Warning and Disclaimer

This book is designed to provide information about the Cisco Networking Academy Introduction to Networks (CCNAv7) 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.

Trademark Acknowledgments

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

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

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

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

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.
About the Contributing Author

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 M.B.A. and an M.Ed. in training and development. He taught CCNA courses at the high school level for 7 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 Curriculum Lead.
About the Technical Reviewer

Dave Holzinger has been a curriculum developer, project manager, author, and technical editor for the Cisco Networking Academy Program in Phoenix, Arizona since 2001. Dave works on the team that develops their online curricula including CCNA, CCNP, and IT Essentials. He has been working with computer hardware and software since 1981. Dave has certifications from Cisco, BICSI, and CompTIA.
Credits

Figure 2-2  Screenshot of Windows 10 Ethernet Properties © Microsoft 2020
Figure 2-3  Screenshot of Windows 10 TCP/IPv4 Properties—Manual IP Address Configuration © Microsoft 2020
Figure 2-4  Screenshot of Windows 10 TCP/IPv4 Properties—Automatic IP Address Configuration © Microsoft 2020
Unnumbered Figure 3-2  Screenshot of Capturing from Ethernet © Wireshark
Unnumbered Figure 7-2  Screenshot of highlights the frame details for an ARP request © Wireshark
Unnumbered Figure 7-3  Screenshot of highlights the frame details for an ARP reply © Wireshark
Figure 12-3  Screenshot of Windows TCP/IPv6 Properties © Microsoft 2020
Unnumbered Figure 13-2  Screenshot of External to PC-A with a Hop limit of 63 © Wireshark
Figure 17-3  Screenshot of Windows 10 Network Connection Details © Microsoft 2020
Figure 17-4  Screenshot of Linux Ubuntu Connection Information © 2020 Microsoft 2020
Figure 17-5  Screenshot of Configuration Information on a macOS Host © 2020 Apple Inc
Contents at a Glance

Introduction xxx
Chapter 1 Networking Today 1
Chapter 2 Basic Switch and End Device Configuration 19
Chapter 3 Protocols and Models 59
Chapter 4 Physical Layer 91
Chapter 5 Number Systems 115
Chapter 6 Data Link Layer 123
Chapter 7 Ethernet Switching 131
Chapter 8 Network Layer 159
Chapter 9 Address Resolution 171
Chapter 10 Basic Router Configuration 191
Chapter 11 IPv4 Addressing 219
Chapter 12 IPv6 Addressing 261
Chapter 13 ICMP 291
Chapter 14 Transport Layer 319
Chapter 15 Application Layer 343
Chapter 16 Network Security Fundamentals 359
Chapter 17 Build a Small Network 389
Contents

Introduction xxx

Chapter 1 Networking Today 1
Networks Affect Our Lives 2
Network Components 2
End Devices, Intermediary Devices, and Media 2
Check Your Understanding: Network Components 3
Network Representations and Topologies 4
Classify and Identify Network Components 4
Topology Diagrams 4
Check Your Understanding: Network Representations and Topologies 4
Common Types of Networks 5
Compare LANs and WANs 5
Check Your Understanding: Common Types of Networks 6
Internet Connections 6
Vocabulary Exercise: Matching 6
Reliable Networks 8
Classify the Requirements for a Reliable Network 8
Check Your Understanding: Reliable Networks 9
Network Trends 9
Identify the Cloud Type 10
Check Your Understanding: Network Trends 10
Network Security 11
Check Your Understanding: Network Security 11
The IT Professional 12
1.5.7 Packet Tracer—Network Representation 13
Objectives 13
Instructions 13
Challenge Question 14
1.9.3 Lab—Research IT and Networking Job Opportunities 16
Objectives 16
Background / Scenario 16
Required Resources 16
Instructions 16
Reflection Questions 17

Chapter 2 Basic Switch and End Device Configuration 19
Cisco IOS Access 20
Check Your Understanding: Cisco IOS Access 20
Introduction to Networks Labs and Study Guide (CCNAv7)

IOS Navigation  
Syntax Checker: Navigate Between IOS Modes  
Check Your Understanding: IOS Navigation

The Command Structure  
Navigate the IOS Matching Exercise  
Hotkeys and Shortcuts

Basic Device Configuration  
Apply a Basic Configuration  
Check Your Understanding: Basic Device Configuration

Save Configurations

Ports and Addresses  
Check Your Understanding: Ports and Addresses

Configure IP Addressing

Verify Connectivity  
Packet Tracer Exercise 2-1: Basic Switch Configuration  
Requirements

Command Reference

2.3.7 Packet Tracer—Navigate the IOS  
Objectives  
Background / Scenario  
Instructions  
Part 1: Establish Basic Connections, Access the CLI, and Explore Help  
Part 2: Explore EXEC Modes  
Part 3: Set the Clock

2.3.8 Lab—Navigate the IOS by Using Tera Term for Console Connectivity  
Topology  
Objectives  
Background / Scenario  
Required Resources  
Instructions  
Part 1: Access a Cisco Switch through the Serial Console Port  
Part 2: Display and Configure Basic Device Settings  
Part 3: (Optional) Access a Cisco Router Using a Mini-USB Console Cable  
Reflection Question  
Router Interface Summary Table

2.5.5 Packet Tracer—Configure Initial Switch Settings  
Objectives  
Background / Scenario  
Instructions  
Part 1: Verify the Default Switch Configuration  
Part 2: Create a Basic Switch Configuration
Part 3: Configure a MOTD Banner 48
Part 4: Save and Verify Configuration Files to NVRAM 49
Part 5: Configure S2 49

2.7.6 Packet Tracer—Implement Basic Connectivity 50
   Addressing Table 50
   Objectives 50
   Background 50
   Instructions 50
   Part 1: Perform a Basic Configuration on S1 and S2 50
   Part 2: Configure the PCs 51
   Part 3: Configure the Switch Management Interface 51

2.9.1 Packet Tracer—Basic Switch and End Device Configuration 53
   Addressing Table 53
   Objectives 53
   Scenario 53
   Instructions 53
   Requirements 53

2.9.2 Lab—Basic Switch and End Device Configuration 55
   Topology 55
   Addressing Table 55
   Objectives 55
   Background / Scenario 55
   Required Resources 56
   Instructions 56
   Reflection Question 57

Chapter 3 Protocols and Models 59
The Rules 60
   Vocabulary Exercise: Matching 60
   Check Your Understanding: The Rules 60
Protocols 61
   Check Your Understanding: Protocols 62
Protocol Suites 63
   Protocol Definitions: Matching 63
   Map the Protocols of the TCP/IP Suite 64
   Check Your Understanding: Protocol Suites 65
Standards Organizations 66
   Standards Organizations: Matching 66
   Check Your Understanding: Standards Organizations 67
Reference Models 68
   OSI Reference Model Layers: Matching 68
   TCP/IP Model Layers: Matching 69
Data Encapsulation 69
Label the PDUs 69
Check Your Understanding: Data Encapsulation 70

