol, 163
- SAN (Storage Area Networks), 29
- satellite Internet connections, 33-35
- saving configurations, 84-87
- scalability
 - defining, 19
 - DNS, 157
 - networks, 19, 557
- SC (Subscriber Connectors), 468
- SDSL (Symmetric Digital Subscriber Line) Internet connections, 35
- security
 - AAA network security services
 - accounting*, 569
 - authentication*, 568-569
 - authorization*, 569
 - ACL, 44
 - adware, 43
 - antispysware, 44
 - antivirus software, 44
 - ARP problems, 515
 - attacks, 564
 - access attacks*, 565
 - defining*, 562
 - DoS attacks*, 565-566
 - reconnaissance attacks*, 565
 - backups, 567
 - BYOD solutions, 37
 - data interception/theft, 43
 - data loss/manipulation, 560
 - defining, 21
 - denial of service attacks, 43
 - device access, 79, 80
 - devices, 572

- banners*, 575
- best practices*, 574-576
- exec timeouts*, 575-576
- pass phrases*, 574
- passwords*, 573-574
- SSH*, 576
- disruption of service, 560
- employees and security breaches, 43
- encryption, 82
- endpoint security, 571, 572
- firewalls, 44, 570
- hacker attacks, 43
- identity theft, 43, 560
- information security, 22, 560
- IPS, 44
- IPv6 packets, 222
- passwords
 - best practices*, 79
 - choosing*, 80
 - encryption*, 82
 - vty*, 81
- patches, 567
- physical security, 561
- privileged EXEC mode access, 80
- RADIUS, 569
- reliable networks, 21-23
- requirements (data)
 - availability*, 23
 - confidentiality*, 22
 - integrity*, 23
- routers, 572
- security passwords min-length command, device
 - command, 575
- service password-encryption command, 82
- solutions, 44
- spyware, 43
- TACACS+, 569
- threats, 42-43, 562
- Trojan horses, 43, 564
- updates, 567
- upgrades, 567
- user EXEC mode access, 81-82
- viruses, 43, 564
- VPN, 44
- vulnerabilities, 562-564
- wireless media, 473
- worms, 43, 564, 567
- zero-day (zero-hour) attacks, 43
- segments (data), 124**
 - HTTP messages, 105
 - SYN segments, TCP three-way handshakes, 192
 - TCP, 175, 180, 187
 - confirming receipt of segments*, 196-197
 - losing*, 197
 - resequencing segments*, 195
 - retransmitting*, 198
 - transport layer (OSI reference model), 172
 - UDP, 181, 187
- sequence numbers**
 - ISN, TCP three-way handshakes, 191
 - TCP segments, confirming receipt of, 196
- serial WAN interfaces and routers, 246**
- servers**
 - client/server model and application protocols, 148
 - defining, 24
 - DNS servers, 91, 156-157
 - firewalls, 570
 - TFTP servers, router bootups, 249
 - UDP, 202
- services**
 - defining, 24
 - disruption of (network security), 560
 - routers and service providers, 241
 - service password-encryption command, 82
 - device security*, 574
 - router configuration*, 251
 - Service Unreachable messages (ICMP), 341
- session layer, OSI reference model, 142**
- SFD (Start of Frame Delimiter) field, Ethernet frames, 496**
- SFP (small form-factor pluggable) ports, modular LAN switch configurations, 533-534**
- sharing**
 - file sharing protocols
 - FTP*, 161-162
 - SAMBA*, 163
 - SMB*, 162
 - media, 420
 - memory buffering, 525
 - P2P files, 8
- shortcuts (keyboard), 72**
- show cdp neighbors command, 592-594**

show commands, 67, 74

- network performance, monitoring, 585
 - viewing router settings, 588-589*
 - viewing switch settings, 589*
- show file systems command, router file systems, 597
- show interface command, verifying IPv6 address configuration, 334
- show ip arp command, ARP tables, 512
- show ip interface brief command, 94, 253, 594-595
- show ip route command, 233, 253
- show ipv6 interface brief command, verifying IPv6 address configuration, 334
- show ipv6 route command, verifying IPv6 address configuration, 335
- show run command, router configuration, 251
- show running-config command, 85, 87
- show startup-config command, 87
- show version command, 75, 249-250

signal attenuation, 452**signaling method, physical layer (OSI reference model), 447-449****SLAAC (Stateless Address Autoconfiguration), global unicast addresses, 327-328****slash notation, prefix length, 279****small networks**

