Numerics

3DES encryption, 600
10-GigE (10-Gigabit Ethernet), 492
10GBASE-ER, 493
10GBASE-EW, 493
10GBASE-LR, 493
10GBASE-LW, 493
10GBASE-LX4, 493
10GBASE-SR, 493
10GBASE-SW, 493
100BASE-FX, 489
100BASE-T. See Fast Ethernet, 489
100BASE-TX, 489
400 status codes (HTTP), 56
500 error codes (HTTP), 56
802.1Q tag all, 187
802.1Q, 516
configuring, 519–520
802.3ad, 33
1000BASE-LX, 491
1000BASE-SX, 491
1000BASE-T, 491
4096 VLANs, 514

A

A (Address) records, 403
AAA (Authentication, Authorization, and Accounting)
RADIUS, 646
security, 197
TACACS+, 645
ABRs (Area Border Routers), 543
summarization, 550
absolute URIs, 312
absolute URLs, 316
Accept field (HTTP request header), 353
Accept-Charset field (HTTP request header), 353
Accept-Encoding field (HTTP request header), 354
Accept-Language field (HTTP header), 979–980
access layer
application segment, 17
back-end segment, 18
front-end segment, 16
access ports, 32, 520, 839–840
access switches, 141
acknowledgment number field (TCP), 263
ACKs (TCP), 48, 666
ACLs (access control lists), 25, 170, 873
dynamic, 171
extended, 170
reflexive, 172–173
router, 170
standard, 169
active-active firewall configuration, 906
active-active load balancing, 229–230
active-backup algorithm, 437
active-standby firewalls, 904
active-standby load balancing, 228
ActiveX controls, 86, 1017–1018
server-side, 89
addresses
formatting (Ethernet), 485–487
MAC address table, 499
advertisement interval, 535
advertising local subnets (OSPF), 854
AES-Rijndael, 601
taggregation layer, 15
taggregation routers, connecting to core routers, 846–849
taggregation switches, 141
taggregation algorithms
cache farm load-balancing, 683–685
hashing, 607
message digest, 607
SHA, 608
1026 algorithms

