# Contents

*Introduction* xxx

*Assessment Test* lxvi

## Chapter 1  Introduction to Networks 1

First Things First: What’s a Network? 2  
The Local Area Network 3  
Common Network Components 5  
Wide Area Network 7  
Network Architecture: Peer-to-Peer or Client-Server? 9  
Physical Network Topologies 11  
Bus Topology 12  
Star Topology 13  
Ring Topology 14  
Mesh Topology 15  
Point-to-Point Topology 16  
Point-to-Multipoint Topology 17  
Hybrid Topology 18  
Topology Selection, Backbones, and Segments 19  
Selecting the Right Topology 19  
The Network Backbone 20  
Network Segments 21  
CAN 21  
SAN 21  
Summary 21  
Exam Essentials 22  
Written Lab 22  
Review Questions 23

## Chapter 2  The Open Systems Interconnection Specifications 27

Internetworking Models 28  
The Layered Approach 29  
Advantages of Reference Models 29  
The OSI Reference Model 30  
The Application Layer 32  
The Presentation Layer 33  
The Session Layer 33  
The Transport Layer 33  
The Network Layer 40
Contents

The Data Link Layer 42
The Physical Layer 45
Introduction to Encapsulation 45
Modulation Techniques 46
Summary 47
Exam Essentials 48
Written Lab 48
Review Questions 50

Chapter 3 Networking Topologies, Connectors, and Wiring Standards 55

Physical Media 57
  Coaxial Cable 58
  Twisted-Pair Cable 60
  Fiber-Optic Cable 64
  Transceivers 69
  Media Converters 69
  Serial Cables 71
Cable Properties 73
  Transmission Speeds 73
  Distance 74
  Duplex 74
  Noise Immunity (Security, EMI) 74
  Frequency 75
Wiring Standards 75
  T568A vs. T568B 75
  Straight-Through Cable 77
  Crossover Cable 78
  Rolled/Rollover Cable 80
  T1 Crossover Cable 80
Installing Wiring Distributions 82
  MDF/IDF 82
Summary 84
Exam Essentials 85
Written Lab 85
Review Questions 87

Chapter 4 The Current Ethernet Specifications 91

Network Basics 92
Ethernet Basics 94
  Collision Domain 94
  Broadcast Domain 94
  CSMA/CD 95
  Broadband/Baseband 96
Chapter 5  Networking Devices  125

Common Network Connectivity Devices  128
   Network Interface Card  129
   Hub  130
   Bridge  131
   Switch  131
   Router  132
   Firewall  136
   IDS/IPS  137
   HIDS  137
   Access Point  138
   Wireless Range Extender  138
   Contention Methods  139
   Dynamic Host Configuration Protocol Server  141
   IPAM  146

Other Specialized Devices  146
   Multilayer Switch  147
   Load Balancer  147
   Domain Name Service Server  148
   Proxy Server  154
   Encryption Devices  155
   Analog Modem  156
   Packet Shaper  157
   VPN Concentrator  157
   Media Converter  158
   VoIP PBX  158
   VoIP Endpoint  158
   NGFW/Layer 7 Firewall  159
   VoIP Gateway  159

Bit Rates vs. Baud Rate  97
Wavelength  97
Half- and Full-Duplex Ethernet  98
Ethernet at the Data Link Layer  99
   Binary to Decimal and Hexadecimal Conversion  100
   Ethernet Addressing  103
   Ethernet Frames  104
Ethernet at the Physical Layer  106
Ethernet over Other Standards (IEEE 1905.1-2013)  111
   Ethernet over Power Line  112
   Ethernet over HDMI  113
Summary  114
Exam Essentials  115
Written Lab  115
Review Questions  120
Planning and Implementing a Basic SOHO Network
Using Network Segmentation 159
Determining Requirements 159
Switches and Bridges at the Data Link Layer 166
Hubs at the Physical Layer 167
Environmental Considerations 168
Summary 169
Exam Essentials 169
Written Lab 170
Review Questions 171

Chapter 6  Introduction to the Internet Protocol 175
Introducing TCP/IP 177
A Brief History of TCP/IP 177
TCP/IP and the DoD Model 178
The Process/Application Layer Protocols 180
The Host-to-Host Layer Protocols 188
The Internet Layer Protocols 192
Data Encapsulation 198
Summary 202
Exam Essentials 202
Written Lab 203
Review Questions 204