- application layer services, 554
- design considerations, 552-553
- devices, selecting, 548
 - cost, 549*
 - expandibility, 550*
 - interfaces, 549*
 - operating system features and services, 550*
 - ports, 549*
 - speed, 549*
- growing, 557-559
- infrastructures, 556
- interfaces, 549
- IP addresses, 550-551
- IP telephony, 557
- network applications, 554
- ports, 549
- protocols, 555
 - analysis of, 558-559*
 - requirements, 559*
- real-time applications, 556-557

redundancy, 551-552

RTCP, 557

RTP, 557

scaling, 557

topologies, 547-548

VoIP, 557

SMB (Server Message Blocks), 162

SMF (Single-Mode Fiber), 467

SMTP (Simple Mail Transfer Protocol), 143, 152-154

social media, defining, 8

socket pairs, 184

sockets, 184

software, defining, 24

solicited-node IPv6 multicast addresses, 338-339

Source Address field (Ethernet frames), 497

source data link addresses, IP packets, 128

source IP addresses

IP packets, 127

communicating with devices on remote networks, 131

communicating with devices on the same network, 128

source IP address field

IPv4 packet headers, 220

IPv6 packet headers, 225

source MAC addresses, IP packets

communicating with devices on remote networks, 132

communicating with devices on the same network, 129

source ports and port addressing, 183

SPI (Stateful Packet Inspection), firewalls and network security, 570

spyware, 43

SSH (Secure Shell)

CLI environments, accessing via routers, 245

device security, 576

IOS access, 60

remote access, 576

ST (Straight-Tip) connectors, 468

standards

Internet standards, 121

proposed standards, RFC creation/validation process, 120

- RFC, 118
 - BCP*, 121
 - creation/validation process*, 120-121
 - development of*, 119
 - errors in*, 122
 - experimental RFC*, 122
 - historic RFC*, 122
 - informational RFC*, 121
 - Internet standards*, 121
 - private addresses*, 120
 - RFC 1918*, 119
 - sample of*, 119
 - types of*, 121-122
- standards-based protocols, 106
- standards organizations
 - EIA*, 112
 - IAB*, 110
 - IANA*, 113
 - ICANN*, 113
 - IEEE*, 111-112
 - IETF*, 110
 - IRTF*, 110
 - ISO*, 112
 - ISOC*, 110
 - ITU-T*, 113
 - open protocol standards*, 109
 - TIA*, 112
- star topologies, 425
- startup configuration files and routers, 247-249
- stateful protocols, TCP, 179
- stateless DHCPv6 (Dynamic Host Configuration Protocol version 6), 328
- stateless protocols, UDP, 181
- static addressing
 - defining, 158
 - static IP addresses, assigning to hosts, 290-292
 - static link-local addresses, 333-334
- store-and-forward switching, 523
- STP (Shielded Twisted Pair) cable, 453-455
- subconfiguration modes, 64-66
- submarine networks, 465
- subnetting, 356
 - defining, 358
 - formulas
 - hosts*, 365
 - subnets*, 364
 - host calculation
 - creating 4 subnets*, 366-367
 - creating 8 subnets*, 371
 - creating 100 subnets with a /16 prefix*, 374
 - creating 1000 subnets with a /8 prefix*, 377
 - IPv4 addressing, 278
 - ANDing*, 287-290
 - broadcast addresses*, 283
 - first host addresses*, 284
 - host addresses*, 282-285
 - last host addresses*, 285
 - network addresses*, 281, 289
 - prefix length*, 279
 - IPv4 networks
 - address assignments*, 393-396
 - addressing schemes*, 393-396
 - basic subnetting*, 359-362
 - creating 4 subnets*, 365-367
 - creating 8 subnets*, 368-371
 - creating 100 subnets with a /16 prefix*, 372-374
 - creating 1000 subnets with a /8 prefix*, 375-376
 - determining subnet masks*, 378-384
 - flat network design*, 357
 - GigabitEthernet interfaces*, 361
 - host requirements*, 378-379
 - ip address command*, 363
 - network requirements*, 379-382
 - network segmentation*, 358-359
 - reasons for subnetting*, 357-358
 - subnet communication*, 358-359
 - Subnet ID, global unicast addresses*, 323
 - subnetting formulas*, 364-365
 - VLSM*, 386-393, 397
 - wasted addresses*, 384-385
 - IPv6 networks
 - Interface ID*, 400
 - subnet allocation*, 399-400
 - Subnet ID*, 397-398
 - LAN interfaces, configuring, 253
 - nibble boundaries, 401
 - subnet masks and IPv4 networks
 - host requirements*, 378-379
 - network requirements*, 379-382
 - VLSM*, 386-393, 397
 - wasted addresses*, 384-385