load balancing, 673
  fastest, 680
  hash address, 681
  least connections, 678
  round-robin, 676
  server farm, 673–675
  source IP, 681
  URL and hash URL, 681
  weighted least connections, 679
  weighted round-robin, 677
alternate Layer 3/Layer 2 designs, 133
alternate ports, 829
analog video streaming, 447
codecs, 448
analyzing SSL traces, 391–393
anomaly-based IDSs, 181
antireplay protection, 190
antispoofing filtering, 870
uRPF, 873
Apache web servers, 330
  virtual hosting configuration, 58–59
    IP-based, 59
    name-based, 61
    port-based, 60
APIs (application programming interfaces),
  server-specific, 88
applets, 86
Java, 1014–1015
application architecture trends, 150–151
application layer, 244
  probes, 713
    DNS probes, 717
    FTP probes, 717
    HTTP probes, 714
    IMAP4 probes, 718
    POP3 probes, 718
    SMTP probes, 718
    SSL probes, 715
application segment (access layer), 17
application services, 24
application tier, 77
applications
  Data Center architecture models
    client/server, 9–10
    multtier, 12
    n-Tier, 11
  enterprise, 71
  integration, 75
    EAI, 75–77
  multtier design (case study), 108–111
  network architecture implications, 97
    clustering, 99–102, 104
    load balancing, 97–98
    security, 104–105, 107
  n-Tier model, 77
  database access, 95–96
  markup languages, 79–83
  middleware, 91–95
  server-side programming, 87–91
  user agents, 84–85
  web servers, 86
portal, 72
TCP, 41
  ACKs, 48
  data processing, 41
  HTTP, 47, 55–56
  maximum burst size on high-speed networks, 49–50
  segments, 42
  Telnet, 43–46
  windows, 47–48
  UDP, 50–51
  upgrades, 71
APPN (advanced peer-to-peer networking), 572
  node types, 579–580
architectures
  MLS, 809
  of Data Centers
    flexibility, 118
    high availability, 118
    scalability, 117
  of load balancers, 232–235
    critical components, 234–235
    generic components, 232–234
Area Border Routers (ABRs), 543
ARP (Address Resolution Protocol), 525–526
  ARP inspection, 184, 895
  ARP spoofing, 167
  timeout values compared with CAM tables, 526
ASBR (autonomous system border router)
  summarization, 550
ASCII character sets
  extended, 965–966
  nonprintable, 963–964
  printable, 964–965
ASPs (active server pages), 88, 1022
asymmetric cryptography, 602
  D-H, 606
  DSS, 605
  RSA, 603–604
asymmetric encryption, 191
attachment options for mainframes, 573
  channel attachments, 573–574
  LAN attachments, 575
attacks
  buffer overflow, 167
  DDoS, 164
  DoS, 163
  eavesdropping, 165
  Internet infrastructure attacks, 166
  Layer 2, 167–168
  mitigation, 202
scanning/probing, 162
session hijacking, 167
smurf, 163
trust exploitation, 166
unauthorized access, 165
viruses and worms, 165
attributes of cookies, 729–731
audio streaming
  transport formats, 442, 454
    RTCP, 457–459
    RTP, 454
authentication, 640, 876
  AAA protocols
    RADIUS, 646
    TACACS+, 645
  challenge/response schemes, 642
digital certificates, 642
HTTP, 364
Kerberos, 644
management network, 911–913
OTPs, 641
SSL, 385–387
  PKI, 388–389
authenticity tags, 194
authoritative name servers, zone transfers, 418–420
Authorization field (HTTP request header), 354
autonegotiation
  Gigabit Ethernet, 492
  NICs, 490
autostate, 810, 814
auto-unfail, 706
availability, optimizing with load balancing, 65
baby giant frames, 496
BackboneFast, 827–828
back-end segment (access layer), 18
backup designated routers (BDRs), 542
backup ports, 829
bandwidth, 444
scaling with Etherchannels, 815
baseline testing, performance metrics, 950
basic data transfer, 256
BDP (Bandwidth Delay Product), 50
BDRs (backup designated routers), 542
B-frames, 451, 991
BIND (Berkeley Internet Name Domain), 408
binding, 94
black-hole problem, 287–288
blade chassis, 152–156
blade servers, 21
bottlenecks, performance metrics, 933
BPDUs (bridge protocol data units), TCN (Topology Change Notification), 527
bridge identifiers, 510
bridging, 654
broadcast suppression, 487
browsers, 84
cookies, 731–732
multiple, 733
session cookies, 769
storage of, 734–735
HTTP compression, 343
buffer overflow attacks, 167
bulk transfer traffic, 47
ACKs, 48
maximum burst size on high-speed networks, 49–50
TCP windows, 47–48
bus and tag technology, 574
bus architecture
PCI, 34
PCI-X, 35
business continuance infrastructure services, 26
business continuance services, 27
BXN (branch extender node), 583
CA servers, 74
cabling, Ethernet, 481
cache load balancing, 210–211
server farms, 683–685
Cache-Control field (HTTP general header), 344–345
caching, 25
cache hits, 681
cacheable objects, 683
DNS, 420
client applications, 422–423
TTL values, 421
hit rate, 673
in site-selection architecture, 436–437
on-demand, 472
RPC, 683
transparent, 684
caching-only servers (DNS), 411
cache-hit rate, 673
cacheable objects, 683
certificate authorities, 619
certificates, 621
deployment options, 623
enrollment, 624
key exchange, 620
revocation, 625
CC metric, 933
load balancers, 942–943
SSL offloaders, 948
CDP (Cisco Discovery Protocol), 500
CEF (Cisco Express Forwarding), 807–809
MLS, 821
certificates, SSL, 629
CF channels, 585
CGI, 88–89, 1018–1019
challenge response schemes, 642
channel link-layer protocols, 576
channeling, 507
channel-protocol lacp command, 508
channels, 569
connecting mainframes to peripheral devices, 573–574
character sets, 326
ASCII
    extended, 965–966
    nonprintable, 963–964
    printable, 964–965
ISO-8859-1, 969
checksum field (TCP), 266
chroma subsampling, 989
ciphers, 188
    export-grade, 611
    overview, 608
    RCs, 602
    SSL cipher suites, 632–633
ciphersuites, 371, 389–390
Cisco IOS Software
    internal redundancy, 835
    switching paths, 807–808
Cisco IPTV, 442
CISCO-SLB-MIB, 698–699
CLASSID, 1017
client error status codes (HTTP response header), 360
client NAT (load balancers), 662
    performance, 672
client tier, 77
client/server application model, 9–10
client/server architecture
    network attachment options, 32
    NICs, 32–33
PCI, 34
PCI-X, 35
server multihoming, 33
NICs, Ethernet driver, 36
packet processing, 35–36
sockets, 39
    system calls (UNIX), 39–40
TCP/IP processing, 37–39
clients
    browsers, 84
    thin, 83
client-side programming, 85
    ActiveX controls, 1017–1018
    Java applets, 1014–1015
    JavaScript, 1013
cluster controllers, 570
clustered proxy servers, persistence, 759
clustering, 97, 382
    cluster modules, 100
    geographical, 101
    implications for application integration, 99–104
    Sysplex, 585–589
CNAME (Canonical Name) records, 404
codecs, 441, 448, 473
    comparison of, 452
    video encoding, 987
coded character sets, 327
CodeRed, 165
collaborative applications, 72
collapsed multitier design, 137–138
collapsed server-farm design, 898–900
collision domains, diameter, 487
commands, netstat -a, 37
communications controller, 570
components of IBM Data Centers, 570–573
compression
    HTTP, 342–343
    redundancy (video), 448
confidentiality, 189
configuring
  802.1s, 519–520
cookie active, 775
cookie match, 772
cookie passive, 770
HTTP redirection stickiness, 783
Layer 2 features
  access ports, 839–840
  overview, 844
  spanning trees, 841–843
  trunks, 840
  VLANs, 837–839
Layer 3 features, 846
  default gateway redundancy, 849–851
  EIGRP, 858–862
  OSPF, 852–857
  routing options, 846–849
load balancers for given applications, 98
loopback interfaces, 995
  Linux, 1005–1006
  Windows 2000, 996–998
  Windows NT, 1002
NAT on routers and firewalls, 558
preemption, 851
rapid PVST+, 518
routing on servers, 524
server farms on a load balancer, 691
source IP stickiness, 765
  mega proxies, 766–767
  source IP hash, 768
SSL stickiness, 786
URL cookies, 779
web servers, 57
  directories, 58
  inserting cookies, 1010
  server processes, 57
  TCP parameters, 57
  virtual hosting, 58–60

