TROY MCMILLAN
ROBIN ABERNATHY

Cert Guide

Learn, prepare, and practice for exam success

CISSP

PEARSON IT
CERTIFICATION

FREE SAMPLE CHAPTER

CISSP Cert Guide

Troy McMillan
Robin M. Abernathy

PEARSON

800 East 96th Street,
Indianapolis, Indiana 46240 USA

CISSP Cert Guide

Troy McMillan
Robin M. Abernathy

ISBN-13: 978-0-7897-5151-5
ISBN-10: 0-7897-5151-8

Library of Congress Control Number: 2013949991

Printed in the United States on America

First Printing: October 2013

Trademarks

Warning and Disclaimer

Bulk Sales

Pearson offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

U.S. Corporate and Government Sales
1-800-382-3419
corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact

International Sales
international@pearsoned.com

Associate Publisher
Dave Dusthimer

Acquisitions Editor
Betsy Brown

Development Editor
Allison Beaumont Johnson

Managing Editor
Sandra Schroeder

Project Editor
Seth Kerney

Copy Editor
Paula Lowell

Indexer
Erika Millen

Proofreader
Anne Goebel

Technical Editors
Chris Crayton
Brock Pearson

Publishing Coordinator
Vanessa Evans

Multimedia Developer
Eric Miller

Book Designer
Chuti Prasertsith

Composition
Jake McFarland

Contents at a Glance

	Introduction	
CHAPTER 1	The CISSP Certification	3
CHAPTER 2	Access Control	13
CHAPTER 3	Telecommunications and Network Security	65
CHAPTER 4	Information Security Governance and Risk Management	159
CHAPTER 5	Software Development Security	203
CHAPTER 6	Cryptography	243
CHAPTER 7	Security Architecture and Design	297
CHAPTER 8	Operations Security	343
CHAPTER 9	Business Continuity and Disaster Recovery	369
CHAPTER 10	Legal, Regulations, Investigations, and Compliance	405
CHAPTER 11	Physical (Environmental) Security	445
	Glossary	481
	Index	538
APPENDIX A	Memory Tables	On CD
APPENDIX B	Memory Tables Answer Key	On CD

Table of Contents

Chapter 1 The CISSP Certification 3

The Goals of the CISSP Certification 3

Sponsoring Bodies 3

Stated Goals 4

The Value of the CISSP Certification 4

To the Security Professional 5

To the Enterprise 5

The Common Body of Knowledge 5

Access Control 5

Telecommunications and Network Security 6

Information Security Governance and Risk Management 6

Software Development Security 7

Cryptography 7

Security Architecture and Design 8

Operations Security 8

Business Continuity and Disaster Recovery Planning 8

Legal, Regulations, Investigations, and Compliance 9

Physical and Environmental Security 9

Steps to Becoming a CISSP 10

Qualifying for the Exam 10

Signing Up for the Exam 10

About the CISSP Exam 10

Chapter 2 Access Control 13

Foundation Topics 13

Access Control Concepts 13

CIA 13

Default Stance 14

Defense In Depth 14

Access Control Process 15

Identify Resources 15

Identify Users 15

Identify Relationships between Resources and Users 16

Identification and Authentication Concepts 16
Three Factors for Authentication 17
Knowledge Factors 17
Identity and Account Management 18
Password Types and Management 19
Ownership Factors 22
Synchronous and Asynchronous Token 22
Memory Cards 22
Smart Cards 23
Characteristic Factors 23
Physiological Characteristics 24
Behavioral Characteristics 25
Biometric Considerations 26
Authorization Concepts 28
Access Control Policies 28
Separation of Duties 29
Least Privilege/Need-to-Know 29
Default to No Access 30
Directory Services 30
Single Sign-on 31
Kerberos 32
SESAME 34
Federated Identity Management 35
Security Domains 35
Accountability 35
Auditing and Reporting 36
Vulnerability Assessment 37
Penetration Testing 38
Access Control Categories 39
Compensative 40
Corrective 40
Detective 40
Deterrent 40
Directive 40

Preventive 41
Recovery 41
Access Control Types 41
Administrative (Management) Controls 41
Logical (Technical) Controls 43
Physical Controls 43
Access Control Models 46
Discretionary Access Control 46
Mandatory Access Control 47
Role-based Access Control 47
Rule-based Access Control 48
Content-dependent Versus Context-dependent 48
Access Control Matrix 48
Capabilities Table 48
Access Control List (ACL) 49
Access Control Administration 49
Centralized 49
Decentralized 49
Provisioning Life Cycle 50
Access Control Monitoring 50
IDS 50
IPS 52
Access Control Threats 52
Password Threats 53
Dictionary Attack 53
Brute-Force Attack 53
Social Engineering Threats 53
Phishing/Pharming 54
Shoulder Surfing 54
Identity Theft 54
Dumpster Diving 55
DoS/DDoS 55
Buffer Overflow 55
Mobile Code 56

Malicious Software 56
Spoofing 56
Sniffing and Eavesdropping 57
Emanating 57
Backdoor/Trapdoor 57
Exam Preparation Tasks 57
Review All Key Topics 57
Complete the Tables and Lists from Memory 58
Define Key Terms 59
Review Questions 59
Answers and Explanations 61
Chapter 3 Telecommunications and Network Security 65
Foundation Topics 66
OSI Model 66
Application Layer 67
Presentation Layer 67
Session Layer 67
Transport Layer 68
Network Layer 68
Data Link Layer 68
Physical Layer 69
Multi-Layer Protocols 70
TCP/IP Model 71
Application Layer 72
Transport Layer 72
Internet Layer 74
Link Layer 76
Encapsulation 76
Common TCP/UDP Ports 77
Logical and Physical Addressing 78
IPv4 78
IP Classes 80
Public Versus Private IP Addresses 81
NAT 81

IPv4 Versus IPv6 82
MAC Addressing 82
Network Transmission 83
Analog Versus Digital 83
Asynchronous Versus Synchronous 84
Broadband Versus Baseband 84
Unicast, Multicast, and Broadcast 85
Wired Versus Wireless 86
Cabling 87
Coaxial 87
Twisted Pair 88
Fiberoptic 90
Network Topologies 91
Ring 91
Bus 92
Star 92
Mesh 93
Hybrid 94
Network Technologies 94
Ethernet 802.3 94
Token Ring 802.5 96
FDDI 97
Contention Methods 97
CSMA/CD Versus CSMA/CA 98
Collision Domains 98
CSMA/CD 99
CSMA/CA 100
Token Passing 101
Polling 101
Network Protocols/Services 101
ARP 101
DHCP 102
DNS 103
FTP, FTPS, SFTP 103

HTTP, HTTPS, SHTTP 104
ICMP 104
IMAP 105
NAT 105
PAT 105
POP 105
SMTP 105
SNMP 105
Network Routing 106
Distance Vector, Link State, or Hybrid Routing 106
RIP 107
OSPF 107
IGRP 108
EIGRP 108
VRRP 108
IS-IS 108
BGP 108
Network Devices 109
Patch Panel 109
Multiplexer 109
Hub 109
Switch 110
VLANs 111
Layer 3 Versus Layer 4 111
Router 111
Gateway 112
Firewall 112
Types 113
Architecture 114
Virtualization 116
Proxy Server 116
PBX 116
Honeypot 117

Cloud Computing 117
Endpoint Security 119
Network Types 119
LAN 119
Intranet 119
Extranet 120
MAN 120
WAN 120
WAN Technologies 121
T Lines 121
E Lines 121
OC Lines (SONET) 122
CSU/DSU 122
Circuit-Switching Versus Packet-Switching 123
Frame Relay 123
ATM 123
X.25 124
Switched Multimegabit Data Service 124
Point-to-Point Protocol 124
High-Speed Serial Interface 124
PSTN (POTS, PBX) 125
VoIP 125
Remote Connection Technologies 126
Dial-up 126
ISDN 127
DSL 127
Cable 128
VPN 129
RADIUS and TACACS 132
Remote Authentication Protocols 133
Telnet 134
TLS/SSL 134
Multimedia Collaboration 134

Wireless Networks 135
FHSS, DSSS, OFDM, FDMA, TDMA, CDMA, OFDMA, and GSM 135
802.11 Techniques 136
Cellular or Mobile Wireless Techniques 136
WLAN Structure 137
Access Point 137
SSID 137
Infrastructure Mode Versus Ad Hoc Mode 137
WLAN Standards 137
802.11a 138
802.11b 138
802.11f 138
802.11g 138
802.11n 138
Bluetooth 139
Infrared 139
WLAN Security 139
WEP 139
WPA 140
WPA2 140
Personal Versus Enterprise 140
SSID Broadcast 141
MAC Filter 141
Satellites 141
Network Threats 142
Cabling 142
Noise 142
Attenuation 142
Crosstalk 143
Eavesdropping 143
ICMP Attacks 143
Ping of Death 143

Smurf *144*
Fraggle *144*
ICMP Redirect *144*
Ping Scanning *145*
DNS Attacks 145
DNS Cache Poisoning *145*
DoS *146*
DDoS *146*
DNSSEC *146*
URL Hiding *146*
Domain Grabbing *147*
Cybersquatting *147*
Email Attacks 147
Email Spoofing *147*
Spear Phishing *148*
Whaling *148*
Spam *148*
Wireless Attacks 148
Wardriving *149*
Warchalking *149*
Remote Attacks 149
Other Attacks 149
SYN ACK Attacks *149*
Session Hijacking *150*
Port Scanning *150*
Teardrop *150*
IP Address Spoofing *150*
Exam Preparation Tasks 151
Review All Key Topics 151
Define Key Terms 151
Review Questions 153
Answers and Explanations 155

Chapter 4 Information Security Governance and Risk Management 159

Foundation Topics 159

Security Principles and Terms 159

CIA 160

Vulnerability 160

Threat 161

Threat Agent 161

Risk 161

Exposure 161

Countermeasure 161

Due Care and Due Diligence 162

Job Rotation 163

Separation of Duties 163

Security Frameworks and Methodologies 163

ISO/IEC 27000 Series 164

Zachman Framework 166

The Open Group Architecture Framework (TOGAF) 168

Department of Defense Architecture Framework (DoDAF) 168

British Ministry of Defence Architecture Framework (MODAF) 168

Sherwood Applied Business Security Architecture (SABSA) 168

Control Objectives for Information and Related Technology (CobiT) 170

National Institute of Standards and Technology (NIST) Special Publication (SP) 170

Committee of Sponsoring Organizations (COSO) of the Treadway Commission Framework 171

Information Technology Infrastructure Library (ITIL) 172

Six Sigma 173

Capability Maturity Model Integration (CMMI) 174

Top-Down Versus Bottom-Up Approach 174

Security Program Life Cycle 174

Risk Assessment 175

Information and Asset (Tangible/Intangible) Value and Costs 177

Vulnerabilities and Threats Identification 177

Quantitative Risk Analysis 178

Qualitative Risk Analysis 179
Safeguard Selection 179
Total Risk Versus Residual Risk 180
Handling Risk 180
Risk Management Principles 181
Risk Management Policy 181
Risk Management Team 181
Risk Analysis Team 182
Information Security Governance Components 182
Policies 183
Organizational Security Policy 184
System-Specific Security Policy 185
Issue-Specific Security Policy 185
Policy Categories 185
Standards 185
Baselines 185
Guidelines 186
Procedures 186
Information Classification and Life Cycle 186
Commercial Business Classifications 186
Military and Government Classifications 187
Information Life Cycle 188
Security Governance Responsibilities and Roles 188
Board of Directors 188
Management 189
Audit Committee 189
Data Owner 190
Data Custodian 190
System Owner 190
System Administrator 190
Security Administrator 190
Security Analyst 191
Application Owner 191
Supervisor 191

User 191
Auditor 191
Third-Party Governance 191
Onsite Assessment 192
Document Exchange/Review 192
Process/Policy Review 192
Personnel Security (Screening, Hiring, and Termination) 192
Security Awareness Training 193
Security Budget, Metrics, and Effectiveness 194
Exam Preparation Tasks 195
Review All Key Topics 195
Complete the Tables and Lists from Memory 195
Define Key Terms 196
Review Questions 196
Answers and Explanations 198
Chapter 5 Software Development Security 203
Foundation Topics 203
System Development Life Cycle 203
Initiate 204
Acquire/Develop 204
Implement 205
Operate/Maintain 205
Dispose 205
Software Development Life Cycle 206
Gather Requirements 206
Design 207
Develop 207
Test/Validate 208
Release/Maintain 209
Change Management and Configuration Management 209
Software Development Security Best Practices 209
WASC 210
OWASP 210
BSI 210

ISO/IEC 27000 210
Software Development Methods 211
Build and Fix 211
Waterfall 212
V-Shaped 213
Prototyping 214
Incremental 214
Spiral 215
Rapid Application Development (RAD) 216
Agile 216
JAD 218
Cleanroom 218
CMMI 218
Programming Concepts 219
Machine Languages 219
Assembly Languages and Assemblers 219
High-level Languages, Compilers, and Interpreters 219
Object-Oriented Programming 220
Polymorphism 221
Cohesion 221
Coupling 221
Data Structures 221
Distributed Object-Oriented Systems 222
CORBA 222
COM and DCOM 222
OLE 223
Java 223
SOA 223
Mobile Code 223
Java Applets 223
ActiveX 224
Database Concepts and Security 224
DBMS Architecture and Models 224
Database Interface Languages 226

ODBC 226
JDBC 227
XML 227
OLE DB 227
Data Warehouses and Data Mining 227
Database Threats 228
Database Views 228
Database Locks 228
Polyinstantiation 228
OLTP ACID Test 229
Knowledge-Based Systems 229
Software Threats 230
Malware 230
Virus 230
Worm 231
Trojan Horse 231
Logic Bomb 232
Spyware/Adware 232
Botnet 232
Rootkit 233
Source Code Issues 233
Buffer Overflow 233
Escalation of Privileges 235
Backdoor 235
Malware Protection 235
Antivirus Software 235
Antimalware Software 236
Security Policies 236
Software Security Effectiveness 236
Certification and Accreditation 236
Auditing 237
Exam Preparation Tasks 237

Review All Key Topics 237
Define Key Terms 238
Complete the Tables and Lists from Memory 238
Review Questions 238
Answers and Explanations 240
Chapter 6 Cryptography 243
Foundation Topics 244
Cryptography Concepts 244
Cryptographic Life Cycle 246
Cryptography History 246
Julius Caesar and the Caesar Cipher 247
Vigenere Cipher 248
Kerckhoff's Principle 249
World War II Enigma 249
Lucifer by IBM 250
Cryptosystem Features 250
Authentication 250
Confidentiality 250
Integrity 251
Authorization 251
Non-repudiation 251
Encryption Systems 251
Running Key and Concealment Ciphers 251
Substitution Ciphers 252
Transposition Ciphers 253
Symmetric Algorithms 253
Stream-based Ciphers 254
Block Ciphers 255
Initialization Vectors (IVs) 255
Asymmetric Algorithms 255
Hybrid Ciphers 256
Substitution Ciphers 257
One-Time Pads 257
Steganography 258

Symmetric Algorithms 258
Digital Encryption Standard (DES) and Triple DES (3DES) 259
DES Modes 259
Triple DES (3DES) and Modes 262
Advanced Encryption Standard (AES) 263
IDEA 263
Skipjack 264
Blowfish 264
Twofish 264
RC4/RC5/RC6 264
CAST 265
Asymmetric Algorithms 265
Diffie-Hellman 266
RSA 267
El Gamal 267
ECC 267
Knapsack 268
Zero Knowledge Proof 268
Message Integrity 268
Hash Functions 269
One-Way Hash 269
MD2/MD4/MD5/MD6 271
SHA/SHA-2/SHA-3 271
HAVAL 272
RIPEMD-160 272
Tiger 272
Message Authentication Code 273
HMAC 273
CBC-MAC 274
CMAC 274
Digital Signatures 274
Public Key Infrastructure 275
Certification Authority (CA) and Registration Authority (RA) 275
OCSP 276

- Certificates 276
- Certificate Revocation List (CRL) 277
- PKI Steps 277
- Cross-Certification 278

Key Management 278

Trusted Platform Module (TPM) 279

Encryption Communication Levels 280

- Link Encryption 280
- End-to-End Encryption 281

E-mail Security 281

- PGP 281
- MIME and S/MIME 282
- Quantum Cryptography 282

Internet Security 282

- Remote Access 283
- SSL/TLS 283
- HTTP, HTTPS, and SHTTP 284
- SET 284
- Cookies 284
- SSH 285
- IPsec 285

Cryptography Attacks 286

- Ciphertext-Only Attack 287
- Known Plaintext Attack 287
- Chosen Plaintext Attack 287
- Chosen Ciphertext Attack 287
- Social Engineering 287
- Brute Force 288
- Differential Cryptanalysis 288
- Linear Cryptanalysis 288
- Algebraic Attack 288
- Frequency Analysis 288
- Birthday Attack 289
- Dictionary Attack 289

Replay Attack 289
Analytic Attack 289
Statistical Attack 289
Factoring Attack 289
Reverse Engineering 289
Meet-in-the-Middle Attack 290
Exam Preparation Tasks 290
Review All Key Topics 290
Complete the Tables and Lists from Memory 290
Define Key Terms 291
Review Questions 291
Answers and Explanations 293
Chapter 7 Security Architecture and Design 297
Foundation Topics 297
Security Model Concepts 297
Confidentiality 297
Integrity 297
Availability 298
Defense in Depth 298
System Architecture 298
System Architecture Steps 299
ISO/IEC 42010:2011 299
Computing Platforms 300
Mainframe/Thin Clients 300
Distributed Systems 300
Middleware 301
Embedded Systems 301
Mobile Computing 301
Virtual Computing 301
Security Services 302
Boundary Control Services 302
Access Control Services 302
Integrity Services 303

Cryptography Services 303

Auditing and Monitoring Services 303

System Components 303

CPU and Multiprocessing 303

Memory and Storage 304

Input/Output Devices 307

Operating Systems 307

Multitasking 308

Memory Management 309

System Security Architecture 310

Security Policy 310

Security Requirements 310

Security Zones 311

Security Architecture Frameworks 312

Zachman Framework 312

SABSA 312

TOGAF 312

ITIL 313

Security Architecture Documentation 314

ISO/IEC 27000 Series 314

CobiT 314

Security Model Types and Security Models 314

Security Model Types 315

State Machine Models 315

Multilevel Lattice Models 315

Matrix-Based Models 315

Noninference Models 316

Information Flow Models 316

Security Models 317

Bell-LaPadula Model 317

Biba Model 318

Clark-Wilson Integrity Model 319

Lipner Model 320

Brewer-Nash (Chinese Wall) Model 320

Graham-Denning Model 320
Harrison-Ruzzo-Ullman Model 321
Security Modes 321
Dedicated Security Mode 321
System High Security Mode 321
Compartmented Security Mode 321
Multilevel Security Mode 321
Assurance 322
System Evaluation 322
TCSEC 322
Rainbow Series 323
Orange Book 323
Red Book 326
ITSEC 326
Common Criteria 328
Certification and Accreditation 329
Security Architecture Maintenance 330
Security Architecture Threats 330
Maintenance Hooks 331
Time-of-Check/Time-of-Use Attacks 331
Web-Based Attacks 332
XML 332
SAML 332
OWASP 333
Server-Based Attacks 333
Data Flow Control 333
Database Security 333
Inference 333
Aggregation 334
Contamination 334
Data Mining Warehouse 334
Distributed Systems Security 334
Cloud Computing 335

Grid Computing 335

Peer-to-Peer Computing 335

Exam Preparation Tasks 336

Review All Key Topics 336

Complete the Tables and Lists from Memory 336

Define Key Terms 336

Review Questions 337

Answers and Explanations 339

Chapter 8 Operations Security 343

Foundation Topics 343

Operations Security Concepts 343

Need-to-Know/Least Privilege 343

Separation of Duties 344

Job Rotation 344

Sensitive Information Procedures 344

Record Retention 345

Monitor Special Privileges 345

Resource Protection 345

Protecting Tangible and Intangible Assets 346

Facilities 346

Hardware 346

Software 347

Information Assets 347

Asset Management 348

Redundancy and Fault Tolerance 348

Backup and Recovery Systems 348

Identity and Access Management 349

Media Management 349

SAN 353

NAS 353

HSM 353

Media History 354

Media Labeling and Storage 354

Sanitizing and Disposing of Media *355*
Network and Resource Management *355*
Operations Processes 356
Incident Response Management 356
Change Management 357
Configuration Management 358
Patch Management 359
Audit and Review 360
Operations Security Threats and Preventative Measures 361
Clipping Levels 361
Deviations from Standards 361
Unusual or Unexplained Events 361
Unscheduled Reboots 362
Trusted Recovery 362
Trusted Paths 362
Input/Output Controls 362
System Hardening 362
Vulnerability Management Systems 363
IDS/IPS 363
Monitoring and Reporting 363
Antimalware/Antivirus 364
Exam Preparation Tasks 364
Review All Key Topics 364
Complete the Tables and Lists from Memory 364
Define Key Terms 364
Review Questions 365
Answers and Explanations 367
Chapter 9 Business Continuity and Disaster Recovery 369
Foundation Topics 369
Business Continuity and Disaster Recovery Concepts 369
Disruptions 370
Disasters 370
Technological Disasters *371*
Man-made Disasters *371*

Natural Disasters 371

Disaster Recovery and the Disaster Recovery Plan (DRP) 371

Continuity Planning and the Business Continuity Plan (BCP) 372

Business Impact Analysis (BIA) 372

Contingency Plan 372

Availability 373

Reliability 373

Business Impact Analysis (BIA) Development 373

Identify Critical Processes and Resources 374

Identify Outage Impacts, and Estimate Downtime 374

Identify Resource Requirements 375

Identify Recovery Priorities 376

Recoverability 376

Fault Tolerance 376

Business Continuity Scope and Plan 376

Personnel Components 377

Project Scope 377

Business Continuity Steps 377

Preventive Controls 378

Redundant Systems, Facilities, and Power 379

Fault-Tolerant Technologies 379

Insurance 379

Data Backup 380

Fire Detection and Suppression 380

Create Recovery Strategies 380

Categorize Asset Recovery Priorities 381

Business Process Recovery 382

Facility Recovery 382

Hot Site 383

Cold Site 383

Warm Site 384

Tertiary Site 384

Reciprocal Agreements 384

Redundant Sites 385

Supply and Technology Recovery 385
Hardware Backup 386
Software Backup 386
Human Resources 387
Supplies 387
Documentation 388
User Environment Recovery 388
Data Recovery 388
Data Backup Types and Schemes 389
Electronic Backup 392
High Availability 392
Training Personnel 393
Critical Teams and Duties 393
Damage Assessment Team 394
Legal Team 394
Media Relations Team 394
Recovery Team 395
Relocation Team 395
Restoration Team 395
Salvage Team 395
Security Team 395
BCP Testing 396
Checklist Test 396
Table-top Exercise 396
Structured Walk-Through Test 397
Simulation Test 397
Parallel Test 397
Full-Interruption Test 397
Functional Drill 397
Evacuation Drill 397
BCP Maintenance 398
Exam Preparation Tasks 398
Review All Key Topics 398
Complete the Tables and Lists from Memory 399
Exam Preparation Tasks 398

Define Key Terms 399

Review Questions 399

Answers and Explanations 401

Chapter 10 Legal, Regulations, Investigations, and Compliance 405

Foundation Topics 406

Computer Crime Concepts 406

Computer-Assisted Crime 406

Computer-Targeted Crime 406

Incidental Computer Crime 406

Computer Prevalence Crime 407

Hackers Versus Crackers 407

Major Legal Systems 407

Civil Code Law 408

Common Law 408

Criminal Law 408

Civil/Tort Law 408

Administrative/Regulatory Law 409

Customary Law 409

Religious Law 409

Mixed Law 409

Intellectual Property Law 409

Patent 410

Trade Secret 410

Trademark 411

Copyright 411

Software Piracy and Licensing Issues 412

Internal Protection 413

Privacy 413

Personally Identifiable Information (PII) 414

Laws and Regulations 414

Sarbanes-Oxley (SOX) Act 415

Health Insurance Portability and Accountability Act (HIPAA) 415

Gramm-Leach-Bliley Act (GLBA) of 1999 415

Computer Fraud and Abuse Act (CFAA) 416

Federal Privacy Act of 1974 *416*
Federal Intelligence Surveillance Act (FISA) of 1978 *416*
Electronic Communications Privacy Act (ECPA) of 1986 *416*
Computer Security Act of 1987 *417*
United States Federal Sentencing Guidelines of 1991 *417*
Communications Assistance for Law Enforcement Act (CALEA) of 1994 *417*
Personal Information Protection and Electronic Documents Act (PIPEDA) *417*
Basel II *417*
Payment Card Industry Data Security Standard (PCI DSS) *418*
Federal Information Security Management Act (FISMA) of 2002 *418*
Economic Espionage Act of 1996 *418*
USA PATRIOT Act *418*
Health Care and Education Reconciliation Act of 2010 *418*
Employee Privacy Issues and Expectation of Privacy *419*
European Union *419*
Export/Import Issues *420*
Compliance 420
Liability 420
Due Diligence Versus Due Care 421
Negligence 421
Liability Issues 422
Incident Response 423
Event Versus Incident 423
Incident Response Team and Incident Investigations 424
Rules of Engagement, Authorization, and Scope 424
Incident Response Procedures 424
Forensic and Digital Investigations 425
Identify Evidence 427
Preserve and Collect Evidence 427
Examine and Analyze Evidence 428
Present Findings 428
Decide 428
IOCE/SWGDE 429

Crime Scene 429
MOM 429
Chain of Custody 430
Interviewing 430
Evidence 430
Five Rules of Evidence 431
Types of Evidence 431
Best Evidence 432
Secondary Evidence 432
Direct Evidence 432
Conclusive Evidence 432
Circumstantial Evidence 432
Corroborative Evidence 433
Opinion Evidence 433
Hearsay Evidence 433
Surveillance, Search, and Seizure 433
Media Analysis 434
Software Analysis 434
Network Analysis 435
Hardware/Embedded Device Analysis 435
Security Professional Ethics 435
$(ISC)^2$ Code of Ethics 436
Computer Ethics Institute 436
Internet Architecture Board 437
Organizational Ethics 437
Exam Preparation Tasks 437
Review All Key Topics 437
Define Key Terms 438
Review Questions 439
Answers and Explanations 441
Chapter 11 Physical (Environmental) Security 445
Foundation Topics 445
Geographical Threats 445
Internal Versus External Threats 445
Natural Threats 446

Hurricane/Tropical Storm *446*
Tornadoes *446*
Earthquakes *446*
Floods *447*
System Threats 447
Electrical *447*
Communications *447*
Utilities *448*
Man-Made Threats 449
Explosions *449*
Fire *449*
Vandalism *450*
Fraud *450*
Theft *450*
Collusion *451*
Politically Motivated Threats 451
Strikes *451*
Riots *451*
Civil Disobedience *452*
Terrorist Acts *452*
Bombing *452*
Site and Facility Design 453
Layered Defense Model 453
CPTED 453
Natural Access Control *453*
Natural Surveillance *454*
Natural Territorials Reinforcement *454*
Physical Security Plan 454
Deter Criminal Activity *454*
Delay Intruders *454*
Detect Intruders *455*
Assess Situation *455*
Respond to Intrusions and Disruptions *455*

Facility Selection Issues 455
Visibility 455
Surrounding Area and External Entities 456
Accessibility 456
Construction 456
Internal Compartments 457
Computer and Equipment Rooms 457
Perimeter Security 458
Gates and Fences 458
Barriers (Bollards) 458
Fences 459
Gates 459
Walls 460
Perimeter Intrusion Detection 460
Infrared Sensors 460
Electromechanical Systems 460
Photoelectric Systems 460
Acoustical Detection Systems 461
Wave Motion Detector 461
Capacitance Detector 461
CCTV 461
Lighting 461
Types of Systems 461
Types of Lighting 462
Patrol Force 462
Access Control 462
Building and Internal Security 463
Doors 463
Door Lock Types 463
Turnstiles and Mantraps 464
Locks 464
Biometrics 466
Glass Entries 466
Visitor Control 466

Equipment Rooms 467
Work Areas 467
Secure Data Center 467
Restricted Work Area 468
Environmental Security 468
Fire Protection 468
Fire Detection 468
Fire Suppression 468
Power Supply 470
Types of Outages 470
Preventative Measures 470
HVAC 471
Water Leakage and Flooding 471
Environmental Alarms 472
Equipment Security 472
Corporate Procedures 472
Tamper Protection 472
Encryption 472
Inventory 473
Physical Protection of Security Devices 473
Tracking Devices 473
Portable Media Procedures 473
Safes, Vaults, and Locking 473
Personnel Privacy and Safety 474
Exam Preparation Tasks 475
Review All Key Topics 475
Define Key Terms 475
Review Questions 476
Answers and Explanations 478
Glossary 481
Index 538
Appendix A Memory Tables On CD
Appendix B Memory Tables Answer Key On CD

About the Authors

Troy McMillan is a Product Developer and Technical Editor for Kaplan Cert Prep as well as a full time trainer and writer. He became a professional trainer 12 years ago teaching Cisco, Microsoft, CompTIA, and Wireless classes.

Troy's book *CCNA Essentials* by Sybex Publishing was released in November 2011. It has been chosen as the textbook for both online and instructor-led classes at several colleges in the United States.

Troy also is a courseware developer. Among the work he has done in this area is wireless training materials for Motorola in 2011 and instructor materials for a series of books by Sybex on Windows Server 2008 R2 in 2011.

Troy also teaches Cisco, Microsoft, CompTIA, and Security classes for several large corporate training companies. Among these are Global Knowledge and New Horizons.

He now creates certification practice tests and study guides for the Transcender and Self-Test brands. Troy lives in Atlanta, Georgia.

Troy's professional accomplishments include B.B.A., MCSE (NT/2000/ 2003, 2008), CCNA, CCNP, MCP+I, CNA, A+, Net+, MCT, Server+, I-Net+, MCSA, CIW p, CIWa, CIW security analyst, CWNA, CWSP, CWNT, CWNE, MCTS: Vista Configuration, MCITP: Enterprise Support Technician, MCITP: Server Administrator, MCITP: Consumer Support Technician, MCTS: Forefront Client and Server Configuration, MCTS: Business Desktop Deployment with BDD, MCTS: Office Project Server 2007, MCTS: Windows Active Directory: Configuration, MCTS: Applications Infrastructure: Configuration, MCTS: Network Infrastructure: Configuration, CCSI, and VCP.

Robin M. Abernathy has been working in the IT certification preparation industry at Kaplan IT Certification Preparation, the owners of the Transcender and Self Test brands, for more than a decade. Robin has written and edited certification preparation materials for many $(ISC)^2$, Microsoft, CompTIA, PMI, Cisco, and ITIL certifications and holds multiple IT certifications from these vendors.

Robin provides training on computer hardware and software, networking, security, and project management. Over the past couple years, she has ventured into the traditional publishing industry by technically editing several publications. More recently, she has presented at technical conferences and hosted webinars on IT certification topics.

Dedications

This is dedicated to my soulmate and wife, Heike. —Troy

For my husband Michael and my son Jonas. —Robin

Acknowledgments

From Troy: Special thanks to all that helped with this book, but especially to Dave Dusthimer for suggesting me for this book, to Betsy Brown for guiding us through the process, to Andrew Cupp and Allison Johnson for keeping us on schedule, and most of all to my co-author, Robin Abernathy.

From Robin: I would be remiss if I did not first of all mention my gratitude to God for blessing me throughout my life. I do nothing on my own. It is only through Him that I have the strength and wisdom to accomplish my goals.

When my father and his business partner asked me to take over a retail computer store in the mid-1990s, I had no idea that a BIG journey was just starting. So thanks, Wayne McDaniel (a.k.a. Dad) and Roy Green for seeing something in me that I didn't even see in myself and for taking a chance on a very green techie. Also, thanks to my mom, Lucille McDaniel, for supporting my career changes over the years, even if you didn't understand them. Thanks to Mike White for sharing your knowledge and giving me a basis on which to build my expertise over the coming years. Thanks to Zackie Bosarge, a great mentor who gave me my first "real" job in the IT field at Alabama Institute for the Deaf and Blind.

Thanks also to my little family, my husband Michael and my son Jonas. Thanks for being willing to have Friday night fun nights without me while I spent my extra time knee-deep in CISSP topics. Thanks to Michael for always making sure that I knew that everything was easier on a Mac. Thanks to Jonas for keeping mom humble by making sure she understood that you couldn't see why someone was paying mom to write a book where Percy Jackson or Harry Potter was NOT the main character. I love you both immensely!

Pearson has put together an outstanding team to help me on my journey. Thanks to Betsy Brown, Andrew Cupp, Allison Johnson, and Seth Kerney for making this first foray into authorship so easy for me. Also, thanks to Chris Crayton and Brock Pearson for providing such a great technical review and giving us suggestions on improvement.

Finally, a thank you to Troy McMillan for contacting me when this book idea was first introduced to you. It has been a great journey! We make a great team, and I look forward to working with you on future projects.

It is my wish that you, the reader, succeed in your IT certification and career goals. I wish you the very best.

About the Technical Editors

Chris Crayton is an author, technical consultant, trainer, and SkillsUSA technology competition judge. Formerly, he worked as a computer technology and networking instructor at Keiser University; as network administrator for Protocol, a global electronic customer relationship management (eCRM) company; and at Eastman Kodak as a computer and network specialist. Chris has authored several print and online books on PC repair, CompTIA A+, CompTIA Security+, and Microsoft Windows. He has also served as technical editor and content contributor on numerous technical titles for several of the leading publishing companies. He holds MCSE, A+, and Network+ certifications.

Brock Pearson has more than 20 years of experience in the Information Technology/Information Security industry specializing in cybersecurity and cyberoperations. As a manager in a large security practice, Brock has assisted fortune 100 companies and government agencies, in the United States and abroad, in their efforts to defend themselves against hackers, cybertheft, and cyberterrorism. Brock Pearson has developed and delivered customized, technical security training; enhanced security policies, processes, and procedures; and integrated multiple information technologies to facilitate a holistic and proactive security posture for his clients.

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.

We welcome your comments. You can email or write us directly to let us 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 we cannot help you with technical problems related to the topic of this book.

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

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
ATTN: Reader Feedback
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.

Introduction

$(ISC)^2$ Certified Information Systems Security Professional (CISSP) Certification is widely respected in the IT world as a premier security certification.

$(ISC)^2$ CISSP Certification is designed to be a vendor-neutral exam that measures your knowledge of industry-standard security practices.

Goals and Methods

The number one goal of this book is a simple one: to help you pass the current version of the $(ISC)^2$ CISSP Certification exam. The CISSP Certification stresses a Common Body of Knowledge (CBK) that defines the architecture, design, management, risk, and controls necessary to secure a business environment. The Candidate Information Bulletin (CIB) from $(ISC)^2$ provides an exam blueprint, reference list, format description, and registration policies.

To aid you in mastering and understanding the CISSP objectives, this book uses the following methods:

- The beginning of each chapter defines the topics to be covered in the chapter.
- The body of the chapter explains the topics from a hands-on and a theory-based standpoint. This includes in-depth descriptions, tables, and figures geared to build your knowledge so that you can pass the exam. The chapters are broken down into several topics each.
- The key topics indicate important figures, tables, and lists of information that you should know for the exam. They are interspersed throughout each chapter and are listed in table format at the end of each chapter.
- You can find memory tables and lists on the disc as Appendix A, "Memory Tables," and Appendix B, "Memory Tables Answer Key." Use them to help memorize important information.
- Key terms without definitions are listed at the end of each chapter. Write down the definition of each term, and check your work against the complete key terms in the Glossary.
- Each chapter includes review questions meant to gauge your knowledge of the subjects. If an answer to a question doesn't come readily to you, be sure to review that portion of the chapter. The answers with detailed explanations are at the end of each chapter.
- The disc accompanying this book includes two practice exams that test you on all the CISSP exam topics.

Who Should Read This Book?

The (ISC)² CISSP exam measures the necessary competencies for a full-time security professional with a minimum of five years in two or more of the 10 domains in the CISSP CBK or a minimum of four years in two or more domains with a four-year college degree. This book is written for people who have that amount of experience working with information systems security.

Readers will range from people who are attempting to attain a position in the IT security field to people who want to keep their skills sharp or perhaps retain their job due to a company policy that mandates that they take the new exams. However, readers with no knowledge of IT security should be cautioned against attempting the CISSP certification as their first IT certification. Beginners would be best served to pursue a more basic IT certification, such as CompTIA's A+, Network+, or Security+ certification.

This book is also aimed at the reader who wants to acquire additional certifications beyond the CISSP certification. The book is designed in such a way to offer easy transition to future certification studies.

Strategies for Exam Preparation

Strategies for exam preparation will vary depending on your existing knowledge. We recommend that you have access to as many devices and hardware as possible so as to be able to examine the different security methods mentioned in this book. A hands-on approach will really help to reinforce the ideas and concepts expressed in the book. However, not everyone has access to this equipment, so the next best step you can take is to read through the chapters in this book, jotting down notes with key concepts or configurations on a separate notepad. Each chapter contains a quiz that you can use to test your knowledge of the chapter's topics. It's located near the end of the chapter.

After you have read through the book, look at the current exam blueprint for the (ISC)² CISSP Certification Exam from https://www.isc2.org/exam-outline/Default.aspx. If there are any areas shown in the blueprint that you would still like to study, find those sections in the book and review them.

When you feel confident in your skills, attempt the practice exams included on the disc with this book. As you work through the practice exams, note the areas where you lack confidence and review those concepts in the book. After you review the areas, work through the practice exam a second time and rate your skills. Keep in mind that the more you work through the practice exam, the more familiar the questions will become.

$(ISC)^2$ CISSP Exam Objectives

Table I-1 lists the objectives for the CISSP exam. Each domain has been given its own chapter in this book.

