



Numerics

3DES (Triple DES) 432, 636
802.1Q tunneling 881

A

- AAA 428, 436, 448–449
 - configuring on PIX Firewall 581, 583, 585–593
 - configuring with RADIUS 569–581
 - user account verification 449–451
 - VPDN configuration 752–761
- access attacks 436
- access control lists. *See* ACLs
- access-list command 756
- accounting, Tripwire 967
- accounts
 - locking 965
 - root account, modifying 964
- ACEs (access control entries) 477
 - applying to interfaces 496–497
 - entry order 496
 - implicit deny statement 495
- ACLs (access control lists) 428, 443, 477, 480–483.
 - See also* advanced ACLs
 - ACEs 477
 - entry order 496
 - implicit deny statement 495
 - applying to interfaces 496, 497, 501
 - assigning to vtys 445
 - Cisco PIX Firewall configuration 824–826
 - configuring 498
 - crypto 477
 - functions of 477
 - implementing 478–479
 - defining 495
 - defining criteria 498–500
 - displaying information 514–515
 - IP, testing Layer 4 information 493
 - lock-and-key 506–507
 - configuring 484–487
 - logging 494–495, 511–512
 - named extended IP ACLs
 - configuring 482
 - creating 503
 - time range function 483–484
 - named MAC extended IP ACLs,
 - configuring 482
 - named standard IP ACLs
 - configuring 482
 - creating 503
 - numbered extended IP ACLs
 - configuring 481
 - creating 502, 503
 - numbered standard IP ACLs
 - configuring 481
 - creating 502
 - port, configuring 490, 491
 - reflexive 507–511
 - configuring 488–489
 - router configuration 490
 - size limitations 517–518
 - time range function
 - implementing 504–506
 - troubleshooting 516–517
 - TurboACL, configuring on PIX Firewall 6.2 850
 - unsupported features on
 - Catalyst 3550 switch 518
 - VLAN map entries
 - creating 513
 - removing 514
- ACS, password recovery 1011
- active routers (HSRP) 527
- active state (EIGRP) 250
- ActiveX objects, filtering 827
- address mapping, configuring on Frame Relay 105–108
- address translation, xlates 814
- addressing, IS-IS 333
 - NSAP format 333–334
 - requirements 334–335
- adjacencies 328
 - configuring on IS-IS 324–325
- adjusting MTU packet size 526
- administrative distance 398
 - configuring on OSPF networks 300–301
- advanced ACLs 482–483
 - defining 495
 - lock-and-key, configuring 484–487, 506–507
 - logging 494–495
 - port ACLs, configuring 490–491

- reflexive, configuring 488–489, 507–511
 - router ACLs
 - configuring 490
 - VLAN maps 491–492
 - size limitations 517–518
 - advanced RIP configuration 233–235
 - advanced security features, practice lab 926–931
 - advanced VPN configuration 718–719
 - EIGRP 720–724
 - GRE tunnels 720
 - loopback interfaces 720
 - advanced VPN implementation 715
 - DMVPN 732–735
 - configuring on hub router 736–738
 - configuring on spokes 739–740
 - IPSec profiles, configuring 735–736
 - verifying configuration 741–745
 - IPSec VPNs 715
 - DMVPNs 716–718
 - GREs 716
 - advertising, default routes 209
 - AES (Advanced Encryption Standard) 637
 - aggressive mode (IKE phase 1) 642
 - AH (authentication header) 428, 634
 - application inspection, configuring on PIX Firewall 835–836
 - applying
 - ACLs to interfaces 496–497, 501
 - patches to Windows 975
 - applying patches to Solaris 958
 - area authentication, IS-IS configuration 342
 - areas
 - configuring on OSPF networks 290–292
 - NSSA, configuring on OSPF networks 292
 - assigning
 - dialer lists to interface 145
 - IP address to PIX Firewall 817–818
 - IS-IS to an interface 325–327
 - privilege levels to Cisco IOS user accounts 447–448
 - ATM (asynchronous transfer mode)
 - cell headers 183–184
 - multiprotocol encapsulation over AAL5, configuring 185–191
 - RFC 2225 implementation
 - classical IP with PVC 192–193
 - classical IP with SVCs 193–194
 - configuring 191–193
 - attacks 436
 - DoS
 - preventing with CAR 879–880
 - preventing with RPF 880, 886
 - IP spoofing 831
 - audit trails 428
 - auditing, enabling in Windows 976
 - authentication 428
 - AH 634
 - EIGRP routing updates 263–264
 - IKE phase 1 641–642
 - IKE phase 2 642–643
 - IS-IS
 - configuring 340–345
 - troubleshooting 345
 - PPP authentication, ISDN configuration 161–164
 - PPP multilink, ISDN configuration 165–166
 - RIP 216–218
 - unidirectional PPP authentication, ISDN configuration 164
 - authentication proxy on TACACS+ 610–615
 - configuring 615–617
 - authorization 429
 - Auto Update support, configuring on PIX Firewall 6.2 852–853
 - automatic metric translations 398
 - autonomous systems 351
 - confederations, configuring 372–377
 - configuring BGP through a firewall with prepend 386–393
 - private, configuring 377–385
 - single-homed, configuring 354–363
 - transit, configuring 363–372
 - autosense feature(LMI) 95
 - availability 428
-
- ## B
- B channel 134
 - backup interfaces, ISDN configuration 158–159
 - banners (motd), changing 965
 - basic ACLs 480
 - extended IP ACLs, configuring 481
 - named extended ACLs, configuring 482
 - named MAC extended ACLs, configuring 482
 - named standard ACLs, configuring 482

- numbered standard IP ACLs, configuring 481
- basic OSPF configuration, case study 279–281
 - administrative distance 300–301
 - area configuration 290–292
 - blocking LSA flooding 304–305
 - configuring interface parameters 282–283
 - creating virtual links 295–297
 - demand circuits 302
 - DNS lookup 298
 - generating default routes 298
 - ignoring MOSPF LSAs 305
 - logging neighbor adjacency changes 303
 - loopback interfaces 298
 - nonbroadcast network configuration 288–289
 - NSSA configuration 292
 - point-to-multipoint broadcast configuration 287–288
 - point-to-multipoint nonbroadcast 284–285
 - route calculation timers 301
 - route summarization 294–295
 - simplex interfaces 301
 - VLSM support 285
- Bc (committed burst) 96
- Be (excess burst) 96
- BECN (backward explicit congestion notification) 97
- BGP (Border Gateway Protocol) 352
 - autonomous systems 351
 - configuring 353
 - configuring through a firewall with AS prepend 386–393
 - path determination 352
 - updates 353
- bgp log-neighbor changes command 357
- bidirectional end-to-end keepalives 101
- Bidirectional NAT, configuring on PIX Firewall 6.2 846–847
- bits 97
- black hats 432
- blocking
 - LSA flooding 304–305
 - LSP flooding on interfaces 335
 - RIP updates on interfaces 207
- BOOTP server, disabling 453
- break sequences, simulating 1013
- BRI (basic rate interface) 134
 - PPP, configuring 160–161
- broadcast queues, configuring on Frame Relay 119
- buffer overflow 963

C

- C2 security policy, Windows compliance 969
- calculating
 - EIGRP composite metric 247
 - Frame Relay MaxR 97
- call setup and teardown, ISDN 138
- CAR (committed access rate)
 - configuring 882–883
 - policies, configuring 884–885
 - preventing DoS attacks 879–880
- CAs (certificate authorities) 639, 429
 - configuring 695–696
 - on PIX-to-PIX VPNs 703–710
 - IKE phase 1 696–703
- Catalyst 3350 switches 467
 - 802.1Q tunneling 881
 - port blocking, configuring 468
 - port security, configuring 469–470
 - port-based traffic control, verifying 470–472
 - protected ports, configuring 468
 - storm control, configuring 467
 - unsupported IOS ACL-related features 518
- CatOS 434–435
- CBAC (content-based access control)
 - configuring 786–798
 - configuring on two interfaces 803–805
 - debugging 798–799
 - disabling 802
 - DoS attack detection error messages 800
 - FTP error messages 801
 - functionality 784–785
 - intrusion detection 783
 - Java-blocking error messages 801
 - limitations of 783–784
 - PAM 806–808
 - configuring 808–810
 - SMTTP attack detection error messages 800–801
 - syslog messages, interpreting 799
 - traffic filtering 781–782
 - traffic inspection 782
 - with IPSec 791
- CC (Common Criteria) certification, Windows 2000 969