congestion avoidance, 279
congestion control, 278
congestion window (TCP), 47
CONNECT method (request header), 351
connection establishment, Telnet sessions, 43–44
Connection field (HTTP general header), 345
connections, 257
  embryonic, 564
  failover, 231
  HTTP, 335, 337
    persistent connections, 339
    pipelining, 340
  load balancing, 674
  long-lived, 929–931
  maxconns, 678
  performance metrics, 935
  persistence, 219
  reassigning, 704
  remapping, 667
  short-lived, 925–927
  spoofing (load balancers), 664–667
    connection remapping, 667–669
    performance, 672
  TCP, 267
    establishment phase, 268–270
    monitoring, 67
    termination phase, 46, 272, 275
  TCP/UDP, stickiness, 674
  tracking, 219
  connectivity, blade chassis options, 152–156
content switching, 205. See also server
  load balancing
    horizontal scaling, 206
    versus DNS round-robin, 207–209
    vertical scaling, 206
  Content-Encoding headers, 343
  control flags (TCP), 264–266
  control protocols, 466
  RTSP, 467–470
  control units, 574
controllers, 493
convergence, 827
  MST, 831
  OSPF, 856
  PVST+, 828
  Rapid PVST+, 829–830
cookies, 221–223, 728
  browser storage, 734–735
  browser treatment of, 731–732
  browser treatment of multiple cookies, 733
  format, 729–730
  inserting, 1010
load balancers
  cookie active, 775
  cookie match, 771–773
  cookie passive, 769
persistent, 728–729
session, 728–729
specifications and standards, 735
stickiness, 222
tracking user sessions, 739
URL, 776–778
CORBA, 92, 95
core routers, connecting to aggregation routers, 846–849
corporate Data Centers, 126
CPS metric, 933
  load balancers, 942
  SSL offloaders, 948
cryptography, 188–189
  asymmetric, 602
    D-H, 606
    DSS, 605
    RSA, 603
    RSA key exchange, 604
  symmetric encryption, 191
ciphers, 608
  export-grade, 611
digital signatures, 195
  FIPS, 609
hashing algorithms, 193, 607
  message digests, 607
  SHA, 608
HMACs, 194
NIST, 609
PKI, 612
  CAs, 619–625
digital certificates, 615–619
  standards, 614
symmetric, 190, 597
  3DES, 600
  DES, 598–600
  RCs, 602
dark fiber, 104
data, 452
  encoding, 448–451
  multimedia transport formats, 454
    RTP, 454, 457–459
    UDP versus TCP, 445–446
packetization, 453
replication, 103
TCP, 463
transport security, 626
  IPSec, 633–634, 637–638
  SGC, 631
  SSL, 626, 628–629
  SSL cipher suites, 632–633
  VPNs, 639
Data Centers
  application architecture
    client/server model, 9–10
    multitier, 12
    n-Tier model, 11
applications
  EAI, 75–77
  integration, 75
multitier design (case study), 108, 111
network architecture implications, 97–107
n-Tier model, 77–96
portal, 72
architecture, 13–14
access layer, 16–18
aggregation layer, 15
layers, 14
storage layer, 19
transport layer, 20–21
design criteria, 6
facilities, 7
goals, 6
high availability, 109
infrastructures, 801–805
spanning trees, 822
virtualizing with VLANs, 804, 810, 813–814
Layer 2 design
access ports, 839–840
configuration overview, 844
spanning trees, 841–843
trunk configuration, 840
VLAN configuration, 837–839
Layer 3 design
default gateway redundancy, 849–851
EIGRP, 858–862
OSPF, 852–857
routing considerations, 846–849
overview, 5
performance metrics, 934–935
firewalls, 938
load balancers, 939–945
multilayer switches, 936–937
SSL offloaders, 946–949
testing, 950–957
redundancy, 833
NSF, 835–837
supervisor redundancy, 834–835
redundant links, 815–817
roles
enterprise, 7
SP environment, 9
security framework
incident response and attack mitigation, 202
secure management framework, 200–201
security life cycle, 198
security policies, 198
zones, 866
server failure detection, 700
probes, 701
SNMP, 701
server management, 689–690
CISCO-SLB-MIB, 698–699
DFP, 708
graceful shutdown feature, 691
HTTP and HTTPS (case study), 722–723
in-band probes, 703–706
load balancing overview, 690
Max/Min Connections, 694–695
out-of-band probes, 707–708, 711, 713–714, 716–718
probe comparison, 709