Table I-1 $(ISC)^2$ CISSP Exam Objectives

Objective
1.0 Access Control
1.1 Control access by applying the following concepts/methodologies/techniques: ■ Policies ■ Types of controls (preventive, detective, corrective, etc.) ■ Techniques (that is, non-discretionary, discretionary, and mandatory) ■ Identification and authentication ■ Decentralized/distributed access control techniques ■ Authorization mechanisms ■ Logging and monitoring
1.2 Understand access control attacks: ■ Threat modeling ■ Asset valuation ■ Vulnerability analysis ■ Access aggregation
1.3 Assess effectiveness of access controls: ■ User entitlement ■ Access review and audit
1.4 Identity and access provisioning life cycle (e.g., provisioning, review, revocation)
2.0 Telecommunications and Network Security
2.1 Understand secure network architecture and design (e.g., IP and non-IP protocols, segmentation): ■ OSI and TCP/IP models ■ IP networking ■ Implications of multilayer protocols
2.2 Securing network components: ■ Hardware (e.g., modems, switches, routers, wireless access points) ■ Transmission media (e.g., wired, wireless, fiber) ■ Network access control devices (e.g., firewalls, proxies) ■ End-point security

2.3 Establish secure communication channels (e.g., VPN, TLS/SSL, VLAN): ■ Voice (e.g., POTS, PBX, VoIP) ■ Multimedia collaboration (e.g., remote meeting technology, instant messaging) ■ Remote access (e.g., screen scraper, virtual application/desktop, telecommuting) ■ Data communications
2.4 Understand network attacks (e.g., DDOS, spoofing)
3.0 Information Security Governance and Risk Management
3.1 Understand and align security function to goals, mission, and objectives of the organization
3.2 Understand and apply security governance: ■ Organizational processes (e.g., acquisitions, divestitures, governance committees) ■ Security roles and responsibilities ■ Legislative and regulatory compliance ■ Privacy requirements compliance ■ Control frameworks ■ Due care ■ Due diligence
3.3 Understand and apply concepts of confidentiality, integrity, and availability
3.4 Develop and implement security policy: ■ Security policies ■ Standards/baselines ■ Procedures ■ Guidelines ■ Documentation
3.5 Manage the information life cycle (e.g., classification, categorization, ownership)
3.6 Manage third-party governance (e.g., onsite assessment, document exchange and review, process/policy review)
3.7 Understand and apply risk management concepts: ■ Identify threats and vulnerabilities ■ Risk assessment/analysis (qualitative, quantitative, hybrid) ■ Risk assignment/acceptance ■ Countermeasure selection ■ Tangible and intangible asset valuation
3.8 Manage personnel security: ■ Employment candidate screening (e.g., reference checks, education verification) ■ Employment agreements and policies ■ Employee termination processes ■ Vendor, consultant, and contractor controls

3.9 Develop and manage security education, training, and awareness
3.10 Manage the security function: ■ Budget ■ Metrics ■ Resources ■ Develop and implement security strategies ■ Assess the completeness and effectiveness of the security program
4.0 Software Development Security
4.1 Understand and apply security in the software development life cycle: ■ Development life cycle ■ Maturity models ■ Operation and maintenance ■ Change management
4.2 Understand the environment and security controls: ■ Security of the software environment ■ Security issues of programming languages ■ Security issues in source code (e.g., buffer overflow, escalation of privilege, backdoor) ■ Configuration management
4.3 Assess the effectiveness of software security
5.0 Cryptography
5.1 Understand the application and use of cryptography: ■ Data at rest (that is, hard drive) ■ Data in transit (that is, "on the wire")
5.2 Understand the cryptographic life cycle (e.g., cryptographic limitations, algorithm/ protocol governance)
5.3 Understand encryption concepts: ■ Foundational concepts ■ Symmetric cryptography ■ Asymmetric cryptography ■ Hybrid cryptography ■ Message digests ■ Hashing
5.4 Understand key management processes: ■ Creation/distribution ■ Storage/destruction ■ Recovery ■ Key escrow

5.5 Understand digital signatures
5.6 Understand non-repudiation
5.7 Understand methods of cryptanalytic attacks: ■ Chosen plaintext ■ Social engineering for key discovery ■ Brute force (i.e., rainbow tables, specialized/scalable architecture) ■ Cipher-text only ■ Known plaintext ■ Frequency analysis ■ Chosen ciphertext ■ Implementation attacks
5.8 Use cryptography to maintain network security
5.9 Use cryptography to maintain application security
5.10 Understand Public Key Infrastructure (PKI)
5.11 Understand certificate-related issues
5.12 Understand information hiding alternatives (e.g., steganography, watermarking)
6.0 Security Architecture and Design
6.1 Understand the fundamental concepts of security models (e.g., Confidentiality, Integrity, and Multilevel models)
6.2 Understand the components of information systems security evaluation models: ■ Product evaluation models (e.g., common criteria) ■ Industry and international security implementation guidelines (e.g., PCI-DSS, ISO)
6.3 Understand security capabilities of information systems (e.g., memory protection, virtualization, trusted platform module)
6.4 Understand the vulnerabilities of security architectures: ■ System (e.g., covert channels, state attacks, emanations) ■ Technology and process integration (e.g., single point of failure, service-oriented architecture)
6.5 Understand software and system vulnerabilities and threats: ■ Web-based (e.g., XML, SAML, OWASP) ■ Client-based (e.g., applets) ■ Server-based (e.g., data flow control) ■ Database security (e.g., inference, aggregation, data mining, warehousing) ■ Distributed systems (e.g., cloud computing, grid computing, peer to peer)
6.6 Understand countermeasure principles (e.g., defense in depth)

7.0 Security Operations
7.1 Understand security operations concepts: ■ Need-to-know/least privilege ■ Separation of duties and responsibilities ■ Monitor special privileges (e.g., operators, administrators) ■ Job rotation ■ Marking, handling, storing, and destroying of sensitive information ■ Record retention
7.2 Employ resource protection: ■ Media management ■ Asset management (e.g., equipment life cycle, software licensing)
7.3 Manage incident response: ■ Detection ■ Response ■ Reporting ■ Recovery ■ Remediation and review (e.g., root cause analysis)
7.4 Implement preventive measures against attacks (e.g., malicious code, zero-day exploit, denial of service)
7.5 Implement and support patch and vulnerability management
7.6 Understand change and configuration management (e.g., versioning, baselining)
7.7 Understand system resilience and fault tolerance requirements
8.0 Business Continuity and Disaster Recovery Planning
8.1 Understand business continuity requirements: ■ Develop and document project scope and plan
8.2 Conduct business impact analysis: ■ Identify and prioritize critical business functions ■ Determine maximum tolerable downtime and other criteria ■ Assess exposure to outages (e.g., local, regional, global) ■ Define recovery objectives
8.3 Develop a recovery strategy: ■ Implement a backup storage strategy (e.g., offsite storage, electronic vaulting, tape rotation) ■ Recovery site strategies

8.4 Understand disaster recovery process: ■ Response ■ Personnel ■ Communications ■ Assessment ■ Restoration ■ Provide training
8.5 Exercise, assess, and maintain the plan (e.g., version control, distribution)
9.0 Legal, Regulations, Investigations, and Compliance
9.1 Understand legal issues that pertain to information security internationally: ■ Computer crime ■ Licensing and intellectual property (e.g., copyright, trademark) ■ Import/export ■ Trans-border data flow ■ Privacy
9.2 Understand professional ethics: ■ (ISC)^2 Code of Professional Ethics ■ Support organization's code of ethics
9.3 Understand and support investigations: ■ Policy, roles, and responsibilities (e.g., rules of engagement, authorization, scope) ■ Incident handling and response ■ Evidence collection and handling (e.g., chain of custody, interviewing) ■ Reporting and documenting
9.4 Understand forensic procedures: ■ Media analysis ■ Network analysis ■ Software analysis ■ Hardware/embedded device analysis
9.5 Understand compliance requirements and procedures: ■ Regulatory environment ■ Audits ■ Reporting
9.6 Ensure security in contractual agreements and procurement processes (e.g., cloud computing, outsourcing, vendor governance)

10.0 Physical (Environmental) Security
10.1 Understand site and facility design considerations
10.2 Support the implementation and operation of perimeter security (e.g., physical access control and monitoring, audit trails/access logs)
10.3 Support the implementation and operation of internal security (e.g., escort requirements/ visitor control, keys and locks)
10.4 Support the implementation and operation of facilities security (e.g. technology convergence): ■ Communications and server rooms ■ Restricted and work area security ■ Data center security ■ Utilities and Heating, Ventilation, and Air Conditioning (HVAC) considerations ■ Water issues (e.g., leakage, flooding) ■ Fire prevention, detection, and suppression
10.5 Support the protection and securing of equipment
10.6 Understand personnel privacy and safety (e.g., duress, travel, monitoring)

Pearson IT Certification Practice Test Engine and Questions on the Disc

The disc in the back of the book includes the Pearson IT Certification Practice Test engine—software that displays and grades a set of exam-realistic multiple-choice questions. Using the Pearson IT Certification Practice Test engine, you can either study by going through the questions in Study Mode or take a simulated exam that mimics real exam conditions.

The installation process requires two major steps: installing the software and then activating the exam. The disc in the back of this book has a recent copy of the Pearson IT Certification Practice Test engine. The practice exam—the database of exam questions—is not on the disc.

NOTE The cardboard disc case in the back of this book includes the disc and a piece of paper. The paper lists the activation code for the practice exam associated with this book. Do not lose the activation code. On the opposite side of the paper from the activation code is a unique, one-time use coupon code for the purchase of the Premium Edition eBook and Practice Test.

Install the Software from the Disc

The Pearson IT Certification Practice Test is a Windows-only desktop application. You can run it on a Mac using a Windows Virtual Machine, but it was built specifically for the PC platform.

The software installation process is pretty routine compared with other software installation processes. If you have already installed the Pearson IT Certification Practice Test software from another Pearson product, there is no need for you to reinstall the software. Simply launch the software on your desktop and proceed to activate the practice exam from this book by using the activation code included in the disc sleeve.

The following steps outline the installation process:

1. Insert the disc into your PC.
2. The software that automatically runs is the Pearson software to access and use all disc-based features, including the exam engine and the disc-only appendixes. From the main menu, click the option to Install the Exam Engine.
3. Respond to Windows prompts as with any typical software installation process.

The installation process gives you the option to activate your exam with the activation code supplied on the paper in the disc sleeve. This process requires that you establish a Pearson website login. You need this login to activate the exam, so please do register when prompted. If you already have a Pearson website login, there is no need to register again. Just use your existing login.

Activate and Download the Practice Exam

After the exam engine is installed, you should then activate the exam associated with this book (if you did not do so during the installation process) as follows:

1. Start the Pearson IT Certification Practice Test software from the Windows Start menu or from your desktop shortcut icon.
2. To activate and download the exam associated with this book, from the My Products or Tools tab, select the Activate button.
3. At the next screen, enter the Activation Key from the paper inside the cardboard disc holder in the back of the book. When it's entered, click the Activate button.
4. The activation process downloads the practice exam. Click Next and then click Finish.

After the activation process finishes, the My Products tab should list your new exam. If you do not see the exam, make sure you have selected the My Products tab on the menu. At this point, the software and practice exam are ready to use. Simply select the exam, and click the Open Exam button.

To update a particular exam you have already activated and downloaded, simply select the Tools tab, and select the Update Products button. Updating your exams will ensure you have the latest changes and updates to the exam data.

If you want to check for updates to the Pearson Cert Practice Test exam engine software, simply select the Tools tab, and select the Update Application button. This will ensure you are running the latest version of the software engine.

Activating Other Exams

The exam software installation process, and the registration process, must happen only once. Then, for each new exam, only a few steps are required. For instance, if you buy another new Pearson IT Certification Cert Guide or Cisco Press Official Cert Guide, extract the activation code from the disc sleeve in the back of that book—you don't even need the disc at this point. From there, all you need to do is start the exam engine (if not still up and running), and perform steps 2–4 from the previous list.

Premium Edition

In addition to the two free practice exams provided on the disc, you can purchase two additional exams with expanded functionality directly from Pearson IT Certification. The Premium Edition eBook and Practice Test for this title contains two additional full practice exams as well as an eBook (in both PDF and ePub format). In addition, the Premium Edition title also has remediation for each question to the specific part of the eBook that relates to that question.

If you have purchased the print version of this title, you can purchase the Premium Edition at a deep discount. There is a coupon code in the disc sleeve that contains a one-time use code as well as instructions for where you can purchase the Premium Edition.

This page intentionally left blank

This chapter covers the following topics:

- **OSI model:** An explanation of the functions of the seven layers of the OSI model
- **TCP/IP model:** A discussion of the TCP/IP model and its relationship to the OSI model
- **Common TCP/UDP ports:** A description of the function of port numbers and common standard ports
- **IP addressing:** A look at both logical and physical addressing systems and their interrelationship in routing and switching
- **Network transmission:** An examination of the processes used to transfer data across various media types
- **Cabling:** Types of bounded media, their characteristics, and proper use
- **Network topologies:** A survey of both logical and physical network topologies
- **Network technologies:** A discussion of the various technologies used to accomplish networking
- **Network protocols/services:** The functions of the major network protocols and services that provide network functionality
- **Network routing:** An explanation of how static and dynamic routing works and a discussion of the major interior and exterior routing protocols
- **Network devices:** Covers the function and placement of major network devices

CHAPTER 3

Telecommunications and Network Security

- **Network types:** An explanation of local area network types including MAN, WAN, LAN, extranet, and intranet
- **WAN technologies:** A discussion of the various methods of connecting local area networks (LANs) with wide area networks (WANs)
- **Remote connection technologies:** A description of the methods of connecting remote users and networks to the LAN and the Internet
- **Wireless networks:** Covers the types of wireless networks and the processes required to secure them
- **Network threats:** An introduction to the various security threats facing networks

Sensitive data must be protected from unauthorized access when the data is at rest (on a hard drive) and in transit (moving through a network). Moreover, sensitive communications of other types such as emails, instant messages, and phone conversations must also be protected from prying eyes and ears. Many communication processes send information in a form that can be read and understood if captured with a protocol analyzer or sniffer.

In today's communication world, assume that your communications are being captured regardless of how unlikely you think that might be. You should also take steps to protect or encrypt the transmissions so they will be useless to anyone capturing them. This chapter covers the protection of wired and wireless transmissions and of the network devices that perform the transmissions, as well as some networking fundamentals required to understand transmission security.

Foundation Topics

OSI Model

A complete understanding of networking requires an understanding of the Open Systems Interconnect (OSI) model. Created in the 1980s by the International Standards Organization (ISO) as a part of its mission to create a protocol set to be used as a standard for all vendors, it breaks the communication process into layers. Although the ensuing protocol set did not catch on as a standard Transmission Control Protocol/Internet Protocol [TCP/IP] was adopted), the model has guided the development of technology since its creation. It also has helped generations of students understand the network communication process between two systems.

The OSI model breaks up the process into seven layers or modules. The benefits of doing this are

- It breaks up the communication process into layers with standardized interfaces between the layers, allowing for changes and improvements on one layer without necessitating changes on other layers.
- It provides a common framework for hardware and software developers, fostering interoperability.

The goal of this open systems architecture is that no vendor owns it and it acts as a blueprint or model for developers to work with. Various protocols operate at different layers of this model. A protocol is a set of communication rules two systems must both use and understand to communicate. Some protocols depend on other protocols for services, and as such, these protocols work as a team to get transmissions done, much like the team at the post office that gets your letters delivered. Some people sort, others deliver, and still others track lost shipments.

The OSI model and the TCP/IP model, explained in the next section, are often both used to describe the process called *packet creation* or *encapsulation*. Until a packet is created to hold the data, it cannot be sent on the transmission medium.

With a modular approach, it becomes possible for a change in a protocol or the addition of a new protocol to be accomplished without having to rewrite the entire protocol *stack* (a term for all the protocols that work together at all layers). The model has seven layers. This section discusses each layer's function and its relationship to the layer above and below it in the model. The layers are often referred to by their number with the numbering starting at the bottom of the model at layer 1, the Physical layer.

The process of creating a packet or encapsulation begins at layer 7, the Application layer rather than layer 1, so we discuss the process starting at layer 7 and work down the model to layer 1, the Physical layer, where the packet is sent out on the transmission medium.

Application Layer

The Application layer (layer 7) is where the encapsulation process begins. This layer receives the raw data from the application in use and provides services, such as file transfer and message exchange to the application (and thus the user). An example of a protocol that operates at this layer is Hypertext Transfer Protocol (HTTP), which is used to transfer web pages across the network. Other examples of protocols that operate at this layer are DNS queries, FTP transfers, and SMTP email transfers.

The user application interfaces with these application protocols through a standard interface called an Application Programming Interface (API). The Application layer protocol receives the raw data and places it in a container called a protocol data unit (PDU). When the process gets down to layer 4, these PDUs have standard names, but at layers 5–7 we simply refer to the PDU as “data.”

Presentation Layer

The information that is developed at layer 7 is then handed to layer 6, the Presentation layer. Each layer makes no changes to the data received from the layer above it. It simply adds information to the developing packet. In the case of the Presentation layer, information is added that standardizes the formatting of the information if required.

Layer 6 is responsible for the manner in which the data from the Application layer is represented (or presented) to the Application layer on the destination device (explained more fully in the section “Encapsulation”). If any translation between formats is required, it will take care of it. It also communicates the type of data within the packet and the application that might be required to read it on the destination device.

Session Layer

The Session layer or layer 5 is responsible for adding information to the packet that makes a communication session between a service or application on the source device possible with the same service or application on the destination device. Do not confuse this process with the one that establishes a session between the two physical devices. That occurs not at this layer but at layers 3 and 4. This session is built and closed after the physical session between the computers has taken place.

The application or service in use is communicated between the two systems with an identifier called a port number. This information is passed on to the Transport layer, which also makes use of these port numbers.

Transport Layer

The protocols that operate at the Transport layer (layer 4) work to establish a session between the two physical systems. The service provided can be either connection-oriented or connectionless, depending on the transport protocol in use. The "TCP/IP Model" section (TCP/IP being the most common standard networking protocol in use) discusses the specific transport protocols used by TCP/IP in detail.

The Transport layer receives all the information from layers 7, 6, and 5 and adds information that identifies the transport protocol in use and the specific port number that identifies the required layer 7 protocol. At this layer, the PDU is called a segment because this layer takes a large transmission and segments it into smaller pieces for more efficient transmission on the medium.

Network Layer

At layer 3 or the Network layer, information required to route the packet is added. This is in the form of a source and destination logical address (meaning one that is assigned to a device in some manner and can be changed). In TCP/IP, this is in terms of a source and destination IP address. An IP address is a number that uniquely differentiates a host from all other devices on the network. It is based on a numbering system that makes it possible for computers (and routers) to identify whether the destination device is on the local network or on a remote network. Any time a packet needs to be sent to a different network or subnet (IP addressing is covered later in the chapter), it must be routed and the information required to do that is added here. At this layer, the PDU is called a packet.

Data Link Layer

The Data Link layer is responsible for determining the destination physical address. Network devices have logical addresses (IP addresses) and the network interfaces they possess have a physical address (Media Access Control [MAC] address), which is permanent in nature. When the transmission is handed off from routing device to routing device, at each stop this source and destination address pair changes, whereas the source and destination logical addresses (in most cases IP addresses) do not. This layer is responsible for determining what those MAC addresses should be at each hop (router interface) and adding them to this part of the packet. The later section "TCP/IP Model" covers how this resolution is performed in TCP/IP. After this is done, we call the PDU a frame.

Something else happens at this layer that is unique to this layer. Not only is a layer 2 header placed on the packet but also a trailer at the "end" of the frame. Information contained in the trailer is used to verify that none of the data contained has been altered or damaged en route.

Physical Layer

Finally, the packet (or frame as it is called at layer 2) is received by the Physical layer (layer 1). Layer 1 is responsible for turning the information into bits (ones and zeros) and sending it out on the medium. The way in which this is accomplished can vary according to the media in use. For example, in a wired network, the ones and zeros are represented as electrical charges. In wireless, they are represented by altering the radio waves. In an optical network, they are represented with light.

The ability of the same packet to be routed through various media types is a good example of the independence of the layers. As a PDU travels through different media types, the physical layer will change but all the information in layers 2–7 will not. Similarly, when a frame crosses routers or hops, the MAC addresses change but none of the information in layers 3–7 changes. The upper layers depend on the lower layers for various services but the lower layers leave the upper layer information unchanged.

Figure 3-1 shows common protocols mapped to the OSI model.

The next section covers another model that perhaps more accurately depicts what happens in a TCP/IP network. Because TCP/IP is the standard now for transmission, comparing these two models is useful. Although they have a different number of layers and some of the layer names are different, they describe the same process of packet creation or encapsulation.

Key Topic

OSI model
7. Application layer
NNTP • SIP • SSI • DNS • FTP • Gopher • HTTP • NFS • NTP • SMPP • SMTP * SNMP • Telnet • DHCP • Netconf • (more)
6. Presentation layer
MIME • XDR
5. Session layer
Named pipe • NetBIOS • SAP • PPTP • RTP • SOCKS • SPDY • TLS/SSL
4. Transport layer
TCP • UDP • SCTP • DCCP • SPX
3. Network layer
IP • (IPv4 • IPV6) • ARP • ICMP • IPsec • IGMP • IPX • Apple Talk
2. Data link layer
ATM • SDLC • HDLC • CSLIP • SLIP • GFP • PLIP • IEEE 802.2 • LLC • L2TP • IEEE 802.3 • Frame Relay • ITU-T G.hn DLL • PPP • X.25
1. Physical layer
EIA/TIA-232 • EIA/TIA-449 • ITU-T V-Series • 1.430 • 1.431 • PDH • SONET/SDH • PON • OTN • DSL • IEEE 802.3 - IEEE 802.11 • IEEE 802.15 • IEEE 802.16 • IEEE 1394 • ITU-T G.hn PHY • USB • Bluetooth • RS-232 • RS-449

Figure 3-1 Protocol Mappings

Multi-Layer Protocols

Many protocols, such as FTP and DNS, operate on a single layer of the OSI model. However, many protocols operate at multiple layers of the OSI model. The best example is TCP/IP, the networking protocol used on the Internet and on the vast majority of local area networks (LANs). In fact, this protocol has its own model that describes the layers on which it operates and the parts of the protocol that operate on each layer. The next section covers this model and the protocol it was designed to describe.

TCP/IP Model

The protocols developed when the OSI model was developed (sometimes referred to as OSI protocols) did not become the standard for the Internet. The Internet as we know it today has its roots in a wide area network (WAN) developed by the Department of Defense (DoD) with TCP/IP being the protocol developed for that network. The Internet is a global network of public networks and Internet Service Providers (ISPs) throughout the world.

Although the OSI model is still often referenced, of the protocols themselves only X.400, X.500, and IS-IS have had much lasting impact. For that reason, a second model exists based on TCP/IP. In a discussion of this model, the protocols that are part of what is called the TCP/IP suite can be mapped to the layer on which they perform their function.

This model bears many similarities to the OSI model, which is not unexpected because they both describe the process of packet creation or encapsulation. The difference is that the OSI model breaks the process into seven layers, whereas the TCP/IP model breaks it into four. If you examine them side by side, however, it becomes apparent that many of the same functions occur at the same layers, while the TCP/IP model combines the top three layers of the OSI model into one and the bottom two layers of the OSI model into one. Figure 3-2 show the two models next to one another.

Key Topic

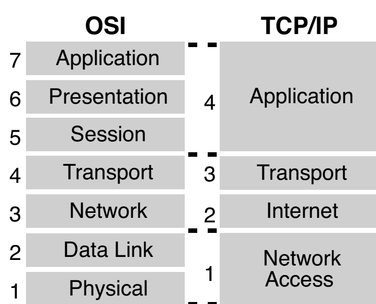

Figure 3-2 TCP/IP and OSI Models

The TCP/IP model has only four layers and is useful to study because it focuses its attention on TCP/IP. This section explores those four layers and their functions and relationships to one another and to layers in the OSI model.

Application Layer

Although the Application layer in the TCP/IP model has the same name as the top layer in the OSI model, the Application layer in the TCP/IP model encompasses all the functions performed in layers 5–7 in the OSI model. Not all functions map perfectly because both are simply conceptual models. Within the Application layer, applications create user data and communicate this data to other processes or applications on another host. For this reason, it is sometimes also referred to as the process-to-process layer.

Examples of protocols that operate at this layer are SMTP, FTP, SSH, and HTTP. These protocols are discussed in the section "Network Protocols/Services" later in this chapter. In general, however, these are usually referred to as higher layer protocols that perform some specific function, whereas protocols in the TCP/IP suite that operate at the Transport and Internet layers perform location and delivery service on behalf of these higher layer protocols.

A port number identifies to the receiving device these upper layer protocols and the programs on whose behalf they function. The number identifies the protocol or service. Many port numbers have been standardized. For example, Domain Name System (DNS) is identified with the standard port number of 53. The "Common TCP/UDP Ports" section covers these port numbers in more detail.

Transport Layer

The Transport layers of the OSI model and the TCP/IP model perform the same function, which is to open and maintain a connection between hosts. This must occur before the session between the processes can occur as described in the Application layer section and can be done in TCP/IP in two ways: connectionless and connection-oriented. A connection-oriented transmission means that a connection will be established before any data is transferred, whereas in a connectionless transmission this is not done. One of two different transport layer protocols is used for each process. If a connection-oriented transport protocol is required, Transmission Control Protocol (TCP) will be used. If the process will be connectionless, User Datagram Protocol (UDP) is used.

Application developers can choose to use either TCP or UDP as the Transport layer protocol used with the application. Regardless of which transport protocol is used, the application or service will be identified to the receiving device by its port number and the transport protocol (UDP or TCP). Port numbers are discussed in more detail in the section "Common TCP/UDP Ports" later in this chapter.

Although TCP provides more functionality and reliability, the overhead required by this protocol is substantial when compared to UDP. This means that a much higher percentage of the packet consists of the header when using TCP than when using UDP. This is necessary to provide the fields required to hold the information needed to provide the additional services. Figure 3-3 shows a comparison of the size of the two respective headers.

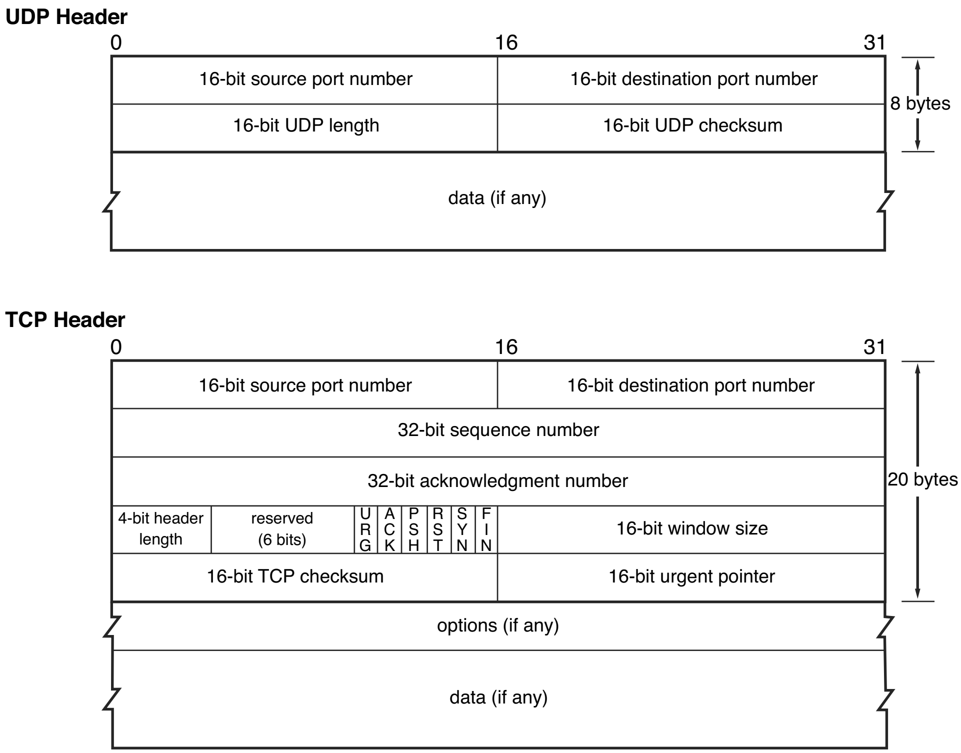

Figure 3-3 TCP/IP and UDP Headers

When an application is written to use TCP, a state of connection is established between the two hosts before any data is transferred. This occurs using a process known as the TCP three-way handshake. This process is followed exactly, and no data is transferred until it is complete. Figure 3-4 shows the steps in this process. The steps are as follows:

1. The initiating computer sends a packet with the SYN flag set (one of the fields in the TCP header), which indicates a desire to create a connection.
2. The receiving host acknowledges receiving this packet and indicates a willingness to create a state of connection by sending back a packet with both the SYN and ACK flags set.
3. The first host acknowledges completion of the connection process by sending a final packet back with only the ACK flag set.

Key Topic

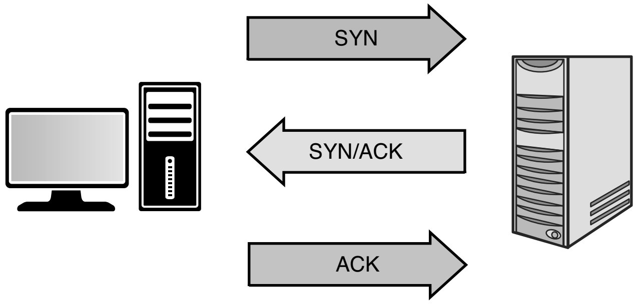

Figure 3-4 TCP Three-Way Handshake

So what exactly is gained by using the extra overhead to use TCP? The following are examples of the functionality provided with TCP:

- **Guaranteed delivery:** If the receiving host does not specifically acknowledge receipt of each packet, the sending system will resend the packet.
- **Sequencing:** In today's routed networks, the packets might take many different routes to arrive and might not arrive in the order in which they were sent. A sequence number added to each packet allows the receiving host to reassemble the entire transmission using these numbers.
- **Flow control:** The receiving host has the capability of sending the acknowledgement packets back to signal the sender to slow the transmission if it cannot process the packets as fast as they are arriving.

Many applications do not require the services provided by TCP or cannot tolerate the overhead required by TCP. In these cases the process will use UDP, which sends on a "best effort" basis with no guarantee of delivery. In many cases some of these functions are provided by the Application layer protocol itself rather than relying on the Transport layer protocol.

Internet Layer

The Transport layer can neither create a state of connection nor send using UDP until the location and route to the destination are determined, which occurs on the Internet layer. The four protocols in the TCP/IP suite that operate at this layer are

- **Internet Protocol (IP):** Responsible for putting the source and destination IP addresses in the packet and for routing the packet to its destination.
- **Internet Control Message Protocol (ICMP):** Used by the network devices to send messages regarding the success or failure of communications and used by humans for troubleshooting. When you use the PING or TRACEROUTE commands, you are using ICMP.

- **Internet Group Management Protocol (IGMP):** Used when multicasting, which is a form of communication whereby one host sends to a group of destination hosts rather than a single host (called a unicast transmission) or to all hosts (called a broadcast transmission).
- **Address Resolution Protocol (ARP):** Resolves the IP address placed in the packet to a physical or layer 2 address (called a MAC address in Ethernet).

The relationship between IP and ARP is worthy of more discussion. IP places the source and destination IP addresses in the header of the packet. As we saw earlier, when a packet is being routed across a network, the source and destination IP addresses never change but the layer 2 or MAC address pairs change at every router hop. ARP uses a process called the ARP broadcast to learn the MAC address of the interface that matches the IP address of the next hop. After it has done this, a new layer 2 header is created. Again, nothing else in the upper layer changes in this process, just layer 2.

That brings up a good point concerning the mapping of ARP to the TCP/IP model. Although we generally place ARP on the Internet layer, the information it derives from this process is placed in the Link layer or layer 2, the next layer in our discussion.

Just as the Transport layer added a header to the packet, so does the Internet layer. One of the improvements made by IPv6 is the streamlining of the IP header. Although the same information is contained in the header and the header is larger, it has a much simpler structure. Figure 3-5 shows a comparison of the two.

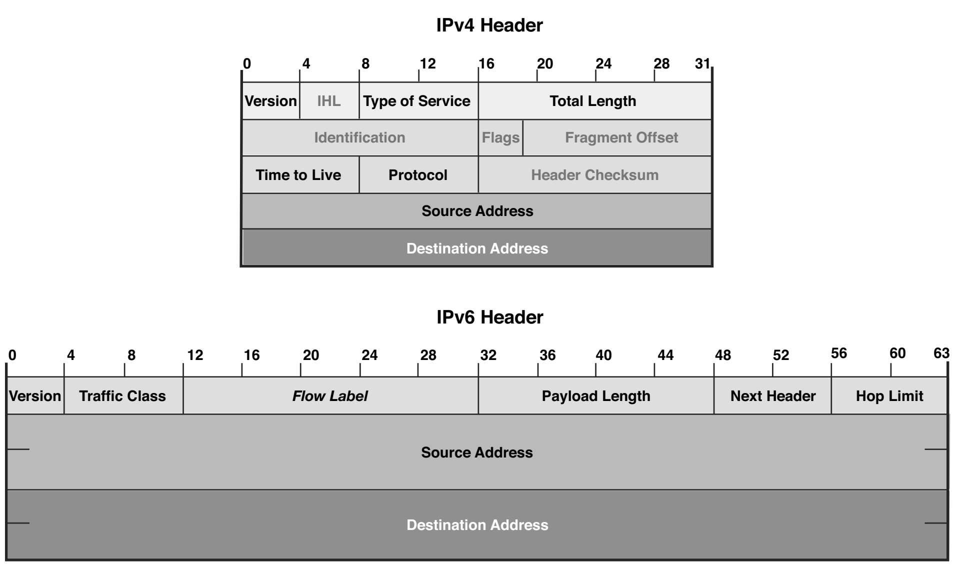

Figure 3-5 IPv6 and IPv4 Headers

Link Layer

The Link layer of the TCP/IP model provides the services provided by both the Data Link and the Physical layers in the OSI model. The source and destination MAC addresses are placed in this layer's header. A trailer is also placed on the packet at this layer with information in the trailer that can be used to verify the integrity of the data.

This layer is also concerned with placing the bits on the medium, as discussed in the section on the OSI model earlier in this chapter. Again, the exact method of implementation varies with the physical transmission medium. It might be in terms of electrical impulses, light waves, or radio waves.

Encapsulation

In either model as the packet is created, information is added to the header at each layer and then a trailer is placed on the packet before transmission. This process is called *encapsulation*. Intermediate devices, such as routers and switches, only read the layers of concern to that device (for a switch, layer 2 and for a router, layer 3). The ultimate receiver strips off the entire header with each layer, making use of the information placed in the header by the corresponding layer on the sending device. This process is called *de-encapsulation*. Figure 3-6 shows a visual representation of encapsulation.

Key Topic

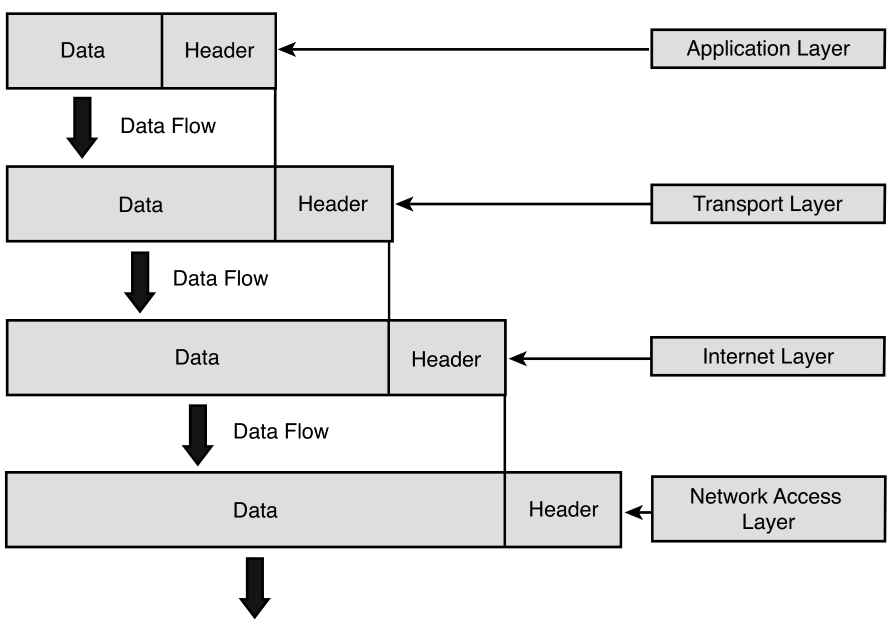

Figure 3-6 Encapsulation and De-encapsulation

Common TCP/UDP Ports

When the Transport layer learns the required port number for the service or application required on the destination device from the Application layer, it is recorded in the header as either a TCP or UDP port number. Both UDP and TCP use 16 bits in the header to identify these ports. These port numbers are software based or logical, and there are 65,535 possible numbers. Port numbers are assigned in various ways, based on three ranges:

- System or well-known ports (0–1023)
- User Ports (1024–49151)
- Dynamic and/or Private Ports (49152–65535)

System Ports are assigned by the Internet Engineering Task Force (IETF) for standards-track protocols, as per [RFC6335]. User ports can be registered with the Internet Assigned Numbers Authority (IANA) and assigned to the service or application using the "Expert Review" process, as per [RFC6335]. Dynamic ports are used by source devices as source ports when accessing a service or application on another machine. For example, if computer A is sending an FTP packet, the destination port will be the well-known port for FTP and the source will be selected by the computer randomly from the dynamic range.

The combination of the destination IP address and the destination port number is called a *socket*. The relationship between these two values can be understood if viewed through the analogy of an office address. The office has a street address but the address also must contain a suite number as there could be thousands (in this case 65,535) suites in the building. Both are required to get the information where it should go.

As a security professional, you should be aware of well-known port numbers of common services. In many instances, firewall rules and access control lists (ACLs) are written or configured in terms of the port number of what is being allowed or denied rather than the name of the service or application. Table 3-1 lists some of the more important port numbers. Some use more than one port.

Table 3-1 Common TCP/UDP Port Numbers

Key Topic

Application Protocol	Transport Protocol	Port Number
Telnet	TCP and UDP	23
SMTP	UDP	25
HTTP	TCP	80
SNMP	TCP and UDP	161 and 162

Application Protocol	Transport Protocol	Port Number
FTP	TCP and UDP	21 and 20
POP3	TCP and UDP	110
DNS	TCP and UDP	53
DHCP	UDP	67 and 68
SSH	TCP	22
LDAP	TCP and UDP	389

Logical and Physical Addressing

During the process of encapsulation at layer 3 of the OSI model, IP places source and destination IP addresses in the packet. Then at layer 2, the matching source and destination MAC addresses that have been determined by ARP are placed in the packet. IP addresses are examples of logical addressing, and MAC addresses are examples of physical addressing. IP addresses are considered logical because these addresses are administered by humans and can be changed at any time. MAC addresses on the other hand are assigned permanently to the interface cards of the devices when the interfaces are manufactured. It is important to note, however, that although these addresses are permanent, they can be spoofed. When this is done, however, the hacker is not actually changing the physical address, but rather telling the interface to place a different MAC address in the layer 2 headers.

This section discusses both address types with a particular focus on how IP addresses are used to create separate networks or subnets in the larger network. It also discusses how IP addresses and MAC addresses are related and used during a network transmission.

IPv4

IPv4 addresses are 32 bits in length and can be represented in either binary or in dotted-decimal format. The number of possible IP addresses using 32 bits can be calculated by raising the number 2 (the number of possible values in the binary number system) to the 32nd power. The result is 4,294,967,296, which on the surface appears to be enough IP addresses. But with the explosion of the Internet and the increasing number of devices that require an IP address, this number has proven to be insufficient.

Due to the eventual exhaustion of the IPv4 address space, several methods of preserving public IP addresses (more on that in a bit, but for now these are addresses that are legal to use on the Internet) have been implemented, including the use of private addresses and Network Address Translation (NAT), both discussed in the following sections. The ultimate solution lies in the adoption of IPv6, a new system that uses 128 bits and allows for enough IP addresses for each man, woman, and child on the planet to have as many IP addresses as the entire IPv4 numbering space. IPv6 is discussed later in this section.

IP addresses that are written in dotted-decimal format, the format in which humans usually work with them, have four fields called octets separated by dots or periods. Each field is called an octet because when we look at the addresses in binary format, we devote 8 bits in binary to represent each decimal number that appears in the octet when viewed in dotted-decimal format. Therefore, if we look at the address 216.5.41.3, four decimal numbers are separated by dots, where each would be represented by 8 bits if viewed in binary. The following is the binary version of this same address:

11011000.00000101.00101001.00000011

There are 32 bits in the address, 8 in each octet.

The structure of IPv4 addressing lends itself to dividing the network into subdivisions called subnets. Each IP address also has a required companion value called a subnet mask. The subnet mask is used to specify which part of the address, is the *network* part and which part is the *host*. The network part, on the left side of the address, determines on which network the device resides whereas the host portion on the right identifies the device on that network. Figure 3-7 shows the network and host portion of the three default classes of IP address.

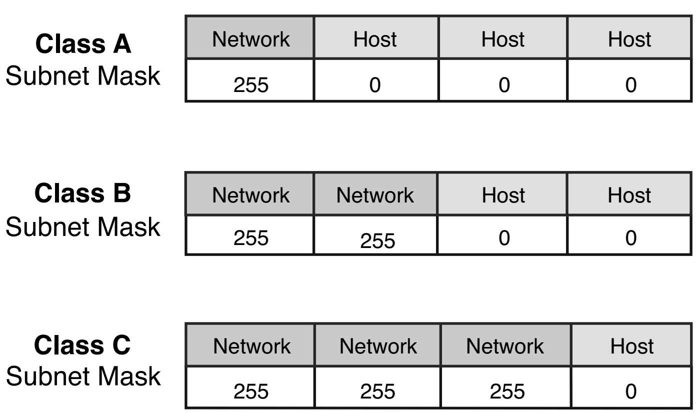

Figure 3-7 Network and Host Bits

When the IPv4 system was first created, there were only three default subnet masks. This yielded only three sizes of networks, which later proved to be inconvenient and wasteful of public IP addresses. Eventually a system called Classless Interdomain Routing (CIDR) was adopted that uses subnet masks that allow you to make subnets or subdivisions out of the major classful networks possible before CIDR. CIDR is beyond the scope of the exam but it is worth knowing about. You can find more information about how CIDR works at http://searchnetworking.techtarget.com/definition/CIDR.

IP Classes

Classful subnetting (pre-CIDR) created five classes of networks. Each class represented a range of IP addresses. Table 3-2 shows the five classes. Only the first three (A, B, and C) are used for individual network devices. The other ranges are for special use.

Key Topic

Table 3-2 Classful Addressing

Class	Range	Mask	Initial Bit Pattern of First Octet	Network/Host Division
Class A	0.0.0.0 – 127.255.255.255	255.0.0.0	01	net.host.host.host
Class B	128.0.0.0 – 191.255.255.255	255.255.0.0	10	net.net.host.host
Class C	192.0.0.0 –223.255.255.255	255.255.255.0	11	net.net.net.host
Class D	224.0.0.0 – 239.255.255.255	Used for multicasting		
Class E	240.0.0.0 – 255.255.255.255	Reserved for research		

As you can see, the key value that changes as you move from one class to another is the value of the first octet (the one on the far left). What might not be immediately obvious is that as you move from one class to another, the dividing line between the host portion and network portion also changes. This is where the subnet mask value comes in. When the mask is overlaid with the IP addresses (thus we call it a mask), every octet in the subnet mask where there is a 255 is a network portion and every octet where there is a 0 is a host portion. Another item to mention is that each class has a distinctive pattern in the first two bits of the first octet. For example, ANY IP address that begins with 01 in the first bit positions MUST be in Class A, also indicated in Table 3-2.