- CCIE exam 5–6
 - developing good study habits 15–18
 - lab exam 9–10
 - lab experience versus real-world experience 18–19
 - preparing for 13–14
 - topics covered 6–9
- CDP, disabling 452
- CEF (Cisco Express Forwarding), enabling 886
- cell headers, ATM 183–184
- certifications, CCIE Security exam 5, 6
 - lab exam 9–10
 - topics covered 6–9
- CHAP (Challenge Handshake Authentication Protocol) 161
- cipher 429
- CIR (committed information rate) 96
- Cisco IDS 859–860
 - configuring 867–870
 - sensors, password recovery 1008–1009
- Cisco IOS Firewall
 - firewalls, creating 776
 - PAM 806–808
 - configuring 808–810
- Cisco IOS Software 433
 - access lists 443
 - FTP administration 449
 - HTTP administration 442
 - limiting connection time 445
 - MNLB Forwarding Agent, configuring 535–537
 - NTP 441
 - configuring 458–463
 - password management 442
 - assigning privileges 447–448
 - creating user accounts 446–447
 - enable password 442
 - line passwords 443
 - privilege levels 442
 - remote access, configuring 446
 - services
 - BOOTP server 453
 - CDP 452
 - finger server 453
 - ICMP messaging 454–455
 - IP source routing 454
 - IP-directed broadcast 454
 - NTP 453
 - Proxy ARP 453
 - router name and DNS resolution 451
 - TCP and UDP small servers 452
 - verifying deactivation 455–456
 - software configuration register, password recovery 995–1003
 - SSH 443
 - configuring 464–466
 - TCP intercept
 - configuring 776–781
 - Telnet addresses, hiding 449
 - user accounts, verifying with AAA 449–451
 - vtys, configuring 445–446
- Cisco PIX Firewalls 860–861
 - ACLs, configuring 824–826
 - ActiveX objects, filtering 827
 - application inspection, configuring 835–836
 - Auto Update support, configuring 852–853
 - Bidirectional NAT, configuring 846–847
 - Configurable Proxy Pinging 834
 - configuring 815, 870–874
 - DHCP server configuration 844–846
 - Flood Guard 832
 - idle timers, configuring 836–837
 - IDS signatures 861–867
 - configuring 842–844
 - inbound connections, resetting 832–833
 - interface MTU, configuring 816–817
 - IP address, configuring 817–818
 - IP spoofing attacks, preventing 831–832
 - Java applets, filtering 828
 - logging, configuring 838–840
 - NAT, configuring 818–819
 - NTP, configuring 851
 - options, configuring 837–838
 - password recovery 1010–1011
 - security levels 813
 - configuring 815
 - SMR, configuring 847–850
 - SNMP functions, configuring 841–842
 - static NAT, configuring 820–822
 - static routes, configuring 822–823
 - TurboACL, configuring 850
 - URLs, filtering 828–831
 - xlates 814
- classful routing protocols 398
- classical IP, implementing
 - with PVCs 192–193
 - with SVCs 193–194
- clearing IP accounting database 557

- combining share permissions and NTFS permissions 980
- commands
 - access-list 756
 - bgp log-neighbor changes 357
 - debug dialer events 174
 - debug frame-relay lmi 125–126
 - debug isdn events 174–175
 - debug isdn q931 177–178
 - debug ppp authentication 176–177
 - debug ppp multilink 175–176
 - debug vtemplate 760
 - service resetinbound 833
 - show dialer 172–173
 - show frame-relay map 125
 - show frame-relay pvc 123–125
 - show interfaces bri 0/0 169–171
 - show ip accounting 548
 - show ip nhrp 745
 - show isdn active 173
 - show isdn status 171–172
 - show ppp multilink 173
 - show route 823
 - show vpdn tunnel 760
 - sysopt connection 837
 - username password 756
 - virtual template 764
 - vpdn-template 769
- commenting out network services 959–960
- conditions 545
- confederations, BGP configuration 372–377
- confidentiality 428–429
- config-register command, password recovery 999–1002
- Configurable Proxy Pinging 834
- configuration files, renaming 1003–1004
- configuring
 - AAA 448–449, 569–581
 - on PIX Firewall 581–593
 - ACLs 498–501
 - logging 494–495, 511–512
 - time range function 483–484
 - advanced security features, practice lab 926–931
 - advanced VPNs 718–719
 - EIGRP 720–724
 - GRE tunnels 720
 - loopback interfaces 720
 - ATM
 - multiprotocol encapsulation over AAL5 185–191
 - RFC 2225 191–194
 - authentication proxy 615–617
 - basic security, practice lab 917–920
 - BGP 353
 - confederations 372–377
 - private autonomous systems 377–385
 - single-homed autonomous systems 354–363
 - through a firewall with AS prepend 386–393
 - transit autonomous systems 363–372
 - CAs 695–696
 - Catalyst 3550 switches
 - port blocking 468
 - port security 469–470
 - protected ports 468
 - storm control 467
 - CBAC 786–798
 - on two interfaces 803–805
 - Cisco IDS 867–870
 - Cisco PIX Firewall 815, 870–874
 - ACLs 824–826
 - ActiveX object filters 827
 - as DHCP server 844–846
 - Flood Guard 832
 - idle timers 836–837
 - IDS signatures 842–844
 - interface MTU 816–817
 - IP address 817–818
 - IP spoofing prevention 831–832
 - Java applet filters 828
 - logging 838–840
 - NAT 818–819
 - options 837–838
 - resetting inbound connections 832–833
 - security levels 815
 - SNMP functions 841–842
 - static NAT 820–822
 - static routes 822–823
 - URL filters 828–831
 - Cisco PIX Firewall 6.2
 - Auto Update support 852–853
 - Bidirectional NAT 846–847
 - NTP 851
 - SMR 847–850

- TurboACL 850
- DDR 144
 - assigning dialer-list to interface 145
 - dialer profiles 147–149
 - legacy DDR 146–147
 - specifying interesting traffic 144
- dial backup, practice lab 915–917
- DMVPN 732–735
 - IPSec profiles 735–736
 - on hub router 736–738
 - on spokes 739–740
 - verifying configuration 741–745
- DRP Server Agent 540–541
- EIGRP 241–243, 253
 - default routing 259–261
 - distribute lists 261–262
 - manual route summarization 258–259
 - over GRE tunnels 266–269
 - route authentication 263–264
 - stub routing 264–265
 - WAN connections 254–255
- extended ACLs 481
- Frame Relay 102
 - address mapping 105–108
 - broadcast queues 119
 - encapsulation 103–05
 - LMI 108–109
 - SVCs 109–113
 - TCP/IP header compression 121–122
 - traffic shaping 114–119
- Frame Relay switch, practice lab 904–905
- HSRP 541, 542–547
- HTTP servers 456–457
- ICMP redirects 539
- IOS-to-IOS VPNs with IKE phase 1 using CA 696–703
- IP accounting 548
- IPSec VPNs 724, 725, 726, 727
 - between two IOS routers 644–662
 - between two PIX firewalls 671–693
 - verifying configuration 728–732
- ISDN 142
 - backup interfaces 158–159
 - encapsulation 160
 - floating static routes 152–154
 - interfaces 158
 - ISDN callback 166–168
 - OSPF demand circuits 155–157
 - passive interfaces 151–152
 - PPP authentication 161–164
 - PPP multilink 165–166
 - SPIDs 143–144
 - static routing 149–151
 - switch type 142–143
 - unidirectional PPP authentication 164
- IS-IS
 - authentication 340–345
 - default routes 337
 - hello timer 339
 - IP 322–327
 - retransmission interval 339
 - route redistribution 337–338
- ISP services
 - rate limiting 882–885
 - RPF 886
- L2VPN
 - on router 887
 - on switches 889–890
 - trunk ports 890–891
 - verifying configuration 891–894
- lock-and-key ACLs 484–487, 506–507
- MAC address accounting 530
- mesh groups 336
- named extended ACLs 482
- named extended IP ACLs 503
- named MAC extended ACLs 482, 512–513
- named standard ACLs 482
- named standard IP ACLs 503
- NAT 549–50, 554–555
 - dynamic translation 550–551
 - overlapping addresses 552–553
 - overloading 551
 - TCP load distribution 553–554
- NTP 458–459, 460–463
- numbered extended IP ACLs 502–503
- numbered standard IP ACLs 502
- OSPF 278–281
 - ABR Type 3 LSA filtering 310–311
 - ABR Type 3 LSAs 310–311
 - administrative distance 300–301
 - areas 290–292
 - default routes 298
 - DNS lookup 298
 - external route summarization 308
 - GRE tunnels 312–314
 - inter-area route summarization 306–308

