Introduction to Networks v5.1

Companion Guide

Cisco | Networking Academy®
Mind Wide Open™

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

Introduction to Networks

Companion Guide v5.1

Cisco Networking Academy

Cisco Press
800 East 96th Street
Indianapolis, Indiana 46240 USA

Introduction to Networks Companion Guide v5.1

Cisco Networking Academy

Copyright© 2016 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 June 2016

Library of Congress Control Number: 2016935525

ISBN-13: 978-1-58713-357-2

ISBN-10: 1-58713-357-1

Warning and Disclaimer

This book is designed to provide information about the Cisco Networking Academy Introduction to Networks 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.

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.

Publisher
Mark Taub

Business Operation Manager, Cisco Press
Jan Cornelssen

Executive Editor
Mary Beth Ray

Managing Editor
Sandra Schroeder

Development Editor
Ellie C. Bru

Project Editor
Mandie Frank

Copy Editor
Celia McCoy

Technical Editor
Bob Vachon

Editorial Assistant
Vanessa Evans

Designer
Chuti Prasertsith

Composition
codeMantra

Indexer
Cheryl Lenser

Proofreader
Jaikumar

Trademark Acknowledgements

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.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.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

Rick Graziani teaches computer science and computer networking courses at Cabrillo College in Aptos, California. Prior to teaching Rick worked in the information technology field for Santa Cruz Operation, Tandem Computers, Lockheed Missiles and Space Corporation, and served in the U.S. Coast Guard. He holds an M.A. in Computer Science and Systems Theory from California State University Monterey Bay. Rick also works as a curriculum developer for the Cisco Networking Academy Curriculum Engineering team. When Rick is not working, he is most likely surfing at one of his favorite Santa Cruz surf breaks.

Allan Johnson entered the academic world in 1999 after 10 years as a business owner/operator to dedicate his efforts to his passion for teaching. He holds both an MBA and an M.Ed. in Occupational Training and Development. He taught CCNA courses at the high school level for seven years and has taught both CCNA and CCNP courses at Del Mar College in Corpus Christi, Texas. In 2003, Allan began to commit much of his time and energy to the CCNA Instructional Support Team, providing services to Networking Academy instructors worldwide and creating training materials. He now works full time for Cisco Networking Academy as a Curriculum Developer.

Contents at a Glance

Introduction xxiv

Chapter 1 Explore the Network 1

Chapter 2 Configure a Network Operating System 53

Chapter 3 Network Protocols and Communications 91

Chapter 4 Network Access 141

Chapter 5 Ethernet 209

Chapter 6 Network Layer 273

Chapter 7 IP Addressing 325

Chapter 8 Subnetting IP Networks 403

Chapter 9 Transport Layer 455

Chapter 10 Application Layer 501

Chapter 11 Build a Small Network 533

Appendix A 613

Glossary 627

Index 645

Contents

Introduction xxiv

Chapter 1 Explore the Network 1

Objectives 1

Key Terms 1

Introduction (1.0.1.1) 3

Globally Connected (1.1) 4

Networking Today (1.1.1) 4

Networks in Our Daily Lives (1.1.1.1) 4
Technology Then and Now (1.1.1.2) 4
No Boundaries (1.1.1.3) 5
Networks Support the Way We Learn (1.1.1.4) 5
Networks Support the Way We Communicate (1.1.1.5) 5
Networks Support the Way We Work (1.1.1.6) 6
Networks Support the Way We Play (1.1.1.7) 7

Providing Resources in a Network (1.1.2) 7

Networks of Many Sizes (1.1.2.1) 8
Clients and Servers (1.1.2.2) 9
Peer-to-Peer (1.1.2.3) 10

LANs, WANs, and the Internet (1.2) 11

Network Components (1.2.1) 11

Overview of Network Components (1.2.1.1) 12
End Devices (1.2.1.2) 13
Intermediary Network Devices (1.2.1.3) 14
Network Media (1.2.1.4) 15
Network Representations (1.2.1.5) 17
Topology Diagrams (1.2.1.6) 19

LANs and WANs (1.2.2) 20

Types of Networks (1.2.2.1) 20
Local Area Networks (1.2.2.2) 22
Wide Area Networks (1.2.2.3) 22

The Internet, Intranets, and Extranets (1.2.3) 23

The Internet (1.2.3.1) 23
Intranets and Extranets (1.2.3.2) 24

Internet Connections (1.2.4) 25

Internet Access Technologies (1.2.4.1) 26
Home and Small Office Internet Connections (1.2.4.2) 26
Businesses Internet Connections (1.2.4.3) 27

The Network as a Platform (1.3) 28

Converged Networks (1.3.1) 28

Traditional Separate Networks (1.3.1.1) 29

The Converging Network (1.3.1.2) 29

Reliable Network (1.3.2) 30

Network Architecture (1.3.2.1) 30

Fault Tolerance (1.3.2.2) 31

Scalability (1.3.2.3) 32

Quality of Service (1.3.2.4) 32

Security (1.3.2.5) 33

The Changing Network Environment (1.4) 35

Network Trends (1.4.1) 35

New Trends (1.4.1.1) 35

Bring Your Own Device (1.4.1.2) 35

Online Collaboration (1.4.1.3) 36

Video Communication (1.4.1.4) 37

Cloud Computing (1.4.1.5) 37

Networking Technologies for the Home (1.4.2) 39

Technology Trends in the Home (1.4.2.1) 39

Powerline Networking (1.4.2.2) 40

Wireless Broadband (1.4.2.3) 41

Network Security (1.4.3) 42

Security Threats (1.4.3.1) 42

Security Solutions (1.4.3.2) 43

Network Architecture (1.4.4) 44

Cisco Network Architecture (1.4.4.1) 44

CCNA (1.4.4.2) 45

Summary (1.5) 47

Warriors of the Net (1.5.1.2) 47

Conclusion (1.5.1.3) 47

Practice 48

Class Activities 48

Labs 49

Packet Tracer Activities 49

Check Your Understanding Questions 49

Chapter 2 Configure a Network Operating System 53

Objectives 53

Key Terms 53

Introduction (2.0.1.1) 54

IOS Bootcamp (2.1) 54

Cisco IOS (2.1.1) 55
Operating Systems (2.1.1.1) 55
Purpose of OS (2.1.1.2) 57
Cisco IOS Access (2.1.2) 58
Access Methods (2.1.2.1) 58
Terminal Emulation Programs (2.1.2.2) 59
Navigate the IOS (2.1.3) 61
Cisco IOS Modes of Operation (2.1.3.1) 61
Primary Command Modes (2.1.3.2) 61
Configuration Command Modes (2.1.3.3) 62
Navigate Between IOS Modes (2.1.3.4) 62
The Command Structure (2.1.4) 64
Basic IOS Command Structure (2.1.4.1) 64
IOS Command Syntax (2.1.4.2) 64
IOS Help Features (2.1.4.3) 65
Hotkeys and Shortcuts (2.1.4.4) 66

Basic Device Configuration (2.2) 68

Hostnames (2.2.1) 68
Device Names (2.2.1.1) 68
Configure Hostnames (2.2.1.2) 69
Limit Access to Device Configurations (2.2.2) 70
Secure Device Access (2.2.2.1) 70
Configure Passwords (2.2.2.2) 71
Encrypt Passwords (2.2.2.3) 72
Banner Messages (2.2.2.4) 72
Save Configurations (2.2.3) 72
Save the Running Configuration File (2.2.3.1) 73
Alter the Running Configuration (2.2.3.2) 74
Capture Configuration to a Text File (2.2.3.3) 74

Address Schemes (2.3) 78

Ports and Addresses (2.3.1) 78
IP Addresses (2.3.1.1) 78
Interfaces and Ports (2.3.1.2) 79
Configure IP Addressing (2.3.2) 81
Manual IP Address Configuration for End Devices (2.3.2.1) 81
Automatic IP Address Configuration for End Devices (2.3.2.2) 83
Switch Virtual Interface Configuration (2.3.2.3) 85

Verifying Connectivity (2.3.3) 85

Interface Addressing Verification (2.3.3.1) 85
End-to-End Connectivity Test (2.3.3.2) 86

Summary (2.4) 87

Practice 88

Class Activities 88

Labs 88

Packet Tracer Activities 88

Check Your Understanding Questions 89

Chapter 3 Network Protocols and Communications 91

Objectives 91

Key Terms 91

Introduction (3.0) 92

Rules of Communication (3.1) 92

The Rules (3.1.1) 93

Communication Fundamentals (3.1.1.1) 93
Rule Establishment (3.1.1.2) 94
Message Encoding (3.1.1.3) 94
Message Formatting and Encapsulation (3.1.1.4) 96
Message Size (3.1.1.5) 97
Message Timing (3.1.1.6) 98
Message Delivery Options (3.1.1.7) 98

Network Protocols and Standards (3.2) 100

Protocols (3.2.1) 100

Rules that Govern Communications (3.2.1.1) 100
Network Protocols (3.2.1.2) 101
Protocol Interaction (3.2.1.3) 103

Protocol Suites (3.2.2) 105

Protocol Suites and Industry Standards (3.2.2.1) 105
Development of TCP/IP (3.2.2.2) 106
TCP/IP Protocol Suite (3.2.2.3) 106
TCP/IP Communication Process (3.2.2.4) 109

Standard Organizations (3.2.3) 114

Open Standards (3.2.3.1) 114
Internet Standards (3.2.3.2) 115
Electronics and Communications Standard Organizations (3.2.3.3) 116

Reference Models (3.2.4) 118

The Benefits of Using a Layered Model (3.2.4.1) 118
The OSI Reference Model (3.2.4.2) 120
The TCP/IP Protocol Model (3.2.4.3) 120
OSI Model and TCP/IP Model Comparison (3.2.4.4) 121

Data Transfer in the Network (3.3) 123

Data Encapsulation (3.3.1) 123

Message Segmentation (3.3.1.1) 123
Protocol Data Units (3.3.1.2) 125
Encapsulation Example (3.3.1.3) 126
De-encapsulation (3.3.1.4) 126

Data Access (3.3.2) 127

Network Addresses (3.3.2.1) 127
Data Link Addresses (3.3.2.2) 128
Devices on the Same Network (3.3.2.3) 130
Devices on a Remote Network (3.3.2.4) 133

Summary (3.4) 135

Practice 136

Class Activities 136

Labs 136

Packet Tracer Activities 136

Check Your Understanding Questions 137

Chapter 4 Network Access 141

Objectives 141

Key Terms 141

Introduction (4.0) 143

Physical Layer Protocols (4.1) 143

Physical Layer Connection (4.1.1) 143

Types of Connections (4.1.1.1) 144
Network Interface Cards (4.1.1.2) 145

Purpose of the Physical Layer (4.1.2) 146

The Physical Layer (4.1.2.1) 147
Physical Layer Media (4.1.2.2) 148
Physical Layer Standards (4.1.2.3) 148

Physical Layer Characteristics (4.1.3) 150

Functions (4.1.3.1) 150
Bandwidth (4.1.3.2) 152
Throughput (4.1.3.3) 153
Types of Physical Media (4.1.3.4) 154

Network Media (4.2) 155

Copper Cabling (4.2.1) 155

Characteristics of Copper Cabling (4.2.1.1) 155
Copper Media (4.2.1.2) 157
Unshielded Twisted-Pair Cable (4.2.1.3) 158
Shielded Twisted-Pair Cable (4.2.1.4) 159

Coaxial Cable (4.2.1.5) *160*
Copper Media Safety (4.2.1.6) *161*
UTP Cabling (4.2.2) 163
Properties of UTP Cabling (4.2.2.1) *163*
UTP Cabling Standards (4.2.2.2) *164*
UTP Connectors (4.2.2.3) *165*
Types of UTP Cable (4.2.2.4) *166*
Testing UTP Cables (4.2.2.5) *167*
Fiber-Optic Cabling (4.2.3) 168
Properties of Fiber-Optic Cabling (4.2.3.1) *168*
Fiber Media Cable Design (4.2.3.2) *170*
Types of Fiber Media (4.2.3.3) *171*
Fiber-Optic Connectors (4.2.3.4) *172*
Testing Fiber Cables (4.2.3.5) *174*
Fiber versus Copper (4.2.3.6) *175*
Wireless Media (4.2.4) 176
Properties of Wireless Media (4.2.4.1) *176*
Types of Wireless Media (4.2.4.2) *177*
Wireless LAN (4.2.4.3) *177*

Data Link Layer Protocols (4.3) 179

Purpose of the Data Link Layer (4.3.1) 179
The Data Link Layer (4.3.1.1) *179*
Data Link Sublayers (4.3.1.2) *181*
Media Access Control (4.3.1.3) *182*
Providing Access to Media (4.3.1.4) *182*
Data Link Layer Standards (4.3.1.5) *184*

Media Access Control (4.4) 185

Topologies (4.4.1) 185
Controlling Access to the Media (4.4.1.1) *185*
Physical and Logical Topologies (4.4.1.2) *186*
WAN Topologies (4.4.2) 187
Common Physical WAN Topologies (4.4.2.1) *187*
Physical Point-to-Point Topology (4.4.2.2) *188*
Logical Point-to-Point Topology (4.4.2.3) *189*
LAN Topologies (4.4.3) 190
Physical LAN Topologies (4.4.3.1) *190*
Half and Full Duplex (4.4.3.2) *191*
Media Access Control Methods (4.4.3.3) *193*
Contention-Based Access – CSMA/CD (4.4.3.4) *194*
Contention-Based Access – CSMA/CA (4.4.3.5) *196*
Data Link Frame (4.4.4) 196
The Frame (4.4.4.1) *197*
Frame Fields (4.4.4.2) *198*

Layer 2 Address (4.4.4.4) 199
LAN and WAN Frames (4.4.4.5) 201

Summary (4.5) 203

Practice 204

Class Activities 204

Labs 204

Packet Tracer Activities 205

Check Your Understanding Questions 205

Chapter 5 Ethernet 209

Objectives 209

Key Terms 209

Introduction (5.0) 210

Ethernet Protocol (5.1) 211

Ethernet Frame (5.1.1) 211

Ethernet Encapsulation (5.1.1.1) 211
MAC Sublayer (5.1.1.2) 213
Ethernet Evolution (5.1.1.3) 214
Ethernet Frame Fields (5.1.1.4) 215

Ethernet MAC Addresses (5.1.2) 216

MAC Address and Hexadecimal (5.1.2.1) 216
MAC Address: Ethernet Identity (5.1.2.2) 219
Frame Processing (5.1.2.3) 220
MAC Address Representations (5.1.2.4) 221
Unicast MAC Address (5.1.2.5) 222
Broadcast MAC Address (5.1.2.6) 223
Multicast MAC Address (5.1.2.7) 224

LAN Switches (5.2) 226

The MAC Address Table (5.2.1) 226

Switch Fundamentals (5.2.1.1) 226
Learning MAC Addresses (5.2.1.2) 227
Filtering Frames (5.2.1.3) 229
MAC Address Tables on Connected Switches (5.2.1.4) 231
Sending a Frame to the Default Gateway (5.2.1.5) 236

Switch Forwarding Methods (5.2.2) 240

Frame Forwarding Methods on Cisco Switches (5.2.2.1) 241
Cut-Through Switching (5.2.2.2) 242
Memory Buffering on Switches (5.2.2.3) 243

Switch Port Settings (5.2.3) 244

Duplex and Speed Settings (5.2.3.1) 244
Auto-MDIX (5.2.3.2) 246

Address Resolution Protocol (5.3) 247

MAC and IP (5.3.1) 247
Destination on Same Network (5.3.1.1) 247
Destination Remote Network (5.3.1.2) 248

ARP (5.3.2) 250
Introduction to ARP (5.3.2.1) 250
ARP Functions (5.3.2.2) 251
ARP Request (5.3.2.3) 252
ARP Reply (5.3.2.4) 256
ARP Role in Remote Communication (5.3.2.5) 259
Removing Entries from an ARP Table (5.3.2.6) 263
ARP Tables (5.3.2.7) 263

ARP Issues (5.3.3) 264
ARP Broadcasts (5.3.3.1) 264
ARP Spoofing (5.3.3.2) 265

Summary (5.4) 266

Practice 267

Class Activities 267

Labs 267

Packet Tracer Activities 267

Check Your Understanding Questions 268

Chapter 6 Network Layer 273

Objectives 273

Key Terms 273

Introduction (6.0) 274

Network Layer Protocols (6.1) 275

Network Layer in Communications (6.1.1) 275
The Network Layer (6.1.1.1) 275
Network Layer Protocols (6.1.1.2) 276

Characteristics of the IP Protocol (6.1.2) 277
Encapsulating IP (6.1.2.1) 277
Characteristics of IP (6.1.2.2) 277
IP – Connectionless (6.1.2.3) 278
IP – Best Effort Delivery (6.1.2.4) 279
IP – Media Independent (6.1.2.5) 280

IPv4 Packet (6.1.3) 281
IPv4 Packet Header (6.1.3.1) 281

IPv6 Packet (6.1.4) 283
Limitations of IPv4 (6.1.4.1) 283
Introducing IPv6 (6.1.4.2) 283
Encapsulating IPv6 (6.1.4.3) 284
IPv6 Packet Header (6.1.4.4) 286

Routing (6.2) 287

How a Host Routes (6.2.1) 287
Host Forwarding Decision (6.2.1.1) 288
Default Gateway (6.2.1.2) 289
Using the Default Gateway (6.2.1.3) 289
Host Routing Tables (6.2.1.4) 290
Router Routing Tables (6.2.2) 291
Router Packet Forwarding Decision (6.2.2.1) 291
IPv4 Router Routing Table (6.2.2.2) 292
Directly Connected Routing Table Entries (6.2.2.4) 293
Remote Network Routing Table Entries (6.2.2.5) 294
Next-Hop Address (6.2.2.6) 295

Routers (6.3) 296

Anatomy of a Router (6.3.1) 296
A Router is a Computer (6.3.1.1) 296
Router CPU and OS (6.3.1.2) 297
Router Memory (6.3.1.3) 297
Inside a Router (6.3.1.4) 299
Connect to a Router (6.3.1.5) 300
LAN and WAN Interfaces (6.3.1.6) 301
Router Boot-up (6.3.2) 303
Bootset Files (6.3.2.1) 303
Router Bootup Process (6.3.2.2) 304
Show Version Output (6.3.2.4) 306

Configure a Cisco Router (6.4) 308

Configure Initial Settings (6.4.1) 308
Basic Switch Configuration Steps (6.4.1.1) 308
Basic Router Configuration Steps (6.4.1.2) 310
Configure Interfaces (6.4.2) 312
Configure Router Interfaces (6.4.2.1) 312
Verify Interface Configuration (6.4.2.2) 313
Configure the Default Gateway (6.4.3) 314
Default Gateway for a Host (6.4.3.1) 315
Default Gateway for a Switch (6.4.3.2) 316

Summary (6.5) 319

Practice 320

Class Activities 321
Labs 321
Packet Tracer Activities 321

Check Your Understanding Questions 321

Chapter 7 IP Addressing 325

Objectives 325

Key Terms 325

Introduction (7.0) 327

IPv4 Network Addresses (7.1) 327

Binary and Decimal Conversion (7.1.1) 327
IPv4 Addresses (7.1.1.1) 328
Positional Notation (7.1.1.3) 330
Binary to Decimal Conversion (7.1.1.4) 331
Decimal to Binary Conversion (7.1.1.6) 334
Decimal to Binary Conversion Examples (7.1.1.7) 336
IPv4 Address Structure (7.1.2) 338
Network and Host Portions (7.1.2.1) 338
The Subnet Mask (7.1.2.2) 338
Logical AND (7.1.2.3) 340
The Prefix Length (7.1.2.5) 341
Network, Host, and Broadcast Addresses (7.1.2.6) 342
IPv4 Unicast, Broadcast, and Multicast (7.1.3) 345
Static IPv4 Address Assignment to a Host (7.1.3.1) 345
Dynamic IPv4 Address Assignment to a Host (7.1.3.2) 345
IPv4 Communication (7.1.3.3) 346
Unicast Transmission (7.1.3.4) 347
Broadcast Transmission (7.1.3.5) 348
Multicast Transmission (7.1.3.6) 349
Types of IPv4 Addresses (7.1.4) 350
Public and Private IPv4 Addresses (7.1.4.1) 350
Special User IPv4 Addresses (7.1.4.3) 352
Legacy Classful Addressing (7.1.4.4) 353
Classless Addressing (7.1.4.6) 355
Assignment of IP Addresses (7.1.4.7) 356

IPv6 Network Addresses (7.2) 357

IPv4 Issues (7.2.1) 357
The Need for IPv6 (7.2.1.1) 357
IPv4 and IPv6 Coexistence (7.2.1.2) 358
IPv6 Addressing (7.2.2) 360
IPv6 Address Representation (7.2.2.1) 360
Rule 1 – Omit Leading 0s (7.2.2.2) 362
Rule 2 – Omit All 0 Segments (7.2.2.3) 362