Chapter 7  IP Addressing 209
IP Terminology 210
The Hierarchical IP Addressing Scheme 211
Network Addressing 212
Private IP Addresses (RFC 1918) 216
IPv4 Address Types 218
Layer 2 Broadcasts 219
Layer 3 Broadcasts 219
Unicast Address 219
Multicast Address (Class D) 219
Internet Protocol Version 6 (IPv6) 220
Why Do We Need IPv6? 220
The Benefits of and Uses for IPv6 221
IPv6 Addressing and Expressions 222
Shortened Expression 223
Address Types 224
Special Addresses 225
Stateless Autoconfiguration (EUI-64) 226
DHCPv6 (Stateful) 227
Migrating to IPv6 227
Summary
Exam Essentials
Written Labs
  Written Lab 7.1
  Written Lab 7.2
  Written Lab 7.3
Review Questions

Chapter 8  IP Subnetting, Troubleshooting IP, and Introduction to NAT

Subnetting Basics
  How to Create Subnets
  Subnet Masks
  Classless Inter-Domain Routing (CIDR)
  Subnetting Class C Addresses
  Subnetting Class B Addresses
Troubleshooting IP Addressing
  Determining IP Address Problems
Introduction to Network Address Translation (NAT)
  Types of Network Address Translation
  NAT Names
  How NAT Works
Summary
Exam Essentials
Written Lab
Review Questions

Chapter 9  Introduction to IP Routing

Routing Basics
The IP Routing Process
Testing Your IP Routing Understanding
Static and Dynamic Routing
Summary
Exam Essentials
Written Lab
Review Questions

Chapter 10  Routing Protocols

Routing Protocol Basics
  Administrative Distances
  Classes of Routing Protocols
Distance Vector Routing Protocols
  Routing Information Protocol (RIP)
  RIP Version 2 (RIPv2)
Contents

VLSM and Discontiguous Networks 309
EIGRP 312
Border Gateway Protocol (BGP) 314
Link State Routing Protocols 315
    Open Shortest Path First (OSPF) 316
    Intermediate System-to-Intermediate System (IS-IS) 318
High Availability 319
    Hot Standby Router Protocol (HSRP) 321
    Virtual Router Redundancy Protocol 325
Advanced IPv6 Concepts 326
    Router Advertisement 326
    Neighbor Discovery 328
    Tunneling 329
    Dual Stack 332
IPv6 Routing Protocols 332
    RIPng 333
    EIGRPv6 333
    OSPFv3 333
Summary 334
Exam Essentials 334
Written Lab 335
Review Questions 336

Chapter 11  Switching and Virtual LANs 341
Networking Before Layer 2 Switching 343
Switching Services 346
    Limitations of Layer 2 Switching 347
    Bridging vs. LAN Switching 348
    Three Switch Functions at Layer 2 348
    Distributed Switching 354
Spanning Tree Protocol 354
    Spanning Tree Port States 355
    STP Convergence 356
    Rapid Spanning Tree Protocol 802.1w 357
Virtual LANs 358
    VLAN Basics 359
    Quality of Service 362
    VLAN Memberships 363
    Static VLANs 363
    Dynamic VLANs 364
    Identifying VLANs 364
    VLAN Identification Methods 366
VLAN Trunking Protocol
  VTP Modes of Operation
  Do We Really Need to Put an IP Address on a Switch?
  Switch Port Protection
  Port Bonding
  Device Hardening
Two Additional Advanced Features of Switches
  Power over Ethernet (802.3af, 802.3at)
  Port Mirroring/Spanning (SPAN/RSPAN)
Summary
Exam Essentials
Written Lab
Review Questions