- interface parameters 282–283
- loopback interfaces 298
- LSA flood blocking 304–305
- nonbroadcast networks 288–289
- NSSAs 292
- on simplex interfaces 301
- over demand circuits 302
- point-to-multipoint broadcast 287–288
- point-to-multipoint nonbroadcast 284–285
- route calculation timers 301
- route summarization 294–295, 306
- virtual links 295–297
- VLSM support 285
- PAM 808–810
- passwords 444
- PIX Firewall, remote-access VPNs 593–608
- PIX2, PPTP 766–768
- PIX-to-PIX VPNs with IKE phase 1 using CA 703–710
- port ACLs 490
 - VLAN maps 491
- PPP 160–161
- precedence accounting 531
- redistribution 399–401
 - between directly connected networks 413–415
 - between EIGRP and IGRP autonomous systems 409–412
 - between EIGRP autonomous systems 408–409
 - between OSPF and RIPv1 407–408
 - between static routes into EIGRP 412–413
 - into OSPF 402
 - NSSAs into BGP 405–407
 - OSPF into BGP 402–405
 - practice lab 915–917
- reflexive ACLs 488–489, 507–511
- remote access on Cisco IOS Software 446
- remote FTP administration 449
- RIP 203
 - advanced techniques 233–235
 - authentication 216–218
 - blocking RIP updates on interfaces 207
 - default route advertisement 209
 - initial setup 204–206
 - over router to PIX 5.2 connection 221–225
 - over router to PIX 6.2 connection with authentication 225–231
 - route filtering 208
 - route summarization 212–215
 - specifying version 210–211
 - troubleshooting 218–220
- router ACLs 490
- SSH 464–466
- standard ACLs 481
- TACACS+
 - PPP callback 621–627
 - privilege levels 617–621
- TCP intercept 776–781
- TCP performance parameters 531
 - connection attempt time 533
 - header compression 532
 - maximum read size 534
 - maximum window 535
 - Path MTU Discovery 533
 - selective acknowledgment 534
 - time stamps 534
- VPDNs 752
 - default group template 768–769
 - TACACS+ 761–765
 - with local AAA 752–761
 - vtys 445–446
- confreg command, password recovery 999–1002
- congestion control mechanisms, Frame Relay 96–97
- DE 98
- DLCI priority levels 98
- end-to-end keepalives 100–101
- error checking 99
- ForeSight 99–100
- notification methods 100
- connected networks, redistribution into OSPF 402
- connection time (Cisco IOS), limiting 445
- controlling EIGRP routes 261–262
- CPE (customer premises equipment) 134–135
- creating
 - Cisco IOS user accounts 446–447
 - customized firewalls 776
 - VLAN map entries 513
- creating baseline security level in Windows operating systems 972–975
- crypto access lists 477
 - functions of 477
 - implementing 478–479
- cryptography 429

D

- D channel 134
- DAC (Discretionary Access Control) 969
- data link layer (OSI), ISDN operation 137
- DCEs (data circuit-terminating equipment) 85
- DDR (Dial On-Demand Routing) 141
 - configuring 144
 - dialer lists 141
 - assigning to interface 145
 - dialer profiles, configuring 146–149
 - interesting traffic, configuring 144
 - legacy DDR, configuring 142, 146–147
- DE (discard eligibility) bit 96–98
- debug dialer events command 174
- debug frame-relay lmi command 125–126
- debug isdn events command 174–175
- debug isdn q931 command 177–178
- debug ppp authentication command 176–177
- debug ppp multilink command 175–176
- debug vtemplate command 760
- debugging
 - CBAC 798–799
 - EIGRP in production environment 271
 - IS-IS 346–348
- decision process, IS-IS state machine 331
- default group templates, VPDN configuration 768–769
- default routes 203
 - advertising 209
 - configuring 337
 - EIGRP 259–261
 - generating on OSPF networks 298
- default umask setting, modifying 964
- defining ACLs 495
 - ACE entry order 496
 - implicit deny statement 495
- deleting VLAN map entries 514
- DES (Data Encryption Standard) 429, 636
- desktop operating systems, Windows 969
- devices
 - CPE 134, 135
 - Frame Relay
 - DTEs 85
 - FRADs, handshake sequence 92
 - required equipment for home-based study labs 24–25
 - resetting for password recovery 1005–1006
- DH (Diffie-Hellman) 429, 638
- DHCP servers, configuring on PIX Firewall 844–846
- dial backup practice lab 915–917
- dialer lists 141
 - assigning to interface 145
 - dialer-group-number 145
- dialer maps, configuring legacy DDR 146
- dialer profiles, configuring 146–149
- dialer-group-number 145
- dialup, VPDNs 749–751
 - configuring 752–765
 - default group templates, configuring 768–769
- digital certificates 430, 639
- digital channels (ISDN) 134
- digital signatures 430
- directly connected networks, redistribution between 413–415
- DIS (Designated IS) 327
 - election process 331–332
- disabling
 - CBAC 802
 - EIGRP route summarization 256–258
 - EIGRP split horizon 269
 - IDENT services 832–833
 - routing on Solaris systems 965
 - services
 - BOOTP server 453
 - DCP 452
 - finger server 453
 - ICMP messaging 454–455
 - IP source routing 454
 - IP-directed broadcast 454
 - NTP 453
 - Proxy ARP 453
 - router name and DNS resolution 451
 - TCP and UDP small servers 452
 - startup scripts 961
 - Stop-A abort sequence 965
- displaying
 - ACL information 514–515
 - resource usage 515
 - active accounting database 548
 - EIGRP topology table information 248–249
 - IP statistics 556–557
 - OSPF routing process information 315
 - OSPF statistics 315–316

- OSPF update packet pacing 317
- distribute lists, controlling EIGRP routes 261–262
- DLCI (Data-Link Connection Identifier) 84
 - priority levels 98
- DMVPNs 716–718
 - configuring 732–735
 - IPSec profiles 735–736
 - on hub router 736–738
 - on spokes 739–740
 - verifying configuration 741–745
- DNS lookup, configuring on OSPF networks 298
- domain authentication, IS-IS configuration 343–344
- “don't care” masks 481
- DoS attacks 436
 - half-open sessions 788
 - preventing
 - with CAR 879–885
 - with RPF 880, 886
- DRP (Director Response Protocol)
 - Server Agents 527
 - configuring 540–541
- DTEs (data terminal equipment) 85
- DUAL 240, 251–252
- Dynamic NHRP 717
- dynamic PVCs, configuring 189–190
- dynamic routing
 - ISDN 152–154
 - over IPSec VPNs 718–724
 - configuring IPSec parameters 724–727
 - verifying configuration 728–732