Types of IPv6 Addresses (7.2.3) 364
IPv6 Address Types (7.2.3.1) 364
IPv6 Prefix Length (7.2.3.2) 365
IPv6 Unicast Addresses (7.2.3.3) 365
IPv6 Link-Local Unicast Addresses (7.2.3.4) 367
IPv6 Unicast Addresses (7.2.4) 369
Structure of an IPv6 Global Unicast Address (7.2.4.1) 369
Static Configuration of a Global Unicast Address (7.2.4.2) 371
Dynamic Configuration – SLAAC (7.2.4.3) 374
Dynamic Configuration – DHCPv6 (7.2.4.4) 376
EUI-64 Process and Randomly Generated (7.2.4.5) 377
Dynamic Link-Local Addresses (7.2.4.6) 380
Static Link-Local Addresses (7.2.4.7) 381
Verifying IPv6 Address Configuration (7.2.4.8) 382
IPv6 Multicast Addresses (7.2.5) 385
Assigned IPv6 Multicast Addresses (7.2.5.1) 385
Solicited-Node IPv6 Multicast Addresses (7.2.5.2) 387

Connectivity Verification (7.3) 388
ICMP (7.3.1) 388
ICMPv4 and ICMPv6 (7.3.1.1) 388
ICMPv6 Router Solicitation and Router Advertisement Messages (7.3.1.2) 389
Testing and Verification (7.3.2) 392
Ping – Testing the Local Stack (7.3.2.1) 392
Ping – Testing Connectivity to the Local LAN (7.3.2.2) 394
Ping – Testing Connectivity to Remote (7.3.2.3) 395
Traceroute – Testing the Path (7.3.2.4) 395

Summary (7.4) 398

Practice 399
Class Activities 399
Labs 400
Packet Tracer Activities 400

Check Your Understanding Questions 400

Chapter 8 Subnetting IP Networks 403

Objectives 403

Key Terms 403

Introduction (8.0) 404

Subnetting an IPv4 Network (8.1) 405

Network Segmentation (8.1.1) 405
Broadcast Domains (8.1.1.1) 405
Problems with Large Broadcast Domains (8.1.1.2) 406
Reasons for Subnetting (8.1.1.3) 407
Subnetting an IPv4 Network (8.1.2) 408
Octet Boundaries (8.1.2.1) 408
Subnetting on the Octet Boundary (8.1.2.2) 409
Classless Subnetting (8.1.2.3) 410
Classless Subnetting Example (8.1.2.6) 412
Creating 2 Subnets (8.1.2.7) 414
Subnetting Formulas (8.1.2.9) 416
Creating 4 Subnets (8.1.2.10) 418
Subnetting a /16 and /8 Prefix (8.1.3) 421
Creating Subnets with a /16 prefix (8.1.3.1) 421
Creating 100 Subnets with a /16 Network (8.1.3.2) 423
Calculating the Hosts (8.1.3.3) 424
Creating 1000 Subnets with a /8 Network (8.1.3.5) 425
Subnetting to Meet Requirements (8.1.4) 427
Subnetting Based on Host Requirements (8.1.4.1) 428
Subnetting Based on Network Requirements (8.1.4.2) 428
Network Requirement Example (8.1.4.3) 429
Benefits of Variable Length Subnet Masking (8.1.5) 432
Traditional Subnetting Wastes Addresses (8.1.5.1) 432
Variable Length Subnet Masks (8.1.5.2) 434
Basic VLSM (8.1.5.3) 435
VLSM in Practice (8.1.5.5) 437
VLSM Chart (8.1.5.6) 439

Addressing Schemes (8.2) 440

Structured Design (8.2.1) 440
IPv4 Network Address Planning (8.2.1.1) 440
Planning to Address the Network (8.2.1.2) 441
Assigning Addresses to Devices (8.2.1.3) 442

Design Considerations for IPv6 (8.3) 443

Subnetting an IPv6 Network (8.3.1) 443
The IPv6 Global Unicast Address (8.3.1.1) 444
Subnetting Using the Subnet ID (8.3.1.2) 445
IPv6 Subnet Allocation (8.3.1.3) 446

Summary (8.4) 449

Practice 450

Class Activities 450

Labs 451

Packet Tracer Activities 451

Check Your Understanding Questions 451

Chapter 9 Transport Layer 455

Objectives 455

Key Terms 455

Introduction (9.0) 456

Transport Layer Protocols (9.1) 457

Transportation of Data (9.1.1) 457

Role of the Transport Layer (9.1.1.1) 457
Transport Layer Responsibilities (9.1.1.2) 458
Conversation Multiplexing (9.1.1.3) 460
Transport Layer Reliability (9.1.1.4) 461
TCP (9.1.1.5) 462
UDP (9.1.1.6) 463
The Right Transport Layer Protocol for the Right Application (9.1.1.7) 463

TCP and UDP Overview (9.1.2) 464

TCP Features (9.1.2.1) 465
TCP Header (9.1.2.2) 466
UDP Features (9.1.2.3) 468
UDP Header (9.1.2.4) 468
Multiple Separate Conversations (9.1.2.5) 469
Port Numbers (9.1.2.6) 470
Socket Pairs (9.1.2.7) 471
Port Number Groups (9.1.2.8) 472
The netstat Command (9.1.2.9) 473

TCP and UDP (9.2) 474

TCP Communication Process (9.2.1) 474

TCP Server Processes (9.2.1.1) 474
TCP Connection Establishment (9.2.1.2) 477
TCP Session Termination (9.2.1.3) 478
TCP Three-way Handshake Analysis (9.2.1.4) 481

Reliability and Flow Control (9.2.2) 482

TCP Reliability – Ordered Delivery (9.2.2.1) 482
TCP Flow Control – Window Size and Acknowledgements (9.2.2.4) 485
TCP Flow Control – Congestion Avoidance (9.2.2.5) 487

UDP Communication (9.2.3) 488

UDP Low Overhead versus Reliability (9.2.3.1) 488
UDP Datagram Reassembly (9.2.3.2) 489
UDP Server Processes and Requests (9.2.3.3) 490
UDP Client Processes (9.2.3.4) 490

TCP or UDP (9.2.4) 491

Applications that Use TCP (9.2.4.1) 491
Applications that Use UDP (9.2.4.2) 492

Summary (9.3) 494

Practice 495

Class Activities 496

Labs 496

Packet Tracer Activities 496

Check Your Understanding Questions 496

Chapter 10 Application Layer 501

Objectives 501

Key Terms 501

Introduction (10.0) 502

Application Layer Protocols (10.1) 502

Application, Presentation, and Session (10.1.1) 502

Application Layer (10.1.1.1) 502

Presentation and Session Layer (10.1.1.2) 503

TCP/IP Application Layer Protocols (10.1.1.3) 504

How Application Protocols Interact with End-User Applications (10.1.2) 506

Client-Server Model (10.1.2.1) 506

Peer-to-Peer Networks (10.1.2.2) 507

Peer-to-Peer Applications (10.1.2.3) 507

Common P2P Applications (10.1.2.4) 508

Well-Known Application Layer Protocols and Services (10.2) 510

Web and Email Protocols (10.2.1) 510

Hypertext Transfer Protocol and Hypertext Markup Language (10.2.1.1) 510

HTTP and HTTPS (10.2.1.2) 512

Email Protocols (10.2.1.3) 513

SMTP Operation (10.2.1.4) 514

POP Operation (10.2.1.5) 514

IMAP Operation (10.2.1.6) 515

IP Addressing Services (10.2.2) 516

Domain Name Service (10.2.2.1) 516

DNS Message Format (10.2.2.2) 519

DNS Hierarchy (10.2.2.3) 520

The nslookup Command (10.2.2.4) 521

Dynamic Host Configuration Protocol (10.2.2.5) 522

DHCP Operation (10.2.2.6) 524

File Sharing Services (10.2.3) 525

File Transfer Protocol (10.2.3.1) 525

Server Message Block (10.2.3.2) 527

Summary (10.3) 529

Practice 530

Class Activities 530

Labs 530

Packet Tracer Activities 531

Check Your Understanding Questions 531

Chapter 11 Build a Small Network 533

Objectives 533

Key Terms 533

Introduction (11.0) 534

Network Design (11.1) 534

Devices in a Small Network (11.1.1) 534

Small Network Topologies (11.1.1.1) 534

Device Selection for a Small Network (11.1.1.2) 535

IP Addressing for a Small Network (11.1.1.3) 536

Redundancy in a Small Network (11.1.1.4) 537

Traffic Management (11.1.1.5) 539

Small Network Applications and Protocols (11.1.2) 539

Common Applications (11.1.2.1) 539

Common Protocols (11.1.2.2) 541

Voice and Video Applications (11.1.2.3) 542

Scale to Larger Networks (11.1.3) 544

Small Network Growth (11.1.3.1) 544

Protocol Analysis (11.1.3.2) 544

Employee Network Utilization (11.1.3.3) 545

Network Security (11.2) 547

Security Threats and Vulnerabilities (11.2.1) 547

Types of Threats (11.2.1.1) 547

Physical Security (11.2.1.2) 548

Types of Vulnerabilities (11.2.1.3) 548

Network Attacks (11.2.2) 550

Types of Malware (11.2.2.1) 550

Reconnaissance Attacks (11.2.2.2) 551

Access Attacks (11.2.2.3) 552

Denial of Service Attacks (11.2.2.4) 554

Network Attack Mitigation (11.2.3) 556

Backup, Upgrade, Update, and Patch (11.2.3.1) 556

Authentication, Authorization, and Accounting (11.2.3.2) 557
Firewalls (11.2.3.3) 558
Endpoint Security (11.2.3.4) 559
Device Security (11.2.4) 559
Device Security Overview (11.2.4.1) 559
Passwords (11.2.4.2) 560
Basic Security Practices (11.2.4.3) 561
Enable SSH (11.2.4.4) 563
Backup and Restore Configuration Files (11.2.5) 564
Router File Systems (11.2.5.1) 564
Switch File Systems (11.2.5.2) 567
Backing Up and Restoring Using Text Files (11.2.5.3) 568
Backing up and Restoring TFTP (11.2.5.4) 569
Using USB Ports on a Cisco Router (11.2.5.5) 570
Backing Up and Restoring Using a USB (11.2.5.6) 570

Network Testing and Verification (11.3) 572

The ping Command (11.3.1) 572
Interpreting Ping Results (11.3.1.1) 573
Extended Ping (11.3.1.2) 574
Network Baseline (11.3.1.3) 575
The traceroute and tracert Command (11.3.2) 577
Interpreting Trace Messages (11.3.2.1) 578
Extended traceroute (11.3.2.2) 579
Show Commands (11.3.3) 581
Common show Commands Revisited (11.3.3.1) 581
Host and IOS Commands (11.3.4) 585
The ipconfig Command (11.3.4.1) 585
The arp Command (11.3.4.2) 587
The show cdp neighbors Command (11.3.4.3) 588
The show ip interface brief Command (11.3.4.4) 591
Debugging (11.3.5) 592
The debug Command (11.3.5.1) 592
The terminal monitor Command (11.3.5.2) 594

Network Troubleshooting (11.4) 594

Troubleshooting Methodologies (11.4.1) 594
Basic Troubleshooting Approaches (11.4.1.1) 595
Resolve or Escalate? (11.4.1.2) 596
Verify and Monitor Solution (11.4.1.3) 596
Troubleshoot Cables and Interfaces (11.4.2) 598
Duplex Operation (11.4.2.1) 598
Duplex Mismatch (11.4.2.2) 599

Troubleshooting Scenarios (11.4.3) 600
IP Addressing Issues on IOS Devices (11.4.3.1) 600
IP Addressing Issues on End Devices (11.4.3.2) 601
Default Gateway Issues (11.4.3.3) 602
Troubleshooting DNS Issues (11.4.3.4) 604

Summary (11.5) 606

Practice 608

Class Activities 608

Labs 608

Packet Tracer Activities 608

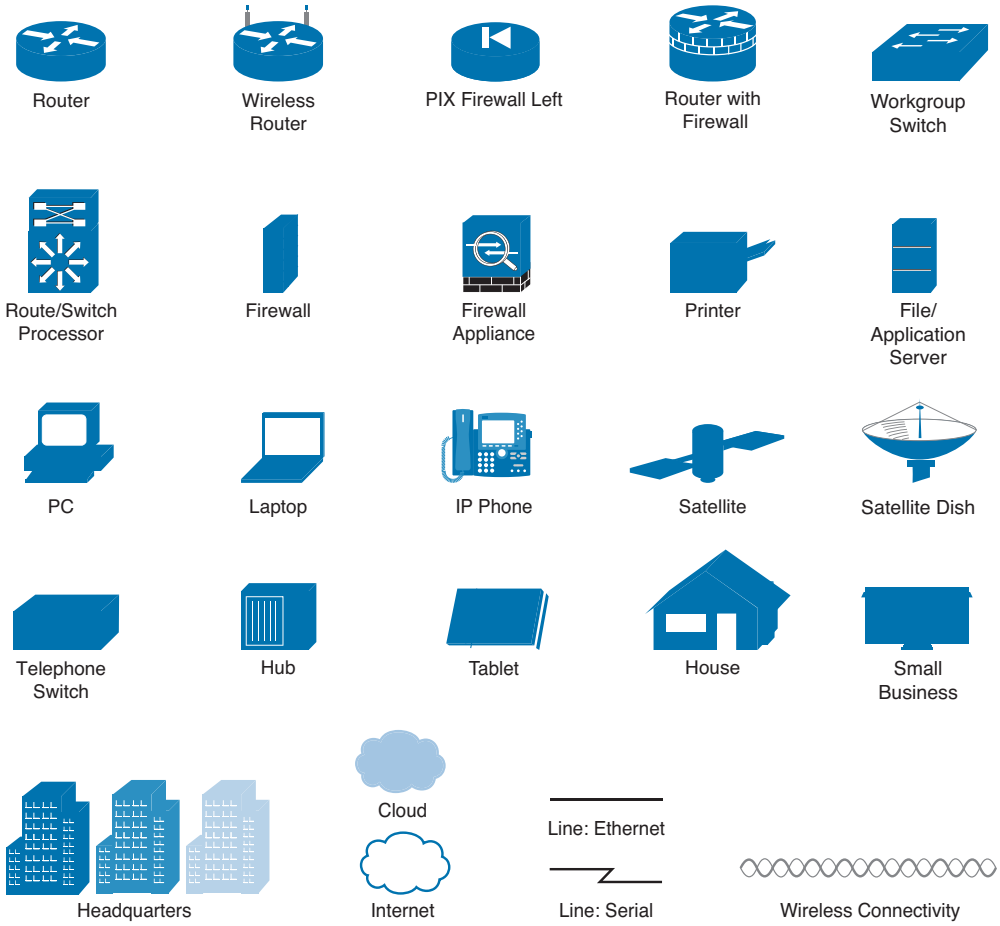
Check Your Understanding Questions 609

Appendix A 613

Glossary 627

Index 645

Syntax Conventions



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

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italics* 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

Introduction to Networks: Companion Guide v5.1 is the official supplemental textbook for the Cisco Network Academy CCNA Introduction to Networks course. Cisco Networking Academy is a comprehensive program that delivers information technology skills to students around the world. The curriculum emphasizes real-world practical application, while providing opportunities for you to gain the skills and hands-on experience needed to design, install, operate, and maintain networks in small- to medium-sized businesses as well as enterprise and service provider environments.

As a textbook, this book provides a ready reference to explain the same networking concepts, technologies, protocols, and devices as the online curriculum. This book emphasizes key topics, terms, and activities and provides some alternate explanations and examples as compared with the 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

The book, as well as the course, is designed as an introduction to data network technology for those pursuing careers as network professionals as well as those who need only an introduction to network technology for professional growth. Topics are presented concisely, starting with the most fundamental concepts and progressing to a comprehensive understanding of network communication. The content of this text provides the foundation for additional Cisco Networking Academy courses and preparation for the CCENT and CCNA Routing and Switching certifications.

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 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.
- **Notes:** These are short sidebars that point out interesting facts, timesaving methods, and important safety issues.
- **Chapter summaries:** At the end of each chapter is a summary of the chapter's key concepts. It provides a synopsis of the chapter and serves as a study aid.
- **Practice:** At the end of chapter there is a full list of all the labs, class activities, and Packet Tracer activities to refer back to for study time.

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 from inside the chapter. The 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 253 terms.

Practice

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

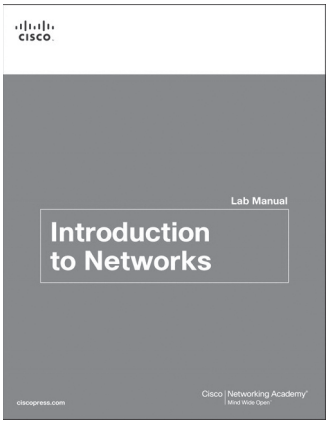
- **Check Your Understanding questions and answer key:** Updated review questions are presented at the end of each chapter as a self-assessment tool. These questions match the style of questions that you see in the online course. Appendix A, "Answers to the 'Check Your Understanding' Questions," provides an answer key to all the questions and includes an explanation of each answer.

- **Labs and activities:** Throughout each chapter, you will be directed back to the online course to take advantage of the activities created to reinforce concepts. In addition, at the end of each chapter, there is a "Practice" section that collects a list of all the labs and activities to provide practice with the topics introduced in this chapter. The labs and class activities are available in the companion *Introduction to Networking v5.1 Lab Manual* [ISBN 978-1-58713-353-4]. The Packet Tracer Activities PKA files are found in the online course.

- **Page references to online course:** After headings, 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.

Lab Manual

The supplementary book *Introduction to Networking v5.1 Lab Manual*, by Cisco Press (ISBN 978-1-58713-353-4), contains all the labs and class activities from the course.



Packet Tracer Activity

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 allows you to create networks, visualize how packets flow in the network, and use basic testing tools to determine whether the network would work. When you see this icon, you can use Packet Tracer with the listed file to perform a task suggested in this book. The activity files are available 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 Academy Introduction to Networking course and is divided into 11 chapters, one appendix, and a glossary of key terms:

- **Chapter 1, "Explore the Network":** Introduces the concept of a network and provides an overview of the different types of networks encountered. It examines how networks impact the way we work, learn, and play. This chapter also examines new trends in networks such as video, cloud computing, and BYOD and how to help ensure that we have a robust, reliable, secure network to support these trends.

- **Chapter 2, "Configure a Network Operating System":** Introduces the operating system used with most Cisco devices: the Cisco IOS. The basic purpose and functions of the IOS are described as well as the methods to access the IOS. The chapter will also present maneuvering through the IOS command-line interface as well as basic IOS device configuration.
- **Chapter 3, "Network Protocols and Communications":** Examines the importance of rules or protocols for network communication. It explores the OSI reference model and the TCP/IP communication suite, examining how these models provide the necessary protocols to allow communication to occur on a modern converged network.
- **Chapter 4, "Network Access":** Introduces the lowest layer of the TCP/IP model: the transport layer. This layer is essentially the equivalent of the OSI data link layer and the physical layer. The chapter discusses how this layer prepares network layer packets for transmission, controls access to the physical media, and transports the data across various media. This chapter includes a description of the encapsulation protocols and processes that occur as data travels across the LAN and the WAN as well as the media used.
- **Chapter 5, "Ethernet":** Examines the functionality of one of the most common LAN protocols in use today. It explores how Ethernet functions and interacts with the TCP/IP protocol suite to provide high-speed data communications.
- **Chapter 6, "Network Layer":** Introduces the function of the network layer—routing—and the basic device that performs this function—the router. The important routing concepts related to addressing, path determination, and data packets for both IPv4 and IPv6 will be presented. The chapter also introduces the construction of a router and the basic router configuration.
- **Chapter 7, "IP Addressing":** Focuses on IPv4 and IPv6 network addressing, including the types of addresses and address assignment. It describes how to use the address mask or prefix length to determine the number of subnetworks and hosts in a network. This chapter also introduces Internet Control Message Protocol (ICMP) tools, such as ping and trace.
- **Chapter 8, "Subnetting IP Networks":** Examines how to improve network performance by optimally dividing the IP address space based on network requirements. It explores the calculation of valid host addresses and the determination of both subnet and subnet broadcast addresses. This chapter examines subnetting for both IPv4 and IPv6.
- **Chapter 9, "Transport Layer":** Introduces Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) and examines how each transports information across the network. It explores how TCP uses segmentation, the three-way handshake, and expectational acknowledgements to ensure reliable

delivery of data. It also examines the best-effort delivery mechanism provided by UDP and describes when this would be preferred over TCP.

