## Contents at a Glance

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>Introduction to Networking</td>
<td>9</td>
</tr>
<tr>
<td>CHAPTER 2</td>
<td>OSI and TCP/IP Models and Network Protocols</td>
<td>43</td>
</tr>
<tr>
<td>CHAPTER 3</td>
<td>Addressing and Routing</td>
<td>93</td>
</tr>
<tr>
<td>CHAPTER 4</td>
<td>Components and Devices</td>
<td>135</td>
</tr>
<tr>
<td>CHAPTER 5</td>
<td>Installation and Configuration</td>
<td>167</td>
</tr>
<tr>
<td>CHAPTER 6</td>
<td>Cabling and Wiring</td>
<td>209</td>
</tr>
<tr>
<td>CHAPTER 7</td>
<td>Wireless</td>
<td>259</td>
</tr>
<tr>
<td>CHAPTER 8</td>
<td>Network Management</td>
<td>303</td>
</tr>
<tr>
<td>CHAPTER 9</td>
<td>Network Optimization</td>
<td>381</td>
</tr>
<tr>
<td>CHAPTER 10</td>
<td>Network Security</td>
<td>413</td>
</tr>
<tr>
<td>CHAPTER 11</td>
<td>Network Troubleshooting</td>
<td>475</td>
</tr>
<tr>
<td></td>
<td>Practice Exam 1</td>
<td>513</td>
</tr>
<tr>
<td></td>
<td>Answers to Practice Exam 1</td>
<td>537</td>
</tr>
<tr>
<td></td>
<td>Practice Exam 2</td>
<td>561</td>
</tr>
<tr>
<td></td>
<td>Answers to Practice Exam 2</td>
<td>585</td>
</tr>
<tr>
<td></td>
<td>Glossary</td>
<td>607</td>
</tr>
<tr>
<td></td>
<td>Index</td>
<td>649</td>
</tr>
</tbody>
</table>
# Table of Contents

**Introduction** .......................................................... 1

- About Network+ Exam Cram ........................................ 1
- About the Network+ Exam ........................................... 2
- CompTIA Network+ Exam Topics ................................ 2
- Booking and Taking the Network+ Certification Exam ........ 4
- What to Expect from the Exam ..................................... 5
- A Few Exam Day Details .............................................. 5
- After the Test ....................................................... 6
- Last-Minute Exam Tips ............................................. 6

**CHAPTER 1: Introduction to Networking** ......................... 9

- LANs, WANs, and Network Models ................................ 10
  - LANs ............................................................. 10
  - WANs ............................................................. 11
  - Network Models ................................................ 12
  - Centralized Computing versus Distributed Computing .... 14
  - Cram Quiz Answers ............................................ 15
- Network Topologies ................................................... 16
  - Bus Topology .................................................... 16
  - Ring Topology .................................................... 18
  - Star Topology .................................................... 19
  - Mesh Topology ................................................... 20
  - Wireless Topologies ............................................. 22
  - Point-to-Point, Point-to-Multipoint, and Wireless Mesh Topologies .................................................... 24
  - Hybrid Topologies .............................................. 27
  - Cram Quiz Answers ............................................. 31
- Going Virtual .......................................................... 32
  - Virtual Private Networks (VPNs) ............................... 32
  - Virtual Local Area Networks (VLANs) ......................... 35
  - Cram Quiz Answers ............................................. 40
- What Next? ........................................................... 41
CHAPTER 2:
OSI and TCP/IP Models and Network Protocols ........................... 43

The Networking Models ............................................. 44
The OSI Seven-Layer Model ........................................... 44
The TCP/IP Four-Layer Model ........................................ 49
Identifying the OSI Layers at Which Various Network Components Operate ........................................ 50
Cram Quiz Answers ....................................................... 51

Protocols ....................................................................... 53
Connection-Oriented Protocols Versus Connectionless Protocols ....... 54
Internet Protocol (IP) ..................................................... 55
Transmission Control Protocol (TCP) ................................ 55
User Datagram Protocol (UDP) ......................................... 56
File Transfer Protocol (FTP) ............................................. 57
Secure File Transfer Protocol (SFTP) ................................ 58
Trivial File Transfer Protocol (TFTP) ................................ 59
Simple Mail Transfer Protocol (SMTP) ............................... 59
Hypertext Transfer Protocol (HTTP) ................................ 60
Hypertext Transfer Protocol Secure (HTTPS) ....................... 60
Telnet ............................................................................. 62
Secure Shell (SSH) .......................................................... 62
Internet Control Message Protocol (ICMP) .......................... 63
Address Resolution Protocol (ARP)/Reverse Address Resolution Protocol (RARP) .......................... 63
Network Time Protocol (NTP) .......................................... 65
Network News Transfer Protocol (NNTP) ............................ 66
Secure Copy Protocol (SCP) ............................................. 66
Lightweight Directory Access Protocol (LDAP) ...................... 66
Internet Group Management Protocol (IGMP) ....................... 67
Transport Layer Security .................................................. 67
Session Initiation Protocol (SIP)/Real-Time Transport Protocol (RTP) ........................................ 68
TCP/IP Protocol Suite Summary ....................................... 69
Cram Quiz Answers ....................................................... 73

Domain Name Service (DNS) ............................................. 74
The DNS Namespace ...................................................... 76
Types of DNS Entries ..................................................... 78
DNS Records ............................................................... 78
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS in a Practical Implementation</td>
<td>79</td>
</tr>
<tr>
<td>Cram Quiz Answers</td>
<td>81</td>
</tr>
<tr>
<td>Simple Network Management Protocol (SNMP)</td>
<td>82</td>
</tr>
<tr>
<td>Components of SNMP</td>
<td>83</td>
</tr>
<tr>
<td>SNMP Management Systems</td>
<td>83</td>
</tr>
<tr>
<td>SNMP Agents</td>
<td>84</td>
</tr>
<tr>
<td>Management Information Bases (MIBs)</td>
<td>85</td>
</tr>
<tr>
<td>SNMP Communities</td>
<td>85</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>86</td>
</tr>
<tr>
<td>Cram Quiz Answers</td>
<td>87</td>
</tr>
<tr>
<td>Dynamic Host Configuration Protocol (DHCP)</td>
<td>88</td>
</tr>
<tr>
<td>The DHCP Process</td>
<td>89</td>
</tr>
<tr>
<td>DHCP and DNS Suffixes</td>
<td>90</td>
</tr>
<tr>
<td>Cram Quiz Answers</td>
<td>91</td>
</tr>
<tr>
<td>What Next?</td>
<td>92</td>
</tr>
<tr>
<td>CHAPTER 3: Addressing and Routing</td>
<td>93</td>
</tr>
<tr>
<td>IP Addressing</td>
<td>94</td>
</tr>
<tr>
<td>IPv4</td>
<td>95</td>
</tr>
<tr>
<td>IP Address Classes</td>
<td>95</td>
</tr>
<tr>
<td>Subnet Mask Assignment</td>
<td>96</td>
</tr>
<tr>
<td>Subnetting</td>
<td>97</td>
</tr>
<tr>
<td>Identifying the Differences Between IPv4 Public and Private Networks</td>
<td>98</td>
</tr>
<tr>
<td>Classless Interdomain Routing (CIDR)</td>
<td>100</td>
</tr>
<tr>
<td>Default Gateways</td>
<td>100</td>
</tr>
<tr>
<td>IPv4 Address Types</td>
<td>102</td>
</tr>
<tr>
<td>IPv6 Addressing</td>
<td>102</td>
</tr>
<tr>
<td>Comparing IPv4 and IPv6 Addressing</td>
<td>106</td>
</tr>
<tr>
<td>Assigning IP Addresses</td>
<td>107</td>
</tr>
<tr>
<td>Identifying MAC Addresses</td>
<td>110</td>
</tr>
<tr>
<td>Network Address Translation (NAT) and Port Address Translation (PAT)</td>
<td>112</td>
</tr>
<tr>
<td>Cram Quiz Answers</td>
<td>116</td>
</tr>
<tr>
<td>Understanding TCP/UDP Port Functions</td>
<td>117</td>
</tr>
<tr>
<td>Cram Quiz Answers</td>
<td>119</td>
</tr>
<tr>
<td>Managing TCP/IP Routing</td>
<td>120</td>
</tr>
<tr>
<td>The Default Gateway</td>
<td>120</td>
</tr>
<tr>
<td>Routing Tables</td>
<td>121</td>
</tr>
</tbody>
</table>
### Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static Routing</td>
<td>122</td>
</tr>
<tr>
<td>Dynamic Routing</td>
<td>123</td>
</tr>
<tr>
<td>Routing Metrics</td>
<td>127</td>
</tr>
<tr>
<td>Cram Quiz Answers</td>
<td>128</td>
</tr>
<tr>
<td>Configuring Routers and Switches</td>
<td>129</td>
</tr>
<tr>
<td>Power over Ethernet (PoE)</td>
<td>129</td>
</tr>
<tr>
<td>The Spanning Tree Protocol (STP)</td>
<td>130</td>
</tr>
<tr>
<td>Trunking</td>
<td>131</td>
</tr>
<tr>
<td>Port Mirroring</td>
<td>132</td>
</tr>
<tr>
<td>Port Authentication</td>
<td>132</td>
</tr>
<tr>
<td>Cram Quiz Answers</td>
<td>133</td>
</tr>
<tr>
<td>What Next?</td>
<td>134</td>
</tr>
</tbody>
</table>

#### CHAPTER 4: Components and Devices

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Network Devices</td>
<td>135</td>
</tr>
<tr>
<td>Bridges</td>
<td>136</td>
</tr>
<tr>
<td>DHCP Server</td>
<td>138</td>
</tr>
<tr>
<td>Firewalls</td>
<td>139</td>
</tr>
<tr>
<td>Hubs</td>
<td>140</td>
</tr>
<tr>
<td>Media Converters</td>
<td>141</td>
</tr>
<tr>
<td>Modems</td>
<td>142</td>
</tr>
<tr>
<td>Network Cards</td>
<td>142</td>
</tr>
<tr>
<td>Routers</td>
<td>145</td>
</tr>
<tr>
<td>Switches</td>
<td>146</td>
</tr>
<tr>
<td>Wireless Access Points</td>
<td>149</td>
</tr>
<tr>
<td>Encryption Devices</td>
<td>150</td>
</tr>
<tr>
<td>Cram Quiz Answers</td>
<td>152</td>
</tr>
<tr>
<td>Specialized Network Devices</td>
<td>153</td>
</tr>
<tr>
<td>Bandwidth Shaper</td>
<td>154</td>
</tr>
<tr>
<td>Content Filter</td>
<td>155</td>
</tr>
<tr>
<td>Load Balancer</td>
<td>155</td>
</tr>
<tr>
<td>Multilayer and Content Switches</td>
<td>155</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>156</td>
</tr>
<tr>
<td>VPN Concentrator</td>
<td>158</td>
</tr>
<tr>
<td>Network Devices Summary</td>
<td>159</td>
</tr>
<tr>
<td>Cram Quiz Answers</td>
<td>161</td>
</tr>
<tr>
<td>Virtual Network Components</td>
<td>162</td>
</tr>
<tr>
<td>Virtual Desktops</td>
<td>162</td>
</tr>
<tr>
<td>Virtual Servers</td>
<td>163</td>
</tr>
</tbody>
</table>
Virtual Switches ........................................ 163
Virtual PBX ........................................... 164
Onsite Versus Offsite .................................. 164
Network as a Service (NaaS) ......................... 165
Cram Quiz Answers .................................. 166
What Next? ............................................. 166

CHAPTER 5: Installation and Configuration ................. 167
Creating a SOHO Network ............................. 168
Cram Quiz Answers .................................. 174
WAN Technologies ..................................... 175
Switching Methods .................................... 175
Integrated Services Digital Network (ISDN) ......... 178
T-carrier Lines ........................................ 180
SONET/OCx Levels .................................... 182
X.25 and Frame Relay .................................. 183
Asynchronous Transfer Mode (ATM) ................. 186
Summary of WAN Technologies ..................... 187
Cram Quiz Answers .................................. 189
Internet Access Technologies ....................... 191
DSL Internet Access .................................. 192
Cable Internet Access ................................ 195
Broadband Security Considerations ................. 197
POTS Internet Access ................................ 198
The Public Switched Telephone Network (PSTN) .... 200
Satellite Internet Access .............................. 201
Wireless Internet Access .............................. 202
Cellular .............................................. 204
Cram Quiz Answers .................................. 206
What Next? ............................................. 207

CHAPTER 6: Cabling and Wiring ............................ 209
General Media Considerations ....................... 210
Broadband Versus Baseband Transmissions ......... 211
Simplex, Half Duplex, and Full Duplex Modes ....... 212
Media Interference .................................... 212
Attenuation ........................................... 213
Data Transmission Rates ............................. 213
CHAPTER 8:
**Network Management** .................................... 303

Documentation Management .................................. 305
  Wiring Schematics ............................................ 307
  Physical and Logical Network Diagrams ................. 310
  Baselines ..................................................... 313
  Policies, Procedures, Configurations, and Regulations 314
  Cram Quiz Answers .......................................... 321

Monitoring Network Performance .......................... 322
  Common Reasons to Monitor Networks .................... 323
  Packet Sniffers ............................................. 324
  Throughput Testing .......................................... 325
  Port Scanners ............................................... 327
  Network Performance, Load, and Stress Testing ....... 329
  Tracking Event Logs ........................................ 331
  Cram Quiz Answers .......................................... 337

Networking Tools ............................................. 338
  Wire Crimpers, Strippers, and Snips .................... 339
  Voltage Event Recorder .................................... 340
  Environmental Monitors ................................... 341
  Toner Probes ................................................ 342
  Protocol Analyzer .......................................... 343
  Media/Cable Testers ........................................ 344
  TDR and OTDR ................................................ 344
  Multimeter .................................................... 345
  Network Qualification Tester .............................. 346
  Butt Set ....................................................... 346
  Wireless Detection .......................................... 347
  Cram Quiz Answers .......................................... 349

Working with Command-Line Utilities .................... 350
  The Trace Route Utility (tracert/traceroute) ............ 352
  ping .......................................................... 355
  ARP ............................................................ 360
  The netstat Command ....................................... 363
  nbtstat ....................................................... 369
The ipconfig Command .................................................. 370
ifconfig ............................................................... 372
nslookup ........................................................... 373
dig ................................................................. 375
The host Command ................................................. 376
The route Utility ..................................................... 376
Cram Quiz Answers .................................................. 379

What Next? ................................................................. 380

CHAPTER 9: Network Optimization ........................................ 381

Uptime and Fault Tolerance ............................................ 382
Types of Fault Tolerance .............................................. 384
Link Redundancy ....................................................... 392
Common Address Redundancy Protocol (CARP) .......... 393
Using Uninterruptible Power Supplies (UPSs) ............ 393
Cram Quiz Answers .................................................. 396

Disaster Recovery ....................................................... 397
Full Backups .......................................................... 398
Differential Backups .................................................. 398
Incremental Backups .................................................. 399
Tape Rotations ........................................................ 400
Backup Best Practices ............................................... 401
Hot and Cold Spares ............................................... 401
Hot, Warm, and Cold Sites ........................................ 403
Cram Quiz Answers .................................................. 406

Network Optimization Strategies ..................................... 407
Quality of Service (QoS) .............................................. 407
Traffic Shaping ........................................................ 408
Caching Engines ....................................................... 409
Cram Quiz Answers .................................................. 411

What Next? ................................................................. 412

CHAPTER 10: Network Security ............................................. 413

Tunneling, Encryption, and Access Control ..................... 414
Internet Security Association and Key Management Protocol (ISAKMP) ........................................ 415
Point-to-Point Tunneling Protocol (PPTP) ....................... 415
Layer 2 Tunneling Protocol (L2TP) .............................. 416
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec</td>
<td>417</td>
</tr>
<tr>
<td>Site-to-Site and Client-to-Site</td>
<td>418</td>
</tr>
<tr>
<td>Overview of Access Control</td>
<td>418</td>
</tr>
<tr>
<td>Remote-Access Protocols and Services</td>
<td>421</td>
</tr>
<tr>
<td>Remote-Control Protocols</td>
<td>424</td>
</tr>
<tr>
<td>MAC Filtering</td>
<td>425</td>
</tr>
<tr>
<td>TCP/IP Filtering</td>
<td>426</td>
</tr>
<tr>
<td>Cram Quiz Answers</td>
<td>427</td>
</tr>
<tr>
<td>Authentication, Authorization, and Accounting (AAA)</td>
<td>429</td>
</tr>
<tr>
<td>Passwords and Password Policies</td>
<td>431</td>
</tr>
<tr>
<td>Kerberos Authentication</td>
<td>433</td>
</tr>
<tr>
<td>Public Key Infrastructure</td>
<td>436</td>
</tr>
<tr>
<td>RADIUS and TACACS+</td>
<td>439</td>
</tr>
<tr>
<td>Remote Authentication Protocols</td>
<td>440</td>
</tr>
<tr>
<td>Secured Versus Unsecured Protocols</td>
<td>442</td>
</tr>
<tr>
<td>Adding Physical Security to the Mix</td>
<td>443</td>
</tr>
<tr>
<td>Two-factor and Multifactor Authentication</td>
<td>445</td>
</tr>
<tr>
<td>Cram Quiz Answers</td>
<td>448</td>
</tr>
<tr>
<td>Managing Common Security Threats</td>
<td>449</td>
</tr>
<tr>
<td>Viruses</td>
<td>450</td>
</tr>
<tr>
<td>Worms and Trojan Horses</td>
<td>451</td>
</tr>
<tr>
<td>Denial of Service and Distributed Denial of Service Attacks</td>
<td>452</td>
</tr>
<tr>
<td>Other Common Attacks</td>
<td>454</td>
</tr>
<tr>
<td>An Ounce of Prevention</td>
<td>456</td>
</tr>
<tr>
<td>Cram Quiz Answers</td>
<td>459</td>
</tr>
<tr>
<td>Firewalls and Other Appliances</td>
<td>460</td>
</tr>
<tr>
<td>Stateful and Stateless Firewalls</td>
<td>462</td>
</tr>
<tr>
<td>Packet-Filtering Firewalls</td>
<td>463</td>
</tr>
<tr>
<td>Circuit-Level Firewalls</td>
<td>465</td>
</tr>
<tr>
<td>Application Layer Firewalls</td>
<td>465</td>
</tr>
<tr>
<td>Comparing Firewall Types</td>
<td>465</td>
</tr>
<tr>
<td>Firewall Wrap-Up</td>
<td>466</td>
</tr>
<tr>
<td>Demilitarized Zones (Perimeter Network)</td>
<td>466</td>
</tr>
<tr>
<td>Other Security Devices</td>
<td>467</td>
</tr>
<tr>
<td>Cram Quiz Answers</td>
<td>473</td>
</tr>
<tr>
<td>What Next?</td>
<td>474</td>
</tr>
</tbody>
</table>
CHAPTER 11:
Network Troubleshooting ........................................ 475
    Troubleshooting Steps and Procedures .................... 476
        Identify the Problem ................................ 477
        Establish a Theory of Probable Cause ............... 478
        Test the Theory to Determine Cause ................. 479
        Establish a Plan of Action ............................ 479
        Implement the Solution or Escalate ................ 480
        Verify Full System Functionality ................... 481
        Document the Findings, Actions, and Outcomes .... 482
    Cram Quiz Answers ....................................... 484
    Troubleshooting the Network ................................ 485
        Common Problems to Be Aware Of .................... 485
        Troubleshooting Wiring ................................ 490
        Wiring Issues ......................................... 492
        Troubleshooting Infrastructure Hardware ............. 496
        Configuring and Troubleshooting Client Connectivity ........................................ 498
        Troubleshooting an Incorrect VLAN .................. 503
        Topology Errors ...................................... 504
        Cram Quiz Answers .................................... 510
    What Next? ............................................... 511

Practice Exam 1 ............................................. 513
    Exam Questions .......................................... 513

Answers to Practice Exam 1 .................................. 537
    Answers at a Glance ..................................... 537
    Answers and Explanations ................................ 538

Practice Exam 2 ............................................. 561
    Exam Questions .......................................... 561

Answers to Practice Exam 2 .................................. 585
    Answers at a Glance ..................................... 585
    Answers and Explanations ................................ 586

Glossary .................................................. 607

Index ...................................................... 649
About the Authors

Emmett Dulaney (Network+, A+, Security+, ManyOthers+) is the author of numerous books on certifications and operating systems. He is a columnist for CertCities and an associate professor at Anderson University. In addition to the Network+ Exam Cram, he is the author of the CompTIA A+ Complete Study Guide and the CompTIA Security+ Study Guide.

Mike Harwood (MCSE, A+, Network+, Server+, Linux+) has more than 14 years experience in information technology and related fields. He has held a number of roles in the IT field including network administrator, instructor, technical writer, website designer, consultant, and online marketing strategist. Mike has been a regular on air technology contributor for CBC radio and has coauthored numerous computer books, including the Network+ Exam Cram published by Pearson.

About the Technical Editor

Dedication

For Karen, Kristin, Evan, and Spencer: the backbone of my network.
—Emmett Dulaney

Acknowledgments

I would like to thank Mike Harwood for creating a great book of which I was honored to join with this edition. Thanks are due to a wonderful team of talented individuals, three of whom deserve special attention: Betsy Brown, Jeff Riley, and Christopher A. Crayton. They represent the best in the business.

—Emmett Dulaney
We Want to Hear from You!

As the reader of this book, you are our most important critic and commentator. We value your opinion and want to know what we’re doing right, what we could do better, what areas you’d like to see us publish in, and any other words of wisdom you’re willing to pass our way.

As an associate publisher for Pearson, I welcome your comments. You can email or write me directly to let me know what you did or didn’t like about this book—as well as what we can do to make our books better.

Please note that I cannot help you with technical problems related to the topic of this book. We do have a User Services group, however, where I will forward specific technical questions related to the book.

When you write, please be sure to include this book’s title and author as well as your name, email address, and phone number. I will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: David Dusthimer
Associate Publisher
Pearson
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at www.pearsonitcertification.com/register for convenient access to any updates, downloads, or errata that might be available for this book.
CompTIA Security+

- Designed for IT professionals focused on system security.
- Covers network infrastructure, cryptography, assessments, and audits.
- Security+ is mandated by the U.S. Department of Defense and is recommended by top companies such as Microsoft, HP, and Cisco.

It Pays to Get Certified

In a digital world, digital literacy is an essential survival skill. Certification proves you have the knowledge and skill to solve business problems in virtually any business environment. Certifications are highly valued credentials that qualify you for jobs, increased compensation, and promotion.

Security is one of the highest demand job categories. Growing in importance as the frequency and severity of security threats continues to be a major concern for organizations around the world.

- Jobs for security administrators are expected to increase by 18% - the skill set required for these types of jobs map to CompTIA Security+ certification.
- Network Security Administrators - can earn as much as $106,000 per year.
- CompTIA Security+ is the first step - in starting your career as a Network Security Administrator or Systems Security Administrator.
- CompTIA Security+ is regularly used in organizations - such as Hitachi Information Systems, Trendmicro, the McAfee Elite Partner program, the U.S. State Department, and U.S. government contractors such as EDS, General Dynamics, and Northrop Grumman.

How Certification Helps Your Career

- IT is Everywhere
  - IT is ubiquitous, needed by most organizations. Globally, there are over 600,000 IT job openings.
- IT Knowledge and Skills Gets Jobs
  - Certifications are essential credentials that qualify you for jobs, increased compensation, and promotion.
- Retain your Job and Salary
  - Make your expertise stand above the rest. Competence is usually retained during times of change.
- Want to Change Jobs
  - Certifications qualify you for new opportunities, whether locked into a current job, see limited advancement, or need to change careers.
- Stick Out from the Resume Pile
  - Hiring managers can demand the strongest skill set.
CompTIA Career Pathway

CompTIA offers a number of credentials that form a foundation for your career in technology and allow you to pursue specific areas of concentration. Depending on the path you choose to take, CompTIA certifications help you build upon your skills and knowledge, supporting learning throughout your entire career.