slowstart feature, 693
SNMP, 697–698
virtual hosting (case study), 718–720
XML, 696–697
services, 22
application, 24
business continuance, 26–27
IP infrastructure, 23
security, 25
storage, 26
static routing, 527
traffic patterns, 924
long-lived traffic, 929–931
performance metrics, 933
short-lived traffic, 925–927
VLANs, 502
data processing on TCP applications, 41
database access, 95–96
database middleware, 91
database servers, 73
database tier, 77
datagrams, 245
Date field (HTTP general header), 346
DBMSs (database management systems), 96
dCOM objects, 93–95
  passing through firewalls, 95, 106
DCT (discrete cosine transform), 988
DDoS (distributed denial-of-service) attacks, 164
debounce feature, 831
decryption, 188
dedicated Internet server farms, 120
defining
  security zones, 865–868
  VTP domains, 504
delayed ACKs, 45, 280
delegated name servers, 428
DELETE method (request header), 351
deploying
  antispoofing filtering, 870
  services in redundant Layer 2/Layer 3 Data Centers, 148
DES encryption, 598–600
designated ports (DPs), 512, 829
designing
  Data Centers
    bus architecture, 34–35
    client/server architecture, 35–39
criteria, 6
  flexibility, 118
  fully redundant Layer 2/Layer 3 designs, 139–157
  high availability, 118
  optimizing performance, 62–67
  scalability, 117
  server multihoming, 33
  EAI networks, 76–77
  high availability, 51
  management network security, 914
  NICs, 32–33
  server farms
    alternate Layer 2/Layer 3 designs, 133
    collapsed server-farm design, 898–900
    expanded server-farm design, 900–902
    generic Layer 2/Layer 3 designs, 126–131
    multiple-tier designs, 133–138
    redundant firewall designs, 904–906
  VLANs, 505–506
devices, codecs, 987
DFP (Dynamic Feedback Protocol), 675, 708
D-H, 606
DHCP servers, 74
diameter, 487
diffusing DUAL, 553
digital certificates, 615, 642
  extensions, 619
  formats, 617
  generating, 616
  SSL authentication, 385–387
digital signatures, 195
Digital Video Compression (DVC), 450
digital video streaming, 447
Direct Server Return (DSR), 669–670
directed mode (load balancers), 654, 660–661
  performance, 672
directories, configuring on web servers, 58
directory servers, 74
directory services (APPN), 579
discarding ports, 511
disk replication, 102
dispatch mode (load balancers), 654, 657–659
  performance, 672
distributed DVIPAs, 588
distributing multiple records
  A records, 425
  client applications, 426
  NS records, 423–424
distribution servers, 471
DivX, 451
DLSw (Data Link Switching), 580–581
DLUR/DLUS (dependent LU requesters/dependent LU servers), 583
DMA (Direct Memory Access), 33
DMZ server farms, 120
DNS (domain naming system), 397
A records, 425
caching, 420
client applications, 422–423
TTL values, 421
forwarders, placement of, 427–428
FQDNs, 399–400
hierarchical name structure, 398–399
name resolution process, 404–406
name servers, 418
NS records, 423–424
probes, 713
queries, communication flows, 420
resolution process, 411
iterative queries, 417
queries, 412
recursive queries, 417
referrals, 414–417
root hints, 413–414
resource records, 402–403
servers, 74, 407
signatures, 881
site-selection architecture, 430–433
caching, 436–437
proximity, 435
referrals to site selectors, 433–435
stickiness, 437–438
split namespace, 428–430
TLDs, 399
zone transfers, 418–420
zones, 400–402
DNS proxy, 409
caching-only servers, 411
forwarders, 410
DNS round-robin, 207–209
domain hash predictor, 685
DoS attacks, 163
preventing with traffic rate limiting, 874
smurf, 163
download-and-play, 442–444
download rate (streaming traffic), 466
DP (designated port), 512
DSR (Direct Server Return), 669–672
DSS (Digital Signature Standard), 605
DTP (Dynamic Trunking Protocol), 501
dual-attached servers, 821
dummy unicast MAC addresses, 98
DV (Digital Video Compression), 450
DVIPA (dynamic VIPA), 587
distributed DVIPAs, 588
dynamic ACLs, 171
Dynamic Feedback Protocol (DFP), 675, 708