- **Chapter 10, "Application Layer":** Introduces some protocols of the TCP/IP application layer, which also relates to the top three layers of the OSI model. The chapter focuses on the role of the application layer and how the applications, services, and protocols within the application layer make robust communication across data networks possible. This will be demonstrated by examining some key protocols and services including HTTP, DNS, DHCP, SMTP/POP, Telnet, and FTP.
- **Chapter 11, "Build a Small Network":** Reexamines the various components found in a small network and describes how they work together to allow network growth. Network security and performance issues are examined along with some of the commands that can be used to examine the configuration of devices and the performance of the network. Router and switch file systems are also examined, along with methods for backing up and restoring their configuration files.
- **Appendix A, "Answers to the 'Check Your Understanding' Questions":** This appendix lists the answers to the "Check Your Understanding" review questions that are included at the end of each chapter.
- **Glossary:** The glossary provides you with definitions for all the key terms identified in each chapter.

CHAPTER 1

Explore 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, learn, work, and play?
- What ways can host devices be used as clients, servers, or both?
- How are network devices used?
- What are the differences between LAN and WAN devices?
- What are the differences between LAN and WAN topologies?
- What is the basic structure of the Internet?
- How do LANs and WANs interconnect to the Internet?
- What is a converged network?
- What are the four basic requirements of a converged network?
- How do trends such as BYOD, online collaboration, video, and cloud computing change the way we interact?
- How are networking technologies changing the home environment?
- What are some basic security threats and solutions for both small and large networks?
- Why is it important to understand the switching and routing infrastructure of a network?

Key Terms

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

Peer-to-Peer (P2P) file sharing *Page 6*

Small Office/Home Office (SOHO) network *Page 8*

Medium to large network *Page 8*

Server *Page 9*

Client *Page 9*

End device *Page 14*

Medium *Page 8*

Network Interface Card (NIC) *Page 18*

Physical port *Page 18*

Interface *Page 18*

Physical topology diagram *Page 19*

Logical topology diagram *Page 19*

Local area network (LAN) *Page 20*

Wide area network (WAN) *Page 20*

Internet *Page 23*

Intranet *Page 25*

Extranet *Page 25*

Internet Service Provider (ISP) *Page 26*

Converged network *Page 29*

Network architecture *Page 31*

Scalable network *Page 32*

Quality of Service (QoS) *Page 32*

Bring Your Own Device (BYOD) *Page 35*

Collaboration *Page 36*

Cloud computing *Page 37*

Private cloud *Page 38*

Public cloud *Page 38*

Hybrid cloud *Page 38*

Custom cloud *Page 38*

Data center *Page 39*

Smart home technology *Page 40*

Powerline networking *Page 40*

Wireless Internet Service Provider (WISP) *Page 41*

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, creating 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

Refer to Lab Activity for this chapter

Welcome to a new component of our Networking Academy curriculum: 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!

Here is your first modeling activity:

Draw Your Concept of the Internet

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. Some items you may wish to include

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

Upon completion, 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.

Globally Connected (1.1)

Networks are all around us. They provide us with a way to communicate and share information and resources with individuals in the same location or around the world. This requires an extensive array of technologies and procedures that can readily adapt to varying conditions and requirements.

Networking Today (1.1.1)

For most individuals, the use of networks has become a daily occurrence. The availability of these networks has altered the way in which we interact with each other.

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.

In today's world, through the use of networks, we are connected like never before. People with ideas can communicate instantly with others to make those ideas a reality. News events and discoveries are known worldwide in seconds. Individuals can even connect and play games with friends separated by oceans and continents.

Play the video to view how connected we are.

Video

Go to the online course to view this video.

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 button. 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.

Play the video to watch how the Internet emerged over the last 25 years and see a glimpse into the future! What else do you think we will be able to do using the network as the platform?

Video

Go to the online course to view this video.

No Boundaries (1.1.1.3)

Advancements in networking technologies are perhaps the most significant changes in the world today. They are helping to create a world in which national borders, geographic distances, and physical limitations become less relevant presenting 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 have changed the way we learn. 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. 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.

Play the video to see how the classroom is expanding.

Video

Go to the online course to view this video.

Networks Support the Way We Communicate (1.1.1.5)

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 communication include

- **Texting –** Texting enables instant real-time communication between two or more people.

- **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 –** Without the constraints of location or time zone, collaboration tools allow individuals to communicate with each other, often across real-time interactive video. The broad distribution of data networks means that people in remote locations can contribute on an equal basis with people in the heart of large population centers.
- **Blogs –** Blogs, which is an abbreviation of the word "weblogs," are web pages that are easy to update and edit. Unlike commercial websites, blogs give anyone a means to communicate their thoughts to a global audience without technical knowledge of web design.
- **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. Many businesses use wikis as their internal collaboration tool.
- **Podcasting –** Podcasting allows people to deliver their audio 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 allows people to share files with each other without having to store and download them from a central server. The user joins the P2P network by simply installing the P2P software. P2P file sharing has not been embraced by everyone. Many people are concerned about violating 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)

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 web site at http://www.cisco.com/web/about/success-stories/index.html.

Networks Support the Way We Play (1.1.1.7)

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 as if we were all 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.

Whatever form of recreation we enjoy, 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 complete the following objectives:

- Part 1: Use Collaboration Tools
- Part 2: Share Documents with Google Drive
- Part 3: Explore Conferencing and Web Meetings
- Part 4: Create Wiki Pages

Providing Resources in a Network (1.1.2)

To efficiently provide resources to end users, networks occur in many sizes and forms.

Networks of Many Sizes (1.1.2.1)

Networks come in all sizes. They can range from simple networks consisting of two computers to networks connecting millions of devices. Figure 1-1 shows four classifications of networks based on size:

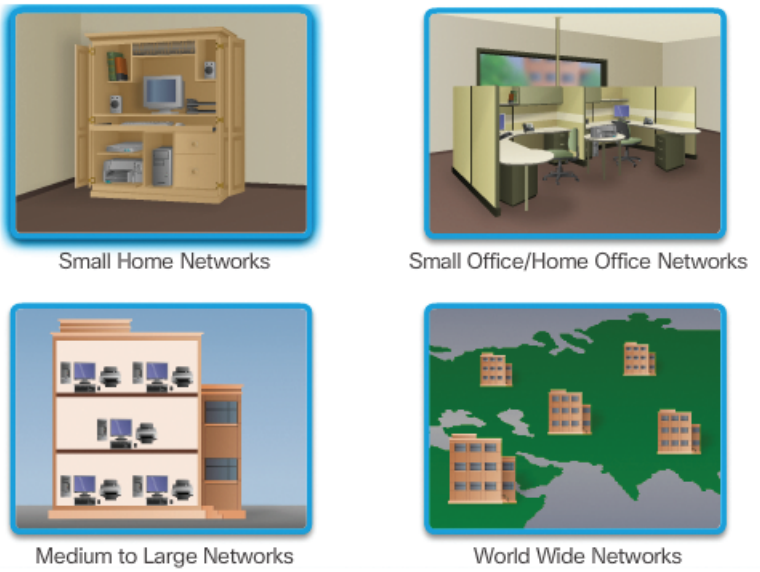


Figure 1-1 Network Sizes

- Small home networks connect a few computers to each other and the Internet.
- The *Small Office/Home Office or SOHO network* enables computers within a home office or a remote office to connect to a corporate network or access centralized, shared resources.
- *Medium to large networks*, such as those used by corporations and schools, can have many locations with hundreds or thousands of interconnected computers.
- The Internet is a network of networks that connects hundreds of millions of computers world-wide.

Simple networks installed in homes enable sharing of resources, such as printers, documents, pictures, and music between a few local computers.

Home office networks and small office networks are often set up by individuals that work from a home or a remote office and need to connect to a corporate network or other centralized resources. Additionally, many self-employed entrepreneurs use home office and small office networks to advertise and sell products, order supplies, and communicate with customers.

In businesses and large organizations, networks can be used on an even broader scale to provide consolidation, storage, and access to information on network servers. Networks also allow for rapid communication such as email, instant messaging, and collaboration among employees. In addition to internal benefits, many organizations use their networks to provide products and services to customers through their connection to the Internet.

The Internet is the largest network in existence. In fact, the term Internet means a 'network of networks.' The Internet is literally a collection of interconnected private and public networks, such as those described above.

Clients and Servers (1.1.2.2)

All computers connected to a network that participate directly in network communication are classified as hosts. Hosts are also called end devices.

Servers are computers with software that enable them to provide information, like email or web pages, to other end devices on the network. Each service requires separate server software. For example, a server requires web server software in order to provide web services to the network. A computer with server software can provide services simultaneously to one or many clients. Additionally, a single computer can run multiple types of server software. In a home or small business, it may be necessary for one computer to act as a file server, a web server, and an email server.

Clients are computers with software installed that enable them to request and display the information obtained from the server. An example of client software is a web browser, like Chrome or Firefox. A single computer can also run multiple types of client software. For example, a user can check email and view a web page while instant messaging and listening to Internet radio.

Figure 1-2 shows different client and server examples.

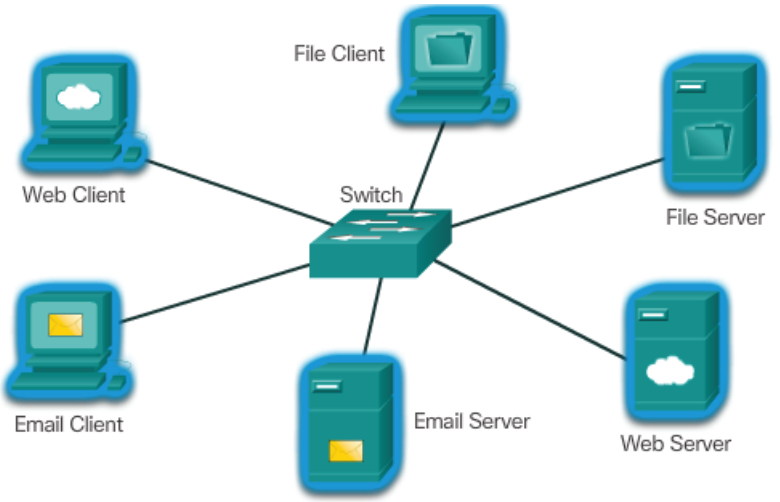


Figure 1-2 Client/Server Examples

- **Web Client and Server:** The Web Server runs web server software and clients use their browser software, such as Windows Internet Explorer, to access web pages on the server.
- **Email Client and Server:** The Email Server runs email server software and clients use their mail client software, such as Microsoft Outlook, to access email on the server.
- **File Client and Server:** The File Server stores corporate and user files in a central location. The client devices access these files with client software such as Windows Explorer.

Peer-to-Peer (1.1.2.3)

Client and server software usually runs on separate computers, but it is also possible for one computer to carry out both roles at the same time. In small businesses and homes, many computers function as the servers and clients on the network. This type of network is called a *peer-to-peer network*, as shown in Figure 1-3.

Figure 1-3 Peer-to-Peer Example

The advantages of peer-to-peer networking:

- Easy to set up
- Less complexity
- Lower cost since network devices and dedicated servers may not be required
- Can be used for simple tasks such as transferring files and sharing printers

The disadvantages of peer-to-peer networking:

- No centralized administration
- Not as secure
- Not scalable
- All devices may act as both clients and servers, which can slow their performance

LANs, WANs, and the Internet (1.2)

Many different components are required to allow a network to provide services and resources. These various components work together to ensure that resources are delivered in an efficient manner to those requiring the services.

Network Components (1.2.1)

Different network components are used within the network to provide services and resources. These various components work together to ensure that resources are delivered in an efficient manner to those requiring the services.

Overview of Network Components (1.2.1.1)

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 collection of networks that literally spans the globe. This network infrastructure provides the stable and reliable channel over which these communications occur.

The network infrastructure contains three categories of network components, as shown in Figures 1-4, 1-5, and 1-6.

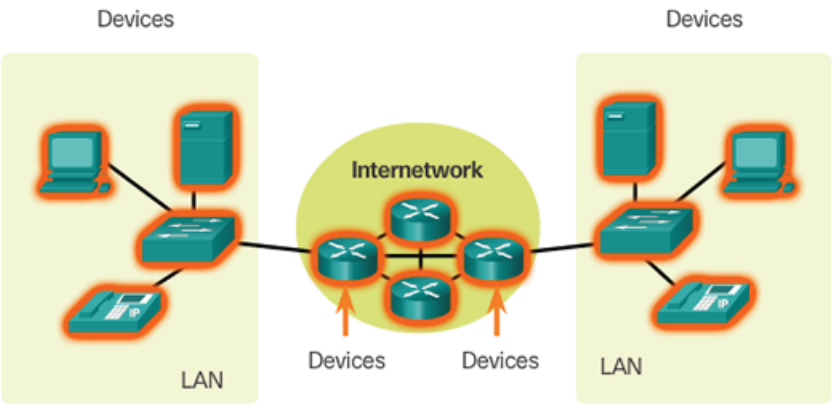


Figure 1-4 Devices

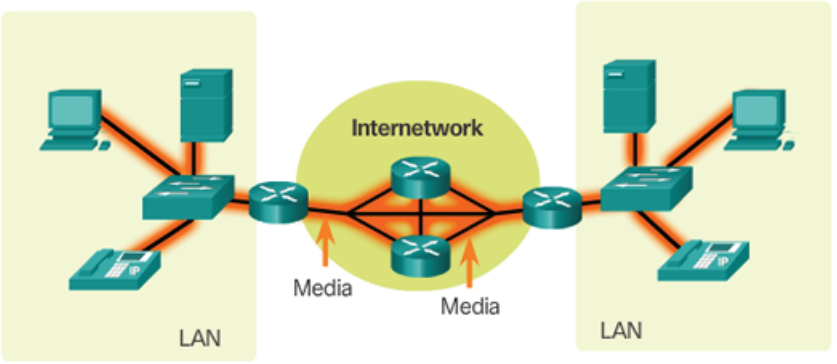


Figure 1-5 Media

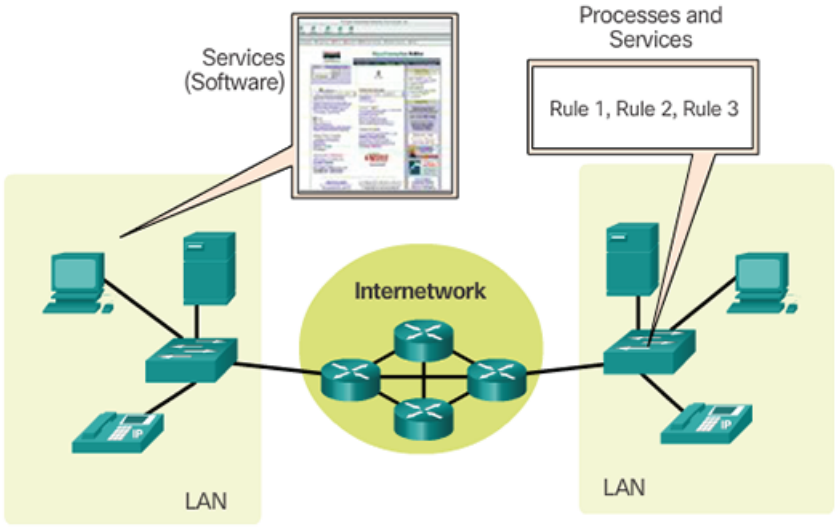


Figure 1-6 Services

Devices and media are the physical elements, or hardware, of the network. Hardware is often the visible components of the network platform such as a laptop, PC, switch, router, wireless access point, or the cabling used to connect the devices.

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 (1.2.1.2)

The network devices that people are most familiar with are called end devices. Some examples of end devices are shown in Figure 1-7.

Figure 1-7 Examples of End Devices

An *end device* is either the source or destination of a message transmitted over the network. To distinguish one end device from another, each end device on a network is identified by an address. When an end device initiates communication, it uses the address of the destination end device to specify where the message should be sent. Devices between the source and destination are responsible for choosing the best path and forwarding messages sent between end devices, as shown in Figure 1-8.

Intermediary Network Devices (1.2.1.3)

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

Intermediary devices use the destination end device address, in conjunction with information about the network interconnections, to determine the path that messages should take through the network, as shown in Figure 1-8.

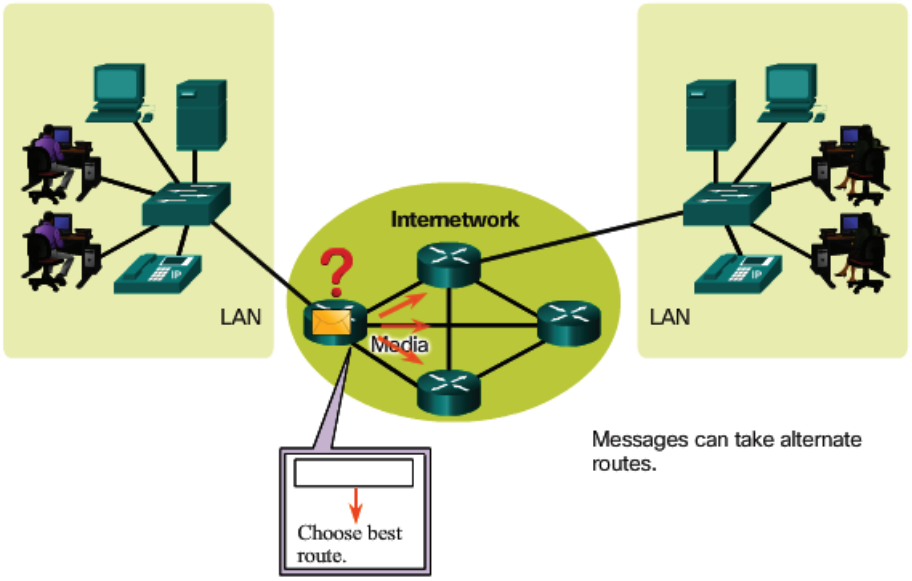


Figure 1-8 End Devices Communicate Across the Internetwork

Examples of the more common intermediary devices are shown in Figure 1-9.

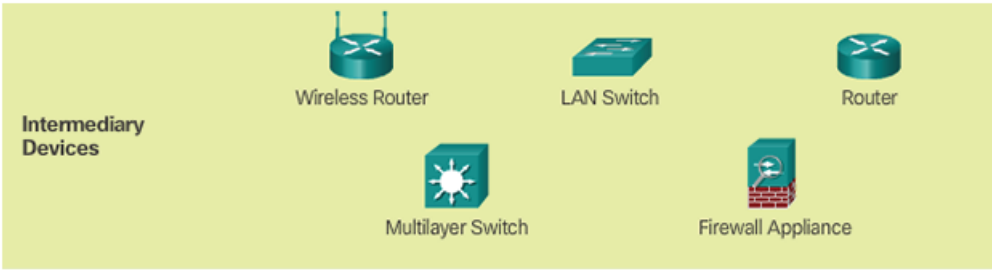


Figure 1-9 Examples of Intermediary Devices

Intermediary network devices perform some or all of these functions:

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

Network Media (1.2.1.4)

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 three types of media to interconnect devices and to provide the pathway over which data can be transmitted. As shown in Figure 1-10, these media are

- **Metallic wires within cables –** data is encoded into electrical impulses
- **Glass or plastic fibers (fiber optic cable) –** data is encoded as pulses of light
- **Wireless transmission –** data is encoded using wavelengths from the electromagnetic spectrum

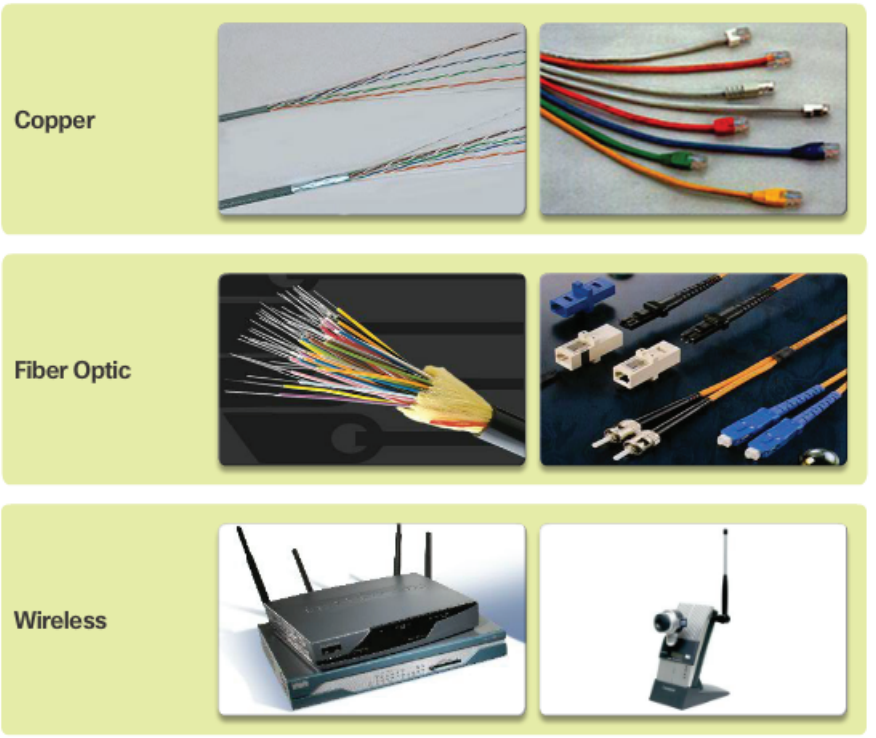


Figure 1-10 Examples of Network Media

Different types of network media have different features and benefits. Not all network media have the same characteristics, nor are they all appropriate for the same purpose.