E

- EBGP (external BGP) 352
- EEPROM, passwords 966
- egress filtering 831
- EIGRP (Enhanced IGRP) 240
 - composite metric, calculating 247
 - configuring 241–243, 253, 720–724
 - controlling routes 261–262
 - default routing, configuring 259–261
 - DUAL 251–252
 - feasible successors 250
 - features 240
 - IGRP interoperability 251
 - manual route summarization, configuring 258–259

- neighbor table 244–246
 - adjacencies, logging 255
- “not on common subnet” error message 245
- over GRE tunnels, configuring 266–269
- packet format 243
- redistribution
 - between autonomous systems 408–409
 - into IGRP autonomous system 409–412
 - into static routes 412–413
- route authentication, configuring 263–264
- route states 250
- route summarization, disabling 256–258
- route tagging 251
- split horizon, disabling 269
- stub routing, configuring 264–265
- topology table 246–247
 - displaying information 248–249
 - troubleshooting 270–272
 - WAN connections, configuring 254–255
- election process of DIS 331–332
- enable password 442
- enabling
 - logging 962
 - OSPF 280–281
- encapsulation
 - configuring on Frame Relay 103–105
 - ISDN options 160
- encryption
 - AES 637
 - DH 638
 - RSA 639
- end-to-end keepalives 100–101
- enhanced distance vector protocols , BGP 352
 - configuring 353
 - path determination 352
 - updates 353
- entry order (ACEs) 496
- equipment list for routing practice lab 911
- error checking, CRC 99
- error codes, ISDN 983–992
- ESP (Encapsulating Security Payload) 430, 635–636
- Ethernet, simplex interfaces 527
- event logs, enabling in Windows 976
- event window 100
- exacting 643
- exploits, buffer overflow 963

- extended ACLs
 - configuring 481
 - named MAC extended, configuring 512–513
- extensions for LMI 92
- external route tags, EIGRP 251
- external routes
 - OSPF 278
 - summarization, configuring 308
- extranet VPNs 435

F

- FAT 977
- FAT32 977
- feasible successors (EIGRP) 250
- features of EIGRP 240
- FECN (forward explicit congestion notification) 97
- fields
 - of EIGRP neighbor table 245
 - of Frame Relay frames 84
 - of Frame Relay LMI frames 92–93
- file and directory auditing, enabling in Windows 976
- file systems
 - FAT 977
 - FAT32 977
 - NTFS 977–978
 - permissions 978–980
 - share-level security 980
- files, world-writeable 966
- filtering
 - ActiveX objects 827
 - Java applets 828
 - OSPF ABR Type 3 LSA filtering, verifying 316
 - OSPF ABR Type 3 LSAs 310–311
 - routing information 416–421
 - to OSPF neighbors, configuring 311
 - URLs 828–831
- finger server, disabling 453
- firewalls
 - Cisco PIX Firewall IDS 860–861
 - configuring 870–874
 - signatures 861–867
 - creating with Cisco IOS Firewall feature set 776
 - PIX Firewall
 - application inspection 835–836
 - Auto Update support 852–853
 - Bidirectional NAT 846–847
 - Configurable Proxy Pinging 834
 - configuring 815–826
 - DHCP server configuration 844–846
 - filtering ActiveX objects 827
 - filtering Java Applets 828
 - filtering URLs 828–831
 - Flood Guard 832
 - idle timers 836–837
 - IDS signatures, configuring 842–844
 - IP spoofing attacks, preventing 831–832
 - logging, configuring 838–840
 - NTP 851
 - options, configuring 837–838
 - resetting inbound connections 832–833
 - security levels 813
 - SMR 847–850
 - SNMP, configuring 841–842
 - TurboACL 850
 - xlates 814
- fixup, configuring on PIX Firewall 835–836
- flapping routes, resolving 157
- floating static routes, ISDN 152–154
- Flood Guard 832
- flooding 328
 - blocking on IS-IS interfaces 335
 - mesh groups, configuring 336
- ForeSight 99–100
- format
 - of EIGRP packets 243
 - of NSAP addresses 333–334
 - of practice labs 901–902
- forward process, IS-IS state machine 331
- FRADs, handshake sequence 92
- fragmentation, IP Path MTU Discovery 525
- Frame Relay
 - address mapping 105–108
 - broadcast queues, configuring 119
 - configuring 102
 - congestion control mechanisms 96–97
 - DE 98
 - DLCI priority levels 98
 - end-to-end keepalives 100–101
 - error checking 99
 - ForeSight 99–100
 - notification methods 100
 - connectivity, troubleshooting 122–126
 - DCEs 85
 - DTEs 85

- encapsulation, configuring 103–105
- frame fields 84
- fully meshed topologies 87
- LMI 91
 - autosense feature 95
 - configuring 108–109
 - frame format 92–93
 - timers 94–95
- NNI 95–96
- partially meshed topologies 87
 - subinterfaces 88–89
- PVCs 91
- signaling 91–92
- star topologies 86
- SVCs 90
 - configuring 109–113
- TCP/IP header compression 121–122
- traffic shaping, configuring 114–119
- FTP (file transfer protocol)
 - remote administration 449
 - services 960
- fully meshed topologies, Frame Relay 87
- functional groups 134–135
 - reference points 135
- functionality
 - of CBAC 784–785
 - of IPSec 640

G

- gray hats 432
- GRE (generic routing encapsulation) 716
 - configuring between OSPF and non-IP networks 312–314
 - implementing on EIGRP 266–269
 - tunnels, configuring 720
- group pacing 303–304

H

- half-open sessions 788
- handshake sequence on FRADs 92
- hello interval (IS-IS), configuring 339
- hello packets, EIGRP 243
- Hfnetchk 971
- hiding Telnet addresses 449

- HMAC (Hashed-based Message Authentication Code) 430
- home-based study labs 22
 - planning 23–25
- hop count 202
- hot fixes, Windows resources 971
- HSRP (Hot Standby Router Protocol) 527
 - and ICMP redirects 528–530
 - configuring 541–547
 - verifying support for MPLS VPNs 556
- HTTP administration 442
 - server configuration 456–457
- Hybrid CatOS 434

I

- IBGP (interior BGP) 352
- ICMP (Internet Control Message Protocol)
 - disabling 454–455
 - mask reply messages 525
 - redirects 524
 - and HSRP 528–530
 - configuring 539
 - unreachables 524
- IDENT services, disabling 832–833
- idle timers, configuring on PIX Firewall 836–837
- IDSs (intrusion detection systems) 436
 - signatures 842
 - configuring on PIX Firewall 842, 843, 844
- IEEE 802.1Q tunneling 881
- ignoring MOSPF LSAs 305
- IGRP (Interior Gateway Routing Protocol), EIGRP
 - interoperability 251
- IIS Lockdown Wizard 971
- IIS logs, enabling in Windows 976
- IKE (Internet Key Exchange) 430, 637, 638
 - aggressive mode 642
 - phase 1 using CA
 - configuring on IOS-to-IOS VPNs 696–703
 - configuring on PIX to-PIX VPNs 703–710
 - phase 2 642–643
- implementing
 - access lists 478–479
 - advanced VPNs
 - DMVPNs 716–718
 - GREs 716