Steps to Getting Certified and Staying Certified

<table>
<thead>
<tr>
<th>Steps to Getting Certified and Staying Certified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review Exam Objectives</td>
</tr>
<tr>
<td>Practice for the Exam</td>
</tr>
<tr>
<td>Purchase an Exam Voucher</td>
</tr>
<tr>
<td>Take the Test!</td>
</tr>
<tr>
<td>Stay Certified!</td>
</tr>
</tbody>
</table>
Join the Professional Community

Join IT Pro Community
http://itpro.comptia.org

The free IT Pro online community provides valuable content to students and professionals.

• Career IT Job Resources
  ▪ Where to start in IT
  ▪ Career Assessments
  ▪ Salary Trends
  ▪ US Job Board
• Forums on Networking, Security, Computing and Cutting Edge Technologies
• Access to blogs written by Industry Experts
• Current information on Cutting Edge Technologies
• Access to various industry resource links and articles related to IT and IT careers

Content Seal of Quality

This courseware bears the seal of CompTIA Approved Quality Content. This seal signifies this content covers 100% of the exam objectives and implements important instructional design principles. CompTIA recommends multiple learning tools to help increase coverage of the learning objectives.

Why CompTIA?

• Global Recognition – CompTIA is recognized globally as the leading IT non-profit trade association and has enormous credibility. Plus, CompTIA’s certifications are vendor-neutral and offer proof of foundational knowledge that translates across technologies.
• Valued by Hiring Managers - Hiring managers value CompTIA certification because it is vendor and technology independent validation of your technical skills.
• Recommended or Required by Government and Businesses - Many government organizations and corporations either recommend or require technical staff to be CompTIA certified. (e.g. Dell, Sharp, Ricoh, the U.S. Department of Defense and many more)

• Three CompTIA Certifications ranked in the top 10. In a study by DICE of 17,000 technology professionals, certifications helped command higher salaries at all experience levels.

How to obtain more information

• Visit CompTIA online - www.comptia.org to learn more about getting CompTIA certified.
• Contact CompTIA - call 866-835-8020 ext. 5 or email questions@comptia.org
• Join the IT Pro Community – http://itpro.comptia.org to join the IT community to get relevant career information.
• Connect with us : 🌀 🌀 🌀 🌀 🌀
This page intentionally left blank
Introduction

Welcome to the *Network+ Exam Cram*. This book is designed to prepare you to take—and pass—the CompTIA Network+ exam. The Network+ exam has become the leading introductory-level network certification available today. It is recognized by both employers and industry giants as providing candidates with a solid foundation of networking concepts, terminology, and skills. The Network+ exam covers a broad range of networking concepts to prepare candidates for the technologies they are likely to work with in today’s network environments.

About Network+ Exam Cram

*Exam Cram*s are designed to give you the information you need to know to prepare for a certification exam. They cut through the extra information, focusing on the areas you need to get through the exam. With this in mind, the elements within the *Exam Cram* titles are aimed at providing the exam information you need in the most succinct and accessible manner.

In this light, this book is organized to closely follow the actual CompTIA objectives for exam N10-005. As such, it is easy to find the information required for each of the specified CompTIA Network+ objectives. The objective focus design used by this *Exam Cram* is an important feature because the information you need to know is easily identifiable and accessible. To see what we mean, compare the CompTIA objectives to the book’s layout, and you can see that the facts are right where you would expect them to be.

Within the chapters, potential exam hot spots are clearly highlighted with Exam Alerts. They have been carefully placed to let you know that the surrounding discussion is an important area for the exam. To further help you prepare for the exam, a Cram Sheet is included that you can use in the final stages of test preparation. Be sure to pay close attention to the bulleted points on the Cram Sheet because they pinpoint the technologies and facts you probably will encounter on the test.

Finally, great effort has gone into the questions that appear throughout the chapter and the practice tests to ensure that they accurately represent the look and feel of the ones you will see on the real Network+ exam. Be sure, before taking the exam, that you are comfortable with both the format and content of the questions provided in this book.
About the Network+ Exam

The Network+ (N10-005 Edition) exam is a revised version of the original exam. The new Network+ objectives are aimed toward those who have at least 9 months of experience in network support and administration. CompTIA believes that new Network+ candidates require more hands-on experience in network administration and troubleshooting, but this should not discourage those who do not. Quite simply, the nature of the questions on the new exam is not dissimilar to the old, and you can get by without actual hands-on experience. Still, a little hands-on experience never hurt anyone and can certainly add to your confidence going into the exam.

You will have a maximum of 90 minutes to answer the 100 questions on the exam. The allotted time is quite generous, so when you finish, you probably will have time to double-check a few of the answers you were unsure of. By the time the dust settles, you need a minimum score of 720 to pass the Network+ exam. This is on a scale of 100 to 900. For more information on the specifics of the Network+ exam, refer to CompTIA’s main website at http://certification.comptia.org/.

CompTIA Network+ Exam Topics

Table I-1 lists general exam topics (that is, objectives) and specific topics under each general topic (that is, subobjectives) for the CompTIA Network+ N10-005 exam. This table also lists the chapter in which each exam topic is covered. Some objectives and subobjectives are addressed in multiple chapters.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>N10-005 Exam Objective</th>
<th>N10-005 Exam Subobjective</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (Introduction to Networking)</td>
<td>3.0 Network Media and Topologies</td>
<td>3.5 Describe different network topologies.</td>
</tr>
<tr>
<td>2 (OSI and TCP/IP Models and Network Protocols)</td>
<td>1.0 Network Concepts 2.0 Network Installation and Configuration 4.0 Network Management</td>
<td>1.1 Compare the layers of the OSI and TCP/IP models. 1.6 Explain the function of common network protocols. 1.7 Summarize DNS concepts and its components. 2.3 Explain the purpose and properties of DHCP 4.4 Given a scenario, use the appropriate network resource to analyze traffic.</td>
</tr>
<tr>
<td>Chapter</td>
<td>N10-005 Exam Objective</td>
<td>N10-005 Exam Subobjective</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>3 (Addressing and Routing)</td>
<td>1.0 Network Concepts and Configuration</td>
<td>1.3 Explain the purpose and properties of IP addressing.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.4 Explain the purpose and properties of routing and switching.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.5 Identify common TCP and UDP default ports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.1 Given a scenario, install and configure routers and switches.</td>
</tr>
<tr>
<td>4 (Components and Devices)</td>
<td>1.0 Network Technologies and Configuration</td>
<td>1.2 Classify how applications, devices, and protocols relate to the OSI model layers.</td>
</tr>
<tr>
<td></td>
<td>4.0 Network Management</td>
<td>1.9 Identify virtual network components.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.1 Explain the purpose and features of various network appliances.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.7 Compare and contrast different LAN technologies.</td>
</tr>
<tr>
<td>5 (Installation and</td>
<td>2.0 Network Installation and Configuration</td>
<td>2.6 Given a set of requirements, plan and implement a basic SOHO network.</td>
</tr>
<tr>
<td>Configuration)</td>
<td>3.0 Network Media and Topologies</td>
<td>3.4 Categorize WAN technology types and properties.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 (Cabling and Wiring)</td>
<td>3.0 Network Media and Topologies</td>
<td>3.1 Categorize standard media types and associated properties.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.2 Categorize standard connector types based on network media.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.7 Compare and contrast different LAN technologies.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.8 Identify components of wiring distribution.</td>
</tr>
<tr>
<td>7 (Wireless)</td>
<td>2.0 Network Installation and Configuration</td>
<td>2.2 Given a scenario, install and configure a wireless network.</td>
</tr>
<tr>
<td></td>
<td>3.0 Network Media and Topologies</td>
<td>2.4 Given a scenario, troubleshoot common wireless problems.</td>
</tr>
<tr>
<td></td>
<td>5.0 Network Security</td>
<td>3.3 Compare and contrast different wireless standards.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.1 Given a scenario, implement appropriate wireless security measures.</td>
</tr>
<tr>
<td>8 (Network Management)</td>
<td>4.0 Network Management</td>
<td>4.2 Given a scenario, use appropriate hardware tools to troubleshoot connectivity issues.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.3 Given a scenario, use appropriate software tools to troubleshoot connectivity issues.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.4 Given a scenario, use the appropriate network monitoring resource to analyze traffic.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.5 Describe the purpose of configuration management documentation.</td>
</tr>
</tbody>
</table>
TABLE I-1  Continued

<table>
<thead>
<tr>
<th>Chapter</th>
<th>N10-005 Exam Objective</th>
<th>N10-005 Exam Subobjective</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 (Network Optimization)</td>
<td>4.0 Network Management</td>
<td>4.6 Explain different methods and rationales for network performance optimization.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 (Network Security)</td>
<td>5.0 Network Security</td>
<td>5.2 Explain the methods of network access security.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.3 Explain methods of user authentication.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.4 Explain common threats, vulnerabilities, and mitigation techniques.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.5 Given a scenario, install and configure a basic firewall.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.6 Categorize different types of network security appliances and methods.</td>
</tr>
<tr>
<td>11 (Network Troubleshooting)</td>
<td>1.0 Network Technologies 2.0 Network Installation and Configuration</td>
<td>1.8 Given a scenario, implement a given troubleshooting methodology.</td>
</tr>
<tr>
<td></td>
<td>3.0 Network Media and Topologies</td>
<td>2.5 Given a scenario, troubleshoot common router and switch problems.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.6 Given a scenario, troubleshoot common physical connectivity problems.</td>
</tr>
</tbody>
</table>

**Booking and Taking the Network+ Certification Exam**

Unfortunately, testing is not free. You’re charged $246 for each test you take, whether you pass or fail. In the United States and Canada, tests are administered by Sylvan Prometric or VUE testing services. To book a test with Prometric or to locate a Prometric testing center near you, refer to the website at http://securereg3.prometric.com/ or call 1-888-895-6116. To access the VUE contact information and book an exam, refer to the website at http://www.vue.com or call 1-877-551-7587. When booking an exam, you need to provide the following information:

- Your name as you would like it to appear on your certificate.
- Your Social Security or Social Insurance number.
- Contact phone numbers (to be called in case of a problem).
- Mailing address, which identifies the address to which you want your certificate mailed.
- Exam number and title.
Email address for contact purposes. This often is the fastest and most effective means to contact you. Many clients require it for registration.

- Credit-card information so that you can pay online. You can redeem vouchers by calling the respective testing center.

What to Expect from the Exam

If you haven’t taken a certification test, the process can be a little unnerving. Even if you’ve taken numerous tests, it is not much better. Mastering the inner mental game often can be as much of a battle as knowing the material. Knowing what to expect before heading in can make the process a little more comfortable.

Certification tests are administered on a computer system at a Prometric or VUE authorized testing center. The format of the exams is straightforward: Each question has several possible answers to choose from. The questions in this book provide a good example of the types of questions you can expect on the exam. If you are comfortable with them, the test should hold few surprises. Many of the questions vary in length; some of them are longer scenario questions, whereas others are short and to the point. Carefully read the questions; the longer questions often have a key point that will lead you to the correct answer.

Most of the questions on the Network+ exam require you to choose a single correct answer, but a few require multiple answers. When there are multiple correct answers, a message at the bottom of the screen prompts you to “Choose all that apply.” Be sure to read these messages.

A Few Exam Day Details

It is recommended that you arrive at the examination room at least 15 minutes early, although a few minutes earlier certainly would not hurt. This will give you time to prepare and will give the test administrator time to answer any questions you might have before the test begins. Many people suggest that you review the most critical information about the test you’re taking just before the test. (Exam Cram books provide a reference—the Cram Sheet, located inside the front of this book—that lists the essential information from the book in distilled form.) Arriving a few minutes early will give you some time to compose yourself and mentally review this critical information.
You will be asked to provide two forms of ID, one of which must be a photo ID. Both of the identifications you choose should have a signature. You also might need to sign in when you arrive and sign out when you leave.

Be warned: The rules are clear about what you can and cannot take into the examination room. Books, laptops, note sheets, and so on are not allowed in the examination room. The test administrator will hold these items, to be returned after you complete the exam. You might receive either a wipe board or a pen and a single piece of paper for making notes during the exam. The test administrator will ensure that no paper is removed from the examination room.

After the Test

Whether you want it or not, as soon as you finish your test, your score displays on the computer screen. In addition to the results appearing on the computer screen, a hard copy of the report prints for you. Like the onscreen report, the hard copy displays the results of your exam and provides a summary of how you did on each section and on each technology. If you were unsuccessful, this summary can help you determine the areas you need to brush up on.

When you pass the Network+ exam, you will have earned the Network+ certification, and your certificate will be mailed to you within a few weeks. Should you not receive your certificate and information packet within 5 weeks of passing your exam, contact CompTIA at fulfillment@comptia.org, or call 1-630-268-1818 and ask for the fulfillment department.

Last-Minute Exam Tips

Studying for a certification exam is no different than studying for any other exam, but a few hints and tips can give you the edge on exam day:

- **Read all the material:** CompTIA has been known to include material not expressly specified in the objectives. This book has included additional information not reflected in the objectives to give you the best possible preparation for the examination.

- **Watch for the Exam Tips and Notes:** The Network+ objectives include a wide range of technologies. Exam Tips and Notes found throughout each chapter are designed to pull out exam-related hot spots. These can be your best friends when preparing for the exam.
Use the questions to assess your knowledge: Don’t just read the chapter content; use the exam questions to find out what you know and what you don’t. If you struggle, study some more, review, and then assess your knowledge again.

Review the exam objectives: Develop your own questions and examples for each topic listed. If you can develop and answer several questions for each topic, you should not find it difficult to pass the exam.

Good luck!
This page intentionally left blank
Without question, the TCP/IP suite is the most widely implemented protocol on networks today. As such, it is an important topic on the Network+ exam. To pass the exam, you definitely need to understand the material presented in this chapter.

This chapter deals with the individual protocols within the protocol suite. It looks at the functions of the individual protocols and their purposes. It starts by discussing one of the more complex facets of TCP/IP: addressing.
### IP Addressing

- Explain the purpose and properties of IP addressing.

#### Cram Saver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then complete the Cram Quiz at the end of the section.

1. How many octets does a Class A address use to represent the network portion?
2. What is the range that Class C addresses span in the first octet?
3. What are the reserved IPv4 ranges for private networks?

#### Answers

1. A Class A address uses only the first octet to represent the network portion, a Class B address uses two octets, and a Class C address uses three octets.
2. Class C addresses span from 192 to 223, with a default subnet mask of 255.255.255.0.
3. A private network is any network to which access is restricted. Reserved IP addresses are 10.0.0.0, 172.16.0.0 to 172.31.0.0, and 192.168.0.0.

IP addressing is one of the most challenging aspects of TCP/IP. It can leave even the most seasoned network administrators scratching their heads. Fortunately, the Network+ exam requires only a fundamental knowledge of IP addressing. The following sections look at how IP addressing works for both IPv4 and the newest version of IP: IPv6.

To communicate on a network using TCP/IP, each system must be assigned a unique address. The address defines both the number of the network to which the device is attached and the number of the node on that network. In other words, the IP address provides two pieces of information. It’s a bit like a street name and house number in a person’s home address.

Each device on a logical network segment must have the same network address as all the other devices on the segment. All the devices on that network segment must then have different node addresses.
In IP addressing, another set of numbers, called a subnet mask, defines which portion of the IP address refers to the network address and which refers to the node address.

IP addressing is different in IPv4 and IPv6. The discussion begins by looking at IPv4.

**IPv4**

An IPv4 address is composed of four sets of 8 binary bits, which are called *octets*. The result is that IP addresses contain 32 bits. Each bit in each octet is assigned a decimal value. The leftmost bit has a value of 128, followed by 64, 32, 16, 8, 4, 2, and 1, left to right.

Each bit in the octet can be either a 1 or a 0. If the value is 1, it is counted as its decimal value, and if it is 0, it is ignored. If all the bits are 0, the value of the octet is 0. If all the bits in the octet are 1, the value is 255, which is 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1.

By using the set of 8 bits and manipulating the 1s and 0s, you can obtain any value between 0 and 255 for each octet.

Table 3.1 shows some examples of decimal-to-binary value conversions.

<table>
<thead>
<tr>
<th>Decimal Value</th>
<th>Binary Value</th>
<th>Decimal Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>00001010</td>
<td>8 + 2 = 10</td>
</tr>
<tr>
<td>192</td>
<td>11000000</td>
<td>128 + 64 = 192</td>
</tr>
<tr>
<td>205</td>
<td>11001101</td>
<td>128 + 64 + 8 + 4 + 1 = 205</td>
</tr>
<tr>
<td>223</td>
<td>11011111</td>
<td>128 + 64 + 16 + 8 + 4 + 2 + 1 = 223</td>
</tr>
</tbody>
</table>

**IP Address Classes**

IP addresses are grouped into logical divisions called *classes*. The IPv4 address space has five address classes (A through E); although, only three (A, B, and C) assign addresses to clients. Class D is reserved for multicast addressing, and Class E is reserved for future development.

Of the three classes available for address assignments, each uses a fixed-length subnet mask to define the separation between the network and the node address. A Class A address uses only the first octet to represent the network portion; a Class B address uses two octets; and a Class C address uses the first
three octets. The upshot of this system is that Class A has a small number of network addresses, but each Class A address has a large number of possible host addresses. Class B has a larger number of networks, but each Class B address has a smaller number of hosts. Class C has an even larger number of networks, but each Class C address has an even smaller number of hosts. The exact numbers are provided in Table 3.2.

**TABLE 3.2** IPv4 Address Classes and the Number of Available Network/Host Addresses

<table>
<thead>
<tr>
<th>Address Class</th>
<th>Range</th>
<th>Number of Networks</th>
<th>Number of Hosts Per Network</th>
<th>Binary Value of First Octet</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>1 to 126</td>
<td>126</td>
<td>16,777,214</td>
<td>0xxxxxxx</td>
</tr>
<tr>
<td>B</td>
<td>128 to 191</td>
<td>16,384</td>
<td>65,534</td>
<td>10xxxxxxx</td>
</tr>
<tr>
<td>C</td>
<td>192 to 223</td>
<td>2,097,152</td>
<td>254</td>
<td>110xxxxx</td>
</tr>
<tr>
<td>D</td>
<td>224 to 239</td>
<td>N/A</td>
<td>N/A</td>
<td>1110xxxx</td>
</tr>
<tr>
<td>E</td>
<td>240 to 255</td>
<td>N/A</td>
<td>N/A</td>
<td>1111xxxx</td>
</tr>
</tbody>
</table>

Notice in Table 3.2 that the network number 127 is not included in any of the ranges. The 127.0.0.1 network ID is reserved for the IPv4 local loopback. The local loopback is a function of the protocol suite used in the troubleshooting process.

Subnet Mask Assignment

Like an IP address, a subnet mask is most commonly expressed in 32-bit dotted-decimal format. Unlike an IP address, though, a subnet mask performs just one function—it defines which parts of the IP address refer to the network address and which refer to the node address. Each class of the IP address
used for address assignment has a default subnet mask associated with it. Table 3.3 lists the default subnet masks.

<table>
<thead>
<tr>
<th>Address Class</th>
<th>Default Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>255.0.0.0</td>
</tr>
<tr>
<td>B</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>C</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

You will likely see questions about address class and the corresponding default subnet mask. Review Table 3.3 before taking the exam.

Subnetting

Now that you have looked at how IP addresses are used, you can learn the process of subnetting. Subnetting is a process by which the node portions of an IP address create more networks than you would have if you used the default subnet mask.

To illustrate subnetting, for example, suppose that you have been assigned the Class B address 150.150.0.0. Using this address and the default subnet mask, you could have a single network (150.150) and use the rest of the address as node addresses. This would give you a large number of possible node addresses, which in reality is probably not useful. With subnetting, you use bits from the node portion of the address to create more network addresses. This reduces the number of nodes per network, but you probably will still have more than enough.

Following are two main reasons for subnetting:

- It enables you to more effectively use IP address ranges.
- It makes IP networking more secure and manageable by providing a mechanism to create multiple networks rather than having just one. Using multiple networks confines traffic to the network that it needs to be on, which reduces overall network traffic levels. Multiple subnets also create more broadcast domains, which in turn reduces networkwide broadcast traffic. A difference exists between broadcast domains and collision domains: The latter is all the connected nodes, whereas the former is all the logical nodes that can reach each other. As such, collision domains are typically subsets of broadcast domains.
Identifying the Differences Between IPv4 Public and Private Networks

IP addressing involves many considerations, not the least of which are public and private networks.

- A public network is a network to which anyone can connect. The best (and perhaps only pure) example of such a network is the Internet.

- A private network is any network to which access is restricted. A corporate network and a network in a school are examples of private networks.

ExamAlert

Subnetting does not increase the number of IP addresses available. It increases the number of network IDs and, as a result, decreases the number of node IDs per network. It also creates more broadcast domains. Broadcasts are not forwarded by routers, so they are limited to the network on which they originate.

Note

The Internet Assigned Numbers Authority (IANA) is responsible for assigning IP addresses to public networks. However, because of the workload involved in maintaining the systems and processes to do this, IANA has delegated the assignment process to a number of regional authorities. For more information, visit http://www.iana.org/ipaddress/ip-addresses.htm.

The main difference between public and private networks, other than access to a private network is tightly controlled and access to a public network is not, is that the addressing of devices on a public network must be carefully considered. Addressing on a private network has a little more latitude.

As already discussed, for hosts on a network to communicate by using TCP/IP, they must have unique addresses. This number defines the logical network that each host belongs to and the host's address on that network. On a private network with, say, three logical networks and 100 nodes on each network, addressing is not a difficult task. On a network on the scale of the Internet, however, addressing is complex.

If you connect a system to the Internet, you need to get a valid registered IP address. Most commonly, you obtain this address from your ISP. Alternatively, if you wanted a large number of addresses, for example, you could contact the
organization responsible for address assignment in your area. You can determine who the regional numbers authority for your area is by visiting the IANA website.

Because of the nature of their business, ISPs have large blocks of IP addresses that they can assign to their clients. If you need a registered IP address, getting one from an ISP is almost certainly a simpler process than going through a regional numbers authority. Some ISPs’ plans actually include blocks of registered IP addresses, working on the principle that businesses want some kind of permanent presence on the Internet. Of course, if you discontinue your service with the ISP, you can no longer use the provided IP address.

**Private Address Ranges**

To provide flexibility in addressing and to prevent an incorrectly configured network from polluting the Internet, certain address ranges are set aside for private use. These address ranges are called *private ranges* because they are designated for use only on private networks. These addresses are special because Internet routers are configured to ignore any packets they see that use these addresses. This means that if a private network “leaks” onto the Internet, it won’t get any farther than the first router it encounters. So a private address cannot be on the Internet because it cannot be routed to public networks.

Three ranges are defined in RFC 1918: one each from Classes A, B, and C. You can use whichever range you want; although, the Class A and B address ranges offer more addressing options than Class C. Table 3.4 defines the address ranges for Class A, B, and C addresses.

<table>
<thead>
<tr>
<th>Class</th>
<th>Address Range</th>
<th>Default Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>10.0.0.0 to 10.255.255</td>
<td>255.0.0.0</td>
</tr>
<tr>
<td>B</td>
<td>172.16.0.0 to 172.31.255</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>C</td>
<td>192.168.0.0 to 192.168.255.255</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

**ExamAlert**

You can expect questions on private IP address ranges and their corresponding default subnet masks.
Classless Interdomain Routing (CIDR)

Classless interdomain routing (CIDR) is a method to assign addresses outside the standard Class A, B, and C structure that is used by IPv6. Specifying the number of bits in the subnet mask offers more flexibility than the three standard class definitions.