<table>
<thead>
<tr>
<th>Chapter 12</th>
<th>Wireless Networking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to Wireless Technology</td>
<td>390</td>
</tr>
<tr>
<td>Cellular</td>
<td>393</td>
</tr>
<tr>
<td>The 802.11 Standards</td>
<td>393</td>
</tr>
<tr>
<td>2.4 GHz (802.11b)</td>
<td>395</td>
</tr>
<tr>
<td>2.4 GHz (802.11g)</td>
<td>396</td>
</tr>
<tr>
<td>5 GHz (802.11a)</td>
<td>397</td>
</tr>
<tr>
<td>5 GHz (802.11h)</td>
<td>397</td>
</tr>
<tr>
<td>2.4 GHz/5 GHz (802.11n)</td>
<td>398</td>
</tr>
<tr>
<td>5 GHz (802.11ac)</td>
<td>399</td>
</tr>
<tr>
<td>Comparing 802.11 Standards</td>
<td>399</td>
</tr>
<tr>
<td>Range Comparisons</td>
<td>400</td>
</tr>
<tr>
<td>Wireless Network Components</td>
<td>401</td>
</tr>
<tr>
<td>Wireless Access Points</td>
<td>401</td>
</tr>
<tr>
<td>Wireless Network Interface Card</td>
<td>402</td>
</tr>
<tr>
<td>Wireless Antennas</td>
<td>403</td>
</tr>
<tr>
<td>Installing a Wireless Network</td>
<td>405</td>
</tr>
<tr>
<td>Ad Hoc Mode: Independent Basic Service Set</td>
<td>405</td>
</tr>
<tr>
<td>Infrastructure Mode: Basic Service Set</td>
<td>406</td>
</tr>
<tr>
<td>Wireless Controllers</td>
<td>407</td>
</tr>
<tr>
<td>Mobile Hot Spots</td>
<td>409</td>
</tr>
<tr>
<td>Signal Degradation</td>
<td>410</td>
</tr>
<tr>
<td>Other Network Infrastructure Implementations</td>
<td>410</td>
</tr>
<tr>
<td>Technologies that facilitate the Internet of Things (IoT)</td>
<td>412</td>
</tr>
<tr>
<td>Installing and Configuring WLAN Hardware</td>
<td>412</td>
</tr>
<tr>
<td>Site Survey</td>
<td>418</td>
</tr>
<tr>
<td>Providing Capacity</td>
<td>418</td>
</tr>
<tr>
<td>Multiple Floors</td>
<td>420</td>
</tr>
<tr>
<td>Location-Based WLAN</td>
<td>421</td>
</tr>
<tr>
<td>Site Survey Tools</td>
<td>421</td>
</tr>
</tbody>
</table>
Wireless Security
  Wireless Threats
  Open Access
  Service Set Identifiers, Wired Equivalent Privacy, and Media Access Control Address Authentication
  Remote Authentication Dial-In User Service (802.1X)
  Temporal Key Integrity Protocol
  Wi-Fi Protected Access or WPA2 Pre-Shared Key
Summary
Exam Essentials
Written Lab
Review Questions

Chapter 13  Authentication and Access Control

Security Filtering
  Access Control Lists
  Tunneling
  Encryption
  Remote Access
Managing User Account and Password Security
  Managing User Accounts
  Managing Passwords
  Single Sign-On
  Local Authentication
  LDAP
  Certificates
  Multifactor Authentication
User-Authentication Methods
  Public Key Infrastructure (PKI)
  Kerberos
  Authentication, Authorization, and Accounting (AAA)
  Web Services
  Unified Voice Services
  Network Controllers
  Network Access Control (NAC)
  Challenge Handshake Authentication Protocol (CHAP)
  MS-CHAP
  Extensible Authentication Protocol (EAP)
  Hashes
  Network Access Control
Summary
Exam Essentials
Written Lab
Review Questions
**Chapter 15  **

**Physical Security and Risk**

Using Hardware and Software Security Devices 545
- Defining Firewalls 547
  - Network-Based Firewalls 548
  - Host-Based Firewalls 548
- Firewall Technologies 548
  - Access Control Lists 549
  - Port Security 551
  - Demilitarized Zone 552
  - Protocol Switching 553
  - Dynamic Packet Filtering 555
  - Proxy Services 556
- Firewalls at the Application Layer vs. the Network Layer 558
  - Stateful vs. Stateless Network Layer Firewalls 559
  - NGFW/Layer7 Firewall 560
- Scanning Services and Other Firewall Features 561
  - Content Filtering 562
  - Signature Identification 563
  - Context Awareness 563
  - Virtual Wire vs. Routed 563
  - Zones 564
- Intrusion Detection and Prevention Systems 566
  - Network-Based IDS 567
  - Host-Based IDS 569
  - Vulnerability Scanners 570
- VPN Concentrators 571
- Understanding Problems Affecting Device Security 572
  - Physical Security 572
  - Logical Security Configurations 577
  - Risk-Related Concepts 579
- Summary 586
- Exam Essentials 587
- Written Lab 588
- Review Questions 589