- IPSec VPNs 715
 - GRE tunnels on EIGRP 266–269
 - NAT 538
 - physical security 967
 - time range function on ACLs 504–506
- implicit deny statement (ACEs) 495
- inbound connections, resetting through Cisco PIX Firewall 832–833
- information 742
- information security policies 430
- ingress filtering 831
- inside address, identifying on Cisco PIX Firewall with NAT 818
- installing
 - Solaris 958
 - Windows 970
- integrity 427, 430
- inter-area route summarization, configuring 306–308
- interesting traffic 141
 - defining 641
 - dialer lists 141
 - specifying for DDR configuration 144
- interfaces
 - Cisco PIX Firewallm, security levels 813
 - ISDN configuration 158
- internal OSPF routing table entries, displaying 315
- interoperability of EIGRP and IGRP 251
- interpreting CBAC syslog messages 799
- intranet VPNs 435
- intrusion detection
 - CBAC 783
 - Cisco IDS, configuring 867–870
 - Cisco IOS software IDS 859–860
 - Cisco PIX Firewall IDS 860–861
 - configuring 870–874
 - signatures 861–867
- IOS. *See* Cisco IOS Software
- IOS-to-IOS VPNs, IKE phase 1 using CA 696–703
- IP, IS-IS configuration 322, 324
 - interface assignment 325–327
 - levels 324–325
- IP accounting
 - clearing database 557
 - configuring 548
 - MAC accounting 530
 - precedence accounting 531
- IP addresses, configuring on PIX Firewall interfaces 817–818
- IP Path MTU Discovery 525
- IP source routing 526
 - disabling 454
- IP spoofing attacks 831
- IP-directed broadcast, disabling 454
- IPSec 431
 - 3DES 636
 - AES 637
 - AH 634
 - CAs, configuring 695–696
 - defining interest traffic 641
 - DES 636
 - DH 638
 - encrypted tunnels 643
 - ESP 635, 636
 - functionality 640
 - IKE 637, 638
 - IKE phase 1 641–642
 - IKE phase 2 642–643
 - MD5 638
 - preshared keys 638
 - RSA signatures 638
 - SHA-1 638
 - transport mode 640
 - tunnel mode 640
 - tunnel termination 643
 - VPNs 718–724
 - configuring between IOS routers 644–662, 696–703
 - configuring between two PIX firewalls 671–693, 703–710
 - DMVPNs 716–718
 - GREs 716
 - implementing 715
 - parameters, configuring 724–727
 - PIX-to-PIX, troubleshooting 687–695
 - troubleshooting 662–670
 - verifying configuration 728,–732
- ISDN
 - backup interface configuration 158–159
 - call stages 138
 - configuring 142
 - CPE 134–135
 - data link layer 137
 - DDR, configuring 144–149

- digital channels 134
- encapsulation options 160
- error codes 983–992
- interface configuration 158
- ISDN callback, configuring 166–168
- network layer 138
- physical layer 136
- PPP 139
 - authentication 161–164
 - configuring 160–161
 - LCP 139–140
 - NCP 140
 - PPP multilink 165–166
- reference points 135
- routing
 - floating static routes 152–154
 - OSPF demand circuits 155–157
 - passive interface 151–152
 - static routes 149–151
- SPIDs, configuring 143–144
- standards support 133–134
- switch type, configuring 142–143
- troubleshooting 169–177

IS-IS

- addressing 333
 - NSAP foramt 333–334
 - requirements 334–335
- authentication
 - configuring 340–345
 - troubleshooting 345
- debugging 346, 348
- default routes, configuring 337
- DIS 327
- hello timer, adjusting 339
- IP configuration 322–324
 - interface assignment 325–327
 - levels 324–325
- LSPs 328–330
 - blocking flooding on interfaces 335
 - mesh groups, configuring 336
- monitoring 346
- PSNs 331–332
- retransmission interval, adjusting 339
- route redistribution, configuring 337–338
- state machine 330–331

ISOs (information security officers) 432

ISP services

- rate limiting 882– 885
- RPF 886

J

- Java applets, filtering 828
- jumper settings
 - changing with software 1007–1008
 - manually shorting 1006

K-L

- keeralives, event window 100

L2 tunneling protocols, PPTP 751

L2F (Layer 2 Forwarding) 749

L2TP (Layer 2 Tunneling Protocol), LNS 749

L2VPNs

- 802.1Q 881
- configuring 887–891
- verifying configuration 891–894

LAN storms 467

LAPD (Link Access Procedure on the D channel) 137

Layer 2 protocol tunneling 881

Layer 4, matching rules for IP ACLs 493

LCP (Link Control Protocol) 139–140

legacy DDR 142

- configuring 146–147

levels, configuring for IS-IS 324, 325

limitations

- of ACL size 517–518
- of CBAC 783–784

limiting Cisco IOS connection time 445

line passwords, Cisco IOS password management 443

link flapping, resolving 157

link-state protocols

- IS-IS
 - addressing 333–335
 - authentication 340–345
 - debugging 346–348
 - default routes, configuring 337
 - DIS 327
 - hello timer, adjusting 339
 - IP configuration 322–327
 - LSPs 328–330, 335–336

- monitoring 346
- PSNs 331–332
- retransmission interval, adjusting 339
- route redistribution, configuring 337–338
- state machine 330–331
- OSPF
 - administrative distance, configuring 300–301
 - areas, configuring 290–292
 - blocking LSA flooding 304–305
 - configuring 278–281
 - configuring on simplex interfaces 301
 - creating virtual links 295–297
 - default route generation 298
 - demand circuits 302
 - DNS lookup 298
 - ignoring MOSPF LSAs 305
 - interface parameters, configuring 282–283
 - logging neighbor adjacency changes 303
 - loopback interfaces 298
 - nonbroadcast configuration 288–289
 - NSSA configuration 292
 - point-to-multipoint broadcast
 - configuration 287–288
 - point-to-multipoint nonbroadcast
 - configuration 284–285
 - route calculation timers 301
 - route summarization 294–295, 306–308
 - VLSM support 285
- LMI (Local Management Interface) 91–92
 - autosense feature 95
 - configuring on Frame Relay 108–109
 - frame format 92–93
 - timers 94–95
- LNS (L2TP network server) 749
- lock-and-key ACLs
 - configuring 484–487, 506–507
 - source-address spoofing 485
- locking user accounts 965
- logging
 - ACLs 494–495, 511–512
 - configuring on PIX Firewall 838–840
 - EIGRP neighbor adjacency changes 255
 - enabling 962
 - on Windows 976
 - OSPF neighbor adjacency changes 303
- loopback interfaces, configuring 720
 - on OSPF networks 298

- lost passwords, recovering 995–1008
- LSAs
 - flood blocking 304–305
 - group pacing, configuring 303–304
- OSPF
 - ABR Type 3, configuring 311
 - type codes 278
 - packet pacing, displaying 317
- LSPs 328–330
 - blocking flooding on interfaces 335
 - flooding 328
 - mesh groups 336

M

- MAC address accounting 530
- manual route summarization, EIGRP configuration 258–259
- manually shorting jumper settings 1006
- mask reply messages (ICMP) 525
- masquerading 431
- master lab 933
 - prestaging 934–940
 - timed portion 942–951
 - versus CCIE Security Lab exam 902–903
- matching rules for testing Layer 4 information on IP ACLs 493
- MaxR, calculating 97
- MBSA (Microsoft Baseline Security Analyzer) 971
- MD5 638
- MD5 (Message Digest 5) 431
- mesh groups, configuring 336
- messages (ICMP)
 - mask reply 525
 - redirects 524
 - unreachables 524
- metrics 397
 - EIGRP composite metric, calculating 247
 - RIP 202
- MLP (Multilink PPP), configuring 165–166
- MNLB (MultiNode Load Balancing) Forwarding Agent
 - configuring 535–537
 - monitoring 558
- modifying
 - default umask setting 964
 - motd file 965

- monitoring
 - ISDN 169–177
 - IS-IS 346
 - MNLB Forwarding Agent 558
 - NAT 559
 - PVCs 190–191
- motd file, modifying 965
- MPLS VPNs, verifying HSRP support 556
- MTU packet size
 - adjusting 526
 - configuring on PIX Firewall interfaces 816–817
- multihomed autonomous systems 351
- multipoint subinterfaces 89
- multiprotocol encapsulation over AAL5, ATM configuration 185–191