Criteria to consider when choosing network media includes the following:

- What is the maximum distance that the media can successfully carry a signal?
- Into what type of environment will the media be installed?
- What is the amount of data and the speed at which it must be transmitted?
- What is the cost of the media and installation?

Network Representations (1.2.1.5)

Diagrams of networks often use symbols, like those shown in Figure 1-11, to represent the different devices and connections that make up a network.

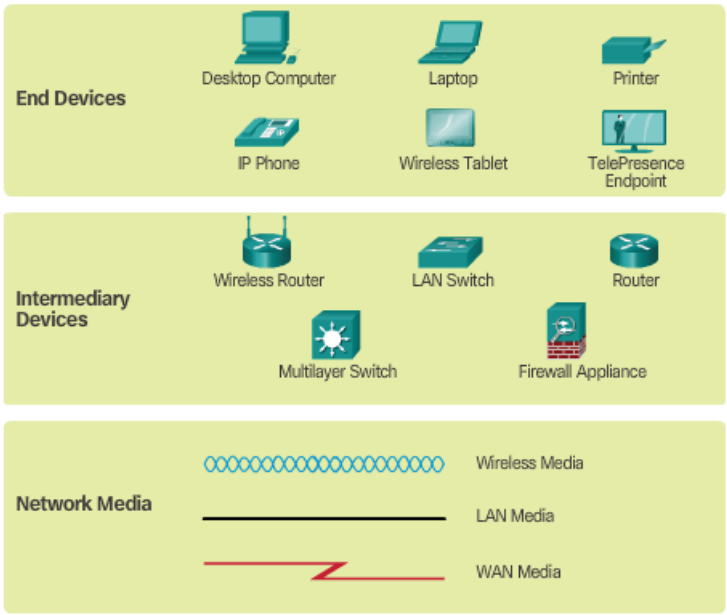


Figure 1-11 Common Icons Use to Represent Network Devices

A diagram provides an easy way to understand how devices in a large network are connected. This type of "picture" of a network is known as a topology diagram. 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.

In addition to these representations, specialized terminology is used when discussing how each of these devices and media connect to each other. Important terms to remember are

- *Network Interface Card* – A NIC, or LAN adapter, provides the physical connection to the network at the PC or other end device. The media that are connecting the PC to the networking device plug directly into the NIC (Figure 1-12).

Figure 1-12 Network Interface Card

- *Physical Port* – A connector or outlet on a networking device where the media is connected to an end device or another networking device.
- *Interface* – Specialized ports on a networking device that connect to individual networks. Because routers are used to interconnect networks, the ports on a router are referred to as network interfaces.

Note

Often, the terms port and interface are often used interchangeably.

Topology Diagrams (1.2.1.6)

Topology diagrams are mandatory for anyone working with a network. They provide a visual map of how the network is connected.

There are two types of topology diagrams:

- *Physical topology diagrams* – Identify the physical location of intermediary devices and cable installation (Figure 1-13).

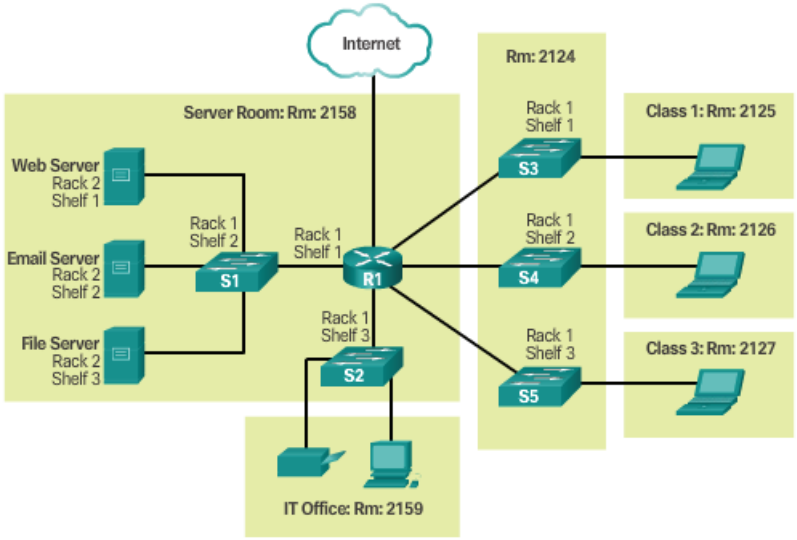


Figure 1-13 Physical Topology

- *Logical topology diagrams* – Identify devices, ports, and addressing scheme (Figure 1-14).

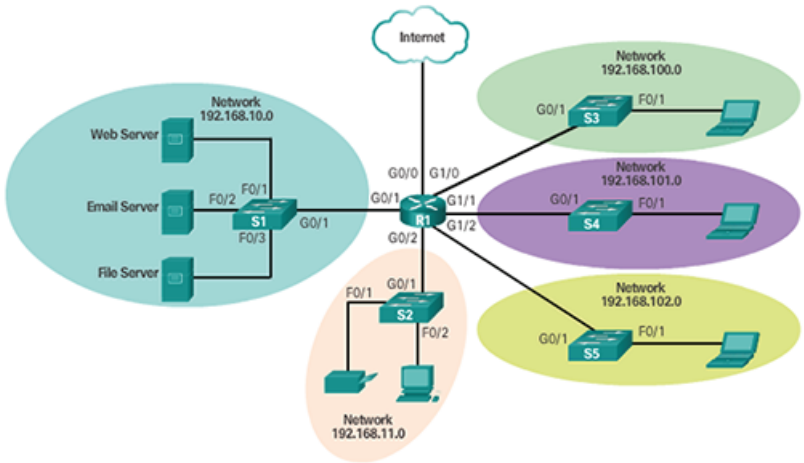


Figure 1-14 Logical Topology

The topologies shown in the physical and logical diagrams are appropriate for your level of understanding at this point in the course. Search the Internet for "network topology diagrams" to see some more complex examples. If you add the "Cisco" to your search phrase, you will find many topologies using similar icons to what you have seen in this chapter.

Interactive Graphic

Activity 1.2.1.7: Network Component Representations and Functions

Go to the online course to perform this practice activity.

LANs and WANs (1.2.2)

Network infrastructures can be differentiated is various ways. Two of the most common types of network infrastructures are LANs and WANs.

Types of Networks (1.2.2.1)

Network infrastructures can vary greatly in terms of

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

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, which is typically an enterprise, home, or small business network owned and managed by an individual or IT department.
- *Wide Area Network (WAN)* – A network infrastructure that provides access to other networks over a wide geographical area, which is typically owned and managed by a telecommunications service provider.

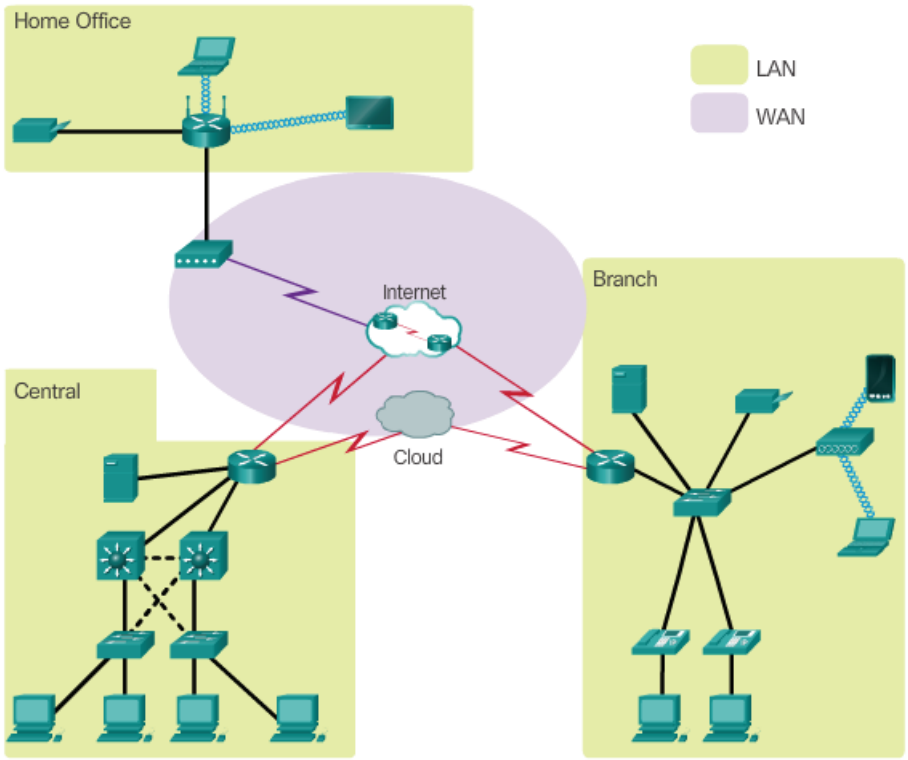


Figure 1-15 LANs and WANs

Video

Play the video to watch Cisco's Jimmy Ray Purser explains the difference between LAN and WAN.

Go to the online course to view this video.

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 end points in a small geographical area.
- **Storage Area Network (SAN) –** A network infrastructure designed to support file servers and provide data storage, retrieval, and replication.

Local Area Networks (1.2.2.2)

LANs are a network infrastructure that spans a small geographical area, as shown in Figure 1-16.

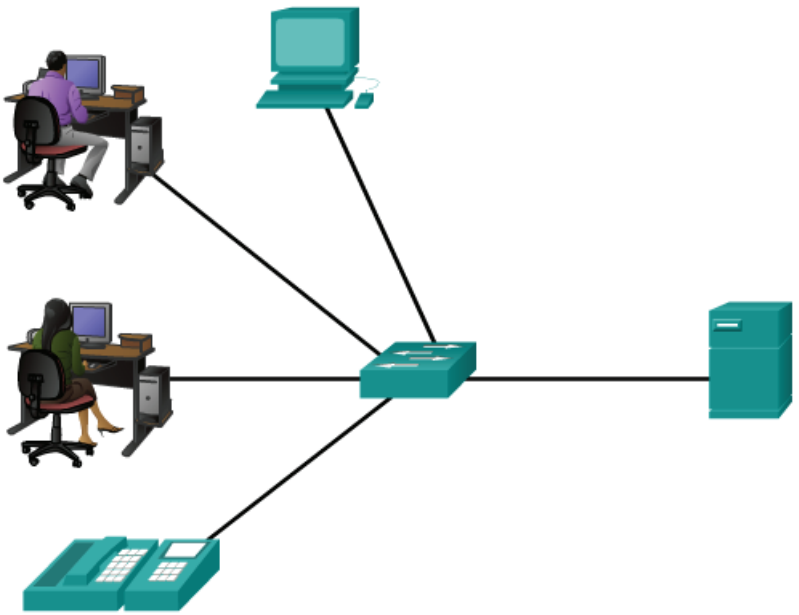


Figure 1-16 Example of a LAN

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.
- LANs provide high-speed bandwidth to internal end devices and intermediary devices.

Wide Area Networks (1.2.2.3)

WANs are a network infrastructure that spans a wide geographical area, as shown in Figure 1-17. WANs are typically managed by service providers (SP) or Internet Service Providers (ISP).

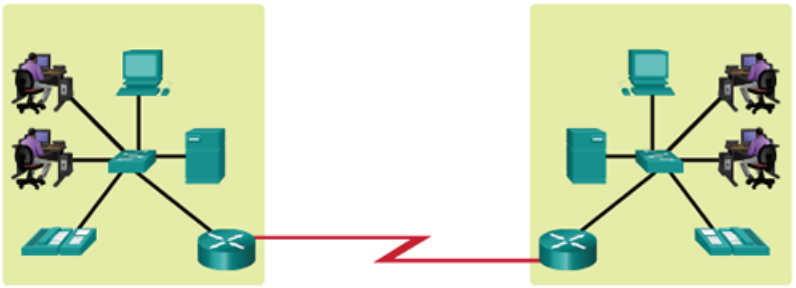


Figure 1-17 Example of a WAN

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, Intranets, and Extranets (1.2.3)

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.

The Internet (1.2.3.1)

The ***Internet*** is a worldwide collection of interconnected networks (internetworks or internet for short). Figure 1-18 one way to view the Internet as a collection of interconnected LANs and WANs.

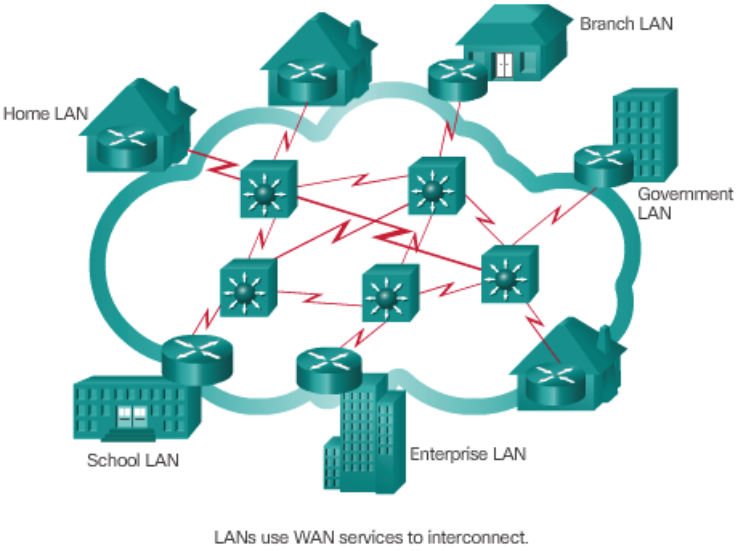


Figure 1-18 Collection of Interconnected LANs and WANs

Some of the LAN examples are connected to each other through a WAN connection. WANs are then connected to each other. The red WAN connection lines represent all the varieties of ways we connect networks. WANs can connect through copper wires, fiber optic cables, and wireless transmissions (not shown).

The Internet is not 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.

Intranets and Extranets (1.2.3.2)

There are two other terms that are similar to the term Internet:

- Intranet
- Extranet

Figure 1-19 shows the relationship of the Internet, extranets, and intranets.

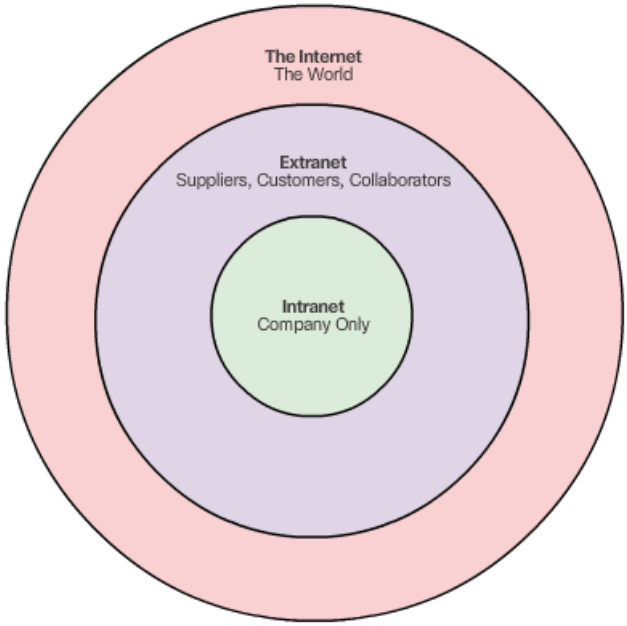


Figure 1-19 Internet, Extranet, and Intranet

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 with authorization.

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

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

Internet Connections (1.2.4)

The type of connection to the Internet will depend on the type of network being connected. A business network will usually require a connection with more bandwidth than a home network.

Internet Access Technologies (1.2.4.1)

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 between ISP and 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 (SP). Popular business-class services include business DSL, leased lines, and Metro Ethernet.

Home and Small Office Internet Connections (1.2.4.2)

Figure 1-20 illustrates common connection options for small office and home office users.

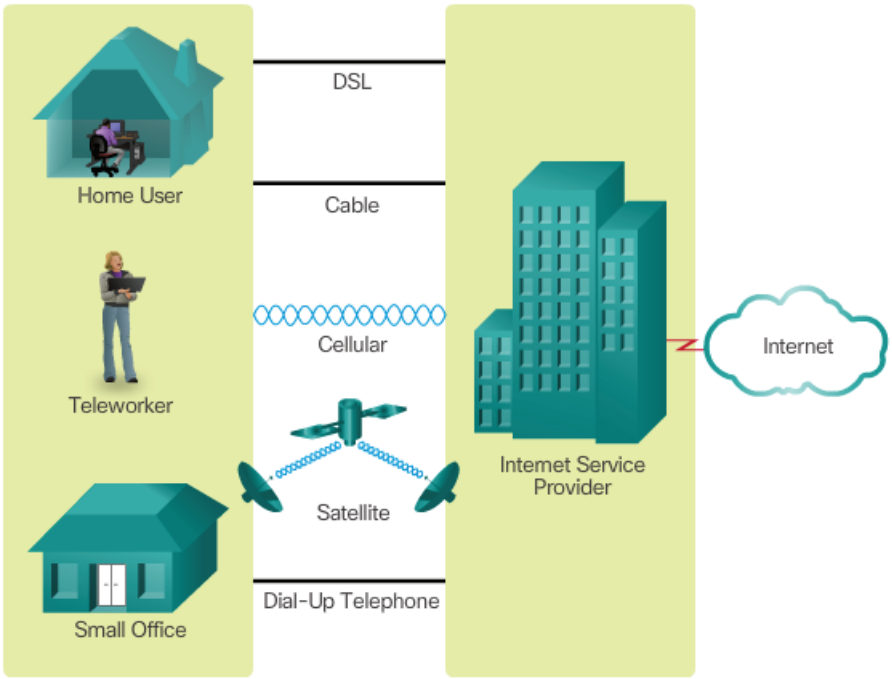


Figure 1-20 Connection Options

- **Cable –** Typically offered by cable television service providers, the Internet data signal is carried on the same cable that delivers cable television. It provides a high bandwidth, always on, connection to the Internet.

- **DSL –** Digital Subscriber Lines provide a high bandwidth, always on, connection to the Internet. DSL runs over a telephone line. In general, small office and home office users connect using Asymmetrical DSL (ADSL), which means that the download speed is faster than the upload speed.
- **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.
- **Satellite –** The availability of satellite Internet access is a real benefit in those areas that would otherwise have no Internet connectivity at all. Satellite dishes require a clear line of sight to the satellite.
- **Dial-up Telephone –** An inexpensive option that uses any phone line and a modem. 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.

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.

Businesses Internet Connections (1.2.4.3)

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 type of service providers located nearby.

Figure 1-21 illustrates common connection options for businesses.

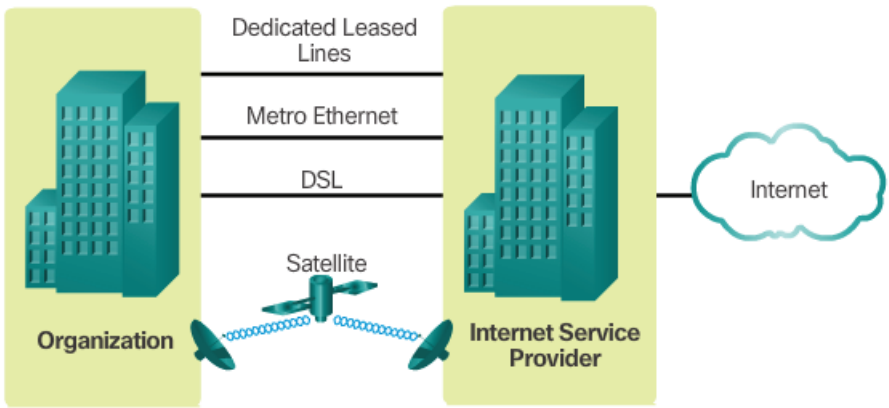


Figure 1-21 Typical Business Connection Options

- **Dedicated Leased Line –** Leased lines are actually reserved circuits within the service provider's network that connect geographically separated offices for private voice and/or data networking. The circuits are typically rented at a monthly or yearly rate. They can be expensive.
- **Ethernet WAN –** Ethernet WANs extend LAN access technology into the WAN. Ethernet is a LAN technology you will learn about in a later chapter. The benefits of Ethernet are now being extended into the WAN.
- **DSL –** Business DSL is available in various formats. A popular choice is Symmetric Digital Subscriber Lines (SDSL), which is similar to the consumer version of DSL but provides uploads and downloads at the same speeds.
- **Satellite –** Similar to small office and home office users, satellite service can provide a connection when a wired solution is not available.