The significance of the network portion is that two devices must share the same values in the network portion to be in the same network. If they do not, they will not be able to communicate.

Public Versus Private IP Addresses

The initial solution used (and still in use) to address the exhaustion of the IPv4 space involved the use of private addresses and NAT. Three ranges of IP addresses were set aside to be used ONLY within private networks and are NOT routable on the Internet. RFC 1918 set aside the IP address ranges in Table 3-3 to be used for this purpose. Because these addresses are not routable on the public network, they must be translated to public addresses before being sent to the Internet. This process, called NAT is discussed in the next section.

Table 3-3 Address Classes

Key Topic

Class	Range
Class A	10.0.0.0 – 10.255.255.255
Class B	172.16.0.0 – 172.31.255.255
Class C	192.168.0.0 – 192.168.255.255

NAT

Network Address Translation (NAT) is a service that can be supplied by a router or by a server. The device that provides the service stands between the LAN and the Internet. When packets need to go to the Internet, the packets go through the NAT service first. The NAT service changes the private IP address to a public address that is routable on the Internet. When the response is returned from the Web, the NAT service receives it, translates the address back to the original private IP address, and sends it back to the originator.

This translation can be done on a one-to-one basis (one private address to one public address), but to save IP addresses, usually the NAT service will represent the entire private network with a single public IP address. This process is called Port Address Translation (PAT). This name comes from the fact that the NAT service keeps the private clients separate from one another by recording their private address and the source port number (usually a unique number) selected when the packets were built.

Allowing NAT to represent an entire network (perhaps thousands of computers) with a single public address has been quite effective in saving public IP addresses.

However, many applications do not function properly through NAT, and thus it has never been seen as a permanent solution to resolving the lack of IP addresses. That solution is IPv6.

IPv4 Versus IPv6

IPv6 was developed to more cleanly address the issue of the exhaustion of the IPv4 space. Although private addressing and the use of NAT have helped to delay the inevitable, the use of NAT introduces its own set of problems. The IPv6 system uses 128 bits so it creates such a large number of possible addresses that it is expected to suffice for many, many years.

The details of IPv6 are beyond the scope of the exam but these addresses look different than IPv4 addresses because they use a different format and use the hexadecimal number system, so there are letters and numbers in them such as you would see in a MAC address (discussed in the next section). There are eight fields separated by colons, not dots. Here is an example address:

2001:00000:4137:9e76:30ab:3035:b541:9693

Many of the security features that were add-ons to IPv4 (such as IPsec) have been built into IPv6, increasing its security. Moreover, while Dynamic Host Configuration Protocol (DHCP) can be used with IPv6, IPv6 provides a host the ability to locate its local router, configure itself, and discover the IP addresses of its neighbors. Finally, broadcast traffic is completely eliminated in IPv6 and replaced by multicast communications.

MAC Addressing

All the discussion about addressing thus far has been addressing that is applied at layer 3, which is IP addressing. At layer 2, physical addresses reside. In Ethernet, these are called Media Access Control (MAC) addresses. They are called physical addresses because these 48-bit addresses expressed in hexadecimal are permanently assigned to the network interfaces of devices. Here is an example of a MAC address:

01:23:45:67:89:ab

As a packet is transferred across a network, at every router hop and then again when it arrives at the destination network, the source and destination MAC addresses change. ARP resolves the next hop address to a MAC address using a process called the ARP broadcast. MAC addresses are unique. This comes from the fact that each manufacturer has a different set of values assigned to it at the beginning of the address called the Organizationally Unique Identifier (OUI). Each manufacturer ensures that it assigns no duplicate within its OUI. The OUI is the first three bytes of the MAC address.

Network Transmission

Data can be communicated across a variety of media types, using several possible processes. These communications can also have a number of characteristics that need to be understood. This section discusses some of the most common methods and their characteristics.

Analog Versus Digital

Data can be represented in various ways on a medium. On a wired medium, the data can be transmitted in either analog or digital format. Analog represents the data as sound and is used in analog telephony. Analog signals differ from digital in that there are an infinite possible number of values. If we look at an analog signal on a graph, it looks like a wave going up and down. Figure 3-8 shows an analog waveform compared to a digital one.

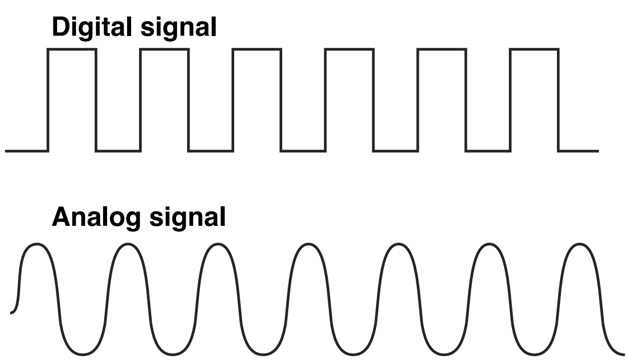

Figure 3-8 Digital and Analog Signals

Digital signaling on the other hand, which is the type used in most computer transmissions, does not have an infinite number of possible values, but only two: on and off. A digital signal shown on a graph exhibits a sawtooth pattern as shown in Figure 3-8. Digital signals are usually preferable to analog because they are more reliable and less susceptible to noise on the line. Transporting more information on the same line at a higher quality over a longer distance than with analog is also possible.

Asynchronous Versus Synchronous

When two systems are communicating, they not only need to represent the data in the same format (analog/digital) but they must also use the same synchronization technique. This process tells the receiver when a specific communication begins and ends so two-way conversations can happen without talking over one another. The two types of techniques are asynchronous transmission and synchronous transmission.

With asynchronous transmissions, the systems use *start* and *stop* bits to communicate when each byte is starting and stopping. This method also uses *parity bits* for the purpose of ensuring that each byte has not changed or been corrupted en route. This introduces additional overhead to the transmission.

Synchronous transmission uses a clocking mechanism to synch up the sender and receiver. Data is transferred in a stream of bits with no start, stop, or parity bits. This clocking mechanism is embedded into the layer 2 protocol. It uses a different form of error checking (cyclical redundancy check or CRC) and is preferable for high-speed, high-volume transmissions. Figure 3-9 shows a visual comparison of the two techniques.

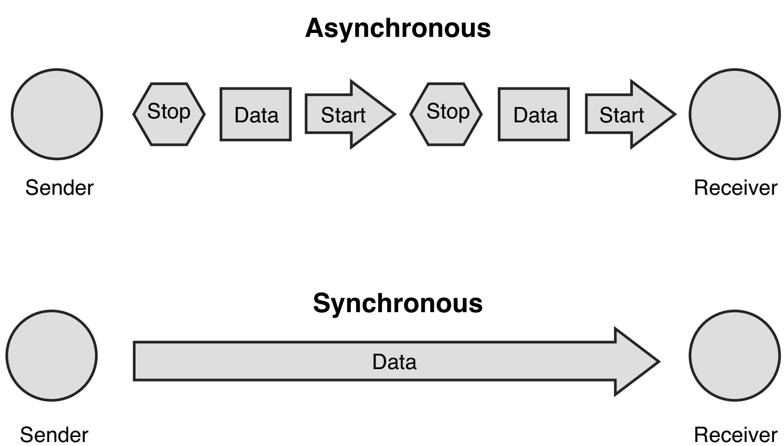

Figure 3-9 Asynchronous Versus Synchronous

Broadband Versus Baseband

All data transfers use a communication channel. Multiple transmissions might need to use the same channel. Sharing this medium can be done in two different ways: broadband or baseband. The difference is in how the medium is shared.

In baseband, the entire medium is used for a single transmission, and then multiple transmission types are assigned time slots to use this single circuit. This is called Time Division Multiplexing (TDM). Multiplexing is the process of using the same medium for multiple transmissions. The transmissions take turns rather than sending at the same time.

Broadband, on the other hand, divides the medium in different frequencies, a process called Frequency Division Multiplexing (FDM). This has the benefit of allowing true simultaneous use of the medium.

An example of broadband transmission is Digital Subscribers Line (DSL), where the phone signals are sent at one frequency and the computer data at another. This is why you can talk on the phone and use the Web at the same time. Figure 3-10 illustrates these two processes.

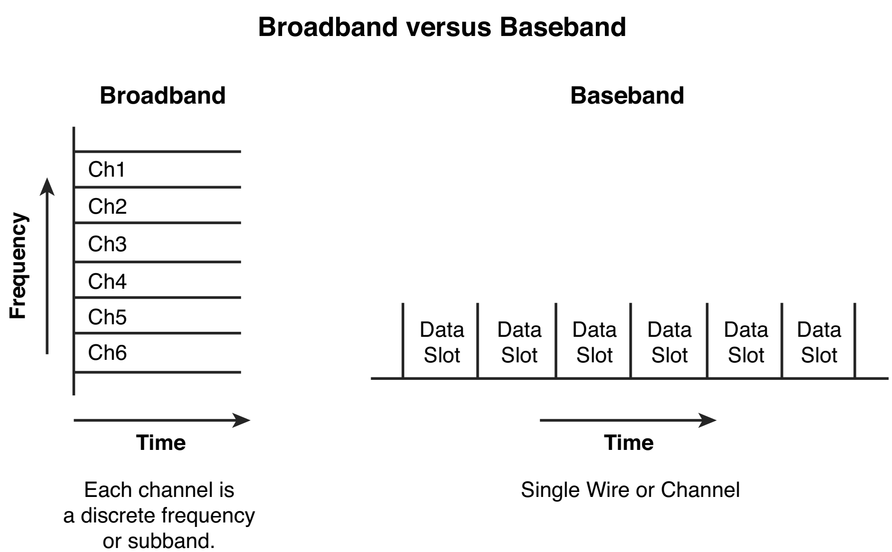

Figure 3-10 Broadband Versus Baseband

Unicast, Multicast, and Broadcast

When systems are communicating in a network, they might send out three types of transmissions. These methods differ in the scope of their reception as follow:

- **Unicast:** Transmission from a single system to another single system. It is considered one-to-one.
- **Multicast:** A signal is received by all others in a group called a multicast group. It is considered one-to-many.

- **Broadcast:** A transmission sent by a single system to all systems in the network. It is considered one-to-all.

Figure 3-11 illustrates the three methods.

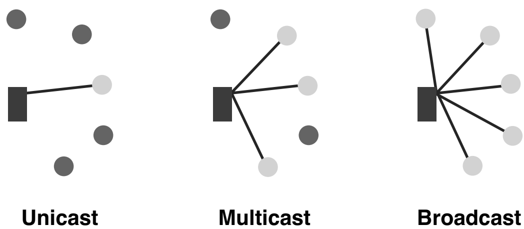

Figure 3-11 Unicast, Multicast, and Broadcast

Wired Versus Wireless

As you probably know by now, not all transmissions occur over a wired connection. Even within the category of wired connections, the way in which the ones and zeros are represented can be done in different ways. In a copper wire, the ones and zeros are represented with changes in the voltage of the signal, whereas in a fiberoptic cable, they are represented with manipulation of a light source (lasers or light-emitting diodes [LEDs]).

In wireless transmission, radios waves or light waves are manipulated to represent the ones and zeros. When infrared technology is used, this is done with infrared light. With wireless LANs (WLANs), radio waves are manipulated to represent the ones and zeros. These differences in how the bits are represented occur at the physical and data link layers of the OSI model. When a packet goes from a wireless section of the network to a wired section, these two layers are the only layers that change.

When a different physical medium is used, typically a different layer 2 protocol is called for. For example, while the data is traveling over the wired Ethernet network, the 802.3 standard is used. However, when the data gets to a wireless section of the network, it needs a different layer 2 protocol. Depending on the technology in use, it could be either 802.11 (WLAN) or 802.16 (WiMAX).

The ability of the packet to traverse various media types is just another indication of the independence of the OSI layers because the information in layers 3–7 remains unchanged regardless of how many layer 2 transitions must be made to get the data to its final destination.

Cabling

Cabling resides at the physical layer of the OSI model and simply provides a medium on which data can be transferred. The vast majority of data is transferred across cables of various types, including coaxial, fiberoptic, and twisted pair. Some of these cables represent the data in terms of electrical voltages whereas fiber cables manipulate light to represent the data. This section discusses each type.

You can compare cables to one another using several criteria. One of the criteria that is important with networking is the cable's susceptibility to *attenuation*. Attenuation occurs when the signal meets resistance as it travels through the cable. This weakens the signal, and at some point (different in each cable type), the signal is no longer strong enough to be read properly at the destination. For this reason, all cables have a maximum length. This is true regardless of whether the cable is fiberoptic or electrical.

Another important point of comparison between cable types is their data rate, which describes how much data can be sent through the cable per second. This area has seen great improvement over the years, going from rates of 10 Mbps in a LAN to 1000 Mbps in today's networks (and even higher rates in data centers).

Another consideration when selecting a cable type is the ease of installation. Some cable types are easier than others to install, and fiberoptic cabling requires a special skill set to install, raising its price of installation.

Finally (and most importantly for our discussion) is the security of the cable. Cables can leak or radiate information. Cables can also be tapped into by hackers if they have physical access to them. Just as the cable types can vary in allowable length and capacity, they can also vary in their susceptibility to these types of data losses.

Coaxial

One of the earliest cable types to be used for networking was coaxial, the same basic type of cable that brought cable TV to millions of homes. Although coaxial cabling is still used, due to its low capacity and the adoption of other cable types, its use is almost obsolete now in LANs.

Coaxial cabling comes in two types or thicknesses. The thicker type, called Thicknet, has an official name of 10Base5. This naming system, used for other cable types as well, imparts several facts about the cable. In the case of 10Bbase5, it means that it is capable of transferring 10 Mbps and can go roughly 500 meters. Thicknet uses two types of connectors: a vampire tap (named thusly because it has a spike that pierces the cable) and N-connectors.

Thinnet or 10Base2 also operates at 10 Mbps. Although when it was named it was anticipated to be capable of running 200 feet, this was later reduced to 185 feet. Both types are used in a bus topology (more on topologies in the section “Network Topologies” later in this chapter). Thinnet uses two types of connectors: BNC connectors and T-connectors.

Coaxial has an outer cylindrical covering that surrounds either a solid core wire (Thicknet) or a braided core (Thinnet). This type of cabling has been replaced over time with more capable twisted-pair and fiberoptic cabling. Coaxial cabling can be tapped, so physical access to this cabling should be restricted or prevented if possible. It should be out of sight if it is used. Figure 3-12 shows the structure of a coaxial cable.

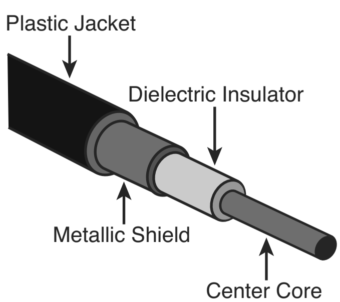

Figure 3-12 Coaxial Cabling

Another security problem with coax in a bus topology is that it is broadcast-based, which means a sniffer attached anywhere in the network can capture all traffic. In switched networks (more on that topic later in this chapter in the section “Network Devices”), this is not a consideration.

Twisted Pair

The most common type of network cabling found today is called twisted-pair cabling. It is called this because inside the cable are four pairs of smaller wires that are braided or twisted. This twisting is designed to eliminate a phenomenon called crosstalk, which occurs when wires that are inside a cable interfere with one another. The number of wire pairs that are used depends on the implementation. In some implementations, only two pairs are used, and in others all four wire pairs are used. Figure 3-13 shows the structure of a twisted-pair cable.

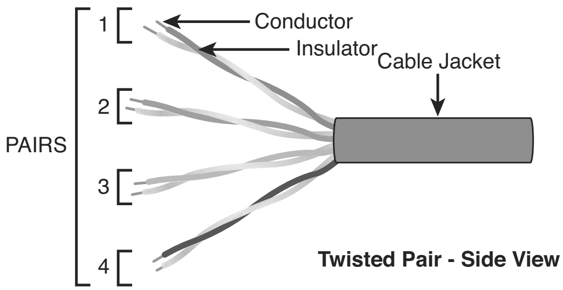

Figure 3-13 Twisted-Pair Cabling

Twisted-pair cabling comes in shielded (STP) and unshielded (UTP) versions. Nothing is gained from the shielding except protection from Radio Frequency Interference (RFI) and Electromagnetic Interference (EMI). RFI is interference from radio sources in the area, whereas EMI is interference from power lines. A common type of EMI is called common mode noise, which is interference that appears on both signal leads (signal and circuit return) or the terminals of a measuring circuit, and ground. If neither EMI nor RFI are a problem, nothing is gained by using STP, and it costs more.

The same naming system used with coaxial and fiber is used with twisted pair. The following are the major types of twisted pair you will encounter:

- **10BaseT:** Operates at 10 Mbps
- **100BaseT:** Also called Fast Ethernet; operates at 100 Mbps
- **1000BaseT:** Also called Gigabit Ethernet; operates at 1000 Mbps
- **10GBaseT:** Operates at 10 Gbps

Twisted-pair cabling comes in various capabilities and is rated in categories. Table 3-4 lists the major types and their characteristics. Regardless of the category, twisted-pair cabling can be run about 100 meters before attenuation degrades the signal.

Table 3-4 Twisted-Pair Categories

Key Topic

Name	Maximum Transmission Speed
Cat3	10 Mbps
Cat4	16 Mbps
Cat5	100 Mbps
Cat5e	100 Mbps

Name	Maximum Transmission Speed
Cat6	1 Gbps
Cat6a	10 Gbps

Fiberoptic

Fiberoptic cabling uses a source of light that shoots down an inner glass or plastic core of the cable. This core is covered by cladding that causes light to be confined to the core of the fiber. Figure 3-14 shows the structure of a fiberoptic cable.

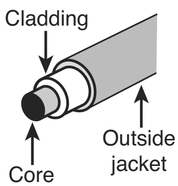

Figure 3-14 Fiberoptic Cabling

Fiberoptic cabling manipulates light such that it can be interpreted as ones and zeros. Because it is not electrically based, it is totally impervious to EMI, RFI, and crosstalk. Moreover, although not impossible, tapping or eavesdropping on a fiber cable is much more difficult. In most cases, attempting to tap into it results in a failure of the cable, which then becomes quite apparent to all.

Fiber comes in a single and multi-mode format. The single mode uses a single beam of light provided by a laser, goes the further of the two, and is the most expensive. Multi-mode uses several beams of light at the same time, uses LEDs, will not go as far, and is less expensive. Either type goes much further than electrical cabling in a single run and also typically provides more capacity. Fiber cabling has its drawbacks, however. It is the most expensive to purchase and the most expensive to install. Table 3-5 shows some selected fiber specifications and their theoretical maximum distances.

Table 3-5 Selected Fiber Specifications

Standard	Distance
100Base-FX	Maximum length is 400 meters for half-duplex connections (to ensure collisions are detected) or 2 kilometers for full-duplex.
1000Base-SX	550 meters

Standard	Distance
1000Base-LX	Multi-mode fiber (up to 550 m) or single-mode fiber (up to 2 km; can be optimized for longer distances, up to 10 km).
10GBase-LR	10 km
10GBase-ER	40 km

Network Topologies

Networks can be described by their logical topology (the data path used) and by their physical topology (the way in which devices are connected to one another. In most cases the logical topology and the physical topology will be the same but not in all. This section discusses both logical and physical network topologies.

Ring

A physical ring topology is one in which the devices are daisy-chained one to another in a circle or ring. If the network is also a logical ring, the data circles the ring from one device to another. Two technologies use this topology, Fiber Distributed Data Interface (FDDI) and Token Ring. Both these technologies are discussed in detail in the section, "Network Technologies." Figure 3-15 shows a typical ring topology.

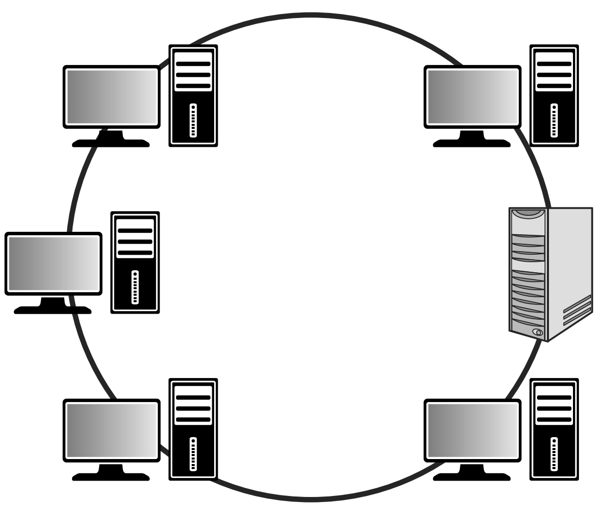

Figure 3-15 Ring Topology

One of the drawbacks of the ring topology is that if a break occurs in the line, all systems will be affected as the ring will be broken. As you will see in the section "Network Technologies," a FDDI network addresses this issue with a double ring for fault tolerance.

Bus

The bus topology was the earliest Ethernet topology used. In this topology, all devices are connected to a single line that has two definitive endpoints. The network does NOT loop back and form a ring. This topology is broadcast-based, which can be a security issue in that a sniffer or protocol analyzer connected at any point in the network will be capable of capturing all traffic. From a fault tolerance standpoint, the bus topology suffers the same danger as a ring. If a break occurs anywhere in the line, all devices are affected. Moreover, a requirement specific to this topology is that each end of the bus must be terminated. This prevents signals from "bouncing" back on the line causing collisions. (More on collisions later, but collisions require the collided packets to be sent again, lowering overall throughput.) If this termination is not done properly, the network will not function correctly. Figure 3-16 shows a bus topology.

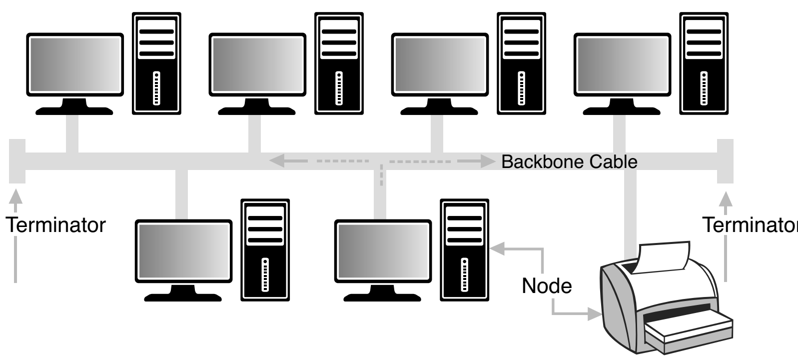

Figure 3-16 Bus Topology

Star

The star topology is the most common in use today. In this topology, all devices are connected to a central device (either a hub or a switch). One of the advantages of this topology is that if a connection to any single device breaks, ONLY that device is affected and no others. The downside of this topology is that a single point of failure (the hub or switch) exists. If the hub or switch fails, all devices are affected. Figure 3-17 shows a star topology.

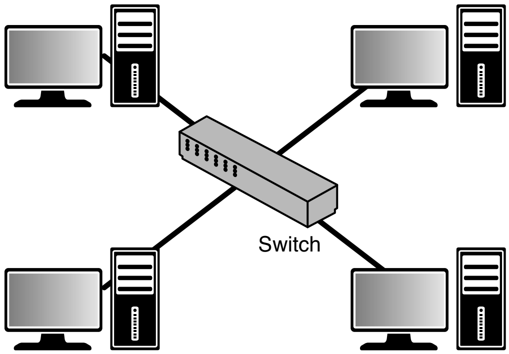

Figure 3-17 Star Topology

Mesh

Although the mesh topology is the most fault tolerant of any discussed thus far, it is also the most expensive to deploy. In this topology, all devices are connected to all other devices. This provides complete fault tolerance but also requires multiple interfaces and cables on each device. For that reason, it is deployed only in rare circumstances where such an expense is warranted. Figure 3-18 shows a mesh topology.

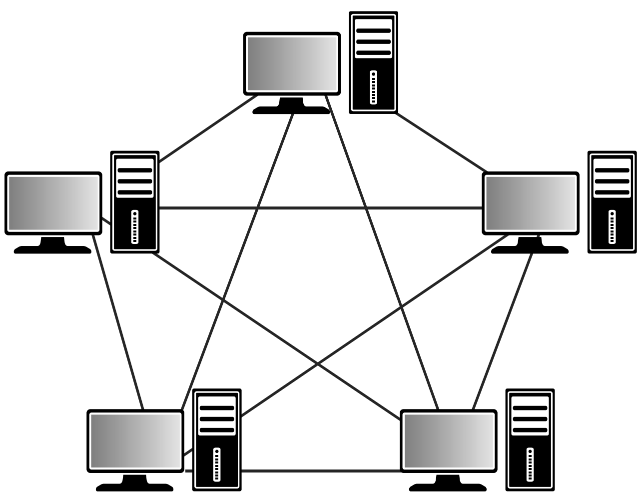

Figure 3-18 Mesh Topology

Hybrid

In many cases an organization's network is a combination of these network topologies, or a hybrid network. For example, one section might be a star that connects to a bus network or a ring network. Figure 3-19 shows an example of a hybrid network.

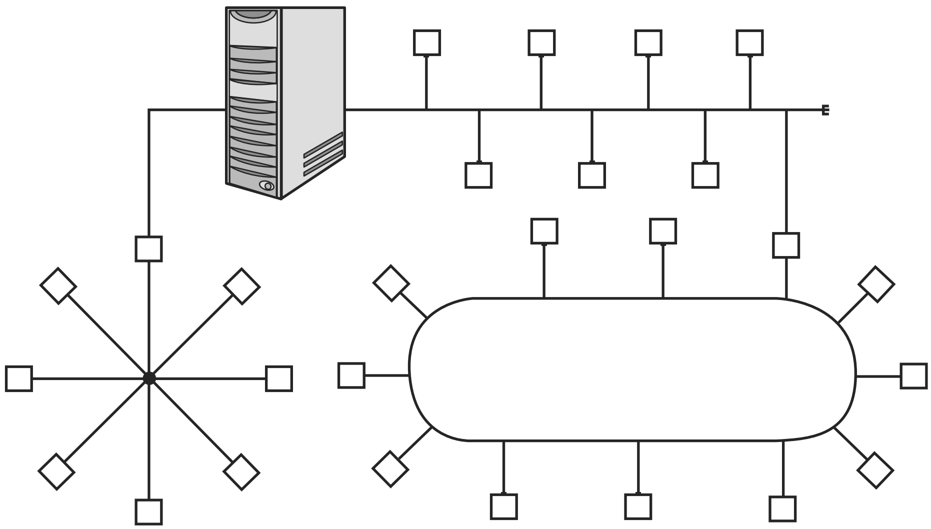

Figure 3-19 Hybrid Topology

Network Technologies

Just as a network can be connected in various topologies, different technologies have been implemented over the years that run over those topologies. These technologies operate at layer 2 of the OSI model, and their details of operation are specified in various standards by the Institute of Electrical and Electronics Engineers (IEEE). Some of these technologies are designed for Local Area Network (LAN) applications whereas others are meant to be used in a Wide Area Network (WAN). In this section, we look at the main LAN technologies and some of the processes that these technologies use to arbitrate access to the network.

Ethernet 802.3

The IEEE specified the details of Ethernet in the 802.3 standard. Prior to this standardization, Ethernet existed in several earlier forms, the most common of which was called Ethernet ll or DIX Ethernet (DIX stands for the three companies that collaborated on its creation, DEC, Intel, and Xerox).

In the section on the OSI model, you learned that the PDU created at layer 2 is called a frame. Because Ethernet is a layer 2 protocol, we refer to the individual Ethernet packets as *frames*. There are small differences in the frame structures of Ethernet ll and 802.3, although they are compatible in the same network. Figure 3-20 shows a comparison of the two frames. The significant difference is that during the IEEE standardization process, the EtherType field was changed to a (data) length field in the new 802.3 standard. For purposes of identifying the data type, another field called the 802.2 header was inserted to contain that information.

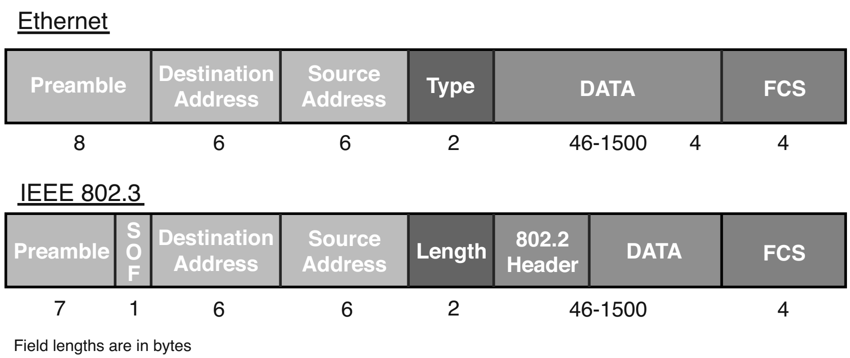

Figure 3-20 Ethernet ll and 802.3

Ethernet has been implemented on coaxial, fiber, and twisted-pair wiring. Table 3-6 lists some of the more common Ethernet implementations.

Table 3-6 Ethernet Implementations

Key Topic

Ethernet Type	Cable Type	Speed
10Base2	Coaxial	10 Mbps
10Base5	Coaxial	10 Mbps
10BaseT	Twisted pair	10 Mbps
100BaseTX	Twisted pair	100 Mbps
1000BaseT	Twisted pair	1000 Mbps
1000BaseX	Fiber	1000 Mbps
10GBaseT	Twisted pair	10 Gbps

> **NOTE** Despite the fact that 1000BaseT and 1000BaseX are faster, 100BaseTX is called *Fast Ethernet*! Also both 1000BaseT and 1000BaseX are usually referred to as Gigabit Ethernet.

Ethernet calls for devices to share the medium on a frame-by-frame basis. It arbitrates access to the media using a process called Carrier Sense Multiple Access with Collision Detection (CSMA/CD). This process is discussed in detail in the section "CSMA/CD Versus CSMA/CA" where the process is contrasted with the method used in 802.11 wireless networks.

Token Ring 802.5

Ethernet is the most common layer 2 protocol, but it has not always been that way. An example of a proprietary layer 2 protocol that enjoyed some small success is IBM Token Ring. This protocol operates using specific IBM connective devices and cables, and the nodes must have Token Ring network cards installed. It can operate at 16 Mbps, which at the time of its release was impressive, but the proprietary nature of the equipment and the soon-to-be faster Ethernet caused Token Ring to fall from favor.

As mentioned earlier, in most cases the physical network topology is the same as the logical topology. Token Ring is the exception to that general rule. It is logically a ring and physically a star. It is a star in that all devices are connected to a central device called a Media Access Unit (MAU), but the ring is formed in the MAU and when you investigate the flow of the data, it goes from one device to another in a ring design by entering and exiting each port of the MAU, as shown in Figure 3-21.

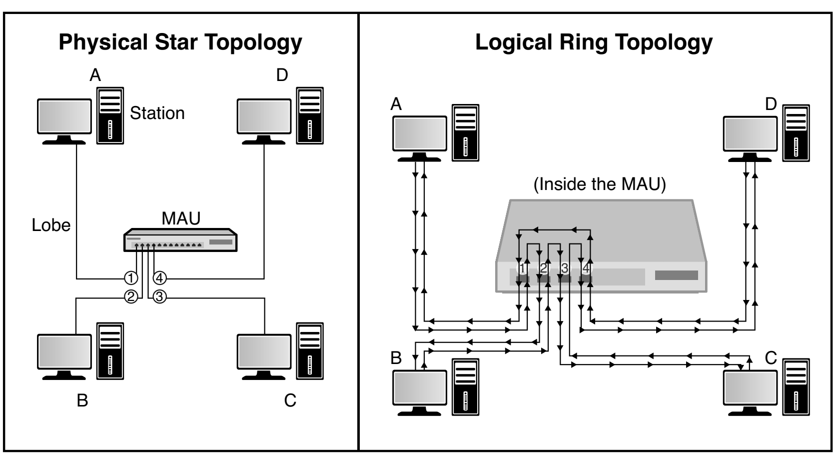

Figure 3-21 Token Ring

FDDI

Another layer 2 protocol that uses a ring topology is Fiber Distributed Data Interface (FDDI). Unlike Token Ring, it is both a physical and a logical ring. It is actually a double ring, each going in a different direction to provide fault tolerance. It also is implemented with fiber cabling. In many cases it is used for a network backbone and is then connected to other network types, such as Ethernet, forming a hybrid network. It is also used in Metropolitan Area Networks (MANs) because it can be deployed up to 100 kilometers.

Figure 3-22 shows an example of an FFDI ring.

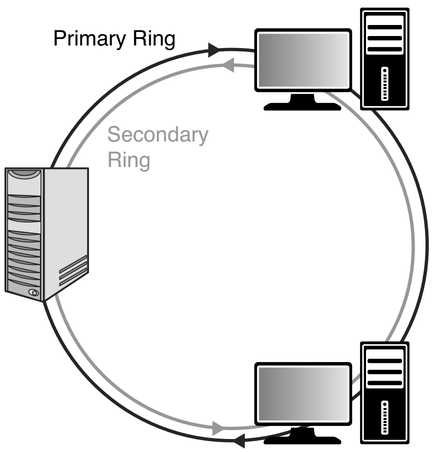

Figure 3-22 FDDI

Contention Methods

Regardless of the layer 2 protocol in use, there must be some method used to arbitrate the use of the shared media. Four basic processes have been employed to act as the traffic cop, so to speak:

- CSMA/CD
- CSMA/CA
- Token passing
- Polling

This section compares and contrasts each and provides examples of technologies that use each.

CSMA/CD Versus CSMA/CA

To appreciate CSMA/CD and CSMA/CA, you must understand the concept of collisions and collision domains in a shared network medium. Collisions occur when two devices send a frame at the same time causing the frames and their underlying electrical signals to collide on the wire. When this occurs, both signals and the frames they represent are destroyed or at the very least corrupted such that they are discarded when they reach the destination. Frame corruption or disposal causes both devices to resend the frames, resulting in a drop in overall throughput.

Collision Domains

A collision domain is any segment of the network where the possibility exists for two or more devices' signals to collide. In a bus topology, that would constitute the entire network because the entire bus is a shared medium. In a star topology, the scope of the collision domain or domains depends on the central connecting device. Central connecting devices include hubs and switches. Hubs and switches are discussed more fully in the section "Network Devices" but their differences with respect to collision domains need to be discussed here.

A hub is an unintelligent junction box into which all devices plug. All the ports in the hub are in the same collision domain because when a hub receives a frame, the hub broadcasts the frame out all ports. So logically, the network is still a bus.

A star topology with a switch in the center does not operate this way. A switch has the intelligence to record the MAC address of each device on every port. After all the devices' MAC addresses are recorded, the switch sends a frame ONLY to the port on which the destination device resides. Because each device's traffic is then segregated from any other device's traffic, each device is considered to be in its own collision domain.

This segregation provided by switches has both performance and security benefits. From a performance perspective, it greatly reduces the number of collisions, thereby significantly increasing overall throughput in the network. From a security standpoint, it means that a sniffer connected to a port in the switch will ONLY capture traffic destined for that port, not all traffic. Compare this security to a hub-centric network. When a hub is in the center of a star network, a sniffer will capture all traffic regardless of the port to which it is connected because all ports are in the same collision domain.

In Figure 3-23, a switch has several devices and a hub connected to it with each collision domain marked to show how the two devices create collision domains. Note that each port on the switch is a collision domain whereas the entire hub is a single collision domain.

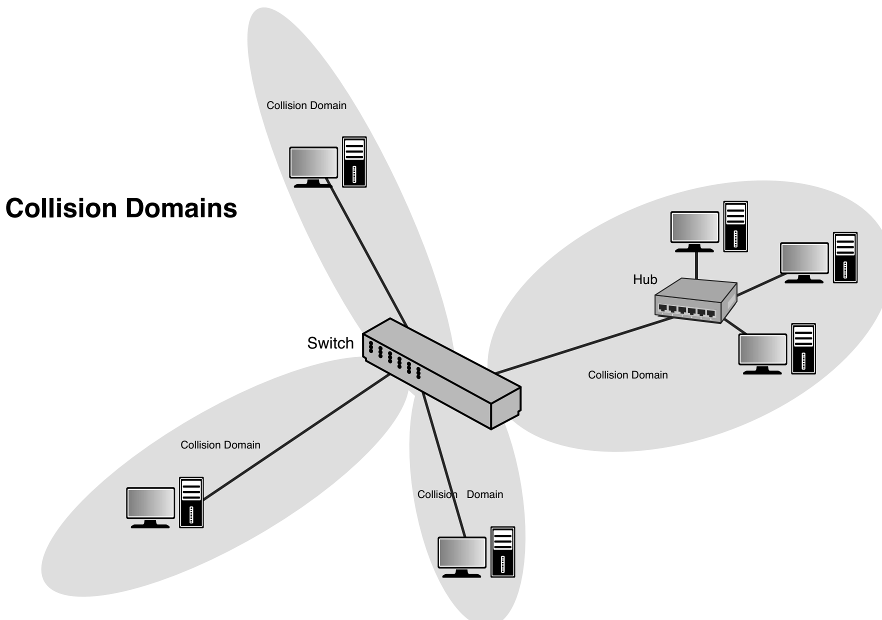

Figure 3-23 Collision Domains

CSMA/CD

In 802.3 networks, a mechanism called Carrier Sense Multiple Access Collision Detection (CSMA/CD) is used when a shared medium is in use to recover from inevitable collisions. This process is a step-by-step mechanism that each station follows every time it needs to send a single frame. The steps to the process are as follow:

Key Topic

1. When a device needs to transmit, it checks the wire for existing traffic. This process is called carrier sense.
2. If the wire is clear, the device transmits and continues to perform carrier sense.
3. If a collision is detected, both devices issue a jam signal to all the other devices, which indicates to them to NOT transmit. Then both devices increment a retransmission counter. This is a cumulative total of the number of times this frame has been transmitted and a collision occurred. There is a maximum number at which it aborts the transmission of the frame.
4. Both devices calculate a random amount of time (called a random back off) and wait that amount of time before transmitting again.
5. In most cases because both devices choose random amounts of time to wait, another collision will not occur. If it does, the procedure repeats.

CSMA/CA

In 802.11 wireless networks, CSMA/CD cannot be used as an arbitration method because unlike when using bounded media, the devices cannot detect a collision. The method used is called Carrier Sense Multiple Access Collision Avoidance (CSMA/CA). It is a much more laborious process because each station must acknowledge each frame that is transmitted.

The "Wireless Networks" section covers 802.11 network operations in more detail, but for the purposes of understanding CSMA/CA we must at least lay some groundwork. The typical wireless network contains an access point (AP) and at least one or more wireless stations. In this type of network (called Infrastructure Mode wireless network), traffic never traverses directly between stations but is always relayed through the AP. The steps in CSMA/CA are as follows:

Key Topic

1. Station A has a frame to send to Station B. It checks for traffic in two ways. First, it performs carrier sense, which means it listens to see whether any radio waves are being received on its transmitter. Secondly, after the transmission is sent, it will continue to monitor the network for possible collisions.
2. If traffic is being transmitted, Station A decrements an internal countdown mechanism called the random back-off algorithm. This counter will have started counting down after the last time this station was allowed to transmit. All stations will be counting down their own individual timers. When a station's timer expires, it is allowed to send.
3. If Station A performs carrier sense, there is no traffic and its timer hits zero, it sends the frame.
4. The frame goes to the AP.
5. The AP sends an acknowledgment back to Station A. Until that acknowledgment is received by Station A, all other stations must remain silent. For each frame that AP needs to relay, it must wait its turn to send using the same mechanism as the stations.
6. When its turn comes up in the cache queue, the frame from Station A is relayed to Station B.
7. Station B sends an acknowledgment back to the AP. Until that acknowledgment is received by the AP, all other stations must remain silent.

As you can see, these processes create a lot of overhead but are required to prevent collisions in a wireless network.

Token Passing

Both FDDI and Token Ring networks use a process called token passing. In this process, a special packet called a token is passed around the network. A station cannot send until the token comes around and is empty. Using this process, NO collisions occur because two devices are never allowed to send at the same time. The problem with this process is that the possibility exists for a single device to gain control of the token and monopolize the network.

Polling

The final contention method to discuss is polling. In this system, a primary device polls each other device to see whether it needs to transmit. In this way, each device gets a transmit opportunity. This method is common in the mainframe environment.

Network Protocols/Services

Many protocols and services have been developed over the years to add functionality to networks. In many cases these protocols reside at the Application layer of the OSI model. These Application layer protocols usually perform a specific function and rely on the lower layer protocols in the TCP/IP suite and protocols at layer 2 (like Ethernet) to perform routing and delivery services.

This section covers some of the most important of these protocols and services, including some that do NOT operate at the Application layer, focusing on the function and port number of each. Port numbers are important to be aware of from a security standpoint because in many cases port numbers are referenced when configuring firewall rules. In cases where a port or protocol number is relevant, they will be given as well.