SVI (switch virtual interfaces), Layer 3 LAN**switches, 537****switch file systems, 598****switches, 76**

Catalyst 2960 switches, 529, 530

Catalyst 3560 switches, 530

Catalyst 3750 switches, 530

Catalyst 4500 switches, 531, 532

Catalyst 4900 switches, 532

Catalyst 6500 switches, 532

Catalyst Express 500 switches, 528

Cisco Catalyst switches, 61

default gateways, configuring, 255-256

interfaces, verifying, 94, 595

IOS, 57-58

LAN switches*Auto-MDIX, 522**cut-through switching, 524**duplex settings, 521-522**fast-forward switching, 524**fixed configurations, 526-530**fragment-free switching, 524**frame forwarding, 523-525**full-duplex communication, 521-522**half-duplex communication, 521**Layer 2 LAN switches, 535**Layer 3 LAN switches, 535-537**MAC address tables, 517-520**mdix auto interface command, 522**memory buffering, 525**modular configurations, 526-527, 531-534**ports, 516**store-and-forward switching, 523*

management addresses, configuring, 95

PC-to-switch connectivity, testing, 94

reloading, 257

settings, viewing, 589

show version command, 75

virtual interfaces, configuring, 90-91

synchronous data signals, 448**SYN control flags, TCP three-way handshakes, 191-193****SYN segments, TCP three-way handshakes, 192****syntax**

commands, 68, 71

error messages, 71

Syntax Checker, global unicast addresses, 326

T**Tab key and IOS, 72****TACACS+ network security, 569****TCP (Transmission Control Protocol), 105, 171, 175**

applications using TCP, 203

connections, establishing, 189-191

flow control, 179

*avoiding congestion, 200**window size, 198-199*

overhead, 179, 189

PDU, 195

ports

*addressing, 183-186**numbers, 182*

reliability, 178, 188

*acknowledgements, 196-199**confirming receipt of segments, 196-197**flow control, 198-200**losing segments, 197**ordered delivery, 195-196**resequencing segments, 195**retransmitting segments, 198**window size, 197-200*

role of, 179

SACK, 198

same-order delivery, 179

segments, 175, 180, 187

*confirming receipt of segments, 196-197**losing, 197**retransmitting, 198*

server processes, 189

sessions

*establishing, 178**terminating, 194-195*

TCP/IP communication process, 108

three-way handshakes, 190

*ACK control flags, 192-193**SYN control flags, 191-193**SYN segments, 192*

UDP versus, 177

TCP/IP (Transmission Control Protocol/Internet Protocol) protocol suite, 106, 114-116

application layer, 141

*BOOTP, 143**DHCP, 143, 158-160**DNS, 143, 155-157**FTP, 143**HTTP, 143, 149-150**IMAP, 143**POP, 143**SMTP, 143**Telnet protocol, 143**TFTP, 143*