E

EAI, 75
network design implications, 76–77
eavesdropping, 165
ECB (electronic code book), 600
e-commerce applications, 727
session persistence, 757, 790
e-commerce applications, 72
dge ports, 829, 840
EEs (enterprise extenders), 582–583
EIGRP (Enhanced IGRP), 551, 858
configuration overview, 862
default advertisement, 555
default routers, 860
failure detection, 552
metric tuning, 553–554
redistribution, 554
summarization, 860
summarization and filtering, 555

topology, 859

EJBs, 93
electronic code book (ECB), 600
e-mail servers, 73
e-mail signatures, 881
embryonic connections, 564
encoding, 448, 473
formats, 450–451
HTTP, MIME comparison, 326
MIME, 323–324
character sets, 326
HTTP comparison, 326
media types, 327–328
transport rate, 452
URLs, 316
reserved characters, 318
unsafe characters, 318
URNs, 320
encoding video, 987
encryption, 910
3DES, 600
asymmetric, 191
control data, 201
cryptography, 188–189
DES, 598, 600
symmetric, 190
ENs (end nodes), 572
enterprise networks
applications, 71
Data Center roles, 7
Data Centers, 126
architecture, 13–21
services, 22–27
entity header, 365
Entity header fields (HTTP), 985
ephemeral RSA, 631
ESCD (ESCON directors), 574
ESCON (enterprise system connections), 574
establishing TCP connections, 268, 270
establishment controllers, 570
Etherchannels, 507
creating channels, 507
scaling bandwidth, 815
Ethernet
10-GigE, 492
physical layers, 495
10GBASE-ER, 493
10GBASE-EW, 493
10GBASE-LR, 493
10GBASE-LW, 493
10GBASE-LX4, 493
10GBASE-SR, 493
10GBASE-SW, 493
100BASE-FX, 489
100BASE-TX, 489
1000BASE-LX, 491
1000BASE-SX, 491
1000BASE-T, 491
address format, 485–487
EtherChannels, 507
creating channels, 507
Fast Ethernet, 489
autonegotiation, 490
frame size, 488
physical layers, 494
frames
baby giant, 496
format, 482–484
jumbo, 496
size, 487–488
Gigabit Ethernet, 491
autonegotiation, 492
flow control, 492
physical layers, 495
Ethernet

Layer 2 protocols, 500–501
overview, 481
physical layers, 493
switching, 498–500
examples of SSL applications
HTTPS, 372–374
expanded multitier design, 135–136
expanded server-farm design, 900–902
Expect field (HTTP header), 980
export-grade ciphers, 611
extended ACLs, 170
extended ASCII character sets, 965–966
Extensible Markup Language. See XML
external redundancy, 833
extranet server farms, 124

F

failure detection
EIGRP, 552
HSRP, 531
OSPF, 545
redundant firewalls, 906
failure recovery, spanning trees, 842
Fast Ethernet, 489
autonegotiation, 490
frame size, 488
transceivers, 495
fast paths, 933
fast recovery, 280
fast retransmission, 446
fast switching, 807
FastCGI, 89
fastest predictor, 680
FCIP (Fibre Channel over IP), 103
FEPIs (front-end processors), 570
FICON (fiber connectivity), 574
fields
HTTP entity headers, 365
HTTP general headers, 344–347
HTTP messages, 334
HTTP response headers, 362–363
IP headers
flags field, 251
fragment offset field, 251
header checksum field, 254
identifier length field, 248
identifier field, 250–251
options field, 255–256
protocol field, 252–254
TOS field, 248–250
total length field, 250
TTL field, 251–252
Version field, 247
request headers, 352
Accept field, 353
Accept-Charset field, 353
Accept-Encoding field, 354
Authorization field, 354
Host field, 354
If-Modified-Since field, 355
Max-Forwards field, 355
Range field, 355
Referer field, 355
User-Agent field, 356
TCP headers
acknowledgment number field, 263
checksum field, 266
control flags, 264, 266
options field, 266–267
sequence number field, 262
TCP header length field, 264
urgent pointer field, 266
window size field, 266
UDP headers, 299–301
file servers, 73
filtering
ACLs, 873
antispooﬁng, 870
EIGRP, 555
OPSF, 550
packet filters, 890
RFC 1918, 870
RFC 2817, 870
route filters, 876
final permutation, 600
FIPS, 609
firewall load balancing, 212–213
Firewall Service Module (FWSM), 887
firewalls, 173
hybrid, 176–177
Internet traffic patterns, 921
limitations, 178
NAT, 557
packet-filtering, 174
passing DCOM through, 95, 106
performance metrics, 938
PIX, NAT, 563–564
proxy, 175
redundant
active-active (clusters), 906
redundant firewall server-farm design, 904
server farm design, 905–906
stateful, 175, 878–879
flags field, 251
flexibility in Data Center design, 118
flooding, 98, 831
unicast, 499
flow control, 257
congestion avoidance, 279
congestion control, 278
delayed ACKs, 280
fast recovery, 280
immediate ACKs, 280
Nagle algorithm, 281–282
retransmission, 276
sliding windows, 277
slow start, 279
flow-based forwarding, 809
flow-based MSL, 820
forking servers, 51
versus threaded servers, 53
form fields, 91
form hidden fields, 737
formal namespaces, 322
forward zones, 402
forwarders (DNS), 410
placement of, 427–428
forwarding delay, 520
forwarding links, failure, 843
forwarding ports, 511
forwarding links, 427–428
frame/packet loss, 937
frames, 42, 245, 487–488
defining nonstandard size, 497
Ethernet
baby giant frames, 496
jumbo frames, 496
formatting (Ethernet), 482–484
jumbo, 33
From field (HTTP header), 980
front-end segment (access layer), 16
FTP (File Transfer Protocol)
probes, 717
session persistence, 755–756
full NAT, 662
full URIs, 312
fully switched topology, 804
FWSM (Firewall Service Module), 887
election process, 905
failure detection, 906
G

gateway redundancy, 849–851
GDPS (geographically dispersed parallel Sysplex), 589
1038  general header (HTTP)

general header (HTTP), 344
  Cache-Control field, 344–345
  Connection field, 345
  Date field, 346
  Pragma field, 346
  Transfer-Encoding field, 347
generic Layer 3/Layer 2 designs, 126–130
  Layer 2 access switches, 130–131
geographical clustering, 101
GET method (request header), 349
Gigabit Ethernet, 491
  10-GigE, 492
  autonegotiation, 492
  flow control, 492
GLBP, 527, 536, 818
  active/standby election, 537
  failure detection, 538–539
  load distribution, 540
glean adjacencies, 808
  glue records, 415
GOP (Group of Pictures), 450
  graceful shutdown feature, 691
  gratuitous ARP, 526
  grid computing, 151
  Group of Pictures (GOP), 450