Using CIDR, addresses are assigned using a value known as the *slash*. The actual value of the slash depends on how many bits of the subnet mask are used to express the network portion of the address. For example, a subnet mask that uses all 8 bits from the first octet and 4 from the second would be described as /12, or “slash 12.” A subnet mask that uses all the bits from the first three octets would be called /24. Why the slash? In actual addressing terms, the CIDR value is expressed after the address, using a slash. So the address 192.168.2.1/24 means that the node’s IP address is 192.168.2.1, and the subnet mask is 255.255.255.0.

You can find a great CIDR calculator that can compute values from ranges at http://www.subnet-calculator.com/cidr/php.

ExamAlert
You will likely see IP addresses in their CIDR format on the exam. Be sure that you understand CIDR addressing for the exam.

Default Gateways

Default gateways are the means by which a device can access hosts on other networks for which it does not have a specifically configured route. Most workstation configurations actually default to just using default gateways rather than having any static routes configured. This enables workstations to communicate with other network segments, or with other networks, such as the Internet.

ExamAlert
You will be expected to identify the purpose and function of a default gateway.
When a system wants to communicate with another device, it first determines whether the host is on the local network or a remote network. If the host is on a remote network, the system looks in the routing table to determine whether it has an entry for the network on which the remote host resides. If it does, it uses that route. If it does not, the data is sent to the default gateway.

**Note**
Although it might seem obvious, it’s worth mentioning that the default gateway must be on the same network as the nodes that use it.

In essence, the default gateway is simply the path out of the network for a given device. Figure 3.1 shows how a default gateway fits into a network infrastructure.

On the network, a default gateway could be a router or a computer with network interfaces for all segments to which it is connected. These interfaces have local IP addresses for the respective segments. If a system is not configured with any static routes or a default gateway, it is limited to operating on its own network segment.
IPv4 Address Types

IPv4 has three primary address types: unicast, broadcast, and multicast. You need to distinguish between these three types of IPv4 addresses.

Unicast Address

With a unicast address, a single address is specified. Data sent with unicast addressing is delivered to a specific node identified by the address. It is a point-to-point address link.

Broadcast Address

A broadcast address is at the opposite end of the spectrum from a unicast address. A broadcast address is an IP address that you can use to target all systems on a subnet or network instead of single hosts. In other words, a broadcast message goes to everyone on the network.

Multicast

Multicasting is a mechanism by which groups of network devices can send and receive data between the members of the group at one time, instead of separately sending messages to each device in the group. The multicast grouping is established by configuring each device with the same multicast IP address.

IPv6 Addressing

Internet Protocol Version 4 (IPv4) has served as the Internet’s protocol for almost 30 years. When IPv4 was in development 30 years ago, it would have been impossible for its creators to imagine or predict the future demand for IP devices and therefore IP addresses.

Note

Does the IETF assign protocol numbers using multiples of 2? Well, no. There was an IPv5. It was an experimental protocol that never went anywhere. But although IPv5 may have fallen into obscurity, because the name had been used, we got IPv6.
Where have all the IPv4 addresses gone?

IPv4 uses a 32-bit addressing scheme. This gives IPv4 a total of 4,294,967,296 possible unique addresses that can be assigned to IP devices. More than 4 billion addresses might sound like a lot, and it is. However, the number of IP-enabled devices increases daily at a staggering rate. Not all these addresses can be used by public networks. Many of these addresses are reserved and are unavailable for public use. This reduces the number of addresses that can be allocated as public Internet addresses.

The IPv6 project started in the mid-1990s, well before the threat of IPv4 limitations. Now network hardware and software are equipped for and ready to deploy IPv6 addressing. IPv6 offers a number of improvements. The most notable is its capability to handle growth in public networks. IPv6 uses a 128-bit addressing scheme, enabling a huge number of possible addresses:

340,282,366,920,938,463,463,374,607,431,768,211,456

**Identifying IPv6 Addresses**

As previously discussed, IPv4 uses a dotted-decimal format: 8 bits converted to its decimal equivalent and separated by periods. An example of an IPv4 address is 192.168.2.1.

Because of the 128-bit structure of the IPv6 addressing scheme, it looks quite a bit different. An IPv6 address is divided along 16-bit boundaries, and each 16-bit block is converted into a four-digit hexadecimal number and separated by colons. The resulting representation is called colon-hexadecimal. Now look at how it works. Figure 3.2 shows the IPv6 address 2001:0:4137:9e50:2811:34ff:3f57:febc from a Windows 7 system.

![IPv6 Address in Windows 7](image)
An IPv6 address can be simplified by removing the leading 0s within each 16-bit block. Not all the 0s can be removed, however, because each address block must have at least a single digit. Removing the 0 suppression, the address representation becomes

2001:0000:4137:9e50:2811:34ff:3f57:febc

Some of the IPv6 addresses you will work with have sequences of 0s. When this occurs, the number is often abbreviated to make it easier to read. In the preceding example you saw that a single 0 represented a number set in hexadecimal form. To further simplify the representation of IPv6 addresses, a contiguous sequence of 16-bit blocks set to 0 in colon hexadecimal format can be compressed to ::, known as the double colon.

For example, the IPv6 address of

2001:0000:0000:0000:3cde:37d1:3f57:fe93

can be compressed to

2001::3cde:37d1:3f57:fe93.

Of course, there are limits on how the IPv6 0s can be reduced. 0s within the IPv6 address cannot be eliminated when they are not first in the number sequence. For instance, 2001:4000:0000:0000:0000:0000:0000:0003 cannot be compressed as 2001:4::3. This would actually appear as 2001:4000::3.

When you look at an IPv6 address that uses a double colon, how do you know exactly what numbers are represented? The formula is to subtract the number of blocks from 8 and then multiply that number by 16. For example, the address 2001:4000::3 uses three blocks: 2001, 4000, and 3. So the formula is as follows:

\((8 - 3) \cdot 16 = 80\)

Therefore, the total number of bits represented by the double colon in this example is 80.

**Note**

You can remove 0s only once in an IPv6 address. Using a double colon more than once would make it impossible to determine the number of 0 bits represented by each instance of ::.
IPv6 Address Types

Another difference between IPv4 and IPv6 is in the address types. IPv4 addressing was discussed in detail earlier. IPv6 addressing offers several types of addresses, as detailed in this section.

Unicast IPv6 Addresses

As you might deduce from the name, a unicast address specifies a single interface. Data packets sent to a unicast destination travel from the sending host to the destination host. It is a direct line of communication. A few types of addresses fall under the unicast banner:

Global Unicast Addresses

Global unicast addresses are the equivalent of IPv4 public addresses. These addresses are routable and travel throughout the network.

Link-Local Addresses

Link-local addresses are designated for use on a single local network. Link-local addresses are automatically configured on all interfaces. This automatic configuration is comparable to the 169.254.0.0/16 APIPA automatically assigned IPv4 addressing scheme. The prefix used for a link-local address is fe80::/64. On a single-link IPv6 network with no router, link-local addresses are used to communicate between devices on the link.

Site-Local Addresses

Site-local addresses are equivalent to the IPv4 private address space (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16). As with IPv4, in which private address ranges are used in private networks, IPv6 uses site-local addresses that do not interfere with global unicast addresses. In addition, routers do not forward site-local traffic outside the site. Unlike link-local addresses, site-local addresses are not automatically configured and must be assigned through either stateless or stateful address configuration processes. The prefix used for the site-local address is FEC0::/10.

Multicast Addresses

As with IPv4 addresses, multicasting sends and receives data between groups of nodes. It sends IP messages to that group rather than to every node on the LAN (broadcast) or just one other node (unicast).
Anycast Addresses

Anycast addresses represent the middle ground between unicast addresses and multicast addresses. Anycast delivers messages to any one node in the multicast group.

Note

You might encounter the terms stateful and stateless configuration. Stateless refers to IP autoconfiguration, in which administrators need not manually input configuration information. In a stateful configuration network, devices obtain address information from a server.

ExamAlert

Earlier you read that IPv4 reserves 127.0.0.1 as the loopback address. IPv6 has the same reservation. IPv6 addresses 0:0:0:0:0:0:0:0 and 0:0:0:0:0:0:0:1 are reserved as the loopback addresses.

ExamAlert

Remember that fe80:: is a private link-local address.

Comparing IPv4 and IPv6 Addressing

Table 3.5 compares IPv4 and IPv6 addressing.

Note

Automatic Private IP Addressing (APIPA) appears in the table and is discussed in detail in the section “Automatic Private IP Addressing (APIPA)” later in this chapter.

<table>
<thead>
<tr>
<th>Address Feature</th>
<th>IPv4 Address</th>
<th>IPv6 Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopback address</td>
<td>127.0.0.1</td>
<td>0:0:0:0:0:0:0:1 (:1)</td>
</tr>
<tr>
<td>Network-wide addresses</td>
<td>IPv4 public address ranges</td>
<td>Global unicast IPv6 addresses</td>
</tr>
</tbody>
</table>
| Private network addresses | 10.0.0.0  
   172.16.0.0  
   192.168.0.0 | Site-local address ranges (FEC0::) |
| Autoconfigured addresses | IPv4 automatic private IP addressing (169.254.0.0) | Link-local addresses of the FE80:: prefix |
Assigning IP Addresses

Now that you understand the need for each system on a TCP/IP-based network to have a unique address, the following sections examine how those systems receive their addresses.

Static Addressing

Static addressing refers to the manual assignment of IP addresses to a system. This approach has two main problems:

- Statically configuring one system with the correct address is simple, but in the course of configuring, say, a few hundred systems, mistakes are likely to be made. If the IP addresses are entered incorrectly, the system probably cannot connect to other systems on the network.

- If the IP addressing scheme for the organization changes, each system must again be manually reconfigured. In a large organization with hundreds or thousands of systems, such a reconfiguration could take a considerable amount of time. These drawbacks of static addressing are so significant that nearly all networks use dynamic IP addressing.

Dynamic Addressing

Dynamic addressing refers to the automatic assignment of IP addresses. On modern networks, the mechanism used to do this is Dynamic Host Configuration Protocol (DHCP). DHCP, part of the TCP/IP suite, enables a central system to provide client systems with IP addresses. Automatically assigning addresses with DHCP alleviates the burden of address configuration and reconfiguration that occurs with static IP addressing.

The basic function of the DHCP service is to automatically assign IP addresses to client systems. To do this, ranges of IP addresses, known as scopes, are defined on a system running a DHCP server application. When another system configured as a DHCP client is initialized, it asks the server for an address. If all things are as they should be, the server assigns an address to the client for a predetermined amount of time, which is known as the lease, from the scope.
A DHCP server typically can be configured to assign more than just IP addresses. It often is used to assign the subnet mask, the default gateway, and Domain Name Service (DNS) information.

Using DHCP means that administrators do not need to manually configure each client system with a TCP/IP address. This removes the common problems associated with statically assigned addresses, such as human error. The potential problem of assigning duplicate IP addresses is also eliminated. DHCP also removes the need to reconfigure systems if they move from one subnet to another, or if you decide to make a wholesale change in the IP addressing structure.

Note

Even when a network is configured to use DHCP, several mission-critical network systems continue to use static addressing: DHCP server, DNS server, web server, and more. They do not have dynamic IP addressing because their IP addresses can never change. If they do, client systems may be unable to access the resources from that server.

Configuring a client for TCP/IP can be relatively complex, or it can be simple. Any complexity involved is related to the possible need to manually configure TCP/IP. The simplicity is because TCP/IP configuration can occur automatically via DHCP or through APIPA. At the least, a system needs an IP address and subnet mask to log on to a network. The default gateway and DNS server IP information is optional, but network functionality is limited without them. The following list briefly explains the IP-related settings used to connect to a TCP/IP network:

- **IP address**: Each system must be assigned a unique IP address so that it can communicate on the network.
- **Subnet mask**: Enables the system to determine what portion of the IP address represents the network address and what portion represents the node address.
- **Default gateway**: Enables the system to communicate on a remote network, without the need for explicit routes to be defined.
- **DNS server addresses**: Enable dynamic hostname resolution to be performed. It is common practice to have two DNS server addresses defined so that if one server becomes unavailable, the other can be used.
BOOT Protocol (BOOTP)

BOOTP was originally created so that diskless workstations could obtain information needed to connect to the network, such as the TCP/IP address, subnet mask, and default gateway. Such a system was necessary because diskless workstations had no way to store the information.

When a system configured to use BOOTP is powered up, it broadcasts for a BOOTP server on the network. If such a server exists, it compares the MAC address of the system issuing the BOOTP request with a database of entries. From this database, it supplies the system with the appropriate information. It can also notify the workstation about a file that it must run on BOOTP.

In the unlikely event that you use BOOTP, you should be aware that, like DHCP, it is a broadcast-based system. Therefore, routers must be configured to forward BOOTP broadcasts.

Automatic Private IP Addressing (APIPA)

Automatic Private IP Addressing (APIPA) was introduced with Windows 98 and has been included in all subsequent Windows versions. The function of APIPA is that a system can give itself an IP address if it is incapable of receiving an address dynamically from a DHCP server. Then APIPA assigns the system an address from the 169.254.0.0 address range and configures an appropriate subnet mask (255.255.0.0). However, it doesn’t configure the system with a default gateway address. As a result, communication is limited to the local network.

ExamAlert

At the very minimum, an IP address and subnet mask are required to connect to a TCP/IP network. With just this minimum configuration, connectivity is limited to the local segment, and DNS resolution is not possible.

ExamAlert

If a system that does not support APIPA cannot get an address from a DHCP server, it typically assigns itself an IP address of 0.0.0.0. Keep this in mind when troubleshooting IP addressing problems on non-APIPA platforms.
The idea behind APIPA is that systems on a segment can communicate with each other if DHCP server failure occurs. In reality, the limited usability of APIPA makes it little more than a last resort. For example, imagine that a system is powered on while the DHCP server is operational and receives an IP address of 192.168.100.2. Then the DHCP server fails. Now, if the other systems on the segment are powered on and cannot get an address from the DHCP server because it is down, they would self-assign addresses in the 169.254.0.0 address range via APIPA. The systems with APIPA addresses would talk to each other, but they couldn’t talk to a system that received an address from the DHCP server. Likewise, any system that receives an IP address via DHCP cannot talk to systems with APIPA-assigned addresses. This, and the absence of a default gateway, is why APIPA is of limited use in real-world environments.

ExamAlert
Be prepared to answer APIPA questions. Know what it is and how you can tell if you have been assigned an APIPA address and why.

Identifying MAC Addresses

Many times this book refers to MAC addresses and how certain devices use them. However, it has not yet discussed why MAC addresses exist, how they are assigned, and what they consist of.

Note
A MAC address is sometimes called a physical address because it is physically embedded in the interface.

A MAC address is a 6-byte (48-bit) hexadecimal address that enables a NIC to be uniquely identified on the network. The MAC address forms the basis of network communication, regardless of the protocol used to achieve network connection. Because the MAC address is so fundamental to network communication, mechanisms are in place to ensure that duplicate addresses cannot be used.

To combat the possibility of duplicate MAC addresses being assigned, the Institute of Electrical and Electronics Engineers (IEEE) took over the assignment of MAC addresses. But rather than be burdened with assigning individual addresses, the IEEE decided to assign each manufacturer an ID and then
let the manufacturer further allocate IDs. The result is that in a MAC address, the first 3 bytes define the manufacturer, and the last 3 are assigned by the manufacturer.

For example, consider the MAC address of the computer on which this book is being written: 00:D0:59:09:07:51. The first 3 bytes (00:D0:59) identify the manufacturer of the card; because only this manufacturer can use this address, it is known as the Organizational Unique Identifier (OUI). The last 3 bytes (09:07:51) are called the Universal LAN MAC address: They make this interface unique. You can find a complete listing of organizational MAC address assignments at http://standards.ieee.org/regauth/oui/oui.txt.

ExamAlert
Because MAC addresses are expressed in hexadecimal, only the numbers 0 through 9 and the letters A through F can be used in them. If you get an exam question about identifying a MAC address and some of the answers contain letters and numbers other than 0 through 9 and the letters A through F, you can immediately discount those answers.

You can discover the NIC’s MAC address in various ways, depending on what system or platform you work on. Table 3.6 defines various platforms and methods you can use to view an interface’s MAC address.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2003/2008/XP/Vista/7</td>
<td>Enter ipconfig /all at a command prompt.</td>
</tr>
<tr>
<td>Linux/some Unix</td>
<td>Enter the ifconfig -a command.</td>
</tr>
<tr>
<td>Novell NetWare</td>
<td>Enter the config command.</td>
</tr>
<tr>
<td>Cisco router</td>
<td>Enter the sh int interface name command.</td>
</tr>
</tbody>
</table>

ExamAlert
Be sure you know the commands used to identify the MAC address in various operating system formats.
Network Address Translation (NAT) and Port Address Translation (PAT)

This chapter has defined many acronyms and continues with two more: NAT and PAT.

NAT

The basic principle of NAT is that many computers can “hide” behind a single IP address. The main reason you need to do this (as pointed out earlier in the section “IP Addressing”) is because there simply aren’t enough IPv4 addresses to go around. Using NAT means that only one registered IP address is needed on the system’s external interface, acting as the gateway between the internal and external networks.

Note

Don’t confuse NAT with proxy servers. The proxy service is different from NAT, but many proxy server applications do include NAT functionality.

NAT enables you to use whatever addressing scheme you like on your internal networks; although, it is common practice to use the private address ranges, which were discussed earlier.

When a system is performing NAT, it funnels the requests given to it to the Internet. To the remote host, the request looks like it is originating from a single address. The system performing the NAT function keeps track of who asked for what and makes sure that when the data is returned, it is directed to the correct system. Servers that provide NAT functionality do so in different ways. For example, you can statically map a specific internal IP address to a specific external one (known as the one-to-one NAT method) so that outgoing requests are always tagged with the same IP address. Alternatively, if you have a group of public IP addresses, you can have the NAT system assign addresses to devices on a first-come, first-served basis. Either way, the basic function of NAT is the same.

There is a transition technology known as Teredo that gives full IPv6 connectivity for IPv6-capable hosts, which are on the IPv4 Internet but lack direct native connection to an IPv6 network. The distinguishing feature of Teredo is that it can do this from behind network address translation (NAT) devices (such as home routers). You can find more information on this at http://ipv6.com/articles/nat/NAT-In-Depth.htm.
PAT enables administrators to conserve public IP addresses and, at the same time, secure the internal network. Port Address Translation (PAT) is a variation on NAT. With PAT, all systems on the LAN are translated to the same IP address, but with a different port number assignment. PAT is used when multiple clients want to access the Internet. However, with not enough available public IP addresses, you need to map the inside clients to a single public IP address. When packets come back into the private network, they are routed to their destination with a table within PAT that tracks the public and private port numbers.

When PAT is used, there is a typically only a single IP address exposed to the public network, and multiple network devices access the Internet through this exposed IP address. The sending devices, IP address, and port number are not exposed. For example, an internal computer with the IP address of 192.168.2.2 wants to access a remote Web server at address 204.23.85.49. The request goes to the PAT router where the sender's private IP and port number are modified, and a mapping is added to the PAT table. The remote web server sees the request coming from the IP address of the PAT router and not the computer actually making the request. The web server sends the reply to the address and port number of the router. When received, the router checks its table to see the packet’s actual destination and forwards it.

ExamAlert

PAT enables nodes on a LAN to communicate with the Internet without revealing their IP address. All outbound IP communications are translated to the router’s external IP address. Replies come back to the router that then translates them back into the private IP address of the original host for final delivery.

Static NAT is a simple form of NAT. Static Network Address Translation (SNAT) directly maps a private IP address to a static unchanging public IP address. This enables an internal system, such as a mail server, to have an unregistered (private) IP address and still be reachable over the Internet. For example, if a network uses a private address of 192.168.2.1 for a mail server, it can be statically linked to a public IP address such as 213.23.213.85.
Cram Quiz

1. What is the IPv6 equivalent of 127.0.0.1? (Choose two.)
   - A. 0:0:0:0:0:0:0:1
   - B. 0:0:0:0:0:0:0:24
   - C. ::1
   - D. ::24

2. Which of the following is a Class B address?
   - A. 129.16.12.200
   - B. 126.15.16.122
   - C. 211.244.212.5
   - D. 193.17.101.27

3. You are the administrator for a network with two Windows Server systems and 65 Windows 7 systems. At 10 a.m., three users call to report that they are experiencing network connectivity problems. Upon investigation, you determine that the DHCP server has failed. How can you tell that the DHCP server failure is the cause of the connectivity problems experienced by the three users?
   - A. When you check their systems, they have an IP address of 0.0.0.0.
   - B. When you check their systems, they have an IP address in the 192.168.x.x address range.
   - C. When you check their systems, they have a default gateway value of 255.255.255.255.
   - D. When you check their systems, they have an IP address from the 169.254.x.x range.

4. Which of the following address types are associated with IPv6? (Choose three.)
   - A. Broadcast
   - B. Multicast
   - C. Unicast
   - D. Anycast

5. Which of the following IP addresses is not from a private address range?
   - A. 192.168.200.117
   - B. 172.16.3.204
   - C. 127.45.112.16
   - D. 10.27.100.143
6. You have been assigned to set up a new network with TCP/IP. For the external interfaces, you decide to obtain registered IP addresses from your ISP, but for the internal network, you choose to configure systems by using one of the private address ranges. Of the following address ranges, which one would you not consider?

- A. 192.168.0.0 to 192.168.255.255
- B. 131.16.0.0 to 131.16.255.255
- C. 10.0.0.0 to 10.255.255.255
- D. 172.16.0.0 to 172.31.255.255

7. You ask your ISP to assign a public IP address for the external interface of your Windows 2008 server, which is running a proxy server application. In the email message you get that contains the information, the ISP tells you that you have been assigned the IP address 203.15.226.12/24. When you fill out the subnet mask field on the IP configuration dialog box on your system, what subnet mask should you use?

- A. 255.255.255.255
- B. 255.255.255.0
- C. 255.255.240.0
- D. 255.255.255.240

8. Examine the diagram shown here. What is the most likely reason that user Spencer cannot communicate with user Evan?

- A. The default gateways should have different values.
- B. Spencer’s IP address is not a loopback address.
- C. The subnet values should be the same.
- D. There is no problem identifiable by the values given.

User: Evan
IP address: 192.168.1.121
Subnet mask: 255.255.255.0
Default gateway: 192.168.1.1

User: Spencer
IP address: 192.168.1.127
Subnet mask: 255.255.248.0
Default gateway: 192.168.1.1
Cram Quiz Answers

1. A and C. The IPv4 address 127.0.0.1 is reserved as the loopback address, and IPv6 has the same reservation. IPv6 addresses 0:0:0:0:0:0:0 and 0:0:0:0:0:0:0:1 are reserved as the loopback addresses. The address 0:0:0:0:0:0:0:1 can be shown using the :: notation with the 0s removed, resulting in ::1.

2. A. Class B addresses fall into the range 128 to 191. Answer A is the only address listed that falls into that range. Answer B is a Class A address, and answers C and D are Class C IP addresses.

3. D. When a Windows 7 system that is configured to obtain an IP address via DHCP fails to obtain an address, it uses APIPA to assign itself an address from the 169.254.x.x address range. An address of 0.0.0.0 normally results from a system that does not support APIPA. APIPA does not use the 192.168.x.x address range. The IP address 255.255.255.255 is the broadcast address. A DHCP failure would not lead to a system assigning itself this address.

4. B, C, and D. A key difference between IPv4 and IPv6 is in the address types. IPv6 addressing has three main types of addresses: unicast, multicast, and anycast. IPv4 uses broadcast addressing, but IPv6 doesn’t.