ARP

Address Resolution Protocol (ARP), one of the protocols in the TCP/IP suite, operates at layer 3 of the OSI model. The information it derives is utilized at layer 2, however. ARP's job is to resolve the destination IP address placed in the header by IP to a layer 2 or MAC address. Remember, when frames are transmitted on a local segment the transfer is done in terms of MAC addresses not IP addresses, so this information must be known.

Whenever a packet is sent across the network, at every router hop and again at the destination subnet, the source and destination MAC address pairs change but the source and destination IP addresses not. The process that ARP uses to perform this resolution is called an ARP broadcast.

First an area of memory called the ARP cache is consulted. If the MAC address has been recently resolved, the mapping will be in the cache and a broadcast is not required. If the record has aged out of the cache, ARP sends a broadcast frame to the local network that all devices will receive. The device that possesses the IP address responds with its MAC address. Then ARP places the MAC address in the frame and sends the frame. Figure 3-24 illustrates this process.

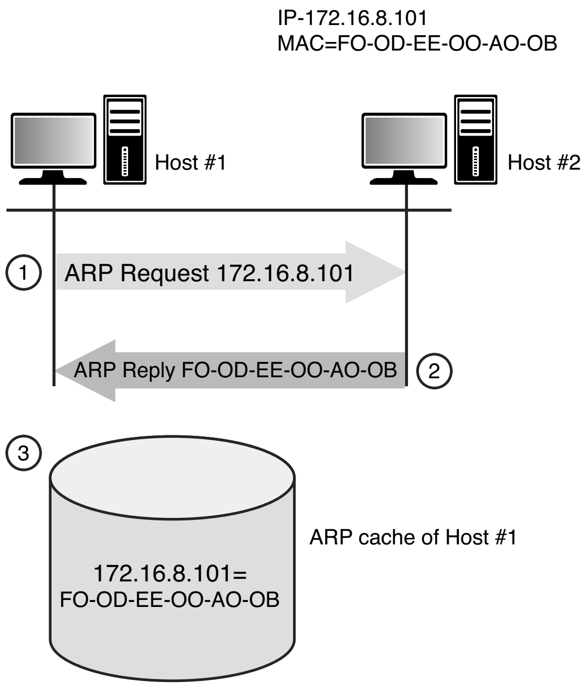

Figure 3-24 ARP Broadcast

DHCP

Dynamic Host Configuration Protocol (DHCP) is a service that can be used to automate the process of assigning an IP configuration to the devices in the network. Manual configuration of an IP address, subnet mask, default gateway, and DNS server is not only time consuming but fraught with opportunity for human error. Using DHCP can not only automate this, but can also eliminate network problems from this human error.

DHCP is a client/server program. All modern operating systems contain a DHCP client, and the server component can be implemented either on a server or on a router. When a computer that is configured to be a DHCP client starts, it performs a precise four-step process to obtain its configuration. Conceptually, the client broadcasts for the IP address of the DHCP server. All devices receive this broadcast, but only DHCP servers respond. The device accepts the configuration offered by the first DHCP server from which it hears. The process uses four packets with distinctive names (see Figure 3-25). DHCP uses UDP ports 67 and 68. Port 67 sends data to the server, and port 68 sends data to the client.

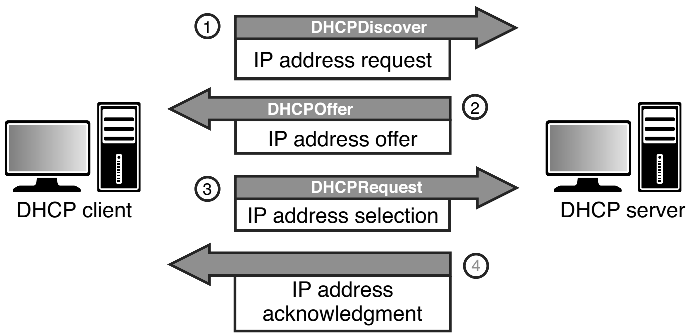

Figure 3-25 DHCP

DNS

Just as DHCP relieves us from having to manually configure the IP configuration of each system, Domain Name System (DNS) relieves all humans from having to know the IP address of every computer with which they want to communicate. Ultimately, an IP address must be known to connect to another computer. DNS resolves a computer name (or in the case of the Web, a domain name) to an IP address.

DNS is another client/server program with the client included in all modern operating systems. The server part resides on a series of DNS servers located both in the local network and on the Internet. When a DNS client needs to know the IP address that goes with a particular computer name or domain name, it queries the local DNS server. If the local DNS server does not have the resolution, it contacts other DNS servers on the client's behalf, learns the IP address, and relays that information to the DNS client. DNS uses UDP port 53 and TCP port 53. The DNS servers use TCP port 53 to exchange information, and the DNS clients use UDP port 53 for queries.

FTP, FTPS, SFTP

File Transfer Protocol (FTP), and its more secure versions FTPS and SFTP, transfers files from one system to another. FTP is insecure in that the username and password is transmitted in clear text. The original clear text version uses TCP port 20 for data and TCP port 21 as the control channel. Using FTP when security is a consideration is not recommended.

FTPS is FTP that adds support for the Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols. FTPS uses TCP ports 989 and 990.

FTPS is not the same as and should not be confused with another secure version of FTP, SSH File Transfer Protocol (SFTP). This is an extension of the Secure Shell Protocol (SSH). There have been a number of different versions with version 6 being the latest. Because it uses SSH for the file transfer, it uses TCP port 22.

HTTP, HTTPS, SHTTP

One of the most frequently used protocols today is Hypertext Transfer Protocol (HTTP) and its secure versions, HTTPS and SHTTP. This protocol is used to view and transfer web pages or web content. The original version (HTTP) has no encryption so when security is a concern, one of the two secure versions should be used. HTTP uses TCP port 80.

Hypertext Transfer Protocol Secure (HTTPS) layers the HTTP on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications. It is often used for secure websites because it requires no software or configuration changes on the web client to function securely. When HTTPS is used, port 80 is not used. Rather, it uses port 443.

Unlike HTTPS, which encrypts the entire communication, SHTTP encrypts only the served page data and submitted data such as POST fields, leaving the initiation of the protocol unchanged. Secure-HTTP and HTTP processing can operate on the same TCP port, port 80. This version is rarely used.

ICMP

Internet Control Message Protocol (ICMP) operates at layer 3 of the OSI model and is used by devices to transmit error messages regarding problems with transmissions. It also is the protocol used when the ping and traceroute commands are used to troubleshoot network connectivity problems. Because IP is part of the TCP/IP suite, it doesn't use a port number but is identified in the packet by its protocol number. Its protocol number is 1.

ICMP is a protocol that can be leveraged to mount several network attacks based on its operation, and for this reason many networks choose to block ICMP. These attacks are discussed in the section "Network Threats."

IMAP

Internet Message Access Protocol (IMAP) is an Application layer protocol for email retrieval. Its latest version is IMAP4. It is a client email protocol used to access email from a server. Unlike POP3, another email client that can only download messages from the server, IMAP4 allows one to download a copy and leave a copy on the server. IMAP 4 uses port 143. A secure version also exists, IMAPS (IMAP over SSL), that uses port 993.

NAT

Network Address Translation (NAT) is a service that maps private IP addresses to public IP addresses. It is discussed in the section “Logical and Physical Addressing” earlier in this chapter.

PAT

Port Address Translation (PAT) is a specific version of NAT that uses a single public IP address to represent multiple private IP addresses. Its operation is discussed in the section “Logical and Physical Addressing” earlier in this chapter.

POP

Post Office Protocol (POP) is an Application layer email retrieval protocol. POP3 is the latest version. It allows for downloading messages only and does not allow the additional functionality provided by IMAP4. POP3 uses port 110. A version that runs over SSL is also available that uses port 995.

SMTP

POP and IMAP are client email protocols used for retrieving email, but when email servers are talking to each other they use a protocol called Simple Mail Transfer Protocol (SMTP), a standard Application layer protocol. This is also the protocol used by clients to send email. SMTP uses port 25, and when it is runs over SSL, it uses port 465.

SNMP

Simple Network Management Protocol (SNMP) is an Application layer protocol that is used to retrieve information from network devices and to send configuration changes to those devices. SNMP uses TCP port 162 and UDP ports 161 and 162.

SNMP devices are organized into communities and the community name must be known to either access information from or send a change to a device. It also can be used with a password. SNMP versions 1 and 2 are susceptible to packet sniffing, and all versions are susceptible to brute-force attacks on the community strings and password used. The defaults of community string names, which are widely known, are often left in place. The latest version, SNMPv3, is the most secure.

Network Routing

Routing occurs at layer 3 of the OSI model, which is also the layer at which IP operates and where the source and destination IP addresses are placed in the packet. Routers are devices that transfer traffic between systems in different IP networks. When computers are in different IP networks, they cannot communicate unless a router is available to route the packets to the other networks.

Routers keep information about the paths to other networks in a routing table. These tables can be populated several ways. Administrators manually enter these routes, or dynamic routing protocols allow the routers running the same protocol to exchange routing tables and routing information. Manual configuration, also called static routing, has the advantage of avoiding the additional traffic created by dynamic routing protocols and allows for precise control of routing behavior, but requires manual intervention when link failures occur. Dynamic routing protocols create traffic but are able to react to link outages and reroute traffic without manual intervention.

From a security standpoint, routing protocols introduce the possibility that routing update traffic might be captured, allowing a hacker to gain valuable information about the layout of the network. Moreover, Cisco devices (perhaps the most widely used) also use a proprietary layer 2 protocol by default called Cisco Discovery Protocol (CDP) that they use to inform each other about their capabilities. If the CDP packets are captured, additional information can be obtained that can be helpful to mapping the network in advance of an attack.

This section compares and contrasts routing protocols.

Distance Vector, Link State, or Hybrid Routing

Routing protocols have different capabilities and operational characteristics that impact when and where they are utilized. Routing protocols come in two basic types: interior and exterior. Interior routing protocols are used within an autonomous system, which is a network managed by one set of administrators, typically a single enterprise. Exterior routing protocols route traffic between systems or company networks. An example of this type of routing is what occurs on the Internet.

Routing protocols also can fall into three categories that describe their operations more than their scope: distance vector, link state, and hybrid (or advanced distance vector). The difference in these mostly revolves around the amount of traffic created and the method used to determine the best path out of possible paths to a network. The value used to make this decision is called a metric, and each has a different way of calculating the metric and thus determining the best path.

Distance vector protocols share their entire routing table with their neighboring routers on a schedule, thereby creating the most traffic of the three categories. They also use a metric called *hop count*. Hop count is simply the number of routers traversed to get to a network.

Link state protocols only share network changes (link outages and recoveries) with neighbors, thereby greatly reducing the amount of traffic generated. They also use a much more sophisticated metric that is based on many factors, such as the bandwidth of each link on the path and the congestion on each link. So when using one of these protocols, a path might be chosen as best even though it has more hops because the path chosen has better bandwidth, meaning less congestion.

Hybrid or advanced distance vector protocols exhibit characteristics of both types. EIGRP, discussed later in this section, is the only example of this type. In the past, EIGRP has been referred to as a hybrid protocol but in the last several years, Cisco (which created IGRP and EIGRP) has been calling this an advanced distance vector protocol so you might see both terms used. In the following sections, several of the most common routing protocols are discussed briefly.

RIP

Routing Information Protocol (RIP) is a standards-based distance vector protocol that has two versions: RIPv1 and RIPv2. Both use hop count as a metric and share their entire routing tables every 30 seconds. Although RIP is the simplest to configure, it has a maximum hop count of 15, so it is only useful in very small networks. The biggest difference between the two versions is that RIPv1 can only perform classful routing whereas RIPv2 can route in a network where CIDR has been implemented.

OSPF

Open Shortest Path First (OSPF) is a standards-based link state protocol. It uses a metric called cost that is calculated based on many considerations. Thus it makes much more sophisticated routing decisions than a distance vector routing protocol such as RIP. It also only updates other routers with changes, greatly reducing the amount of traffic generated. To take full of advantage of OSPF, a much deeper knowledge of routing and OSPF itself is required. It can scale successfully to very large networks because it has no minimum hop count.

IGRP

Interior Gateway Routing Protocol (IGRP) is an obsolete classful Cisco-proprietary routing protocol that you will not likely see in the real world because of its inability to operate in an environment where CIDR has been implemented. It has been replaced with the classless version Enhanced IGRP (EIGRP) discussed next.

EIGRP

Enhanced IGRP (EIGRP) is a classless Cisco-proprietary routing protocol that is considered a hybrid or advanced distance vector protocol. It exhibits some characteristics of both link state and distance vector operations. It also has no limitations on hop count and is much simpler to implement than OSPF. It does, however, require that all routers be Cisco.

VRRP

When a router goes down, all hosts that use that router for routing will be unable to send traffic to other networks. Virtual Router Redundancy Protocol (VRRP) is not really a routing protocol but rather is used to provide multiple gateways to clients for fault tolerance in the case of a router going down. All hosts in a network are set with the IP address of the *virtual router* as their default gateway. Multiple physical routers are mapped to this address so there will be an available router even if one goes down.

IS-IS

Intermediate System to Intermediate System (IS-IS) is a complex interior routing protocol that is based on OSI protocols rather than IP. It is a link state protocol. The TCP/IP implementation is called Integrated IS-IS. OSPF has more functionality, but IS-IS creates less traffic than OSPF and is much less widely implemented than OSPF.

BGP

Border Gateway Protocol (BGP) is an exterior routing protocol considered to be a path vector protocol. It routes between autonomous systems (ASs) and is used on the Internet. It has a rich set of attributes that can be manipulated by administrators to control path selection and to control the exact way in which traffic enters and exits the AS. However, it is one of the most complex to understand and configure.

Network Devices

Network devices operate at all layers of the OSI model. The layer at which they operate reveals quite a bit about their level of intelligence and about the types of information used by each device. This section covers common devices and their respective roles in the overall picture.

Patch Panel

Patch panels operate at the Physical layer (layer 1) of the OSI model and simply function as a central termination point for all the cables running through the walls from wall outlets, which in turn are connected to computers with cables. The cables running through the walls to the patch panel are permanently connected to the panel. Short cables called patch cables are then used to connect each panel port to a switch or hub.

Multiplexer

A multiplexer is a Physical layer (layer 1) device that combines several input information signals into one output signal, which carries several communication channels, by means of some multiplex technique. Conversely, a demultiplexer takes a single input signal that carries many channels and separates those over multiple output signals. Sharing the same physical medium can be done in a number of different ways: on the basis of frequencies used (frequency division multiplexing or FDM) or by using time slots (time division multiplexing or TDM).

Hub

A hub is a Physical layer (layer 1) device that functions as a junction point for devices in a star topology. It is considered a Physical layer device because it has no intelligence. When a hub receives traffic, it broadcasts that traffic out of every port because it does not have the intelligence to make any decisions about where the destination is located.

Although this results in more collisions and poor performance, from a security standpoint the problem is that it broadcasts all traffic to all ports. A sniffer connected to any port will be able to sniff all traffic. The operation of a hub is shown in Figure 3-26. When a switch is used, that is not the case (more on those next).

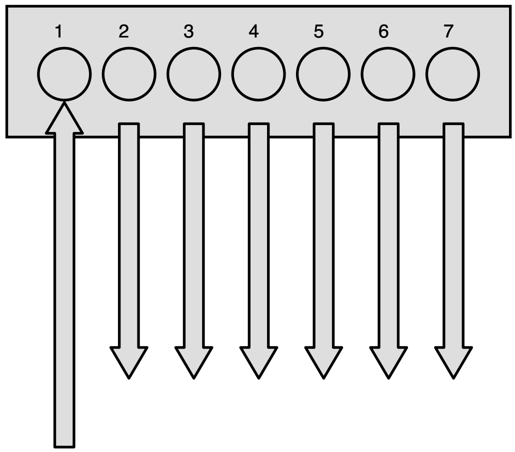

Figure 3-26 Hub

Switch

Switches are intelligent and operate at layer 2 of the OSI model. We say they map to this layer because they make switching decisions based on MAC addresses, which reside at layer 2. This process is called *transparent bridging*. Figure 3-27 shows this process.

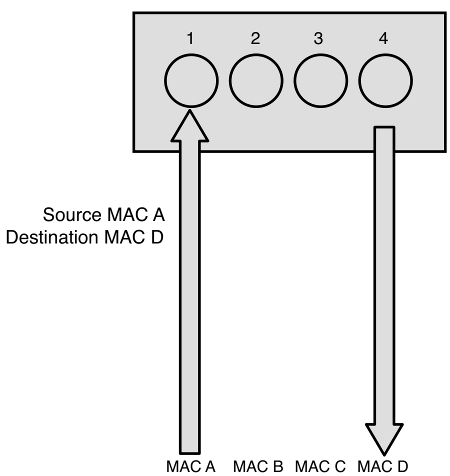

Figure 3-27 Transparent Bridging

Switches improve performance over hubs because they eliminate collisions. Each switch port is in its own collision domain, whereas all ports of a hub are in the same collision domain. From a security standpoint, switches are more secure in that a sniffer connected to any single port will only be able to capture traffic destined for or originating from that port.

Some switches, however, are both routers and switches, and in that case we call them layer 3 switches because they route and switch.

VLANs

Enterprise-level switches are also capable of another functionality called virtual local area networks (VLANs). These are logical subdivisions of a switch that segregate ports from one another as if they were in different LANs. These VLANs can also span multiple switches, meaning that devices connected to switches in different parts of a network can be placed in the same VLAN regardless of physical location.

VLANs offer another way to add a layer of separation between sensitive devices and the rest of the network. For example, if only two devices should be able to connect to the HR server, the two devices and the HR server could be placed in a VLAN separate from the other VLANs. Traffic between VLANs can only occur through a router. Routers can be used to implement ACLs that control the traffic allowed between VLANs.

Layer 3 Versus Layer 4

Typically we map the switching process to layer 2 of the OSI model because layer 2 addresses are used to make frame-forwarding decisions. That doesn't mean that a single physical device cannot be capable of both functions. A layer 3 switch is such a device. It is a switch with the routing function also built in. It can both route and switch and can combine the two functions in an integrated way such that a single data stream can be routed when the first packet arrives and then the rest of the packets in the stream can be fast switched, resulting in better performance.

Layer 4 switches take this a step further by providing additional routing above layer 3 by using the port numbers found in the Transport layer header to make routing decisions. The largest benefit of layer 4 switching is the ability to prioritize data traffic by application, which means a quality of service (QoS) can be defined for each user.

Router

Routers operate at layer 3 (Network layer) when we are discussing the routing function in isolation. As previously discussed, certain devices can combine routing functionality with switching and layer 4 filtering. However, because routing uses layer 3 information (IP addresses) to make decisions, it is a layer 3 function.

Routers use a routing table that tells the router in which direction to send traffic destined for a particular network. Although routers can be configured with routes to individual computers, typically they route toward networks, not individual computers. When the packet arrives at the router that is directly connected to the destination network, that particular router performs an ARP broadcast to learn the MAC address of the computer and send the packets as frames at layer 2.

Routers perform an important security function because on them ACLs are typically configured. These are ordered sets of rules that control the traffic that is permitted or denied the use of a path through the router. These rules can operate at layer 3 making these decisions on the basis of IP addresses or at layer 4 when only certain types of traffic are allowed. When this is done, the ACL typically references a port number of the service or application that is allowed or denied.

Gateway

The term *gateway* doesn't refer to a particular device but rather to any device that performs some sort of translation or acts as a control point to entry and exit. For example, if a router has one interface that uses TCP/IP and another interface that uses IPX/SPX (a now obsolete LAN protocol), we would say it performs as a gateway between the two protocols.

Another example of a device performing as a gateway would be an email server. It receives email from all types of email servers (Exchange, IBM Notes, Novell GroupWise) and performs any translation of formats that is necessary between these different implementations.

Finally, but certainly not the last example would be a Network Access Server (NAS) that controls access to a network. This would be considered a gateway in that all traffic might need to be authenticated before entry is allowed. This type of server might even examine the computers themselves for the latest security patches and updates before entry is allowed.

Firewall

The network device that perhaps is most connected with the idea of security is the firewall. Firewalls can be software programs that are installed over server operating systems or they can be appliances that have their own operating system. In either case their job is to inspect and control the type of traffic allowed.

Firewalls can be discussed on the basis of their type and their architecture. They can also be physical devices or exist in a virtualized environment. This section looks at them from all angles.

Types

When we discuss *types* of firewalls, we are focusing on the differences in the way they operate. Some firewalls make a more thorough inspection of traffic than others. Usually there is tradeoff in the performance of the firewall and the type of inspection that it performs. A deep inspection of the contents of each packet results in the firewall having a detrimental effect on throughput whereas a more cursory look at each packet has somewhat less of an impact on performance. It is for this reason we make our selections of what traffic to inspect wisely, keeping this tradeoff in mind.

Packet filtering firewalls are the least detrimental to throughput because they only inspect the header of the packet for allowed IP addresses or port numbers. Although even performing this function will slow traffic, it involves only looking at the beginning of the packet and making a quick allow or disallow decision.

Although packet filtering firewalls serve an important function, they cannot prevent many attack types. They cannot prevent IP spoofing, attacks that are specific to an application, attacks that depend on packet fragmentation, or attacks that take advantage of the TCP handshake. More advanced inspection firewall types are required to stop these attacks.

Stateful firewalls are those that are aware of the proper functioning of the TCP handshake, keep track of the state of all connections with respect to this process, and can recognize when packets are trying to enter the network that don't make sense in the context of the TCP handshake. You might recall the discussion of how the TCP handshake occurs from the section "Transport Layer" earlier in this chapter.

To review that process, a packet should never arrive at a firewall for delivery that has both the SYN flag and the ACK flag set unless it is part of an existing handshake process and it should be in response to a packet sent from inside the network with the SYN flag set. This is the type of packet that the stateful firewall would disallow. It also has the ability to recognize other attack types that attempt to misuse this process. It does this by maintaining a state table about all current connections and the status of each connection process. This allows it to recognize any traffic that doesn't make sense with the current state of the connection. Of course, maintaining this table and referencing the table causes this firewall type to have more effect on performance than a packet filtering firewall.

Proxy firewalls actually stand between each connection from the outside to the inside and make the connection on behalf of the endpoints. Therefore there is no direct connection. The proxy firewall acts as a relay between the two endpoints. Proxy firewalls can operate at two different layers of the OSI model. Both are discussed shortly.

Circuit-level proxies operate at the Session layer (layer 5) of the OSI model. They make decisions based on the protocol header and Session layer information. Because they do not do deep packet inspection (at layer 7 or the Application layer), they are considered application-independent and can be used for wide ranges of layer 7 protocol types.

A SOCKS firewall is an example of a circuit-level firewall. This requires a SOCKS client on the computers. Many vendors have integrated their software with SOCKS to make using this type of firewall easier.

Application-level proxies perform deep packet inspection. This type of firewall understands the details of the communication process at layer 7 for the application of interest. An application-level firewall maintains a different proxy function for each protocol. For example, for HTTP the proxy will be able to read and filter traffic based on specific HTTP commands. Operating at this layer requires each packet to be completely opened and closed, making this firewall the most impactful on performance.

Dynamic packet filtering rather than describing a different type of firewall describes functionality that a firewall might or might not possess, When internal computers attempt to establish a session with a remote computer, it places both a source and destination port number in the packet. For example, if the computer is making a request of a web server, because HTTP uses port 80, the destination will be port 80.

The source computer selects the source port at random from the numbers available above the well-known port numbers, or above 1023. Because predicting what that random number will be is impossible, creating a firewall rule that anticipates and allows traffic back through the firewall on that random port is impossible. A dynamic packet filtering firewall will keep track of that source port and dynamically add a rule to the list to allow return traffic to that port.

A kernel proxy firewall is an example of a *fifth-generation firewall.* It inspects the packet at every layer of the OSI model but does not introduce the performance hit that an Application layer firewall will because it does this at the kernel layer. It also follows the proxy model in that it stands between the two systems and creates connections on their behalf.

Architecture

Although the type of firewall speaks to the internal operation of the firewall, the architecture refers to the way in which the firewall or firewalls are deployed in the network to form a system of protection. This section looks at the various ways firewalls can be deployed and what the names of these various configurations are.

A bastion host might or might not be a firewall. The term actually refers to the position of any device. If it is exposed directly to the Internet or to any untrusted network, we would say it is a bastion host. Whether it is a firewall, a DNS server, or a web server, this means all standard hardening procedures become even more important for these exposed devices. Any unnecessary services should be stopped, all unneeded ports should be closed, and all security patches must be up to date. These procedures are referred to as *reducing the attack surface*.

A dual-homed firewall is one that has two network interfaces, one pointing to the internal network and another connected to the untrusted network. In many cases routing between these interfaces is turned off. The firewall software allows or denies traffic between the two interfaces based on the firewall rules configured by the administrator. The danger of relying on a single dual-homed firewall is that there is a single point of failure. If this device is compromised, the network is also. If it suffers a denial of service (DoS) attack, no traffic will pass. Neither is a good situation.

In some cases the firewall may be multihomed. One popular type is the three-legged firewall. In this configuration are three interfaces: one connected to the untrusted network, one to the internal network, and the last to a part of the network called a Demilitarized Zone (DMZ). A DMZ is a portion of the network where systems are placed that will be accessed regularly from the untrusted network. These might be web servers or an email server, for example. The firewall can then be configured to control the traffic that flows between the three networks, being somewhat careful with traffic destined for the DMZ and then treating traffic to the internal network with much more suspicion.

Although the firewalls discussed thus far typically connect directly to the untrusted network (at least one interface does), a screened host is a firewall that is between the final router and the internal network. When traffic comes into the router and is forwarded to the firewall, it will be inspected before going into the internal network.

Taking this concept a step further is a screened subnet. In this case, two firewalls are used, and traffic must be inspected at both firewalls to enter the internal network. It is called a screen subnet because there will be a subnet between the two firewalls that can act as a DMZ for resources from the outside world.

In the real world, these various approaches are mixed and matched to meet requirements, so you might find elements of all these architectural concepts being applied to a specific situation.

Virtualization

Today physical servers are increasingly being consolidated as virtual servers on the same physical box. Virtual networks using virtual switches even exist in the physical devices that host these virtual servers. These virtual network systems and their traffic can be segregated in all the same ways as in a physical network using subnets, VLANs, and of course, virtual firewalls. Virtual firewalls are software that has been specifically written to operate in the virtual environment. Increasingly, virtualization vendors such as VMware are making part of their code available to security vendors to create firewalls (and antivirus products) that integrate closely with the product.

Keep in mind that in any virtual environment each virtual server that is hosted on the physical server must be configured with its own security mechanisms. These mechanisms include antivirus and antimalware software and all the latest service packs and security updates for ALL the software hosted on the virtual machine. Also, remember that all the virtual servers share the resources of the physical device.

Proxy Server

Proxy servers can be appliances or they can be software that is installed on a server operating system. These servers act like a proxy firewall in that they create the web connection between systems on their behalf, but they can typically allow and disallow traffic on a more granular basis. For example, a proxy server might allow the Sales group to go to certain websites while not allowing the Data Entry group access to these same sites. The functionality extends beyond HTTP to other traffic types, such as FTP and others.

Proxy servers can provide an additional beneficial function called *web caching*. When a proxy server is configured to provide web caching, it saves a copy of all web pages that have been delivered to internal computers in a web cache. If any user requests the same page later, the proxy server has a local copy and need not spend the time and effort to retrieve it from the Internet. This greatly improves web performance for frequently requested pages.

PBX

A private branch exchange (PBX) is a private telephone switch that resides on the customer premises. It has a direct connection to the telecommunication provider’s switch. It performs call routing within the internal phone system. This is how a company can have two “outside” lines but 50 internal phones. The call comes in on one of the two outside lines, and the PBX routes it to the proper extension. Sometimes the system converts analog to digital but not always.

The security considerations with these devices revolve around their default configurations. They typically are configured with default administrator passwords that should be changed, and they often contain backdoor connections that can be used by vendor support personnel to connect in and help with problems. These back doors are usually well known and should be disabled until they are needed.

Honeypot

Honeypots are systems that are configured to be attractive to hackers and lure them into spending time attacking them while information is gathered about the attack. In some cases entire networks called honeynets are attractively configured for this purpose. These types of approaches should only be undertaken by companies with the skill to properly deploy and monitor them.

Care should be taken that the honeypots and honeynets do not provide direct connections to any important systems. This prevents providing a jumping-off point to other areas of the network. The ultimate purpose of these systems is to divert attention from more valuable resources and to gather as much information about an attack as possible. A *tarpit* is a type of honeypot designed to provide a very slow connection to the hacker so that the attack can be analyzed.

Cloud Computing

Cloud computing is all the rage these days, and it comes in many forms. The basic idea of cloud computing is to make resources available in a web-based data center so the resources can be accessed from anywhere. When a company pays another company to host and manage this environment, we call it a public cloud solution. When companies host this environment themselves, we call it a private cloud solution.

There is trade-off when a decision must be made between the two architectures. The private solution provides the most control over the safety of your data but also requires the staff and the knowledge to deploy, manage, and secure the solution. A public cloud puts your data's safety in the hands of a third party, but that party is often more capable and knowledgeable about protecting data in this environment and managing the cloud environment.

When a public solution is selected, various levels of service can be purchased. Some of these levels include

- **Infrastructure as a service (IaaS)** involves the vendor providing the hardware platform or data center and the company installing and managing its own operating systems and application systems. The vendor simply provides access to the data center and maintains that access.

Key Topic

- **Platform as a service (PaaS)** involves the vendor providing the hardware platform or data center and the software running on the platform. This includes the operating systems and infrastructure software. The company is still involved in managing the system.
- **Software as a service (SaaS)** involves the vendor providing the entire solution. This includes the operating system, infrastructure software, and the application. It might provide you with an email system, for example, whereby the vendor hosts and manages everything for you.

Figure 3-28 shows the relationship of these services to one another.

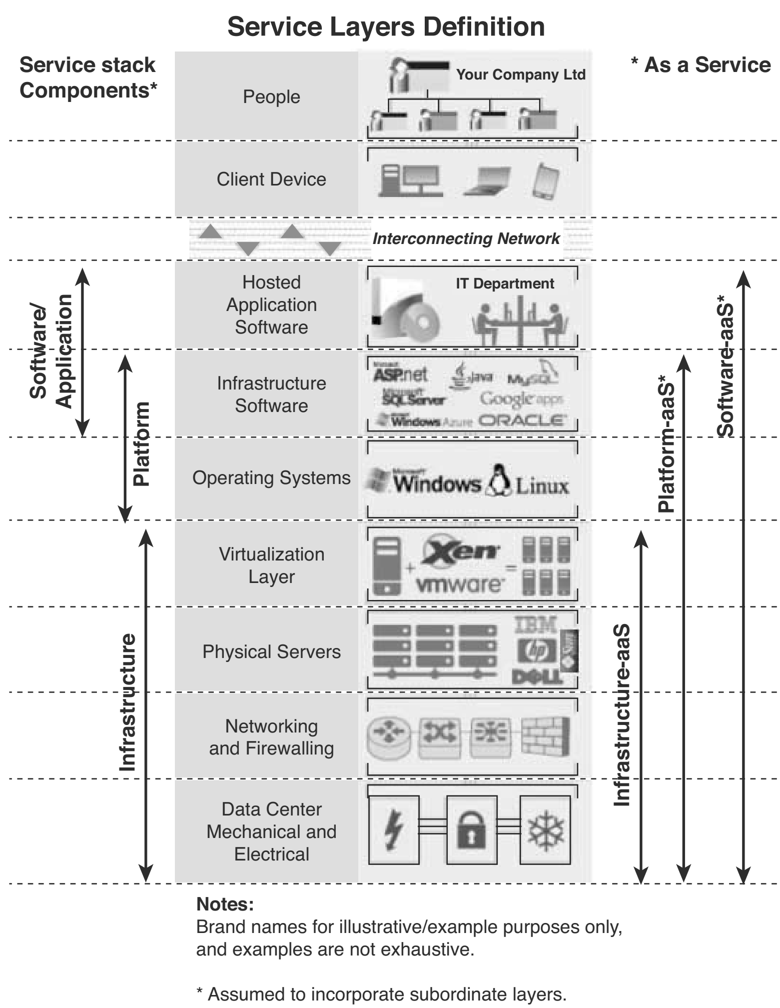

Figure 3-28 Cloud Computing

Endpoint Security

Endpoint security is a field of security that attempts to protect individual systems in a network by staying in constant contact with these individual systems from a central location. It typically works on a client server model in that each system will have software that communicates with the software on the central server. The functionality provided can vary.

In its simplest form, this incudes monitoring and automatic updating and configuration of security patches and personal firewall settings. In more advanced systems, it might include an examination of the system each time it connects to the network. This examination would ensure that all security patches are up to date and in even more advanced scenarios it could automatically provide remediation to the computer. In either case the computer would not be allowed to connect to the network until the problem is resolved, either manually or automatically.

Network Types

So far we have discussed network topologies and technologies, so now let's look at a third way to describe networks: *network type*. Network type refers to the scope of the network. Is it a LAN or a WAN? Is it a part of the internal network, or is it an extranet? This section discusses and differentiates all these network types.

LAN

First let's talk about what makes a local area network (LAN) local. Although classically we think of a LAN as a network located in one location, such as a single office, referring to a LAN as a group of systems that are connected with a *fast* connection is more correct. For purposes of this discussion, that is any connection over 10 Mbps.

That might not seem very fast to you, but it is when compared to a wide area connection (WAN). Even a T1 connection is only 1.544 Mbps. Using this as our yardstick, if a single campus network has a WAN connection between two buildings, then the two networks are considered two LANs rather than a single LAN. In most cases, however, networks in a single campus are typically NOT connected with a WAN connection, which is why usually you hear a LAN defined as a network in a single location.

Intranet

Within the boundaries of a single LAN, there can be subdivisions for security purposes. The LAN might be divided into an intranet and an extranet. The intranet is the internal network of the enterprise. It would be considered a trusted network and typically houses any sensitive information and systems and should receive maximum protection with firewalls and strong authentication mechanisms.

Extranet

An extranet is a network logically separate from the intranet where resources that will be accessed from the outside world are made available. Access might be granted to customers, business partners, and the public in general. All traffic between this network and the intranet should be closely monitored and securely controlled. Nothing of a sensitive nature should be placed in the extranet.

MAN

A Metropolitan Area Network (MAN) is a type of LAN that encompasses a large area such as the downtown of a city. In many cases it is a backbone that is provided for LANs to hook into. Three technologies are usually used in a MAN:

- Fiber Distributed Data Interface (FDDI)
- Synchronous Optical Networks (SONET)
- Metro Ethernet

FDDI and SONET rings, which both rely on fiber cabling, can span large areas, and businesses can connect to the rings using T1, fractional T1, or T3 connections. As you saw earlier, FDDI rings are a double ring with fault tolerance built in. SONET is also *self-healing*, meaning it has a double ring with a backup line if a line goes bad.

Metro Ethernet is the use of Ethernet technology over a wide area. It can be pure Ethernet or a combination of Ethernet and other technologies such as the ones mentioned in this section. Traditional Ethernet (the type used on a LAN) is less scalable. It is often combined with Multiple Protocol Label Switching (MPLS) technology, which is capable of carrying packets of various types, including Ethernet.

Less capable MANs often feed into MANs of higher capacity. Conceptually, you can divide the MAN architecture into three sections: customer, aggregation, and core layer. The customer section is the local loop that connects from the customer to the aggregation network, which then feeds into the high-speed core. The high-speed core connects the aggregation networks to one another.

WAN

Finally, WANs are used to connect LANs and MANs together. Many technologies can be used for these connections. They vary in capacity and cost, and access to these networks is purchased from a telecommunications company. The ultimate WAN is the Internet, the global backbone to which all MANs and LANs are connected. However, not all WANs connect to the Internet because some are private, dedicated links to which only the company paying for them has access. WAN technologies are discussed more fully in the next section.

WAN Technologies

Many different technologies have evolved for delivering WAN access to a LAN. They differ in capacity, availability, and, of course, cost. This section compares the various technologies.

T Lines

T carriers are dedicated lines to which the subscriber has private access and does not share with another customer. Customers can purchase an entire T1, or they can purchase a part of a T1 called a fractional T1. T1 lines consist of 24 channels, each capable of 64 Kbps. This means a T1 has a total capacity of 1.544 Mbps. The T1 is split into channels through a process called time division multiplexing (TDM).

The drawback of a T1 is that the customer is buying the full capacity of the number of channels purchased, and any capacity left unused is wasted. This inflexibility and the high cost have made this option less appealing that it was at one time. The cost is a function of not only the number of channels but the distance of the line as well.

T carriers also come in larger increments as well. Table 3-7 shows a summary of T carriers and their capacity.

Table 3-7 T Carriers

Key Topic

Carrier	# of T1s	# of Channels	Speed (Mbps)
Fractional	1/24	1	.064
T1	1	24	1.544
T3	28	672	44.736

E Lines

In Europe, a similar technology to T-carrier lines exists called E carriers. With this technology, 30 channels are bundled rather than 24. These technologies are not compatible, and the available sizes are a bit different. Table 3-8 shows some selected increments of E carriers.

Key Topic

Table 3-8 E Carriers

Signal	Rate
E0	64 Kbps
E1	2.048 Mbps
E3	8.448 Mbps

OC Lines (SONET)

Synchronous Optical Networks (SONET) use fiber-based links that operate over lines measured in optical carrier (OC) transmission rates. These lines are defined by an integer value of the basic unit of rate. The basic OC-1 rate is 55.84 Mbps, and all other rates are multiples of that. For example, an OC3 yields 155.52 Mbps. Table 3-9 shows some of these rates. Smaller increments such as OC-2 or OC-9 might be used by a company, whereas the larger pipes such as OC-3072 would be used by a service provider.

Key Topic

Table 3-9 Carrier Rates

Optical Carrier	Speed
OC-9	466.56 Mbps
OC-19	933.12 Mbps
OC-48	2.488 Gbps
OC-3072	160 Gbps

CSU/DSU

A discussion of WAN connections would not be complete without discussing a device that many customers connect to for their WAN connection. A Channel Service Unit/Data Service Unit (CSU/DSU) connects a LAN to a WAN. This device performs a translation of the information from a format that is acceptable on the LAN to one that can be transmitted over the WAN connection.

The CSU/DSU is considered a Data Communications Equipment (DCE) device, and it provides an interface for the router, which is considered a Data Terminal Equipment (DTE) device. The CSU/DSU will most likely be owned by the Telco, but not always, and in some cases this functionality might be built into the interface of the router, making a separate device unnecessary.

Circuit-Switching Versus Packet-Switching

On the topic of WAN connections, discussing the types of networks that these connections might pass through is also helpful. Some are circuit-switched, whereas others are packet-switched. Circuit-switching networks (such as the telephone) establish a set path to the destination and only use that path for the entire communication. It results in a predictable operation with fixed delays. These networks usually carry voice-oriented traffic.

Packet-switching networks (such as the Internet or a LAN) establish an optimal *path-per-packet*. This means each packet might go a different route to get to the destination. The traffic on these networks experiences performance bursts and the amount of delay can vary widely. These types of networks usually carry data-oriented traffic.

Frame Relay

Frame relay is a layer 2 protocol used for WAN connections. Therefore, when Ethernet traffic must traverse a frame relay link, the layer 2 header of the packet will be completely recreated to conform to frame relay. When the frame relay frame arrives at the destination, a new Ethernet layer 2 header will be placed on the packet for that portion of the network.

When frame relay connections are provisioned, the customer pays for a minimum amount of bandwidth called the Committed Information Rate (CIR). That will be the floor of performance. However, because frame relay is a packet-switched network using frame relay switches, the actual performance will vary based on conditions. Customers are sharing the network rather than having a dedicated line, such as a T1 or Integrated Services Digital Network (ISDN) line. So in many cases the actual performance will exceed the CIR.

ATM

Asynchronous Transfer Mode (ATM) is a cell-switching technology. It transfers fixed size cells of 53 bytes rather than packets, and after a path is established, it uses the same path for the entire communication. The use of a fixed path makes performance more predictable, making it a good option for voice and video, which need such predictability. Where IP networks depend on the source and destination devices to ensure data is properly transmitted, this responsibility falls on the shoulders of the devices between the two in the ATM world.

ATM is used mostly by carriers and service providers for their backbones, but some companies have implemented their own ATM backbones and ATM switches. This allows them to make an ATM connection to the carrier, which can save money over connection with a T link because the ATM connection cost will be based on usage, unlike the fixed cost of the T1.

X.25

X.25 is somewhat like frame relay in that traffic moves through a packet-switching network. It charges by bandwidth used. The data is divided into 128-byte High-Level Data Link Control (HDLC) frames. It is, however, an older technology created in a time when noisy transmission lines were a big concern. Therefore, it has many error-checking mechanisms built in that make it very inefficient.

Switched Multimegabit Data Service

Switched Multimegabit Data Service (SMDS) is a connectionless, packet-switched technology that communicates across an established public network. It has been largely repacked with other WAN technologies. It can provide LAN-like performance to a WAN. It's generally delivered over a SONET ring with a maximum effective service radius of around 30 miles.