N

- named extended ACLs
 - configuring 482
 - time range function 483–484
- named extended IP ACLs, creating 503
- named MAC extended ACLs
 - configuring 482, 512–513
- named standard ACLs, configuring 482
- named standard IP ACLs, creating 503
- NAS (network access server) 749
- NAT (Network Address Translation) 537
 - Cisco PIX Firewall configuration 818–819
 - configuring 549–555
 - dynamic translation, configuring 550–551
 - implementing 538
 - monitoring 559
 - overlapping addresses, configuring 552–553
 - overloading, configuring 551
 - TCP load distribution, configuring 553–554
- Native CatOS 434
- NCP (Network Control Protocol) 139–140
- NCSC (National Computer Security Centre) C2 rating, Windows compliance 969
- neighbor adjacency changes, logging
 - EIGRP 255
 - OSPF 303
- neighbor table (EIGRP) 244–246
 - logging neighbor adjacency changes 255
- NETs (network entity titles) 323

- network layer (OSI), ISDN operation 138
- network services
 - FTP 960
 - NS 961
 - rlogin 960
 - RPC 961
 - stopping 959–960
- NFS services 961
- NHRP 717
- NNI (Network-to-Network Interface) 95
- NNI cell headers 183–184
- nonbroadcast OSPF configuration 288–290
- nonrepudiation 431
- “not on common subnet” error message 245
- notification methods for Frame Relay congestion control 100
- NSAP (network service access point) addresses 333
 - format 333–334
- NSSAs (not-so-stubby areas)
 - OSPF configuration 292
 - redistribution into BGP 405–407
- NT1 (Network Termination 1) 135
- NT2 (Network Termination 2) 135
- NTFS 977–978
 - permissions 978–980
 - share-level security 980
- NTP (Network Time Protocol) 441
 - configuring 458–463
 - configuring on PIX Firewall 6.2 851
 - disabling 453
- numbered extended ACLs, time range function 483–484
- numbered extended IP ACLs
 - creating 502–503
- numbered standard ACLs, configuring 481
- numbered standard IP ACLs, creating 502

O

- o/r command, password recovery 1002–1003
- obtaining equipment for home-based labs 24, 25
- on-demand circuits, OSPF configuration 302
- options, configuring on PIX Firewall 837, 838
- OSI (Open Systems Interconnection) model, ISDN operation
 - data link layer 137
 - network layer 138

physical layer 136

OSPF (Open Shortest Path First)

ABR Type 3 filtering, configuring 310–311

administrative distance, configuring 300–301

areas, configuring 290–292

configuring 278–281

default routes, generating 298

demand circuits, ISDN configuration 155–157

DNS lookup, configuring 298

external routes 278

GRE, configuring for non-IP traffic 312–314

interface parameters, configuring 282–283

loopback interfaces, configuring 298

LSA flood blocking, configuring 304–305

LSAs

group pacing 303–304

type codes 278

MOSPF LSAs, ignoring 305

neighbor adjacency changes, logging 303

nonbroadcast networks, configuring 288–289

NSSAs

configuring 292

redistribution into BGP 405–407

over demand circuits, configuring 302

point-to-multipoint broadcast, configuring
287–288

point-to-multipoint nonbroadcast, configuring
284–285

redistribution

into BGP 402–405

into RIPv1 407–408

route calculation timers, configuring 301

route summarization 306

configuring 294–295

external 308

inter-area 306–308

routing processes, displaying information 315

simplex interfaces, configuring 301

statistics, displaying 315–316

virtual links, creating 295–297

VLSM support, configuring 285

packet filtering

ACLs 477, 480–483

ACE entry order 496

ACEs 477

applying to interfaces 496, 497, 501

configuring 498

crypto 477

defining criteria 498–500

displaying information 514–515

extended ACLs 481

implementing 478–479

implicit deny statement 495

lock-and-key 484–487, 506–507

logging 494–495, 511–512

named extended ACLs 482

named MAC extended ACLs 482
512–513

named standard ACLs 482

numbered standard IP ACLs 481

port 490–491

reflexive 488–489, 507–511

router 490

size limitations 517, 518

time range function 483–484

time range function, implementing
504–506

troubleshooting 516–517

VLAN map entries, creating 513

unsupported features on Catalyst 3550
switch 518

packet pacing, displaying information 317

packets

EIGRP, format 243

IS-IS LSPs 328–330

LSAs, OSPF 278

NSAPs 333

format 333–334

PAM (Port-to-Application Mapping) 806–808

configuring 808–810

PAP 161

partially meshed topologies, Frame Relay 87
subinterfaces 88–89

passive routing, ISDN 151–152

passive state (EIGRP) 250

passive-reply end-to-end keepalives 101

password management (Cisco IOS) 442

enable password 442

line passwords 443

P

PAC (PPTP access concentrator) 751

- privilege levels 442
- password recovery 995–997
 - break sequence 997–1002
 - changing jumper settings with software 1007–1008
 - manually shorting jumper settings 1006
 - o/r command 1002, 1003
 - on ACS running Solaris 1011
 - on Cisco IDS sensors 1008–1009
 - on Cisco PIX Firewall 1010–1011
 - on VPN concentrators 1012–1013
 - renaming software 1003–1004
 - replacing software 1005
 - resetting devices 1005–1006
- passwords
 - configuring 444
 - EEPROM, configuring 966
- patches
 - applying to Solaris 958
 - applying to Windows 975
- path determination, BGP 352
- performance, TCP configuration 531–535
- permissions, NTFS 978–980
- physical layer (OSI), ISDN operation 136
- physical security, implementing 967
- PIX Firewall. *See also* PIX Firewall 6.2
 - AAA configuration 581–593
 - ACLs, configuring 824–826
 - ActiveX objects, filtering 827
 - application inspection, configuring 835–836
 - Configurable Proxy Pinging 834
 - configuring PIX-to-PIX IPSec VPNs 671–693, 815
 - DHCP server configuration 844, 845, 846
 - Flood Guard 832
 - idle timers, configuring 836–837
 - IDS signatures, configuring 842–844
 - inbound connections, resetting 832–833
 - interface MTU, configuring 816–817
 - IP address, configuring 817–818
 - IP spoofing attacks, preventing 831–832
 - Java applets, filtering 828
 - logging 838–840
 - NAT, configuring 818–819
 - options, configuring 837–838
 - PPTP, configuring 766–768
 - remote-access VPNs, configuring 593–608
 - security levels 813–815
 - SNMP functions, configuring 841, 842
 - static NAT, configuring 820, 822
 - static routes, configuring 822–823
 - troubleshooting PIX-to-PIX IPSec VPNs 687–695
 - URLs, filtering 828–831
 - xlates 814
- PIX Firewall 6.2
 - Auto Update support, configuring 852–853
 - Bidirectional NAT, configuring 846–847
 - NTP, configuring 851
 - SMR, configuring 847–850
 - TurboACL, configuring 850
- PIX-to-PIX VPNs, IKE phase 1 using CA 703–710
- PKI (Public Key Infrastructure) 431
- planning home-based labs 23–25
- point-to-multipoint broadcast OSPF configuration 287–288
- point-to-multipoint nonbroadcast OSPF configuration 284–285
- point-to-point subinterfaces 89
- port ACLs
 - configuring 490
 - VLAN maps, configuring 491
- port blocking, configuring on Catalyst 3550 switches 468
- port security, configuring on Catalyst 3550 switches 469–470
- port-based traffic control, verifying on Catalyst 3550 switches 470–472
- PPP (Point-to-Point Protocol) 139
 - configuring 160–161
 - LCP 139–140
 - NCP 140
- PPP authentication
 - ISDN configuration 161–164
 - unidirectional, ISDN configuration 164
- PPP callback
 - configuring with TACACS+ 621–627
- PPP multilink, configuring 165–166
- PPTP (Point-to-Point Tunneling Protocol) 751
 - configuring on PIX firewall 766, 767, 768
- practice labs
 - bulding layer 2
 - equipment list 903
 - prestaging 904–909
 - timed lab portion 909–911
 - configuring security