H

H.261, 450
H.263, 450
half-closed connections, 282
handshakes (SSL), 374–375
  session negotiation phases, 376–378
  session resumption, 380–382
hard failures, 117
hardware
  load balancing, 98
  performance metric testing, 953
hash address predictor, 681
hashing algorithms, 607
  message digests, 607
  SHA, 608
HEAD method (request header), 349
head checksum field, 254
header compression, 296–298
  UDP, 305
header fields of IPv4, 246
  flags field, 251
  fragment offset field, 251
  header checksum field, 254
  header length field, 248
  identifier field, 250–251
  options field, 255–256
  protocol field, 252–254
  TOS field, 248–250
  total length field, 250
  TTL field, 251–252
  Version field, 247
header length field, 248
health checks, 690
hierarchical DNS name structure, 398–399
  FQDN, 400
  resource records, 402–403
  zones, 400–402
high availability, 51, 109, 227
  in Data Center design, 118
  redundancy protocol, 226, 228
    active-active environments, 229–230
    active-standby environments, 228
  server failures, 54
    SYN retransmission, 55
    TCP timeouts, 54
hint-tracks, 453
hit rate, 673
HMACs (hash method authentication codes),
  cryptographic, 194
horizontal scaling, 206
Host field (HTTP request header), 354
host replication, 102
host-based IDSs, 180, 880–882, 893
host-route adjacencies, 808
HSRP (Hot Standby Routing Protocol), 527–528
  failure detection, 531
groups, 530
preempt option, 529
tracking, 533
HTML (Hypertext Markup Language), 79–80
form fields, 91
HTTP (HyperText Transfer Protocol), 47
  applications, 55–56
  authentication, 364
  character sets, 327
  configuring on web servers, 57
  connection remapping, 667–669
  connections, 335–337
  cookies, 728
entity header, 365
Entity header fields, 985
functionality, 329–330
general header, 344
  Cache-Control field, 344–345
  Connection field, 345
  Date field, 346
  Pragma field, 346
  Transfer-Encoding field, 347
header fields
  Accept-Language, 979–980
Expect, 980
From, 980
If-Match, 981
If-Modified-Since, 982
If-None-Match, 981
If-Range, 981
Proxy-Authorization, 982
TE, 982
Trailer, 977
Upgrade, 978
Via, 978
Warning, 978
HTTP redirection, 782–784, 792
message format, 332
  components, 334
  fields, 333
methods, 309
MIME comparison, 326
overview, 328
performance
  attribute comparison, 341
  compression, 342–343
  version differences, 340
persistent connections, 339
pipelining, 340
probes, 714
RDT, 466
redirection, 782–784, 792
request header, 347
  CONNECT method, 351
  DELETE method, 351
  fields, 352–356
  GET method, 349
  HEAD method, 349
  methods, 348
  OPTION method, 348
  POST method, 349
  PUT method, 350
  request URI, 351
  TRACE method, 351
request/response, 333
  fields, 362–363
  Status-Codes, 356–362
servers, 87
  health management (case study), 722–723
  virtual hosting, 58–61
session persistence, 754–755, 757
signatures, FTP signatures, 881
status codes, 983–985
streaming, 442–444
tunneling, 461, 466
URIs, 310
versions, 330
HTTPS (HTTP over SSL), 372–374
server health (case study), 722–723
hybrid firewalls, 176–177
hybrid servers, 53

I/O handling, 35–36
IANA, language tags, 980
IBM Data Centers, 570–573, 590–591
IBM networking, 577
  APPN, 572
  mainframes, 569–575
  SNA
    APPN, 579–580
    over TCP/IP, 580–585
    subnetwork SNA, 577–579
    VTAM, 571
  Sysplex, 585–588
  GDPS, 589
ICANN (Internet Corporation for Assigned Names and Numbers), 399
ICMP (Internet Control Message Protocol) probes, 711
IDCs (Internet Data Centers), 9, 125
identifier field, 250–251
IDSs (intrusion detection systems), 178
  anomaly-based versus signature-based, 181
  host-based, 180
  Internet edge, 880–882
  intranet server farms, 891–893
  network-based, 179, 891
  responses, 182
  signatures, 107, 181, 891
IEEE 802.1D, 501
IEEE 802, 479
IEEE 802.1Q, 501
IEEE 802.3ad, 33, 501
If-Match field (HTTP header), 981
If-Modified-Since field (HTTP header), 982
If-Modified-Since field (HTTP request header), 355
If-None-Match field (HTTP header), 981
I-frames, 450, 990
If-Range field (HTTP header), 981
IKE (Internet Key Exchange), 637
IMAP4 probes, 718
immediate ACKs, 280
in-band health verification, 67
in-band probes, 703–705
  HTTP return code checks, 706
  server recovery, 706
incomplete adjacencies, 808
informational status codes (HTTP response header), 357
infrastructure (Data Centers), 801–805
inserting cookies, 1010
inside global addresses, 558
inside local addresses, 558
integrating applications, 75
  EAI, 75–77
  network architecture implications, 97
integrity, 189
Internet infrastructure security attacks, 166
interactive traffic, 41–43
  connection termination, 46
  delayed ACKs, 45
  MSS, 44
  Nagle algorithm, 46
  TCP retransmission, 44
interfaces
  database access, 96
  SVIs, 813
interleaving, 470
internal redundancy, 833
  NSF, 835, 837
  supervisor redundancy, 834–835
Internet