5. C. The 127.x.x.x network range is reserved for the loopback function. It is not one of the recognized private address ranges. The private address ranges as defined in RFC 1918 are 10.x.x.x, 172.16.x.x to 172.31.x.x, and 192.168.x.x.

6. B. The 131.16 range is from the Class B range and is not one of the recognized private IP address ranges. All the other address ranges are valid private IP address ranges.

7. B. In CIDR terminology, the number of bits to be included in the subnet mask is expressed as a slash value. If the slash value is 24, the first three octets form the subnet mask, so the value is 255.255.255.0.

8. C. The most likely problem, given the IP values for each user’s workstation, is that the subnet value is not correct on Spencer’s machine and should be 255.255.255.0.
Understanding TCP/UDP Port Functions

- Identify common TCP and UDP default ports.

**CramSaver**

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then complete the Cram Quiz at the end of the section.

1. What is the default port used by NTP?
2. True or False: Although FTP is a TCP-based protocol, TFTP uses UDP.

**Answers**

1. By default, NTP uses port 123.
2. True. Although FTP is a TCP-based protocol, TFTP uses UDP.

Each TCP/IP or application has a port associated with it. When a communication is received, the target port number is checked to determine which protocol or service it is destined for. The request is then forwarded to that protocol or service. For example, consider HTTP, whose assigned port number is 80. When a web browser forms a request for a web page, that request is sent to port 80 on the target system. When the target system receives the request, it examines the port number. When it sees that the port is 80, it forwards the request to the web server application.

TCP/IP has 65,535 ports available, with 0 to 1023 labeled as the well-known ports. Although a detailed understanding of the 65,535 ports is not necessary for the Network+ exam, you need to understand the numbers of some well-known ports. Network administration often requires you to specify port assignments when you work with applications and configuring services. Table 3.7 shows some of the most common port assignments.

**ExamAlert**

You should concentrate on the information provided in Table 3.7 and answer any port-related questions you might receive. The exam may present you with a situation in which you can’t access a particular service; you may have to determine whether a port is open or closed on a firewall.
TABLE 3.7  TCP/IP Port Assignments for Commonly Used Protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TCP Ports</strong></td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td>20</td>
</tr>
<tr>
<td>FTP</td>
<td>21</td>
</tr>
<tr>
<td>SSH</td>
<td>22</td>
</tr>
<tr>
<td>Telnet</td>
<td>23</td>
</tr>
<tr>
<td>SMTP</td>
<td>25</td>
</tr>
<tr>
<td>DNS</td>
<td>53</td>
</tr>
<tr>
<td>HTTP</td>
<td>80</td>
</tr>
<tr>
<td>POP3</td>
<td>110</td>
</tr>
<tr>
<td>NNTP</td>
<td>119</td>
</tr>
<tr>
<td>NTP</td>
<td>123</td>
</tr>
<tr>
<td>IMAP4</td>
<td>143</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
</tr>
<tr>
<td>RDP</td>
<td>3389</td>
</tr>
<tr>
<td><strong>UDP Ports</strong></td>
<td></td>
</tr>
<tr>
<td>TFTP</td>
<td>69</td>
</tr>
<tr>
<td>DNS</td>
<td>53</td>
</tr>
<tr>
<td>DHCP (and BOOTP server)</td>
<td>67</td>
</tr>
<tr>
<td>DHCP (and BOOTP client)</td>
<td>68</td>
</tr>
<tr>
<td>SNMP</td>
<td>161</td>
</tr>
<tr>
<td>RDP</td>
<td>3389</td>
</tr>
</tbody>
</table>

The term *well-known ports* identifies the ports ranging from 0 to 1023. When CompTIA says to “identify the well-known ports,” this is what it refers to.

**ExamAlert**

You might have noticed in Table 3.7 that two ports are associated with FTP. Port 20 is considered the data port, whereas port 21 is considered the control port. In practical use, FTP connections use port 21. Port 20 is rarely used in modern implementations.
Cram Quiz

1. As the network administrator, you decide to block port 80. Which of the following services will be unavailable for network users?
   - A. DNS
   - B. POP3
   - C. FTP
   - D. HTTP

2. Which of the following is the most commonly used port for FTP in modern implementations?
   - A. 20
   - B. 21
   - C. 23
   - D. 27

Cram Quiz Answers

1. D. The HTTP service uses port 80, so blocking port 80 prevents users from using the HTTP service. Answer A is incorrect because DNS uses port 53. Answer B is incorrect because POP3 uses port 110. Answer C is incorrect because FTP uses port 21.

2. B. The most commonly used port for FTP in modern implementations is 21.
Managing TCP/IP Routing

- Explain the purpose and properties of routing and switching.

CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then complete the Cram Quiz at the end of the section.

1. What are the most common distance-vector routing protocols?
2. What are the most common link-state protocols?
3. What is convergence?

Answers

1. Distance-vector routing protocols include RIP, RIPv2, BGP, and EIGRP.
2. Link-state protocols include OSPF and IS-IS.
3. Convergence represents the time it takes routers to detect change on the network.

Because today’s networks branch out between interconnected offices all over the world, networks may have any number of separate physical network segments connected using routers. Routers are devices that direct data between networks. Essentially, when a router receives data, it must determine the destination for the data and send it there. To accomplish this, the network router uses two key pieces of information: the gateway address and the routing tables.

The Default Gateway

A default gateway is the router’s IP address, which is the pathway to any and all remote networks. To get a packet of information from one network to another, the packet is sent to the default gateway, which helps forward the packet to its destination network. Computers that live on the other side of routers are said to be on remote networks. Without default gateways, Internet communication is not possible because your computer doesn’t have a way to send a packet destined for any other network. On the workstation, it is common for the default gateway option to be configured automatically through DHCP configuration.
Routing Tables

Before a data packet is forwarded, a chart is reviewed to determine the best possible path for the data to reach its destination. This chart is the computer’s routing table. Maintaining an accurate routing table is essential for effective data delivery. Every computer on a TCP/IP network has a routing table stored locally. Figure 3.3 shows the routing table on a Windows 7 system.

As shown in Figure 3.3, the information in the routing table includes the following:

- **Destination**: The host IP address.
- **Network mask**: The subnet mask value for the destination parameter.
- **Gateway**: Where the IP address is sent. This may be a gateway server, router, or another system acting as a gateway.
- **Interface**: The address of the interface that’s used to send the packet to the destination.
- **Metric**: A measurement of the directness of a route. The lower the metric, the faster the route. If multiple routes exist for data to travel, the one with the lowest metric is chosen.

Routing tables play an important role in the network routing process. They are the means by which the data is directed through the network. For this reason, a routing table needs to be two things. It must be up to date and complete. The router can get the information for the routing table in two ways: through static routing or dynamic routing.
Static Routing

In environments that use static routing, routes and route information are manually entered into the routing tables. Not only can this be a time-consuming task, but also errors are more common. In addition, when a change occurs to the network's layout, or topology, statically configured routers must be manually updated with the changes. Again, this is a time-consuming and potentially error-laden task. For these reasons, static routing is suited to only the smallest environments, with perhaps just one or two routers. A far more practical solution, particularly in larger environments, is to use dynamic routing.

You can add a static route to a routing table using the `route add` command. To do this, specify the route, the network mask, and the destination IP address of the network card your router will use to get the packet to its destination network.

The syntax for the `route add` command is as follows:

```
route add 192.168.2.1 mask (255.255.255.0) 192.168.2.4
```

Adding a static address is not permanent; in other words, it will most likely be gone when the system reboots. To make it persistent (the route is still in the routing table on boot), you can use the switch with the command.
Dynamic Routing

In a *dynamic routing* environment, routers use special routing protocols to communicate. The purpose of these protocols is simple: They enable routers to pass on information about themselves to other routers so that other routers can build routing tables. Two types of routing protocols are used: the older distance-vector protocols and the newer link-state protocols.

**Distance-Vector Routing**

With distance-vector router communications, each router on the network communicates all the routes it knows about to the routers to which it is directly attached. In this way, routers communicate only with their router neighbors and are unaware of other routers that may be on the network.

The communication between distance-vector routers is known as *hops*. On the network, each router represents one hop, so a network using six routers has five hops between the first and last router.

The `tracert` command is used in a Windows environment to see how many hops a packet takes to reach a destination. To try this at the command prompt, enter `tracert comptia.org`. Figure 3.4 shows an example of the output on a Windows 7 workstation.

![FIGURE 3.4 The results of running tracert on a Windows 7 system.](image)
Several distance-vector protocols are in use today, including Routing Information Protocol (RIP and RIPv2), Enhanced Interior Gateway Routing Protocol (EIGRP), and Border Gateway Protocol (BGP):

- **RIP**: As mentioned, RIP is a distance-vector routing protocol. RIP is limited to a maximum of 15 hops. One of the downsides of the protocol is that the original specification required router updates to be transmitted every 30 seconds. On smaller networks this is acceptable; however, this can result in a huge traffic load on larger networks. The original RIP specification also did not support router authentication, leaving it vulnerable to attacks.

- **RIPv2**: The second version of RIP dealt with the shortcomings of the original design. Authentication was included to enable secure transmissions, also, it changed from a networkwide broadcast discovery method to a multicast method to reduce overall network traffic. However, to maintain compatibility with RIP, RIPv2 still supports a limit of 15 hops.

- **BGP**: A routing protocol often associated with the Internet. BGP can be used between gateway hosts on the Internet. BGP examines the routing table, which contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen. BGP communicates between the routers using TCP.

- **EIGRP**: A protocol that enables routers to exchange information more efficiently than earlier network protocols. EIGRP uses its neighbors to help determine routing information. Routers configured to use EIGRP keep copies of their neighbors’ routing information and query these tables to help find the best possible route for transmissions to follow. EIGRP uses Diffusing Update Algorithm (DUAL) to determine the best route to a destination.

Distance-vector routing protocols operate by having each router send updates about all the other routers it knows about to the routers directly connected to it. The routers use these updates to compile their routing tables. The updates are sent automatically every 30 or 60 seconds. The interval depends on the
routing protocol used. Apart from the periodic updates, routers can also be configured to send a *triggered update* if a change in the network topology is detected. The process by which routers learn of a change in the network topology is called *convergence*.

Routing loops can occur on networks with slow convergence. Routing loops occur when the routing tables on the routers are slow to update and a redundant communication cycle is created between routers. Two strategies can combat potential routing loops:

- **Split horizon**: Works by preventing the router from advertising a route back to the other router from which it was learned. This prevents two nodes from bouncing packets back and forth between them, creating a loop.

- **Poison reverse (also called split horizon with poison reverse)**: Dictates that the route *is* advertised back on the interface from which it was learned, but it has a hop count of infinity, which tells the node that the route is unreachable.

**ExamAlert**

If a change in the routing is made, it takes some time for the routers to detect and accommodate this change. This is known as convergence.

Although distance-vector protocols can maintain routing tables, they have three problems:

- The periodic update system can make the update process slow.

- The periodic updates can create large amounts of network traffic—much of the time unnecessarily, because the network’s topology should rarely change.

- Perhaps the most significant problem is that because the routers know about only the next hop in the journey, incorrect information can be propagated between routers, creating routing loops.

**ExamAlert**

Know that “next hop” in routing is the next closest router that a packet can go through.
Link-State Routing

A router that uses a link-state protocol differs from a router that uses a distance-vector protocol because it builds a map of the entire network and then holds that map in memory. On a network that uses a link-state protocol, routers send link-state advertisements (LSAs) that contain information about the networks to which they connect. The LSAs are sent to every router on the network, thus enabling the routers to build their network maps.

When the network maps on each router are complete, the routers update each other at a given time, just like with a distance-vector protocol; however, the updates occur much less frequently with link-state protocols than with distance-vector protocols. The only other circumstance under which updates are sent is if a change in the topology is detected, at which point the routers use LSAs to detect the change and update their routing tables. This mechanism, combined with the fact that routers hold maps of the entire network, makes convergence on a link-state-based network quickly occur.

Although it might seem like link-state protocols are an obvious choice over distance-vector protocols, routers on a link-state-based network require more powerful hardware and more RAM than those on a distance-vector-based network. Not only do the routing tables need to be calculated, but they must also be stored. A router that uses distance-vector protocols need only maintain a small database of the routes accessible by the routers to which it is directly connected. A router that uses link-state protocols must maintain a database of all the routers in the entire network.

Link-state protocols include the following:

- **Open Shortest Path First (OSPF)**: A link-state routing protocol based on the SPF (Shortest Path First) algorithm to find the least-cost path to any destination in the network. In operation, each router using OSPF sends a list of its neighbors to other routers on the network. From this information, routers can determine the network design and the shortest path for data to travel.

- **Intermediate System-to-Intermediate System (IS-IS)**: A link-state protocol that discovers the shortest path for data to travel using the shortest path first (SPF) algorithm. IS-IS routers distribute topology information to other routers, enabling them to make the best path decisions.

So what’s the difference between the two? OSPF (a network layer protocol) is more often used in medium to large enterprise networks because of its special
tunneling features. IS-IS is more often used in large ISP networks because of its stability features and that it can support more routers.

**IGP Versus EGP**

Now that routing protocols have been discussed, you need to understand the difference between Interior Gateway Protocols (IGPs) and Exterior Gateway Protocols (EGPs). An IGP identifies the protocols used to exchange routing information between routers within a LAN or interconnected LANs. IGP is not a protocol itself but describes a category of link-state routing protocols that support a single, confined geographic area such as a LAN. IGPs fall into two categories: distance-vector protocols, which include RIP and IGRP, and link-state protocols, which include OSPF and IS-IS.

Whereas IGPs are geographically confined, EGPs are used to route information outside the network, such as on the Internet. On the Internet, an EGP is required. An EGP is a distance-vector protocol commonly used between hosts on the Internet to exchange routing table information. BGP is an example of an EGP.

---

**Routing Metrics**

Following are a number of metrics related to routing that you should know for the exam:

- *Hop counts* are the number of hops necessary to reach a node. A hop count of infinity means the route is unreachable.

- The *Maximum Transmission Unit (MTU)* defines the largest data unit that can be passed without fragmentation.

- *Bandwidth* specifies the maximum packet size permitted for Internet transmission.

- *Costs* are the numbers associated with traveling from point A to point B (often hops). The lower the total costs (the less links in the route), the more that route should be favored.

- *Latency* is the amount of time it takes for a packet to travel from one location to another.
Cram Quiz

1. Which of the following best describes the function of the default gateway?
   - A. It provides the route for destinations outside the local network.
   - B. It enables a single Internet connection to be used by several users.
   - C. It identifies the local subnet and formulates a routing table.
   - D. It is used to communicate in a multiple-platform environment.

2. What is the term used for the number of hops necessary to reach a node?
   - A. Jump list
   - B. Link stops
   - C. Connections
   - D. Hop count

Cram Quiz Answers

1. A. The default gateway enables systems on one local subnet to access those on another. Answer B does not accurately describe the role of the default gateway. Answers C and D don’t describe the main function of a default gateway, which is to provide the route for destinations outside the local network.

2. D. The hop count is the number of hops necessary to reach a node.
Configuring Routers and Switches

Given a scenario, install and configure routers and switches.

CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then complete the Cram Quiz at the end of the section.

1. Which technology enables electrical power to transmit over twisted-pair Ethernet cable?

2. True or False: With the help of FSL, STP avoids or eliminates loops on Layer 2 bridges.

Answers

1. Power over Ethernet (PoE) is the technology that enables electrical power to transmit over twisted-pair Ethernet cable.

2. False. With the help of Spanning Tree Algorithm (STA), STP avoids or eliminates loops on a Layer 2 bridge.

The next chapter focuses on actual hardware components of a network, but the reason for the hardware is to carry out the operations discussed in this chapter. This section looks at a few of the more advanced features that routers and switches perform.

Power over Ethernet (PoE)

The purpose of Power over Ethernet (PoE) is pretty much described in its name. Essentially, PoE is a technology that enables electrical power to transmit over twisted-pair Ethernet cable. The power transfers, along with data, to provide power to remote devices. These devices may include remote switches, wireless access points, voice over IP (VoIP) equipment, and more.

One of the key advantages of PoE is the centralized management of power. For instance, without PoE, all remote devices need to be independently powered. In the case of a power outage, each of these devices requires an uninterruptible power supply (UPS) to continue operating. A UPS is a battery pack that enables devices to operate for a period of time. With PoE supplying
power, a UPS is required only in the main facility. In addition, centralized power management enables administrators to power up or down remote equipment.

**Note**

VLAN and spanning tree were outlined in the CompTIA objectives for this chapter. Spanning tree is covered next. VLANs are discussed in Chapter 1, “Introduction to Networking.”

### The Spanning Tree Protocol (STP)

An Ethernet network can have only a single active path between devices on a network. When multiple active paths are available, switching loops can occur. Switching loops are simply the result of having more than one path between two switches in a network. Spanning Tree Protocol (STP) is designed to prevent these loops from occurring.

STP is used with network bridges and switches. With the help of Spanning Tree Algorithm (STA), STP avoids or eliminates loops on a Layer 2 bridge.

**Note**

As a heads-up, talking about STP refers to Layer 2 of the OSI model. Both bridges and switches work at Layer 2. Routers work at Layer 3.

STA enables a bridge or switch to dynamically work around loops in a network's topology. Both STA and STP were developed to prevent loops in the network and provide a way to route around any failed network bridge or ports. If the network topology changes, or if a switch port or bridge fails, STA creates a new spanning tree, notifies the other bridges of the problem, and routes around it. STP is the protocol, and STA is the algorithm STP uses to correct loops.

If a particular port has a problem, STP can perform a number of actions, including blocking the port, disabling the port, or forwarding data destined for that port to another port. It does this to ensure that no redundant links or paths are found in the spanning tree and that only a single active path exists between any two network nodes.

STP uses bridge protocol data units (BPDUs) to identify the status of ports and bridges across the network. BPDUs are simple data messages exchanged between switches. BPDUs contain information on ports and provide the status
of those ports to other switches. If a BPDU message finds a loop in the network, it is managed by shutting down a particular port or bridge interface.

Redundant paths and potential loops can be avoided within ports in several ways:

- **Blocking**: A blocked port accepts BPDU messages but does not forward them.
- **Disabled**: The port is offline and does not accept BPDU messages.
- **Forwarding**: The port is part of the active spanning tree topology and forwards BPDU messages to other switches.
- **Learning**: In a learning state, the port is not part of the active spanning tree topology but can take over if another port fails. Learning ports receive BPDUs and identify changes to the topology when made.
- **Listening**: A listening port receives BPDU messages and monitors for changes to the network topology.

Most of the time, ports are in either a forwarding or blocked state. When a disruption to the topology occurs or a bridge or switch fails for some reason, listening and learning states are used.

**ExamAlert**

STP actively monitors the network, searching for redundant links. When it finds some, it shuts them down to prevent switching loops. STP uses STA to create a topology database to find and then remove the redundant links. With STP operating from the switch, data is forwarded on approved paths, which limits the potential for loops.

**Trunking**

In computer networking, the term *trunking* refers to the use of multiple network cables or ports in parallel to increase the link speed beyond the limits of any one cable or port. Sound confusing? If you have network experience, you might have heard the term *link aggregation*, which is essentially the same thing. It is just using multiple cables to increase the throughput. The higher-capacity trunking link is used to connect switches to form larger networks.

*VLAN trunking*—or *VLAN (trunking)*, as CompTIA lists it—is the application of trunking to the virtual LAN—now common with routers, firewalls, VMWare hosts, and wireless access points. VLAN trunking provides a simple
and cheap way to offer a nearly unlimited number of virtual network connections. The requirements are only that the switch, the network adapter, and the OS drivers all support VLANs. The VLAN Trunking Protocol (VTP) is a proprietary protocol from Cisco for just such a purpose.

**Port Mirroring**

You need some way to monitor network traffic and monitor how well a switch works. This is the function of port mirroring. To use port mirroring, administrators configure a copy of all inbound and outbound traffic to go to a certain port. A protocol analyzer examines the data sent to the port and therefore does not interrupt the flow of regular traffic.

---

**ExamAlert**

Port mirroring enables administrators to monitor the traffic outbound and inbound to the switch.

---

**Port Authentication**

Port authentication is what it sounds like—authenticating users on a port-by-port basis. One standard that specifies port authentication is the 802.1X standard, often associated with wireless security. Systems that attempt to connect to a LAN port must be authenticated. Those who are authenticated can access the LAN; those who are not authenticated get no further. Chapter 10 provides more information on the 802.1X standard and port authentication.
Cram Quiz

1. Port mirroring enables administrators to monitor which traffic to the switch?
   - A. Inbound only
   - B. Outbound only
   - C. Inbound and outbound
   - D. Neither inbound nor outbound

2. Which of the following is NOT used to avoid redundant paths and potential loops within ports?
   - A. Blocking
   - B. Learning
   - C. Forwarding
   - D. Jamming

Cram Quiz Answers

1. C. Port mirroring enables administrators to monitor the traffic outbound and inbound to the switch.

2. D. The common methods to avoid redundant paths and potential loops within ports include blocking, disabled, forwarding, learning, and listening. Jamming is not one of the methods employed.
What Next?