communication process, 108-109

development of, 107

OSI reference model comparisons to, 117

telecommunications rooms, LAN cabling, 463

telephone (dial-up) Internet connections, 34

telephone networks, 13

TelePresence, collaboration architectures, 46

television networks, 13

Telnet

CLI environments, accessing via routers, 245

defining, 60

IOS access, 60

Telnet protocol, application layer, 143

terminal emulation programs, IOS access, 61**testing**

connectivity via ping command, 344-346

copper cable, 464

fiber optic cable, 470

loopbacks, 579-580

paths, traceroute command, 347-348

TEST-NET addresses, 301

text

captures

*configuration backups, 87**IOS configuration files, restoring
(Tera Term), 600*

configurations, restoring, 87-88, 600-601

text files, restoring IOS configuration files, 600

texting, 7. See also IM**TFTP (Trivial File Transfer Protocol)**

application layer, 143

IOS configuration files

*backups, 601-602**restoring, 602*

servers, router bootups, 249

theft

data interception/theft, 43

identity theft, 43

threats (security), defining, 562**three-way handshakes, TCP, 190**

ACK control flags, 192, 193

SYN control flags, 191, 192, 193

SYN segments, 192

throughput, physical layer (OSI reference model), 450**TIA (Telecommunications Industry Association), 112****Time Exceeded messages (ICMP), 341****time sensitive communication (QoS data
classifications), 21****timestamps (route), remote network routes, 236****token passing, 431****topologies**

bus topologies, 426

diagrams, 28

extended star (hybrid) topologies, 426

hub and spoke topologies, 422

LAN topologies

*bus topologies, 426**connection-based access, 427**controlled access, 427-429**extended star (hybrid) topologies, 426**multi-access topologies, 429**ring topologies, 426, 431**star topologies, 425*

logical topologies

*diagrams, 28**MAC, 420**point-to-point topologies, 423*

mesh topologies, 422

multi-access topologies, 429

physical topologies

*diagrams, 28**MAC, 420**point-to-point topologies, 422-423*

point-to-point topologies

*full-duplex communication, 425**half-duplex communication, 424*

- logical topologies*, 423
 - physical topologies*, 422-423
 - ring topologies, 426, 431
 - small networks, 547-548
 - star topologies, 425
 - WAN topologies
 - hub and spoke topologies*, 422
 - mesh topologies*, 422
 - point-to-point topologies*, 422-425
 - ToS (Type of Service) field. *See* DS (Differentiated Services) field (IPv4 packet headers)
 - total internal reflection, 466
 - total length field (IPv4 packet headers), 220
 - traceroute command
 - network performance, monitoring, 583-584
 - paths, testing
 - IPv4 TTL fields*, 347-348
 - IPv6 hop limits*, 347-348
 - RTT*, 347
 - syntax of, 68
 - TTL fields, 219
 - traditional networks, 13
 - traffic class field, IPv6 packet headers, 224
 - trailers (Layer 2 frames), 416, 435
 - translation (NAT64), 310
 - transport input ssh command, SSH and remote access, 576
 - transport layer
 - identifying applications, 172
 - individual conversations, tracking, 171-172
 - multiple communications, separating, 181
 - multiplexing conversations, 173
 - OSI reference model, 170
 - port numbers, 172
 - protocols, choosing, 176
 - reliability of, 174
 - role of, 170
 - segmenting/reassembling data, 172
 - TCP, 171, 175
 - applications using TCP*, 203
 - establishing connections*, 189-191
 - establishing sessions*, 178
 - flow control*, 179, 198-200
 - overhead*, 179, 189
 - PDU*, 195
 - port numbers*, 182
 - port port addressing*, 183-186
 - reliability*, 178, 188, 195-200
 - role of*, 179
 - SACK*, 198
 - same-order delivery*, 179
 - segmentation*, 187
 - segments*, 175, 180
 - server processes*, 189
 - terminating sessions*, 194-195
 - three-way handshakes*, 190-193
 - UDP versus*, 177
 - transport layer protocol, 105
 - UDP, 171, 174-176
 - applications using TCP*, 203-204
 - client requests*, 202
 - connectionless sessions*, 201
 - datagrams*, 181
 - features of*, 180
 - flow control*, 180
 - overhead*, 201
 - port addressing*, 183-186
 - port numbers*, 182
 - reassembling datagrams*, 201-202
 - reliability*, 201
 - role of*, 181
 - segmentation*, 187
 - segments*, 181
 - server processes/requests*, 202
 - TCP versus*, 177
 - Trojan horses, 43, 564
 - TTL (Time to Live) field (IPv4 packet headers), 219, 347-348
 - tunneling, 309
-
- ## U
- UCLA, RFC development, 119
 - UDP (User Datagram Protocol), 171, 174-176
 - applications using TCP, 203-204
 - clients
 - processes*, 202
 - requests*, 202
 - connectionless sessions, 201
 - datagrams, 181, 201-202
 - features of, 180
 - flow control, 180