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

Packet Tracer ☐ Activity

Packet Tracer 1.2.4.4: Help and Navigation Tips

Packet Tracer is a fun, take-home, flexible software program that will help you with your Cisco Certified Network Associate (CCNA) studies. Packet Tracer allows you to experiment with network behavior, build network models, and ask "what if" questions. In this activity, 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. You will also learn how to switch between various modes and workspaces.

Packet Tracer ☐ Activity

Packet Tracer 1.2.4.5: Network Representation

In this activity, you will explore how Packet Tracer serves as a modeling tool for network representations.

The Network as a Platform (1.3)

The network has become a platform for distributing a wide range of services to end users in a reliable, efficient, and secure manner.

Converged Networks (1.3.1)

Modern networks are constantly evolving to meet user demands. Today's networks are used for data, phone, and video.

Traditional Separate Networks (1.3.1.1)

Consider a school built thirty years ago. Back then, some classrooms were cabled for the data network, telephone network, and video network for televisions. These separate networks could not communicate with each other, as shown in Figure 1-22.

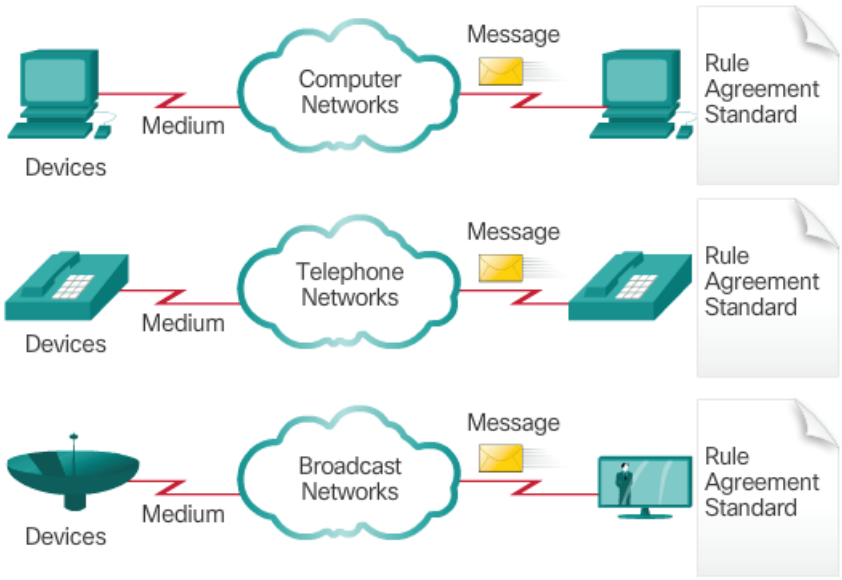
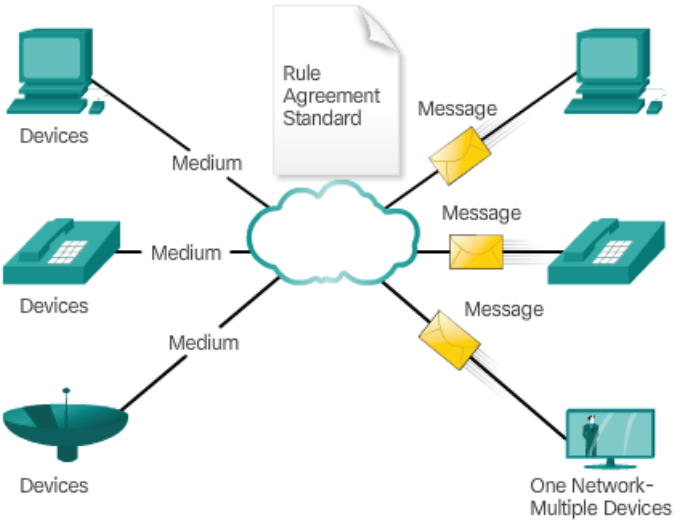


Figure 1-22 Multiple Networks

Each network used different technologies to carry the communication signal. Each network had its own set of rules and standards to ensure successful communication.

The Converging Network (1.3.1.2)

Today, the separate data, telephone, and video networks are converging. Unlike dedicated networks, ***converged networks*** are capable of delivering data, voice, and video between many different types of devices over the same network infrastructure, as shown in Figure 1-23. This network infrastructure uses the same set of rules, agreements, and implementation standards.



Converged data networks carry multiple services on one network.

Figure 1-23 Converged Networks

Lab 1.3.1.3: Researching Converged Network Services

In this lab, you will complete the following objectives:

- Part 1: Survey Your Understanding of Convergence
- Part 2: Research ISPs Offering Converged Services
- Part 3: Research Local ISPs Offering Converged Services
- Part 4: Select Best Local ISP Converged Service
- Part 5: Research Local Company or Public Institution Using Convergence Technologies

Reliable Network (1.3.2)

With our reliance on networks, certain precautions must be taken to ensure that the network functions as designed, even if things go wrong. Networks must be able to expand to meet the increased needs of an organization. The services provided by the network must be secure and provide the quality of service to meet the expectations of the organization.

Network Architecture (1.3.2.1)

Networks must support a wide range of applications and services as well as operate over many different types of cables and devices, which 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 data 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
- Quality of Service (QoS)
- Security

Fault Tolerance (1.3.2.2)

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 impact of a failure, so that the fewest number of devices are affected. It is also built in a way that allows quick recovery when such a failure occurs. These 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.

One way reliable networks provide redundancy is by implementing a *packet-switched network*. Packet switching splits traffic into packets that are routed over a shared network. A single message, such as an email or a video stream, is broken into multiple message blocks, called packets. Each packet has the necessary addressing information of the source and destination of the message. The routers within the network switch the packets based on the condition of the network at that moment. This means that all the packets in a single message could take very different paths to the destination. In Figure 1-24, the user is not aware and is unaffected by the router dynamically changing the route when a link fails.

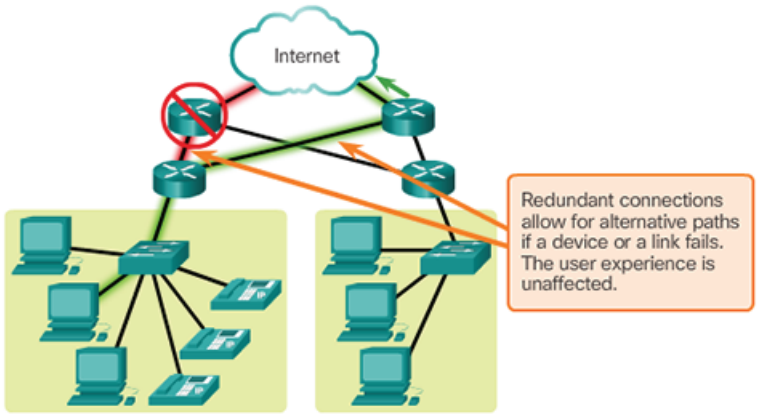


Figure 1-24 Fault Tolerance

This is not the case in circuit-switched networks traditionally used for voice communications. A *circuit-switched network* is one that establishes a dedicated circuit between the source and destination before the users may communicate. If the call is unexpectedly terminated, the users must initiate a new connection.

Scalability (1.3.2.3)

A *scalable network* can expand quickly to support new users and applications without impacting the performance of the service being delivered to existing users. Figure 1-25 shows how a new network can be easily added to an existing network.

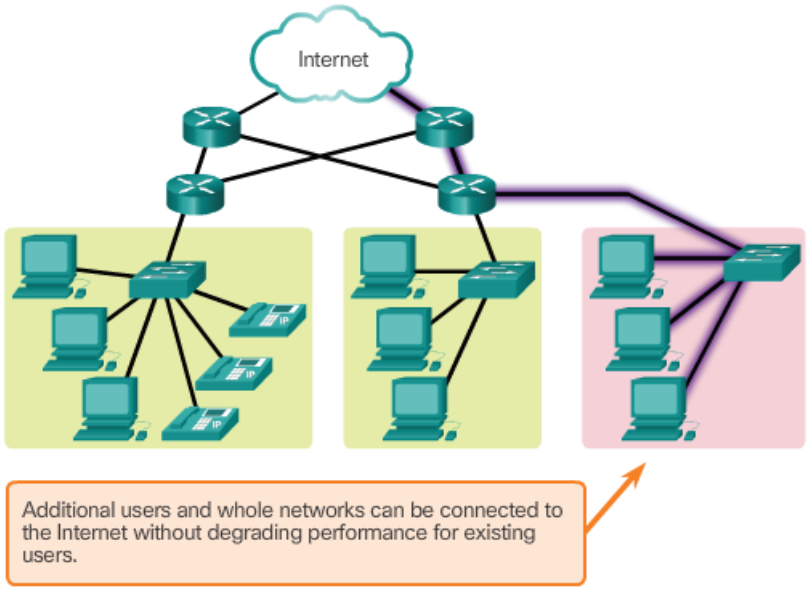


Figure 1-25 Scalability

In addition, networks are scalable because the designers follow accepted standards and protocols. This allows software and hardware vendors to focus on improving products and services without worrying about designing a new set of rules for operating within the network.

Quality of Service (1.3.2.4)

Quality of Service (QoS) is also an ever-increasing requirement of networks today. New applications available to users over internetworks, such as voice and live video transmissions, create higher expectations for the quality of the delivered services. Have you ever tried to watch a video with constant breaks and pauses? As data, voice, and video content continue to converge onto the same network, QoS becomes a primary mechanism for managing congestion and ensuring reliable delivery of content to all users.

Congestion occurs when the demand for bandwidth exceeds the amount available. *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.

When the volume of traffic 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. In Figure 1-26, one user is requesting a web page and another is on a phone call. With a QoS policy in place, the router can manage the flow of data and voice traffic, giving priority to voice communications if the network experiences congestion.

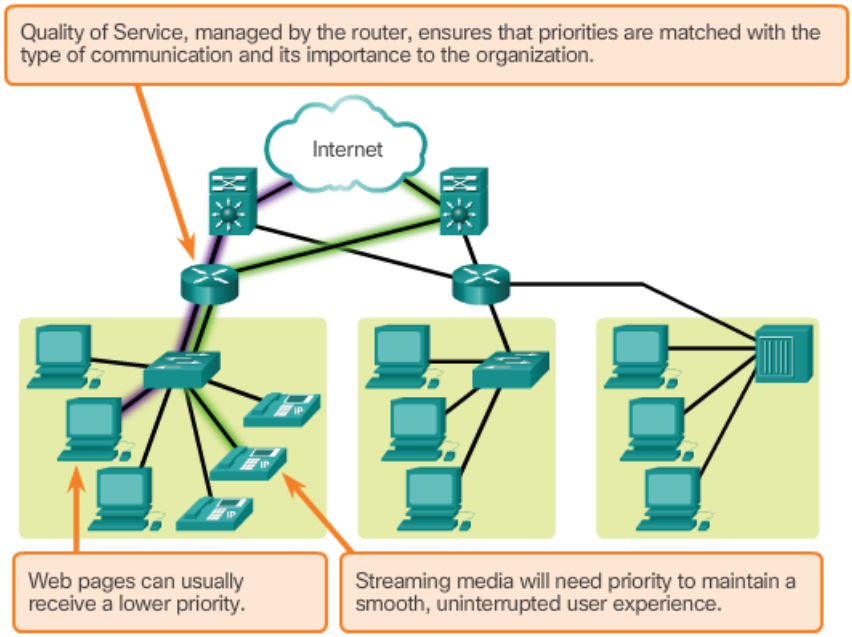


Figure 1-26 Quality of Service (QoS)

Security (1.3.2.5)

The network infrastructure, services, and the data contained on network-attached devices are crucial personal and business assets. There are two types of network security concerns that must be addressed: network infrastructure security and information security.

Securing a network infrastructure includes the physical securing of devices that provide network connectivity, and preventing unauthorized access to the management software that resides on them, as shown in Figure 1-27.

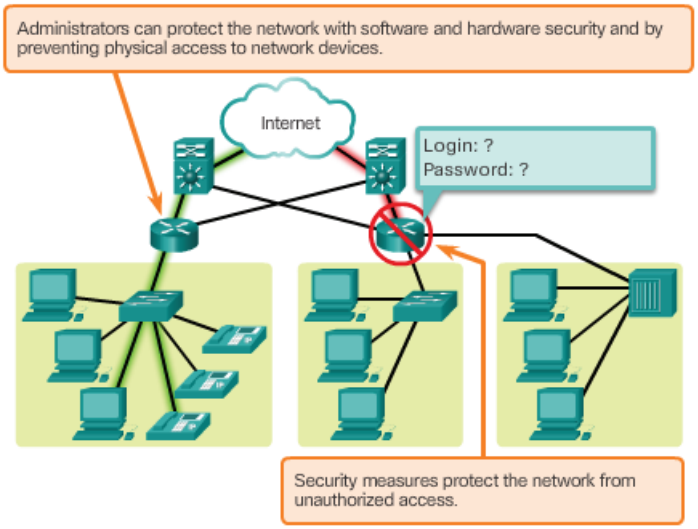


Figure 1-27 Security

Information security refers to protecting the information contained within the packets being transmitted over the network and the information stored on network attached devices. In order to achieve the goals of network security, there are three primary requirements, as shown in Figure 1-28.

Figure 1-28 CIA Triad

- **Confidentiality –** Data confidentiality means that only the intended and authorized recipients can access and read data.
- **Integrity –** Data integrity means having the assurance that the information has not been altered in transmission, from origin to destination.
- **Availability –** Data availability means having the assurance of timely and reliable access to data services for authorized users.

Interactive Graphic

Activity 1.3.2.6: Reliable Networks

Go to the online course to perform this practice activity.

The Changing Network Environment (1.4)

The network environment continues to evolve, providing new experiences and opportunities for end users. The network is now capable of delivering services and applications in a manner that couldn't be imagined years ago.

Network Trends (1.4.1)

Just as the way we work, play, and learn impacts the network, the availability of a robust reliable network has an impact on our daily lives.

New Trends (1.4.1.1)

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 between 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

Bring Your Own Device (1.4.1.2)

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

BYOD is about end users having the freedom to use personal tools to access information and communicate across a business or campus network. With the growth of consumer devices, and the related drop in cost, employees and students can be expected to have some of the most advanced computing and networking tools for personal use. These personal tools include laptops, netbooks, tablets, smartphones, and e-readers. These can be devices purchased by the company or school, purchased by the individual, or both.

BYOD means any device, with any ownership, used anywhere. For example, in the past, a student who needed to access the campus network or the Internet had to use one of the school's computers. These devices were typically limited and seen as tools only for work done in the classroom or in the library. Extended connectivity through mobile and remote access to the campus network gives students tremendous flexibility and more learning opportunities for the student.

Online Collaboration (1.4.1.3)

Individuals 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." Collaboration tools, like Cisco WebEx shown in Figure 1-29, give employees, students, teachers, customers, and partners a way to instantly connect, interact, and achieve their objectives.

Figure 1-29 Cisco WebEx

For businesses, collaboration is a critical and strategic priority that organizations are using to remain competitive. Collaboration is also a priority in education. Students need to collaborate to assist each other in learning, to develop team skills used in the work force, and to work together on team-based projects.

Video Communication (1.4.1.4)

Another trend in networking that is critical to the communication and collaboration effort is video. Video is being used for communications, collaboration, and entertainment. Video calls can be made to and from anywhere with an Internet connection. Consider how many people are now using Skype or FaceTime to communicate with friends and family.

Video conferencing is a powerful tool for communicating with others at a distance, both locally and globally. Video is becoming a critical requirement for effective collaboration as organizations extend across geographic and cultural boundaries. Play the video to view how TelePresence can be incorporated into everyday life and business.

Video

Go to the online course to view this video.

Cloud Computing (1.4.1.5)

Cloud computing is another global trend changing the way we access and store data. Cloud computing allows us to store personal files, even backup our entire hard disk drive on servers over the Internet. Applications such as word processing and photo editing can be accessed using the Cloud.

For businesses, Cloud computing extends IT's capabilities 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.

There are four primary types of Clouds, as shown in Figure 1-30.

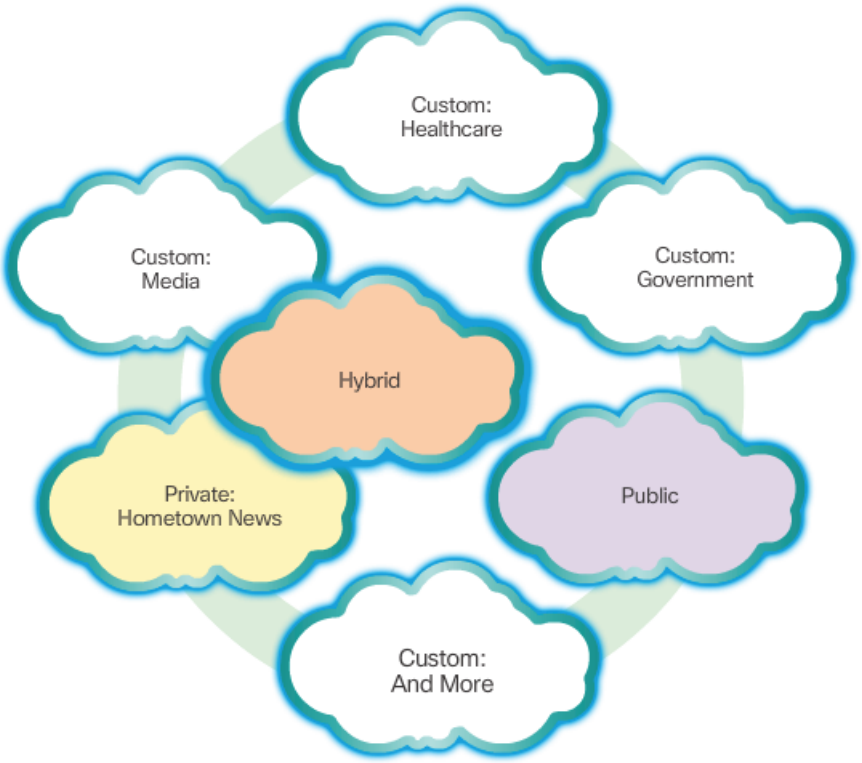


Figure 1-30 Types of Clouds

- *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, although this can be expensive to build and maintain. A private cloud can also be managed by an outside organization with strict access security.
- *Public clouds* – Cloud-based applications and services offered in a public cloud are made available to the general population. Services may be free or are offered on a pay-per-use model, such as paying for online storage. The public cloud uses the Internet to provide services.
- *Hybrid clouds* – A hybrid cloud is made up of two or more clouds (example: part custom, part public), where each part remains a distinctive object, but both 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.
- *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.

Cloud computing is possible because of data centers. A *data center* is a facility used to house computer systems and associated components. A data center can occupy one room of a building, one or more floors, or an entire building. 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. 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.

Networking Technologies for the Home (1.4.2)

Today's home networks are used in every aspect of our daily lives, for entertainment, education, communications, and business.

Technology Trends in the Home (1.4.2.1)

Networking trends are not only affecting the way we communicate at work and at school, but they are also changing just about every aspect of the home, as shown in Figure 1-31.