Point-to-Point Protocol

Point-to-Point-Protocol (PPP) is a layer 2 protocol that performs framing and encapsulation of data across point-to-point connections. These are connections to the ISP where only the customer device and the ISP device reside on either end. It can encapsulate a number of different LAN protocols such as TCP/IP, IPX/SPX, and so on. It does this by using a Network Core Protocol (NCP) for each of the LAN protocols in use.

Along with the use of multiple NCPs, it uses a single Link Control Protocol (LCP) to establish the connection. PPP provides the ability to authenticate the connection between the devices using either Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). Whereas PAP transmits the credentials in clear text, CHAP does NOT send the credentials across the line and is much safer.

High-Speed Serial Interface

High-Speed Serial Interface (HSSI) is one of the many physical implementations of a serial interface. Because these interfaces exist on devices, they are considered to operate at layer 1 of the OSI model. The Physical layer is the layer that is concerned with the signaling of the message and the interface between the sender or receiver and the medium. Examples of other serial interface are

- X.25
- V.35
- X.21

The HSSI interface is found on both routers and multiplexers and provides a connection to services such as frame relay and ATM. It operates at speeds up to 52 Mbps.

PSTN (POTS, PBX)

Probably the least attractive WAN connection available, at least from a performance standpoint, is the Public Switched Telephone Network (PSTN). Also referred to as the Plain Old Telephone Service (POTS), this is the circuit-switched network that has been used for analog phone service for years and is now mostly a digital operation.

This network can be utilized using modems for an analog line or with ISDN for digital phone lines. Both these options are discussed in more detail in the section "Remote Connection Technologies" because that is their main use. In some cases these connections might be used between offices but due to the poor performance, typically only as a backup solution in case a more capable option fails. These connections must be established each time they are used as opposed to "always on" solutions, such as cable or DSL.

PBX devices were discussed in the earlier section "Network Devices."

VoIP

Although voice over the PSTN is circuit-switched, voice can also be encapsulated in packets and sent across packet-switching networks. When this is done over an IP network, it is called Voice over IP (VoIP). Where circuit-switching networks use the Signaling System 7 (SS7) protocol to set up, control, and disconnect a call, VoIP uses Session Initiation Protocol (SIP) to break up the call sessions. In VoIP implementations, QoS is implemented to ensure that certain traffic (especially voice) is given preferential treatment over the network.

SIP is an application layer protocol that can operate over either TCP or UDP. Addressing is in terms of IP addresses, and the voice traffic uses the same network used for regular data. Because latency is always possible on these networks, protocols have been implemented to reduce the impact as this type of traffic is much more affected by delay. Applications such as voice and video need to have protocols and devices that can provide an isochronous network. Isochronous networks guarantee continuous bandwidth without interruption. It doesn't use an internal clock source or start and stop bits. All bits are of equal importance and are anticipated to occur at regular intervals.

VoIP can be secured by taking the following measures:

- Create a separate VLAN or subnet for the IP phones and prevent access to this VLAN by PCs.
- Deploy a VoIP-aware firewall at the perimeter.
- Ensure that all passwords related to VoIP are strong.
- Secure the network layer with IPsec.

Remote Connection Technologies

In many cases connections must be made to the main network from outside the network. The reasons for these connections are varied. In some cases it is for the purpose of allowing telecommuters to work on the network as if sitting in the office with all network resources available to them. In another instance, it is for the purposes of managing network devices, whereas in others it could be to provide connections between small offices and the main office.

In this section, some of these connection types are discussed along with some of the security measures that go hand in hand with them. These measures include both encryption mechanisms and authentication schemes.

Dial-up

A dial-up connection is one that uses the PSTN. If it is initiated over an analog phone line, it requires a modem that converts the digital data to analog on the sending end with a modem on the receiving end converting it back to digital. These lines operate up to 56 Kbps.

Dial-up connections can use either Serial Line Internet Protocol (SLIP) or PPP at layer 2. SLIP is an older protocol that has been made obsolete by PPP. PPP provides authentication and multilink capability. The caller is authenticated by the remote access server. This authentication process can be centralized by using either a TACACS+ or RADIUS server. These servers are discussed more fully later in this section.

Some basic security measures that should be in place when using dial-up are

- Have the remote access server call back the initiating caller at a preset number. Do NOT allow call forwarding because it can be used to thwart this security measure.
- Modems should be set to answer after a set number of rings to thwart war dialers (more on them later).

- Consolidate the modems in one place for physical security, and disable modems not in use.
- Use the strongest possible authentication mechanisms.

If the connection is done over a digital line, it can use ISDN. It also must be dialed up to make the connection but offers much more capability and the entire process is all digital. ISDN is discussed next.

ISDN

Integrated Services Digital Network (ISDN) is sometimes referred to as digital dial-up. The really big difference between ISDN and analog dial-up is the performance. ISDN can be provisioned in two ways:

- **Basic rate (BRI):** Provides three channels—two B channels that provide 64 Kbps each and a D channel that is 16 Kbps for a total of 144 Kbps.
- **Primary Rate (PRI):** Can provide up to 23 B channels and a D channel for a total of 1.544 Mbps.

Although ISDN is typically now only used as a backup connection solution and many consider ISDN to be a dedicated connection and thus safe, attacks can be mounted against ISDN connections, including

- **Physical attacks:** These are attacks by persons who are able to physically get to network equipment. With regard to ISDN, shared telecom closets can provide an AP. Physical security measures to follow are described in Chapter 11, “Physical (Environmental) Security.”
- **Router attacks:** If a router can be convinced to accept an ISDN call from a rogue router, it might allow an attacker access to the network. Routers should be configured to authenticate with one another before accepting call requests.

DSL

Digital Subscribers Line (DSL) is a very popular option that provides a high-speed connection from a home or small office to the ISP. Although it uses the existing phone lines, it is an always-on connection. By using different frequencies than the voice transmissions over the same copper lines, talking on the phone and using the data network (Internet) at the same time is possible.

It also is many times faster than ISDN or dial-up. It comes in several variants, some of which offer the same speed uploading and downloading (which is called symmetric service) while most offer better download performance than upload performance (called asymmetric service). Some possible versions are:

- **Symmetric DSL (SDSL)** usually provides from 192 Kbps to 1.1 Gbps in both directions. It is usually used by businesses.
- **Asymmetric DSL (ADSL)** usually provides uploads from 128 Kbps–384 Kbps and downloads up to 768 Kbps. It is usually used in homes.
- **High Bit-Rate DSL (HDSL)** provides T1 speeds.
- **Very High Bit-Rate DSL (VDSL**) is capable of supporting High Definition TV (HDTV) and VoIP.

Unlike cable connections, DSL connections are dedicated links, but there are still security issues to consider. The PCs that are used to access the DSL line should be set with the following options in Internet Options:

- Check for publisher's certificate revocation.
- Enable memory protection to help mitigate online attacks.
- Enable SmartScreen Filter.
- Use SSL 3.0.
- Use TLS 1.0.
- Warn about certificate address mismatch.
- Warn if POST submittal is redirected to a zone that does not permit posts.

Another issue with DSL is the fact it is always connected. This means that the PC typically keeps the same IP address. A static IP address provides a fixed target for the attacker. Therefore, taking measures such as NAT helps to hide the true IP address of the PC to the outside world.

Cable

Getting connections to the ISP using the same cabling system used to deliver cable TV is also possible. Cable modems can provide up to 50 Mbps over the coaxial cabling used for cable TV. Cable modems conform to the Data-Over-Cable Service Interface Specification (DOCSIS) standard.

A security and performance concern with cable modems is that each customer is on a shared line with neighbors. This means performance varies with the time of day and congestion and the data is traveling over a shared medium. For this reason, many cable companies now encrypt these transmissions.

VPN

Virtual Private Network (VPN) connections are those that use an untrusted carrier network but provide protection of the information through strong authentication protocols and encryption mechanisms. Although we typically use the most untrusted network, the Internet as the classic example, and most VPNs do travel through the Internet, they can be used with interior networks as well whenever traffic needs to be protected from prying eyes.

When discussing VPN connections, many new to the subject become confused by the number and type of protocols involved. Let's break down what protocols are required, which are optional, and how they all play together. Recall how the process of encapsulation works. Earlier we discussed this concept when we talked of packet creation, and in that context we applied it to how one layer of the OSI model "wraps around" or encapsulates the other data already created at the other layers.

In VPN operations, entire protocols wrap around other protocols (a process called encapsulation). They include

- A LAN protocol (required)
- A remote access or line protocol (required)
- An authentication protocol (optional)
- An encryption protocol (optional)

Let's start with the original packet before it is sent across the VPN. This is a LAN packet, probably a TCP/IP packet. The change that will be made to this packet is it will be wrapped in a line or remote access protocol. This protocol's only job is to carry the TCP/IP packet still fully intact across the line and then, just like a ferry boat drops a car at the other side of a river, it de-encapsulates the original packet and delivers it to the destination LAN unchanged.

Several of these remote access or line protocols are available. Among them are

- Point-to-Point-Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)

PPTP is a Microsoft protocol based on PPP. It uses built-in Microsoft Point-to-Point Encryption (MPPE) and can use a number of authentication methods, including CHAP, MS-CHAP, and EAP-TLS. One shortcoming of PPTP is that it only works on IP-based networks. If a WAN connection is in use that is not IP-based, L2TP must be used.

MS-CHAP comes in two versions. Both versions can be susceptible to password attacks. Version 1 is inherently insecure and should be avoided. Version 2 is much safer but can still suffer brute-force attacks on the password, although such attacks usually take up to 23 hours to crack the password. Moreover, the MPPE used with MS-CHAP can suffer attacks on the RC4 algorithm on which it is based. Although PPTP is a better solution, it also has been shown to have known vulnerabilities related to the PPP authentication protocols used and is no longer recommended by Microsoft.

Although EAP-TLS is superior to both MS-CHAP and PPTP, its deployment requires a public key infrastructure (PKI), which is often not within the technical capabilities of the network team or the resources to maintain it are not available.

L2TP is a newer protocol that operates at layer 2 of the OSI model. It can use various authentication mechanisms such as PPTP can but does not provide any encryption. It is typically used with IPsec, a very strong encryption mechanism.

With PPTP, the encryption is included, and the only remaining choice to be made is the authentication protocol. These authentication protocols are discussed later in the section "Remote Authentication Protocols."

With L2TP, both encryption and authentication protocols, if desired, must be added. IPsec can provide encryption, data integrity, and system-based authentication, which makes it a flexible and capable option. By implementing certain parts of the IPsec suite, these features can be used or not.

IPsec is actually a suite of protocols in the same way that TCP/IP is. It includes the following components:

- **Authentication Header (AH):** Provides data integrity, data origin authentication, and protection from replay attacks.
- **Encapsulating Security Payload (ESP):** Provides all that AH does as well as data confidentiality.
- **Internet Security Association and Key Management Protocol (ISAKMP):** Handles the creation of a security association for the session and the exchange of keys.
- **Internet Key Exchange (IKE), also sometimes referred to as IPsec Key Exchange:** Provides the authentication material used to create the keys exchanged by ISAKMP during peer authentication. This was proposed to be performed by a protocol called Oakley that relied on the Diffie-Hellman algorithm, but Oakley has been superseded by IKE.

You can find more information on IPsec in Chapter 6, "Cryptography."

IPsec is a framework, which means it does not specify many of the components used with it. These components must be identified in the configuration, and they must match for the two ends to successfully create the required security association that must be in place before any data is transferred. The selections that must be made are:

- The encryption algorithm (encrypts the data)
- The hashing algorithm (ensures the data has not been altered and verifies its origin)
- The mode (tunnel or transport)
- The protocol (AH, ESP, or both)

All these settings must match on both ends of the connection. It is not possible for the systems to select these on the fly. They must be preconfigured correctly to match.

When the tunnel is configured in tunnel mode, the tunnel exists only between the two gateways but all traffic that passes through the tunnel is protected. This is normally used to protect all traffic between two offices. The security association (SA) is between the gateways between the offices. This is the type of connection that would be called a site-to-site VPN.

The SA between the two endpoints is made up of the security parameter index (SPI) and the AH/ESP combination. The SPI, a value contained in each IPsec header, help the devices maintain the relationship between each SA (of which there could be several happening at once) and the security parameters (also called the transform set) used for each SA.

Each session has a unique session value which help to prevent:

- Reverse engineering
- Content modification
- Factoring attacks (the attacker tries all the combinations of numbers that can be used with the algorithm to decrypt ciphertext)

With respect to authenticating the connection, the keys can be pre-shared or derived from a PKI. A PKI creates a public/private key pair that is associated with individual users and computers that use a certificate. These key pairs are used in the place of pre-shared keys in that case. Certificates can also be used that are not derived from a PKI.

In transport mode, the SA is either between two end stations or an end station and a gateway or remote access server. In this mode, the tunnel extends from computer to computer or from computer to gateway. This is the type of connection that would be for a remote access VPN. This is but one application of IPsec. It is also used in other applications such as a General Packet Radio Service (GPRS), a VPN solution for devices using a 2G cell phone network.

When the communication is from gateway to gateway or host to gateway, either transport or tunnel mode can be used. If the communication is computer to computer, the tunnel must be in transport mode. If the tunnel is configured in transport mode from gateway to host, the gateway must operate as a host.

The most effective attack against IPsec VPN is a man-in-the-middle attack. In this attack, the attacker proceeds through the security negotiation phase until the key negotiation when the victim reveals its identity. In a well-implemented system, the attacker will fail when the attacker cannot likewise prove his identity.

RADIUS and TACACS

When users are making connections to the network through a variety of mechanisms, they should be authenticated first. These users could be accessing the network through

- Dial-up remote access servers
- VPN access servers
- Wireless Access Points
- Security-enabled switches

At one time each of these access devices would perform the authentication process locally on the device. The administrators would need to ensure that all remote access policies and settings were consistent across them all. When a password required changing, it had to be done on all devices.

Remote Authentication Dial In User Service (RADIUS) and Terminal Access Controller Access-Control System Plus (TACACS+) are networking protocols that provide centralized authentication and authorization. These services can be run at a central location, and all the access devices (AP, remote access, VPN, and so on) can be made clients of the server. Whenever authentication occurs, the TACACS+ or RADIUS server performs the authentication and authorization. This provides one location to manage the remote access policies and passwords for the network. Another advantage of using these systems is that the audit and access information (logs) are not kept on the access server.

TACACS and TACACS+ are Cisco proprietary services that operate in Cisco devices, whereas RADIUS is a standard defined in RFC 2138. Cisco has implemented several versions of TACACS over time. It went from TACACS to XTACACS to the latest version, TACACS+. The latest version provides authentication, accounting, and authorization, which is why it is sometimes referred to as an AAA service. TACACS+ employs tokens for two-factor, dynamic password authentication. It also allows users to change their passwords.

RADIUS is designed to provide a framework that includes three components. The *supplicant* is the device seeking authentication. The authenticator is the device to which they are attempting to connect (AP, switch, remote access server), and the RADIUS server is the authentication server. With regard to RADIUS, the device seeking entry is *not* the RADIUS client. The authenticating server is the RADIUS server, and the authenticator (AP, switch, remote access server) is the RADIUS client.

In some cases a RADIUS server can be the client of another RADIUS server. In that case the RADIUS server acts as a proxy client for its RADIUS clients.

Diameter is another authentication protocol based on RADIUS and is *not* compatible with RADIUS. Diameter has a much larger set of attribute-value pairs (AVPs) than RADIUS, allowing more functionality and services to communicate, but has not been widely adopted.

Remote Authentication Protocols

Earlier we said that one of the protocol choices that must be made when provisioning a remote access solution is the authentication protocol. This section discusses some of the most important of those protocols:

- **Password Authentication Protocol (PAP**) provides authentication but the credentials are sent in clear text and can be read with a sniffer.
- **Challenge Handshake Authentication Protocol (CHAP)** solves the cleartext problem by operating without sending the credentials across the link. The server sends the client a set of random texts called a challenge. The client encrypts the text with the password and sends it back. The server then decrypts it with the same password and compares the result with what was sent originally. If the results match, then the server can be assured that the user or system possesses the correct password without ever needing to send it across the untrusted network.
- **Extensible Authentication Protocol (EAP)** is not a single protocol but a framework for port-based access control that uses the same three components that are used in RADIUS. A wide variety of these implementations can use all sorts of authentication mechanisms, including certificates, a PKI, or even simple passwords.

Telnet

Telnet is a remote access protocol used to connect to a device for the purpose of executing commands on the device. It can be used to access servers, routers, switches, and many other devices for the purpose of managing them. Telnet is not considered a secure remote management protocol because like another protocol used with UNIX-based systems, rlogin, it transmits all information including the authentication process in clear text. Alternatives such as SSH have been adopted to perform the same function while providing encryption. Telnet and rlogin connections are connection-oriented so they use TCP as the transport protocol.

TLS/SSL

Transport Layer Security/Secure Sockets Layer (TLS/SSL) is another option for creating secure connections to servers. It works at the Application layer of the OSI model. It is used mainly to protect HTTP traffic or web servers. Its functionality is embedded in most browsers, and its use typically requires no action on the part of the user. It is widely used to secure Internet transactions. It can be implemented in two ways:

- **SSL portal VPN**, in which a user has a single SSL connection used to access multiple services on the web server. After being authenticated, the user is provided a page that acts as a portal to other services.
- **SSL tunnel VPN** uses an SSL tunnel to access services on a server that is not a web server. It uses custom programming to provide access to non-web services through a web browser.

TLS and SSL are very similar but not the same. TLS 1.0 is based on the SSL 3.0 specification but they are not operationally compatible. Both implement confidentiality, authentication, and integrity above the Transport layer. The server is always authenticated and optionally the client also can be. SSL v2 must be used for client-side authentication. When configuring SSL, a session key length must be designated. The two options are 40 bit and 128 bit. It prevents man-in-the middle attacks by using self-signed certificates to authenticate the server public key.

Multimedia Collaboration

In today's modern enterprises, the sharing of multimedia during both web presentations or meetings and instant messaging programs has exploded. Note that not all collaboration tools and products are created equally in regard to the security. Many were built with an emphasis on ease of use rather than security. This is a key issue to consider when choosing a product. For both the presenter and the recipient, the following security requirements should be met:

- Data confidentiality
- Origin authentication
- Identity confidentiality
- Data integrity
- Non-repudiation of receipt
- Repudiation of transmission
- Non-repudiation of transmission
- Availability to present
- Availability to receive

Wireless Networks

Perhaps the area of the network that keeps more administrators awake at night is the wireless portion of the network. In the early days of 802.11 WLAN deployments, many chose to simply not implement wireless for fear of the security holes it creates. However, it became apparent that not only did users demand this, but in some cases users were bringing home APs to work and hooking them up and suddenly there was a wireless network!

Today WLAN security has evolved to the point that security is no longer a valid reason to avoid wireless. This section offers a look at the protocols used in wireless, the methods used to convert the data into radio waves, the various topologies in which WLANs can be deployed, and security measures that should be taken.

FHSS, DSSS, OFDM, FDMA, TDMA, CDMA, OFDMA, and GSM

When data leaves an Ethernet network interface controller (NIC) and is sent out on the network, the ones and zeros that constitute the data are represented with different electric voltages. In wireless, this information must be represented in radio waves. A number of different methods exist for performing this operation, which is called modulation. You should also understand some additional terms to talk intelligently about wireless. This section defines a number of terms to provide a background for the discussion found in the balance of this section. The first section covers techniques used in WLAN and the second covers techniques used in cellular networking.

802.11 Techniques

- **Frequency Hopping Spread Spectrum (FHSS**) is one of two technologies (along with DSSS) that were a part of the original 802.11 standard. It is unique in that it changes frequencies or channels every few seconds in a set pattern that both transmitter and receiver know. This is not a security measure because the patterns are well known, although it does make capturing the traffic difficult. It helps avoid inference by only occasionally using a frequency where the inference is present. Later amendments to the 802.11 standard did not include this technology. It can attain up to 2 Mbps.
- **Direct Sequence Spread Spectrum (DSSS)** is one of two technologies (along with FHSS) that were a part of the original 802.11 standard. This is the modulation technique used in 802.11b. The modulation technique used in wireless has a huge impact on throughput. In the case of DSSS, it spreads the transmission across the spectrum at the same time as opposed to hopping from one to another as in FHSS. This allows it to attain up to 11 Mbps.
- **Orthogonal Frequency Division Multiplexing (OFDM)** is a more advanced technique of modulation where a large number of closely spaced orthogonal sub-carrier signals are used to carry the data on several parallel data streams. It is used in 802.11a and 802.11g. It makes speed up to 54 Mbps possible.

Cellular or Mobile Wireless Techniques

- **Frequency Division Multiple Access (FDMA)** is one of the modulation techniques used in cellular wireless networks. It divides the frequency range into bands and assigns a band to each subscriber. This was used in 1G cellular networks.
- **Time Division Multiple Access (TDMA)** increases the speed over FDMA by dividing the channels into time slots and assigning slots to calls. This also helps to prevent eavesdropping in calls.
- **Code Division Multiple Access (CDMA)** assigns a unique code to each call or transmission and spreads the data across the spectrum, allowing a call to make use of all frequencies.
- **Orthogonal Frequency Division Multiple Access (OFDMA)** takes FDMA a step further by subdividing the frequencies into subchannels. This is the technique required by 4G devices.
- **Global System Mobile (GSM)** is a type of cellphone that contains a Subscriber Identity Module (SIM) chip. These chips contain all the information about the subscriber and must be present in the phone for it to function. One of the dangers with these phones is cell *phone cloning*, a process where copies

of the SIM chip are made, allowing another user to make calls as the original user. Secret key cryptography is used (using a common secret key) when authentication is performed between the phone and the network.

WLAN Structure

Before we can discuss 802.11 wireless, which has come to be known as WLAN, we need to discuss the components and the structure of a WLAN. This section covers basic terms and concepts.

Access Point

An access point (AP) is a wireless transmitter and receiver that hooks into the wired portion of the network and provides an access point to this network for wireless devices. In some cases they are simply wireless switches, and in other cases they are also routers. Early APs were devices with all the functionality built into each device, but increasingly these “fat” or intelligent APs are being replaced with “thin” APs that are really only antennas that hook back into a central system called a controller.

SSID

The service set identifier (SSID) is a name or value assigned to identify the WLAN from other WLANs. The SSID can either be broadcast by the AP as is done in a free hot spot or it can be hidden. When it is hidden, a wireless station will have to be configured with a profile that includes the SSID to connect. Although some view hiding the SSID as a security measure, it is not an effective measure because hiding the SSID only removes one type of frame, the beacon frame, while it still exists in other frame types and can be easily learned by sniffing the wireless network.

Infrastructure Mode Versus Ad Hoc Mode

In most cases a WLAN includes at least one AP. When an AP is present, the WLAN is operating in *Infrastructure* mode. In this mode, all transmissions between stations go through the AP, and no direct communication between stations occurs. In *Ad Hoc* mode, there is no AP, and the stations communicate directly with one another.

WLAN Standards

The original 802.11 wireless standard has been amended a number of times to add features and functionality. This section discusses these amendments, which are sometimes referred to as standards although they really are amendments to the original standard. The original 802.11 standard specified the use of either FHSS or DSSS and supported operations in the 2.4 GHz frequency range at speeds of 1 Mbps and 2 Mbps.

Key Topic

802.11a

The first amendment to the standard was 802.11a. This standard called for the use of OFDM. Because that would require hardware upgrades to existing equipment, this standard saw limited adoption for some time. It operates in a different frequency than 802.11 (5 GHz) and by using OFDM supports speeds up to 54 Mbps.

802.11b

The 802.11b amendment dropped support for FHSS and enabled an increase of speed to 11 Mbps. It was widely adopted because it both operates in the same frequency as 802.11 and is backward compatible with it and can coexist in the same WLAN.

802.11f

The 802.11f amendment addressed problems introduced when wireless clients roam from one AP to another. This causes the station to need to reauthenticate with the new AP, which in some cases introduced a delay that would break the application connection. This amendment improves the sharing of authentication information between APs.

802.11g

The 802.11g amendment added support for OFDM, which made it capable of 54 Mbps. This also operates in the 2.4 GHz frequency so it is backward compatible with both 802.11 and 802.11b. While just as fast as 802.11a, one reason many switched to 802.11a is that the 5 GHz band is much less crowded than the 2.4 GHz band.

802.11n

The 802.11n standard uses several newer concepts to achieve up to 650 Mbps. It does these using channels that are 40 MHz wide, using multiple antennas that allow for up to four spatial streams at a time (a feature called Multiple Input Multiple Output or MIMO). It can be used in both the 2.4 GHz and 5.0 GHz bands but performs best in a pure 5.0 GHz network because in that case it does not need to implement mechanisms that allow it to coexist with 802.11b and 802.11g devices. These mechanisms slow the performance.

Bluetooth

Bluetooth is a wireless technology that is used to create Personal Area Networks (PANs). These are simply short-range connections that are between devices and peripherals, such as headphones. It operates in the 2.4 GHz frequency at speeds of 1 Mbps to 3 Mbps at a distance of up to 10 meters.

Several attacks can take advantage of Bluetooth technology. Bluejacking is when an unsolicited message is sent to a Bluetooth-enabled device often for the purpose of adding a business card to the victim's contact list. This can be prevented by placing the device in non-discoverable mode.

Bluesnarfing is the unauthorized access to a device using the Bluetooth connection. In this case the attacker is trying to access information on the device rather than send messages to the device.

Infrared

Finally, infrared is a short-distance wireless process that uses light rather than radio waves, in this case infrared light. It is used for short connections between devices that both have an infrared port. It operates up to 5 meters at speeds up to 4 Mbps and requires a direct line of sight between the devices. There is one infrared mode or protocol that can introduce security issues. The IrTran-P (image transfer) protocol is used in digital cameras and other digital image capture devices. All incoming files sent over IrTran-P are automatically accepted. Because incoming files might contain harmful programs, users should ensure that the files originate from a trustworthy source.

WLAN Security

To safely implement 802.11 wireless technologies, you must understand all the methods used to secure a WLAN. In this section, the most important measures are discussed including some measures that, although they are often referred to as security measures, provide no real security whatsoever.

WEP

Wired Equivalent Privacy (WEP) was the first security measure used with 802.11. It was specified as the algorithm in the original specification. It can be used to both authenticate a device and encrypt the information between the AP and the device. The problem with WEP is that it implements the RC4 encryption algorithm in a way that allows a hacker to crack the encryption. It also was found that the mechanism designed to guarantee the integrity of data (that the data has not changed) was inadequate and that it was possible for the data to be changed and for this fact to go undetected.

WEP is implemented with a secret key or password that is configured on the AP, and any station will need that password to connect. Above and beyond the problem with the implementation of the RC4 algorithm, it is never good security for all devices to share the same password in this way.

WPA

To address the widespread concern with the inadequacy of WEP, the Wi-Fi Alliance, a group of manufacturers that promotes interoperability, created an alternative mechanism called Wi-Fi Protected Access (WPA) that is designed to improve on WEP. There are four types of WPA but first let's talk about how the original version improves over WEP.

First, WPA uses the Temporal Key Integrity Protocol (TKIP) for encryption, which generates a new key for each packet. Second, the integrity check used with WEP is able to detect any changes to the data. WPA uses a message integrity check algorithm called Michael to verify the integrity of the packets. There are two versions of WPA (covered in the section "Personal Versus Enterprise").

Some legacy devices might only support WPA. You should always check with a device's manufacturer to find out whether a security patch has been released that allows for WPA2 support.

WPA2

WPA2 is an improvement over WPA. WPA2 uses Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) based on Advanced Encryption Standard (AES), rather than TKIP. AES is a much stronger method and is required for Federal Information Processing Standards (FIPS)-compliant transmissions. There are also two versions of WPA2 (covered in the next section).

Personal Versus Enterprise

Both WPA and WPA2 come in Enterprise and Personal versions. The Enterprise versions require the use of an authentication server, typically a RADIUS server. The Personal versions do not and use passwords configured on the AP and the stations. Table 3-10 provides a quick overview of WPA and WPA2.

Table 3-10 WPA and WPA2

Key Topic

Variant	Access Control	Encryption	Integrity
WPA Personal	Preshared key	TKIP	Michael
WPA Enterprise	802.1X (RADIUS)	TKIP	Michael
WPA2 Personal	Preshared key	CCMP, AES	CCMP
WPA2 Enterprise	802.1X (RADIUS)	CCMP, AES	CCMP

SSID Broadcast

Issues surrounding the SSID broadcast were covered in the section "WLAN Structure" earlier in this chapter.

MAC Filter

Another commonly discussed security measure that can be taken is to create a list of allowed MAC addresses on the AP. When this is done, only the devices with MAC addresses on the list can make a connection to the AP. Although on the surface, this might seem like a good security measure, in fact a hacker can easily use a sniffer to learn the MAC addresses of devices that have successfully authenticated. Then by changing the MAC address on his device to one that is on the list he can gain entry.

MAC filters can also be configured to deny access to certain devices. The limiting factor in this method is that only the devices with the denied MAC addresses are specifically denied access. All other connections will be allowed.

Satellites

Satellites can be used to provide TV service and have for some time but now they can also be used to deliver Internet access to homes and businesses. The connection is two-way rather than one-way as is done with TV service. This is typically done using microwave technology. In most cases, the downloads come from the satellite signals, whereas the uploads occur through a ground line. Microwave technology can also be used for *terrestrial transmission*, which means ground station to ground station rather than satellite to ground. Satellite connections are very slow but are useful in remote locations where no other solution is available.

Network Threats

Before you can address network security threats, you must be aware of them, understand how they work, and know the measures to take to prevent the attacks from succeeding. This section covers a wide variety of attack types along with measures that should be taken to prevent them from occurring.

Cabling

Although it's true that a cabled network is easier to secure from eavesdropping than a wireless network, you must still be aware of some security issues. You should also understand some general behaviors of cabling that affect performance and ultimately can affect availability. As you might recall, maintaining availability to the network is also one of the goals of CIA, which is explained in Chapter 2, "Access Control." Therefore, performance characteristics of cabling that can impact availability are also discussed.

Noise

Noise is a term used to cover several types of interference than can be introduced to the cable that causes problems. This can be from large electrical motors, other computers, lighting, and other sources. This noise combines with the data signals (packets) on the line and distorts the signal. When even a single bit in a transmission is misread (read as a 1 when it should be a 0 or vice versa), nonsense data is received and retransmissions must occur. Retransmissions lead to lower throughput and in some cases no throughput whatsoever.

In any case where this becomes a problem, the simplest way to mitigate the problem is use shielded cabling. In cases where the noise is still present, locating the specific source and taking measures to remove it (or least the interference it is generating) from the environment might be necessary.

Attenuation

Attenuation is the weakening of the signal as it travels down the cable and meets resistance. In the discussion on cabling earlier in this chapter, you learned that all cables have a recommended maximum length. When you use a cable that is longer than its recommended length, attenuation weakens the signal to the point it cannot be read correctly, resulting in the same problem that is the end result of noise. The data must be sent again lowering throughput.

The solution to this problem is in design. Follow the length recommendations listed in the section on cables earlier in this chapter with any type of cabling. This includes coaxial, twisted pair, and fiberoptic. All types have maximum lengths that should not be exceeded without risking attenuation.

Crosstalk

Crosstalk is a behavior that can occur whenever individual wires within a cable are run parallel to one another. Crosstalk occurs when the signals from the two wires (or more) interfere with one another and distort the transmission. Cables such as twisted-pair cables would suffer from this were the cables not twisted as they are. The twisting prevents the crosstalk from occurring.

Eavesdropping

Although cabling is a bounded media and much easier to secure than wireless, eavesdropping can still occur. All cabling that depends on electrical voltages, such as coaxial and twisted pair, can be tapped or monitored with the right equipment. The least susceptible to eavesdropping (although not completely immune) is fiberoptic cabling because it doesn't use electrical voltages, but rather light waves. In any situation where eavesdropping is a concern, using fiberoptic cabling can be a measure that will at least drastically raise the difficulty of eavesdropping. The real solution is ensuring physical security of the cabling. The cable runs should not be out in the open and available.

ICMP Attacks

Earlier in this chapter you learned about Internet Control Message Protocol (ICMP), one of the protocols in the TCP/IP suite. This protocol is used by devices to send error messages to sending devices when transmission problems occur and is also used when either the ping command or the traceroute command is used for troubleshooting. Like many tools and utilities that were created for good purposes, this protocol can also be used by attackers who take advantage of its functionality.

This section covers ICMP-based attacks. One of the ways to prevent ICMP-based attacks is disallow its use by blocking the protocol number for ICMP, which is 1. Many firewall products also have the ability to only block certain types of ICMP messages as opposed to prohibiting its use entirely. Some of these problematic ICMP message types are discussed in this section as well.

Ping of Death

The Ping of Death is an attack that takes advantage of the normal behavior of devices that receive oversized ICMP packets. ICMP packets are normally a predictable 65,536 bytes in length. Hackers have learned how to insert additional data into

ICMP packets. The Ping of Death attack sends several of these oversized packets, which can cause the victim system to be unstable at the least and possibly freeze up. That results in a denial-of-service attack because it makes the target system less able or even unable to perform its normal function in the network.

Smurf

The Smurf attack is also a denial-of-service attack that uses a type of ping packet called an ICMP ECHO REQUEST. This is an example of a Distributed Denial of Service (DDoS) attack in that the perpetuator enlists the aid of other machines in the network.

When a system receives an ICMP ECHO REQUEST packet, it attempts to answer this request with an ICMP ECHO REPLY packet (usually four times by default). Normally this reply is sent to a single sending system. In this attack, the ECHO REQUEST has its destination address set to the network broadcast address of the network in which the target system resides and the source address is set to the target system. When every system in the network replies to the request, it overwhelms the target device causing it to freeze or crash.

Fraggle

Although not really an ICMP attack because it uses UDP, the Fraggle attack is a DDoS attack with the same goal and method as the Smurf attack. In this attack, an attacker sends a large amount of UDP echo traffic to an IP broadcast address, all of it having a fake source address, which will, of course, be the target system. When all systems in the network reply, the target is overwhelmed.

ICMP Redirect

One of the many types of error messages that ICMP uses is called an ICMP redirect or an ICMP Packet type 5. ICMP redirects are used by routers to specify better routing paths out of one network. When it does this, it changes the path that the packet will take.

By crafting ICMP redirect packets, the attacker alters the route table of the host that receives the redirect message. This changes the way packets are routed in the network to his advantage. After its routing table is altered, the host will continue to use the path for 10 minutes. For this reason, ICMP redirect packets might be one of the types you might want to disallow on the firewall.

Ping Scanning

ICMP can be used to scan the network for live or active IP addresses. This attack basically pings every IP address and keeps track of which IP addresses respond to the ping. This attack is usually accompanied or followed by a port scan, covered later in this chapter.

DNS Attacks

As you might recall in the discussion of DNS earlier in this chapter, DNS resolves computer and domain names to IP addresses. It is a vital service to the network and for that reason multiple DNS servers are always recommended for fault tolerance. DNS servers are a favorite target of DoS and DDoS attacks because of the mayhem taking them down causes.

DNS servers also can be used to divert traffic to the attacker by altering DNS records. In this section, all types of DNS attacks are covered along with practices that can eliminate or mitigate the effect of these attacks.

DNS Cache Poisoning

DNS clients send requests for name-to-IP address resolution (called queries) to a DNS server. The search for the IP address that goes with a computer or domain name usually starts with a local DNS server that is not authoritative for the DNS domain in which the requested computer or website resides. When this occurs, the local DNS server makes a request of the DNS server that does hold the record in question. After the local DNS server receives the answer, it returns it to the local DNS client. After this, the local DNS server maintains that record in its DNS cache for a period called the Time to Live (TTL), which is usually an hour but can vary.

In a DNS cache poisoning attack, the attacker attempts to refresh or update that record when it expires with a different address than the correct address. If he can convince the DNS server to accept this refresh, the local DNS server will then be responding to client requests for that computer with the address inserted by the attacker. Typically the address they now receive is for a fake website that appears to look in every way like the site the client is requesting. The hacker can then harvest all the name and password combinations entered on his fake site.

To prevent this type of attack, the DNS servers should be limited in the updates they accept. In most DNS software, you can restrict the DNS servers from which a server will accept updates. This can help prevent the server from accepting these false updates.

DoS

DNS servers are a favorite target of Denial of Service (DoS) attacks. This is because the loss of DNS service in the network typically brings the network to a halt as many network services depend on its functioning. Any of the assorted type of DoS attacks discussed in this book can be targeted to DNS servers. For example, the Ping of Death might be the attack of choice.

DDoS

Any of the assorted DoS attacks can be amplified by the attacker by recruiting other devices to assist in the attack. Some examples of these attacks are the Smurf and Fraggle attacks (covered earlier).

In some cases the attacker might have used malware to install software on thousands of computers (called zombies) to which he sends commands at a given time, instructing all the devices to launch the attack. Not only does this amplify the attack but it also helps to hide the source of the attack because it appears to come from many places at once.

DNSSEC

One of the newer approaches to preventing DNS attacks is a stronger authentication mechanism called Domain Name System Security Extensions (DNSSEC). Many current implementations of DNS software contain this functionality. It uses digital signatures to validate the source of all messages to ensure they are not spoofed.

The problem with DNSSEC illustrates the classic tradeoff between security and simplicity. To deploy DNSSEC, a PKI must be built and maintained to issue, validate, and renew the public/private key pairs and certificates that must be issued to all the DNS servers. (PKI is covered more fully in Chapter 6.) Moreover, for complete security of DNS, all the DNS servers on the Internet would also need to participate, which complicates the situation further. The work on this continues today.

URL Hiding

An alternate and in some ways simpler way for an attacker to divert traffic to a fake website is a method called URL hiding. This attack takes advantage of the ability to embed URLs in web pages and email. The attacker might refer to the correct name of the website in the text of the webpage or email, but when he inserts the URL that goes with the link he inserts the URL for the fake site. The best protection against this issue is to ask users to not click links on unknown or untrusted websites.

Domain Grabbing

Domain grabbing occurs when individuals register a domain name of a well-known company before the company has the chance to do so. Then later the individuals hold the name hostage until the company becomes willing to pay to get the domain name. In some cases these same individuals monitor the renewal times for well-known websites and register the name before the company has a chance to perform the renewal. Some practices that can help to prevent this are to register domain names for longer periods of time and to register all permutations of the chosen domain name (misspellings and so on).

Cybersquatting

When domain names are registered with no intent to use them but with intent to hold them hostage (as described in the preceding), it is called cybersquatting. The same practices to prevent domain grabbing are called for to prevent the company from becoming a victim of cybersquatting.

Email Attacks

One of the most popular avenues for attacks is a tool we all must use every day, email. In this section, several attacks that use email as the vehicle are covered. In most cases the best way to prevent these attacks is user training and awareness because many of these attacks are based upon poor security practices on the part of the user.

Email Spoofing

Email spoofing is the process of sending an email that appears to come from one source when it really comes from another. It is made possible by altering the fields of email headers such as From, Return Path, and Reply-to. Its purpose is to convince the receiver to trust the message and reply to it with some sensitive information that the receiver would not have shared unless it was a trusted message.

Often this is one step in an attack designed to harvest usernames and passwords for banking or financial sites. This attack can be mitigated in several ways. One is SMTP authentication, which when enabled, disallows the sending of an email by a user that cannot authenticate with the sending server.

Another possible mitigation technique is to implement a Sender Policy Framework (SPF). An SPF is an email validation system that works by using DNS to determine whether an email sent by someone has been sent by a host sanctioned by that domain's administrator. If it can't be validated, it is not delivered to the recipient's box.

Spear Phishing

Phishing is a social engineering attack where a recipient is convinced to click on a link in an email that appears to go to a trusted site but in fact goes to the hacker's site. This is used to harvest usernames and passwords.

Spear phishing is the process of foisting this attack on a specific person rather than a random set of people. The attack might be made more convincing by learning details about the person through social media that the email might reference to boost its appearance of legitimacy.

Whaling

Just as spear phishing is a subset of phishing, whaling is a subset of spear phishing. It targets a single person and in the case of whaling, that person is someone of significance or importance. It might be a CEO, COO, or CTO, for example. The attack is based on the assumption that these people have more sensitive information to divulge.

Spam

No one enjoys the way our email boxes fill every day with unsolicited emails, usually trying to sell us something. In many cases we cause ourselves to receive this email by not paying close attention to all the details when we buy something or visit a site. When email is sent out on a mass basis that is not requested, it is called spam.

Spam is more than an annoyance because it can clog email boxes and cause email servers to spend resources delivering it. Sending spam is illegal so many spammers try to hide the source of the spam by relaying through other corporations' email servers. Not only does this practice hide the email's true source, but it can cause the relaying company to get in trouble.

Today's email servers have the ability to deny relaying to any email servers that you do not specify. This can prevent your email system from being used as a spamming mechanism. This type of relaying should be disallowed on your email servers.