**Chapter 16  **

**Wide Area Networks**

- What’s a WAN? 596
  - Defining WAN Terms 596
  - The Public Switched Telephone Network 598
Chapter 17  Troubleshooting Tools  635

WAN Connection Types  599
Bandwidth or Speed  600
T-Series Connections  601
The T1 Connection  602
The T3 Connection  603
Transmission Media  603
Wired Connections  603
Wavelength Division Multiplexing  604
Passive Optical Network  605
Wireless Technologies  605
Broadband Services  607
DSL Technology and xDSL  608
Cable Modem  610
Wireless WAN Technologies  611
Cellular WAN  612
WAN Protocols  613
Integrated Services Digital Network  613
Frame Relay Technology  615
Point-to-Point Protocol  618
DMVPN  621
SIP Trunks  621
Asynchronous Transfer Mode  622
MPLS  623
WAN Troubleshooting  623
Loss of Internet Connectivity  624
Interface Errors/Monitoring  624
Split Horizon  627
DNS Issues  628
Router Configurations  628
Company Security Policy  629
Summary  629
Exam Essentials  630
Written Lab  631
Review Questions  632

Protocol Analyzers  637
Throughput Testers  638
Connectivity Software  639
Using \texttt{traceroute}  640
Using \texttt{ipconfig} and \texttt{ifconfig}  642
Using the \texttt{ifconfig} Utility  646
Using the \texttt{iptables} utility  646
Using the ping Utility 647
Using the Address Resolution Protocol 650
   The Windows ARP Table 651
   Using the arp Utility 651
Using the nslookup Utility 654
Resolving Names with the Hosts Table 656
Using the Mtr Command (pathping) 657
   Using the Nmap Utility 658
Using the route Command 659
   Using the route Command Options 661
   Some Examples of the route Command 662
Using the nbtstat Utility 663
   The –a Switch 663
   The –A Switch 665
   The –c Switch 665
   The –n Switch 666
   The –r Switch 666
   The –R Switch 667
   The –S Switch 668
   The –s Switch 668
Using the netstat Utility 669
   The –a Switch 671
   The –c Switch 672
   The –r Switch 673
   The –s Switch 673
   The –p Switch 673
   The –n Switch 675
Using tcpdump 676
   Examples of Using tcpdump 676
Using the File Transfer Protocol 677
   Starting FTP and Logging In to an FTP Server 678
   Downloading Files 679
   Uploading Files 681
Using the Telnet Utility 682
   How to Enable Telnet in Windows 682
   Don’t Use Telnet, Use Secure Shell 683
Summary 684
Exam Essentials 684
Written Lab 685
Review Questions 686
Chapter 18  Software and Hardware Tools  691

Understanding Network Scanners  693
   Packet Sniffers/Network Monitors  693
   Intrusion Detection and Prevention Software  695
Port Scanners  697
Wi-Fi Analyzer  700
Bandwidth Speed Tester  701
Baseline  702
Network Monitoring and Logging  703
   Network Monitoring  703
   SNMP  704
   Syslog  705
   SIEM  707
Utilization  710
Identifying Hardware Tools  712
   Cable Testers  712
   Protocol Analyzer  715
   Certifiers  716
   Time-Domain Reflectometer  717
   Optical Time-Domain Reflectometer  717
   Multimeter  718
   Spectrum Analyzer  719
   Toner Generator (Probe)  720
   Metrics  721
   Butt Set  721
   Punch-Down Tool  722
   Cable Stripper/Snips  723
   Voltage Event Recorder (Power)  723
   Environmental Monitors  724
Summary  725
Exam Essentials  725
Written Lab  726
Review Questions  727