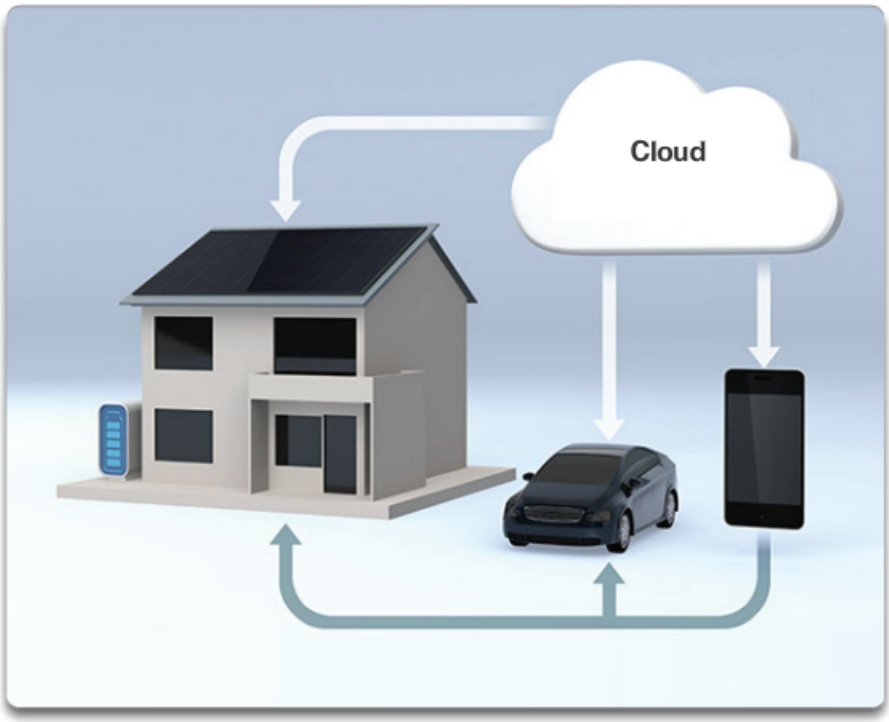


Figure 1-31 Smart Home Technology

The newest home trends include '*smart home technology*.' Smart home technology is technology that is integrated into everyday appliances, allowing them to interconnect with other devices, making them more 'smart' or automated. For example, imagine being able to prepare a dish and place it in the oven for cooking prior to leaving the house for the day. Imagine if the oven was 'aware' of the dish it was cooking and was connected to your 'calendar of events' so that it could determine what time you should be available to eat, and adjust start times and length of cooking accordingly. It could even adjust cooking times and temperatures based on changes in schedule. Additionally, a smartphone or tablet connection allows the user the ability to connect to the oven directly to make any desired adjustments. When the dish is "available," the oven sends an alert message to a specified end user device that the dish is done and warming.

This scenario is not far off in the future. In fact, smart home technology is currently being developed for all rooms within a house. Smart home technology will become more of a reality as home networking and high-speed Internet technology become more widespread. New home networking technologies are being developed daily to meet these types of growing technology needs.

Powerline Networking (1.4.2.2)

Powerline networking is an emerging trend for home networking that uses existing electrical wiring to connect devices, as shown in Figure 1-32.

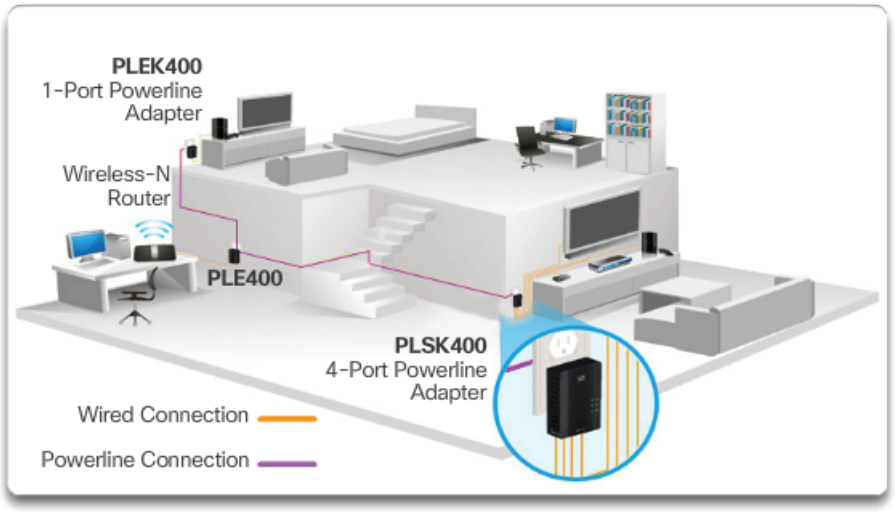


Figure 1-32 Powerline Networking

The concept of "no new wires" means the ability to connect a device to the network wherever there is an electrical outlet. This saves the cost of installing data cables and without any additional cost to the electrical bill. Using the same wiring that delivers electricity, powerline networking sends information by sending data on certain frequencies.

Using a standard powerline adapter, devices can connect to the LAN wherever there is an electrical outlet. Powerline networking is especially useful when wireless access points cannot be used or cannot reach all the devices in the home. Powerline networking is not designed to be a substitute for dedicated cabling in data networks. However, it is an alternative when data network cables or wireless communications are not a viable option.

Wireless Broadband (1.4.2.3)

Connecting to the Internet is vital in smart home technology. DSL and cable are common technologies used to connect homes and small businesses to the Internet. However, wireless may be another option in many areas.

Wireless Internet Service Provider (WISP) is an ISP that connects subscribers to a designated access point or hot spot using similar wireless technologies found in home wireless local area networks (WLANs). WISPs are more commonly found in rural environments where DSL or cable services are not available.

Although a separate transmission tower may be installed for the antenna, it is common that the antenna is attached to an existing elevated structure, such as a water tower or a radio tower. A small dish or antenna is installed on the subscriber's roof in range of the WISP transmitter. The subscriber's access unit is connected to the wired network inside the home. From the perspective of the home user, the setup is not much different than DSL or cable service. The main difference is that the connection from the home to the ISP is wireless instead of a physical cable.

Another wireless solution for the home and small businesses is wireless broadband, as shown in Figure 1-33.

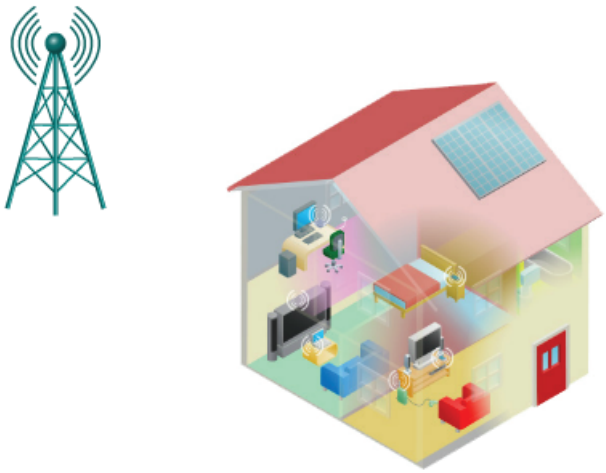


Figure 1-33 Wireless Broadband Service

This uses the same cellular technology used to access the Internet with a smart phone or tablet. An antenna is installed outside the house providing either wireless or wired connectivity for devices in the home. In many areas, home wireless broadband is competing directly with DSL and cable services.

Network Security (1.4.3)

For a network to be entrusted with the communications of personal and business information, that network must be secure.

Security Threats (1.4.3.1)

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 as large as a corporation with thousands of users. The network security that is implemented must take into account the environment as well as the tools and requirements of the network. It must be able to secure data while still allowing for the quality of service that is expected of the network.

Securing a network involves protocols, technologies, devices, tools, and techniques to secure data and mitigate threats. Threat vectors may be external or internal. 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 attacks, also called zero-hour attacks –** an attack that occurs on the first day that a vulnerability becomes known
- **Hacker attacks –** an attack by a knowledgeable person to user devices or network resources
- **Denial of service attacks –** attacks 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 internal users of the network. This can be attributed to lost or stolen devices, accidental misuse by

employees, and in the business environment, even malicious employees. 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.

Security Solutions (1.4.3.2)

No single solution can protect the network from the variety of threats that exist, both internal and external, as shown in Figure 1-34.

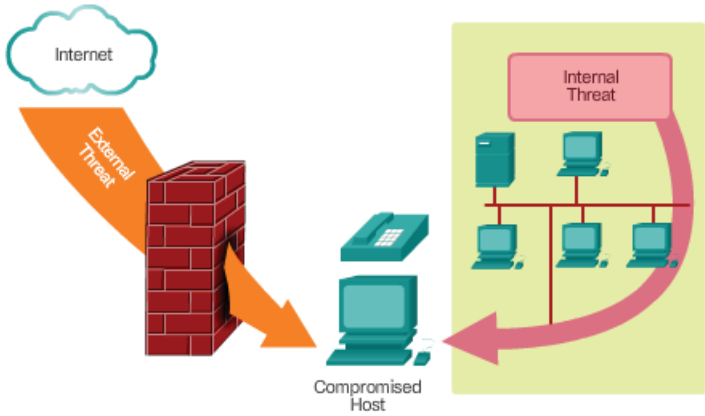


Figure 1-34 Threats to Networks

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.

A home network security implementation is usually rather basic. It is generally implemented on the connecting end devices as well as at the point of connection to the Internet and can even rely on contracted services from the ISP.

In contrast, 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

- **Antivirus and antispyware –** These are used to protect end devices from becoming infected with malicious software.
- **Firewall filtering –** This is used to block unauthorized access to the network. This may include a host-based firewall system that is implemented to prevent unauthorized access to the end device or a basic filtering service on the home router to prevent unauthorized access from the outside world into the network.

In addition to the above, larger networks and corporate networks often have other security requirements:

- **Dedicated firewall systems –** These are used to provide more advanced firewall capabilities that can filter large amounts of traffic with more granularity.
- **Access control lists (ACL) –** These are used to further filter access and traffic forwarding.
- **Intrusion prevention systems (IPS) –** These are used to identify fast-spreading threats, such as zero-day or zero-hour attacks.
- **Virtual private networks (VPN) –** These are used to provide secure access to remote workers.

Network security requirements must take into account the network environment, as well as the various applications, and 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.

Interactive Graphic

Activity 1.4.3.3: Network Security Terminology

Go to the online course to perform this practice activity.

Network Architecture (1.4.4)

[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 in this type of environment, the network must be built upon a standard network architecture.

Cisco Network Architecture (1.4.4.1)

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 ensure the connection of any device across any combination of networks. While ensuring connectivity, it also increases cost efficiency by integrating network security and management and improves business processes. At the foundation of all network architectures, and, in fact, at the foundation of the Internet itself, are routers and switches. Routers and switches transport data, voice, and video communications, as well as allow for wireless access, and provide for security.

Building networks that support our needs of today and the needs and trends of the future starts with a clear understanding of the underlying switching and routing infrastructure. After a basic routing and switching network infrastructure is built, individuals, small businesses, and organizations can grow their network over time, adding features and functionality in an integrated solution.

CCNA (1.4.4.2)

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. Other certifications beyond the Associate are also available, as shown in Figure 1-35.

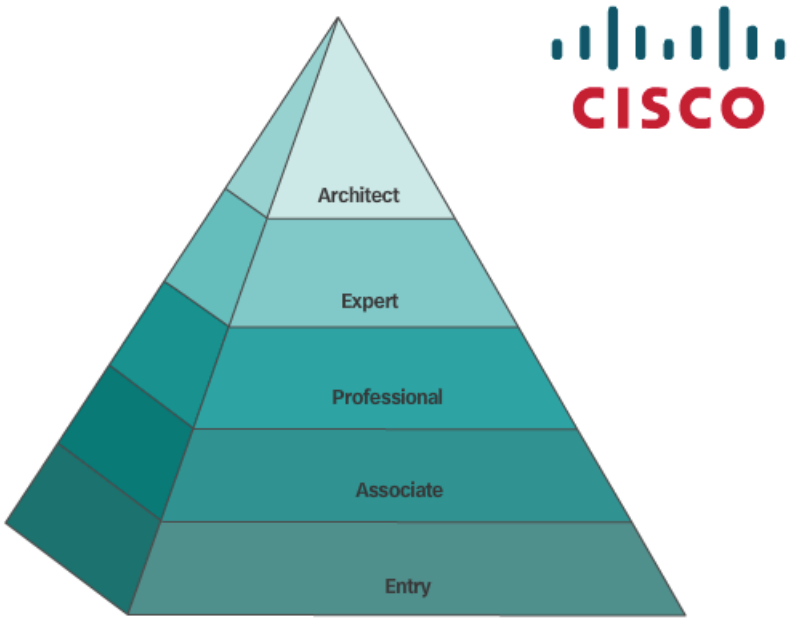


Figure 1-35 Cisco Certification Hierarchy

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. CCNA curriculum also includes basic mitigation of security threats, introduction to wireless networking concepts and terminology, and performance-based skills. This CCNA curriculum includes the use of various protocols, such as Ethernet, VLANs, IPv4, IPv6, Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), 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 toward CCNA certification.

Lab 1.4.4.3: Researching IT and Networking Job Opportunities

In this lab, you will complete the following objectives:

- Part 1: Research Job Opportunities
- Part 2: Reflect on Research

Summary (1.5)

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. You may also refer to the other activities completed in this chapter, including Packet Tracer activities.

Draw a map of the Internet as you see it now. Use the icons presented in the chapter for media, end devices, and intermediary devices.

In your revised drawing, you may wish to include some of the following:

- WANs
- LANs
- Cloud computing
- Internet Service Providers (tiers)

Save your drawing in hard-copy format. If it is an electronic document, save it to a server location provided by your instructor. Be prepared to share and explain your revised work in class.

Warriors of the Net (1.5.1.2)

An entertaining resource to help you visualize networking concepts is the animated movie "Warriors of the Net" by TNG Media Lab. Before viewing the video, there are a few things to consider. In terms of concepts you have learned in this chapter, think about when, in the video, you are on the LAN, on the WAN, on the intranet, on the Internet, and what are end devices versus intermediate devices.

Although all animations often have simplifications in them, there is one outright error in the video. About 5 minutes in, the statement is made "What happens when Mr. IP doesn't receive an acknowledgment, he simply sends a replacement packet." This is not a function of the Layer 3 Internet Protocol, which is an "unreliable," best effort delivery protocol, but rather a function of the transport layer TCP protocol. IP is explained in Chapter 6 and TCP is explained in Chapter 9.

Download the movie from http://www.warriorsofthe.net

Conclusion (1.5.1.3)

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, work, and interests.

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, 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 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. 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 Introduction to Networks v5.1 Lab Manual (ISBN 9781587133534). 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 1.1.1.8: Researching Network Collaboration Tools

Lab 1.3.1.3: Researching Converged Network Services

Lab 1.4.4.3: Researching IT and Networking Job Opportunities

Packet Tracer Activities

Packet Tracer 1.2.4.4: Help and Navigation Tips

Packet Tracer 1.2.4.5: Network Representation

Check Your Understanding Questions

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

1. What is a group of web pages that groups of individuals can edit and view together called?

   A. Podcasting
   B. Wiki
   C. Weblog (blog)
   D. Instant messaging
   E. Access point
   F. TelePresence endpoint

2. Which of the following are disadvantages of peer-to-peer networking? (Choose two.)

   A. Expensive to set up and maintain
   B. No centralized administration
   C. Complex configuration
   D. Scalability

3. Which devices would be considered end devices on a network? (Choose four.)

   A. Switch
   B. Printer
   C. IP phone

D. Server
E. Tablet computer
F. Wireless access point

4. What type of information would be found on a logical topology diagram?

A. Location of departmental printer
B. Length and type of all cable runs
C. IP addressing scheme
D. Location of departmental switch

5. What is a network infrastructure that provides access to other networks over a wide geographic area?

A. LAN
B. WLAN
C. MAN
D. WAN
E. SAN

6. Which of the following are business-class Internet connection technologies normally supplied by a service provider? (Choose two.)

A. Leased lines
B. Broadband cable
C. Metro Ethernet
D. Mobile services
E. Cellular

7. Which technology would be best to provide a home user with a high-speed, always-on Internet connection?

A. Dial-up
B. DSL
C. Satellite
D. Cellular

8. What is a converged network?

A. A network that makes use of both fiber-optic and copper connections
B. A network where voice, video, and data move over the same infrastructure
C. A network that makes use of both wired and wireless technology
D. A network that makes use of both satellite and terrestrial connections to move data

9. What is a fault-tolerant network?

   A. A network that can provide priority treatment of voice and video traffic
   B. A network that offers secure transactions
   C. A network that can reroute traffic in case of device failure
   D. A network that is incapable of failing

10. Which type of traffic must receive the highest priority from QoS?

   A. Web traffic
   B. Email
   C. VoIP
   D. Order processing

11. What are the primary requirements of information security? (Choose three.)

   A. Confidentiality
   B. Integrity
   C. Availability
   D. QoS
   E. Scalability

12. In which scenario would the use of a WISP be recommended?

   A. an Internet cafe in a city
   B. a farm in a rural area without wired broadband access
   C. any home with multiple wireless devices
   D. an apartment in a building with cable access to the Internet

13. List four current network trends.

14. Describe some common everyday uses of a modern-day network.

15. In what ways has the network transformed the way we learn?

This page intentionally left blank

Index

Symbols

/8 subnets, creating, 425-427
/16 subnets, creating, 421-424
/25 subnets, creating, 414-416
/26 subnets, creating, 418-421

A

AAA (authentication, authorization, accounting), 557-558
access attacks, 552-553
access control list (ACL), 44
access methods
  for Cisco IOS
    terminal emulation programs, 59-61
    types of, 58-59
  for messages, 98
  in multi-access networks, 193-194
    CSMA/CA, 196
    CSMA/CD, 194-195
  for network resources, 127
    data link addresses, 128-130
    devices on remote networks, 133-134
    devices on same network, 130-132
    Media Access Control (MAC). See Media Access Control (MAC)
    network addresses, 127-128
access technologies. *See* connections
accounting, 557-558
acknowledgement, 98
address resolution, 390
Address Resolution Protocol (ARP), 108, 223
  performance and security issues, 264-265
  purpose, 250-251
  removing ARP table entries, 263
  resolving IP addresses to MAC addresses, 251-252
    for remote communication, 259-263
    reply messages, 256-259
    request messages, 252-256
  viewing ARP table entries, 263-264
addresses
  data link addresses, 128-130, 199-201
    devices on remote networks, 133-134
    devices on same network, 132
  IP addresses. *See* IP addresses
  MAC addresses. *See* MAC addresses
  network addresses, 127-128
    devices on remote networks, 133
    devices on same network, 130-132
  next-hop address, 295
addressing schemes, 440-443
Advanced Research Projects Agency Network (ARPANET), 106
adware, 42
American National Standards Institute (ANSI), 149
antispyware software, 43
antivirus software, 43
anycast IPv6 addresses, 364
application filtering, 558
application layer (OSI model), 120
  designing small networks, 540-541
  purpose, 502-503
application layer (TCP/IP model) protocols, 502-503
  client-server model, 506
  email protocols, 513-516
  file sharing services, 525-528
  IP addressing services, 516-525
  list of, 504-506
  peer-to-peer model, 507-509
  web protocols, 510-512
applications
  designing small networks, 539-541
  peer-to-peer applications, 507-509
  port numbers, 459, 470, 472-473
  TCP applications, 491
  UDP applications, 492
ARP cache, 251
arp command, 587-588
ARP table, 251
  removing entries, 263
  viewing entries, 263-264

assigned multicast address, 385-386
assigning IPv4 addresses, 356
asymmetric switching, 244
attacks
  access attacks, 552-553
  Denial of Service (DoS) attacks, 554-556
  malware, 550-551
  mitigation of, 556-559
  reconnaissance attacks, 551-552
authentication, 557-558
authorization, 557-558
automatic medium-dependent interface crossover (auto-MDIX), 246
autonegotiation, 244
auxiliary (AUX) port, 59
availability (of data), 35

B

backing up device configuration
  from text files, 74-77, 568
  with TFTP, 569
  with USB flash drive, 570-571
bandwidth, 33, 152-153, 244-246
banner messages, 72
banner motd command, 72
best-effort delivery, 279-280
binary numbers
  hexadecimal conversion, 216-218, 361
  in IPv4 addresses, 327-330
    binary to decimal conversion, 331-333
    decimal to binary conversion, 334-337
    positional notation, 330-331
blogs, 6
Bluetooth, 177
Bootstrap Protocol (BOOTP), 107, 505
bootup process, 303-307
bring your own device (BYOD), 35-36
broadcast, 99
  addresses, 342-344
  ARP performance issues, 264-265
  communication method, 348-349
  domains, 405-406
  MAC addresses, 223-224
browsers, opening web pages, 510-511
burned-in address (BIA), 220
bus topology, 191