Wireless Attacks

Wireless attacks are some of the hardest to prevent because of the nature of the medium. If you want to make the radio transmissions available to the users then you must make them available to anyone else in the area as well. Moreover, there is no way to determine when someone is capturing your radio waves! You might be able to prevent someone from connecting to or becoming a wireless client on the network, but you can't stop them from using a wireless sniffer to capture the packets.

In this section, some of the more common attacks are covered and some mitigation techniques are discussed as well.

Wardriving

Wardriving is the process of riding around with a wireless device connected to a high-power antenna searching for WLANs. It could be for the purpose of obtaining free Internet access, or it could be to identify any open networks vulnerable to an attack.

Warchalking

Warchalking is a practice that typically accompanies wardriving. When a wardriver locates a WLAN, he indicates in chalk on the sidewalk the SSID and the types of security used on the network. This activity has gone mostly online now as many sites are dedicated to compiling lists of found WLANs and their locations.

Remote Attacks

Although in a sense all attacks such as DoS attacks, DNS poisoning, port scanning, and ICMP attacks are remote in the sense they can be launched from outside the network, remote attacks can also be focused on remote access systems such as VPN servers or dial-up servers. As security practices have evolved, these types of attacks have somewhat diminished.

Wardialing is not the threat that it once was simply because we don't use modems and modem banks as much as we used to. In this attack, software programs attempt to dial large lists of phone numbers for the purpose of identifying numbers attached to modems. When a person or fax machine answers, it records that fact, and when a modem answers, it attempts to make a connection. If this connection is successful, the hacker now has an entryway into the network.

Other Attacks

In this final section of this chapter, some other attacks are covered that might not fall into any of the other categories discussed thus far.

SYN ACK Attacks

The SYN ACK attack takes advantage of the TCP three-way handshake, covered in the section "Transport Layer" earlier in this chapter.

In this attack, the hacker sends a large number of packets with the SYN flag set, which causes the receiving computer to set aside memory for each ACK packet it expects to receive in return. These packets never come and at some point the resources of the receiving computer are exhausted, making this a form of DoS attack.

Session Hijacking

In a session highjacking attack, the hacker attempts to place himself in the middle of an active conversation between two computers for the purpose of taking over the session of one of the two computers, thus receiving all data sent to that computer. A couple of tools can be used for this attack. Juggernaut and the Hunt Project allow the attacker to spy on the TCP session between the computers. Then he uses some sort of DoS attack to remove one of the two computers from the network while spoofing the IP address of that computer and replacing that computer in the conversation. This results in the hacker receiving all traffic that was originally intended for the computer that suffered the DoS attack.

Port Scanning

ICMP can also be used to scan the network for open ports. Open ports indicate services that might be running and listening on a device that might be susceptible to being used for an attack. This attack basically pings every address and port number combination and keeps track of which ports are open on each device as the pings are answered by open ports with listening services and not answered by closed ports.

Teardrop

A teardrop attack is a type of fragmentation attack. The Maximum Transmission Unit (MTU) of a section of the network might cause a packet to be broken up or fragmented, which requires the fragments to be reassembled when received. The hacker sends malformed fragments of packets that when reassembled by the receiver cause the receiver to crash or become unstable.

IP Address Spoofing

IP address spoofing is one of the techniques used by hackers to hide their trail or to masquerade as another computer. The hacker alters the IP address as it appears in the packet. This can sometimes allow the packet to get through an ACL that is based on IP addresses. It also can be used to make a connection to a system that only trusts certain IP addresses or ranges of IP addresses.

Exam Preparation Tasks

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 3-11 lists a reference of these key topics and the page numbers on which each is found.

Table 3-11 Key Topics

Key Topic Element	Description	Page Number
Figure 3-1	Protocol Mappings	70
Figure 3-2	TCP/IP and OSI models	71
Figure 3-4	TCP three-way handshake	74
Figure 3-6	Encapsulation and de-encapsulation	76
Table 3-1	Common UDP and TCP ports	77
Table 3-2	Classful IP addressing	80
Table 3-3	Private IP address ranges	81
Table 3-4	Twisted-pair categories	89
Table 3-6	Ethernet implementations	95
Ordered steps	CSMA/CD	99
Ordered steps	CSMA/CA	100
Section	Cloud computing services	117
Table 3-7	T carriers	121
Table 3-8	E-carriers	122
Table 3-9	Optical carriers	122
Section	WLAN Standards	138
Table 3-10	WPA and WPA2	141

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

Open Systems Interconnect (OSI) model, Application layer, Presentation layer, Session layer, Transport layer (layer 4), Network layer (layer 3), Data Link layer

(layer 2), Physical layer (layer 1), TCP/IP model, TCP three-way handshake, Internet Protocol (IP), Internet Message Control Protocol (ICMP), Internet Group Messaging Protocol (IGMP), Address Resolution Protocol (ARP), Encapsulation, Private IP addresses, Media Access Control (MAC) addresses, Digital, Asynchronous transmission, Synchronous transmission, Baseband, Time Division Multiplexing (TDM), Broadband, Frequency Division Multiplexing (FDM), Unicast, Multicast, Broadcast, Attenuation, Coaxial, Thicknet, Thinnet, Twisted Pair, Radio Frequency Interference (RFI), EMI, Fiberoptic, Single mode, Multimode, Ring, Bus, Star, Mesh, Hybrid, Ethernet, Token Ring, Fiber Distributed Data Interface (FDDI), Carrier Sense Multiple Access Collision Detection (CSMA/CD), Carrier Sense Multiple Access Collision Avoidance (CSMA/CA), token passing, polling, Dynamic Host Configuration Protocol (DHCP), DNS, File Transfer Protocol (FTP), FTPS, Secure File Transfer Protocol (SFTP), HTTP, Hypertext Transfer Protocol Secure (HTTPS), SHTTP, Internet Message Access Protocol (IMAP), Network Address Translation (NAT), Port Address Translation (PAT), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP), distance vector, link state, hybrid, Routing Internet Protocol (RIP), Open Shortest Path First (OSPF), Interior Gateway Protocol, Enhanced IGRP (EIGRP), Virtual Router Redundancy Protocol (VRRP), Intermediate System to Intermediate System (IS-IS), Border Gateway Protocol (BGP), patch panels, multiplexer, demultiplexer, hub, switches, VLANs, layer 3 switch, layer 4 switches, routers, gateway, Network Access Server (NAS), firewall, packet filtering firewalls, stateful firewalls, proxy firewalls, circuit level proxies, SOCKS firewall, application-level proxies, dynamic packet filtering firewall, kernel proxy firewall, bastion host, dual-homed firewall, three legged firewall, DMZ, screened host, screened subnet, virtual firewalls, proxy firewall, private branch exchange (PBX), honeypots, honeynets, cloud computing, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), LAN, intranet, extranet, Metropolitan Area Network (MAN), Metro Ethernet, wide area networks (WANs), T carriers, fractional T1, E carriers, Synchronous Optical Networks (SONET), Channel Service Unit/Data Service Unit (CSU/DSU), circuit-switching networks, packet-switching networks, Asynchronous Transfer Mode (ATM), X.25, Switched Multimegabit Data Service (SMDS), Point-to-Point Protocol (PPP), HSSI, PSTN, VOIP, Signaling System 7 (SS7), Session Initiation Protocol (SIP), dial-up, SLIP, Integrated Services Digital Network (ISDN), Basic Rate (BRI), Primary Rate (PRI), Digital Subscribers Line (DSL), Asymmetric DSL (ADSL), High Bit Data Rate DSL (HDSL), Very High Bit Data Rate DSL (VDSL), cable modems, Data-Over-Cable Service Interface Specifications (DOCSIS), Virtual Private Network (VPN), PPTP, L2TP, IPsec, Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Security Association and Key Management Protocol (ISAKMP), Internet Key Exchange

(IKE), TACACS+, RADIUS, supplicant, authenticator, authenticating server, Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), Extensible Authentication Protocol (EAP), Telnet, Transport Layer Security/Secure Sockets Layer (TLS/SSL), Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), Orthogonal Frequency Division Multiplexing (OFDM), Frequency Division Multiple Access (FDMA), Code Division Multiple Access (CDMA), Global System Mobile (GSM), phone cloning, access point, Service Set Identifier (SSID), Infrastructure mode, Ad Hoc mode, 802.11a, 802.11b, 802.11f, 802.11g, 802.11n, Multiple Input Multiple Output, Bluetooth, bluejacking, bluesnarfing, infrared, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, noise, attenuation, crosstalk, Ping of Death, Distributed Denial of Service (DDOS), Smurf attack, ping scanning, DNS cache poisoning attack, DNSSEC (DNS security), URL hiding, domain grabbing, cybersquatting, email spoofing, phishing, spear phishing, whaling, spam, wardriving, warchalking, SYN ACK attack, session highjacking attack, port scan, teardrop, IP address spoofing

Review Questions

1. At which layer of the OSI model does the encapsulation process begin?
   a. Transport
   b. Application
   c. Physical
   d. Session

2. Which two layers of the OSI model are represented by the Link layer of the TCP/IP model? (Choose two.)
   a. Data Link
   b. Physical
   c. Session
   d. Application
   e. Presentation

3. Which of the following represents the range of port numbers that are referred to as “well-known” port numbers?
   a. 49152–65535
   b. 0–1023
   c. 1024–49151
   d. all above 500

4. What is the port number for HTTP?

   a. 23
   b. 443
   c. 80
   d. 110

5. What protocol in the TCP/IP suite resolves IP addresses to MAC addresses?

   a. ARP
   b. TCP
   c. IP
   d. ICMP

6. How many bits are contained in an IPv4 IP address?

   a. 128
   b. 48
   c. 32
   d. 64

7. Which of the following is a Class C address?

   a. 172.16.5.6
   b. 192.168.5.54
   c. 10.6.5.8
   d. 224.6.6.6

8. Which of the following is a private IP address?

   a. 10.2.6.6
   b. 172.15.6.6
   c. 191.6.6.6
   d. 223.54.5.5

9. Which service converts private IP addresses to public IP addresses?

   a. DHCP
   b. DNS
   c. NAT
   d. WEP

10. Which type of transmission uses stop and start bits?
    a. Asynchronous
    b. Unicast
    c. Multicast
    d. Synchronous

Answers and Explanations

1. **b**. The Application Layer (layer 7) is where the encapsulation process begins. This layer receives the raw data from the application in use and provides services such as file transfer and message exchange to the application (and thus the user).
2. **a**, **b**. The Link layer of the TCP/IP model provides the services provided by both the Data Link and the Physical layers in the OSI model.
3. **b**. System Ports, also called well-known ports, are assigned by the IETF for standards-track protocols, as per [RFC6335].
4. **c**. The listed ports numbers are as follows:

   23–Telnet

   443–HTTPS

   80–HTTP

   110–POP3
5. **a**. Address Resolution Protocol (ARP) resolves IP addresses to MAC addresses.
6. **c**. IPv4 addresses are 32 bits in length and can be represented in either binary or in dotted decimal format.
7. **b**. The calls C range of addresses is from 192.0.0.0 -223.255.255.255.
8. **a**.

   Here are the private IP address ranges:

Class	Range
Class A	10.0.0.0 – 10.255.255.255
Class B	172.16.0.0 – 172.31.255.255
Class C	192.168.0.0 – 192.168.255.255

9. **c.** Network Address Translation (NAT) is a service that can be supplied by a router or by a server. The device that provides the service stands between the local LAN and the Internet. When packets need to go to the Internet, the packets go through the NAT service first. The NAT service changes the private IP address to a public address that is routable on the Internet. When the response is returned from the Web, the NAT service receives it and translates the address back to the original private IP address and sends it back to the originator.

10. **a.** With asynchronous transmission, the systems use what are called start and stop bits to communicate when each byte is starting and stopping. This method also uses what are called parity bits to be used for the purpose of ensuring that each byte has not changed or been corrupted en route. This introduces additional overhead to the transmission.

Index

Numbers

3DES (Triple DES)
modes, 262-263, 495, 514
overview, 262
10Base2 cabling, 88
10BaseT cabling, 89
10GBaseT cabling, 89
100BaseT cabling, 89
802.11 wireless standard
amendments, 138
802.11a, 138
802.11b, 138
802.11g, 138
modulation techniques, 136
1000BaseT cabling, 89

A

A - Verified protection, 325
A1 - Verified Design, 325-326
absolute addressing, 306
acceptability (biometrics), 503
access control, 5-6
accountability, 36
auditing/reporting, 36-37
penetration testing, 38-39
vulnerability assessments, 37-38
administration, 49-50
centralized, 49
decentralized, 49
provisioning life cycle, 50
authentication
factors, 17
identity/account management, 18-19
knowledge factors, 17
passwords, 19-22
authorization, 28
access control policies, 29
default to no access, setting, 30
directory services, 30-31
federated identities, 35
Kerberos, 32-34
least privilege, 29-30, 343
need to know principles, 29-30
security domains, 35
separation of duties, 29
SESAME, 34
SSO, 31-32
Brewer-Nash model, 320
categories, 39
compensative, 40
corrective, 40
detective, 40
deterrent, 40
directive, 40
preventive, 41
recovery, 41

CIA triad, 12-14
default stance, 14
defense-in-depth strategy, 15, 298
facilities, 462-463
  biometrics, 466
  door locks, 463
  doors, 463
  glass entries, 466
  locks, 464-465
  mantraps, 464
  perimeters. See *perimeters*
  turnstiles, 464
  visitors, 466-467
Harrison-Ruzzo-Ullmen model, 321
identifying
  relationships between resources and users, 16
  resources, 15
  users, 16
least privilege, 343
lists (ACLs), 49
managing, 349
matrix, 48
models, 46
  access control matrix, 48
  ACLs, 49
  capabilities tables, 48
  content-dependent, 48
  context-dependent, 48
  discretionary (DAC), 46
  mandatory (MAC), 47
  RBAC, 47
  rule-based, 48
monitoring, 50
  IDS. See *IDS*
  IPS, 52, 363
natural, 453-454
policies, 29
resources, maintaining, 355-356
services, 302
threats, 52-53
  backdoor/trapdoor, 57
  brute-force, 53
  buffer overflow, 55
  dictionary attacks, 53
  DOS/DDOS, 55
  dumpster diving, 55
  emanating, 57
  identity theft, 54
  malware, 56
  mobile code, 56
  passwords, 53
  phishing/pharming, 54
  shoulder surfing, 54
  sniffing, 57
  social engineering, 53
  spoofing, 56
types, 41
  administrative, 41-42
  logical/technical, 43-44
  physical, 43-45
access points (APs), 137
accessibility (facilities), 456
accountability, 36
auditing/reporting, 36-37
  audit trails, 37
  guidelines, 36
  scrubbing, 36
penetration testing, 38-39
  categories, 39
  performing, 38
  strategies, 38-39
vulnerability assessments, 37-38

accreditation, 236-237, 329-330

accuracy (biometrics), 503

ACLs (access control lists), 49

acoustical detection systems, 461

Acquire/Develop phase (system development life cycle), 204-205

acrylic glass, 466

active cryptography attacks, 286

ActiveX, 224

AD (architectural description), 299

Ad Hoc mode (WLANs), 137

Adams, Carlisle, 265

addresses

- absolute, 306
- implied, 306
- indirect, 306
- IP
  - *classes, 80-81*
  - *IPv4, 77-80, 82*
  - *IPv6, 82*
  - *NAT, 81-89*
  - *public versus private, 81*
  - *spoofing, 150*
- logical, 306
- MAC, 82-83
- relative, 306
- Resolution Protocol (ARP), 75, 101-102

Adleman, Leonard, 267

administration

- access control, 49-50
  - *centralized, 49*
  - *decentralized, 49*
  - *provisioning life cycle, 50*
- controls, 41-42, 484, 504
- security responsibilities, 190

administrative law, 409

ADSL (Asymmetric DSL), 128

advisory security policies, 185

adware, 232

AES (Advanced Encryption Standard), 263

aggregation, 334

Agile software development method, 216-217

AH (Authentication Header), 130

ALE (annual threat event), 178

algebraic attacks, 288

algorithms, 513. *See also* ciphers

- asymmetric, 255-256
  - *confidentiality, 256*
  - *defined, 265*
  - *Diffie-Hellman, 266*
  - *ECC, 267-268*
  - *El Gamal, 267*
  - *Knapsack, 268*
  - *private/public keys, 255*
  - *RSA, 267*
  - *strengths/weaknesses, 256, 495, 514*
  - *zero-knowledge proof, 268*
- defined, 245
- MD, 271
- SHA (Secure Hash Algorithm), 271-272
- symmetric, 253-254, 258
  - *3DES.* See *3DES*
  - *AES, 263*
  - *block ciphers, 255*
  - *Blowfish, 264*
  - *CAST, 265*
  - *DES.* See *DES*
  - *IDEA, 263*
  - *Initialization Vectors (IVs), 255*
  - *key facts, 496, 514*
  - *RC, 264*

Skipjack, *264*
stream-based ciphers, *254*
strengths/weaknesses, *254*, *495*, *514*
Twofish, *264*
alternate facility locations, 382-385
cold sites, 383
hot sites, 383
reciprocal agreements, 384
redundant sites, 385
selecting, 382
tertiary sites, 384
testing, 383
warm sites, 384
ALU (arithmetic logic unit), 304
analog transmissions, 83
analytic attacks, 289
annual threat event, 178
anomaly-based IDS, 51, 507
antimalware software, 236
antivirus software, 236
application-based IDS, 52
application layer
OSI, 67
TCP/IP, 72
application-level proxies, 114
application owner security responsibilities, 191
APs (access points), 137
architectural description (AD), 299
architectures, 8
defined, 299
frameworks, 312-313
ITIL, *172*, *313*
SABSA, *168*, *490*, *509*
TOGAF, *166-167*, *312*, *489*, *508*
Zachman, *312*
maintenance, 330
system security, 310
documentation, *314*
models. See *security*, *models*
modes. See *security*, *modes*
policies, *310*
requirements, *310-311*
zones, *311*
systems, 298
computing platforms, *300-301*
CPUs, *303-304*
design phase, *299*
development phase, *299*
input/output devices, *307*
ISO-IEC 42010:2011, *299*
maintenance phase, *299*
memory, *304-306*
multitasking, *308-309*
operating systems, *307-308*
security services, *302-303*
threats, 330
data flow control, *333*
database, *333-334*
maintenance hooks, *331*
OWASP, *333*
SAML, *332*
server-based attacks, *333*
time-of-check/time-of-use attacks, *331-332*
web-based attacks, *332*
XML, *332*
arithmetic logic unit (ALU), 304
ARP (Address Resolution Protocol), 75, 101-102
assembly languages, 219
assessing risks. *See* risks, assessment

assets. ***See also*** **resources**
critical, identifying, 374
criticality, 374-375, 495-498, 517
equipment security, 472-473
managing, 348-349
backup/recovery, 349
fault tolerance, 348
redundancy, 348
protecting, 346
corporate procedures, 472-473
facilities, 346
hardware, 347
information assets, 347
security device protection, 473-474
software, 347
threats, mitigating, 362-364
qualitative risk analysis, 179
quantitative risk analysis, 178-179
tangible/intangible, 177
technological, recovering
hardware, 386
software, 386-387
threats
clipping levels, 361
deviations from standards, 361
unexplained events, 361
value, determining, 177
vulnerabilities/threats, 177-178
associative memory, 306
assurance
accreditation and certification, 329-330
evaluation systems, 322
Common Criteria, 328-329
ITSEC, 326-327
Rainbow Series. See *Rainbow Series*
TCSEC, 323
asymmetric algorithms, 255-256
confidentiality, 256
defined, 265
Diffie-Hellman, 266
ECC, 267-268
El Gamal, 267
Knapsack, 268
private/public keys, 255
RSA, 267
strengths/weaknesses, 256, 495, 514
zero-knowledge proof, 268
Asymmetric DSL (ADSL), 128
asymmetric multitasking, 308
asynchronous encryption/decryption, 244, 493, 512
asynchronous transmissions, 84
ATM (Asynchronous Transfer Mode), 123
attacks. ***See also*** **threats**
cryptography
algebraic, 288
analytic, 289
birthday, 289
brute-force, 288
chosen ciphertext, 287
chosen plaintext, 287
ciphertext-only, 287
dictionary, 289
differential, 288
factoring, 289
frequency analysis, 288
known plaintext, 287
linear cryptanalysis, 288
meet-in-the middle, 290
passive versus active, 286
replay, 289
reverse engineering, 289

social engineering, 287
statistical, 289
database, 333-334
aggregation, 334
contamination, 334
inference, 334
DNS, 145
cache poisoning, 145
cybersquatting, 147
DDoS, 146
DNSSEC, 146
domain grabbing, 147
DoS, 146
URL hiding, 146
email
spam, 148
spear phishing, 148
spoofing, 147
whaling, 148
ICMP
Fraggle, 144
Ping of Death, 144
ping scanning, 145
redirect, 144
Smurf, 144
port scanning, 150
server-based, 333
session hijacking, 150
SYN ACK, 149
teardrop, 150
time-of-check/time-of-use, 331-332
web-based, 332
wireless, 149
attenuation, 142-143
attributes, 225, 510
auditing
accountability, 36-37
committee security responsibilities, 189
guidelines, 36
policies, 360
record retention, 345
scrubbing, 36
services, 303
software security, 237
trails, 37
auditor security responsibilities, 191
authentication
categories, 481, 501
characteristic factors, 23
behavioral, 25
biometric considerations, 26-28
biometric methods ranked by effectiveness, 26-27
biometric user acceptance rankings, 27
physiological, 24-25
cryptosystems, 250
factors, 17
knowledge factors, 17
identity/account management, 18-19
passwords, 19-22
ownership factors, 22
memory cards, 22-23
smart cards, 23
token devices, 22
remote access protocols, 133
Authentication Header (AH), 130
author identification, 434
authorization, 28
access control policies, 29
cryptosystems, 251
default to no access, setting, 30
directory services, 30-31

federated identities, 35
incident response, 424
Kerberos, 32-34
advantages, 33
disadvantages, 33
ticket-issuing process, 33
least privilege, 29-30, 343
need to know principles, 29-30
security domains, 35
separation of duties, 29
SESAME, 34
SSO, 31-32
advantages, 31
disadvantages, 32
objectives, 31
Open Group Single Sign-On Standard Web site, 31
availability, 298
business continuity planning, 373
high, 392-393, 498-499, 518
clustering, 518
failover, 518
failsoft, 518
load balancing, 518
RAID, 518
SAN, 518
resources, maintaining, 355-356
avalanche effect, 245, 513
awareness training (security), 193-194

B

B - Mandatory protection, 324
B1 - Labeled Security Protection, 324-325
B2 - Structured Protection, 325
B3 - Security Domains, 325
backdoor, 57, 235
backups
asset management, 349
business continuity, 380
copy, 390
daily, 390
differential, 390
electronic, 392
electronic vaulting, 498, 517
full, 389
hardware, 386
HSM, 498, 517
incremental, 390
optical jukeboxes, 517
remote journaling, 498, 517
replication, 498, 518
rotation schemes, 391
schemes, 391
software, 386-387
tape vaulting, 517
transaction log, 390
types, 389-390
barriers (perimeters), 459
base relations, 225, 510
baseband transmissions, 84-85
Basel II, 417
baselines (information security governance), 185-186
basic rate (BRI) ISDN, 127
bastion hosts, 115
BCP (business continuity plan), 372
contingency plans, 372-373
maintenance, 398
personnel
components, 377
training, 393

scope, 377
SP 800-34 Revision 1 standard, 378
tests, 396-397
checklist, 396
evacuation drills, 397
full-interruption, 397
functional drills, 397
parallel, 397
simulation, 397
structured walk-through, 397
table-top exercises, 397
behavioral characteristics (authentication), 25
Bell-LaPadula model, 317-318
confidentiality, 318
flow of information rules, 317
limitations, 318
best evidence, 432
BGP (Border Gateway Protocol), 108
BIA (business impact analysis), 372-373
critical processes/resources, identifying, 374
criticality levels, 374-375
fault tolerance, 376
recoverability, 376
recovery priorities, 376
resource requirements, 375
steps, 495, 516-517
Biba model, 319
biometric authentication, 25, 466
considerations, 26-28
effectiveness rankings, 26-27
keystroke dynamics, 25
signature dynamics, 25
terms, 483
user acceptance rankings, 27
voice patterns, 25
birthday attacks, 289
black hats, 407
blackouts, 470
block ciphers, 255
Blowfish, 264
Bluejacking, 139
Bluesnarfing, 139
Bluetooth, 139
board of directors security responsibilities, 188
bollards, 459
bombings, 452
boot sector viruses, 231, 511
Border Gateway Protocol (BGP), 108
botnets, 232
boundary control services, 302
Brewer-Nash model, 320
BRI (basic rate) ISDN, 127
British Ministry of Defence Architecture Framework (MODAF), 168
broadband transmissions, 84-85
broadcast transmissions, 86
brownouts, 470
brute-force attacks, 288
BSI (Build Security In), 210
budgets (security), 194-195
buffer overflow, 55, 233-235
Build and Fix software development method, 211-212
Build Security In (BSI), 210
bullet-resistant doors, 463
bus topology, 92
business continuity, 8
asset criticality, 495-498, 517
availability, 373

backups
electronic vaulting, 498, 517
HSM, 498, 517
optical jukeboxes, 517
remote journaling, 498, 517
replication, 498, 518
tape vaulting, 517
BCP. *See* BCP
BIA, 372-373
critical processes/resources, identifying, 374
criticality levels, 374-375
fault tolerance, 376
recoverability, 376
recovery priorities, 376
resource requirements, 375
steps, 495, 516-517
contingency plans, 372-373
continuity planning, 372
disaster recovery. *See* disaster recovery
disruptions, 370
high-availability, 498-499, 518
personnel training, 393
plan, 372
personnel components, 377
scope, 377
SP 800-34 R1 standard, 378
preventive controls, 378
data backups, 380
fault tolerance, 379
fire detection and suppression systems, 380
insurance, 379-380
redundancy, 379
recovery priorities, 376
recovery strategies, 380-381
business processes, 382
data. See *data, recovery*
documentation, 388
facilities, 382-385
hardware, 386
human resources, 387
recovery priorities, categorizing, 381
software, 386-387
supplies, 387
user environment, 388
reliability, 373
business impact analysis. *See* BIA
business process recovery, 382
business unit manager security responsibilities, 189

C

C - Discretionary protection, 324
C1 - Discretionary Security Protection, 324
C2 - Controlled Access Protection, 324
cable modems, 128
cabling, 87
coaxial, 87-88
fiberoptic, 89-91
selecting, 87
twisted pair, 88-90
categories, 89-90
shielded versus unshielded, 89
types, 89
WLAN security, 142
caches, 306
CALEA (Communications Assistance to Law Enforcement Act) of 1994, 417

candidate keys, 225, 511

capabilities tables, 48

Capability Maturity Model Integration (CMMI), 174, 218

capacitance detectors, 461

cardinality, 225, 511

cards

memory, 22-23

smart, 23

carrier lines

E, 121

OC, 122

T, 121

Carrier Sense Multiple Access Collision Avoidance (CSMA/CA), 100

Carrier Sense Multiple Access Collision Detection (CSMA/CD), 99

CAs (certification authorities), 275-276

CAST (Carlisle, Adams, Stafford, Tavares) algorithm, 265

categories

access control, 39

compensative, 40

corrective, 40

detective, 40

deterrent, 40

directive, 40

preventive, 41

recovery, 41

authentication, 481, 501

IDS, 487-488, 503-507

penetration testing, 39

programming languages, 219

assembly, 219

high-level, 219

machine, 219

natural, 220

very-high-level, 219

routing protocols, 107

security policies, 185

twisted pair cabling, 89-90

CBC (Cipher Block Chaining), 260

CBC-MAC (cipher block chaining MAC), 274

CC (Common Criteria), 328-329

CCTV (closed-circuit television system), 461

CDMA (Code Division Multiple Access), 136

CDP (Cisco Discovery Protocol), 106

central processing units (CPUs), 303-304

centralized access control, 49

CEO (chief executive officer), 189

CER (crossover error rate), 503

certificate revocation lists (CRLs), 277

certificates. ***See*** **digital certificates**

certification, 329-330

authorities (CAs), 275-276

software, 236-237

Certified Information Systems Security Professional. ***See*** **CISSP**

CFAA (Computer Fraud and Abuse Act), 416

CFB (Cipher Feedback), 261

CFO (chief financial officer), 189

chain of custody, 430

change control policies, 356-357

change management (software development), 209

Channel Service Unit/Data Service Unit (CSU/DSU), 122

CHAP (Challenge Handshake Authentication Protocol), 133
characteristic factor authentication, 23
behavioral characteristics, 25
biometrics
considerations, 26-28
effectiveness rankings, 26-27
user acceptance rankings, 27
physiological characteristics, 24-25
checklist tests, 396
chief executive officer (CEO), 189
chief financial officer (CFO), 189
chief information officer (CIO), 189
chief privacy officer (CPO), 189
chief security officer (CSO), 189
Chinese Wall model, 320
chosen ciphertext attacks, 287
chosen plaintext attacks, 287
CIA (confidentiality, integrity, and availability) triad, 12-14, 160
CIDR (Classless Inter-Domain Routing), 80
CIO (chief information officer), 189
cipher-based MAC (CMAC), 274
Cipher Block Chaining (CBC), 260
cipher block chaining MAC (CBC-MAC), 274
Cipher Feedback (CFB), 261
ciphers. ***See also*** **algorithms**
block, 255
Caesar, 247
concealment, 252
hybrid, 256-257
running key, 252
scytale, 246
stream-based, 254
substitution, 252, 257
defined, 252
modulo 26, 252
one-time pads, 257-258
steganography, 258
transposition, 253
Vigenere, 248-249
ciphertext, 244, 512
ciphertext-only attacks, 287
circuit-level proxies, 114
circuit-switching networks, 123
circumstantial evidence, 432
Cisco Discovery Protocol (CDP), 106
CISSP (Certified Information Systems Security Professional), 2
additional versions, 4
exam specifications, 10
goals, 4
qualifications needed, 10
signing up, 10
sponsoring bodies, 2-4
value, 5
civil code law, 408
civil disobedience, 452
civil law, 408-409
Clark-Wilson Integrity model, 319-320
classifications (data), 186
commercial business, 186-187
military and government, 187-188
Classless Inter-Domain Routing (CIDR), 80
Cleanroom software development method, 218
clearing data, 355
cleartext, 244, 493, 512
clipping levels, 21, 361

closed-circuit television system (CCTV), 461
cloud computing, 117-118, 335
clustering, 393, 518
CMAC (cipher-based MAC), 274
CMMI (Capability Maturity Model Integration), 174, 218
coaxial cabling, 87-88
COBIT (Control Objectives for Information and related Technology), 170, 314
Code Division Multiple Access (CDMA), 136
cognitive passwords, 20, 502
cohesion, 221
cold sites, 383
collaboration, 134-135
collisions, 98, 494, 513
avoidance, 100
cryptography, 245
detection, 99
domains, 98
collusion, 451
combination locks, 465
combination passwords, 19, 501
commercial business data classifications, 186-187
commercial software, 412
Committee of Sponsoring Organizations (COSO), 171
Common Body of Knowledge, 5
Common Criteria (CC), 328-329
common law, 408
Common Object Request Broker Architecture (CORBA), 222
communication. *See also* transmissions
analysis, 435
encryption levels
end-to-end, 281
link, 280
threats, 447-448
trusted entities, 277-278
Communications Assistance to Law Enforcement Act (CALEA) of 1994, 417
compartmented security mode, 321
compensative controls, 40
compiled code, 220
complex passwords, 19, 501
compliance (legal), 420
computer crimes
computer-assisted, 406
computer prevalence, 407
computer-targeted, 406
evidence, 430-431
five rules, 431
hardware/embedded device analysis, 435
media analysis, 434
network analysis, 435
search warrants, 433
seizure, 434
software analysis, 434
surveillance, 433
types, 431-433
hackers *versus* crackers, 407
incident responses. *See* incident responses
incidental, 406
investigations, 9, 406
chain of custody, 430
crime scenes, 429
decisions, 428
examination and analysis, 428
identification, 427

interviews, *430*
IOCE/SWGDE, *428-429*
law enforcement involvement, *426*
MOM, *429*
presentation, *428*
preservation and collection, *427-428*
process, *426*
standardized procedures, *425*
white/gray/black hat, 407
Computer Ethics Institute, Ten Commandments of Computer Ethics, 436
Computer Fraud and Abuse Act (CFAA), 416
Computer Security Act of 1987, 417
computers
equipment rooms (facilities), 457-458
prevalence crimes, 407
targeted crimes, 406
computing platforms, 300-301
distributed, 300
embedded, 301
mainframe/thin clients, 300
middleware, 301
mobile, 301
virtual, 301
concealment ciphers, 252
conclusive evidence, 432
confidentiality, 297
Bell-LaPadula model, 318
cryptosystems, 250
confidentiality, integrity, and availability (CIA) triad, 12-14, 160
configuration management
policies, 358-359
software development, 209
confusion, 245, 513
connections
LANs. *See* LANs
remote, 126
attacks, *149*
authentication protocols, *133*
cable, *128*
dial-up, *126-127*
DSL, *127-128*
Internet security, *283*
ISDN, *127*
multimedia collaboration, *134-135*
RADIUS, *132-133*
SSL, *134*, *283*
TACACS, *132-133*
Telnet, *134*
TLS, *134*, *284*
VPNs, *129-132*
satellite, 141
WANs
ATM, *123*
circuit-switching, *123*
CSU/DSU, *122*
E lines, *121*
frame relay, *123*
HSSI, *124-125*
OC lines, *122*
packet-switching, *123*
PPP, *124*
PSTN, *125*
SMDS, *124*
T lines, *121*
VoIP, *125-126*
X.25, *124*
wireless. *See* WLANs
construction (facilities), 456-457

contact/contactless cards, 23
contamination, 334
content analysis, 434
content-dependent access control, 48
contention methods, 97-101
- collisions, 98
- CSMA/CA, 100
- CSMA/CD, 99
- polling, 101
- token passing, 101

context analysis, 434
context-dependent access control, 48
contingency plans, 372-373
continuity planning, 372
continuous lighting systems, 461
Control Objectives for Information and related Technology (COBIT), 170, 314
controlled security mode, 322
controls
- administrative, 41-42, 484, 504
- compensative, 40
- corrective, 40
- detective, 40
- deterrent, 40
- directive, 40
- logical, 43-44, 485, 505
- NIST SP 800-53 families, 488, 507
- physical, 43-45, 486, 506
- preventive, 41
- recovery, 41
- technical, 43-44

cookies, 284-285
copy backups, 390
copyrights, 411-412
CORBA (Common Object Request Broker Architecture), 222
corrective controls, 40
corroborative evidence, 433
COSO (Committee of Sponsoring Organizations), 171
Counter Mode (CTR), 262
countermeasures, 161
coupling, 221
covert channels, 362
CPO (chief privacy officer), 189
CPTED (Crime Prevention through Environmental Design), 453
CPUs (central processing units), 303-304
crackers, 407
Crime Prevention through Environmental Design (CPTED), 453
crime scenes, 429
criminal activity, deterring, 454
criminal law, 408
critical processes/resources, identifying, 374
criticality (assets), 374-375, 495-498, 517
CRLs (certificate revocation lists), 277
cross-certification model, 35, 278
crossover error rate (CER), 503
crosstalk, 143
cryptanalysis, 245, 513
cryptography, 7
- 3DES
  - *modes, 262-263, 495, 514*
  - *overview, 262*
- asymmetric, 255-256
  - *confidentiality, 256*
  - *defined, 265*
  - *Diffie-Hellman, 266*
  - *ECC, 267-268*

El Gamal, 267
Knapsack, 268
private/public keys, 255
RSA, 267
strengths/weaknesses, 256, 495, 514
zero-knowledge proof, 268
asynchronous encryption/decryption, 512
attacks
algebraic, 288
analytic, 289
birthday, 289
brute-force, 288
chosen ciphertext, 287
chosen plaintext, 287
ciphertext-only, 287
dictionary, 289
differential cryptanalysis, 288
factoring, 289
frequency analysis, 288
known plaintext, 287
linear cryptanalysis, 288
meet-in-the-middle, 290
passive versus active, 286
replay, 289
reverse engineering, 246
social engineering, 287
statistical, 289
avalanche effect, 245, 513
ciphertext, 244, 512
collisions, 245, 494, 513
confusion, 245, 513
cryptanalysis, 245, 513
cryptology, 245, 513
cryptosystems, 245, 250, 512
authentication, 250
authorization, 251
confidentiality, 250
integrity, 251
non-repudiation, 251
decoding, 245, 513
decryption, 244, 493, 512
diffusion, 245, 513
digital certificates, 276, 493, 512
CAs, 275-276
classes, 277
cross-certification, 278
defined, 244
requesting, 277
revocation lists, 277
trusted entity communication, 277-278
X.509, 276-277
digital signatures, 244, 274-275, 493, 512
email, 281
MIME, 282
PGP, 281-282
quantum cryptography, 282
S/MIME, 282
encoding, 245, 513
encryption. *See* encryption
hash functions, 244, 512
HAVAL, 272
MD algorithms, 271
one-way hash, 269-270
RIPEMD-160, 272
SHA, 271-272
Tiger, 272
history, 246-247
Caesar cipher, 247
Kerckhoff principles, 249
Lucifer project, 250

scytale ciphers, *246*
World War II, *249-250*
Internet, 283
cookies, *284-285*
HTTP, *284*
HTTPS, *284*
IPsec, *285-286*
remote access, *283*
S-HTTP, *284*
SET, *284*
SSH, *285*
SSL, *134*, *283*
TLS, *134*, *284*
keys
clustering, *245*, *513*
defined, *244*, *512*
management, *278-279*
keyspace, 245, 513
life cycle, 246
MACs
CBC-MAC, *274*
CMAC, *274*
HMAC, *273*
one-way functions, 246, 513
PKI, 275
CAs, *275-276*
CRLs, *277*
cross-certification, *278*
digital certificates, *276-277*
OCSP, *276*
RAs, *275*
trusted entity communication, *277-278*
plaintext, 244, 493, 512
services, 303
substitution, 245, 494-495, 513
substitution ciphers, 257
defined, *252*
modulo 26, *252*
one-time pads, *257-258*
steganography, *258*
symmetric algorithms, 253-254, 258
3DES. See *3DES*
AES, *263*
block ciphers, *255*
Blowfish, *264*
CAST, *265*
DES. See *DES*
IDEA, *263*
Initialization Vectors (IVs), *255*
key facts, *496*, *514*
RC, *264*
Skipjack, *264*
stream-based ciphers, *254*
strengths/weaknesses, *254*, *495*, *514*
Twofish, *264*
synchronous encryption/decryption, 244, 493, 512
TPM, 279-280
transposition, 245, 494, 513
trapdoors, 246, 514
Vigenere ciphers, 248-249
work factors, 246, 513
cryptology, 245, 513
cryptosystems, 245, 250, 512
authentication, 250
authorization, 251
confidentiality, 250
integrity, 251
non-repudiation, 251
CSMA/CA (Carrier Sense Multiple Access Collision Avoidance), 100

CSMA/CD (Carrier Sense Multiple Collision Detection), 99
CSO (chief security officer), 189
CSU/DSU (Channel Service Unit/Data Service Unit), 122
CTR (Counter Mode), 262
customary law, 409
cybersquatting, 147

D

D - Minimal protection, 324
DAC (discretionary access control), 46
daily backups, 390
damage assessment teams, 394
data
availability, 298
centers, 467
classifications, 186
commercial business, 186-187
military and government, 187-188
clearing, 355
confidentiality, 297
custodian security responsibilities, 190
decoding, 245
encoding, 245
flow control, 333
integrity. *See* integrity
mining, 227, 334
owner security responsibilities, 190
purging, 355
recovery, 388
backup rotation schemes, 391
backup types, 389-390
electronic backups, 392
high availability, 392-393
remanence, 355
structures, 222
warehousing, 227
Data Link layer (OSI), 68-69
Data Terminal Equipment (DTE), 122
databases
data
mining, 227
warehousing, 227
locks, 228
models, 224
hierarchical, 226
network, 226
object-oriented, 226
object-relational, 226
relational, 225
OLTP ACID tests, 229
polyinstantiation, 228
programming languages, 226-227
JDBC, 227
ODBC, 226
OLE DB, 227
XML, 227
relational management systems. *See* relational databases
threats, 228, 333-334
aggregation, 334
contamination, 334
inference, 334
views, 225, 228, 299, 511
DDoS (Distributed Denial of Service) attacks, 55, 146
DDR SDRAM (Double Data Rate Synchronous Dynamic Random Access Memory), 305
DDR2 SDRAM (Double Data Rate Two Synchronous Dynamic Random Access Memory), 305