Chapter 4, “Components and Devices,” introduces you to commonly used networking devices. All but the most basic of networks require devices to provide connectivity and functionality. Understanding how these networking devices operate and identifying the functions they perform are essential skills for any network administrator and are requirements for a Network+ candidate.
Index

Numerics

3G (HSPA+), 204
4G (LTE), 204
10 Gigabit Ethernet standard, 253
10BaseT LAN standard, 249-250
10GBaseER/EW Gigabit Ethernet standard, 254
10GBaseLR/LW Gigabit Ethernet standard, 254
10GBaseSR/SW Gigabit Ethernet standard, 253-254
10GBaseT Gigabit Ethernet standard, 255
100BaseFX LAN standard, 250-251
100BaseTX LAN standard, 250-251
110 blocks (T568A, T568B), 235-236
568A wiring standard, 227
568B wiring standard, 227
802.11 wireless standards (IEEE), 277-278, 284, 286-287
802.11a wireless standard (IEEE), 268, 271, 285-286
802.11b wireless standard (IEEE), 285-286
802.11b/g wireless standard (IEEE), 269-270
802.11g wireless standard (IEEE), 285, 287
802.11i wireless standard (IEEE), 293
802.11n wireless standard (IEEE), 270, 285-287
802.1Q IEEE specification, VLAN and, 36
802.1X wireless standard (IEEE), 294-295
1000BaseCX LAN standard, 252
administration

command-line utilities
  arp command, 351, 360-361
  arp ping command, 351, 362-363
  dig command, 351, 375-376
  host command, 351, 376
  ifconfig command, 351, 372-373
  ipconfig command, 351, 370-372
  nbtstat command, 351, 369-370
  netstat command, 351, 363-369
  nslookup command, 351, 373-374
  ping command, 351, 355-360
  route command, 351, 376
  traceroute command, 351-355
  tracert command, 351-355

consultants, 304
contractors, 303, 305
documentation, 303, 305
  advantages of, 304
  applications, 306
  baselines, 313-314
  capturing statistics, 313
  configuration documentation, 317
  logical network diagrams, 310
  network hardware, 306
  network procedures, 306
  network services, 306
  network topologies, 305
  physical diagrams, 310-313
  physical network diagrams, 310
  policies, 314-315
  procedures, 315-316
  regulations, 317-318
  server configurations, 306
  updating, 312
  wiring layouts, 306
  wiring schematics, 307-310

management tools, fault detection, 323
network configuration, 324
network maintenance, 324
performance monitoring, 322-323
  application logs, 333, 335
  event logs, 331-335
  history logs, 334-335
  LM, 335
  load testing, 330
  packet sniffers, 324-325
  performance tests, 329-330
  port scanners, 327-329
  security logs, 332, 335
  stress tests, 330
  syslog, 334
  system logs, 334-335
  throughput testing, 325, 327
remote management, 324
security monitoring, 324
tools, 338
  butt sets, 346
  cable certifiers, 344
  environmental monitors, 341
  media testers, 344
  multimeters, 345-346
  network qualification testers, 346
  optical cable testers, 345
  OTDR, 345
  protocol analyzers, 343-344
  punchdown tools, 340
  snips, 339
  strippers, 339
  TDR, 344
  toner probes, 342-343
  voltage event recorders, 340
  Wi-Fi detectors, 347
  wire crimpers, 339
training, 304
virtual desktops, 163
VLAN, 36

**ADSL (Asymmetric Digital Subscriber Line) Internet access, 192-193**

**AH protocol (Authentication Header protocol), IPSec, 417**

**air conditioning, 342**

**alarms, remote (smart jacks), 238**

**analog modems, VPN and, 34**

**ANSWER SECTION (dig command), 375**

**answers**

  format of, Network+ exams, 5
  practice exams
    exam 1, 537-559
    exam 2, 585-606

**antennas (wireless), 264**

  adjusting, 263
  directional antennas, 266
  gain values, 265
  interference, 267
  MIMO antennas, 285
  omnidirectional antennas, 265-266
  polarization, 267
  ratings, 265
  replacing, 263
  signal quality, 267
  troubleshooting, 263, 267-268, 299
  wireless connections, configuring, 279

**antivirus software**

  features of, 456-457
  scanning for viruses, 456-457, 461

**anycast addresses, 106**

**AP (access points), 259-261**

  ad hoc wireless topologies, 23
  beacons, 272
  bridges, AP as, 261, 276
  BSA and, 263
  BSS, 262, 276
  BSSID and, 262
ESS, 262, 276
ESSID and, 262
infrastructure wireless topologies, 23
LAN and, 22
OSI seven-layer networking model, mapping to, 50
rogue AP, 455
security, 262
SSID and, 262
troubleshooting, 263, 497
   adjusting/replacing antennas, 263
   increasing transmission power, 263
   relocating AP, 263
   repeaters, 264
   RF amplifiers, 264
   signal amplification, 264
wireless AP, 149
   LAN and, 22
   OSI model, 150
wireless device communication, 276
   association, 276
   authentication, 277
   reassociation, 276
   SSID, 277
APIDS (application protocol-based intrusion detection systems), 469
APIPA (Automatic Private IP Addressing), 109-110
application layer
   firewalls, 465-466
   OSI seven-layer networking model, 48-49
   TCP/IP four-layer networking model, 50
application logs, 333, 335
applications, documentation (administration), 306
archive bits, differential backups, 399
ARP (Address Resolution Protocol), 63-65, 70
   -a command switch, 64
   -d command switch, 64
   proxy ARP, troubleshooting, 486
   -s command switch, 64
arp command, 351, 360-361
arp ping command, 351, 362-363
arpa top-level domain name (DNS namespace), 78
ascii command, 58
assessing personal knowledge via exam questions, 7
association (wireless device communication), 276
asymmetric key encryption, 435, 437
ATM (Asynchronous Transfer Mode), WAN configurations, 186-187
attenuation, 213, 493
audio files, presentation layer (layer 6), 48
auditing events (security), 431
authentication, 429-430, 440-441
   CHAP, 441
   EAP, 292, 441
   Kerberos authentication, 433-436
   MS-CHAP, 440
   MS-CHAPv2, 441
   multifactor authentication, 445
   PAP, 441
   passwords, 432
   policies, 432
   strength of, 433
   port authentication, 132
   RADIUS, 439-440
   remote authentication, 440-441
   SNMPv3, 86
   TACACS+, 440
two-factor authentication, 445
wireless connections, configuring, 281
wireless device communication, 277
WPA, 292
authentication servers (802.1X wireless standard), 294
authenticators (802.1X wireless standard), 294-295
AUTHORITY SECTION (dig command), 375
authorization, 429-430
RADIUS, 439-440
TACACS+, 440
autoconfigured addresses, IP addressing, 106

B
back door attacks, 455
backbone cabling. See vertical (backbone) cabling
backoff periods, 247
backups
best practices, 401
differential backups, 398-400
full backups, 398, 400
GFS backup rotations, 400
incremental backups, 399-400
procedures, 316
tape rotations, 400
verifying, 401
bad/missing routes, troubleshooting, 488
bandwidth, 245
bandwidth shapers, 154, 160
dedicated local bandwidth, DSL Internet access, 196
firewalls and, 462
as routing metric, 127
shared bandwidth, cable Internet access, 196
baseband transmissions (TDM), 211
baselines, 313-314
beacons (wireless networks), 272
active scanning, 273
AP, 272
data rates, 272
passive scanning, 272
SSID, 272
time stamps, 272
behavior-based IDS (intrusion detection systems), 468
Bell Communications Research, 182
BGP (Border Gateway Protocol), distance-vector routing, 124
binary, decimal-to-binary value conversions, 95
binary command, 58
biometrics (physical security), 445
black holes, troubleshooting, 487-488
blackouts, UPS and, 394
blocked ports, BPDU messages, 131
BNC connectors, 221
bonding, IEEE 802.3 standard, 248
booking exams, 4
BOOTP (BOOT protocol), 109
BPDU (bridge protocol data units), STP and, 130
BPL (Broadband over Power Lines), 211
BRI (Basic Rate Interface), 179
bridges, 136, 159
AP as, 149, 261, 276
learning bridges, 137
loops, eliminating, 137
MAC addresses and, 137
multiport bridges. See switches network placement, 137
OSI model, 50, 141
source route bridges, 138
translational bridges, 138
bridges

transparent bridges, 138
troubleshooting, 497

broadband connections
Internet access, 191, 197
VPN and, 34
wireless connections, configuring, 278

broadband transmissions
BPL, 211
FDM, 211
HomePlug Powerline Alliance, 212
IEEE 1901, 212
IEEE 1905, 212

broadcast addresses, 102
broadcast storms, troubleshooting, 487

brownouts, UPS and, 394

BSA (Basic Service Areas), 263
BSS (Basic Service Sets), 262, 276
BSSID (Basic Service Set Identifiers), 262

buffer overflows, 453
buffering (flow control), 47

bus topologies, 16
advantages/disadvantages of, 17
physical bus topologies, 17

buses
compatibility, 498
NIC installations, system bus compatibility, 142
troubleshooting, 498

butt sets, 346

C
CA (certificate authorities), PKI, 436
cable certifiers, 344
cable connections, VPN and, 34
cable Internet access, 195
broadband security, 197
cabling, 195
modems, 195
shared bandwidth, 196
troubleshooting, 196-197
modems, 196
physical connections, 196
protocol configuration, 196
technical support, 196
user configurations, 196
UTP cable, 195
cabling
110 blocks (T568A, T568B), 235-236
568A wiring standard, 227
568B wiring standard, 227
attenuation, 213, 493
bad cabling, troubleshooting, 494
baseband transmissions, TDM, 211
broadband transmissions
BPL, 211
FDM, 211
HomePlug Powerline Alliance, 212
IEEE 1901, 212
IEEE 1905, 212
cable Internet access, 195
cable placement, troubleshooting, 496
cable Internet access, 195
cable placement, troubleshooting, 496
coaxial cable, 214, 218-219
connectors, troubleshooting, 494
crossover cables, 148, 228, 230, 495-496
CSU/DSU, 238
data transmission rates, 213-214
DB loss, troubleshooting, 495
demarcation points, 237-238
EMI, 492-493
fiber-optic cable, 213-215, 219-221
full-duplex mode, 212
half-duplex mode, 212
horizontal cabling, 231-232
horizontal cross-connects, 232
hub and switch cabling, 148
IDC, 235
IDF telecommunications rooms, 236
installation, verifying, 239-240
intermediate cross-connects, 232
layouts, documentation (administration), 306
loopback cabling, 231
MDF telecommunications rooms, 236
media connectors
  BNC connectors, 221
  F-Type connectors, 223
  fiber connectors, 224
  RG-6 connectors, 223
  RG-59 connectors, 223
  RJ-11 connectors, 222
  RJ-45 connectors, 223
  RS-232 standard connectors, 225
  Type A connectors, 226
  Type B connectors, 226
  USB connectors, 226
media converters, 226-227
media interference, 212-213
crosstalk, 213
EMI, 213
open impedance mismatch (echo), troubleshooting, 494
open/short faults, troubleshooting, 494
optical cable testers, 345
patch panels, 234
plenum cable, 221
punchdown tools, 235, 340
risers, 491
rollover cabling, 230
schematics, 307-310
simplex mode, 212
smart jacks, 238
snips, 339
SOHO networks, 169, 171
split cables, troubleshooting, 495
star topologies, 505
STP cable, 215
straight-through cabling, 228
stripers, 339
switch and hub cabling, 148
T-carrier lines
  T3 lines, 181
  WAN configurations, 180-181, 187
T568A wiring standard, 228
T568B wiring standard, 228
termination, verifying, 239-240
troubleshooting, 490-491
  attenuation, 493
  bad cabling, 494
cable placement, 496
  connectors, 494
crossover cables, 495-496
crosstalk, 492-493
DB loss, 495
determining where cable is used, 491-492
EMI, 492-493
FEXT, 493
interference, 492-493
NEXT, 492
open impedance mismatch (echo), 494
open/short faults, 494
split cables, 495
TXRX reversed cables, 495-496
twisted pair cable, 214-216
categories of, 216-218
longitudinal separators, 217
STP cable, 215
UTP cable, 215
TXRX reversed cables, troubleshooting, 495-496
UTP cable, 213, 215
vertical (backbone) cabling, 231, 233
vertical (main) cross-connects, 232
wire crimpers, 339
caching, 157
caching engines, 409-410
capturing statistics, 313
cards (network). See NIC
CARP (Common Address Redundancy Protocol), 393
CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), 293
cd command, 58
cellular Internet access, 204
centralized computing networks, 14
certificate templates, PKI, 436
certificates, PKI, 436, 439
certification, receiving, 6
changes, determining (troubleshooting procedures), 478
channel bonding. See bonding
canals (wireless), 268, 270
802.11a wireless standard (IEEE), 271
802.11b/g wireless standard (IEEE), 269-270
802.11n wireless standard (IEEE), 270
frequency hopping, 273
narrowband transmissions, 273
nonoverlapping channels, 268-269
overlapping channels, 269
troubleshooting, 269, 299
wireless connections, configuring, 281
wireless device communication, 277
CHAP, 441
chips, 274
chromatic dispersion. See attenuation
CIDR (Classless Interdomain Routing), 100
circuit switching, WAN configurations, 177-178
circuit-level firewalls, 465-466
Citrix ICA, 425
cladding (fiber-optic cable), 220
classes (IPv4), 95-96
cleaning tapes, backup strategies, 401
client connections, troubleshooting, 498
client requests, filtering via proxy servers, 157
client-side content filters, 155
client-to-site tunneling, 418
client/server networks, 13-14
clustering
failovers, 392
load balancing, 391
performance, 391
scalability, 392
server clustering, fault tolerance, 391-392
CNAME (Canonical Name) records, 79
coaxial cable, 214, 218-219
coaxial networks, connecting to, 498
cold recovery sites (disaster recovery), 403-404
cold spares (disaster recovery), cold swapping and, 402
collision detection, 247
com top-level domain name (DNS namespace), 77
command-line utilities
arp command, 351, 360-361
arp ping command, 351, 362-363
dig command, 351, 375-376
host command, 351, 376
ifconfig command, 351, 372-373
ipconfig command, 351, 370-372
nbtstat command, 351, 369-370
netstat command, 351, 363-364
netstat –a command, 366
netstat –c command, 365
netstat –r command, 367
netstat –s command, 368-369
nslookup command, 351, 373-374
ping command, 351, 355-356
Destination host unreachable error messages, 356
Expired TTL error messages, 358
Request timed out error messages, 357-358
troubleshooting via, 359-360
Unknown host error messages, 358
route command, 351, 376
traceroute command, 351-355
tracert command, 351-355

connections (SNMP), 85-86
components, failures, 384-385
CompTIA contact information, 6
confidentiality, PKI, 438
configuration utilities (software), NIC installations, 144
configuring
configuration documentation, 317
networks, 324
servers, documentation (administration), 306
SOHO networks, 169
wireless network connections, 278, 281-282
connection file transfer method, TFTP as, 59
connection speeds (modems), troubleshooting POTS Internet access, 200
connection-oriented protocols, 54-55
connectionless protocols, 54-55

cost
routings, 127
VPN, 34
wireless mesh networks, 27

Cram Sheet, Network+ exam cram, 1, 5

credit cards, exam scheduling requirements, 5
crimpers (wire), 339
CRL (Certificate Revocation Lists), PKI, 436
crossover cabling, 148, 228, 230, 495-496
crosstalk, 213, 492-493. See also FEXT; NEXT
CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) access method, 248
CSMA/CD (Carrier Sense Multiple Access/Collision Detection) access method, 246-248
CSU/DSU (Channel Service Units/Data Service Units), 159, 238
cut-through switching environments, 147
CuteFTP, 57

cross-over cabling

d-d command switch (ARP), 64
DAC (discretionary access control), 419
data (text) files, presentation layer (layer 6), 48
data flow control
  buffering, 47
  transport layer (layer 4), 47
  windowing, 47
data link layer (layer 2), OSI seven-layer networking model, 46, 49
data rates, 325
  cabling and, 213-214
  wireless networks, 271-272
datagram packet switching, 177
DB loss, troubleshooting, 495
DCE (data circuit-terminating equipment), Frame Relay WAN, 185
DDNS (Dynamic DNS), 76
de top-level domain name (DNS namespace), 78
decimal-to-binary value conversions, 95
dedicated broadband connections, VPN and, 34
dedicated local bandwidth, DSL Internet access, 196
default gateways
  IP addressing, 108
  IPv4 addressing, 100-102
  TCP/IP client configurations, 500
  TCP/IP routing, 120
demarcation points, 237
  smart jacks, 238
  SOHO networks, 172-173
desktops, virtual, 162
  remote administration, 163
  VDI, 163
Destination host unreachable error messages, 356
DHCP (Dynamic Host Configuration Protocol), 88-89
  DNS suffixes, 90
  dynamic addressing, 107
  process of, 89-90
  reservations, 89
DHCP servers, 138-139, 160
dial tones, troubleshooting POTS Internet access, 199
dial-up Internet access. See POTS (plain old telephone system) Internet access
dialog modes, 212
differential backups, 398-400
diffused infrared wireless networking, 275
dig command, 351, 375-376
digital certificates, PKI and, 439
digital signatures, PKI and, 438
dip switches, 144
directed (line-of-sight) infrared wireless networking, 275
directional antennas, 266
disabled ports, BPDU messages, 131
disaster recovery, 397
best practices, 401
cold recovery sites, 403-404
cold spares
cold swapping and, 402
warm swaps, 403
differential backups, 398-400
full backups, 398, 400
hot recovery sites, 403-404
hot spares, hot swapping and, 401-402
incremental backups, 399-400
tape rotations, 400
warm recovery sites, 404
disk duplexing (RAID 1), 387, 390
disk mirroring (RAID 1), 386-387
disk striping with parity (RAID 5), 387, 389
distance-vector routing, 123-124
distributed networks, 14
distributed parity (RAID 5), 387, 389
DMZ (perimeter networks), 466-467
DNS (Domain Name Service), 74-75
AAAA records, 79
CNAME records, 79
DDNS, 76
DNS namespace, 76-78
arpa top-level domain name, 78
com top-level domain name, 77
de top-level domain name, 78
ded top-level domain name, 77
edu top-level domain name, 77
FQDN, 77
gov top-level domain name, 77
mil top-level domain name, 78
net top-level domain name, 77
org top-level domain name, 77
entries, types of, 78
IP address-to-hostname resolution, 78
MX records, 79
name resolution, 75
NS records, 79
practical implementation of, 79
PTR records, 78-79
resolvers (DNS clients) and, 75
reverse lookups, 78
SOA records, 79
suffixes, 90
troubleshooting, 490
DNS servers, 160
IP addressing, 108
load balancing, 155
TCP/IP client configurations, 301
documentation (administration), 303-305
advantages of, 304
applications, 306
baselines, 313-314
configuration documentation, 317
logical network diagrams, 310-313
network hardware, 306
network procedures, 306
network services, 306
network topologies, 305
physical diagrams, 310
physical network diagrams, 310-311
policies, 314-315
email usage policies, 314
Internet usage policies, 314
network usage policies, 314
ownership policies, 315
personal software policies, 315
user account policies, 315
procedures, 315
backup procedures, 316
network monitoring procedures, 316
new user procedures, 316
remote-access procedures, 316
reporting security violations, 316
security procedures, 316
software procedures, 316
regulations, 317-318
server configurations, 306
statistics, capturing, 313
updating, 312
wiring layouts, 306-310
documenting findings (troubleshooting procedures), 482
DoS (denial of service) attacks, 452-454
double colons (::), IPv6 addressing, 104
downtime (networks), 383-384
drivers
DSL Internet access, troubleshooting, 194
NIC installations, 144
DSL Internet access, 192
ADSL, 192-193
broadband security, 197
dedicated local bandwidth, 196
HDSL, 192-193
IDSL, 192-193
LED, troubleshooting, 194
RADSL, 192-193
SDSL, 192-193
speed comparison table, 193
troubleshooting
drivers, 194
DSL LED, 194
NIC, 194
physical connections, 194
protocol configuration, 194
VHDSL, 192-193
VPN and, 34
DSSS (Direct-Sequence Spread-Spectrum) technology, 274, 287
DTE (data terminal equipment), Frame Relay WAN, 184
DTIM periods, configuring wireless connections, 282
DUAL (Diffusing Update Algorithm), 124
duplexes, troubleshooting client configurations, 502
duplexing (disk), RAID 1, 387, 390
duplicate IP addresses, troubleshooting, 489
DWDM (dense wavelength division multiplexing), 183
dynamic addressing, 107-109
dynamic routing, TCP/IP routing, 123
distance-vector routing, 123-124
link-state routing, 126
EAP (Extensible Authentication Protocol), 292, 441
eavesdropping attacks, 454
echo. See open impedance mismatch (echo)
EDFA (erbium doped fiber amplifiers), 183
edu top-level domain name (DNS namespace), 77
EGP (Exterior Gateway Protocols), 127
EIA/TIA (Electronic Industries Association/Telecommunications Industry Association) twisted-pair cabling, 216
EIGRP (Enhanced Interior Gateway Routing Protocol), distance-vector routing, 124
e-mail
addresses, exam scheduling requirements, 5
broadband security, 197
NNTP, 66
secure email, PKI and, 439
SMTP and, 60
usage policies, 314
vetting, 457

EMI (electromagnetic interference), 213, 492-493

encryption
asymmetric key encryption, 437
encryption devices, 150
PKI, 436
asymmetric key encryption, 437
CA, 436
certificate templates, 436
certificates, 436
confidentiality, 438
CRL, 436
digital certificates, 439
digital signatures, 438
private key encryption, 437
public key encryption, 437
secure email, 439
symmetric key encryption, 437
uses of, 438
web security, 438
presentation layer (layer 6), OSI
seven-layer networking model, 48
private key encryption, 437
public key encryption, 437
SNMPv3, 86
symmetric key encryption, 437
TKIP, 292
VPN, 34
WPA, 292

environmental monitors, 341

error checking, transport layer (layer 4), 47

error messages
Destination host unreachable error messages, 356
Expired TTL error messages, 358
Request timed out error messages, 357-358
Unknown host error messages, 358

escalation, determining (troubleshooting procedures), 480-481

ESD (electrostatic discharges), 143

ESP protocol (Encapsulating Security Payloads protocol), IPSec, 417

ESS (Extended Service Sets), 262, 276

ESSID (Extended Service Set Identifiers), 262

Ethernet
10BaseT LAN standard, 249-250
100BaseFX LAN standard, 250-251
100BaseTX LAN standard, 250-251
1000BaseCX LAN standard, 252
1000BaseLX LAN standard, 252
1000BaseSX LAN standard, 252
1000BaseT LAN standard, 253
1000BaseX LAN standards, 251-252
Fast Ethernet standards, 250-251
Gigabit Ethernet standards, 251-252
10 Gigabit Ethernet standards, 253
10GBaseER/EW Gigabit Ethernet standard, 254
10GBaseLR/LW Gigabit Ethernet standard, 254
10GBaseSR/SW Gigabit Ethernet standard, 253-254
10GBaseT Gigabit Ethernet standard, 255

PoE, 129
PPPoE, 423
STP, 130
switches, 146
switching loops, 130

Ethernet networks
troubleshooting, switching loops, 486
wireless AP, 149
EUI-64, 137

event logs, 331
  application logs, 333, 335
  history logs, 334-335
  LM, 335
  security logs, 332, 335
  syslog, 334
  system logs, 334-335
evil twin attacks, 455

Exam Alerts, Network+ exam cram, 1
Exam Tips and Notes sections (Network+ exam cram), 6

exams
  Network+ exam
    allotted test time, 2
    answer formats, 5
    CompTIA contact information, 6
    determining success, 6
    exam day recommendations, 5-6
    exam day rules, 6
    expectations for, 5
    format of, 2
    objectives, 2-4, 7
    passing, 6
    question formats, 5
    receiving certification, 6
    scheduling, 4
    strategies for taking, 6-7
  objectives, 2
  practice exams
    exam 1 answers, 537-559
    exam 1 questions, 513-535
    exam 2 answers, 585-606
    exam 2 questions, 561-584
    scheduling, 4
    strategies for taking, 6-7
    allotted test time, 2
  subobjectives, 2-4
  Sylvan Prometric testing service, scheduling exams, 4
  VUE testing service, scheduling exams, 4
expiration dates, passwords, 432
Expired TTL error messages, 358