- advanced features 926–931
- basic features 917–920
- dial and application security 921–925
- format 901–902
- master lab 933
 - prestaging 934–940
 - timed portion 942–951
- protocol redistribution and dial backup
 - configuration 915–917
- routing 911
 - timed portion 913–914
- service provider 931–932
- precedence accounting 531
- preparing for CCIE exam 13–14
 - developing good study habits 15–18
 - lab experience versus real-world experience 18–19
- preparing for lab exam
 - home-based study labs 22
 - planning 23–25
 - remote study labs 23
 - work-based study labs 22
- preshared keys 638
- prestaging (practice labs), building layer 2 905–909
- preventing IP spoofing attacks 831, 832
- PRI (primary rate interface) 134
- priority classes of CAR 879
- private autonomous systems
 - BGP configuration 377–385
 - numbering 351
- private IP addressing, NAT 537–538
 - configuring 549–555
 - monitoring 559
- privilege levels
 - assigning to Cisco IOS user accounts 447–448
 - Cisco IOS password management 442
 - configuring on TACACS+ 617–621
- protected ports, configuring on Catalyst 3550
 - switches 468
- Proxy ARP
 - disabling 453
- PSNs (pseudonodes) 331–332
- public-key encryption 638
- PVCs 91
 - dynamic, configuring 189–190
 - static, configuring 186–189
 - troubleshooting 190–191

Q-R

- Q series protocols (ISDN) 134
- query packets, EIGRP 243
- RA (registration authority) 431
- RADIUS
 - AAA configuration 569–581
 - packet encryption 568
 - router management 568
 - versus TACACS+ 567
- rate limiting
 - CAR 879–885
 - configuring 882
- receive process, IS-IS state machine 330
- reconnaissance attacks 436
- recovering passwords 995–997
 - break sequence 997–1002
 - changing jumper settings with software 1007–1008
 - manually shorting jumper settings 1006
 - o/r command 1002–1003
 - on ACS running Solaris 1011
 - on Cisco IDS sensors 1008–1009
 - on Cisco PIX Firewall 1010–1011
 - on VPN concentrators 1012–1013
 - renaming software 1003–1004
 - replacing software 1005
 - resetting devices 1005–1006
- redirects
 - and HSRP 528–530
 - configuring 539
 - ICMP 524
 - MNLB Forwarding Agent, configuring 535–537
- redistribution 399–401
 - between directly connected networks 413–415
 - between EIGRP and IGRP autonomous systems 409–412
 - between EIGRP and static routes 412–413
 - between EIGRP autonomous systems 408–409
 - between OSPF and RIPv1 407–408
 - connected networks into OSPF 402
 - filtering routing information 416–421
 - metrics 397
 - OSPF into BGP
 - configuring 402–405
 - NSSAs into BGP 405–407

- practice lab 915–917
- troubleshooting 399
- redundancy, HSRP 527
 - and ICMP redirects 528–530
 - configuring 541–547
- reference points 135
- reflexive ACLs, configuring 488–511
- reinitializing EIGRP routing process 270
- remote access, configuring on Cisco IOS 446
- remote FTP administration 449
- remote study labs 23
- remote-access VPNs 435, 633
 - configuring on PIX Firewall 593–608
- removing VLAN map entries 514
- renaming configuration files 1003–1004
- replacing software, password recovery 1005
- reply end-to-end keepalives 101
- reply packets, EIGRP 243
- request end-to-end keepalives 101
- request packets, EIGRP 243
- required equipment for requirements
 - home-based study lab equipment 24–25
 - of IS-IS addressing 334–335
- resetting devices, password recovery 1005–1006
- resource usage for ACLs, displaying 515
- retransmission interval, IS-IS 339
- RFC 2225 ATM configuration 191–193
 - classical IP with PVC 192–193
 - classical IP with SVCs 193–194
- RIB (Routing Information Base) 330
- RIP (Routing Information Protocol)
 - advanced configuration 233–235
 - configuring 203–220
 - over router to PIX 5.2 connection 221–225
 - over router to PIX 6.2 connection with authentication 225–231
- redistribution into OSPF 407–408
- structure 201
 - default routes 203
 - metric 202
 - routing updates and timers 201–202
 - split horizon 202
- risk assessment 431
- rlogin services 960
- root account, modifying 964
- route authentication, EIGRP configuration 263–264
- route calculation timers, OSPF configuration 301

- route filtering 208
- route redistribution, configuring 337–338
- route states (EIGRP) 250
- route summarization
 - configuring on EIGRP 258–259
 - configuring on OSPF networks 294–295
 - disabling on EIGRP 256–258
- route tagging (EIGRP) 251
- router ACLs
 - configuring 490
 - VLAN maps, configuring 491–492
- routing
 - ISDN
 - floating static routes 152–154
 - OSPF demand circuits 155–157
 - passive interfaces 151–152
 - static routes 149–151
 - practice lab 911
 - timed portion 913–914
- routing protocols
 - classful 398
 - classless 398
 - ships in the night 321
- RPC services 961
- RPF (Reverse Path Forwarding)
 - configuring 886
 - preventing attacks
 - DoS attacks 880
 - IP spoofing attacks 831
- RSA (Rivest, Shamir, and Adleman) 432
- RSA signatures 638

S

- SAs (security associations) 637
- SCEP (CA Server with Simple Certificate Enrollment Protocol) 695
- Security Notifications Bulletin 975
- Security Roll Up Packages 975
- selective acknowledgment (TCP) 534
- sername password command 756
- server operating systems, Windows 969
- service packs, Windows resources 971
- service resetinbound command 833
- services
 - BOOTP server 453
 - CDP 452

- finger server 453
- FTP 960
- HTTP servers
 - configuring 456–457
- ICMP messaging 454–455
- IP source routing 454
- IP-directed broadcast 454
- NFS 961
- NTP 453
 - configuring 458–463
- Proxy ARP 453
- rlogin 960
- router name and DNS resolution 451
- RPC 961
- startup scripts, disabling 961
- TCP and UDP small servers 452
 - verifying deactivation 455, 456
- SHA-1 (Secure Hash Algorithm) 432, 638
- share-level security, NTFS 980
- ships in the night 321
- show dialer command 172–173
- show frame-relay map command 125
- show frame-relay pvc command 123–125
- show interfaces bri 0/0 command 169–171
- show ip accounting command 548
- show ip nhrp command 745
- show isdn active 173
- show isdn status command 171–172
- show ppp multilink command 173
- show route command 823
- show vpdn tunnel command 760
- signaling, Frame Relay 91, 92
 - LMI autosense feature 95
 - LMI frame format 92–93
 - LMI timers 94–95
- signatures 842
- signatures (IDS) 861–867
- simplex interfaces 527
 - OSPF configuration 301
- simulating break sequences 1013
- single-homed autonomous systems 351
 - BGP configuration 354–363
- site-to-site VPNs 631–632
- SMR (Stub Multicast Routing), configuring on PIX Firewall 6.2 847–850
- smurf attacks 454
- SNMP (Simple Network Message Protocol), configuring on PIX Firewall 841–842
- software configuration register, password recovery 995–998
 - config-register command 999–1002
 - o/r command 1002–1003
- Solaris
 - applying patches 958
 - default umask setting, changing 964
 - disabling routing 965
 - installing 958
 - network services, stopping 959–960
 - SSH, implementing 967
 - user accounts, locking 965
- source routing 526
- source-address spoofing on lock-and-key ACLs 485
- specifying RIP version 210, 211
- SPIDs (service profile identifiers), ISDN
 - configuration 143–144
- split horizon 88, 202
 - disabling on EIGRP 269
- split tunneling 600
- SSH (Secure Shell) 443
 - configuring 464–466
 - implementing on Solaris systems 967
- stack-based buffer-overflow, preventing 963
- standards, ISDN-related protocols 133–134
- standby routers (HSRP) 527
- star topologies, Frame Relay 86
- startup scripts, disabling 961
- state machine (IS-IS) 330–331
- static NAT, Cisco PIX Firewall configuration 820–822
- static PVCs, configuring 186–189
- static routes
 - Cisco PIX Firewall configuration 822–823
 - ISDN 149–151
 - redistribution to EIGRP interfaces 412–413
- Stop-A abort sequence, disabling 965
- stopping network services 959–960
- storm control, configuring on Catalyst 3550 switches 467
- structure of RIP 201
 - default routes 203
 - metric 202
 - routing updates and timers 201–202
 - split horizon 202
- stub routingm EIGRP configuration 264, 265
- study labs
 - home-based 22