HTTP, 328
traffic patterns, 919–921
long-lived traffic, 931
protocols, 922
short-lived traffic, 926

Internet Data Centers, 9, 125
Internet edge security, 869
ACLs, 873
antispoofing filtering, 870
IDSs, 880–882
Internet edge design, 882
securing routing protocols, 875–876
stateful firewalls, 878–879
traffic rate limiting, 874
uRPF, 872–873

Internet server farms, 120
dedicated, 120
DMZ server farms, 120
interrupt coalescing, 33, 63
interrupt processing, optimizing, 62–63
intranet server farms, 122–124
security, 885–886
ARP inspection, 895
IDSs, 891–893
packet filters, 890
port security, 894
server-farm design alternatives, 896–906
stateful firewalls, 887–888
VLAN features, 895

intranets
traffic patterns, 919–920, 923
long-lived, 931
short-lived, 926

IOS NAT, 561–562
IP addressing, DVIPAs, 587–588
IP header compression, enabling on Cisco routers, 298
IP infrastructure services, 23
IP spoofing, 167

IP-based virtual web hosting, 59
IPSec, 633
IKE, 637
security parameters, 638
TCP/IP layers, 634
VPNs, 639

IPTV, 442
IPv4 header, 246
flags field, 251
fragment offset field, 251
header checksum field, 254
header length field, 248
identifier field, 250–251
options field, 255–256
protocol field, 252–254
TOS field, 248–250
total length field, 250
TTL field, 251–252
Version field, 247

ISAPI, 88
iSCSI, 103
ISL (InterSwitch Link), 501–503
ISO-8859-1 character set, 969
isolation, 910
iterative queries (DNS), resolution process, 417

J

J2EE (Java 2 Enterprise Edition), 92
Java
applets, 86, 1014–1015
database access, 96
J2EE, 92
servlets
case study, 90–91
user session tracking, 743
Java Virtual Machine (JVM), 1014–1015
JavaScript, 86, 1013
server-side, 88
JSPs, 88, 1021
jumbo frames, 33, 496
optimizing interrupt processing, 63
JVM (Java Virtual Machine), 86, 1014–1015

K–L

Keep-Alive field (HTTP messages), 334
keepalives, TCP, 55
Kerberos, 644
kernel mode, 35–36

language tags, IANA, 980
LANs
10-GigE, 492
physical layers, 495
connecting mainframes to peripheral devices, 575
Ethernet
addresses, 485–487
baby giant frames, 496
frame size, 487–488
frames, 482–484
jumbo frames, 496
Layer 2 protocols, 500–501
overview, 481
physical layers, 493
switching, 498–500
Fast Ethernet, 489
autonegotiation, 490
physical layers, 494
Gigabit Ethernet, 491
autonegotiation, 492
flow control, 492
physical layers, 495
IEEE 802, 479
VLANs. See VLANs

latency
load balancers, 942, 944
multilayer switch metrics, 937
SSL offloaders, 949

Layer 2
access ports, 839–840
attacks, 167–168
configuration overview, 844
convergence, 827
MST, 831
PVST+, 828
Rapid PVST+, 829–830
dual-attached servers, 821
Ethernet. See Ethernet
security, 183
802.1Q tag all, 187
ARP inspection, 184
port security, 183
private VLANs, 185–187
spanning trees, 841, 843
STP, 508–520
traffic distribution, 818
trunk configuration, 840
VLAN configuration, 837–839
Layer 2/Layer 3 designs, redundancy, 139
access layer, 141–146
application architecture trends, 150–151
network infrastructure trends, 152–157
services, 146–150

Layer 3
design options, 846
default gateway redundancy, 849–851
EIGRP, 858, 860, 862
OSPF, 852–854, 856–857
routing considerations, 846, 849
links, 805
protocols, 523
ARP, 525–526
EIGRP, 551–555
GLBP, 536–540
load balancing