F

F-Type connectors, 223
failover configurations, fault tolerance in standby servers, 391
failovers, clustering, 392
failures (networks)
  costs of, 382-383
  hardware, 384-385
Fast Ethernet standards, 250-251
fault detection, 323
fault tolerance, 382-384
  adapter teaming, 392-393
  CARP, 393
  hard disks, 385
  link redundancy, 392-393
  mesh topologies, 21
  primary function of, 385
  RAID, 384
  RAID 0, 386, 390
  RAID 1, 386-387, 390
  RAID 5, 387-390
  RAID 10, 389-390
  servers
    clustering, 391-392
    standby servers, 390
  UPS, 393-394
FDM (Frequency Division Multiplexing), 211
FEXT (Far End Crosstalk), troubleshooting, 493. See also crosstalk
FHSS (Frequency-Hopping Spread-Spectrum) technology, 273, 287
fiber connectors, 224

fiber-optic cable, 213-215, 219-221

filtering

  client requests via proxy servers, 157
  client-side filters, 155
  content filters, 155, 461
  MAC filtering, 425-426
  packet-filtering
    implicit denies, 464
    IP addresses, 463
    MAC addresses, 464
    port numbers, 463
    protocol identification, 464
  packet-filtering firewalls, 463-465
  server-side filters, 155
  TCP/IP filtering, 426
  URL, firewalls and, 462

findings, documenting (troubleshooting procedures), 482

firewalls, 139, 160, 460-461, 466

  application layer firewalls, 465-466
  bandwidth management, 462
  circuit-level firewalls, 465-466
  content filtering, 461
  features of, 461-462
  hardware firewalls, 140
  NAT, 462
  packet-filtering firewalls, 463-465
  security, 197
  signature identification, 461
  stateful firewalls, 462-463
  stateless firewalls, 462-463
  URL filtering, 462
  virus scanning, 461

flow control (data)

  buffering, 47
  transport layer (layer 4), OSI seven-layer networking model, 47
  windowing, 47

forwarding ports, BPDU messages, 131

fox and hound. See toner probes

FQDN (fully qualified domain names), DNS namespace, 77

fractional T (T-carrier lines), 180

Fraggle attacks, 453

FragmentFree switching environments, 148

Frame Relay

  DCE, 185
  DTE, 184
  PVC, 184-185
  SVC, 185
  WAN configurations, 184-187

frequency hopping, 273

FTP (File Transfer Protocol), 57, 69, 442

  ascii command, 58
  binary command, 58
  bounce attacks, 455
  cd command, 58
  CuteFTP, 57
  get command, 58
  lcd command, 58
  ls command, 58
  mget command, 58
  mput command, 58
  put command, 58
  SmartFTP, 57

full backups, 398, 400

full system functionality, verifying (troubleshooting procedures), 481

full-duplex configuration mode (switches), 147

full-duplex mode cabling, 212
gain values (antennas), 265

Gateways, 159

TCP/IP client configurations, 500

troubleshooting, 489

Get command, 58

GFS backup rotations, 400

Gigabit Ethernet standards, 251-252

10 Gigabit Ethernet standard, 253

10GBaseER/EW Gigabit Ethernet standard, 254

10GBaseLR/LW Gigabit Ethernet standard, 254

10GBaseSR/SW Gigabit Ethernet standard, 253-254

10GBaseT Gigabit Ethernet standard, 255

global unicast addresses, 105

gov top-level domain name (DNS namespace), 77

graphics files, presentation layer (layer 6), 48

Half-duplex configuration mode (switches), 147

Half-duplex mode cabling, 212

Hard disks, 385

Hardware

documentation (administration), 306

failures, 384-385

firewalls, 140

troubleshooting, 496-497

HDSL (High Bit Rate DSL) Internet access, 192-193

Heartbeats, 391

Help

CompTIA contact information, 6

technical support, troubleshooting
cable Internet access, 196

HIDS (host-based intrusion detection systems), 468

Hierarchical name trees, 85

High-density devices, 141

History logs, 334-335

HomePlug Powerline Alliance, broadband transmissions, 212

Honeynets, 470

Honeypots, 469-470

Hop counts, 127

Horizontal cabling, 231-232

Horizontal cross-connects, 232

Host command, 351, 376

HOSTS files, 74-75

Hot recovery sites (disaster recovery), 403-404

Hot spots (disaster recovery), hot swapping and, 401-402

Hotspots, 203

HSPA+ (High Speed Packet Access), 3G, 204

HTTP (Hypertext Transfer Protocol), 60, 70, 442

HTTPS (Hypertext Transfer Protocol Secure), 60, 70, 438, 442

Hubs, 159

defining, 140

MDI ports, 148

MDI-X ports, 148

OSI seven-layer networking model, mapping to, 50

Star topologies, 19, 505

Switch and hub cabling, 148

troubleshooting, 496, 505

Workgroup hubs, 141

HVAC, 342

Hybrid home networks, IEEE 1905, 212

Hybrid mesh topologies, 21

Hybrid topologies, 27

Hz (Hertz), RF channels, 268
I/O addresses, memory, 142, 144
IANA (Internet Assigned Numbers Authority), assigning IP addresses to public networks, 98
IBSS (Independent Basic Service Sets). See ad hoc mode
ICMP (Internet Control Message Protocol), 63, 70
   flood attacks, 362, 454
   source quench, 63
IDC (insulation displacement connectors), 235
identifying the problem (troubleshooting procedures), 477-478
IDF (Intermediate Distribution Frame) telecommunications rooms, 236
IDS (intrusion detection systems), 468-469
IDs (photo), exam day requirements, 6
IDSL (ISDN DSL), Internet access, 192-193
IEEE (Institute of Electrical and Electronics Engineers)
   802.11 wireless standards, 284, 286-287
   802.11a wireless standard, 268, 271, 285-286
   802.11b wireless standard, 285-286
   802.11b/g wireless standard, 269-270
   802.11g wireless standard, 285, 287
   802.11i wireless standard, 293
   802.11n wireless standard, 270, 285-287
   802.1X wireless standard, 294-295
   802.1Q specification, VLAN and, 36
   IEEE 802 networking standards, 244-245
   IEEE 802.2 standard, 245
   IEEE 802.3 standard
   10 Gigabit Ethernet standards, 253-255
   10BaseT LAN standard, 249-250
   100BaseFX LAN standard, 250-251
   100BaseT LAN standard, 253
   100BaseTX LAN standard, 250-251
   100BaseX LAN standard, 251-252
   access methods, 246-248
   bonding, 248
   CSMA/CA access method, 248
   CSMA/CD access method, 246-248
   media, 249
   speed, 245-246
   topologies, 249
MAC address assignments, 110
WEP, 290
wireless device communication, 277-278
IEEE 1901, 212
IEEE 1905, 212
IETF (Internet Engineer Task Force), RFC, 54
ifconfig command, 269, 351, 372-373
IGMP (Internet Group Management Protocol), 67, 70
IGP (Interior Gateway Protocols), 127
IMAP4 (Internet Message Protocol – version 4), 61, 70
implicit denies, packet-filtering, 464
incremental backups, 399-400
independent routing, 176
infrared wireless networking, 274-275
infrastructure hardware, troubleshooting, 496-497
infrastructure wireless topologies, 22
   AP and, 23, 261
   LAN and, 22
installing

ESD, precautions against, 143
NIC, 143
  built-in network interfaces, 144
drivers, 144
IRQ, 142, 144
media compatibility, 142
memory I/O addresses, 142, 144
slot availability, 144
software configuration utilities, 144
  system bus compatibility, 142
wiring installation, verifying, 239-240

interference, 212-213
  antennas (wireless), 267
crosstalk, 213
DSSS and, 274
wireless networks, 300-301
wiring
  attenuation, 493
crosstalk, 492-493
EMI, 213, 492-493
FEXT, 493
NEXT, 492
open impedance mismatch (echo), 494

intermediate cross-connects, 232

Internet access
  broadband access, 191, 197
cable Internet access, 195
  broadband security, 197
cabling, 195
modems, 195-196
shared bandwidth, 196
troubleshooting, 196-197
UTP cable, 195
  cellular Internet access, 204
  DSL Internet access, 192
    ADSL, 192-193
    broadband security, 197
dedicated local bandwidth, 196
HDSL, 192-193
RADSL, 192-193
SDSL, 192-193
  speed comparison table, 193
troubleshooting, 194
VHDSL, 192-193
IDS Internet access, 192-193
POTS Internet access, 198-200
PSTN Internet access, 200
satellite Internet access, 201
  hotspots, 203
  latency, 201-202
  one-way satellite systems, 191, 201
  propagation time, 202
troubleshooting, 202
two-way satellite systems, 191, 201
WISP, 203

Internet server providers. See ISPs

Internet usage policies, 314

IP (Internet Protocol), 55, 69, 106
IP address-to-hostname resolution,
  DNS and, 78
IP addresses
  duplicate IP addresses, troubleshooting, 489
  packet-filtering, 463
  scopes, 88
  TCP/IP client configurations, 499, 501
ipconfig command, 269, 351, 370-372
IPS (intrusion prevention systems), 468
IPSec (Internet Protocol Security), 417-418
IPv4 addressing, 95, 102
  address classes, 95-96
  addressing schemes, 103
  APIPA, 109-110
  autoconfigured addressing, 106
  BOOTP, 109
  broadcast addresses, 102
  CIDR, 100
  default gateways, 100-102
  DHCP servers, 139
  dynamic addressing, 107-109
  IPv6 comparisons to, 106-107
  loopback addressing, 106
  MAC addresses, identifying, 110-111
  multicasting, 105
  NAT, 112-113
  network-wide addressing, 106
  octets, 138
  PAT, 113
  private network addressing, 106
  site-local addresses, 105
  static addressing, 107
  unicast addresses, 105

IPv6 addressing, 95, 103
  anycast addresses, 106
  APIPA, 109-110
  autoconfigured addressing, 106
  BOOTP, 109
  DHCP servers, 139
  double colons (::), 104
  dynamic addressing, 107-109
  EUI-64, 137
  global unicast addresses, 105
  identifying, 103-104
  IPv4 comparisons to, 106-107
  link-local addresses, 105
  loopback addressing, 106
  MAC addresses, identifying, 110-111
  multicasting, 105
  NAT, 112-113
  network-wide addressing, 106
  octets, 138
  PAT, 113
  private network addressing, 106
  site-local addresses, 105
  static addressing, 107
  unicast addresses, 105

IrDA (Infrared Data Association), 274
IRQ (Interrupt Requests), NIC installations, 142, 144
IS-IS (Intermediate System-to-Intermediate System), link-state routing, 126
ISAKMP (Internet Security Association and Key Management Protocol), 415, 442
ISDN (Integrated Services Digital Networks)
  BRI, 179
  PRI, 179
  VPN and, 34
  WAN configurations, 178-179, 187
ISO (International Organization for Standardization), OSI seven-layer model, 43
ISP (Internet service providers)
  POTS Internet access, troubleshooting, 199
  SOHO network configurations, 172
iwconfig command, troubleshooting wireless networks, 269

J
  jam signals, 247
  jumpers, 144
Kerberos authentication, 433-436
key and lock (physical security), 443-444
knowledge assessments, exam questions as, 7

L
L2TP (Layer 2 Tunneling Protocol), 34, 416
labeling tables, backup strategies, 401
LAN (local area networks), 10
   Ethernet LAN, wireless AP, 149
   IEEE 802 networking standards, 244-245
      IEEE 802.2 standard, 245
      IEEE 802.3 standard, 245-255
infrastructure wireless topologies, 22
LAN-to-LAN internetworking, VPN and, 33
   PAT and, 113
   VLAN, troubleshooting, 503-504
   WLAN
      security, 289
      wireless AP, 149
LAN-to-LAN internetworking, VPN and, 33
latency
   routing, 127
   satellite Internet access, 201-202
latency-insensitive applications, QoS and, 408
latency-sensitive applications, QoS and, 407
Layer 3 addresses, 37
Layer 3 switches. See multilayer switches
lcd command, 58
LDAP (Lightweight Directory Access Protocol), 66, 70
learning bridges, 137
learning ports, BPDU messages, 131
least privilege concept (network security), 421
line of sight, troubleshooting satellite Internet access, 202
line-of-sight (directed) infrared wireless networking, 275
Link (Network Access) layer (TCP/IP four-layer networking model), 50
link aggregation, 131, 393
link lights (NIC), 143
link redundancy, 392-393
link-local addresses, 105
link-state routing, 126
listening ports, BPDU messages, 131
LLC (Logical Link Control) layer (data link layer (level 2), 46. See also IEEE 802.2 standard
LM (Log Management), 335
LMHOSTS files, 80
load balancers, 155, 160
   adapter teaming, 393
   clustering, 391
   content servers, 156
   DNS servers, 155
   multilayer switches, 155
load testing, 330
lock and key (physical security), 443-444
logical network diagrams, 310-313
logical topologies
   defining, 16
   logical ring topologies, 18
longitudinal separators, 217
loopback addresses, IP addressing, 106
loopback cabling, 231
loopback feature (smart jacks), 238
loopbacks, 359
loops
  avoiding, 131
  bridging loops, eliminating, 137
  routing loops, 125, 486
  switching loops, 130, 486
ls command, 58
LSA (link state advertisements), 126
LTE (Long Term Evolution), 4G, 204

M
MAC (mandatory access control), 419
MAC (Media Access Control) layer
  (data link layer (level 2)), 46
MAC address-based VLAN memberships, 37-38
MAC addresses
  assigning, 110
  bridges, 137
  identifying, 110-111
  NIC, viewing MAC addresses of, 111
  packet-filtering, 464
  switches, 146
MAC filtering, 425-426
macro viruses, 451
mailing addresses, exam scheduling requirements, 4
main cross-connects. See vertical (main) cross-connects
maintenance, 324
malware
  Trojan horses, 451-452
  viruses, 450-452
  antivirus software, 456-457
  scanning for, 456-457, 461
  worms, 451-452
MAN (metropolitan area networks),
  fiber-optic cable, 215. See also WAN (wide area networks)
man-in-the-middle attacks, 416, 455
managed wireless topologies. See infrastructure wireless topologies
managers (SNMP), 83
MD-IDS (misuse-detection intrusion detection systems), 468
MDF (Main Distribution Frame) telecommunications rooms, 236
MDI ports, 148
MDI-X ports, 148, 195
media connections, troubleshooting, 498-501
media connectors
  BNC connectors, 221
  F-Type connectors, 223
  fiber connectors, 224
  RG-6 connectors, 223
  RG-59 connectors, 223
  RJ-11 connectors, 222
  RJ-45 connectors, 223
  RS-232 standard connectors, 225
  Type A connectors, 226
  Type B connectors, 226
  USB connectors, 226
media converters, 141-142, 159, 226-227
media interference, 212-213
media testers, 344
memberships, VLAN, 37-38
memory I/O addresses, NIC installations, 142, 144
mesh topologies, 20
  advantages/disadvantages of, 21
  fault tolerance, 21
  hybrid mesh topologies, 21
  MPLS, 21-22
  redundancy, 20
  troubleshooting, 506
  wireless mesh networks, 25-27
mget command, 58
MIB (Management Information Bases), 85
mil top-level domain name (DNS namespace), 78
MIMO antennas, 285
mirrored stripe sets (RAID 10), 389
mirroring (disk), RAID 1, 386-387
mirroring (ports), 132
mismatched MTU/MUT black holes, troubleshooting, 487-488
missing/bad routes, troubleshooting, 488
modems, 142, 159
  analog modems, VPN and, 34
  broadband modems, 191
  cable Internet access, 195-196
  MDI-X ports, 195
  POTS Internet access, troubleshooting, 199-200
  SOHO networks, 171
modules, troubleshooting, 488
MPLS (Multiprotocol Label Switching), 21-22
mput command, 58
MS-CHAP, 440
MS-CHAPv2, 441
MSAU (multistation access units), ring topologies, 18
MTU (Maximum Transmission Units), 127, 487-488
multicasting, 102
  IGMP, 67
  IPv6 addressing, 105
multifactor authentication, 445
multifunction devices, 160
multilayer switches, 160
  load balancing, 155
  OSI model, 156
multimeters, 345-346
multimode fiber-optic cable, 220
multiplexing
  DWDM, 183
  FDM, 211
OFDM, 274, 287
TDM, 211
WD-PON, 183
multiport bridges. See switches
MX (Mail Exchange) records, reverse lookups, 79

N
NaaS (Network as a Service), 165
NAC (Network Access Control), 423
name resolution
  DNS and, 75
  NetBIOS, 80
narrowband transmissions, RF channels and, 273
NAT (Network Address Translation), 112
  firewalls and, 462
  SNAT, 113
nbtstat command, 351, 369-370
net top-level domain name (DNS namespace), 77
NetBIOS (Network Basic Input/Output System), name resolution, 80
netstat command, 351, 363-364
  netstat –a command, 366
  netstat –e command, 365
  netstat –r command, 367
  netstat –s command, 368-369
Network Access (Link) layer (TCP/IP four-layer networking model), 50
network cards. See NIC
Network Interface layer (TCP/IP four-layer networking model), 50
network layer (layer 3), OSI seven-layer networking model, 46, 49
network usage policies, 314
Network+ exam
  allotted test time, 2
  answers, format of, 5
certification, receiving, 6
CompTIA contact information, 6
exam day recommendations, 5-6
exam day requirements, 6
exam day rules, 6
expectations for, 5
format of, 2
objectives, 2
reviewing (test-taking strategies), 7
subobjectives, 2-4
passing, 6
questions
format of, 5
knowledge assessments, 7
scheduling, 4
strategies for taking, 6-7
success, determining, 6

Network+ exam cram
Cram Sheet, 1, 5
Exam Alerts, 1
Exam Tips and Notes sections, 6
organization of, 1, 5

network-wide addresses, IP addressing, 106

networking models
OSI seven-layer model, 43-44
application layer (layer 7), 48-49
data link layer (layer 2), 46, 49
mapping network devices to, 50
network layer (layer 3), 46, 49
physical layer (layer 1), 45, 49
presentation layer (layer 6), 48-49
session layer (layer 5), 47, 49
summary of, 49
TCP/IP four-layer networking model comparisons, 49-50
transport layer (layer 4), 47, 49

TCP/IP four-layer model, 43
Application layer, 50
Network Access (Link) layer, 50
Network Interface layer, 50
OSI seven-layer model comparisons, 49-50
Transport layer, 50

networks
ad hoc wireless networks, 11
administration
command-line utilities, 351-376
documentation, 303-318
network configuration, 324
network maintenance, 324
network management tools, 323
performance monitoring, 322-335
remote management, 324
security monitoring, 324
tools, 338-347
applications, documentation, 306
baselines, 313-314
centralized computing networks, 14
client/server networks, 13-14
coxial networks, connecting to, 498
command-line utilities
arp command, 351, 360-361
arp ping command, 351, 362-363
dig command, 351, 375-376
host command, 351, 376
ifconfig command, 351, 369-370
ipconfig command, 351, 370-372
nbtstat command, 351, 369-370
netstat command, 351, 363-369
nslookup command, 351, 373-374
ping command, 351, 355-360
route command, 351, 376
traceroute command, 351-355
tracert command, 351-355
configuring, 324
demarcation points, 237-238
distributed networks, 14
downtime, 383-384
Ethernet networks, 486
failures
  costs of, 382-383
  hardware, 384-385
hardware, documentation, 306
hybrid home networks, IEEE 1905, 212
ISDN
  BRI, 179
  PRI, 179
  WAN configurations, 178-179, 187
LAN, 10
  IEEE 802.11 networking standards, 244-255
  infrastructure wireless topologies, 22
  LAN-to-LAN internetworking, 33
  PAT and, 113
  VLAN, 503-504
  WLAN, security, 289
logical network diagrams, 310, 312-313
maintenance, 324
MAN, fiber-optic cable, 215. See also WAN
management tools, fault detection, 323
monitoring procedures, 316
network qualification testers, 346
optimization
  caching engines, 409-410
  costs of failure, 382-383
  disaster recovery, 397-404
downtime, 383-384
  fault tolerance, 382-394
hardware failures, 384-385
QoS, 407-408
  traffic shaping, 408-409
peer-to-peer networks, 12-14
performance monitoring, 322-323
  application logs, 333, 335
  event logs, 331-335
  history logs, 334-335
LM, 335
load testing, 330
packet sniffers, 324-325
performance tests, 329-330
port scanners, 327-329
security logs, 332, 335
stress tests, 330
syslog, 334
system logs, 334
systems logs, 335
throughput testing, 325, 327
perimeter networks. See DMZ
physical network diagrams, 310-311
  policies, 314-315
PON, 183
private IPv4 networks, 98-99
procedures, 315-316
  documentation (administration), 306
PSTN Internet access, 200
PtMP networks, 25
PtP networks, 24
public IPv4 networks, 98
remote management, 324
security
  access control, 418-421, 425-426
  accounting, 431, 439-440
  antivirus software, 456-457
  auditing events, 431
  authentication, 429-436, 439-441, 445
authorization, 429-430, 439-440
back door attacks, 455
biometrics, 445
CHAP, 441
Citrix ICA, 425
DMZ (perimeter networks), 466-467
DoS attacks, 452-454
EAP, 441
eavesdropping attacks, 454
encryption, 436-439
evil twin attacks, 455
firewalls, 460-466
FTP bounce attacks, 455
honeynets, 470
honeypots, 469-470
IDS, 468-469
IPS, 468
ISAKMP, 415
Kerberos authentication, 433-436
least privilege concept, 421
lock and key, 443-444
MAC filtering, 425-426
man-in-the-middle attacks, 416, 455
MS-CHAP, 440
MS-CHAPv2, 441
multifactor authentication, 445
NAC, 423
PAP, 441
password attacks, 454
passwords, 432-433
patches, 457
phishing attacks, 456
physical security, 443-445
PIN pads, 444-445
PKI, 436-439
posture assessments, 424
PPP, 422
PPPoE, 423
preventing attacks, 456-457
privileges, 421
RADIUS, 439-440
RAS, 421
RDP, 424
remote-access protocols, 421-423
remote-control protocols, 424
rogue AP, 455
secured versus unsecured protocols table, 442
social engineering attacks, 454
spoofing attacks, 455
SSH, 424
swipe cards, 444-445
TACACSp, 440
TCP/IP filtering, 426
Trojan horses, 451-452
tunneling, 415-418
two-factor authentication, 445
updating, 457
viruses, 450-452, 456-457, 461
VPN, 414
VPN concentrators, 469
vulnerability scanners, 470
war chalking, 455-456
war driving, 455
WEP cracking, 455
wireless networks, 455-456
worms, 451-452
WPA cracking, 455
security monitoring, 324
self-healing networks, 27
services, documentation, 306
SOHO networks, 168
configuring, 169
Internet service providers and, 172
modems, 171
point of demarcation, 172-173
routing, 169, 173
wiring, 169, 171
token ring networks, 246
tools, 338
  butt sets, 346
cable certifiers, 344
environmental monitors, 341
media testers, 344
multimeters, 345-346
network qualification testers, 346
optical cable testers, 345
OTDR, 345
protocol analyzers, 343-344
punchdown tools, 340
snips, 339
stripers, 339
TDR, 344
toner probes, 342-343
voltage event recorders, 340
Wi-Fi detectors, 347
wire crimpers, 339
topologies
  convergence, 125
documentation (administration), 305
mesh topologies, 506
star topologies, 505-506
troubleshooting, 504-506
troubleshooting
  black holes, 487-488
  broadcast storms, 487
  DNS, 490
duplicate IP addresses, 489
  gateways, 489
  ipconfig command, 371
  mismatched MTU/MUT black holes, 487-488
  missing/bad routes, 488
modules, 488
ping command, 359-360
port configuration, 487
power failures, 488
proxy ARP, 486
routing loops, 486
routing problems, 486
subnet masks, 489
switching loops, 486
twisted-pair networks, connecting to, 499
VLAN, 35-36
  802.1Q IEEE specification, 36
  administration, 36
  advantages/disadvantages of, 36
  MAC address-based VLAN memberships, 37-38
  memberships, 37-38
  organization, 36
  performance, 36
  port-based VLAN memberships, 37
  protocol-based VLAN memberships, 37
  security, 36
  segmentation, 38
  troubleshooting, 503-504
VPN, 32, 414
  access methods, 34
  advantages/disadvantages of, 34-35
  analog modems and, 34
  cable connections and, 34
  clients, 34
  components of connections, 33-34
  cost, 34
  dedicated broadband connections and, 34
  DSL connections and, 34
  encryption, 34
ISDN and, 34
L2TP and, 34
LAN-to-LAN internetworking, 33
PPTP, 34, 415
reliability, 35
remote access, 33
scalability, 35
security, 35
servers, 34
VPN concentrators, 469
wireless connections and, 34
WAN, 11, 175-176. See also MAN
ATM, 186-187
circuit switching, 177-178
Frame Relay, 184-185, 187
ISDN, 178-179, 187
packet switching, 176-177
PSTN Internet access, 200
SONET, 182-183, 187
T-carrier lines, 180-181, 187
X.25, 183-184, 187
wireless mesh networks, 25-27
wireless networks, 259
802.11 wireless standards, 284, 286-287
802.11a wireless standard, 271, 285-286
802.11b wireless standard, 285-286
802.11b/g wireless standard (IEEE), 269-270
802.11g wireless standard, 285, 287
802.11n wireless standard, 270, 285-287
antennas, 263-268, 279, 285, 299
AP, 259-264, 272, 276-277
beacons, 272-273
BSA, 263
BSS, 262
BSSID, 262
configuring connections, 278, 281-282
data rates, 271-272
ESS, 262
ESSID, 262
establishing communication between wireless devices, 275-278, 298-300
infrared wireless networking, 274-275
infrastructure wireless networks, 261
interference, 300-301
OFDM, 274, 287
repeaters, 264
RF channels, 268-271, 273, 277, 281, 299
security, 262, 290-295
spread spectrum technology, 273-274, 287
SSID, 262, 272, 277-278, 281, 300
throughput, 271-272
time stamps, 272
troubleshooting, 298-300
war chalking, 455-456
war driving, 455
WEP cracking, 455
WLAN, 260-261
WPA cracking, 455
WLAN security, 289
WPAN, 11
new user procedures, 316
newsgroups, NNTP, 66
NEXT (Near End Crosstalk), troubleshooting, 492. See also crosstalk
NIC (network interface cards), 142, 159
activity lights, 143
DSL Internet access, troubleshooting, 194
installing, 143
built-in network interfaces, 144
drivers, 144
IRQ, 142, 144
media compatibility, 142
memory I/O addresses, 142, 144
slot availability, 144
software configuration utilities, 144
system bus compatibility, 142
link lights, 143
MAC addresses, viewing, 111
OSI seven-layer networking model, mapping to, 50
speed lights, 143
NID (Network Interface Devices). See smart jacks
NIDS (network-based intrusion detection systems), 468
NMS (Network Management System), 83
NNTP (Network News Transport Protocol), 66, 70
nodes, defining, 246
nonoverlapping channels (wireless), 268-269
nonoverwriting viruses, 451
NS (Name Server) records, 79
nslookup command, 351, 373-374
NTP (Network Time Protocol), 65-66, 70