Data Access 71
The Role of Addressing in Network Communications 71
Check Your Understanding: Data Access 72

3.0.3 Class Activity—Design a Communications System 73
Objectives 73
Background / Scenario 73
Reflection Question 73

3.4.4 Lab—Research Networking Standards 74
Objectives 74
Background / Scenario 74
Required Resources 74
Instructions 74

3.5.5 Packet Tracer—Investigate the TCP/IP and OSI Models in Action 77
Objectives 77
Background 77
Instructions 77
Part 1: Examine HTTP Web Traffic 77
Part 2: Display Elements of the TCP/IP Protocol Suite 80
Challenge Questions 81

3.7.9 Lab—Install Wireshark 82
Objectives 82
Background / Scenario 82
Required Resources 82
Instructions 82

3.7.10 Lab—Use Wireshark to View Network Traffic 84
Topology 84
Objectives 84
Background / Scenario 84
Required Resources 84
Instructions 85
Part 1: Capture and Analyze Local ICMP Data in Wireshark 85
Part 2: Capture and Analyze Remote ICMP Data in Wireshark 87
Reflection Question 88
Appendix A: Allowing ICMP Traffic Through a Firewall 89
Part 1: Create a new inbound rule allowing ICMP traffic through the firewall 89
Part 2: Disabling or deleting the new ICMP rule 89

Chapter 4  Physical Layer 91
Purpose of the Physical Layer 92
Check Your Understanding: Purpose of the Physical Layer 92
Physical Layer Characteristics 92
   Completion Exercise 93
   Check Your Understanding: Physical Layer Characteristics 94

Copper Cabling 94
   Completion Exercise 94
   Compare UTP, STP, and Coaxial Characteristics 95

UTP Cabling 96
   Limiting the Negative Effect of Crosstalk 96
   UTP Cable Wiring Standards 96
   UTP Cable Pinouts 96

Fiber-Optic Cabling 97
   Completion Exercise 97
   Check Your Understanding: Fiber-Optic Cabling 98

Wireless Media 99
   Completion Exercise 99
   Check Your Understanding: Wireless Media 100

4.6.5 Packet Tracer—Connect a Wired and Wireless LAN 101
   Addressing Table 101
   Objectives 101
   Background 101
   Instructions 102
   Part 1: Connect to the Cloud 102
   Part 2: Connect Router0 102
   Part 3: Connect Remaining Devices 102
   Part 4: Verify Connections 103
   Part 5: Examine the Physical Topology 103

4.6.6 Lab—View Wired and Wireless NIC Information 105
   Objectives 105
   Background / Scenario 105
   Required Resources 105
   Instructions 105
   Part 1: Identify and Work with PC NICs 105
   Part 2: Identify and Use the System Tray Network Icons 108
   Reflection Question 108

4.7.1 Packet Tracer—Connect the Physical Layer 109
   Objectives 109
   Background 109
   Part 1: Identify Physical Characteristics of Internetworking Devices 109
   Part 2: Select Correct Modules for Connectivity 110
   Part 3: Connect Devices 111
   Part 4: Check Connectivity 112
Chapter 5  Number Systems  115
  Binary Number System  116
    Positional Notation  116
    Convert Binary to Decimal  117
    Convert Decimal to Binary  118
    Activity: Binary Game  118
  Hexadecimal Number System  118
    Decimal to Hexadecimal Conversion  120
    Hexadecimal to Decimal Conversion  120
    Check Your Understanding: Hexadecimal Number System  120

Chapter 6  Data Link Layer  123
  Purpose of the Data Link Layer  124
    Check Your Understanding: Purpose of the Data Link Layer  125
  Topologies  126
    Completion Exercise  126
    Check Your Understanding: Topologies  127
  Data Link Frame  128
    Label the Generic Frame Fields  128
    Check Your Understanding: Data Link Frame  128

Chapter 7  Ethernet Switching  131
  Ethernet Frames  132
    Identify the Ethernet Frame Attributes  133
    Check Your Understanding: Ethernet Switching  133
  Ethernet MAC Address  134
    Completion Exercise  134
  The MAC Address Table  135
    LAN Switches  135
    Build the MAC Address Table  136
    Forward the Frame  136
  Switch Speeds and Forwarding Methods  140
    Compare Switch Forwarding Methods  140
    Port Settings Completion Exercise  140
    Check Your Understanding: Switch Speeds and Forwarding Methods  141
  7.1.6 Lab—Use Wireshark to Examine Ethernet Frames  142
    Topology  142
    Objectives  142
    Background / Scenario  142
    Required Resources  142
    Instructions  142
Part 1: Examine the Header Fields in an Ethernet II Frame 142
Part 2: Use Wireshark to Capture and Analyze Ethernet Frames 146
Reflection Question 148

7.2.7 Lab—View Network Device MAC Addresses 149
  Topology 149
  Addressing Table 149
  Objectives 149
  Background / Scenario 149
  Required Resources 149
  Instructions 150
  Part 1: Configure Devices and Verify Connectivity 150
  Part 2: Display, Describe, and Analyze Ethernet MAC Addresses 151
  Reflection Questions 154

7.3.7 Lab—View the Switch MAC Address Table 155
  Topology 155
  Addressing Table 155
  Objectives 155
  Background / Scenario 155
  Required Resources 156
  Instructions 156
  Part 1: Build and Configure the Network 156
  Part 2: Examine the Switch MAC Address Table 156
  Reflection Question 158

Chapter 8 Network Layer 159

Network Layer Characteristics 160
  Network Layer Operations 160
  Characteristics of IP 160
  Check Your Understanding: IP Characteristics 161

IPv4 Packet 161
  Fields of the IPv4 Packet 162
  Check Your Understanding: IPv4 Packet 162

IPv6 Packet 163
  Fields of the IPv6 Packet 163
  Check Your Understanding: IPv6 Packet 164

How a Host Routes 164
  Completion Exercise 165
  Check Your Understanding: How a Host Routes 166

Introduction to Routing 166
  Routing Table Entry: Matching 168
  Check Your Understanding: Introduction to Routing 169
Chapter 9  Address Resolution  171
MAC and IP  172
  Identify the MAC and IP Addresses  172
  Check Your Understanding: MAC and IP  172
ARP  173
  Completion Exercise  173
  Check Your Understanding: ARP  174
IPv6 Neighbor Discovery  175
  Five ICMPv6 Messages  175
  Check Your Understanding: Neighbor Discovery  175
9.1.3 Packet Tracer—Identify MAC and IP Addresses  177
  Objectives  177
  Background  177
  Instructions  177
  Part 1: Gather PDU Information for Local Network Communication  177
  Part 2: Gather PDU Information for Remote Network Communication  178
  Reflection Questions  179
  Suggested Scoring Rubric  180
9.2.9 Packet Tracer—Examine the ARP Table  181
  Addressing Table  181
  Objectives  181
  Background  181
  Instructions  181
  Part 1: Examine an ARP Request  181
  Part 2: Examine a Switch MAC Address Table  182
  Part 3: Examine the ARP Process in Remote Communications  183
9.3.4 Packet Tracer—IPv6 Neighbor Discovery  185
  Addressing Table  185
  Objectives  185
  Background  185
  Instructions  185
  Part 1: IPv6 Neighbor Discovery Local Network  185
  Part 2: IPv6 Neighbor Discovery Remote Network  187
  Reflection Questions  190