- planning 23–25
- remote 23
- required equipment 24–25
- work-based 22
- studying for CCIE exam, developing good habits 15–18
- summarization
 - OSPF 306
 - external 308
 - inter-area 306–308
 - RIP routes 212–215
- SVCs 90
 - configuring on Frame Relay 109–113
- switch type, ISDN configuration 142, 143
- switches
 - Catalyst 3550, unsupported IOS ACL-related features 518
 - CatOS 434
- sysopt connection command 837

T

- TA (terminal adapter) 134
- TACACS+
 - authentication proxy 610–615
 - configuring 615–617
 - packet encryption 568
 - PPP callback, configuring 621–627
 - privilege levels, configuring 617–621
 - router management 568
 - versus RADIUS 567
 - VPDN configuration 761–765
- TCP 814
 - performance parameters, configuring 531–535
 - settings, securing 964
 - small servers, disabling 452
- TCP intercept, configuring 776–781
- TCP/IP header compression, configuring on Frame Relay 121–122
- TE1 (Terminal equipment 1) 134
- TE2 (Terminal equipment 2) 134
- TEI (terminal endpoint identifier) 137
- Telnet addresses, hiding 449
- terminal equipment (ISDN) 134–135
- time range function
 - configuring on ACLs 483–484
 - implementing on ACLs 504–506

- timed portion (practice lab)
 - configuring advanced security features 927–931
 - configuring basic security 919–920
 - building layer 2 909–911
 - master lab 942–951
 - redistribution and dial backup configuration 916–917
 - routing 913–914
 - service provider 932
- timers
 - LMI, tuning 94–95
 - RIP 201–202
- topics covered on CCIE Security exam 6–9
- topologies, partially meshed 87
 - subinterfaces 88–89
- topology table, EIGRP 246–247
 - displaying information 248–249
 - DUAL 251–252
- ToS classes, CAR rate limiting 879
- traffic filtering
 - ACLs 477–483
 - ACE entry order 496
 - ACEs 477
 - applying to interfaces 496–497, 501
 - configuring 498
 - crypto 477
 - defining 495
 - defining criteria 498–500
 - displaying information 514–515
 - extended ACLs 481
 - implementing 478–479
 - implicit deny statement 495
 - lock-and-key 484–487, 506–507
 - logging 494–512
 - named extended ACLs 482
 - named MAC extended 482, 512–513
 - named standard ACLs 482
 - numbered standard IP ACLs 481
 - port 490–491
 - reflexive 488–511
 - router 490
 - size limitations 517–518
 - time range function 483–484
 - time range function, implementing 504–506
 - troubleshooting 516–517

- unsupported features on Catalyst 3550
 - switch 518
 - VLAN map entries, creating 513
- CBAC 781–782
- traffic inspection, CBAC 782
- traffic shaping, configuring on Frame Relay 114–119
- transform sets 651
- transit autonomous systems 351
 - BGP configuration 363–372
- transitivity 88
- transparent bridging, split horizon 88
- transport mode (IPSec) 640
- Tripwire 967
- troubleshooting
 - ACLs 516–517
 - EIGRP 270–272
 - flapping routes 157
 - Frame Relay connectivity 122–126
 - IPSec VPNs 662–670
 - PIX-to-PIX 687–695
 - ISDN 169–177
 - IS-IS authentication 345
 - PVCs 190–191
 - redistribution 399
 - RIP 218–220
- tuning LMI timers 94, 95
- tunnel mode (IPSec) 640
- tunnel ports 881
- tunneling
 - 802.1Q 881
 - L2F 749
 - L2VPN
 - configuring 887–891
 - verifying configuration 891–894
 - Layer 2 protocol tunneling 881
 - PPTP 751
 - PIX2 firewall configuration 766–768
- TurboACL, configuring on PIX Firewall 6.2 850
- turning off CBAC 802

U

- UDP 814
 - small servers, disabling 452
- umask setting, modifying 964

- UNI (User-Network Interface) 96
 - cell headers 183–184
- unidirectional PPP authentication, configuring 164
- uninteresting traffic 141
- UNIX
 - ACS running Solaris, password recovery 1011
 - EEPROM passwords, configuring 966
 - Solaris
 - applying patches 958
 - installing 958
- unreachables (ICMP) 524
- update packets
 - BGP 353
 - EIGRP 243
 - RIP 201–202
 - blocking on interfaces 207
- update process, IS-IS state machine 331
- URLs, filtering 828–831
- UrlScan 971
- user accounts
 - AAA verification 449–451
 - locking 965
 - Windows 970
- user accounts (Cisco IOS)
 - assigning privilege levels 447–448
 - creating 446–447

V

- VCs
 - PVCs 91
 - SVCs 90
 - configuring 109–113
- verifying
 - DMVPN configuration 741–745
 - HSRP support for MPLS VPNs 556
 - installation information 963–964
 - IPSec VPN configuration 728–732
 - L2VPN configuration 891–894
 - OSPF ABR Type 3 LSA filtering 316
 - port-based traffic control on Catalyst 3550
 - switches 470–472
 - user accounts with AAA 449–451
- verifying service deactivation 455–456
- virtual links, creating on OSPF networks 295–297
- virtual templates, creating 759
- virtual-template command 764

- VLAN maps
 - configuring on port ACLs 491
 - configuring on router ACLs 491–492
 - entries
 - creating 513
 - removing 514
 - VLSM, OSPF configuration 285
 - VPDNs 749, 750, 751
 - configuring 752
 - default group templates, configuring 768–769
 - local AAA, configuring 752–761
 - TACACS+, configuring 761–765
 - vpdn-template command 769
 - VPN concentrators, password recovery 1012–1013
 - VPNs (Virtual Private Networks) 432
 - advanced configuration 718–719
 - EIGRP 720–724
 - GRE tunnels 720
 - IPSec VPNs 715–718
 - loopback interfaces 720
 - IOS-to-IOS, IKE phase 1 using CA 696–703
 - IPSec 718–724
 - configuring between two IOS routers 644–662
 - configuring between two PIX firewalls 671–693
 - parameters, configuring 724–727
 - troubleshooting 662–670, 687–695
 - verifying configuration 728–732
 - L2VPN
 - 802.1Q tunneling 881
 - configuring 887–891
 - verifying configuration 891–894
 - PIX-to-PIX, IKE phase 1 using CA 703–710
 - remote-access 633
 - site-to-site 631–632
 - vtys, configuring 445, 446
 - fully meshed topologies 87
 - NNI 95
 - partially meshed topologies 87–89
 - PVC 91
 - signaling 91–92
 - star topology 86
 - SVCs 90
 - troubleshooting connectivity 122–126
 - UNI 96
 - white hats 432
 - Windows operating system
 - auditing, enabling 976
 - file systems
 - FAT 977
 - FAT32 977
 - NTFS 977–980
 - installing 970
 - logging, enabling 976
 - MBSA 971
 - patches, applying 975
 - user accounts 970
 - Windows 2000, creating baseline security level 972–975
 - Windows NT 4 Server, creating baseline security level 972–975
 - work-based study labs 22
 - world-writeable files, checking for 966
- xlates 814

W-X-Y-Z

- WANs
 - connections, configuring on EIGRP 254–255
 - Frame Relay
 - configuring 102–122
 - congestion control mechanisms 96–101
 - error checking 99