DDR3-SDRAM (Double Data Rate Three Synchronous Dynamic Random Access Memory), 305

decentralized access control, 49

decoding, 245, 513

decryption, 493

asynchronous, 244, 493, 512

defined, 244, 512

synchronous, 244, 493, 512

dedicated security mode, 321

de-encapsulation, 76, 129

defense-in-depth model, 15, 298

degaussing, 355

degrees, 225, 511

deluge sprinkler systems, 469

Demilitarized Zone (DMZ), 115

denial-of-service attacks, 144

Denial of Service (DoS) attacks, 55, 146

Department of Defense Architecture Framework (DoDAF), 168

DES (Digital Encryption Standard)

defined, 259

Double-DES, 259

key length, 259

modes, 259-262

CBC, 260

CFB, 261

CTR, 262

ECB, 259

OFB, 261-262

DES-X, 259

design models, 8

design phase

software development life cycle, 207

system architecture, 299

detective controls, 40

deterrent controls, 40

Develop phase (software development life cycle), 207

development (software)

knowledge-based systems, 229

life cycle, 206

change/configuration management, 209

Design, 207

Develop, 207

Gather Requirements, 206-207

Release/Maintain, 209

Test/Validate, 208-209

malware, 230

botnets, 232

logic bombs, 232

protection, 235-236

rootkits, 233

spyware/adware, 232

Trojan horses, 231

viruses, 230-231

worms, 231

methods, 211

Agile, 216-217

Build and Fix, 211-212

Cleanroom, 218

CMMI, 218

Incremental, 214

JAD, 218

Prototyping, 214

RAD, 216

Spiral, 215

V-shaped, 213

Waterfall, 212-213

programming, 219

ActiveX, 224

assembly languages, 219

cohesion, *221*
compiled versus interpreted code, *220*
CORBA, *222*
coupling, *221*
data structures, *222*
distributed object-oriented systems, *222*
high-level languages, *219*
Java, *223*
machine languages, *219*
mobile code, *223*
natural languages, *220*
object-oriented, *220-221*
OLE, *223*
polymorphism, *221*
SOA, *223*
very-high-level languages, *219*
security, 210
auditing, *237*
backdoors, *235*
BSI, *210*
buffer overflow, *233-235*
certification/accreditation, *236-237*
ISO/IEC 27000, *210*
malware protection, *235-236*
OWASP,
privilege escalation, *235*
source code issues, *233*
WASC, *210*
development (system life cycle), 202-204
Acquire/Develop, 204-205
Dispose, 205-206
Implement, 205
Initiate, 204
Operate/Maintain, 205
development phase (system architecture), 299
deviations from standards, 361
devices
embedded, analyzing, 435
input/output, 307
network, 109
architecture, *115*
cloud computing, *117-118*
endpoint security, *119*
firewalls, *112-114*
gateways, *112*
honeypots, *117*
hubs, *109*
multiplexers, *109*
patch panels, *109*
PBXs, *116-117*
proxy servers, *116*
routers, *112*
switches, *110-111*
virtualization, *116*
VLANs, *111*
security, protecting, 473-474
portable media, *473*
safes/vaults/locking, *474*
tracking devices, *473*
DHCP (Dynamic Host Configuration Protocol), 102-103
dial-up connections, 126-127
dictionary attacks, 53, 289
differential backups, 390
differential cryptanalysis, 288
Diffie, Whitfield, 266
Diffie-Hellman algorithm, 266
diffusion, 245, 513
digital certificates, 276, 493, 512
CAs, 275-276
classes, 277
cross-certification, 278

defined, 244
requesting, 277
revocation lists, 277
trusted entity communication, 277-278
X.509, 276-277
Digital Encryption Standard. *See* DES
Digital Signature Standard (DSS), 275
digital signatures, 244, 274-275, 493, 512
Digital Subscribers Line. *See* DSL
digital transmissions, 83
direct evidence, 432
Direct Memory Access (DMA), 306
Direct Sequence Spread Spectrum (DSSS), 136
directive controls, 40
directory services, 30-31
disaster recovery, 8, 371
alternate facility locations, 383
asset criticality, 374-375, 495-498, 517
availability, 373
backups
electronic vaulting, 498, 517
HSM, 498, 517
optical jukeboxes, 517
remote journaling, 498, 517
replication, 498, 518
tape vaulting, 517
BIA, 372-373
critical processes/resources, identifying, 374
criticality levels, 374-375
fault tolerance, 376
recoverability, 376
recovery priorities, 376
resource requirements, 375
business continuity plan, 372
personnel components, 377
scope, 377
SP 800-34 Revision 1 standard, 378
business processes, 382
committee, 381
contingency plans, 372-373
continuity planning, 372
data, 388
backup rotation schemes, 391
backup types, 389-390
electronic backups, 392
high availability, 392-393
disasters, 371
man-made, 371
natural, 371
technological, 371
disruptions, 370
documentation, 388
DRP. *See* DRP
facility alternate locations, 382-385
cold sites, 383
hot sites, 383
reciprocal agreements, 384
redundant sites, 385
selecting, 382
tertiary sites, 384
testing, 383
warm sites, 384
financial management, 393
hardware, 386
high-availability, 498-499, 518
human resources, 387
personnel training, 393
press, handling, 381

preventive controls, 378
data backups, 380
fault tolerance, 379
fire detection and suppression systems, 380
insurance, 379-380
redundancy, 379
recovery priorities, 381
reliability, 373
software, 386-387
supplies, 387
teams
damage assessment, 394
legal, 394
listing of, 394
media relations, 395
restoration, 395
salvage, 395
security, 395-396
user environment, 388
disasters, 371
man-made, 371
natural, 371
technological, 371
discretionary access control (DAC), 46
disks
imaging, 434
mirroring, 350
striping, 349
Dispose phase (system development life cycle), 205-206
disposing media, 355
disruptions, 370, 455
distance vector protocols, 107
Distributed Denial of Service (DDoS) attacks, 55, 146
distributed systems, 300
cloud computing, 335
grid computing, 335
object-oriented, 222
peer-to-peer computing, 335
DMA (Direct Memory Access), 306
DMZ (Demilitarized Zone), 49
DNS (Domain Name System) attacks, 103, 145-146
cache poisoning, 145
cybersquatting, 147
DDoS, 146
DNSSEC, 146
domain grabbing, 147
DoS, 146
URL hiding, 146
DNSSEC (Domain Name System Security Extensions), 146
document exchanges/reviews, 192
documentation, 314
COBIT, 314
disaster recovery, 388
ISO/IEC 27000 series, 314
DoDAF (Department of Defense Architecture Framework), 168
Domain Name System. *See* DNS attacks
Domain Name System Security Extensions (DNSSEC), 146
domains, 511
authorization, 35
collision, 98
grabbing, 147
relational databases, 225
door locks, 463
doors, 463
DoS (Denial of Service) attacks, 55, 146

Double Data Rate Synchronous Dynamic Random Access Memory (DDR SDRAM), 305
Double Data Rate Three Synchronous Dynamic Random Access Memory (DDR3-SDRAM), 305
Double Data Rate Two Synchronous Dynamic Random Access Memory (DDR2 SDRAM), 305
Double-DES, 259
downstream liability, 422
downtime, estimating, 374-375
DRP (disaster recovery plan), 372
business processes, 382
committee, 381
data, 388
backup rotation schemes, 391
backup types, 389-390
electronic backups, 392
high availability, 392-393
documentation, 388
facility alternate locations, 382-385
cold sites, 383
hot sites, 383
reciprocal agreements, 384
redundant sites, 385
selecting, 382
tertiary sites, 384
testing, 383
warm sites, 384
hardware, 386
human resources, 387
personnel training, 393
press, handling, 381
recovery priorities, categorizing, 381
software, 386-387
supplies, 387
teams
damage assessment, 394
legal, 394
listing of, 394
media relations, 395
restoration, 395
salvage, 395
security, 395-396
tests, 396-397
checklist, 396
evacuation drills, 397
full-interruption, 397
functional drills, 397
parallel, 397
simulation, 397
structured walk-through, 397
table-top exercises, 397
user environment, 388
dry pipe sprinkler systems, 469
DSL (Digital Subscribers Line), 127-128
security, 128
versions, 127-128
DSS (Digital Signature Standard), 275
DSSS (Direct Sequence Spread Spectrum), 136
DTE (Data Terminal Equipment), 122
dual-homed firewalls, 115
due care/diligence, 162, 421
dumpster diving, 55
Dynamic Host Configuration Protocol (DHCP), 102-103
dynamic packet filtering firewalls, 114
dynamic ports, 77
dynamic routing, 106

E

E carrier lines, 121
EAP (Extensible Authentication Protocol), 133
earthquakes, 446
eavesdropping, 57, 143
ECB (Electronic Code Book), 259
ECC (Elliptic Curve Cryptosystems), 267-268
Economic Espionage Act of 1996, 418
ECPA (Electronic Communications Privacy Act) of 1986, 416
EIGRP (Enhanced IGRP), 108
El Gamal, 267
electrical threats, 447
electromechanical systems, 460
electronic backups, 392
electronic vaulting, 392, 498, 517
Elliptic Curve Cryptosystems (ECC), 267-268
email
- attacks, 147-148
  - *spam, 148*
  - *spear phishing, 148*
  - *spoofing, 147*
  - *whaling, 148*
- cryptography, 281
  - *MIME, 282*
  - *PGP, 281-282*
  - *quantum cryptography, 282*
  - *S/MIME, 282*

emanating, 57
embedded device analysis, 435
embedded systems, 301
emergency lighting systems, 462
employee privacy issues, 419
Encapsulating Security Payload (ESP), 130
encapsulation, 129
encoding, 245, 513
encryption, 251, 493
- asymmetric algorithms, 255-256
  - *confidentiality, 256*
  - *defined, 265*
  - *Diffie-Hellman, 266*
  - *ECC, 267-268*
  - *El Gamal, 267*
  - *Knapsack, 268*
  - *private/public keys, 255*
  - *RSA, 267*
  - *strengths/weaknesses, 256, 495, 514*
  - *zero-knowledge proof, 268*
- asynchronous, 244, 493, 512
- ciphers
  - *block, 255*
  - *concealment, 252*
  - *hybrid, 256-257*
  - *running key, 252*
  - *stream-based, 254*
  - *substitution, 252*
  - *transposition, 253*
- communication levels, 280-281
  - *end-to-end encryption, 281*
  - *link, 280*
- defined, 244, 512
- equipment protection, 472
- IVs, 255
- substitution ciphers, 257
  - *defined, 252*
  - *modulo 26, 252*
  - *one-time pads, 257-258*
  - *steganography, 258*

symmetric, 253-254, 258

3DES. See 3DES

AES, 263

block ciphers, 255

Blowfish, 264

CAST, 265

DES. See DES

IDEA, 263

Initialization Vectors (IVs), 255

key facts, 496, 514

RC, 264

Skipjack, 264

stream-based ciphers, 254

strengths/weaknesses, 254, 495, 514

Twofish, 264

synchronous, 244, 493, 512

TKIP, 140

end-to-end encryption, 281

endpoint security, 119

Enhanced IGRP (EIGRP), 108

Enigma machine, 249-250

enrollment time (biometrics), 503

enterprise resources. *See* resource protection

environmental security, 9

alerts, 472

fire protection, 468

detection, 468

suppression, 468-470

HVAC, 471

overview, 9

power supplies, 470

outages, 470

preventative measures, 470-471

water leakages/flooding, 471

equipment rooms, 467

equipment security, 472

corporate procedures, 472-473

encryption, 472

inventory, 473

tamper protection, 472

security device protection, 473-474

portable media, 473

safes/vaults/locking, 474

tracking devices, 473

ESP (Encapsulating Security Payload), 130

Ethernet 802.3, 94-96

ethical hacking. *See* penetration testing

ethics

Computer Ethics Institute, Ten Commandments of Computer Ethics, 436

Internet Architecture Board (IAB), 437

$(ISC)^2$ Code of Ethics, 435-436

organizational, 437

Ethics and the Internet (RFC 1087), 437

EU (European Union) privacy laws, 419

European E carrier lines, 121

evacuation drills, 397

evaluation systems

Common Criteria, 328-329

ITSEC, 326

assurance requirements, 327

functional requirements, 326-327

TSEC, mapping, 327

Rainbow Series. *See* Rainbow Series

TCSEC, 323

events *versus* incidents, 423

evidence, 430-431

analyzing, 428

chain of custody, 430

collecting, 427-428
examining, 428
five rules, 431
hardware/embedded device analysis, 435
identifying, 427
IOCE/SWGDE, 428-429
media analysis, 434
network analysis, 435
presenting in court, 428
preserving, 427-428
search warrants, 433
seizure, 434
software analysis, 434
surveillance, 433
types
best, 432
circumstantial, 432
conclusive, 432
corroborative, 433
direct, 432
hearsay, 433
opinion, 433
secondary, 432
exam
prerequisites, 10
signing up, 10
specifications, 10
expert systems, 229
explosion threats, 449
export legal issues, 420
exposures, 161
Extensible Authentication Protocol (EAP), 133
exterior routing protocols, 106
external entities (facilities), 456
external geographical threats, 437
extranets, 120

F

facial scans, 25
facilities
access control, 463
biometrics, 466
door locks, 463
doors, 463
glass entries, 466
locks, 464-465
mantraps, 464
turnstiles, 464
visitors, 466-467
alternate locations, 382-385
cold sites, 383
hot sites, 383
reciprocal agreements, 384
redundant sites, 385
selecting, 382
tertiary sites, 384
testing, 383
warm sites, 384
design, 453
computer and equipment rooms, 457-458
construction, 456-457
CPTED, 453
facility selection, 455
internal compartments, 457
layered defense model, 453
environmental alerts, 472
fire protection, 468
detection, 468
suppression, 468-470
HVAC, 471

interior security
data centers, 467
equipment rooms, 467
restricted work areas, 468
work areas, 467
perimeters
access control, 462-463
acoustical detection systems, 461
barriers, 459
capacitance detectors, 461
CCTV, 461
electromechanical systems, 460
fences, 459
gates, 459-460
infrared sensors, 460
intrusion detection, 460
lighting, 461-462
natural access control, 453-454
natural surveillance, 454
natural territorials reinforcement, 454
patrol force, 462
photoelectric systems, 460
walls, 460
wave motion detectors, 461
physical security plan, 454-455
criminal activity, deterring, 454
delaying intruders, 455
detecting intruders, 455
intrusions/disruptions response, 455
situation assessment, 455
power supplies, 470
outages, 470
preventative measures, 470-471
protection, 346
redundant, 379
selection
accessibility, 456
surrounding area/external entities, 456
visibility, 456
water leakages/flooding, 471

factoring attacks, 289
failovers, 392, 518
failsoft, 393, 518
false rejection rate (FRR), 503
FAR (false acceptance rate), 503
Fast Ethernet, 89
fault tolerance
asset management, 348
BIA, 376
business continuity, 379
resource availability, 355
faults (power), 470
FDDI (Fiber Distributed Data Interface), 97, 120
FDMA (Frequency Division Multiple Access), 136
feature extraction (biometrics), 503
Federal Information Security Management Act (FISMA) of 2002, 418
Federal Intelligence Surveillance Act (FISA) of 1978, 416
Federal Privacy Act of 1974, 416
federated identities, 35
fences, 459
FHSS (Frequency Hopping Spread Spectrum), 136
Fiber Distributed Data Interface (FDDI), 97, 120
fiberoptic cabling, 89-91
Field Programmable Gate Array (FPGA), 305

FIFO (first in, first out) backup rotation scheme, 391

File Transfer Protocol (FTP), 104

File Transfer Protocol Secure (FTPS), 104

filters, 141

financial management (disaster recovery), 393

finger scans, 24

fingerprint scans, 24

fires, 449-450

detection and suppression systems, 380

protection, 468

detection, 468

suppression, 468-470

firewalls, 112-114

application-level proxies, 114

circuit-level proxies, 114

deploying, 115

dual-homed, 115

dynamic packet filtering, 114

kernel proxy, 114

multihomed, 115

packet filtering, 113

proxy, 114

screened hosts, 115

screened subnet, 115

SOCKS, 114

stateful, 113

firmware, 305

first in, first out (FIFO) backup rotation scheme, 391

FISA (Federal Intelligence Surveillance Act) of 1978, 416

FISMA (Federal Information Security Management Act) of 2002, 418

five rules of evidence, 431

flame actuated fire detection, 468

flash memory, 305

floods

facilities, 471

natural, 447

fluorescent lighting, 462

foreign keys, 225, 511

forensic investigations. ***See*** **investigations**

FPGA (Field Programmable Gate Array), 305

Fraggle attacks, 144

frame relay, 123

frameworks, 312-313

COBIT, 170, 314

COSO, 171

DoDAF, 168

ITIL, 313

listing of, 163-164

MODAF, 168

NIST SP 800-53, 170-171

SABSA, 168, 312, 490, 509

TOGAF, 168, 312

Zachman, 166-167, 312, 489, 508

fraud, 450

freeware, 412

frequency analysis attacks, 288

Frequency Division Multiple Access (FDMA), 136

Frequency Hopping Spread Spectrum, 136

FRR (false rejection rate), 503

FTP (File Transfer Protocol), 104

FTPS (File Transfer Protocol Secure), 104

full backups, 389

full-interruption tests, 397

full-knowledge tests, 39

functional drills, 397
functions
hash
defined, 244, 512
HAVAL, 272
MD algorithms, 271
one-way hash, 269-270
RIPEMD-160, 272
SHA, 271-272
Tiger, 272
one-way, 246
fuzzy expert systems, 229

G

gates, 459-460
gateways, 112
geographical threats, 445
internal *versus* external, 437
natural, 446-447
earthquakes, 446
floods, 447
hurricanes/tropical storms, 446
tornadoes, 446
GFS (grandfather/father/son) backup rotation scheme, 391
Gigabit Ethernet, 89
glass entryways, 466
GLBA (Gramm-Leach-Bliley Act), 415
government data classifications, 187-188
Graham-Denning model, 320
Gramm-Leach-Bliley Act (GLBA), 415
graphical passwords, 20, 502
gray hats, 407
grid computing, 335
GSM (Global System Mobile), 137

H

hackers, 407
Halon gas, 469
hand geometry scans, 24
handling
risks, 180-181
sensitive information, 344-345
hardware
disaster recovery, 386
evidence analysis, 435
protection, 347
redundant, 355
Harrison-Ruzzo-Ullmen model, 321
hash functions
defined, 244, 512
HAVAL, 272
MD algorithms, 271
one-way, 269-270
RIPEMD-160, 272
SHA, 271-272
Tiger, 272
hash MAC (HMAC), 273
HAVAL hash function, 272
HDSL (High Bit-Rate DSL), 128
Health Care and Education Reconciliation Act of 2010, 418
Health Insurance Portability and Accountability Act (HIPAA), 415
hearsay evidence, 433
heat activated fire detection, 468
heating and air conditioning (HVAC), 471
Hellman, Martin, 266
hierarchical databases, 226
hierarchical storage management (HSM), 354, 392

high availability, 392-393, 498-499, 518
clustering, 518
failover, 518
failsoft, 518
load balancing, 518
RAID, 518
SAN, 518
High Bit-Rate DSL (HDSL), 128
high-level languages, 219
High-Speed Serial Interface (HSSI), 124-125
HIPAA (Health Insurance Portability and Accountability Act), 415
history
cryptography, 246-247
Caesar cipher, 247
Kerckhoff principles, 249
Lucifer project, 250
scytale ciphers, 246
Vigenere ciphers, 248-249
World War II, 249-250
media, 354
HMAC (hash MAC), 273
honeypots, 117
host-based IDS, 50-51
hot sites, 383
HSM (hierarchical storage management), 354, 392, 498, 517
HSSI (High-Speed Serial Interface), 124-125
HTTP (Hypertext Transfer Protocol), 104, 284
HTTPS (Hypertext Transfer Protocol Secure), 104, 284
hubs, 109
human resources recovery, 387
hurricanes, 446
HVAC (heating and air conditioning), 471
hybrid ciphers, 256-257
hybrid routing protocols, 107
hybrid topologies (networks), 94

I

IaaS (infrastructure as a service), 117
IAB (Internet Architecture Board), 437
IBM Lucifer project, 250
ICCs (integrated circuit cards), 23
ICMP (Internet Control Message Protocol), 74
attacks, 143-144
Fraggle, 144
ICMP redirect, 144
Ping of Death, 144
ping scanning, 145
Smurf, 144
defined, 104
IDEA (International Data Encryption Algorithm), 263
identities
federated, 35
management, 18-19, 349
theft, 54
IDS (Intrusion Detection System)
acoustical, 461
anomaly-based, 51, 507
application-based, 52
capacitance, 461
categories, 487-488, 503-507
CCTV, 461
electromechanical systems, 460
infrared sensors, 460
operations security, 363

patrol force, 462
perimeters, 460
photoelectric systems, 460
responses, 455
rule-based, 52, 507
signature-based, 51, 503
wave motion, 461

IEC (International Electrotechnical Commission), 164

IGMP (Internet Group Management Protocol), 75

IGRP (Interior Gateway Routing Protocol), 108

IKE (Internet Key Exchange), 130

IMAP (Internet Message Access Protocol), 105

Implement phase (system development life cycle), 205

implied addressing, 306

import legal issues, 420

incident responses, 423
events *versus* incidents, 423
management, 356-357
procedures, 424-425
rules of engagement/authorization/scope, 424
teams, 424
creating, 424
investigations, 424

incidental computer crimes, 406

incidents *versus* events, 423

incremental backups, 390

Incremental software development method, 214

indirect addressing, 306

industrial doors, 463

inference, 334

information
assets, protecting, 347
flow models, 316
life cycle, 188

information security governance, 6-7, 182-183
baselines, 185-186
components, 183
data classifications, 186
commercial businesses, 186-187
military and government, 187-188
guidelines, 186
information life cycle, 188
management approval, 182
Maturity Model, 330
organizational information security statements, 183
policies/procedures, 183-186
categories, 185
issue-specific, 185
organization security, 184
system-specific, 185
standards, 185

Information Technology Infrastructure Library (ITIL), 172, 313

Information Technology Security Evaluation Criteria. *See* ITSEC

informative security policies, 185

infrared sensors, 460

infrared wireless, 139

infrastructure as a service (IaaS), 117

Infrastructure mode (WLANs), 137

Initialization Vectors (IVs), 255

Initiate phase (system development life cycle), 204

input/output
controls, 362
devices, 307
insurance, 379-380
intangible asset protection, 177, 346
facilities, 346
hardware, 347
information assets, 347
software, 347
integrated circuit cards (ICCs), 23
Integrated Services Digital Network (ISDN), 127
integrity, 268-269, 297-298
Biba model, 319
Clark-Wilson model, 319-320
cryptosystems, 251
goals, 298
hash functions
HAVAL, 272
MD algorithms, 271
one-way hash, 269-270
RIPEMD-160, 272
SHA, 271-272
Tiger, 272
Lipner model, 320
MACs
CBC-MAC, 274
CMAC, 274
HMAC, 273
services, 303
intellectual property laws, 409
copyrights, 411-412
internal protection, 413
patents, 410
software piracy and licensing issues, 412-413
trademarks, 411
trade secrets, 410-411
interior facility security, 463
biometrics, 466
data centers, 467
door locks, 463
doors, 463
equipment rooms, 467
glass entries, 466
locks, 464-465
mantraps, 464
restricted work areas, 468
turnstiles, 464
visitors, 466-467
work areas, 467
Interior Gateway Routing Protocol (IGRP), 108
interior routing protocols, 106
Intermediate system to Intermediate system (IS-IS) protocol, 108
internal compartments (facilities), 457
internal geographical threats, 437
International Data Encryption Algorithm (IDEA), 263
International Electrotechnical Commission (IEC), 164
International Information Systems Security Certification Consortium. *See* (ISC)^2
International Organization for Standardization (ISO), 164
International Organization on Computer Evidence (IOCE), 428-429
Internet Architecture Board (IAB), 437
Internet Control Message Protocol. *See* ICMP
Internet Group Management Protocol (IGMP), 75

Internet Key Exchange (IKE), 130
Internet layer (TCP/IP), 74-75
Internet Message Access Protocol (IMAP), 105
Internet Protocol (IP), 74
Internet security, 283
cookies, 284-285
HTTP, 284
HTTPS, 284
IPsec, 285-286
remote access, 283
S-HTTP, 284
SET, 284
SSH, 285
SSL, 134, 283
TLS, 134, 284
Internet Security Association and Key Management Protocol (ISAKMP), 130
interpreted code, 220
interviews (investigations), 430
intranets, 119-120
intruders
delaying, 455
detecting, 455
intrusion detection. *See* IDS
inventory, 473
investigations, 9, 425-426
crime scenes, 429
decisions, 428
evidence, 430-431
chain of custody, 430
examining/analyzing, 428
five rules, 431
hardware/embedded device analysis, 435
identifying, 427
media analysis, 434
network analysis, 435
presenting in court, 428
preserving and collecting, 427-428
search warrants, 433
seizure, 434
software analysis, 434
surveillance, 433
types, 431-433
incident responses
incidents versus events, 423
procedures, 424-425
rules of engagement/authorization/scope, 424
teams, 424
interviews, 430
IOCE/SWGDE, 428-429
law enforcement involvement, 426
MOM, 429
process, 426
standardized procedures, 425
IOCE (International Organization on Computer Evidence), 428-429
IP (Internet Protocol), 74
IP addresses
classes, 80-81
IPv4, 77-80, 82
IPv6, 82
NAT, 81-89
public *versus* private, 81
spoofing, 150
IPS (Intrusion Prevention System), 52, 363
IPsec, 285-286
AH (Authentication Header), 130
ESP, 130
IKE, 130

ISAKMP, 130
VPNs, 130-132

IPv4
IPv6, compared, 82
overview, 77-80

IPv6, 82

iris scans, 25

IS-IS (Intermediate system to Intermediate system) protocol, 108

ISAKMP (Internet Security Association and Key Management Protocol), 130

(ISC)^2 International Information Systems Security Certification Consortium, 2-4
certifications offered, 4
Code of Ethics, 435-436
defined, 2
goals, 4

ISDN (Integrated Services Digital Network), 127

ISO (International Organization for Standardization), 164

ISO/IEC 27000 series
security architecture documentation, 314
software development security, 210

ISO-IEC 42010:2011, 166, 299

issue-specific security policies, 185

ITIL (Information Technology Infrastructure Library), 172, 313

ITSEC (Information Technology Security Evaluation Criteria), 326
assurance requirements, 327
functional requirements, 326-327
TSEC, mapping, 327

IVs (Initialization Vectors), 255

J

JAD (Joint Analyses Development) software development method, 218

Java
applets, 223
Database Connectivity (JDBC), 227
Enterprise Edition, 223

JDBC (Java Database Connectivity), 227

job rotation, 163, 344

K

KDC (Key Distribution Center), 33

Kerberos, 32-34
advantages, 33
disadvantages, 33
ticket-issuing process, 33

Kerckhoff principles, 249

kernel proxy firewalls, 114

kernels (security), 311

Key Distribution Center (KDC), 33

keys
clustering, 245, 513
defined, 244, 512
distribution center, 33
managing, 278-279
primary, 225, 511

keyspaces, 245, 513

keystroke dynamics scanning, 25

Knapsack, 268

knowledge-based systems, 229

knowledge factor authentication, 17
identity/account management, 18-19

passwords, 19-22
changing, 21
Linux, 21
lockout policies, 21
management, 20
types, 19-20
Windows, 22
known plaintext attacks, 287

L

L2TP (Layer 2 Tunneling Protocol), 130
labeling media, 354
laminated glass, 466
LANs (local area networks), 94
contention methods, 97-101
collisions, 98
CSMA/CA, 100
CSMA/CD, 99
polling, 101
token passing, 101
Ethernet 802.3, 94-96
FDDI, 97
overview, 119
Token Ring, 96
wireless. *See* WLANs
laptop memory, 305
laws
administrative, 409
civil, 408-409
civil code, 408
common, 408
compliance, 420
criminal, 408
customary, 409
export/import issues, 420
intellectual property, 409
copyrights, 411-412
internal protection, 413
patents, 410
software piracy and licensing issues, 412-413
trade secrets, 410-411
trademarks, 411
liability, 420
due diligence versus due care, 421
issues, 422-423
negligence, 421-422
mixed, 409
privacy, 415
Basel II, 417
CALEA of 1994, 417
CFAA, 416
Computer Security Act of 1987, 417
Economic Espionage Act of 1996, 418
ECPA of 1986, 416
employee privacy issues, 419
European Union, 419
expectations of privacy, 419
Federal Privacy Act of 1974, 416
FISA of 1978, 416
FISMA of 2002, 418
GLBA, 415
Health Care and Education Reconciliation Act of 2010, 418
HIPAA, 415
PCI DSS, 418
PIPEDA, 417
SOX Act, 415
United States Federal Sentencing Guidelines of 1991, 417
USA PATRIOT Act, 418
religious, 409

Layer 2 Tunneling Protocol (L2TP), 130

layered defense model, 453

layers

OSI

Application, 67

Data Link, 68-69

Network, 68

Physical, 69

Presentation, 67

Session, 67-68

Transport, 68

TCP/IP

Application, 72

Internet, 74-75

Link, 76

Transport, 72-74

LDAP (Lightweight Directory Access Protocol), 31

leaks (memory), 306

least privilege principles, 29-30, 343

legal systems, 9

administrative, 409

civil, 408-409

civil code, 408

common, 408

criminal, 408

customary, 409

mixed, 409

religious, 409

legal teams, 394

liability, 420

due diligence *versus* due care, 421

issues, 422-423

negligence, 421-422

life cycles

cryptography, 246

information, 188

software development, 206

change/configuration management, 209

design, 207

develop, 207

gather requirements, 206-207

release/maintain, 209

test/validate, 208-209

system development, 203-204

acquire/develop, 204-205

dispose, 205-206

implement, 205

initiate, 204

operate/maintain, 205

lighting, 461

feet of illumination ratings, 462

systems, 461-462

types, 462

Lightweight Directory Access Protocol (LDAP), 31

linear cryptanalysis, 288

Link layer (TCP/IP), 76

links

encryption, 280

state protocols, 107

Linux password management, 21

Lipner model, 320

load balancing, 393, 518

local area networks. *See* LANs

locking

databases, 228

security devices, 474

lockout policies (passwords), 21

locks, 464-465

logic bombs, 232
logical addressing, 306
IP classes, 80-81
IPv4, 77-80, 82
IPv6, 82
NAT, 81-89
public *versus* private, 81
logical controls, 43-44, 485, 505
logs
analysis, 435
audit, scrubbing, 36
transaction log backups, 390
Lucifer project, 250

M

MAC (mandatory access control), 47
MAC (Media Access Control) addresses, 82-83, 141
machine languages, 219
macro viruses, 231, 511
MACs (Message Authentication Code), 273
CBC-MAC, 274
CMAC, 274
HMAC, 273
mainframe platforms, 300
maintenance
architecture, 330
BCP, 398
hooks, 331
system architecture, 299
malware, 56, 230
botnets, 232
classes, 488, 507
logic bombs, 232
protection, 235-236
antimalware software, 236
antivirus software, 236
security policies, 236
rootkits, 233
spyware/adware, 232
Trojan horses, 231
viruses, 230-231
worms, 231
management
accounts, 18-19
controls, 41-42, 484, 504
identity, 18-19
security responsibilities, 189
managing
access, 349
assets, 348-349
backup/recovery, 349
fault tolerance, 348
redundancy, 348
configurations, 358-359
finances during disaster recovery, 393
identities, 349
incident responses, 356-357
keys, 278-279
media
disposal, 355
HSM, 354
labeling, 354
media history, 354
NAS, 353
RAID, 349-352
SAN, 353
memory, 309
passwords, 20, 482-483, 502-503
patches, 359-360
relational databases, 491-492, 510-511
responsibilities. *See* responsibilities

risks, 181
analysis teams, 182
management teams, 181
policies, 181
vulnerabilities, 363
mandatory access control (MAC), 47
man-made disasters, 371
man-made threats, 449-451
collusion, 451
explosions, 449
fires, 449-450
fraud, 450
theft, 450
vandalism, 450
MANs (Metropolitan Area Networks), 120
mantraps, 464
matrix-based models, 315-316
maximum period time of disruption (MPTD), 374
maximum tolerable downtime (MTD), 374, 517
MD algorithms, 271
mean time between failure (MTBF), 356, 374, 517
mean time to repair (MTTR), 356, 374, 517
media
analysis (evidence), 434
disposal, 355
history, 354
labeling, 354
managing
HSM, 354
NAS, 353
RAID, 349-352
SAN, 353
multimedia collaboration, 134-135
portable, 473
relations teams, 395
Media Access Control (MAC) addresses, 82-83, 141
meet-in-the middle attacks, 290
memory, 304-306
addressing
absolute, 306
implied, 306
indirect, 306
logical, 306
relative, 306
associative, 306
caches, 306
cards, authentication, 22-23
DMA, 306
leaks, 306
managing, 309
primary, 306
RAM, 305
ROM, 305
TPM, 280
virtual, 306
mercury vapor lighting, 462
mesh topology, 93-94
Message Authentication Code. *See* MACs
message integrity, 268-269
hash functions
HAVAL, 272
MD algorithms, 271
one-way hash, 269-270
RIPEMD-160, 272
SHA, 271-272
Tiger, 272

MACs
CBC-MAC, 274
CMAC, 274
HMAC, 273
methodologies (security)
CMMI, 174
ISO/IEC 27000, 164-166
ITIL, 172
listing of, 163-164
program life cycle, 174-175
Six Sigma, 173
top-down/bottom-up, 174
metrics (security), 194-195
Metro Ethernet, 120
Metropolitan Area Networks (MANs), 120
middleware, 301
military data classifications, 187-188
MIME (Multipurpose Internet Mail Extension), 282
mirrored sites, 385
mixed law, 409
mobile code, 56, 223
mobile computing platforms, 301
MODAF (British Ministry of Defence Architecture Framework), 168
models
access control, 46
ACLs, 49
capabilities tables, 48
content-dependent, 48
context-dependent, 48
discretionary, 46
mandatory, 47
matrix, 48
RBAC, 47
rule-based, 48
databases, 224
hierarchical, 226
network, 226
object-oriented, 226
object-relational, 226
relational, 225
OSI, 66-67
advantages, 66
Application layer (layer 7), 67
Data Link layer (layer 2), 68-69
encapsulation/de-encapsulation, 76
multi-layer protocols, 70
Network layer (layer 3), 68
Physical layer (layer 1), 69
Presentation layer (layer 6), 67
protocol mappings, 70
Session layer, 67-68
Transport layer (layer 4), 68
security
Bell-LaPadula, 317-318
Biba, 319
Brewer-Nash, 320
Clark-Wilson Integrity, 319-320
Graham-Denning, 320
Harrison-Ruzzo-Ullmen, 321
Lipner, 320
summary, 495, 514
types, 315-316
software development, 211
Agile, 216-217
Build and Fix, 211-212
Cleanroom, 218
CMMI, 218
Incremental, 214
JAD, 218
Prototyping, 214
RAD, 216

Spiral, *215*
V-shaped, *213*
Waterfall, *212-213*
TCP/IP, 71
Application layer, *72*
ARP, *101-102*
encapsulation/de-encapsulation, *76*
Internet layer, *74-75*
Link layer, *76*
TCP/UDP ports, *77-78*
Transport layer, *72-74*
modes
3DES, 262-263, 495, 514
security, 321
compartmented, *321*
dedicated, *321*
multilevel, *322*
system high, *321*
modulation, 135
802.11 techniques, 136
cellular/mobile, 136-137
modulo 26 substitution cipher, 252
MOM (motive, opportunity, means), 429
monitoring
access control, 50
identity theft, *54*
IDS, *50-52*
IPS, *52*
operations security, 363-364
reference, 311
services, 303
special privileges, 345
threats, 52-53
backdoor/trapdoor, *57*
brute-force, *53*
buffer overflow, *55*
dictionary attacks, *53*
DOS/DDOS, *55*
dumpster diving, *55*
emanating, *57*
malware, *56*
mobile code, *56*
passwords, *53*
phishing/pharming, *54*
shoulder surfing, *54*
sniffing, *57*
social engineering, *53*
spoofing, *56*
motive, opportunity, means (MOM), 429
movable lighting systems, 461
MPTD (maximum period time of disruption), 374
MTBF (mean time between failure), 356, 374, 517
MTD (maximum tolerable downtime), 374, 517
MTTR (mean time to repair), 356, 374, 517
multicast transmissions, 85
multihomed firewalls, 115
multi-layer protocols, 70
multilevel
lattice models, 315
security mode, 322
multimedia collaboration, 134-135
multi-mode fiberoptic cabling, 89
multipartite viruses, 231, 511
multiplexers, 109
Multipurpose Internet Mail Extension (MIME), 282
multitasking, 308-309
mutual-aid agreements, 385

N

NAS (Network-Attached Storage), 353

NAT (Network Address Translation), 81-89, 105

National Information Assurance Certification and Accreditation Process (NIACAP), 329

National Institute of Standards and Technology Special Publication. *See* NIST SP

natural access control, 453-454

natural disasters, 371

natural languages, 220

natural surveillance, 454

natural territorials reinforcement, 454

natural threats, 446

earthquakes, 446

floods, 447

hurricanes/tropical storms, 446

tornadoes, 446

NDAs (non-disclosure agreements), 411

need-to-know principles, 29-30, 343

negligence, 421-422

Network Address Translation (NAT), 81-89, 105

Network-Attached Storage (NAS), 353

Network layer (OSI), 68

networks

cabling, 87

coaxial, 87-88

fiberoptic, 89-91

selecting, 87

twisted pair, 88-90

databases, 226

devices, 109

architecture, 115

cloud computing, 117-118

endpoint security, 119

firewalls, 112-114

gateways, 112

honeypots, 117

hubs, 109

multiplexers, 109

patch panels, 109

PBXs, 116-117

proxy servers, 116

routers, 112

switches, 110-111

virtualization, 116

VLANs, 111

encapsulation/de-encapsulation, 76

evidence analysis, 435

IDS, 50

IP addresses

classes, 80-81

IPv4, 77-80, 82

IPv6, 82

NAT, 81-89

public versus private, 81

LANs. *See* LANs

MAC addresses, 82-83

OSI model, 66-67

advantages, 66

Application layer (layer 7), 67

Data Link layer (layer 2), 68-69

multi-layer protocols, 70

Network layer (layer 3), 68

Physical layer (layer 1), 69

Presentation layer (layer 6), 67

protocol mappings, 70

Session layer (layer 5), 67-68

Transport layer (layer 4), 68

protocols
- *ARP*, *101-102*
- *DHCP*, *102-103*
- *FTP*, *104*
- *FTPS*, *104*
- *HTTP*, *104*
- *HTTPS*, *104*
- *ICMP*, *104*
- *IMAP*, *105*
- *POP*, *105*
- *SFTP*, *104*
- *SHTTP*, *104*
- *SMTP*, *105*
- *SNMP*, *105-106*

remote connections, 126
- *authentication protocols*, *133*
- *cable*, *128*
- *dial-up*, *126-127*
- *DSL*, *127-128*
- *ISDN*, *127*
- *multimedia collaboration*, *134-135*
- *RADIUS*, *132-133*
- *SSL*, *134*, *283*
- *TACACS*, *132-133*
- *Telnet*, *134*
- *TLS*, *134*, *284*
- *VPNs*, *129-132*

routing, 106

routing protocols
- *BGP*, *108*
- *categories*, *107*
- *distance vector*, *107*
- *EIGRP*, *108*
- *hybrid*, *107*
- *IGRP*, *108*
- *IS-IS*, *108*
- *link state*, *107*
- *OSPF*, *107*
- *RIP*, *107*
- *security*, *106*
- *static versus dynamic*, *106*
- *types*, *106*
- *VRRP*, *108*

security, 139-141
- *attenuation*, *142*
- *cabling*, *142*
- *crosstalk*, *143*
- *DNS attacks*, *145-147*
- *eavesdropping*, *143*
- *email attacks*, *147-148*
- *ICMP attacks*, *143-145*
- *IP address spoofing*, *150*
- *MAC filters*, *141*
- *noise*, *142*
- *overview*, *6-7*
- *port scanning*, *150*
- *satellites*, *141*
- *session hijacking*, *150*
- *SYN ACK attacks*, *149*
- *teardrop attacks*, *150*
- *WEP*, *140*
- *wireless*, *149*
- *WPA*, *140*
- *WPA2*, *140*

services
- *DNS*, *103*
- *NAT*, *105*
- *PAT*, *105*

TCP/IP, 101-102

transmissions, 86

types
- *extranets*, *119-120*
- *intranets*, *120*

LANs, 119
MANs, 120
wireless. *See* WLANs
NIACAP (National Information Assurance Certification and Accreditation Process), 329
NIST (National Institute of Standards and Technology) SP (Special Publication)
800-30, 176
800-34 Revision 1, 378
800-53, 170-171, 488, 507
noise (WLANs), 142
non-disclosure agreements (NDAs), 411
noninterference models, 316
non-repudiation (cryptosystems), 251
normalization (databases), 225
null ciphers, 252
numeric passwords, 20, 502