Chapter 10  Basic Router Configuration  191
Configure Initial Router Settings  192
  Basic Router Configuration Exercise  192
  Configure Initial Settings Exercise  193
Configure Interfaces  194
  Configure Router Interfaces Exercise  194
  Packet Tracer Exercise 10-1: Basic Router Configuration  196
Configure the Default Gateway  196
Command Reference  197

10.1.4 Packet Tracer—Configure Initial Router Settings  198
Objectives  198
Background  198
Instructions  198
Part 1: Verify the Default Router Configuration  198
Part 2: Configure and Verify the Initial Router Configuration  199
Part 3: Save the Running Configuration File  200

10.3.4 Packet Tracer—Connect a Router to a LAN  202
Addressing Table  202
Objectives  202
Background  202
Part 1: Display Router Information  202
Part 2: Configure Router Interfaces  204
Part 3: Verify the Configuration  205

10.3.5 Packet Tracer—Troubleshoot Default Gateway Issues  207
Addressing Table  207
Objectives  207
Background  207
Instructions  208
Part 1: Verify Network Documentation and Isolate Problems  208
Part 2: Implement, Verify, and Document Solutions  209

10.4.3 Packet Tracer—Basic Device Configuration  210
Topology  210
Addressing Table  210
Objectives  210
Scenario  210
Requirements  211

10.4.4 Lab—Build a Switch and Router Network  212
Topology  212
Addressing Table  212
Objectives  212
Background / Scenario  212
Required Resources  213
Instructions  213
Part 1: Set Up Topology and Initialize Devices  213
Part 2: Configure Devices and Verify Connectivity  214
Part 3: Display Device Information  215
Reflection Questions  216
Router Interface Summary Table  216
Chapter 11  IPv4 Addressing  219

IPv4 Address Structure  220
- Network and Host Portions  220
- IPv4 Subnet Mask  220
- The Prefix Length  221
- Determining the Network: Logical AND  221
- ANDing to Determine the Network Address  222
- Activity: ANDing to Determine the Network Address  222
- Check Your Understanding: IPv4 Address Structure  223

IPv4 Unicast, Broadcast, and Multicast  224

Types of IPv4 Addresses  224
- Public and Private Addresses  224
- Special Use IPv4 Addresses  224
- Legacy Classful Addressing  225
- Assignment of IP Addresses  225
- Check Your Understanding: Types of IPv4 Addresses  226

Network Segmentation  226
- Broadcast Domains and Segmentation  226
- Problems with Large Broadcast Domains  226
- Reasons for Segmenting Networks  227
- Check Your Understanding: Network Segmentation  227

Subnet an IPv4 Network  227
- Subnetting in Four Steps  228
- Subnetting Example  228
- Subnetting Scenario 1  230
- Subnetting Scenario 2  230
- Subnetting Scenario 3  230

VLSM Addressing Schemes  231
- VLSM Review  231
- VLSM Addressing Design Exercises  233

11.5.5 Packet Tracer—Subnet an IPv4 Network  236
- Addressing Table  236
- Objectives  236
- Background / Scenario  236
- Instructions  237
- Part 1: Subnet the Assigned Network  237
- Part 2: Configure the Devices  240
- Part 3: Test and Troubleshoot the Network  240

11.6.6 Lab—Calculate IPv4 Subnets  241
- Objectives  241
- Background / Scenario  241
- Required Resources  241
Instructions 241
Problem 1 241
Problem 2 242
Problem 3 242
Problem 4 243
Problem 5 243
Problem 6 244
Reflection Question 244

11.7.5 Packet Tracer—Subnetting Scenario 245
Addressing Table 245
Objectives 245
Scenario 245
Instructions 245
Part 1: Design an IP Addressing Scheme 245
Part 2: Assign IP Addresses to Network Devices and Verify Connectivity 248

11.9.3 Packet Tracer—VLSM Design and Implementation Practice 249
Topology 249
Addressing Table 249
Objectives 249
Background 249
Instructions 250
Part 1: Examine the Network Requirements 250
Part 2: Design the VLSM Addressing Scheme 251
Part 3: Assign IP Addresses to Devices and Verify Connectivity 252

11.10.1 Packet Tracer—Design and Implement a VLSM Addressing Scheme 253
Addressing Table 253
Objectives 253
Background / Scenario 253
Instructions 254
Requirements 254

11.10.2 Lab—Design and Implement a VLSM Addressing Scheme 255
Topology 255
Objectives 255
Background / Scenario 255
Required Resources 255
Instructions 256
Part 1: Examine Network Requirements 256
Part 2: Design the VLSM Address Scheme 258
Part 3: Cable and Configure the IPv4 Network 259
Reflection Question 260
Router Interface Summary Table 260
Chapter 12  IPv6 Addressing  261
IPv4 Issues  262
   IPv4 and IPv6 Coexistence  262
   Check Your Understanding: IPv4 Issues  262
IPv6 Address Representation  263
IPv6 Address Types  263
   IPv6 Prefix Length  263
   Types of IPv6 Addresses  264
   IPv6 GUA  264
GUA and LLA Static Configuration  265
   Static Configuration of Global Unicast Addressing  265
   Static GUA Configuration on a Windows Host  266
   Static Configuration of a Link-Local Unicast Address  266
Dynamic Addressing for IPv6 GUAs  267
   RS and RA Messages  267
   Method 1: SLAAC  268
   Method 2: SLAAC and Stateless DHCPv6  268
   Method 3: Stateful DHCPv6  269
   EUI-64 Process  270
   Randomly Generated Interface IDs  271
   Check Your Understanding: Dynamic Addressing for IPv6 GUAs  271
Dynamic Addressing for IPv6 LLAs  272
IPv6 Multicast Addresses  272
Subnet an IPv6 Network  272
   IPv6 Subnetting Example  273
   IPv6 Subnetting Scenario 1  273
   IPv6 Subnetting Scenario 2  274
   IPv6 Subnetting Scenario 3  274
   Check Your Understanding: Subnet an IPv6 Network  274
12.6.6 Packet Tracer—Configure IPv6 Addressing  276
   Addressing Table  276
   Objectives  276
   Background  276
   Part 1: Configure IPv6 Addressing on the Router  276
   Part 2: Configure IPv6 Addressing on the Servers  278
   Part 3: Configure IPv6 Addressing on the Clients  278
   Part 4: Test and Verify Network Connectivity  278
12.7.4 Lab—Identify IPv6 Addresses  280
   Topology  280
   Objectives  280
   Background / Scenario  280
   Required Resources  280
Instructions 280
Part 1: Practice with Different Types of IPv6 Addresses 280
Part 2: Examine a Host IPv6 Network Interface and Address 281
Reflection Questions 283