overhead, 201
 port addressing, 183-186
 port numbers, 182
 reliability, 201
 role of, 181
 segmentation, 187
 segments, 181
 servers
 processes, 202
 requests, 202
 TCP versus, 177
undesirable communication (QoS data classifications), 21
undoing, command effects, 79
unicast IPv4 addresses, 293-294
 embedded IPv4 addresses, 320
unicast IPv6 addresses, 317-318
 embedded IPv4 addresses, 320
 EUI-64, 330-331
 global unicast addresses, 319, 322, 332
 DHCPv6, 328-330
 dynamic configuration, 327-330
 global routing prefixes, 323
 host configuration, 325
 Interface ID, 323, 330
 reading, 324
 router configuration, 324
 SLAAC, 327-328
 static configuration, 324-325
 Subnet ID, 323
 link-local addresses, 320-321
 dynamic link-local addresses, 332-333
 static link-local addresses, 333-334
 loopbacks, 320
 randomly generated Interface ID, 331-332
 unique local addresses, 320
 unspecified addresses, 320
unicast MAC addresses, 500
unified communications, collaboration architectures, 47
unique local addresses, IPv6 addressing, 320
unreliable (best effort) delivery, IP, 215-216
unspecified addresses, IPv6 addressing, 320
updates, network security, 567
Up/Down arrows and IOS, 73
upgrades, network security, 567

URL filtering (firewalls), network security, 570
USB (Universal Serial Bus)
 USB flash drives, IOS configuration files
 backups, 603
 restoring, 605
 USB ports and Cisco routers, 602-603
user EXEC mode
 defining, 63
 IOS operation, 63
 privileged EXEC mode, moving between, 65-66
 securing access, 81-82
username secret command, SSH and remote access, 576
UTP (unshielded twisted pair) cable, 453-454
 connectors, 460-461
 Ethernet crossover cable, 461
 Ethernet straight through cable, 461
 LAN cabling, 462-463
 properties of, 458-459
 rollover cable, 462
 standards, 459-460
 testing, 464
 types of, 461

V

verifying
 connectivity
 address resolution, 343
 DAD, 343
 ICMP, 340-341
 NDP, 342-343
 testing end-to-end connectivity, 94
 testing interface assignments, 94
 testing loopback addresses, 93
 testing PC-to-switch connectivity, 94
 dynamic IPv4 addresses, 293
 IPv6 address configuration, 334-337
 router configurations, 253
version field
 IPv4 packet headers, 219
 IPv6 packet headers, 224
video communication, 39-40
viewing network traffic, 133
virtual circuits, 423
virtual interfaces (switches), configuring, 89-91

viruses, 43-44, 564

VLAN (Virtual Local-Area Network) interfaces,
verifying assignments, 94

VLSM (Variable Length Subnet Masks),
386-393, 397

VoIP (Voice over Internet Protocol), small
networks, 557

VPN (Virtual Private Networks), 44

vtty

login local command, 576

SSH and remote access, 576

transport input ssh command, 576

vtty password, 81

vulnerabilities (security), 562-564

W

WAN (Wide-Area Networks), 29

frames, 435-436

hub and spoke topologies, 422

Internet and, 30

mesh topologies, 422

point-to-point topologies

full-duplex communication, 425

half-duplex communication, 424

logical topologies, 423

physical topologies, 422-423

routers and, 241, 245-246

serial WAN interfaces and routers, 246

weblogs (blogs), 8

Wikipedia, 8

wikis, defining, 8

WiMAX (Worldwide Interoperability for Microwave
Access), 474

window size

dynamic window sizes, 200

reducing, 200

TCP flow control, 198-200

TCP reliability, 197-200

Windows Calculator, network addresses, 289

wireless devices, coaxial cable, 456

Wireless frames (802.11), 438-440

wireless media

coverage areas, 473

interference, 473

physical layer (OSI reference model), 442

properties of, 472

security, 473

types of, 473

WiMAX, 474

WLAN, 29, 474

AP, 475

NIC adapters, 475

standards, 476

work areas and LAN cabling, 462

worms, 43, 564, 567

WPAN (Wireless Personal Area Networks), 474

X - Y - Z

Xerox, Ethernet development, 107

zero-day (zero-hour) attacks, 43