O

Object Linking and Embedding (OLE), 223
Object Linking and Embedding Database (OLE DB), 227
object-oriented databases, 226
object-oriented programming (OOP), 220-221
object-relational databases, 226
Object Request Broker (ORB), 222
OC carrier lines, 122
OCSP (Online Certificate Status Protocol), 276
ODBC (Open Database Connectivity), 226
OEP (Occupant Emergency Plan), 474
OFB (Output Feedback), 261-262
OFDM (Orthogonal Frequency Division Multiplexing), 136
OFDMA (Orthogonal Frequency Division Multiple Access), 136
off-the-shelf software packages, 229
OLE (Object Linking and Embedding), 223
OLE DB (Object Linking and Embedding Database), 227
OLTP (Online Transaction Processing) ACID tests, 229
one-time pads, 257-258
one-time passwords, 20, 482, 502
one-way functions, 246, 514
one-way hash, 269-270
Online Certificate Status Protocol (OCSP), 276
Online Transaction Processing (OLTP) ACID tests, 229
onsite assessment security responsibilities, 192
OOP (object-oriented programming), 220-221
Open Database Connectivity (ODBC), 226
The Open Group Architecture Framework (TOGAF), 168, 312
Open Group Single Sign-On Standard website, 31
Open Shortest Path First (OSPF) protocol, 107
Open systems Interconnect model. *See* OSI model
Open Web Application Security Project (OWASP), 210, 333
Operate/Maintain phase (system development life cycle), 205
operating systems, 307-308

operations security, 8
access management, 349
job rotation, 344
least privilege, 343
preventative measures
antivirus/antimalware, 364
IDS/IPS, 363
input/output controls, 362
monitoring/reporting, 363-364
system hardening, 362-363
trusted paths, 362
unscheduled reboots, 362
vulnerability management, 363
procedures, 356
audits, 360
change control, 357-358
configuration management, 358-359
incident response management, 356-357
patches, 359-360
RAID, 497, 514
record retention, 345
resource protection, 346
access, maintaining, 355-356
asset management, 348-349
facilities, 346
hardware, 347
identity management, 349
information assets, 347
media management. See *media, managing*
software, 347
tangible/intangible assets, 346
sensitive information procedures, 344-345
separation of duties, 344
special privileges, monitoring, 345
threats
clipping levels, 361
deviations from standards, 361
unexplained events, 361
opinion evidence, 433
optical jukeboxes, 392, 517
Orange Book, 323-326
assurance requirements
life cycle, 324
operational, 323
classification system, 324-326
A - Verified protection, 325
A1 - Verified Design, 325-326
B - Mandatory protection, 324
B1 - Labeled Security Protection, 324-325
B2 - Structured Protection, 325
B3 - Security Domains, 325
C - Discretionary protection, 324
C1 - Discretionary Security Protection, 324
C2 - Controlled Access Protection, 324
D - Minimal protection, 324
ORB (Object Request Broker), 222
order of volatility, 427
organizations
ethics, 437
information security governance. *See* information security governance
security policies, 184
Orthogonal Frequency Division Multiple Access (OFDMA), 136
Orthogonal Frequency Division Multiplexing (OFDM), 136
OSI (Open Systems Interconnect) model, 66-67
advantages, 66
encapsulation/de-encapsulation, 76

layers
Application (layer 7), 67
Data Link (layer 2), 68-69
Network (layer 3), 68
Physical (layer 1), 69
Presentation (layer 6), 67
Session (layer 5), 67-68
Transport (layer 4), 68
multi-layer protocols, 70
protocol mappings, 70
OSPF (Open Shortest Path First) protocol, 107
outages (power)
impacts, identifying, 374-375
types, 470
Output Feedback (OFB), 261-262
OWASP (Open Web Application Security Project), 210, 333
ownership factor authentication, 22
memory cards, 22-23
smart cards, 23
token devices, 22

P

PaaS (platform as a service), 118
packets
filtering firewalls, 113
switching networks, 123
PACs (Privileged Attribute Certificates), 34
palm/hand scans, 24
PAP (Password Authentication Protocol), 133
parallel tests, 397
parasitic viruses, 231, 511
partial-knowledge tests, 39
passive cryptography attacks, 286
passive infrared systems (PIR), 460
passphrase passwords, 19, 502
passwords
changing, 21
Linux, 21
lockout policies, 21
managing, 20, 482-483, 502-503
static, 481-482
threats, monitoring, 53
types, 481-482, 501-502
cognitive, 20
combination, 19
complex, 19
graphical, 20
numeric, 20
one-time, 20, 482
passphrase, 19
standard, 19
static, 19
Windows, 22
PAT (Port Address Translation), 105
patches
management, 359-360
panels, 109
patents, 410
paths
tracing, 435
trusted, 362
patrol force, 462
PBXs (private branch exchanges), 116-117
PCI DSS (Payment Card Industry Data Security Standard), 418
peer-to-peer computing, 335
penetration testing, 38-39
categories, 39

performing, 38
strategies, 38-39

perimeters, 458
access control, 462-463
acoustical detection systems, 461
barriers, 459
capacitance detectors, 461
CCTV, 461
electromechanical systems, 460
fences, 459
gates, 459-460
infrared sensors, 460
intrusion detection, 460
lighting
feet of illumination ratings, 462
systems, 461-462
types, 462
patrol force, 462
photoelectric systems, 460
walls, 460
wave motion detectors, 461

Personal Information Protection and Electronic Documents Act (PIPEDA), 417

personally identifiable information (PII), 414

personnel
components (BCP), 377
doors, 463
privacy, protecting, 474
safety, 474
security responsibilities, 192-193

PGP (Pretty Good Privacy), 281-282

pharming, 54

phishing, 54, 148

photoelectric systems, 460

physical addressing, 82-83

physical controls, 43-45, 472, 486, 506

Physical layer (OSI), 69

physical security, 9
equipment, 472
corporate procedures, 472-473
security device protection, 473-474
geographical threats, 445
internal versus external, 445
natural, 446-447
interior building, 463
biometrics, 466
data centers, 467
door locks, 463
doors, 463
equipment rooms, 467
glass entries, 466
locks, 464-465
mantraps, 464
restricted work areas, 468
turnstiles, 464
visitors, 466-467
work areas, 467
lighting, 461
feet of illumination ratings, 462
systems, 461-462
types, 462
man-made threats, 449
collusion, 451
explosions, 449
fires, 449-450
fraud, 450
theft, 450
vandalism, 450
natural access control, 453-454
perimeters, 458
access control, 462-463

acoustical detection systems, *461*
barriers, *459*
capacitance detectors, *461*
CCTV, *461*
electromechanical systems, *460*
fences, *459*
gates, *459-460*
infrared sensors, *460*
intrusion detection, *460*
patrol force, *462*
photoelectric systems, *460*
walls, *460*
wave motion detectors, *461*
personnel
privacy, *474*
safety, *474*
politically motivated threats, 451-452
bombings, *452*
civil disobedience, *452*
riots, *451*
strikes, *451*
terrorist acts, *452*
site and facility design, 453
computer and equipment rooms, *457-458*
construction, *456-457*
CPTED, *453*
facility selection, *455*
internal compartments, *457*
layered defense model, *453*
natural surveillance, *454*
natural territorials reinforcement, *454*
physical security plan, *454-455*
system threats, 447
communications, *447-448*
electrical, *447*
utilities, *448*

physiological characteristics (authentication), 24-25
PII (personally identifiable information), 414
Ping of Death, 144
ping scanning, 145
PIPEDA (Personal Information Protection and Electronic Documents Act), 417
PIR (passive infrared systems), 460
PKI (Public Key Infrastructure), 275
CAs, 275-276
CRLs, 277
cross-certification, 278
digital certificates, 276
classes, *277*
requesting, *277*
X.509, *276-277*
OCSP, 276
RAs, 275
trusted entity communication, 277-278
plaintext, 244, 493, 512
platform as a service (PaaS), 118
PLD (Programmable Logic Device), 305
Point-to-Point Protocol (PPP), 124, 126
Point-to-Point Tunneling Protocol (PPTP), 129-130
policies
access control, 29
corporate, 472-473
encryption, *472*
inventory, *473*
tamper protection, *472*
equipment security, 472-473
encryption, *472*

inventory, 473
tamper protection, 472
incident response, 424-425
information security governance, 183-186
categories, 185
issue-specific, 185
organizational security, 184
system-specific, 185
job rotation, 344
least privilege, 29-30, 343
lockout, 21
malware protection, 236
operations, 356
audits, 360
change control, 356-359
configuration management, 358-359
incident response management, 356-357
patches, 359-360
portable media, 473
record retention, 345
risk management, 181
sensitive information, 344-345
separation of duties, 344
special privileges, monitoring, 345
politically motivated threats, 451-452
bombings, 452
civil disobedience, 452
riots, 451
strikes, 451
terrorist acts, 452
polling, 101
polyinstantiation (databases), 228
polymorphic viruses, 231, 511
polymorphism, 221
POP (Post Office Protocol), 105
portable media procedures, 473
ports
address translation (PAT), 105
scanning attacks, 150
TCP/UDP, 77-78
Post Office Protocol (POP), 105
power
conditioners, 471
outages
impacts, 374-375
types, 470
preventative measures, 470-471
redundancy, 379
supplies, 470
PPP (Point-to-Point-Protocol), 124, 126
PPTP (Point-to-Point Tunneling Protocol), 129-130
preaction sprinkler systems, 469
preemptive multitasking, 309
prerequisites for exam, 10
Presentation layer (OSI), 67
Pretty Good Privacy (PGP), 281-282
preventive controls, 41
PRI (primary rate) ISDN, 127
primary keys, 228, 511
primary memory, 306
primary rate (PRI) ISDN, 127
privacy, 413
expectations, 419
laws, 415
Basel II, 417
CALEA of 1994, 417
CFAA, 416
Computer Security Act of 1987, 417
Economic Espionage Act of 1996, 418
ECPA of 1986, 416

employee privacy issues, 419
European Union, 419
expectations of privacy, 419
Federal Privacy Act of 1974, 416
FISA of 1978, 416
FISMA of 2002, 418
GLBA, 415
Health Care and Education Reconciliation Act of 2010, 418
HIPAA, 415
PCI DSS, 418
PIPEDA, 417
SOX Act, 415
United States Federal Sentencing Guidelines of 1991, 417
USA PATRIOT Act, 418
personnel, protecting, 474
PII (personally identifiable information), 414
private branch exchanges (PBXs), 116-117
private IP addresses, 81
private key encryption. ***See*** **symmetric algorithms**
Privileged Attribute Certificates (PACs), 34
privileges
escalation, 235
special, monitoring, 345
procedures. ***See*** **policies**
process/policy reviews, 192
professional ethics. ***See*** **ethics**
programmable logic device (PLD), 305
programming, 219
ActiveX, 224
cohesion, 221
compiled *versus* interpreted code, 220
CORBA, 222
coupling, 221
data structures, 222
distributed object-oriented systems, 222
Java
applets, 223
Enterprise Edition, 223
languages
assembly, 219
databases, 226-227
high-level, 219
machine, 219
natural, 220
very-high-level, 219
mobile code, 223
object-oriented, 220-221
OLE, 223
polymorphism, 221
SOA, 223
protocols
anomaly-based IDS, 51
ARP, 75, 101-102
CHAP, 133
DHCP, 102-103
EAP, 133
FDDI, 97
frame relay, 123
FTP, 104
FTPS, 104
HTTP, 104, 284
HTTPS, 104, 284
ICMP. *See* ICMP
IGMP, 75
IMAP, 105
IP, 74
IPsec, 285-286

ISAKMP, 130
L2TP, 130
OCSP, 276
OSI
mapping, 70
multi-layer, 70
PAP, 133
POP, 105
PPP, 124, 126
PPTP, 129-130
remote authentication, 133
routing
BGP, 108
categories, 107
distance vector, 107
EIGRP, 108
hybrid, 107
IGRP, 108
IS-IS, 108
link state, 107
OSPF, 107
RIP, 107
security, 106
static versus dynamic, 106
types, 106
VRRP, 108
SFTP, 104
SHTTP, 104, 284
SIP, 125
SLIP, 126
SMTP, 105
SNMP, 105-106
SSL, 134, 283
TCP
functionality examples, 74
ports, 77-78
three-way handshake, 73
UDP, compared, 73
TCP/IP. *See* TCP/IP
Telnet, 134
TKIP, 140
TLS, 134, 284
Token Ring, 96
UDP
ports, 77-78
TCP, compared, 73
Prototyping software development method, 214
provisioning life cycle, 50
proxy firewalls, 113-114
proxy servers, 116
PSTN (Public Switched Telephone Network), 125
public IP addresses, 81
public key encryption. *See* asymmetric algorithms
Public Key Infrastructure. *See* PKI
punitive damages, 408
purging data, 355

Q

qualitative risk analysis, 179
quantitative risk analysis, 178-179
quantum cryptography, 282
quartz lamps, 462

R

RAD (Rapid Application Development) software development method, 216
RADIUS (Remote Authentication Dial In User Service), 132-133

RAID (Redundant Array of Independent Disks), 349-352
data recovery, 392
defined, 518
implementing, 352
levels
0 (disk striping), 349
1 (disk mirroring), 350
3, 350
5, 351
7, 351
summary, 352
Rainbow Series, 323
Orange Book, 323-326
classification system, 324-326
life cycle assurance requirements, 324
operational assurance requirements, 323
Red Book, 326
RAM (Random Access Memory), 305
Rapid Application Development (RAD) software development method, 216
RAs (Registration Authorities), 275
RBAC (role-based access control), 47
RC algorithms, 264
Read Only Memory (ROM), 305
reciprocal agreements, 384
records
defined, 225
retention, 345
recoverability, 376
recovery
asset management, 349
controls, 41
disasters. *See* disaster recovery
point objective (RPO), 375, 517
priorities, 376, 381
time objective (RTO), 374, 517
trusted, 362
Red Book, 326
redundancy
asset management, 348
hardware, 355
sites, 385
systems, facilities, power, 379
Virtual Router Redundancy Protocol (VRRP), 108
Redundant Array of Independent Disks. *See* RAID
reference monitors, 311
referential integrity, 225, 522
Registration Authorities (RAs), 275
regulations. *See* laws
regulatory law, 409
regulatory security policies, 185
relational databases, 225
attributes, 225
base relations, 225
cardinality, 225
degrees, 225
domains, 225
keys
candidate, 225
foreign, 225
primary, 225
managing, 510
normalization, 225
records, 225
referential integrity, 225
relations, 225
schemas, 225
tuples, 225
views, 225
relations, 225

relative addresses, 306
Release/Maintenance phase (software development life cycle), 209
religious law, 409
remanence (media disposal), 355
Remote Authentication Dial In User Service (RADIUS), 132-133
remote connections, 126
attacks, 149
authentication protocols, 133
cable, 128
dial-up, 126-127
DSL, 127-128
security, 128
versions, 127-128
Internet security, 283
ISDN, 127
multimedia collaboration, 134-135
RADIUS, 132-133
SSL, 134, 283
TACACS, 132-133
Telnet, 134
TLS, 134, 284
VPNs, 129-132
encapsulation/de-encapsulation, 76, 129
IPsec, 130-132
L2TP, 130
PPTP, 129-130
remote journaling, 392, 498, 517
replay attacks, 289
replication, 392, 498, 518
reporting
accountability, 36-37
operations security, 363-364
Request for Comments (RFC) 1087, 437
requirements
ITSEC, 326
assurance, 327
functional, 326-327
Orange Book assurance, 323-326
life cycle, 324
operational, 323
resources, 375
system security, 310-311
residual risks, 180
resource protection, 346
access
maintaining, 355-356
management, 349
asset management, 348-349
backup/recovery systems, 349
fault tolerance, 348
redundancy, 348
identity management, 349
media management
HSM, 354
labeling, 354
media disposal, 355
media history, 354
NAS, 353
RAID, 349-352
SAN, 353
preventative measures
antivirus/antimalware, 364
IDS/IPS, 363
input/output controls, 362
monitoring/reporting, 363-364
system hardening, 362-363
trusted paths, 362
trusted recovery, 362
vulnerability management, 363

tangible/intangible assets, 346
facilities, 346
hardware, 347
information assets, 347
software, 347
threats
clipping levels, 361
deviations from standards, 361
unexplained events, 361
resources. *See also* assets
critical, identifying, 374
criticality levels, 374-375
identifying, 15
protection. *See* resource protection
relationships with users, identifying, 16
requirements, 375
application owners, 183
audit committee, 189
auditors, 191
board of directors, 188
data custodians, 190
data owners, 190
document exchange/review, 192
management, 189
onsite assessment, 192
personnel, 192-193
process/policy reviews, 192
security administrators, 190
security analysts, 191
supervisors, 191
system administrators, 190
system owners, 190
third-party governance, 191
users, 191
responsibilities, 188
restoration teams, 395
restricted work areas, 468
retina scans, 25
reverse engineering, 289, 434
RFC (Request for Comments) 1087, 437
ring topology, 91
riots, 451
RIP (Routing Information Protocol), 107
RIPEMD-160 hash function, 272
risks
assessment, 175
asset value, determining, 177
handling risks, 180-181
NIST SP 800-30, 176
qualitative risk analysis, 179
quantitative risk analysis, 178-179
safeguards, selecting, 179-180
total risk versus residual risk, 180
vulnerabilities/threats, 177-178
defined, 161
handling, 180-181
managing, 6-7, 181
analysis teams, 182
management teams, 181
policies, 181
residual, 180
total, 180
Rivest, Shamri, Adleman (RSA) algorithm, 267
Rivest, Ron, 267
role-based access control (RBAC), 47
ROM (Read Only Memory), 305
rootkits, 233
routers, 112
routing
networks, 106

protocols
BGP, 108
categories, 107
distance vector, 107
EIGRP, 108
hybrid, 107
IGRP, 108
IS-IS, 108
link state, 107
OSPF, 107
RIP, 107
security, 106
static versus dynamic, 106
types, 106
VRRP, 108
Routing Information Protocol (RIP), 107
RPO (recovery point objective), 375, 517
RSA (Rivest, Shamir, Adleman) algorithm, 267
RTO (recovery time objective), 374
rule-based
access control, 48
IDS, 52, 507
rules of engagement (incident response), 424
running key ciphers, 252

S

SaaS (software as a service), 118
SABSA (Sherwood Applied Business Security Architecture) framework, 168, 312, 490, 509
safeguards, selecting, 179-180
safes, 474
sags, 470
salvage teams, 395
SAML (Security Assertion Markup Language), 332
SAN (Storage Area Networks)
data recovery, 392
defined, 353
Sarbanes-Oxley (SOX) Act, 415
satellite connection security, 141
schemas, 225, 510
Scientific Working Group on Digital Evidence (SWGDE), 428-429
scope (incident responses), 424
screened host firewalls, 115
screened subnet firewall, 115
scrubbing, 36
scytale ciphers, 246
SDRAM (Synchronous Dynamic Random Access Memory), 305
SDSL (Symmetric DSL), 128
search warrants, 433
secondary evidence, 432
secret key encryption. *See* symmetric algorithms
Secure Electronic Transactions (SETs), 284
Secure European System for Applications in a Multi-vendor Environment (SESAME), 34
Secure Hash Algorithm (SHA), 271-272
Secure-HTTP (SHTTP), 104, 284
Secure MIME (S/MIME), 282
Secure Shell. *See* SSH
Secure Sockets Layer (SSL), 134, 283
security
budgets, 194-195
effectiveness, 194-195
job rotation, 163

methodologies
CMMI, 174
ISO/IEC 27000 Series, 164-166
ITIL, 172
listing of, 163-164
program life cycle, 174-175
Six Sigma, 173
top-down/bottom-up, 174
metrics, 194-195
models
Bell-LaPadula, 317-318
Biba, 319
Brewer-Nash, 320
Clark-Wilson Integrity, 319-320
Graham-Denning, 320
Harrison-Ruzzo-Ullmen, 321
Lipner, 320
summary, 495, 514
types, 315-316
modes, 321
compartmented, 321
dedicated, 321
multilevel, 322
system high, 321
teams, 395-396
Security Assertion Markup Language (SAML), 332
security device protection, 473-474
portable media, 473
safes/vaults/locking, 474
tracking devices, 473
seizure of evidence, 434
sensitive information procedures, 344-345
separation of duties, 29, 163, 344
Serial Line Internet Protocol (SLIP), 126
servers
attacks, 333
proxy, 116
Service Level Agreements (SLAs), 356
Service-Oriented Architecture (SOA), 223
service set identifiers (SSIDs), 137
services
directory, 30-31
DNS attacks, 103, 145-146
cache poisoning, 145
cybersquatting, 147
DDoS, 146
DNSSEC, 146
domain grabbing, 147
DoS, 146
URL hiding, 146
network
DNS, 103
NAT, 105
PAT, 105
public cloud computing, 117-118
RADIUS, 132-133
security, 302-303
access control, 302
auditing, 303
boundary control, 302
cryptography, 303
integrity, 303
monitoring, 303
SMDS, 124
TACACS/TACACS+, 132-133
SESAME (Secure European System for Applications in a Multi-vendor Environment), 34
Session Initiation Protocol (SIP), 125
Session layer (OSI), 67-68

SETs (Secure Electronic Transactions), 284
SFTP (SSH File Transfer Protocol), 104
SHA (Secure Hash Algorithm), 271-272
Shamir, Adi, 267
shareware, 412
Sherwood Applied Business Security Architecture (SABSA), 168, 312, 490, 509
shielded twisted pair (STP) cabling, 89
shoulder surfing, 54
SHTTP (Secure-HTTP), 104, 284
signature-based IDS, 51, 503
signature dynamics scanning, 25
signing up for the exam, 10
Simple Mail Transfer Protocol (SMTP), 105
Simple Network Management Protocol (SNMP), 105-106
simple passwords, 19
simulation tests, 397
single loss expectancy (SLE), 178
single mode fiberoptic cabling, 89
Single Point of Failure (SPOF), 356
single sign-on. *See* SSO
SIP (Session Initiation Protocol), 125
site design, 453
computer and equipment rooms, 457-458
construction, 456-457
CPTED, 453
facility selection, 455
accessibility, 456
surrounding area/external entities, 456
visibility, 456
internal compartments, 457
layered defense model, 453
lighting, 461
feet of illumination ratings, 462
systems, 461-462
types, 462
natural access control, 453-454
natural surveillance, 454
natural territorials reinforcement, 454
perimeters, 458
access control, 462-463
acoustical detection systems, 461
barriers, 459
capacitance detectors, 461
CCTV, 461
electromechanical systems, 460
fences, 459
gates, 459-460
infrared sensors, 460
intrusion detection, 460
patrol force, 462
photoelectric systems, 460
walls, 460
wave motion detectors, 461
physical security plan, 454-455
criminal activity, deterring, 454
delaying intruders, 455
detecting intruders, 455
intrusions/disruptions response, 455
situation assessment, 455
Six Sigma, 173
Skipjack, 264
slack space analysis, 434
SLAs (Service Level Agreements), 356
SLE (single loss expectancy), 178
SLIP (Serial Line Internet Protocol), 126

Small Outline DIMM (SODIMM), 305
smart cards, 23
SMDS (Switched Multimegabit Data Service), 124
S/MIME (Secure MIME), 282
smoke activated fire detection, 468
SMTP (Simple Mail Transfer Protocol), 105
Smurf attacks, 144
sniffing, 57
SNMP (Simple Network Management Protocol), 105-106
SOA (Service-Oriented Architecture), 223
social engineering threats, 53, 287
SOCKS firewalls, 114
SODIMM (Small Online DIMM), 305
sodium vapor lighting, 462
software
commercial, 412
development. *See* software development
disaster recovery, 386-387
evidence analysis, 434
freeware, 412
piracy and licensing issues, 412-413
protection, 347
shareware, 412
software as a service (SaaS), 118
software development
knowledge-based systems, 229
life cycle, 206
change/configuration management, 209
design, 207
Develop, 207
Gather Requirements, 206-207
Release/Maintain, 209
Test/Validate, 208-209
malware, 230
botnets, 232
logic bombs, 232
protection, 235-236
rootkits, 233
spyware/adware, 232
Trojan horses, 231
viruses, 230-231
worms, 231
methods, 211
Agile, 216-217
Build and Fix, 211-212
Cleanroom, 218
CMMI, 218
Incremental, 214
JAD, 218
Prototyping, 214
RAD, 216
Spiral, 215
V-shaped, 213
Waterfall, 212-213
programming, 219
ActiveX, 224
assembly languages, 219
cohesion, 221
compiled versus interpreted code, 220
CORBA, 222
coupling, 221
data structures, 222
distributed object-oriented systems, 222
high-level languages, 219
Java, 223
machine languages, 219
mobile code, 223

natural languages, 220
object-oriented, 220-221
OLE, 223
polymorphism, 221
SOA, 223
very-high-level languages, 219
security, 210
auditing, 237
backdoors, 235
BSI, 210
buffer overflow, 233-235
certification/accreditation, 236-237
ISO/IEC 27000, 210
malware protection, 235-236
overview, 7
OWASP, 210
privilege escalation, 235
source code issues, 233
WASC, 210
SONET (Synchronous Optical Networks), 120, 122
source code issues (software), 233
SOX (Sarbanes-Oxley) Act, 415
SP (Special Publication) 800-34 Revision 1, 378
spam, 148
spear phishing, 148
special privileges, monitoring, 345
Special Publication (SP) 800-34 Revision 1, 378
Spiral software development method, 215
SPOF (Single Point of Failure), 356
sponsoring bodies, 2-4
spoofing, 56
email, 147
IP addresses, 150
sprinkler systems, 469
spyware, 56, 232
SSH (Secure Shell)
File Transfer Protocol (SFTP), 104
Internet security, 285
SSIDs (service set identifiers), 137
SSL (Secure Sockets Layer), 134, 283
SSO (single sign-on), 31-32
advantages, 31
authorization, 31
disadvantages, 32
Open Group Single Sign-On Standard website, 31
stakeholders, 299
standard glass, 466
standard passwords, 19, 501
standards
deviations, 361
information security governance, 185
ISO/IEC 27000, 164-166
wireless
802.11a, 138
802.11b, 138
802.11g, 138
standby lighting systems, 461
star topology, 92
state machine models, 315
stateful firewalls, 113
static passwords, 19, 481-482, 501
static routing, 106
statistical anomaly-based IDS, 51
statistical attacks, 289
statutory damages, 408
stealth viruses, 231, 511
steganography, 258, 434

storage. *See also* memory
HSM, 354, 392, 498, 517
NAS, 353
SAN
data recovery, 392
defined, 353
Storage Area Networks. *See* SAN
STP (shielded twisted pair) cabling, 89
stream-based ciphers, 254
strikes, 451
structured walk-through tests, 397
substitution, 245, 494-495, 513
substitution ciphers, 257
defined, 252
modulo 26, 252
one-time pads, 257-258
steganography, 258
supervisor security responsibilities, 191
supplies, recovering, 387
surges (power), 470
surrounding areas (facilities), 456
surveillance, 433
SWGDE (Scientific Working Group on Digital Evidence), 428-429
Switched Multimegabit Data Service (SMDS), 124
switches, 110-111
layer 3 *versus* layer 4, 111
transparent bridging, 110
symmetric algorithms, 253-254, 258
3DES
modes, 262-263, 495, 514
overview, 262
AES, 263
block ciphers, 255
Blowfish, 264
CAST, 265
DES
defined, 259
Double-DES, 259
key length, 259
modes, 259-262
IDEA, 263
Initialization Vectors (IVs), 255
key facts, 496, 514
RC, 264
Skipjack, 264
stream-based ciphers, 254
strengths/weaknesses, 254, 495, 514
Twofish, 264
Symmetric DSL (SDSL), 128
symmetric multitasking, 308
SYN ACK attacks, 149
Synchronous Dynamic Random Access Memory (SDRAM), 305
synchronous encryption/decryption, 244, 493, 512
Synchronous Optical Networks (SONET), 120, 122
synchronous transmissions, 84
systems
administrator security responsibilities, 190
architecture, 298
computing platforms, 300-301
CPUs, 303-304
design phase, 299
development phase, 299
input/output devices, 307
ISO-IEC 42010:2011, 299
maintenance, 299

memory, 304-306
multitasking, 308-309
operating systems, 307-308
security services, 302-303
development life cycle, 203-204
Acquire/Develop, 204-205
Dispose, 205-206
Implement, 205
Initiate, 204
Operate/Maintain, 205
distributed, 300
cloud computing, 335
grid computing, 335
peer-to-peer computing, 335
embedded, 301
hardening, 362-363
high security mode, 321
owner security responsibilities, 190
ports, 77
redundant, 379
security architecture, 310
documentation, 314
frameworks. See *frameworks*
models. See *security, models*
modes. See *security, modes*
policies, 310
requirements, 310-311
zones, 311
specific security policies, 185
threats, 447
communications, 447-448
electrical, 447
utilities, 448

T

T carrier lines, 121
table-top exercises, 397
tables
capabilities, 48
routing, 106
TACACS+ (Terminal Access Controller Access-Control System Plus), 132-133
TACACS (Terminal Access Controller Access-Control System), 132-133
tamper protection, 472
tangible asset protection, 177, 346
facilities, 346
hardware, 347
information assets, 347
software, 347
tape vaulting, 392, 517
Tavares, Stafford, 265
TCB (Trusted Computer Base), 310
TCP (Transmission Control Protocol), 72
functionality examples, 74
ports, 77-78
three-way handshake, 73
UDP, compared, 73
TCP/IP, 71
ARP, 101-102
encapsulation/de-encapsulation, 76
IP, 74
layers
Application, 72
Link, 76
Internet, 74-75
Transport, 72-74

TCP
functionality examples, 74
ports, 77-78
three-way handshake, 73
UDP, compared, 73
TCP/UDP ports, 77-78
TCSEC (Trusted Computer System Evaluation Criteria)
ITSEC, mapping, 327
overview, 323
TDMA (Time Division Multiple Access), 136
teams
disaster recovery
damage assessment, 394
legal, 394
listing of, 394
media relations, 395
restoration, 395
salvage, 395
security, 395-396
incident response, 424
creating, 424
investigations, 424
procedures, 424-425
rules of engagement/authorization/ scope, 424
teardrop attacks, 150
technical controls, 43-44
technological disasters, 371
technologies, recovering
hardware, 386
software, 386-387
telecommunications, 6
Telnet, 134
tempered glass, 466
Ten Commandments of Computer Ethics, 436
Terminal Access Controller Access-Control System (TACACS), 132-133
Terminal Access Controller Access-Control System Plus (TACACS+), 132-133
Temporal Key Integrity Protocol (TKIP), 140
terrorist acts, 452
tertiary sites, 384
Test/Validate phase (Software Development Life Cycle), 208-209
testing
alternate facility locations, 383
BCP/DRP, 396-397
checklist tests, 396
evacuation drills, 397
full-interruption tests, 397
functional drills, 397
parallel tests, 397
simulation tests, 397
structured walk-through tests, 397
table-top exercises, 397
OLTP ACID, 229
penetration, 38-39
categories, 39
performing, 38
strategies, 38-39
theft, 450
Thicknet, 87
thin client platforms, 300
Thinnet, 88
third-party
governance security responsibilities, 191
outsourcing, 422

threats. *See also* attacks
access control, 52-53
backdoor/trapdoor, *57*
brute-force, *53*
buffer overflow, *55*
dictionary attacks, *53*
DoS/DDoS, *55*
dumpster diving, *55*
emanating, *57*
identity theft, *54*
malware, *56*
mobile code, *56*
passwords, *53*
phishing/pharming, *54*
shoulder surfing, *54*
sniffing, *57*
social engineering, *53*
spoofing, *56*
agents, 161
architecture, 330
data flow control, *333*
maintenance hooks, *331*
OWASP, *333*
SAML, *332*
server-based attacks, *333*
time-of-check/time-of-use attacks, *331-332*
web-based, *332*
XML, *332*
assets, 177-178
data mining warehouses, 334
database, 228, 333-334
aggregation, *334*
contamination, *334*
inference, *334*
defined, 161
distributed systems
cloud computing, *335*
grid computing, *335*
peer-to-peer computing, *335*
geographical, 444
networks, 142-150
attenuation, *142-143*
cabling, *142*
crosstalk, *143*
DNS attacks, *145-146*
eavesdropping, *143*
email attacks, *147-148*
ICMP attacks, *143-144*
noise, *142*
operations
antivirus/antimalware, *364*
clipping levels, *361*
deviations from standards, *361*
IDS/IPS, *363*
input/output controls, *362*
monitoring/reporting, *363-364*
system hardening, *362-363*
trusted paths, *362*
trusted recovery, *362*
unexplained events, *361*
vulnerability management, *363*
physical
internal versus external, *437*
man-made, *449-451*
natural, *446-447*
politically motivated, *451-452*
system, *447-449*
software, 230
backdoors, *235*
botnets, *232*
buffer overflow, *233-235*
logic bombs, *232*

malware protection, 235-236
privilege escalation, 235
rootkits, 233
source code issues, 233
spyware/adware, 232
Trojan horses, 231
viruses, 230-231
worms, 231
throughput rate, 503
Tiger hash functions, 272
Time Division Multiple Access (TDMA), 136
time-of-check/time-of-use attacks, 331-332
TKIP (Temporal Key Integrity Protocol), 140
TLS (Transport Layer Security), 134, 284
TOGAF (The Open Group Architecture Framework), 168, 312
tokens
device authentication methods, 22
passing, 101
ring, 96
topologies (networks), 89
bus, 92
hybrid, 94
mesh, 93-94
ring, 91
star, 92
tornadoes, 446
tort law, 408-409
total risks, 180
TPM (Trusted Platform Module), 279-280
tracking devices, 473
trade secrets, 410-411
trademarks, 411
traffic anomaly-based IDS, 51
transaction log backups, 390
Transmission Control Protocol. *See* TCP
transmissions, 83
analog *versus* digital, 83
asynchronous *versus* synchronous, 84
broadband *versus* baseband, 84-85
broadcast, 86
multicast, 85
unicast, 85
wired *versus* wireless, 86
transparent bridging, 110
Transport layer
OSI, 68
TCP/IP, 72-74
TCP functionality, 74
TCP three-way handshake, 73
TCP/IP and UDP headers, 73
Transport Layer Security (TLS), 134, 284
transposition, 245, 253, 494, 513
trapdoors, 57, 246, 514
Triple DES. *See* 3DES
Trojan horses, 56, 231
tropical storms, 446
trust
levels. *See also* Rainbow Series
accreditation and certification, 329-330
evaluation systems, 326-329
paths, 362
recovery, 362
Trusted Computer Base (TCB), 310
Trusted Computer System Evaluation Criteria (TCSEC), 323, 327
Trusted Platform Module (TPM), 279-280

trusted third-party model (federated identities), 35

tumbler locks, 465

tuples, 225, 510

turnstiles, 464

twisted pair cabling, 88-90
- categories, 89-90
- shielded *versus* unshielded, 89
- types, 89

Twofish, 264

Type I authentication, 17
- identity/account management, 18-19
- passwords, 19-22
  - *changing, 21*
  - *Linux, 21*
  - *lockout policies, 21*
  - *management, 20*
  - *types, 19-20*
  - *Windows, 22*

Type II authentication, 22
- memory cards, 22-23
- smart cards, 23
- token devices, 22

Type III authentication, 23
- behavioral characteristics, 25
- biometrics
  - *considerations, 26-28*
  - *effectiveness rankings, 26-27*
  - *user acceptance rankings, 27*
- physiological characteristics, 24-25

U

UDP (User Datagram Protocol)
- ports, 77-78
- TCP, compared, 73

unexplained events, 361

unicast transmissions, 85

United States Federal Sentencing Guidelines of 1991, 417

unshielded twisted pair (UTP) cabling, 89

UPS (uninterruptible power supplies), 471

URL hiding, 146

USA PATRIOT (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act, 418

User Datagram Protocol. *See* UDP

users
- environment recovery, 388
- identifying, 16
- job rotation, 344
- least privilege, 29-30, 343
- ports, 77
- relationships with resources, identifying, 16
- security responsibilities, 191
- separation of duties, 344
- special privileges, monitoring, 345

utilities systems threats, 448

UTP (unshielded twisted pair) cabling, 89

V

V-shaped software development method, 213

value of CISSP certification
- enterprise, 5
- security professionals, 5

vandalism, 450

vascular scans, 25

vaults, 463, 474

VDSL (Very High Bit-Rate DSL), 128
vehicle access doors, 463
Very High Bit-Rate DSL (VDSL), 128
very-high-level languages, 219
viewpoints, 299
views, 225, 228, 299, 511
Vigenere ciphers, 248-249
virtual local area networks (VLANs),111
virtual memory, 306
virtual platforms, 301
Virtual Private Networks. *See* **VPNs**
Virtual Router Redundancy Protocol (VRRP), 108
virtualization, 116
viruses
- antivirus software, 236
- boot sector, 231, 511
- defined, 56
- Trojan horses, 231
- macro, 231, 511
- multipartite, 231, 511
- parasitic, 231, 511
- polymorphic, 231, 511
- stealth, 231, 511
- types, 492, 511
- worms, 231

visibility (facility selection), 456
visitor control, 466-467
VLANs (virtual local area networks), 111
voice pattern scanning, 25
VoIP (Voice over IP), 125-126
VPNs (Virtual Private Networks), 129-132
- encapsulation/de-encapsulation, 129
- IPsec, 130-132
- L2TP, 130
- PPTP, 129-130

VRRP (Virtual Router Redundancy Protocol), 108
vulnerabilities. ***See also*** **threats**
- assessments, 37-38
- assets, 177-178
- defined, 160
- managing, 363

W

walls (perimeters), 460
WANs (wide area networks), 121
- ATM, 123
- carrier lines
  - *E, 121*
  - *OC, 122*
  - *T, 121*
- circuit-switching, 123
- CSU/DSU, 122
- frame relay, 123
- HSSI, 124-125
- packet-switching, 123
- PPP, 124
- PSTN, 125
- SMDS, 124
- VoIP, 125-126
- X.25, 124

warchalking, 149
wardriving, 149
warm sites, 384
WASC (Web Application Security Consortium), 210
water leakages, 471
Waterfall software development method, 212-213

wave motion detectors, 461
web-based attacks, 332
websites
CIDR, 80
CISSP registration, 10
ISO, 166
Open Group Single Sign-On Standard, 31
RFC 1087, 437
WEP (Wired Equivalent Privacy), 140
wet pipe sprinkler systems, 469
whaling, 148
white hats, 407
wide area networks. *See* WANs
Wi-Fi Protected Access. *See* WPA
Windows password management, 22
WIPO (World Intellectual Property Organization), 412
Wired Equivalent Privacy (WEP), 140
wired/wireless transmissions, 86
WLANs (wireless networks), 135
802.11 techniques, 136
access points, 137
attacks, 149
Bluetooth, 139
cellular/mobile, 136-137
CSMA/CA, 100
infrared, 139
Infrastructure mode *versus* Ad Hoc mode, 137
modulation, 135
802.11 techniques, 136
cellular/mobile, 136-137
security, 139-141
MAC filters, 141
WEP, 139-140
WPA, 140
WPA2, 140
SSIDs, 137
standards, 138
802.11a, 138
802.11b, 138
802.11f, 138
structure
access points, 137
SSIDs, 137
TCP/IP model, 71
ARP, 101-102
Application layer, 72
encapsulation/de-encapsulation, 76
Internet layer, 74-75
IP, 74
Link layer, 76
TCP. See *TCP*
TCP/UDP ports, 77-78
Transport layer, 72-74
threats, 142-150
attenuation, 142-143
cabling, 142
crosstalk, 143
DNS attacks, 145-146
eavesdropping, 143
email attacks, 147-148
ICMP attacks, 143-144
noise, 142
topologies, 89
bus, 92
hybrid, 94
mesh, 93604+-94
ring, 91
star, 92

transmissions, 83
analog versus digital, 83
asynchronous versus synchronous, 84
broadband versus baseband, 84-85
multicast, 85
unicast, 85
wired versus wireless, 86
WANs
ATM, 123
circuit-switching, 123
CSU/DSU, 122
E carrier lines, 121
frame relay, 123
HSSI, 124-125
OC carrier lines, 122
overview, 121
packet-switching, 123
PPP, 124
PSTN, 125
SMDS, 124
T carrier lines, 121
VoIP, 125-126
X.25, 124
work areas (facilities), 467
work factors, 246, 513
World Intellectual Property Organization (WIPO), 412
World War II cryptography, 249-250
worms, 56, 231
WPA (Wi-Fi Protected Access)
overview, 140
personal *versus* enterprise versions, 140
WPA2 (Wi-Fi Protected Access 2)
overview, 140
personal *versus* enterprise versions, 140
WRT (work recovery time), 374, 517

X

X.25, 124
X.400 directory service standard, 31
X.500 directory service standard, 30
X.509 certificates, 276-277
XML
architecture threats, 332
databases, 227

Z

Zachman framework, 166-167, 312, 489, 508
zero-knowledge
proof, 268
tests, 39
zones (security), 311