objectives (Network+ exam), 2
reviewing (test-taking strategies), 7
subobjectives, 2-4
octets (IP addressing), 95, 138
OCx (Optical Carrier) levels
SONET, 182, 187
transmission rates table, 182
OFDM (Orthogonal Frequency Division Multiplexing), 274, 287
office space, disaster recovery, 404
offsite datacenters, onsite datacenters versus, 164
offsite storage, backup strategies, 401
OLT (optical line termination), PON, 183
omnidirectional antennas, 265-266
one-way satellite systems, 191, 201
onsite datacenter, offsite datacenters versus, 164
ONU (optical network units), PON, 183
open authentication (wireless device communication), 277
open impedance mismatch (echo), troubleshooting, 494
open/short faults, troubleshooting, 494
OpenStack open source project, 165
optical cable testers, 345
optimization
caching engines, 409-410
disaster recovery, 397
best practices, 401
cold recovery sites, 403-404
cold spares, 402
cold swapping, 402
differential backups, 398-400
full backups, 398, 400
hot recovery sites, 403-404
hot spares, 401-402
hot swapping, 401-402
incremental backups, 399-400
tape rotations, 400
warm recovery sites, 404
warp swaps, 403
downtime, 383-384
failures
costs of, 382-383
hardware, 384-385
fault tolerance, 382-384
adapter teaming, 392-393
CARP, 393
hard disks, 385
link redundancy, 392-393
primary function of, 385
RAID, 384
RAID 0, 386, 390
RAID 1, 386-387, 390
RAID 5, 387-390
RAID 10, 389-390
server clustering, 391-392
standby servers, 390
UPS, 393-394
QoS, 407-408
traffic shaping, 408-409
org top-level domain name (DNS namespace), 77
organizing
  Network+ exam cram, organization of, 1, 5
  Network+ exam format, 2
  VLAN, 36
OSI (Open Systems Interconnect) seven-layer networking model, 43-44
  application layer (layer 7), 48-49
  bridges, 141
data link layer (layer 2), 46, 49
  Layer 3 addresses, 37
  multilayer switches, 156
  network devices, mapping to OSI model, 50
  network layer (layer 3), 46, 49
  physical layer (layer 1), 45, 49
  presentation layer (layer 6), 48-49
  session layer (layer 5), 47, 49
  summary of, 49
  switches, 148
  TCP/IP four-layer networking model comparisons, 49-50
  transport layer (layer 4), 47-49
  wireless AP, 150
OSPF (Open Shortest Path First)
  link-state routing, 126
  network layer (layer 3), OSI seven-layer networking model, 46
OTDR (optical time domain reflectometers), 345
overlapping channels (wireless), troubleshooting, 269
overwriting viruses, 451
ownership policies, 315

P
packet sniffers, 324-325
packet switching
  ATM, 186-187
  datagram packet switching, 177
  Frame Relay, 184-187
  independent routing, 176
  virtual-circuit packet switching, 176-177
  WAN configurations, 176-177
  X.25, 183-184, 187
packet-filtering
  firewalls, 463-465
  implicit denies, 464
  IP addresses, 463
  MAC addresses, 464
  port numbers, 463
  protocol identification, 464
PAD (packet assembler/disassembler), 184
PAP, 441
passing exams, determining, 6
passive scanning (beacons), 272
passwords
attacks using, 454
expiration dates, 432
modems, troubleshooting POTS Internet access, 200
policies, 432
reusing, 432
strength of, 433
PAT (Port Address Translation), 113
patch panels, 234
patches (security), 457
PBX (private branch exchanges), virtual, 164
peer-to-peer networks, 12-14
performance
clustering, 391
VLAN, 36
performance monitoring, 322-323
event logs, 331
application logs, 333, 335
history logs, 334-335
LM, 335
security logs, 332, 335
syslog, 334
system logs, 334-335
load testing, 330
packet sniffers, 324-325
performance tests, 329-330
port scanners, 327-329
stress tests, 330
throughput testing, 325, 327
performance tests, 329-330
perimeter networks. See DMZ
permanent cable. See horizontal cabling
personal information, scheduling exams, 4
personal software policies, 315
phishing attacks, 456
phone numbers, exam scheduling requirements, 4
photo IDs, exam day requirements, 6
physical addresses. See MAC addresses
physical layer (layer 1), OSI seven-layer networking model, 45, 49
physical network diagrams, 310-311
physical security, adding to networks, 443
biometrics, 445
lock and key, 443-444
PIN pads, 444-445
swipe cards, 444-445
physical topologies
defining, 16
physical bus topologies, 17
PIDS (protocol-based intrusion detection systems), 469
PIN pads (physical security), 444-445
ping command, 351, 355-356
error messages
Destination host unreachable error messages, 356
Expired TTL error messages, 358
Request timed out error messages, 357-358
Unknown host error messages, 358
troubleshooting via, 359-360
ping floods, 454
ping of death attacks, 453
PKI (Public Key Infrastructure), 436
asymmetric key encryption, 437
CA, 436
certificate templates, 436
certificates, 436
confidentiality, 438
CRL, 436
digital certificates, 439
digital signatures, 438
private key encryption, 437
public key encryption, 437
secure email, 439
symmetric key encryption, 437
uses of, 438
web security, 438

plans of action, establishing (troubleshooting procedures), 479-480
plenum cable, 221
plugs. See loopback cabling
PoE (Power over Ethernet), 129
point of demarcation, SOHO networks, 172-173
poison reverses, 125
polarization (antennas), 267
policies, 314-315. See also regulations
polymorphic viruses, 450
PON (passive optical networks), 183
POP3 (Post Office Protocol – version 3), 61, 70
port numbers, packet-filtering, 463
port scanners, 327-329
port-based VLAN memberships, 37
ports
authentication, 132
blocked ports, BPDU messages, 131
client configurations, troubleshooting, 502
configuring, troubleshooting, 487
disabled ports, BPDU messages, 131
forwarding ports, BPDU messages, 131
hub ports, 148
learning ports, BPDU messages, 131
listening ports, BPDU messages, 131
MDI ports, 148
MDI-X ports, 148
mirroring, 132
straight-through cables, 148
switch ports, 148
TCP/UDP ports
assigning, 117-118
broadband security, 197

posture assessments, 424
POTS (plain old telephone system)
Internet access, 198
ADSL and, 192
troubleshooting, 198
dial tones, 199
ISP, 199
modems, 199-200
phone numbers, 199
physical connections, 199

power failures, troubleshooting, 488
PPP, 422
PPPoE (Point-to-Point Protocol over Ethernet), 423
PPTP (Point-to-Point Tunneling Protocol), 34, 415-416
practice exams
exam 1
answers, 537-559
questions, 513-535
exam 2
answers, 585-606
questions, 561-584

presentation layer (layer 6), OSI
seven-layer networking model, 48-49

preset connection time limits (modems), troubleshooting POTS
Internet access, 200
PRI (Primary Rate Interface), ISDN (Integrated Services Digital Networks), 179
primary server configurations, 391
printing, route print command, 364, 367, 377
priority queuing (QoS), 408
priority traffic shaping, 409
private IPv4 networks, 98-99
private key encryption, 437
private network addresses, IP
addressing, 106
privileges (network security), least
privilege, 421
probable cause (troubleshooting pro-
cedures)
  establishing theory of, 478
testing theory, 479
procedures, 315
  backup procedures, 316
documentation (administration), 306
  network monitoring procedures, 316
  new user procedures, 316
remote-access procedures, 316
security procedures, 316
software procedures, 316
violations (security), reporting, 316
propagation time, satellite Internet
access, 202
protocol-based VLAN memberships,
37
protocols, 53
  AH, IPSec and, 417
  APIDS, 469
  ARP, 63-65, 70
  BGP, distance-vector routing, 124
  BOOTP, 109
cable Internet access configurations,
troubleshooting, 196
CARP, 393
CCMP, 293
CHAP, 441
Citrix ICA, 425
connection-oriented protocols, 54-55
connectionless protocols, 54-55
DHCP, 88-89
  DNS suffixes, 90
dynamic addressing, 107
  process of, 89-90
  reservations, 89
DSL Internet access, troubleshooting,
194
EAP, 292, 441
EGP, 127
EIGRP, distance-vector routing, 124
ESP, IPSec and, 417
FTP, 57-58, 69, 442
HTTP, 60, 70, 442
HTTPS, 60, 70, 438, 442
ICMP, 63, 70
identifying, packet-filtering, 464
IGMP, 67, 70
IGP, 127
IMAP4, 61, 70
IP, 55, 69, 106
IPSec, 417-418
IS-IS, link-state routing, 126
ISAKMP, 415, 442
L2TP, 416
LDAP, 66, 70
MS-CHAP, 440
MS-CHAPv2, 441
NNTP, 66, 70
NTP, 65-66, 70
OSPF
  link-state routing, 126
  network layer (layer 3), OSI
  seven-layer networking model),
  46
PAP, 441
PIDS, 469
POP3, 61, 70
PPTP, 415-416
protocol analyzers, 343-344
RADIUS, 439-440
RARP, 65, 70
RCP, 442
RDP, 424
remote-access protocols, 421-423
remote-control protocols, 424
RIP
distance-vector routing, 124
network layer (layer 3), OSI
seven-layer networking model, 46
RIPv2, distance-vector routing, 124
RSH, 442
RTP, 68-69, 71
SCP, 66, 70, 442
secured versus unsecured protocols
table, 442
SFTP, 58-59, 69, 442
SIP, 68, 71
SMTP, 59-60, 70
SNMP, 82
agents, 84
communities, 85-86
components of, 83
management systems, 83-84
managers, 83
MIB, 85
SNMPv3, 86
trap managers, 84
SNMPv1, 442
SNMPv2, 442
SNMPv3, 442
SSH, 62, 70, 424, 442
SSL, 438
TACACS+, 440
TCP, 55-56, 69
ACK messages, 56
network layer (layer 3), OSI
seven-layer networking model, 47
SYN messages, 56
TCP three-way handshake, 56
Telnet, 62, 70, 442
TFTP, 59, 69
TKIP, 292
TLS, 67, 71, 438, 442
UDP, 56-57, 69
network layer (layer 3), OSI
seven-layer networking model, 47
RTP and, 68
VTP, 132
proxy ARP, troubleshooting, 486
proxy servers, 156, 160
ACL, 158
caching, 157
client requests, filtering, 157
PSTN (public switched telephone networks) Internet access, 200
PtMP (point-to-multipoint) networks, 25
PtP (point-to-point) networks, 24
PTR (Pointer) records, reverse lookups, 78-79
public IPv4 networks, 98
public key encryption, 435, 437
punchdown tools, 235, 340
put command, 58
PVC (permanent virtual circuits), Frame Relay connections, 184-185

QoS (Quality of Service), 407-408
questions
format of, Network+ exams, 5
knowledge assessments, 7
practice exam 1, 513-535
practice exam 2, 561-584
queueing (priority), QoS, 408
RADIUS, 439-440
RADSL (Rate-Adaptive DSL) Internet access, 192-193
RAID, 384
RAID 0, 386, 390
RAID 1, 386-387, 390
RAID 5, 387-390
RAID 10, 389-390
rain fade, 202
RARP (Reverse Address Resolution Protocol), 65, 70
RAS (Remote Access Service), 421
RBAC (rule-based access control), 420
RCP, 442
RDP (Remote Desktop Protocol), 424
reassociation (wireless device communication), 276
redundancy, mesh topologies, 20
redundant paths, avoiding, 131
regulations, 318. See also policies
reliability
VPN, 35
wireless mesh networks, 27
remote access
RADIUS, 439-440
TACACS+, 440
VPN, 33
remote administration, virtual desktops, 163
remote alarms (smart jacks), 238
remote authentication, 440-441
remote management, 324
remote-access procedures, 316
remote-access protocols, 421
NAC, 423
PPP, 422
PPPoE, 423
RAS, 421
remote-control protocols, 424
repeaters (wireless), AP and, 264
Request timed out error messages, 357-358
reservations, DHCP, 89
resident viruses, 450
resolvers (DNS clients), DNS and, 75
reusing passwords, 432
reverse lookups, DNS and, 78
RF amplifiers, AP and, 264
RF channels (wireless), 268, 270
802.11a wireless standard (IEEE), 271
802.11b/g wireless standard (IEEE), 269-270
802.11n wireless standard (IEEE), 270
frequency hopping, 273
narrowband transmissions, 273
nonoverlapping channels, 268-269
overlapping channels, 269
troubleshooting, 269, 299
wireless connections, configuring, 281
wireless device communication, 277
RF interference
antennas (wireless), 267
DSSS and, 274
wireless networks, 300-301
RFC (requests for comment), 54
RFC 768 (UDP), 56
RFC 791 (IP), 55
RFC 792 (ICMP), 63
RFC 793 (IP), 55
RFC 821 (SMTP), 59
RFC 826 (ARP), 63
RFC 854 (Telnet), 62
RFC 903 (RARP), 65
RFC 958 (NTP), 65
RFC 959 (FTP), 57
RFC 977 (NNTP), 66
RFC 1350 (TFTP), 59
RFC 1731 (IMAP4), 61
RFC 1939 (POP3), 61
RFC 2068 (HTTP), 60
RFC 2131 (DHCP), 88
RG-6 connectors, 223
RG-59 connectors, 223
ring topologies
advantages/disadvantages of, 18-19
logical ring topologies, 18
MSAU, 18
RIP (Routing Information Protocol)
distance-vector routing, 124
network layer (layer 3), OSI seven-layer networking model, 46
RIPv2 (Routing Information Protocol version 2), distance-vector routing, 124
risers, 491
RJ-11 connectors, 222
RJ-45 connectors, 223
RoBAC (role-based access control), 420-421
rollover cabling, 230
rouge AP (access points), 455
route command, 351
routing, 159
AP as routers, 149
bandwidth as routing metric, 127
broadband routers, 191
convergence, 125
costs, 127
distance-vector routing, 123-124
EGP, 127
hop counts, 127
IGP, 127
independent routing, 176
latency, 127
link-state routing, 126
loops, avoiding, 131
LSA, 126
mapping to OSI seven-layer networking model, 50
metrics, 127
missing/bad routes, troubleshooting, 488
MTU, 127
multilayer switches, 156
PoE, 129
poison reverses, 125
problems, troubleshooting, 486
redundant paths, avoiding, 131
route command, 376
route print command, 364, 367, 377
router operation, 145
routers, troubleshooting, 497
routing loops, 125, 486
SOHO networks, 169, 173
SOHO routers, 145
split horizons, 125
STP, 130
switching loops, 130
TCP/IP routing, 120
default gateways, 120
dynamic routing, 123-124, 126
routing tables, 121
static routing, 122
wireless connections, configuring, 278
wireless networks, troubleshooting, 299
RS-232 standard connectors, 225
RSH, 442
RTP (Real-time Transport Protocol), 68-71
S

-s command switch (ARP), 64
SaaS (Software as a Service), 165
sags (power), UPS and, 394
satellite Internet access, 201
  latency, 201-202
  one-way satellite systems, 191, 201
  propagation time, 202
  troubleshooting, 202
  two-way satellite systems, 191, 201
scalability
  clustering, 392
  VPN, 35
  wireless mesh networks, 27
scanning, vulnerability scanners, 470
scheduling
  exams, 4
  virus scanning (antivirus software), 456
schematics (wiring), 307-310
scopes, 88
SCP (Secure Copy Protocol), 66, 70, 442
SDH (Synchronous Digital Hierarchy),
  SONET and, 182
SDSL (Symmetric Digital Subscriber Line) Internet access, 192-193
secure email, PKI and, 439
security
  access control, 418
    ACE, 419
    ACL, 419, 425-426
    DAC, 419
    MAC, 419, 425-426
    RBAC, 420
    RoBAC, 420-421
    TCP/IP filtering, 426
  accounting, 431
    RADIUS, 439-440
    TACACS+, 440
    ACL, 158
    AP, 262
    auditing events, 431
    authentication, 429-430, 440-441
      CHAP, 441
      EAP, 441
      Kerberos authentication, 433-436
      MS-CHAP, 440
      MS-CHAPv2, 441
      multifactor authentication, 445
      PAP, 441
      passwords, 432-433
      RADIUS, 439-440
      remote authentication, 440-441
      TACACS+, 440
      two-factor authentication, 445
      WPA, 292
    authorization, 429-430
      RADIUS, 439-440
      TACACS+, 440
    back door attacks, 455
    broadband Internet access, 197
    CCMP, 293
    CHAP, 441
    DMS (perimeter networks), 466-467
    DoS attacks, 452-454
    EAP, 441
    eavesdropping attacks, 454
    email, 197
    encryption
      asymmetric key encryption, 437
      PKI, 436-439
      private key encryption, 437
      public key encryption, 437
      symmetric key encryption, 437
      TKIP, 292
    evil twin attacks, 455
firewalls, 197, 460-461, 466
application layer firewalls, 465-466
bandwidth management, 462
circuit-level firewalls, 465-466
content filtering, 461
features of, 461-462
NAT, 462
packet-filtering firewalls, 463-465
signature identification, 461
stateful firewalls, 462-463
stateless firewalls, 462-463
URL filtering, 462
virus scanning, 461
FTP bounce attacks, 455
honeynets, 470
honeypots, 469-470
ICMP flood attacks, 362
IDS, 468-469
IPS, 468
ISAKMP, 415
man-in-the-middle attacks, 455
monitoring, 324
MS-CHAP, 440
MS-CHAPv2, 441
multifactor authentication, 445
PAP, 441
passwords, attacks using, 454
patches, 457
phishing attacks, 456
physical security, 443
biometrics, 445
lock and key, 443-444
PIN pads, 444-445
swipe cards, 444-445
PKI, 436
asymmetric key encryption, 437
CA, 436
certificate templates, 436
certificates, 436
confidentiality, 438
CRL, 436
digital certificates, 439
digital signatures, 438
private key encryption, 437
public key encryption, 437
secure email, 439
symmetric key encryption, 437
uses of, 438
web security, 438
posture assessments, 424
preventing attacks, strategies for, 456-457
privileges, least privilege concept, 421
procedures, 316
RADIUS, 439-440
remote authentication, 440-441
remote-access protocols, 421-423
remote-control protocols, 424
rogue AP, 455
secured versus unsecured protocols table, 442
social engineering attacks, 454
spoofing attacks, 455
SSID, 262
TACACS+, 440
TCP/UDP ports, 197
threat management, man-in-the-middle attacks, 416
TKIP, 292
Trojan horses, 451-452
tunneling
client-to-site tunneling, 418
IPSec, 417-418
L2TP, 416
PPTP, 415-416
site-to-site tunneling, 418
two-factor authentication, 445
violations, reporting, 316
viruses, 450-452
antivirus software, 456-457
scanning for, 456-457, 461
VLAN, 36
VPN, 35, 414
VPN concentrators, 158, 469
vulnerability scanners, 470
war chalking, 455-456
war driving, 455
WEP cracking, 455
wireless connections, configuring, 278
wireless device communication, 277-278
wireless networks
WEP, 290-291, 300
WPA, 292
WPA Enterprise, 294-295
WPA2, 293
WLAN, 289
worms, 451-452
WPA cracking, 455
security logs, 332, 335
segmentation
transport layer (layer 4), 47
VLAN, 38
self-healing networks, wireless mesh networks, 27
server farms, 391
server rooms, vertical cabling, 233
server-side content filters, 155
servers
authentication servers (802.1X wireless standard), 294
clustering, fault tolerance, 391-392
configuring, documentation, 306
DHCP servers, 138-139, 160
DNS servers, 160
load balancing, 155
TCP/IP client configurations, 501
primary server configurations, 391
proxy servers, 156, 160
ACL, 158
caching, 157
filtering client requests, 157
standby servers, fault tolerance, 390
virtual servers, 163
service addressing, transport layer (layer 4), 47
services (networks), documentation, 306
session layer (layer 5), OSI seven-layer networking model, 47, 49
session layer firewalls. See circuit-level firewalls
SFTP (Secure File Transfer Protocol), 58-59, 69, 442
shaping traffic, 408-409
shared bandwidth, cable Internet access, 196
shared key authentication (wireless device communication), 277
signal amplification
AP and, 264
smart jacks, 238
signature identification, firewalls and, 461
signature-based IDS (intrusion detection systems), 468
simplex mode cabling, 212
single-mode fiber-optic cable, 220
SIP (Session Initiation Protocol), 68, 71
site-local addresses, 105
site-to-site tunneling, 418
smart jacks, 238
SmartFTP, 57
SMTP (Simple Mail Transfer Protocol), 59-60, 70
Smurf attacks, 453
SNAT (Static NAT), 113
snips (wire), 339
SNMP (Simple Network Management Protocol), 82
agents, 84
communities, 85-86
components of, 83
management systems, 83-84
managers, 83
MIB, 85
SNMPv3, 86
trap managers, 84
SNMPv1, 442
SNMPv2, 442
SNMPv3, 442
SOA (Start of Authority) records, 79
social engineering attacks, 454
Social Security numbers, exam scheduling requirements, 4
software
personal software policies, 315
procedures, 316
software configuration utilities, NIC installations, 144
SOHO networks, 168
configuring, 169
Internet service providers and, 172
modems, 171
point of demarcation, 172-173
routing, 169, 173
wiring, 169, 171
SOHO routers, 145
solutions, implementing (troubleshooting procedures), 480
SONET (Synchronous Optical Network), 182-183, 187, 254
sound files, presentation layer (layer 6), 48
source quench, ICMP, 63
source route bridges, 138
speed lights (NIC), 143
spikes (power), UPS and, 394
split cables, troubleshooting, 495
split horizons, 125
spoofing attacks, 455
spread spectrum technology, 273
DSSS, 274, 287
FHSS, 273, 287
SSH (Secure Shell), 62, 70, 424, 442
SSID (Service Set Identifiers), 262
beacons, 272
troubleshooting, 300
wireless connections, configuring, 278, 281
wireless device communication, 277
SSL (Secure Socket Layer) protocol, 438
STA (Spanning Tree Algorithm), 130
standby servers, fault tolerance, 390
star topologies, 19
advantages/disadvantages of, 20
hubs, 19
switches, 19
troubleshooting, 505-506
wiring, 505
stateful configurations (IP), 106
stateful firewalls, 462-463
stateless configurations (IP), 106
stateless firewalls, 462-463
static addressing, 107
static routing, TCP/IP routing, 122
statistics, capturing, 313
stealth viruses, 451
store-and-forward switching environments, 147
STP (Shielded Twisted Pair) cable, 215
STP (Spanning Tree Protocol), 130
straight-through cabling, 148, 228
stress tests, 330
strippers (wire), 339
structure cable. See horizontal cabling
subnet masks
  IP addressing, 108
  IPv4 assignments, 96
  TCP/IP client configurations, 500-501
troubleshooting, 489
subnetting (IPv4), 97-98
subobjectives (Network+ exam), 2-4
supplicants (802.1X wireless standard), 294-295
surface jacks, SOHO network configurations, 169
surge protection (smart jacks), 238
surges (power), UPS and, 394
SVC (switched virtual circuits), Frame Relay connections, 185
swipe cards (physical security), 444-445
switches, 138, 146, 159
  ARP command switches, 64, 361
  circuit switching, WAN configurations, 177-178
  content switches, 156, 160
  cut-through switching environments, 147
dip switches, 144
FragmentFree switching environments, 148
full-duplex configuration mode, 147
half-duplex configuration mode, 147
hub and switch cabling, 148
ipconfig command, 372
Layer 3 switches. See multilayer switches
MAC addresses, 146
MDI ports, 148
multilayer switches, 160
  load balancing, 155
  OSI model, 156
nbtstat command, 369-370
netstat command switches, 363
nslookup command, 374
OSI model, 50, 148
packet switching
  ATM, 186-187
datagram packet switching, 177
  Frame Relay, 184-187
  independent routing, 176
  virtual-circuit packet switching, 176-177
  WAN configurations, 176-177
  X.25, 183-184, 187
port authentication, 132
port mirroring, 132
route command, 377
star topologies, 19, 505
store-and-forward switching environments, 147
troubleshooting, 497, 505
trunking, 131
virtual switches, 163-164
VLAN trunking, 131
WAN configurations, 176
  circuit switching, 177-178
  packet switching, 176-177
wireless connections, configuring, 278
switching loops, 130, 486
Sylvan Prometric testing service, scheduling exams, 4
symmetric key encryption, 435, 437
symptoms, identifying (troubleshooting procedures), 478
SYN floods, 453
SYN messages, TCP, 56
syslog, 334
system functionality, verifying (troubleshooting procedures), 481
system logs, 334-335
T
T connectors (taps), 17
T-carrier lines
fracional T, 180
T3 lines, 181
WAN configurations, 180-181, 187
T568A (110 blocks), 235-236
T568A wiring standard, 228
T568B (110 blocks), 235-236
T568B wiring standard, 228
TACACS+, 440
tape rotations, 400
tapes
backup strategies, 401
cleaning, 401
taps. See T connectors (taps)
TCP (Transfer Control Protocol), 47, 55-56, 69
TCP/IP
client configurations, troubleshooting, 499-501
filtering, 426
network connections, IP-related settings, 108
port assignments, 117-118
routing, 120
default gateways, 120
dynamic routing, 123-126
routing tables, 121
static routing, 122
TCP/IP four-layer networking model, 43
Application layer, 50
Network Access (Link) layer, 50
Network Interface layer, 50
OSI seven-layer model comparisons, 49-50
Transport layer, 50
TCP/IP protocol stack, loopbacks, 359
TCP/IP protocol suite, summary of, 69-71
TCP/UDP ports, broadband security, 197
TDM (Time Division Multiplexing), 211
TDR (time domain reflectometer), 344
technical support, troubleshooting
cable Internet access, 196
telecommunications rooms
110 blocks (T568A, T568B), 235-236
horizontal cabling, 232
IDF telecommunications rooms, 236
MDF telecommunications rooms, 236
patch panels, 234
vertical cabling, 233
Telnet, 62, 70, 442
temperature
air conditioning, 342
environmental monitors, 341
HVAC, 342
templates, PKI certificate templates, 436
termination (wiring), verifying, 239-240
test-taking strategies, Network+ exam, 2, 6-7
testing theory of probable cause
(troubleshooting procedures), 479
tests. See exams
text (data) files, presentation layer (layer 6), 48
TFTP (Trivial File Transfer Protocol), 59, 69
theory of probable cause (troubleshooting procedures)
establishing theory, 478
testing theory, 479
thicknet (thick coax) coaxial cable, 218
thin client computing, 424
thinnet (thin coax) coaxial cable, 218-219