C

cable Internet connections, 26
cabling. *See* copper cable; fiber-optic cable
Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA), 196
Carrier Sense Multiple Access/Collision Detection (CSMA/CD), 194-195
cd command, 566
cellular Internet connections, 27
central processing unit (CPU), 297
certification hierarchy, 45
changing running configuration file, 74
channel, 93
CIA triad, 34
circuit-switched networks, 32
Cisco Certified Network Associate (CCNA), 45-46
Cisco Discovery Protocol (CDP), 588-591
Cisco Internetwork Operating System (CIOS), 54, 56
  access methods
    terminal emulation programs, 59-61
    types of, 58-59
  commands. *See also names of individual commands*
    help features, 65-66
    Hotkeys and shortcuts, 66-67
    structure of, 64
    syntax, 64-65
  device configuration
    backing up with TFTP, 569
    backing up with USB flash drive, 570-571
    banner messages, 72
    capturing to text file, 74-77, 568
    changing running configuration file, 74
    hostnames, 68-70
    interfaces and ports, 79-81
    IP addresses, 78-79, 81-85
    passwords, 70-72
    restoring configuration file, 77, 568-569
    restoring with TFTP, 570
    restoring with USB flash drive, 571
    saving running configuration file, 72-73
    verifying connectivity, 85-86
  modes of operation, 61
    global configuration mode, 62
    primary command modes, 61-62
    switching among, 62-63

purpose, 57
routers. *See* routers
troubleshooting devices, 600-601
Cisco security appliances, 559
classful addressing, 353-354
classless addressing, 355-356
Classless Inter-Domain Routing (CIDR), 355
classless subnetting, 410-413
clients, 9, 490
client-server model, 506
cloud computing, 37-39
coaxial cable (coax), 160-161
collaboration, 36-37
collaboration tools, 6
collision fragment, 215
command-line interface (CLI), 55-56
access methods
terminal emulation programs, 59-61
types of, 58-59
commands. ***See also names of individual commands***
help features, 65-66
Hotkeys and shortcuts, 66-67
structure of, 64
switching among modes (Cisco IOS), 62-63
syntax, 64-65
communication. ***See also*** **messages**
data access, 127
data link addresses, 128-130
devices on remote networks, 133-134
devices on same network, 130-132
network addresses, 127-128
duplex mismatch, troubleshooting, 598-600
full-duplex, 192
half-duplex, 192
network usage for, 5-6
rules
establishing, 94
message delivery options, 98-100
message encoding, 94-96
message formatting and encapsulation, 96-97
message size, 97
message timing, 98
network protocols, 101-103
protocol interaction, 103-104
protocol suites, 100-101. See also protocol suites
terminology, 93
standards organizations, 114
electronics and communications standards, 116-118
Internet standards, 115-116
open standards, 114-115
TCP process
establishing connection, 477-478
server processes, 474-477
terminating session, 478-481
three-way handshake, 481-482
UDP process
client processes, 490
datagram reassembly, 489
overhead versus reliability, 488-489
server processes, 490
compressed format, 362
confidentiality (of data), 35
configuration
devices
backing up with TFTP, 569
backing up with USB flash drive, 570-571
banner messages, 72
capturing to text file, 74-77, 568
changing running configuration file, 74
hostnames, 68-70
interfaces and ports, 79-81
IP addresses, 78-79, 81-85
passwords, 70-72
restoring configuration file, 77, 568-569
restoring with TFTP, 570
restoring with USB flash drive, 571
saving running configuration file, 72-73
verifying connectivity, 85-86
global configuration mode, 62
routers
default gateway, 314-316
DHCPv6, 376-377
dynamic link-local addresses, 380-381
initial settings, 308-311
interfaces, 311-314
SLAAC, 374-375
static IPv6 unicast addresses, 371-373
static link-local addresses, 381-382
verifying IPv6 configuration, 382-384
SSH, 563
vulnerabilities, 549

configure terminal command, 63, 69
congestion, 33, 487-488
connectionless, 278-279
connection-oriented, 465
connections
device connectivity, verifying, 85-86
to Internet, 25-26
for businesses, 27-28
for homes and small offices, 26-27
IP connectivity
local network testing, 394
local stack testing, 392-393
remote network testing, 395
traceroute (tracert), 395-396
verifying, 388-392
in physical layer (OSI model)
NICs, 145-146
types of, 144-145
routers, 300-301
TCP connectivity
establishing connection, 477-478
terminating session, 478-481
three-way handshake, 481-482
verifying
arp command, 587-588
debug command, 592-594
ipconfig command, 585-587
ping command, 572-575
show arp command, 583
show cdp neighbors command, 588-591
show interfaces command, 582
show ip route command, 583-584
show running-config command, 581-582
show version command, 584-585
terminal monitor command, 594
traceroute command, 577-580
connectors
fiber-optic cable, 172-174
UTP cabling, 165-166
console, 58
content addressable memory (CAM) table. *See* MAC address table
contention-based access, 193, 214
CSMA/CA, 196
CSMA/CD, 194-195
controlled access, 193
converged networks, 28-30
conversations
multiplexing, 460-461, 469
tracking, 458
copper cable, 148, 155-158
coaxial cable (coax), 160-161
fiber-optic cable versus, 175-176
safety issues, 161-162
STP cabling, 159-160
troubleshooting, 598-600
UTP cabling, 158-159, 163-168
connectors, 165-166
properties of, 163
standards, 164-165
testing, 167-168
types of, 166-167
copy running-config startup-config command, 73
copy startup-config running-config command, 74
crosstalk, 156
custom clouds, 38
cut-through switching, 242-243
cyclic redundancy check (CRC), 216

D

data access, 127
data link addresses, 128-130
devices on remote networks, 133-134
devices on same network, 130-132
network addresses, 127-128
data centers, 39
data encapsulation. *See* encapsulation
Data field (Ethernet frames), 216
data interception and theft, 42
data link addresses, 128-130
devices on remote networks, 133-134
devices on same network, 132
data link layer (OSI model), 120
Ethernet in, 211-213
frames, 196-197
addresses, 199-201
fields, 198-199
protocols, 201-202
interaction with physical layer, 143
Media Access Control (MAC)
encapsulation and, 182-183
full-duplex, 192
half-duplex, 192

in multi-access networks, 193-196
purpose, 185-186
topologies. See topologies
purpose, 179-181
standards, 184
sublayers, 181
data loss, 547
data transfer. *See* communication
debug command, 592-594
decapsulation (de-encapsulation), 96, 126, 276
decimal numbers
binary to decimal conversion, 331-333
decimal to binary conversion, 334-337
hexadecimal conversion, 216-218, 361
positional notation, 330-331
decoding messages, 94-96
dedicated firewalls, 44
dedicated leased lines, 28
default gateway, 133-134. *See also* routers
ARP role in communication, 259-263
configuration, 314-316
in host routing, 289-290
sending frames to, 236-240
troubleshooting, 602-603
delimiting characters, 72
denial of service attacks, 42
Denial of Service (DoS) attacks, 554-556
designing small networks
applications, 539-541
device selection, 535-536
IP addressing, 536-537
protocols, 541-542
real-time traffic support, 542-544
redundancy, 537-538
scaling for growth, 544-546
topologies, 534-535
traffic management, 539
destination, 93
destination MAC address, 250
Destination MAC Address field (Ethernet frames), 215
devices
configuration
backing up with TFTP, 569
backing up with USB flash drive, 570-571
banner messages, 72
capturing to text file, 74-77, 568
changing running configuration file, 74
hostnames, 68-70
interfaces and ports, 79-81
IP addresses, 78-79, 81-85
passwords, 70-72
restoring configuration file, 77, 568-569
restoring with TFTP, 570
restoring with USB flash drive, 571
saving running configuration file, 72-73
verifying connectivity, 85-86
Ethernet identity, 219-220
security, 559-560
endpoint security, 559
executive timeouts, 562
passwords, 560-562
SSH configuration, 563
selecting for small networks, 535-536
troubleshooting
end devices, 601-602
IOS devices, 600-601
dial-up Internet connections, 27
digital subscriber line (DSL), 27, 28
dir command, 565
directed broadcast, 348
disable command, 62
dispersion, 172
disruption of service, 548
Domain Name System (DNS), 83, 107, 505
hierarchy, 520-521
message format, 519-520
nslookup command, 521-522
resolution steps, 516-519
troubleshooting, 604-605
dotted decimal notation, 328
dual stack, 358
duplex mismatch, troubleshooting, 598-600
Duplex Multimode LC connectors, 173
duplex settings for switches, 244-246
Duplicate Address Detection (DAD), 391
dynamic configuration
global unicast address (GUA)
DHCPv6, 376-377
SLAAC, 374-375
link-local addresses, 380-381
Dynamic Host Configuration Protocol (DHCP), 83, 107, 505
IPv4 address assignment, 345-346
IPv6 address assignment, 376-377

messages, 524-525
purpose, 522-524
dynamic IPv4 address assignment, 345-346
dynamic ports, 472

E

education, network usage for, 5
electrical threats, 548
electromagnetic interference (EMI), 156
Electronic Industries Alliance (EIA), 117
electronics and communications standards, 116-118
email protocols, 513-516
email servers, 10
employee network utilization studies, 545-546
enable command, 62
enable mode. *See* privileged executive (EXEC) mode
enable secret command, 71
encapsulation, 96-97, 123
Ethernet MAC sublayer, 214
example, 126
Internet Protocol (IP), 277
IPv6 packets, 284-286
Media Access Control (MAC), 182-183
message segmentation, 123-125
in network layer, 275
protocol data unit (PDU), 125-126
encoding, 94-96, 150-151
encrypting passwords, 72
end command, 63
end devices, 9, 13-14, 601-602
endpoint security, 559
end-to-end connectivity tests, 86
Enhanced Interior Gateway Routing Protocol (EIGRP), 108
entertainment, network usage for, 7
environmental threats, 548
ephemeral ports, 472
erase startup-config command, 74
escalating problems, 596
Ethernet, 104, 108, 211
ARP. *See* Address Resolution Protocol (ARP)
crossover cables, 167
frames
fields, 215-216
filtering, 229-231
forwarding, 240-244
learning MAC addresses, 227-229
processing, 220-221
sending to default gateway, 236-240
history, 214-215
MAC addresses, 216
broadcast, 223-224
device identity, 219-220
devices on remote networks, 133-134
devices on same network, 132
frame processing, 220-221
hexadecimal conversion, 216-218
multicast, 224-226
representations, 221-222
unicast, 222-223
MAC sublayer, purpose, 212-214
in OSI model, 211-213
straight-through cables, 167
switches. *See* switches
Ethernet II, 215
Ethernet WAN, 28
EtherType field (Ethernet frames), 216
executive timeouts, 562
exit command, 63
expectational acknowledgement, 484
experimental addresses, 353
extended star topology, 190
Extended Unique Identifier (EUI-64), 377-380
extranet, 24-25

F

fast-forward switching, 243
fault tolerance, 31-32
fiber-optic cable, 148, 168
components, 170-171
connectors, 172-174
copper cable versus, 175-176
properties of, 168-169
testing, 174-175
troubleshooting, 598-600
types of, 171-172
file servers, 10
file sharing services, 525-528
file systems

router file systems
flash file system, 565-566
NVRAM file system, 566-567
viewing, 564-565
switch file systems, 567
File Transfer Protocol (FTP), 107, 505, 525-526
filtering Ethernet frames, 229-231
firewall filtering, 43
firewalls, 558-559
firmware, 56
flash drives. ***See*** **Universal Serial Bus (USB) flash drives**
flash file system, 565-566
flow control, 98
congestion, 487-488
window size, 485-487
formatting messages, 96-97
formulas for subnetting, 416-418
forwarding
frames, 240-241
cut-through switching, 242-243
memory buffering, 243-244
store-and-forward switching, 241-242
in host routing, 288
in router routing, 291-292
fragmentation, 281
fragment-free switching, 243
Frame Check Sequence (FCS) field (Ethernet frames), 216
frames, 96
in data link layer, 196-197
addresses, 199-201
fields, 198-199
protocols, 201-202
Ethernet
fields, 215-216
filtering, 229-231
forwarding, 240-244
learning MAC addresses, 227-229
processing, 220-221
sending to default gateway, 236-240
size of, 97
full-duplex, 192, 244, 598-600

G

global configuration mode, 62
global routing prefix, 370, 444
global unicast address (GUA), 366
dynamic configuration
DHCPv6, 376-377
SLAAC, 374-375
EUI-64 process, 377-380
static configuration, 371-373
structure of, 369-371, 444
globalization of networks, 5
graphical user interface (GUI), 55-56

H

hacker attacks, 42
half-duplex, 192, 244, 598-600
hardware, 55
router hardware, 296-297, 299-300
connections and ports, 300-301
CPU and OS, 297
LAN and WAN interfaces, 301-302
memory, 297-298
threats, 548
help features of Cisco IOS command, 65-66
hexadecimal numbers, 216-218, 361
history
of Ethernet, 214-215
of Internet, 4-5
home networks, 8, 9
trends
powerline networking, 40-41
smart home technology, 39-40
wireless broadband, 41-42
host addresses, 342-344
host portion, 338
hostname command, 69
hostnames, 68-70
hosts, 9
communication methods, 346-347
broadcast transmission, 348-349
multicast transmission, 349-350
unicast transmission, 347-348
default gateway configuration, 314-315
dynamic IPv4 address assignment, 345-346
routing
default gateway, 289-290
forwarding decisions, 288
routing tables, 290-291
static IPv4 address assignment, 345

for subnets
calculating, 424-425
requirements, 428
Hotkeys, 66-67
hub-and-spoke topology, 187
human network (globalization), 5
hybrid clouds, 38
hybrid topology, 188
Hypertext Markup Language (HTML), 510-511
Hypertext Transfer Protocol (HTTP), 104, 107, 505
HTML and, 510-511
HTTPS and, 512
Hypertext Transfer Protocol Secure (HTTPS), 505, 512

I

identity theft, 42, 547
in-band router interfaces, 301-302
information security, 34
information theft, 547
initial sequence number (ISN), 483
Institute of Electrical and Electronics Engineers (IEEE), 117, 149
integrated service router (ISR), 144
integrity (of data), 35
interface command, 85
interface drivers, 108
interface ID, 370, 377-380, 444
interfaces, 18
device configuration, 79-81
for operating systems, 55-56
routers, 301-302, 311-314
troubleshooting, 598-600
verifying, 591-592
intermediary devices, 14-15
International Organization for Standardization (ISO), 149
International Telecommunications Union (ITU), 149
International Telecommunications Union-Telecommunication Standardization Sector (ITU-T), 118
Internet, 8, 9, 23-24
connection types, 25-26
for businesses, 27-28
for homes and small offices, 26-27
history, 4-5
internet versus, 24
internet, Internet versus, 24
Internet Architecture Board (IAB), 115
Internet Assigned Numbers Authority (IANA), 116, 356
Internet Control Message Protocol (ICMP), 108, 388-392
Internet Corporation for Assigned Names and Numbers (ICANN), 116
Internet Engineering Task Force (IETF), 116
Internet Message Access Protocol (IMAP), 107, 505, 515-516
Internet Protocol (IP), 104, 108. ***See also*** **IP addresses**
characteristics, 277-278
best-effort delivery, 279-280
connectionless, 278-279
media independent, 280-281
encapsulation, 277
Internet Research Task Force (IRTF), 116
Internet service provider (ISP), 26
Internet Society (ISOC), 115
Internet standards, 115-116
intranet, 24-25
intrusion prevention system (IPS), 44
ip address command, 85
IP addresses
application layer protocols, 516-525
designing small networks, 536-537
device configuration, 78-79, 81-85
automatic configuration, 83-85
manual configuration, 81-83
SVI configuration, 85
devices on remote networks, 133
devices on same network, 131
IPv4 addresses. *See* IPv4 addresses
IPv6 addresses. *See* IPv6 addresses
MAC addresses versus, 247-249
parts of, 131
resolving to MAC addresses, 251-252
ARP reply messages, 256-259
ARP request messages, 252-256
for remote communication, 259-263
troubleshooting

on default gateways, 602-603
on end devices, 601-602
on IOS devices, 600-601
verifying connectivity
ICMP, 388-392
local network testing, 394
local stack testing, 392-393
remote network testing, 395
traceroute (tracert), 395-396
IP telephony, 544
ipconfig command, 85, 221-222, 585-587
default gateway troubleshooting, 603
DNS troubleshooting, 604-605
end device troubleshooting, 602
IPv4 addresses, 78
assigning, 356
binary to decimal conversion, 331-333
classful addressing, 353-354
classless addressing, 355-356
decimal to binary conversion, 334-337
dynamic assignment to host, 345-346
experimental addresses, 353
host communication methods, 346-347
broadcast transmission, 348-349
multicast transmission, 349-350
unicast transmission, 347-348
limitations, 357-358
link-local address, 353
logical AND operations, 340-341
loopback addresses, 352
network, host, broadcast addresses, 342-344
network and host portions, 338
positional notation, 330-331
prefix length, 341-342
private addresses, 350-352
public addresses, 350-352
representations, 327-330
static assignment to host, 345
subnet mask, 338-340
subnetting
/8 subnets, creating, 425-427
/16 subnets, creating, 421-424
addressing schemes, 440-443
broadcast domains, 405-406
classless subnetting, 410-413
formulas for, 416-418
four subnets, creating, 418-421
host calculations, 424-425
host requirements, 428
limitations, 432-434
network requirements, 428-432
octet boundary, 408-410
purpose, 407-408
two subnets, creating, 414-416
VLSM, 434-440
TEST-NET address, 353
transition from, 358-359
IPv4 packets
header fields, 281-283
limitations, 283
router routing table
directly connected entries, 293-294
example, 292-293
next-hop address, 295
remote network entries, 294-296
IPv6 addresses
multicast addresses
assigned, 385-386
solicited-node, 387
prefix length, 365
purpose, 283-284, 357-358
representations, 360-363
subnetting
example allocation, 446-448
global unicast address (GUA), 444
with subnet ID, 445-446
transition to, 358-359
types of, 364
unicast addresses, 365-367
DHCPv6, 376-377
EUI-64 process, 377-380
link-local addresses, 367-368, 380-382
SLAAC, 374-375
static configuration, 371-373
structure of, 369-371
verifying configuration, 382-384
IPv6 packets
encapsulation, 284-286
header fields, 286-287

J

jumbo frame, 215

K

kernel, 55

L

latency, 153
Layer 2 addresses. *See* data link addresses
learning, network usage for, 5
limited broadcast, 348
line command, 63, 71
link-local IPv4 address, 353
link-local IPv6 address, 366, 367-368
dynamic configuration, 380-381
static configuration, 381-382
local area network (LAN), 20, 22
data link layer protocols, 201-202
router interfaces, 301-302
switches. *See* switches
testing connections, 394
topologies, 190-191
local stack, 392-393
logical addresses. *See* IP addresses
logical AND operations, 340-341
Logical Link Control (LLC), 181, 212
logical topologies, 186, 189-190
logical topology diagrams, 19
login command, 71
loopback addresses, 352
loopback interface, 288, 574
Lucent Connector (LC) Simplex Connector, 173

M

MAC address table, 226-227
on connected switches, 231-236
filtering frames, 229-231
learning addresses, 227-229
sending frames to default gateway, 236-240
MAC addresses, 216
broadcast, 223-224
device identity, 219-220
devices on remote networks, 133-134
devices on same network, 132
frame processing, 220-221
hexadecimal conversion, 216-218
IP addresses versus, 247-249
multicast, 224-226
representations, 221-222
resolving IP addresses to, 251-252
ARP reply messages, 256-259
ARP request messages, 252-256
for remote communication, 259-263
unicast, 222-223
maintenance threats, 548
malware, 550-551
Manchester encoding, 150
maximum transmission unit (MTU), 280
media (for networks), 15-16, 79-81
bandwidth, 152-153
coaxial cable (coax), 160-161
comparison of copper and fiber-optic cable, 175-176
copper cable, 155-158
fiber-optic cable, 168-175
safety issues, 161-162
STP cabling, 159-160
throughput, 153-154
types of, 148, 154-155
UTP cabling, 158-159, 163-168
wireless media, 176-178
Media Access Control (MAC), 181. *See also* MAC addresses
encapsulation and, 182-183
Ethernet in, 212-214
full-duplex, 192
half-duplex, 192
in multi-access networks, 193-194
CSMA/CA, 196
CSMA/CD, 194-195
purpose, 185-186
topologies, 185
LAN topologies, 190-191
logical topologies, 186
physical topologies, 186
WAN topologies, 187-190
media independent, 280-281
medium to large network, 8, 9
memory, 297-298
memory buffering on switches, 243-244
mesh topology, 187
messages. *See also* communication
ARP replies, 256-259
ARP requests, 252-256
communication terminology, 93

delivery options, 98-100
DHCP messages, 524-525
DNS message format, 519-520
encapsulation, 96-97, 123
example, 126
protocol data unit (PDU), 125-126
segmentation, 123-125
encoding, 94-96
formatting, 96-97
protocol requirements, 94
size of, 97
timing, 98
metropolitan area network (MAN), 21
modes of operation (Cisco IOS), 61
global configuration mode, 62
primary command modes, 61-62
switching among, 62-63
modulation, 151
multi-access networks, access control methods, 193-194
CSMA/CA, 196
CSMA/CD, 194-195
multicast, 99
communication method, 349-350
IPv6 addresses, 364
assigned, 385-386
solicited-node, 387
MAC addresses, 224-226
multicast group/client, 350
multimode fiber (MMF), 172
multiplexing, 124, 460-461, 469