12.9.1 Packet Tracer—Implement a Subnetted IPv6 Addressing
Scheme 284
Addressing Table 284
Objectives 284
Background / Scenario 284
Instructions 284

12.9.2 Lab—Configure IPv6 Addresses on Network Devices 286
Topology 286
Addressing Table 286
Objectives 286
Background / Scenario 286
Required Resources 287
Instructions 287
Part 1: Cable the Network and Configure Basic Router and Switch
Settings 287
Part 2: Configure IPv6 Addresses Manually 287
Part 3: Verify End-to-End Connectivity 289
Reflection Questions 289
Router Interface Summary Table 289

Chapter 13  ICMP 291
ICMP Messages 292
Host Reachability 292
Destination or Service Unreachable 292
Time Exceeded 293
ICMPv6 Messages 293
Check Your Understanding: ICMP Messages 295

Ping and Traceroute Tests 296
Ping—Test Connectivity 296
Traceroute—Test the Path 296

Command Reference 297

13.2.6 Packet Tracer—Verify IPv4 and IPv6 Addressing 297
Addressing Table 297
Objectives 298
Background 298
Part 1: Complete the Addressing Table Documentation 298
Part 2: Test Connectivity Using Ping 298
Part 3: Discover the Path by Tracing the Route 299
13.2.7 Packet Tracer—Use Ping and Traceroute to Test Network Connectivity 301
   Addressing Table 301
   Objectives 301
   Scenario 301
   Instructions 302
   Part 1: Test and Restore IPv4 Connectivity 302
   Part 2: Test and Restore IPv6 Connectivity 303

13.3.1 Packet Tracer—Use ICMP to Test and Correct Network Connectivity 305
   Addressing Table 305
   Objectives 305
   Background 305
   Instructions 306

13.3.2 Lab—Use Ping and Traceroute to Test Network Connectivity 307
   Topology 307
   Addressing Table 307
   Objectives 307
   Background / Scenario 308
   Required Resources 308
   Instructions 309
   Part 1: Build and Configure the Network 309
   Part 2: Use Ping Command for Basic cork Testing 310
   Part 3: Use Tracert and Traceroute Commands for Basic Network Testing 315
   Part 4: Troubleshoot the Topology 316
   Reflection Questions 317
   Router Interface Summary Table 317

Chapter 14 Transport Layer 319
   Transportation of Data 320
   Transmission Control Protocol (TCP) 320
   User Datagram Protocol (UDP) 320
   The Right Transport Layer Protocol for the Right Application 320
   Check Your Understanding: Transportation of Data 321

TCP Overview 322
   TCP Features 322
   TCP Header 323
   TCP Header Fields 323
   Applications That Use TCP 324
   Check Your Understanding: TCP Overview 324
UDP Overview  325

UDP Features  325
UDP Header  325
Applications That Use UDP  325
Check Your Understanding: UDP Overview  326
Compare TCP and UDP  327

Port Numbers  327

Socket Pairs  327
Port Number Groups  328
Check Your Understanding: Port Numbers  328

TCP Communication Process  329

TCP Server Processes  329
TCP Connection Establishment  329
Session Termination  330
Control Bits Field  331
Check Your Understanding: TCP Communication Process  331

Reliability and Flow Control  332

TCP Reliability—Guaranteed and Ordered Delivery  332
TCP Reliability—Data Loss and Retransmission  332
TCP Flow Control—Window Size and Acknowledgments  332
TCP Flow Control—Maximum Segment Size (MSS)  333
TCP Flow Control—Congestion Avoidance  333
Check Your Understanding: Reliability and Flow Control  334

UDP Communication  334

UDP Datagram Reassembly  334
UDP Client Processes  334
Check Your Understanding: UDP Communication  335

Command Reference  336

14.8.1 Packet Tracer—TCP and UDP Communications  336

Objectives  336
Background  336
Instructions  336
Part 1: Generate Network Traffic in Simulation Mode and View Multiplexing  336
Part 2: Examine Functionality of the TCP and UDP Protocols  338

Chapter 15 Application Layer  343

Application, Presentation, and Session  344

Application Layer  344

Presentation and Session Layer  344
TCP/IP Application Layer Protocols  344
Check Your Understanding: Application, Session, Presentation  345
Peer-to-Peer 346
Check Your Understanding: Peer-to-Peer 346

Web and Email Protocols 347
Hypertext Transfer Protocol and Hypertext Markup Language 347
HTTP and HTTPS 347
Email Protocols 348
Check Your Understanding: Web and Email Protocols 348

IP Addressing Services 349
Domain Name Service 349
DNS Message Format 349
DNS Hierarchy 349
The nslookup Command 350
Dynamic Host Configuration Protocol 351
DHCP Operation 351
Check Your Understanding: IP Addressing Services 352

File Sharing Services 353
File Transfer Protocol 353
Server Message Block 353
Check Your Understanding: File Sharing Services 354

Command Reference 355
15.4.8 Lab—Observe DNS Resolution 355
Objectives 355
Background / Scenario 355
Required Resources 355
Part 1: Observe the DNS Conversion of a URL to an IP Address 355
Part 2: Observe DNS Lookup Using the nslookup Command on a Website 357
Part 3: Observe DNS Lookup Using the nslookup Command on Mail Servers 358
Reflection Question 358

Chapter 16 Network Security Fundamentals 359
Security Threats and Vulnerabilities 360
Types of Threats 360
Types of Vulnerabilities 360
Physical Security 361

Network Attacks 361
Types of Malware 361
Reconnaissance Attacks 362
Access Attacks 362
Denial of Service Attacks 362
Check Your Understanding: Network Attacks 363
Network Attack Mitigation 364
   Matching Exercise: Network Attack Mitigation 364
   Check Your Understanding: Network Attack Mitigation 365

Device Security 366
   Passwords 366
   Additional Password Security 366
   Enable SSH 366
   Packet Tracer Exercise 16-1: SSH Configuration and Verification 367

Command Reference 368
16.2.6 Lab—Research Network Security Threats 368
   Objectives 368
   Background / Scenario 368
   Required Resources 369
   Instructions 369
   Part 1: Exploring the SANS Website 369
   Part 2: Identify Recent Network Security Threats 370
   Part 3: Detail a Specific Network Security Attack 370
   Reflection Questions 371