threat management (security)
  antivirus software, 456-457
  back door attacks, 455
  buffer overflows, 453
  DMZ (perimeter networks), 466-467
  DoS attacks, 452-453
  eavesdropping attacks, 454
  evil twin attacks, 455
  firewalls, 460-461, 466
    application layer firewalls, 465-466
    bandwidth management, 462
    circuit-level firewalls, 465-466
    content filtering, 461
    features of, 461-462
    NAT, 462
    packet-filtering firewalls, 463-465
    signature identification, 461
    stateful firewalls, 462-463
    stateless firewalls, 462-463
    URL filtering, 462
    virus scanning, 461
  Fraggle attacks, 453
  FTP bouncing attacks, 455
  honeynets, 470
  honeypots, 469-470
  ICMP floods, 454
  IDS, 468-469
  IPS, 468
  man-in-the-middle attacks, 416, 455
  password attacks, 454
  patches, 457
  phishing attacks, 456
  ping of death attacks, 453
  preventing attacks, strategies for, 456-457
  rogue AP, 455
  security updates, 457
  Smurf attacks, 453
  social engineering attacks, 454
  spoofing attacks, 455
  SYN floods, 453
  Trojan horses, 451-452
  viruses, 450-452, 456-457, 461
  VPN concentrators, 469
  vulnerability scanners, 470
  war chalking, 455-456
  war driving, 455
  WEP cracking, 455
  worms, 451-452
  WPA cracking, 455

three-way handshake (TCP), 56
throughput
  testing, 325, 327
  wireless networks, 271-272

tickets, Kerberos authentication, 435-436

time
  Network+ exam allotted test time, 2
  synchronization, NTP, 65

time stamps, beacons, 272

TKIP (Temporal Key Integrity Protocol), 292

TLS (Telnet Layer Security), 71, 442
TLS (Transport Layer Security) protocol, 67, 438
token ring networks, speed, 246
toner probes, 342-343
topics (Network+ exam). See objectives
topologies
  ad hoc wireless topologies, 22-23
  bus topologies, 16-17
  convergence, 125
defining, 16
documentation (administration), 305
hybrid mesh topologies, 21
hybrid topologies, 27
IEEE 802.3 standard, 249
infrastructure wireless topologies, 22-23
logical topologies
defining, 16
logical ring topologies, 18
mesh topologies, 20
advantages/disadvantages of, 21
fault tolerance, 21
hybrid mesh topologies, 21
MPLS, 21-22
redundancy, 20
wireless mesh networks, 25-27
physical topologies
defining, 16
physical bus topologies, 17
PtMP network topologies, 25
PtP network topologies, 24
ring topologies, 18-19
star topologies, 19
advantages/disadvantages of, 20
hubs, 19
switches, 19
wiring, 505
troubleshooting, 504
mesh topologies, 506
star topologies, 505-506
wireless mesh network topologies, 25-27
wireless topologies
ad hoc wireless topologies, 22-23
infrastructure wireless topologies, 22-23
mesh network topologies, 25-27
PtMP network topologies, 25
PtP network topologies, 24
traceroute command, 351-355
tracert command, 123, 351-355
traffic shaping, 154, 408-409
training, administration, 304
translational bridges, 138
transmission rates (data), cabling and, 213-214
transparent bridges, 138
transport layer
OSI seven-layer networking model, 47, 49
TCP/IP four-layer networking model, 50
trap managers, 84
Trojan horses, 451-452
troubleshooting
antennas (wireless), 263, 267-268, 299
AP, 497
AP coverage, 263-264
bridges, 497
buses, 498
cable Internet access, 196-197
connectivity
client connections, 498
duplexes, 502
media connections, 498-501
port speeds, 502
documentation (administration), advantages of, 304
DSL Internet access, 194
hardware, 496-497
hubs, 496, 505
ipconfig command, 371
modems, 196
networks
black holes, 487-488
broadcast storms, 487
DNS, 490
duplicate IP addresses, 489
<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>gateways</td>
<td>489</td>
</tr>
<tr>
<td>ipconfig command</td>
<td>371</td>
</tr>
<tr>
<td>mismatched MTU/MUT black holes</td>
<td>487-488</td>
</tr>
<tr>
<td>missing/bad routes</td>
<td>488</td>
</tr>
<tr>
<td>modules</td>
<td>488</td>
</tr>
<tr>
<td>port configuration</td>
<td>487</td>
</tr>
<tr>
<td>power failures</td>
<td>488</td>
</tr>
<tr>
<td>proxy ARP</td>
<td>486</td>
</tr>
<tr>
<td>routing loops</td>
<td>486</td>
</tr>
<tr>
<td>routing problems</td>
<td>486</td>
</tr>
<tr>
<td>subnet masks</td>
<td>489</td>
</tr>
<tr>
<td>switching loops</td>
<td>486</td>
</tr>
<tr>
<td>ping command</td>
<td>359-360</td>
</tr>
<tr>
<td>POTS Internet access</td>
<td>198</td>
</tr>
<tr>
<td>dial tones</td>
<td>199</td>
</tr>
<tr>
<td>ISP</td>
<td>199</td>
</tr>
<tr>
<td>modems</td>
<td>199-200</td>
</tr>
<tr>
<td>phone numbers</td>
<td>199</td>
</tr>
<tr>
<td>physical connections</td>
<td>199</td>
</tr>
<tr>
<td>procedures</td>
<td></td>
</tr>
<tr>
<td>determining changes</td>
<td>478</td>
</tr>
<tr>
<td>determining escalation</td>
<td>480-481</td>
</tr>
<tr>
<td>documenting findings</td>
<td>482</td>
</tr>
<tr>
<td>establishing plans of action</td>
<td>479-480</td>
</tr>
<tr>
<td>establishing theory of probable cause</td>
<td>478</td>
</tr>
<tr>
<td>identifying the problem</td>
<td>477-478</td>
</tr>
<tr>
<td>implementing solutions</td>
<td>480</td>
</tr>
<tr>
<td>testing theory of probable cause</td>
<td>479</td>
</tr>
<tr>
<td>verifying full system functionality</td>
<td>481</td>
</tr>
<tr>
<td>RF channels</td>
<td>269, 299</td>
</tr>
<tr>
<td>routers</td>
<td>497</td>
</tr>
<tr>
<td>satellite Internet access</td>
<td>202</td>
</tr>
<tr>
<td>SSID</td>
<td>300</td>
</tr>
<tr>
<td>switches</td>
<td>497, 505</td>
</tr>
<tr>
<td>TCP/IP client configurations</td>
<td>499-501</td>
</tr>
<tr>
<td>topologies</td>
<td>504</td>
</tr>
<tr>
<td>mesh topologies</td>
<td>506</td>
</tr>
<tr>
<td>star topologies</td>
<td>505-506</td>
</tr>
<tr>
<td>VLAN</td>
<td>503-504</td>
</tr>
<tr>
<td>WEP</td>
<td>300</td>
</tr>
<tr>
<td>wireless networks</td>
<td>298-300</td>
</tr>
<tr>
<td>wiring</td>
<td>490-491</td>
</tr>
<tr>
<td>attenuation</td>
<td>493</td>
</tr>
<tr>
<td>bad wiring</td>
<td>494</td>
</tr>
<tr>
<td>cable placement</td>
<td>496</td>
</tr>
<tr>
<td>connectors</td>
<td>494</td>
</tr>
<tr>
<td>crossover cables</td>
<td>495-496</td>
</tr>
<tr>
<td>crosstalk</td>
<td>492-493</td>
</tr>
<tr>
<td>DB loss</td>
<td>495</td>
</tr>
<tr>
<td>determining where cable is used</td>
<td>491-492</td>
</tr>
<tr>
<td>EMI</td>
<td>492-493</td>
</tr>
<tr>
<td>FEXT</td>
<td>493</td>
</tr>
<tr>
<td>interference</td>
<td>492-493</td>
</tr>
<tr>
<td>NEXT</td>
<td>492</td>
</tr>
<tr>
<td>open impedance mismatch (echo)</td>
<td>494</td>
</tr>
<tr>
<td>open/short faults</td>
<td>494</td>
</tr>
<tr>
<td>schematics</td>
<td>309</td>
</tr>
<tr>
<td>split cables</td>
<td>495</td>
</tr>
<tr>
<td>TXRX reversed cables</td>
<td>495-496</td>
</tr>
<tr>
<td>trunking</td>
<td>131</td>
</tr>
<tr>
<td>TTL (Time To Live)</td>
<td>358</td>
</tr>
<tr>
<td>tunneling</td>
<td>32</td>
</tr>
<tr>
<td>client-to-site tunneling</td>
<td>418</td>
</tr>
<tr>
<td>IPSec</td>
<td>417-418</td>
</tr>
<tr>
<td>L2TP</td>
<td>416</td>
</tr>
<tr>
<td>PPTP</td>
<td>415-416</td>
</tr>
<tr>
<td>site-to-site tunneling</td>
<td>418</td>
</tr>
<tr>
<td>twisted pair cable</td>
<td>214-216</td>
</tr>
<tr>
<td>categories of</td>
<td>216-218</td>
</tr>
<tr>
<td>longitudinal separators</td>
<td>217</td>
</tr>
</tbody>
</table>
SOHO network configuration, 171
STP cable, 215
UTP cable, 215
twisted-pair networks, connecting to, 499
two-factor authentication, 445
two-way satellite systems, 191, 201
TXRX reversed cables, troubleshooting, 495-496
Type A connectors, 226
Type B connectors, 226

UDP (User Datagram Protocol), 56-57, 69
   network layer (layer 3), 47
   RTP and, 68
unicast addresses, 102
unicast IPv6 addresses, 105
Unknown host error messages, 358
unmanaged wireless topologies. See ad hoc wireless topologies
updating
   antivirus software, 457
distance-vector routing, 124
documentation, 312
security, 457
UPS (uninterrupted power supplies), 393-394
URL filtering, firewalls and, 462
USB (Universal Serial Bus) connectors, 226
user account policies, 315
UTP (unshielded twisted-pair) cable, 215
cable Internet access, 195
EMI, 213

V
vampire taps. See T connectors (taps)
variant viruses, 450
VDI (virtual desktop interface), 163
VDSL. See VHDSL
verifying
   backups, 401
   full system functionality (troubleshooting procedures), 481
   wiring installation, 239-240
   wiring termination, 239-240
vertical (backbone) cabling, 231, 233
vertical (main) cross-connects, 232
vetting email, 457
VHDSL (Very High Bit Rate DSL)
   Internet access, 192-193
video files, presentation layer (layer 6), 48
violations (security), reporting, 316
virtual circuits, Frame Relay connections, 184-185
virtual desktops, 162-163
virtual PBX (private branch exchanges), 164
virtual servers, 163
virtual switches, 163-164
virtual-circuit packet switching, 176-177
virtualization, 162
VLAN, 35-36
   administration, 36
   advantages/disadvantages of, 36
   MAC address-based VLAN memberships, 37-38
   memberships, 37-38
   organization, 36
   performance, 36
   port-based VLAN memberships, 37
protocol-based VLAN memberships, 37
security, 36
segmentation, 38
VPN, 32
802.1Q IEEE specification, 36
access methods, 34
advantages/disadvantages of, 34-35
analog modems and, 34
cable connections and, 34
clients, 34
components of connections, 33-34
cost, 34
dedicated broadband connections and, 34
DSL connections and, 34
cost, 34
encryption, 34
ISDN and, 34
L2TP and, 34
LAN-to-LAN internetworking, 33
PPTP and, 34
reliability, 35
remote access, 33
scalability, 35
security, 35
servers, 34
wireless connections and, 34
viruses, 450-452
antivirus software, features of, 456-457
scanning for, 456-457, 461
VLAN (virtual local area networks), 35-36
802.1Q IEEE specification, 36
administration, 36
advantages/disadvantages of, 36
memberships, 37-38
organization, 36
performance, 36
security, 36
segmentation, 38
troubleshooting, 503-504
trunking, 131
VoIP (Voice over IP), 68
RTP, 68-69
SIP, 68
virtual PBX, 164
voltage event recorders, 340
VPN (virtual private networks), 32, 414
access methods, 34
advantages/disadvantages of, 34-35
analog modems and, 34
cable connections and, 34
clients, 34
connections, components of, 33-34
cost, 34
dedicated broadband connections and, 34
DSL connections and, 34
cost, 34
encryption, 34
ISDN and, 34
L2TP and, 34
LAN-to-LAN internetworking, 33
PPTP, 34, 415
reliability, 35
remote access, 33
scalability, 35
security, 35
servers, 34
wireless connections and, 34
VPN concentrators, 158, 469
VTP (VLAN Trunking Protocol), 132
VUE testing service, scheduling exams, 4
vulnerability scanners, 470
W

wall jacks, SOHO network configurations, 169

WAN (wide area networks), 11, 175.
See also MAN (metropolitan area networks)

ATM, 186-187
Frame Relay, 184-187
ISDN, 178-179, 187
PSTN Internet access, 200
SONET, 182-183, 187
switching, 176
  circuit switching, 177-178
  packet switching, 176-177
T-carrier lines, 180-181, 187
X.25, 183-184, 187

WAP (wireless application protocol), 22
war chalking, 455-456
war driving, 455
warm recovery sites (disaster recovery), 404
warm swaps, 403

WDM-PON (wavelength division multiplexing passive optical networks), 183

websites, ACL, 158
WEP (Wired Equivalent Privacy), 290-291
  cracking, 455
  troubleshooting, 300

Wi-Fi detectors, 347

WiMax (Worldwide Interoperability for Microwave Access), 204

windowing (flow control), 47

WINS (Windows Internet Name Service), 80

wireless access points, 149. See also AP (access points)
  LAN and, 22
  OSI model, 150

wireless connections, VPN and, 34
wireless Internet access, 203
wireless mesh networks, 25-27

wireless networks, 259

802.11 wireless standards (IEEE), 284, 286-287
802.11a wireless standard (IEEE), 271, 285-286
802.11b wireless standard (IEEE), 285-286
802.11b/g wireless standard (IEEE), 269-270
802.11g wireless standard (IEEE), 285, 287
802.11n wireless standard (IEEE), 270, 285-287

antennas, 264
  adjusting, 263
  configuring wireless connections, 279
  directional antennas, 266
  gain values, 265
  interference, 267
  MIMO antennas, 285
  omnidirectional antennas, 265-266
  polarization, 267
  ratings, 265
  replacing, 263
  signal quality, 267
  troubleshooting, 263, 267-268, 299

AP, 259-261
  beacons, 272
  bridges, 261
  bridges, AP as, 276
  BSA and, 263
  BSS, 262, 276
  BSSID and, 262
  ESS, 262, 276
ESSID and, 262
security, 262
SSID and, 262
troubleshooting coverage, 263-264
wireless device communication, 276-277
beacons, 272-273
communication between wireless devices, establishing, 275
association, 276
authentication, 277
reassociation, 276
RF channels, 277
security, 277-278
SSID, 277
troubleshooting, 298-300
connections, configuring, 278, 281-282
data rates, 271-272
infrared wireless networking, 274-275
infrastructure wireless networks, 261
interference, 300-301
OFDM, 274, 287
repeaters, 264
RF channels, 268, 270
802.11a wireless standard (IEEE), 271
802.11b/g wireless standard (IEEE), 269-270
802.11n wireless standard (IEEE), 270
configuring wireless connections, 281
frequency hopping, 273
narrowband transmissions, 273
nonoverlapping channels, 268-269
overlapping channels, 269
troubleshooting, 269, 299
wireless device communication, 277
security
AP, 262
WEP, 290-291, 300
WPA, 292
WPA Enterprise, 294-295
WPA2, 293
spread spectrum technology, 273
DSSS, 274, 287
FHSS, 273, 287
SSID, 262
beacons, 272
configuring wireless connections, 278, 281
troubleshooting, 300
wireless device communication, 277
throughput, 271-272
time stamps, beacons, 272
troubleshooting, 298-300
war chalking, 455-456
war driving, 455
WEP cracking, 455
WLAN, 260-261
WPA cracking, 455
wireless topologies
ad hoc wireless topologies, 22-23
infrastructure wireless topologies, 22-23
mesh network topologies, 25-27
PtMP network topologies, 25
PtP network topologies, 24
wiring
110 blocks (T568A, T568B), 235-236
568A wiring standard, 227
568B wiring standard, 227
attenuation, 213, 493
bad wiring, troubleshooting, 494
baseband transmissions, TDM, 211
broadband transmissions
  BPL, 211
  FDM, 211
HomePlug Powerline Alliance, 212
IEEE 1901, 212
IEEE 1905, 212
cable Internet access, 195
cable placement, troubleshooting, 496
coaxial cable, 214, 218-219
connectors, troubleshooting, 494
crossover cabling, 148, 228-230, 495-496
CSU/DSU, 238
data transmission rates, 213-214
DB loss, troubleshooting, 495
demarcation points, 237-238
EMI, 492-493
fiber-optic cable, 213-215, 219-221
full-duplex mode, 212
half-duplex mode, 212
horizontal cabling, 231-232
horizontal cross-connects, 232
hub and switch cabling, 148
IDC, 235
IDF telecommunications rooms, 236
installation, verifying, 239-240
intermediate cross-connects, 232
layouts, documentation (administration), 306
loopback cabling, 231
MDF telecommunications rooms, 236
media connectors
  BNC connectors, 221
  F-Type connectors, 223
  fiber connectors, 224
  RG-6 connectors, 223
  RG-59 connectors, 223
  RJ-11 connectors, 222
  RJ-45 connectors, 223
  RS-232 standard connectors, 225
  Type A connectors, 226
  Type B connectors, 226
  USB connectors, 226
media converters, 141, 226-227
media interference, 212-213
NIC installations, 142
open impedance mismatch (echo), troubleshooting, 494
open/short faults, troubleshooting, 494
optical cable testers, 345
patch panels, 234
plenum cable, 221
punchdown tools, 235, 340
risers, 491
rollover cabling, 230
schematics, 307-310
simplex mode, 212
smart jacks, 238
snips, 339
SOHO networks, 169, 171
split cables, troubleshooting, 495
star topologies, 505
STP cable, 215
straight-through cabling, 228
strippers, 339
switch and hub cabling, 148
T-carrier lines
  T3 lines, 181
  WAN configurations, 180-181, 187
T568A wiring standard, 228
T568B wiring standard, 228
termination, verifying, 239-240
troubleshooting, 490-491
  attenuation, 493
  bad wiring, 494
  cable placement, 496
  connectors, 494
  crossover cables, 495-496
  crosstalk, 492-493
  DB loss, 495
determining where cable is used, 491-492
  EMI, 492-493
  FEXT, 493
  interference, 492-493
  NEXT, 492
  open impedance mismatch (echo), 494
  open/short faults, 494
  split cables, 495
  TXRX reversed cables, 495-496
twisted pair cable, 214-216
  categories of, 216-218
  longitudinal separators, 217
  STP, 215
  UTP, 215
  TXRX reversed cables, troubleshooting, 495-496
  UTP cable, 213, 215
  vertical (backbone) cabling, 231, 233
  vertical (main) cross-connects, 232
  wire crimpers, 339

wiring closets. See telecommunications rooms

WISP (Wireless Internet Service Providers), 203
WLAN (wireless local area networks), 260
  AP, 261
  security, 289
  wireless AP, 149

workgroup hubs, 141
worms, 451-452
WPA (Wi-Fi Protected Access), 292
WPA cracking, 455
WPA Enterprise, 294-295
WPA2 (Wi-Fi Protected Access version 2), 293
WPAN (wireless personal area networks), 11

X

X.25
  PAD, 184
  WAN configurations, 183-184, 187