N

neighbor advertisement (NA) message, 389-392
neighbor solicitation (NS) message, 389-392
netstat command, 473-474
Network Address Translation 64 (NAT64), 359
Network Address Translation (NAT), 108, 283, 351
network addresses, 127-128
devices on remote networks, 133
devices on same network, 130-132
IPv4, 342-344
network architecture, 30-31, 44-45
network baseline, establishing, 575-577
network interface card (NIC), 18, 145-146
network layer (OSI model), 120
protocols, 276
IP characteristics, 277-281
IPv4 packets, 281-283
IPv6 packets, 283-287
purpose, 275-276
routers
bootup process, 303-307
computer hardware, 296-297, 299-300
connections and ports, 300-301
CPU and OS, 297
default gateway configuration, 314-316
initial settings configuration, 308-311
interface configuration, 311-314
LAN and WAN interfaces, 301-302
memory, 297-298
routing
default gateway, 289-290
directly connected routing table entries, 293-294
host forwarding decisions, 288
host routing tables, 290-291
IPv4 router routing table, 292-293
next-hop address, 295
remote network routing table entries, 294-296
router forwarding decisions, 291-292
network operating systems, 54
Cisco IOS. *See* Cisco Internetwork Operating System (CIOS)
purpose, 57
network portion, IPv4 addresses, 338
network protocols, 101-103
networks
client/server networks, 9-10
communication. *See* communication
components, 11-13
end devices, 13-14
intermediary devices, 14-15
media, 15-16
converged networks, 28-30
daily usage, 4-7
for communication, 5-6
for entertainment, 7
human network (globalization), 5
Internet history, 4-5
for learning, 5
in workplace, 6-7

designing small networks
applications, 539-541
device selection, 535-536
IP addressing, 536-537
protocols, 541-542
real-time traffic support, 542-544
redundancy, 537-538
scaling for growth, 544-546
topologies, 534-535
traffic management, 539
extranet, 24-25
Internet. *See* Internet
intranet, 24-25
peer-to-peer networks, 10-11, 507
protocols. *See* protocols
reliability, 30
fault tolerance, 31-32
network architecture, 30-31
Quality of Service (QoS), 32-33
scalability, 32
security, 33-35
representations, 17-20
security
access attacks, 552-553
attack mitigation, 556-559
Denial of Service (DoS) attacks, 554-556
malware, 550-551
physical security, 548
reconnaissance attacks, 551-552
solutions, 43-44
threat types, 42-43
threats, 547-548
vulnerabilities, 548-550
sizes, 8-9
subnetting requirements, 428-432
testing and verification
arp command, 587-588
debug command, 592-594
establishing network baseline, 575-577
ipconfig command, 585-587
ping command, 572-575
show arp command, 583
show cdp neighbors command, 588-591
show interfaces command, 582
show ip interface brief command, 591-592
show ip route command, 583-584
show running-config command, 581-582
show version command, 584-585
terminal monitor command, 594
traceroute command, 577-580
trends, 35
bring your own device (BYOD), 35-36
cloud computing, 37-39
collaboration, 36-37
powerline networking, 40-41
smart home technology, 39-40
video communication, 37
wireless broadband, 41-42
troubleshooting
cables and interfaces, 598-600
default gateways, 602-603
DNS issues, 604-605
end device IP addresses, 601-602
IOS device IP addresses, 600-601
steps in, 594-596
verifying solutions, 596-597
types of, 20-21
local area network (LAN), 22
wide area network (WAN), 22-23
next-hop address, 295
no hostname command, 69
no shutdown command, 85
nodes, 180
MAC versus IP addresses, 250
topologies, 185
non-volatile RAM (NVRAM), 73
nslookup command, 521-522, 605
NVRAM file system, 566-567

O

octet, 328
octet boundary, 408-410
Open Shortest Path First (OSPF), 108
open standards, 114-115
Open Systems Interconnection (OSI) reference model, 119
comparison with TCP/IP model, 121-122
Ethernet in, 211-213
layers of, 120. *See also names of individual layers*
operating systems
firmware, 56
interfaces, 55-56
network operating systems, 54

Cisco IOS. See Cisco Internetwork Operating System (CIOS)
purpose, 57
purpose, 57
routers, 297
optical fiber cable. *See* fiber-optic cable
ordered delivery, 482-485
Organizationally Unique Identifier (OUI), 219
out-of-band access, 58

P

packet filtering, 558
packets
forwarding
in host routing, 288
in router routing, 291-292
IPv4
header fields, 281-283
limitations, 283
router routing table, 292-296
IPv6
encapsulation, 284-286
header fields, 286-287
segmentation, 458-459
packet-switched networks, 31
password command, 71
passwords
for device configuration
configuring, 71
encrypting, 72
selecting, 70
security of, 561-562
strong versus weak, 560-561
patches, 556-557
path, testing, 395-396
peer-to-peer (P2P) file sharing, 6
peer-to-peer applications, 507-509
peer-to-peer model, 507-509
peer-to-peer networks, 10-11, 507
performance
ARP issues, 264-265
establishing network baseline, 575-577
personal firewalls, 559
physical addresses. *See* data link addresses; MAC addresses
physical layer (OSI model), 120
connection types, 144-145
Ethernet in, 211-213
functions, 150-152
interaction with data link layer, 143
NICs, 145-146
purpose, 146-147
standards, 148-149
physical media, 150
bandwidth, 152-153
copper cable, 155-158
coaxial cable (coax), 160-161
safety issues, 161-162
STP cabling, 159-160
UTP cabling, 158-159, 163-168
fiber-optic cable, 168
components, 170-171
connectors, 172-174
copper cable versus, 175-176
properties of, 168-169
testing, 174-175
types of, 171-172
throughput, 153-154
types of, 148, 154-155
wireless media, 176-178
properties of, 176-177
standards, 177
WLANs, 177-178
physical ports, 18
physical security, 548
physical topologies, 186
LAN topologies, 190-191
WAN topologies, 187-189
physical topology diagrams, 19
ping command, 86, 572
extended mode, 574-575
indicators, 573-574
local network testing, 394
local stack testing, 392-393
remote network testing, 395
testing loopback interface, 574
in troubleshooting, 596-597
planning addressing schemes, 440-442
podcasting, 6
Point-to-Point Protocol (PPP), 108

point-to-point topology, 187
logical, 189-190
physical, 188-189
policy vulnerabilities, 550
port numbers, 459, 470, 472-473
port-based memory buffering, 243
ports
device configuration, 79-81
routers, 300-301
USB ports, 570
positional notation, 330-331
Post Office Protocol (POP), 505, 514-515
Post Office Protocol version 3 (POP3), 107
powerline networking, 40-41
Preamble field (Ethernet frames), 215
preferred format, 360
prefix length
IPv4 addresses, 341-342
IPv6 addresses, 365
presentation layer (OSI model), 120, 503-504
private clouds, 38
private IPv4 addresses, 350-352
private ports, 472
privileged executive (EXEC) mode, 61-62, 71
problem-solving. *See* troubleshooting
proprietary protocols, 115
protocol analyzer, 544-545
protocol data unit (PDU), 125-126
protocol models, 119
protocol suites, 100-101
industry standards and, 105-106
TCP/IP
communication process, 109-113
list of protocols, 106-109
protocols, 93
application layer (TCP/IP model), 502-503
client-server model, 506
email protocols, 513-516
file sharing services, 525-528
IP addressing services, 516-525
list of, 504-506
peer-to-peer model, 507-509
web protocols, 510-512
connection-oriented, 465
data link layer (OSI model), 201-202
designing small networks, 541-542
interaction, 103-104
network layer (OSI model), 276
IP characteristics, 277-281
IPv4 packets, 281-283
IPv6 packets, 283-287
network protocols, 101-103
protocol suites, 100-101
industry standards and, 105-106
TCP/IP, 106-113
reference models, 118
benefits of layered models, 118-119
comparison of OSI and TCP/IP models, 121-122
OSI model, 120
TCP/IP protocol model, 120-121
requirements, 94
standards organizations, 114
electronics and communications standards, 116-118
Internet standards, 115-116
open standards, 114-115
stateful, 466
stateless, 468
transport layer (OSI model)
reliability, 461-462
selecting, 463-464
TCP. See Transmission Control Protocol (TCP)
UDP. See User Datagram Protocol (UDP)
public clouds, 38
public IPv4 addresses, 350-352
pwd command, 567

Q

Quality of Service (QoS), 32-33

R

radio frequency interference (RFI), 156
Random Access Memory (RAM), 73
real-time traffic, 539, 542-544
Real-Time Transport Control Protocol (RTCP), 544
Real-Time Transport Protocol (RTP), 544
reconnaissance attacks, 551-552
redundancy, 31, 537-538
reference models, 118
benefits of layered models, 118-119
comparison of OSI and TCP/IP models, 121-122

OSI model. *See* Open Systems Interconnection (OSI) reference model
TCP/IP protocol model. *See* TCP/IP protocol model
Regional Internet Registry (RIR), 356
registered ports, 472
reliability
of networks, 30
fault tolerance, 31-32
network architecture, 30-31
Quality of Service (QoS), 32-33
redundancy, 537-538
scalability, 32
security, 33-35
transport layer protocols, 461-462
TCP features, 465-466, 482-485
UDP overhead versus reliability, 488-489
reload command, 74
remote networks
ARP role in communication, 259-263
device access, 133-134
MAC versus IP addresses, 248-249
routing table entries, 294-296
testing connections, 395
removing ARP table entries, 263
Request for Comments (RFC), 184
response timeout, 98
restoring device configuration
from text files, 77, 568-569
with TFTP, 570
with USB flash drive, 571
ring topology, 191
RJ-45 connectors, 165-166
rollover cables, 167
router advertisement (RA) message
DHCPv6, 376-377
ICMPv6, 389-392
SLAAC, 374-375
router solicitation (RS) message
DHCPv6, 376-377
ICMPv6, 389-392
SLAAC, 374-375
routers. *See also* default gateway
bootup process, 303-307
computer hardware, 296-297, 299-300
connections and ports, 300-301
CPU and OS, 297
LAN and WAN interfaces, 301-302
memory, 297-298
configuration
default gateway, 314-316
DHCPv6, 376-377
dynamic link-local addresses, 380-381
initial settings, 308-311
interfaces, 311-314
SLAAC, 374-375
static IPv6 unicast addresses, 371-373
static link-local addresses, 381-382
verifying IPv6 configuration, 382-384
file systems
flash file system, 565-566
NVRAM file system, 566-567
viewing, 564-565
IPv4 router routing table
directly connected entries, 293-294
example, 292-293
next-hop address, 295
remote network entries, 294-296
packet forwarding decisions, 291-292
troubleshooting, 600-601
USB flash drives on, 570
verifying interfaces, 591
routing, 274
host routing
default gateway, 289-290
forwarding decisions, 288
routing tables, 290-291
in network layer, 276
router routing
directly connected entries, 293-294
forwarding decisions, 291-292
IPv4 router routing table, 292-293
next-hop address, 295
remote network entries, 294-296
routing tables
hosts, 290-291
routers
directly connected entries, 293-294
forwarding decisions, 291-292
IPv4 routing table, 292-293
next-hop address, 295
remote network entries, 294-296
running configuration file
backing up
to text file, 74-77, 568
with TFTP, 569
with USB flash drive, 570-571

changing, 74
restoring
with TFTP, 570
with USB flash drive, 571
saving, 72-73
running-config file, 73
runt frame, 215

S

safety issues for copper cabling, 161-162
satellite Internet connections, 27, 28
saving running configuration file, 72-73
scalable networks, 32, 544-546
Secure Shell (SSH), 58, 563
security
ARP issues, 264-265
of devices, 559-560
endpoint security, 559
executive timeouts, 562
passwords, 560-562
SSH configuration, 563
of networks, 33-35
access attacks, 552-553
attack mitigation, 556-559
Denial of Service (DoS) attacks, 554-556
malware, 550-551
physical security, 548
reconnaissance attacks, 551-552
solutions, 43-44
threat types, 42-43
threats, 547-548
vulnerabilities, 548-550
segmentation, 123-125. ***See also*** **subnetting**
multiplexing, 460-461
ordered delivery, 482-485
packets, 458-459
socket pairs, 471-472
selecting
devices for small networks, 535-536
transport layer protocols, 463-464
selective acknowledgement (SACK), 485
Server Message Block (SMB), 527-528
server-based firewalls, 559
servers, 9
TCP processes, 474-477
UDP processes, 490
service password-encryption command, 72
session layer (OSI model), 120, 503-504
shared memory buffering, 244
shell, 55
shielded twisted-pair (STP) cable, 159-160
shortcuts, 66-67
show arp command, 583
show cdp neighbors command, 588-591
show file systems command, 564, 567
show interfaces command, 582
show ip command, 85
show ip interface brief command, 591-592, 597
show ip interface command, 601
show ip route command, 583-584, 603
show running-config command, 73, 581-582
show startup-config command, 73
show version command, 306-307, 584-585
signaling, 151-152
Simple Mail Transfer Protocol (SMTP), 107, 505, 514
single-mode fiber (SMF), 171
size of messages, 97
slash notation, 341
small office/home office (SOHO) network, 8, 9
smart home technology, 39-40
social media, 6
sockets, 471-472
solicited-node multicast address, 387
source, 93
source MAC address, 250
Source MAC Address field (Ethernet frames), 215
speed settings for switches, 244-246
spoofing ARP packets, 265
spyware, 42
standards, 115
data link layer (OSI model), 184
physical layer (OSI model), 148-149
protocol suites and, 105-106
UTP cabling, 164-165
wireless media, 177
standards organizations, 114
electronics and communications standards, 116-118
Internet standards, 115-116
open standards, 114-115
star topology, 190
Start Frame Delimiter (SFD) field (Ethernet frames), 215
startup-config file, 73

stateful DHCPv6, 376-377
stateful packet inspection (SPI), 558
stateful protocols, 466
Stateless Address Autoconfiguration (SLAAC), 374-375
stateless DHCPv6, 376-377
stateless protocols, 468
static configuration
global unicast address (GUA), 371-373
link-local addresses, 381-382
static IPv4 address assignment, 345
storage area network (SAN), 21
store-and-forward switching, 241-242
Straight-Tip (ST) connectors, 173
subnet ID, 370, 444, 445-446
subnet mask, 78, 131, 338-340
subnetting
IPv4 addresses
/8 subnets, creating, 425-427
/16 subnets, creating, 421-424
addressing schemes, 440-443
broadcast domains, 405-406
classless subnetting, 410-413
formulas for, 416-418
four subnets, creating, 418-421
host calculations, 424-425
host requirements, 428
limitations, 432-434
network requirements, 428-432
octet boundary, 408-410
purpose, 407-408
two subnets, creating, 414-416
VLSM, 434-440
IPv6 addresses
example allocation, 446-448
global unicast address (GUA), 444
with subnet ID, 445-446
Subscriber Connector (SC), 173
switch fabric, 226
switch virtual interface (SVI), 81, 85
switches, 226
auto-MDIX feature, 246
configuration, 308-309
default gateway configuration, 315-316
duplex settings, 244-246
file systems, 567
frame forwarding, 240-241
cut-through switching, 242-243
memory buffering, 243-244
store-and-forward switching, 241-242
MAC address table, 226-227
on connected switches, 231-236
filtering frames, 229-231
learning addresses, 227-229
sending frames to default gateway, 236-240
speed settings, 244-246
troubleshooting, 600-601
verifying interfaces, 592
switching modes of operation (Cisco IOS), 62-63
Symmetric Digital Subscriber Line (SDSL), 28
syntax of Cisco IOS command, 64-65

T

TCP/IP protocol model, 119
communication process, 109-113
comparison with OSI model, 121-122
layers of, 120-121
list of protocols, 106-109
technological vulnerabilities, 548-549
Telecommunications Industry Association (TIA), 117
Telecommunications Industry Association/Electronic Industries Association (TIA/EIA), 149
Telnet, 58
terminal emulation programs, 59-61
terminal monitor command, 594
terminating TCP sessions, 478-481
testing
fiber-optic cable, 174-175
interface connections, 591-592
local network connections, 394
local stack, 392-393
network connections
arp command, 587-588
debug command, 592-594
establishing network baseline, 575-577
ipconfig command, 585-587
ping command, 572-575
show arp command, 583
show cdp neighbors command, 588-591
show interfaces command, 582
show ip route command, 583-584
show running-config command, 581-582

show version command, 584-585
terminal monitor command, 594
traceroute command, 577-580
path, 395-396
remote network connections, 395
UTP cabling, 167-168
TEST-NET address, 353
text files
capturing device configuration to, 74-77, 568
restoring device configuration, 568-569
texting, 5
threat types, 42-43, 547-548
three-way handshake, 481-482
throughput, 153-154
timing of messages, 98
topologies, 185
designing small networks, 534-535
LAN topologies, 190-191
logical topologies, 186
physical topologies, 186
WAN topologies, 187-190
topology diagrams, 17, 19-20
traceroute (tracert) command, 395-396, 577
extended mode, 579-580
messages, 578
in troubleshooting, 597
traffic management, 539
transferring data. ***See*** **communication**
translation. ***See*** **Network Address Translation 64 (NAT64); Network Address Translation (NAT)**
Transmission Control Protocol (TCP), 104, 108, 462-463
applications, 491
communication process
establishing connection, 477-478
server processes, 474-477
terminating session, 478-481
three-way handshake, 481-482
features, 465-466
flow control
congestion, 487-488
window size, 485-487
header fields, 466-467
multiplexing, 469
netstat command, 473-474
reliability, 482-485
well-known port numbers, 472-473
when to use, 463-464
transport layer (OSI model), 120
multiplexing, 460-461, 469
port numbers, 470, 472-473
protocols
reliability, 461-462, 482-485
selecting, 463-464
TCP. See Transmission Control Protocol (TCP)
UDP. See User Datagram Protocol (UDP)
purpose, 457-460
sockets, 471-472
Trivial File Transfer Protocol (TFTP), 107, 505
backing up device configuration, 569
restoring configuration file, 570
Trojan horses, 42, 551
troubleshooting
cables and interfaces, 598-600
default gateways, 602-603
DNS issues, 604-605
end device IP addresses, 601-602
IOS device IP addresses, 600-601
steps in, 594-596
verifying solutions, 596-597
tunneling, 359

U

unicast, 98
communication method, 347-348
IPv6 addresses, 364, 365-367
DHCPv6, 376-377
EUI-64 process, 377-380
link-local addresses, 367-368, 380-382
SLAAC, 374-375
static configuration, 371-373
structure of, 369-371
MAC addresses, 222-223
Uniform Resource Identifier (URI), 510
uniform resource locator (URL), 510-511
unique local address, 367
Universal Serial Bus (USB) flash drives
backing up device configuration, 570-571
restoring configuration file, 571
on routers, 570
unknown unicast, 38

unshielded twisted-pair (UTP) cable, 158-159, 163-168
connectors, 165-166
properties of, 163
standards, 164-165
testing, 167-168
types of, 166-167
updates, 556-557
URL filtering, 558
User Datagram Protocol (UDP), 108, 463
applications, 492
communication process
client processes, 490
datagram reassembly, 489
overhead versus reliability, 488-489
server processes, 490
features, 468
header fields, 468-469
multiplexing, 469
well-known port numbers, 472-473
when to use, 463-464
user executive (EXEC) mode, 61-62, 71

V

Variable Length Subnet Masking (VLSM), 434-440
verifying
device connectivity, 85-86
interfaces, 591-592
network connections
arp command, 587-588
debug command, 592-594
establishing network baseline, 575-577
ipconfig command, 585-587
ping command, 572-575
show arp command, 583
show cdp neighbors command, 588-591
show interfaces command, 582
show ip route command, 583-584
show running-config command, 581-582
show version command, 584-585
terminal monitor command, 594
traceroute command, 577-580
router interface configuration, 313
routing tables, 314
troubleshooting solutions, 596-597
video applications, 542-544
video communication, 37
viewing
ARP table entries, 263-264
router file systems, 564-565
virtual circuits, 189
virtual private network (VPN), 44
virtual terminal line (vty), 71
viruses, 42, 550-551
voice applications, 542-544
voice over IP (VoIP), 543
vulnerabilities, 548-550

W

"Warriors of the Net" (TNG Media Lab), 47
web pages, opening, 510-511
web protocols, 510-512
web servers, 10
well-known port numbers, 472-473
wide area network (WAN), 20, 22-23
data link layer protocols, 201-202
router interfaces, 301-302
topologies, 187-190
Wi-Fi, 177
wikis, 6
WiMax, 177
window size, 485-487
wireless access point (WAP), 144, 178
wireless broadband, 41-42
wireless Internet service provider (WISP), 41
wireless LAN (WLAN), 21, 177-178
wireless media, 148, 176-178
properties of, 176-177
standards, 177
WLANs, 177-178
wireless NIC adapters, 178
wireless router with integrated firewall, 559
workplace, network usage in, 6-7
worms, 42, 551

Z

zero-day attacks, 42