16.4.6 Packet Tracer—Configure Secure Passwords and SSH 372
   Addressing Table 372
   Scenario 372
   Instructions 372

16.4.7 Lab—Configure Network Devices with SSH 375
   Topology 375
   Addressing Table 375
   Objectives 375
   Background / Scenario 375
   Required Resources 376
   Instructions 376
   Part 1: Configure Basic Device Settings 376
   Part 2: Configure the Router for SSH Access 377
   Part 3: Configure the Switch for SSH Access 377
   Part 4: SSH from the CLI on the Switch 378
   Reflection Question 379
   Router Interface Summary Table 379

16.5.1 Packet Tracer—Secure Network Devices 381
   Addressing Table 381
   Requirements 381
   Instructions 381

16.5.1 Lab—Secure Network Devices 383
   Topology 383
   Addressing Table 383
Objectives 383
Background / Scenario 383
Required Resources 384
Instructions 384
Part 1: Configure Basic Device Settings 384
Part 2: Configure Basic Security Measures on the Router 385
Part 3: Configure Security Measures 385
Part 4: Configure Basic Security Measures on the Switch 386
Reflection Questions 387
Router Interface Summary Table 388

Chapter 17  Build a Small Network 389

Devices in a Small Network 390
Small Network Topologies 390
Device Selection for a Small Network 390
IP Addressing for a Small Network 391
Matching Exercise: Devices in a Small Network 391
Check Your Understanding: Devices in a Small Network 392

Small Network Applications and Protocols 392
Common Applications 392
Common Protocols 393
Check Your Understanding: Small Network Applications and Protocols 393

Scale to Larger Networks 394
Check Your Understanding: Scale to Larger Networks 394

Verify Connectivity 395
Verify Connectivity with Ping 395
Verify Connectivity with Traceroute 396
Extended Traceroute 396
Network Baseline 397

Host and IOS Commands 397
IP Configuration on a Windows Host 397
IP Configuration on a Linux Host 398
IP Configuration on a macOS Host 399
The arp Command 400
show Commands 400
Matching Exercise: show Commands 401

Troubleshooting Methodologies 402
Basic Troubleshooting Approaches 402
Check Your Understanding: Troubleshooting Methodologies 402
17.4.6 Lab—Test Network Latency with Ping and Traceroute 406
   Topology 406
   Objectives 406
   Background / Scenario 406
   Required Resources 406
   Instructions 406
   Part 1: Use Ping to Document Network Latency 406
   Part 2: Use Traceroute to Document Network Latency 408
   Part 3: Extended Traceroute 409
   Reflection Questions 410

17.5.9 Packet Tracer—Interpret show Command Output 411
   Objectives 411
   Background 411
   Instructions 411
   Reflection Questions 411

17.7.6 Lab—Troubleshoot Connectivity Issues 413
   Topology 413
   Addressing Table 413
   Objectives 413
   Background / Scenario 413
   Required Resources 414
   Troubleshooting Configuration 414
   Part 1: Identify the Problem 415
   Part 2: Implement Network Changes 416
   Part 3: Verify Full Functionality 416
   Part 4: Document Findings and Configuration Changes 416
   Reflection Question 416
   Router Interface Summary Table 416

17.7.7 Packet Tracer—Troubleshoot Connectivity Issues 418
   Addressing Table 418
   Objectives 418
   Background / Scenario 418
   Instructions 418

17.8.1 Lab—Design and Build a Small Network 422
   Objectives 422
   Background / Scenario 422
   Required Resources 422
   Reflection 422
17.8.2 Packet Tracer—Skills Integration Challenge  423
   Addressing Table  423
   Background / Scenario  424
   Instructions  424

17.8.3 Packet Tracer—Troubleshooting Challenge  426
   Addressing Table  426
   Objectives  427
   Background / Scenario  427
   Instructions  427
Command Syntax Conventions

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

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

This book supports instructors and students in Cisco Networking Academy, an IT skills and career building program for learning institutions and individuals worldwide. Cisco Networking Academy provides a variety of curricula choices including the very popular CCNA curriculum. It includes three courses oriented around the topics of Cisco Certified Network Associate (CCNA) certifications.

Introduction to Networks Labs and Study Guide is a supplement to your classroom and laboratory experience with the Cisco Networking Academy. To be successful on the exam and achieve your CCNA certification, you should do everything in your power to arm yourself with a variety of tools and training materials to support your learning efforts. This book provides just such a collection of tools. Used to its fullest extent, it will help you gain the knowledge as well as practice the skills associated with the content area of the Introduction to Networks v7 course. Specifically, this book will help you work on these main areas:

■ Understand advances in modern network technologies.
■ Implement initial settings, including passwords, IP addressing, and default gateway parameters on network switches and end devices.
■ Understand how network protocols enable devices to access local and remote network resources.
■ Understand how physical layer protocols, services, and network media support communications across data networks.
■ Convert between decimal, binary, and hexadecimal systems.
■ Understand how media access control in the data link layer supports communication across networks.
■ Understand how Ethernet operates in a switched network.
■ Understand how routers use network layer protocols and services to enable end-to-end connectivity.
■ Understand how ARP and ND enable communication on a network.
■ Implement initial settings on a router and end devices.
■ Calculate an IPv4 subnetting scheme to efficiently segment a network.
■ Implement an IPv6 addressing scheme.
■ Use various tools to test network connectivity.
■ Compare the operations of transport layer protocols in supporting end-to-end communication.
■ Understand the operation of application layer protocols in providing support to end-user applications.
■ Configure switches and routers with device-hardening features to enhance security.
■ Implement a network design for a small network to include a router, a switch, and end devices.

Labs and Study Guides similar to this one are also available for the other two courses: Switching, Routing, and Wireless Essentials Labs and Study Guide and Enterprise Networking, Security, and Automation Labs and Study Guide.
Who Should Read This Book

This book's main audience is anyone taking the Introduction to Networks course of the Cisco Networking Academy curriculum. Many Academies use this Labs and Study Guide as a required tool in the course, whereas other Academies recommend the Labs and Study Guide as an additional resource to prepare for class exams and the CCNA certification. The secondary audiences for this book is people taking CCNA-related classes from professional training organizations. This book can also be used for college- and university-level networking courses, as well as anyone wanting to gain a detailed understanding of routing. However, the reader should know that the content of this book tightly aligns with the Cisco Networking Academy course. It may not be possible to complete some of the “Study Guide” sections and labs without having access to the online course. Fortunately, you can purchase the Introduction to Networks v7.0 Companion Guide (ISBN: 9780136633662).