Chapter 19  Network Troubleshooting  731

Narrowing Down the Problem  734
   Did You Check the Super Simple Stuff?  735
   Is Hardware or Software Causing the Problem?  738
   Is It a Workstation or a Server Problem?  739
   Which Segments of the Network Are Affected?  740
   Is It Bad Cabling?
Troubleshooting Steps 749
  Step 1: Identify the Problem 750
  Step 2: Establish a Theory of Probable Cause 754
  Step 3: Test the Theory to Determine Cause 762
  Step 4: Establish a Plan of Action to Resolve the Problem and Identify Potential Effects 764
  Step 5: Implement the Solution or Escalate as Necessary 766
  Step 6: Verify Full System Functionality, and If Applicable, Implement Preventative Measures 769
  Step 7: Document Findings, Actions, and Outcomes 769
Troubleshooting Tips 770
  Don’t Overlook the Small Stuff 770
  Prioritize Your Problems 771
  Check the Software Configuration 771
  Don’t Overlook Physical Conditions 772
  Don’t Overlook Cable Problems 772
  Check for Viruses 773
Summary 773
Exam Essentials 774
Written Lab 774
Review Questions 776

Chapter 20  Management, Monitoring, and Optimization 781
Managing Network Documentation 785
  Using SNMP 785
  Schematics and Diagrams 786
Network Monitoring 795
  Baselines 795
  Processes 796
  On-Boarding and Off-Boarding of Mobile Devices 796
  NAC 796
  Policies, Procedures, and Regulations 797
  Safety Practices 801
  Implementing Network Segmentation 805
Network Optimization 808
  Reasons to Optimize Your Network’s Performance 808
  How to Optimize Performance 811
  Unified Communications 813
  Traffic Shaping 813
  Load Balancing 814
  High Availability 814
  Caching Engines 815
  Fault Tolerance 815
Appendix A  Answers to Written Labs  841

Chapter 1: Introduction to Networks  842
Chapter 2: The Open Systems Interconnection Specifications  842
Chapter 3: Networking Topologies, Connectors, and Wiring Standards  843
Chapter 4: The Current Ethernet Specifications  843
Chapter 5: Networking Devices  845
Chapter 6: Introduction to the Internet Protocol  846
Chapter 7: IP Addressing
  Written Lab 7.1  847
  Written Lab 7.2  847
  Written Lab 7.3  848
Chapter 8: IP Subnetting, Troubleshooting IP, and Introduction to NAT  848
Chapter 9: Introduction to IP Routing  849
Chapter 10: Routing Protocols  849
Chapter 11: Switching and Virtual LANs  850
Chapter 12: Wireless Networking  850
Chapter 13: Authentication and Access Control  850
Chapter 14: Network Threats and Mitigation  851
Chapter 15: Physical Security and Risk  851
Chapter 16: Wide Area Networks  852
Chapter 17: Troubleshooting Tools  852
Chapter 18: Software and Hardware Tools  853
Chapter 19: Network Troubleshooting  853
Chapter 20: Management, Monitoring, and Optimization  854

Appendix B  Answers to Review Questions  855

Chapter 1: Introduction to Networks  856
Chapter 2: The Open Systems Interconnection Specifications  857
Chapter 3: Networking Topologies, Connectors, and Wiring Standards  859
Chapter 4: The Current Ethernet Specifications  860
<table>
<thead>
<tr>
<th>Appendix C Subnetting Class A</th>
<th>887</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnetting Practice Examples: Class A Addresses</td>
<td>888</td>
</tr>
<tr>
<td>Practice Example #1A: 255.255.0.0 (/16)</td>
<td>888</td>
</tr>
<tr>
<td>Practice Example #2A: 255.255.240.0 (/20)</td>
<td>889</td>
</tr>
<tr>
<td>Practice Example #3A: 255.255.255.192 (/26)</td>
<td>889</td>
</tr>
<tr>
<td>Subnetting in Your Head: Class A Addresses</td>
<td>890</td>
</tr>
<tr>
<td>Written Lab 1</td>
<td>891</td>
</tr>
<tr>
<td>Written Lab 2</td>
<td>892</td>
</tr>
<tr>
<td>Answers to Written Lab 1</td>
<td>892</td>
</tr>
<tr>
<td>Answers to Written Lab 2</td>
<td>893</td>
</tr>
</tbody>
</table>

Index 895