Goals and Methods

The most important goal of this book is to help you pass the 200-301 Cisco Certified Network Associate exam, which is associated with the Cisco Certified Network Associate (CCNA) certification. Passing the CCNA exam shows that you have the knowledge and skills required to manage a small enterprise network. You can view the detailed exam topics online at http://learningnetwork.cisco.com. They are divided into six broad categories:

- Network Fundamentals
- Network Access
- IP Connectivity
- IP Services
- Security Fundamentals
- Automation and Programmability

The Introduction to Networks v7 course covers introductory material related to the first five bullets. The next two courses, Switching, Routing, and Wireless Essentials v7 and Enterprise Networking, Security, and Automation v7, cover the material in more detail. Each chapter of this book is divided into a “Study Guide” section followed by a “Labs and Activities” section. The “Study Guide” section offers exercises that help you learn the concepts, configurations, and troubleshooting skills crucial to your success as a CCNA exam candidate. Each chapter is slightly different and includes some or all of the following types of exercises:

- Vocabulary matching exercises
- Concept question exercises
- Skill-building activities and scenarios
- Configuration scenarios
- Packet Tracer exercises
- Troubleshooting scenarios

The “Labs and Activities” sections include all the online course labs and Packet Tracer activity instructions. In some chapters, this section begins with a Command Reference that you will complete to show that you understand all the commands introduced in the chapter.
Packet Tracer and Companion Website

This book includes the instructions for all the Packet Tracer activities in the online course. You need to be enrolled in the Introduction to Networks v7 course to access these Packet Tracer files.

Four Packet Tracer activities have been created exclusively for this book. You can access these unique Packet Tracer files at this book's companion website.

To get your copy of Packet Tracer software and the four unique files for this book, please go to the companion website for instructions. To access this companion website, follow these steps:

Step 1. Go to www.ciscopress.com/register and log in or create a new account.
Step 2. Enter the ISBN 9780136634454.
Step 3. Answer the challenge question as proof of purchase.
Step 4. Click on the Access Bonus Content link in the Registered Products section of your account page to be taken to the page where your downloadable content is available.

How This Book Is Organized

This book corresponds closely to the Cisco Networking Academy Introduction to Networks v7 course and is divided into 17 chapters:

- **Chapter 1, “Networking Today”**: This chapter 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 recent trends in networks, such as video, cloud computing, and BYOD and how to help ensure robust, reliable, secure networks to support these trends.

- **Chapter 2, “Basic Switch and End Device Configuration”**: This chapter introduces the operating system used with most Cisco devices: Cisco IOS. The basic purpose and functions of IOS are described, as are methods to access IOS. The chapter also describes how to maneuver through the IOS command-line interface as well as basic IOS device configuration.

- **Chapter 3, “Protocols and Models”**: This chapter examines the importance of rules or protocols for network communication. It explores the OSI reference model and the TCP/IP communication suite and examines how these models provide the necessary protocols to allow communication to occur on a modern converged network.

- **Chapter 4, “Physical Layer”**: This chapter introduces the lowest layer of the OSI model: the physical layer. This chapter explains the transmission of bits over the physical medium.

- **Chapter 5, “Number Systems”**: This chapter explains how to convert between decimal, binary, and hexadecimal number systems. Understanding these number systems is essential to understanding IPv4, IPv6, and Ethernet MAC addressing.

- **Chapter 6, “Data Link Layer”**: This chapter discusses how the data link layer prepares network layer packets for transmission, controls access to the physical media, and transports 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.

- **Chapter 7, “Ethernet Switching”**: This chapter examines the functionality of the Ethernet LAN protocols. It explores how Ethernet functions, including how devices use Ethernet MAC addresses to communicate in a multiaccess network. The chapter discusses how Ethernet switches build MAC address tables and forward Ethernet frames.
Chapter 8, “Network Layer”: This chapter introduces the function of the network layer—routing—and the basic device that performs this function—the router. It presents important routing concepts related to addressing, path determination, and data packets for both IPv4 and IPv6. The chapter also introduces how routers perform packet forwarding, static and dynamic routing, and the IP routing table.

Chapter 9, “Address Resolution”: This chapter discusses how host computers and other end devices determine the Ethernet MAC address for a known IPv4 or IPv6 address. This chapter examines the ARP protocol for IPv4 address resolution and the Neighbor Discovery Protocol for IPv6.

Chapter 10, “Basic Router Configuration”: This chapter explains how to configure a Cisco router, including IPv4 and IPv6 addressing on an interface.

Chapter 11, “IPv4 Addressing”: This chapter focuses on IPv4 network addressing, including the types of addresses and address assignment. It describes how to use subnet masks to determine the number of subnetworks and hosts in a network. It examines how to improve network performance by optimally dividing the IPv4 address space based on network requirements. It explores the calculation of valid host addresses and the determination of both subnet and broadcast addresses.

Chapter 12, “IPv6 Addressing”: This chapter focuses on IPv6 network addressing, including IPv6 address representation, types of addresses, and the structure of different types of IPv6 address. The chapter introduces the different methods that an end device can receive an IPv6 address automatically.

Chapter 13, “ICMP”: This chapter introduces Internet Control Message Protocol (ICMP) tools, such as ping and trace.

Chapter 14, “Transport Layer”: This chapter introduces Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) and examines how each of these protocols transports information across the network. It explores how TCP uses segmentation, the three-way handshake, and expectational acknowledgments to ensure reliable delivery of data. It also examines the best-effort delivery mechanism provided by UDP and describes when its use would be preferred over the use of TCP.

Chapter 15, “Application Layer”: This chapter 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 in the application layer make robust communication across data networks possible. This will be demonstrated by examining some key protocols and services, including HTTP, HTTPS, DNS, DHCP, SMTP/POP, and FTP.

Chapter 16, “Network Security Fundamentals”: This chapter introduces network security threats and vulnerabilities. Various network attacks and mitigation techniques are discussed, along with how to secure network devices.

Chapter 17, “Build a Small Network”: This chapter reexamines the various components in a small network and describes how they work together to allow network growth. It examines network configuration and troubleshooting issues, along with different troubleshooting methodologies.
The “Study Guide” portion of this chapter uses a variety of exercises to test your knowledge of the advances in modern network technologies. The “Labs and Activities” portion of this chapter includes all the online curriculum research lab and Packet Tracer activity instructions.

As you work through this chapter, use Chapter 1 in *Introduction to Networks v7 Companion Guide* or use the corresponding Module 1 in the Introduction to Networks online curriculum for assistance.
Study Guide

Networks Affect Our Lives

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 reality. 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 cloud lets us store documents and pictures and access them anywhere, anytime. So, whether we are on a train, in a park, or standing on top of a mountain, we can seamlessly access our data and applications on a variety of devices.

Network Components

If you want to be a part of a global online community, your computer, tablet, or smartphone must first be connected to a network. That network must be connected to the internet. All computers that are connected to a network and participate directly in network communication are classified as hosts. Hosts can be called end devices. Some hosts are also called clients.

End Devices, Intermediary Devices, and Media

Servers are computers with software that allow them to provide information, like email or web pages, to other end devices on the network. Each service requires separate server software.

Client and server software usually run on separate computers, but it is also possible for one computer to be used for both roles at the same time. In Table 1-1, list the advantages and disadvantages of peer-to-peer networking.

<table>
<thead>
<tr>
<th>Table 1-1</th>
<th>Advantages and Disadvantages of Peer-to-Peer Networking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advantages</td>
<td>Disadvantages</td>
</tr>
</tbody>
</table>

The network devices that people are most familiar with are end devices. An end device is either the source or destination of a message transmitted over the network. When an end device initiates communication, it uses the address of the destination end device to specify where to deliver the message.

Intermediary devices connect the individual end devices to the network. They can connect multiple individual networks to form an internetwork. Intermediary devices use the destination end device address and information about the network interconnections to determine the path that messages should take through the network.
List three examples of intermediary network devices:


List at least three of the main functions of intermediary devices:


Communication transmits across a network on media. The media provides the channel over which the message travels from source to destination. List the three types of media used to interconnect devices:


Check Your Understanding: Network Components

Check your understanding of network components by choosing the BEST answer to each of the following questions.

1. Which of the following is the name for all computers connected to a network that participate directly in network communication?
   a. servers
   b. intermediary devices
   c. hosts
   d. media

2. When data is encoded as pulses of light, which media is being used to transmit the data?
   a. wireless
   b. fiber-optic cable
   c. copper cable

3. Which two devices are intermediary devices? (Choose two.)
   a. hosts
   b. routers
   c. servers
   d. switches
Network Representations and Topologies

Diagrams of networks often use symbols to represent the different devices and connections that make up a network.

Classify and Identify Network Components

In Figure 1-1, label the three major classifications of network components. Then, underneath each icon, label the network component.

**Figure 1-1  Common Network Component Icons**

Topology Diagrams

There are two types of topology diagrams:

- A _______ diagram identifies the physical location of intermediary devices, configured ports, and cable installation.
- A _______ diagram identifies devices, ports, and IP addressing schemes.

Check Your Understanding: Network Representations and Topologies

Check your understanding of network representations and topologies by choosing the BEST answer to each of the following questions.

1. Which connection physically connects an end device to the network?
   - a. port
   - b. NIC
   - c. interface
2. Which connections are specialized ports on a networking device that connect to individual networks?
   a. ports
   b. NICs
   c. interfaces

3. Which type of network topology lets you see which end devices are connected to which intermediary devices and what media is being used?
   a. physical topology
   b. logical topology

4. Which type of network topology lets you see the actual locations of intermediary devices and cable installation?
   a. physical topology
   b. logical topology

Common Types of Networks

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

- Small home networks connect a few computers to each other and to the internet.
- A small office and home office (SOHO) network allows computers in 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 hosts.
- The internet is a network of networks that connects hundreds of millions of computers worldwide.

Compare LANs and WANs

In Table 1-2, indicate whether each feature is a LAN feature or a WAN feature by marking the appropriate column.

<table>
<thead>
<tr>
<th>LANs</th>
<th>WANs</th>
<th>LAN or WAN Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interconnect end devices in a limited area such as a home, a school, an office building, or a campus</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Typically provide slower-speed links between networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provide high-speed bandwidth to internal end devices and intermediary devices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interconnect networks over wide geographic areas, such as between cities, states, provinces, countries, or continents</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Usually administered by multiple service providers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Usually administered by a single organization or individual</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Check Your Understanding: Common Types of Networks

Check your understanding of common types of networks by choosing the BEST answer to each of the following questions.

1. Which network infrastructure provides access to users and end devices in a small geographic area and is typically a network in a department in an enterprise, a home, or a small business?
   a. extranet
   b. intranet
   c. LAN
   d. WAN

2. Which network infrastructure might an organization use to provide secure and safe access to individuals who work for a different organization but require access to the organization’s data?
   a. extranet
   b. intranet
   c. LAN
   d. WAN

3. Which network infrastructure provides access to other networks over a large geographic area and is often owned and managed by a telecommunications service provider?
   a. extranet
   b. intranet
   c. LAN
   d. WAN

Internet Connections

Home users, remote workers, and small offices typically require ISP connections to access the internet. Connection options vary greatly between ISPs and geographic locations. Popular choices include broadband cable, broadband digital subscriber line (DSL), wireless WANs, and mobile services.

Vocabulary Exercise: Matching

Match each definition with the appropriate term. This exercise is a one-to-one matching: Each definition has exactly one matching term.

Definitions

a. Similar to a LAN but wirelessly interconnects users and endpoints in a small geographic area.

b. Requires a clear line of sight, installation costs can be high, and connections tend to be slower and less reliable than its terrestrial competition.
c. Also called a LAN adapter, it provides the physical connection to a network at the PC or other host device.

d. Available from a provider to the customer premises over a dedicated copper or fiber connection providing bandwidth speeds of 10 Mbps to 10 Gbps.

e. The availability of this type of internet access is a real benefit in areas that would otherwise have no internet connectivity at all or for those constantly on the go.

f. Provide the interface between users and the underlying communication network.

g. A network infrastructure that provides access to users and end devices in a small geographic area.

h. Devices that interconnect end devices.

i. Reserved circuits that connect geographically separated offices for private voice and/or data networking. In North America, circuits include T1 (1.54 Mbps) and T3 (44.7 Mbps); in other parts of the world, they are available in E1 (2 Mbps) and E3 (34 Mbps).

j. A private connection of LANs and WANs that belongs to an organization—basically an internetwork that is usually only accessible from within the organization.

k. An inexpensive, very low-bandwidth option to connect to an ISP that should be considered only as a backup to higher-speed connection options.

l. Carries a data signal on the same coaxial media that delivers the television signal. It provides a high-bandwidth, always-on connection to the internet.

m. Provides secure and safe access to individuals who work for different organizations but require access to the company’s data.

n. A network infrastructure that is larger than a LAN but smaller than a WAN and is usually operated by a single organization.

o. Provides the channel over which a message travels from source to destination.

p. A network infrastructure that provides access to other networks over a wide geographic area.

q. Provides a high-bandwidth, always-on connection that runs over a telephone line, with the line split into three channels.

r. A network infrastructure designed to support file servers and provide data storage, retrieval, and replication.

Terms

- DSL
- medium
- metropolitan-area network (MAN)
- network interface card
- Metro Ethernet
- wireless LAN (WLAN)
- dedicated leased line
- satellite
- wide-area network (WAN)
- intranet
- storage-area network (SAN)
- cellular
- dial-up telephone
- cable
- local-area network (LAN)
- end devices
- intermediary devices
- extranet
Reliable Networks
Networks support a wide range of applications and services and must operate over many different types of cables and devices that make up the physical infrastructure. As networks evolve, we are discovering that the underlying architectures need to address four basic characteristics to meet user expectations:

- Fault tolerance
- Scalability
- Quality of service (QoS)
- Security

Classify the Requirements for a Reliable Network

In Table 1-3, select the appropriate column to classify each of the requirements for a reliable network.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Characteristic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preventing unauthorized access to the management software that resides on network devices.</td>
<td>Fault Tolerance</td>
</tr>
<tr>
<td>Common network standards allow hardware and software vendors to focus on product improvements and services.</td>
<td>Scalability</td>
</tr>
<tr>
<td>The fewest number of devices are impacted by a network outage.</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>Networks can grow or expand with minimal impact on performance.</td>
<td>Security</td>
</tr>
<tr>
<td>Protecting the information contained in packets as they are transmitted over the network.</td>
<td></td>
</tr>
<tr>
<td>Priority queues are implemented when demand for network bandwidth exceeds supply.</td>
<td></td>
</tr>
<tr>
<td>Data can travel through more than one route for delivery from a remote source.</td>
<td></td>
</tr>
<tr>
<td>The primary mechanism for managing congestion and ensuring reliable delivery of content.</td>
<td></td>
</tr>
<tr>
<td>Includes the goals of confidentiality, integrity, and availability.</td>
<td></td>
</tr>
</tbody>
</table>
Check Your Understanding: Reliable Networks

Check your understanding of reliable networks by choosing the BEST answer to each of the following questions.

1. When designers follow accepted standards and protocols, which of the four basic characteristics of network architecture is achieved?
   a. fault tolerance
   b. scalability
   c. QoS
   d. security

2. Confidentiality, integrity, and availability are requirements of which of the four basic characteristics of network architecture?
   a. fault tolerance
   b. scalability
   c. QoS
   d. security

3. With which type of policy can a router manage the flow of data and voice traffic, giving priority to voice communications if the network experiences congestion?
   a. fault tolerance
   b. scalability
   c. QoS
   d. security

4. Having multiple paths to a destination is known as redundancy. This is an example of which characteristic of network architecture?
   a. fault tolerance
   b. scalability
   c. QoS
   d. security

Network Trends

As new technologies and end-user devices come to market, businesses and consumers must continue to adjust to this ever-changing environment. Several networking trends affect organizations and consumers:

- **Bring your own device (BYOD):** Enables end users the freedom to use personal tools to access information and communicate across a business or campus network. BYOD means any device, with any ownership, used anywhere.

- **Online collaboration:** Includes network-enabled tools that give employees, students, teachers, customers, and partners a way to instantly connect, interact, and achieve their objectives. Collaboration is a critical and strategic priority that organizations are using to remain competitive and that students use to assist each other in learning.
- **Video communications**: Used for communications, collaboration, and entertainment. In addition to video calls made anywhere to anywhere, video conferencing has become an effective collaboration tool as organizations extend across geographic and cultural boundaries.

- **Cloud computing**: Allows us to store personal files and even back up an entire drive on servers over the internet. Applications such as word processing and photo editing can be accessed using the cloud.

### Identify the Cloud Type

In Table 1-4, fill in the cloud type for each description.

<table>
<thead>
<tr>
<th>Cloud Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cloud-based applications and services offered in this cloud type are intended for a specific organization or entity, such as a government. This cloud type can be set up using the organization’s private network, although this can be expensive to build and maintain. This cloud type can also be managed by an outside organization with strict access security.</td>
</tr>
<tr>
<td></td>
<td>Cloud-based applications and services offered in this cloud type 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. This cloud type uses the internet to provide services.</td>
</tr>
<tr>
<td></td>
<td>This cloud type is made up of two or more clouds, where each part remains a distinct object but the parts are connected using a single architecture. Individuals using this cloud type would be able to have degrees of access to various services based on user access rights.</td>
</tr>
<tr>
<td></td>
<td>This cloud type is created for exclusive use by specific entities or organizations. The differences between public clouds and this cloud type are the functional needs that have been customized for a group of users. For example, healthcare organizations must remain compliant with policies and laws (for example, HIPAA) that require special authentication and confidentiality. This cloud type would be used by multiple organizations that have similar needs and concerns.</td>
</tr>
</tbody>
</table>

### Check Your Understanding: Network Trends

Check your understanding of network trends by choosing the BEST answer to each of the following questions.

1. Which feature is a good conferencing tool to use with others who are located elsewhere in your city, in another city, or even in another country?
   - a. BYOD
   - b. video communications
   - c. cloud computing
2. Which feature describes using personal tools to access information and communicate across a business or campus network?
   a. BYOD
   b. video communications
   c. cloud computing

3. Which of the following offers options such as public, private, custom, and hybrid?
   a. BYOD
   b. video communications
   c. cloud computing

4. Which feature is being used when connecting a device to the network using an electrical outlet?
   a. smart home technology
   b. powerline
   c. wireless broadband

5. Which feature uses the same cellular technology as a smartphone?
   a. smart home technology
   b. powerline
   c. wireless broadband

Network Security

Network security is an integral part of computer networking, regardless of whether the network is in a home with a single connection to the internet or is a corporation with thousands of users. Network security must consider 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 users expect of the network.

Securing a network involves protocols, technologies, devices, tools, and techniques in order to protect data and mitigate threats. Threat vectors may be external or internal. Many external network security threats today originate from the internet.

Check Your Understanding: Network Security

Check your understanding of network security by choosing the BEST answer to each of the following questions.

1. Which attack slows down or crashes equipment and programs?
   a. firewall
   b. virus, worm, or Trojan horse
   c. zero-day or zero-hour
   d. virtual private network (VPN)
   e. denial of service (DoS)
2. Which option creates a secure connection for remote workers?
   a. firewall
   b. virus, worm, or Trojan horse
   c. zero-day or zero-hour
   d. virtual private network (VPN)
   e. denial of service (DoS)

3. Which option blocks unauthorized access to a network?
   a. firewall
   b. virus, worm, or Trojan horse
   c. zero-day or zero-hour
   d. virtual private network (VPN)
   e. denial of service (DoS)

4. Which option describes a network attack that occurs on the first day that a vulnerability becomes known?
   a. firewall
   b. virus, worm, or Trojan horse
   c. zero-day or zero-hour
   d. virtual private network (VPN)
   e. denial of service (DoS)

5. Which option describes malicious code running on user devices?
   a. Firewall
   b. virus, worm, or Trojan horse
   c. zero-day or zero-hour
   d. virtual private network (VPN)
   e. denial of service (DoS)

The IT Professional

The roles and skills of network engineers are evolving and are more vital than ever. The Cisco Certified Network Associate (CCNA) certification demonstrates that you have a knowledge of foundational technologies and ensures that you stay relevant with skill sets needed for the adoption of next-generation technologies. The new CCNA focuses on IP foundation and security topics along with wireless, virtualization, automation, and network programmability.

Your CCNA certification will prepare you for a variety of jobs in today’s market. At www.netacad.com, you can click the Careers menu and then select Employment Opportunities. You can also search for IT jobs using online search engines such as Indeed, Glassdoor, and Monster.