- HSRP, 528–533
- NAT, 556–566
- OSPF, 541–551
- VRRP, 534–535
- redundant paths, 814
- switches, 807
- traffic distribution, 819–820
- Layer 4 load balancing, 216
- Layer 5 load balancing, 217
- persistence, 754
- layers of OSI reference model, 241–243
- application layer, 244
- learning ports, 511
- least connections predictor, 678
- LEN (low-entry networking) nodes, 579
- links
  - EtherChannels, 816
  - Layer 3, 805
  - load distribution, 815, 817
  - Layer 2, 818
  - Layer 3, 819–820
  - redundant, 815–817
- Linux
  - configuring loopback interfaces, 1005–1006
  - enabling PMTUD, 291–292
- load balancers
  - HTTP redirection, 782–784
  - Internet traffic patterns, 921
  - NAT, 557
  - performance metrics, 939–941
    - CC metric, 943
    - CPS metric, 942
    - latency, 942, 944
    - PPS metric, 944
    - response time, 945
  - persistence, 754
  - comparing mechanisms, 789
  - cookies, 769–775
  - predictors, 761
  - SSL persistence, 791
- sticky groups, 764
- sticky methods, 762
- URL cookies, 794
- PIX, NAT, 565–566
- reassigning connections, 705
- server failure detection, 700
  - probes, 701
  - SNMP, 701
- server health management, 690
  - CISCO-SLB-MIB, 698–699
  - DFP, 708
  - graceful shutdown feature, 691
  - in-band probes, 703–706
  - Max/Min Connections, 694–695
  - out-of-band probes, 707–708, 711–718
  - probe comparison, 709
  - slowstart feature, 693
  - SNMP, 697–698
  - XML, 696–697
  - source IP hash, 768
  - source IP stickiness, 765–767
  - SSL stickiness, 785
  - challenges and concerns, 787–788
  - configuring, 786
  - traffic patterns, 939
  - URL cookies, 776–778
  - URL hash, 780–781
  - URL match, 779
- load balancing, 24, 97, 205
  - algorithms, 673
    - cache farm load-balancing, 683–685
    - fastest, 680
    - hash address, 681
    - least connections, 678
    - round-robin, 676
    - server farm, 673–675
    - source IP, 681
    - URL and hash URL, 681
    - weighted least connections, 679
    - weighted round-robin, 677
architecture, 232–235
critical components, 234–235
generic components, 232–234
cache load balancing, 210–211
client NAT, 662
connection failover, 231
connection persistence, 219
connection spoofing, 664–669
connection tracking, 219
directed mode, 660–661
dispatch mode, 657–659
DSR, 669–670
firewall load balancing, 212–213
flexibility, 659
hardware, 98
high availability, redundancy protocol, 226, 228–230
horizontal scaling, 206
implications for application integration, 97–98
Layer 4 load balancing, 216
Layer 5 load balancing, 217
modes of operation overview, 653
optimizing server availability, 65
overview, 690
performance, 671–672
process description, 215–216
proxy servers, 760
RTP, 472
server health, 224
  in-band server health tracking, 224
  out-of-band server health tracking, 225
server load balancing, 209–210
server-selection mechanism, 654
session persistence, 219
  cookies, 222–223
  session-sharing servers, 761
SSL traffic, 382, 384
stateful failover, 231
stateless failover, 231
sticky failover, 231
unicast streaming, 472
versus DNS round-robin, 207–209
vertical scaling, 206
VPN/IPSec load balancing, 211
load distribution, 815, 817
dual-attached servers, 821
EtherChannels, 816
Layer 2, 818
Layer 3, 819–820
looped topologies, 819
loop-free topologies, 818
load-share adjacencies, 808
local DUAL, 552
lock and key, 171
logical ports, 517–518
long-lived traffic, 929–931
  performance metrics, 933
loop-free topology, 818
loopback interfaces, configuring, 995
  Linux, 1005–1006
  Windows 2000, 996–998
  Windows NT, 1002
looped topologies, 818–819
loop-free topologies, 832–833
  load distribution, 818
  spanning trees, 822–825
Loopguard, 832–833
LPAR (logical partitions), 570, 576
LSAs, 544
LU Type 6.2, 579
LUs (logical units), 571
M

MAC address tables, 499
MAC addresses, 486
flooding, 168
Layer 2 protocols, 501
reducing, 514
redundant firewalls, 905
mac-address-table aging-time command, 500
macrowlocks, 991
mainframes, 569
  attachment options, 573
    channel attachments, 573–574
    LAN attachments, 575
  FEP, 570
  LPAR, IP addressing, 576
  operating systems, 570
Management Information Bases. See MIBs
management networks, security, 908
  authentication, 911–913
  encryption, 910
  isolation, 908–910
  secure design, 914
man-in-the-middle attacks, 184
MANs, IEEE 802, 479
markup languages
  HTML, 79–80
  WML, 83
  XML, 79, 82–83
master-down interval, 535
Max Connections parameter, 694–695
maxconns, 678
Max-Forwards field (HTTP request header), 355
maximum connections, 682
Maximum Transmission Unit, 488
MD5 (Message Digest-5), 607
media types, 327–328
mega proxies, 766–767
messages
  HTTP, 309, 332
    components, 334
    fields, 333
  MIME, 323–324
    character sets, 326
    HTTP comparison, 326
    media types, 327–328
messaging middleware, 91
META tag, configuring web servers to insert cookies, 1010
methods
  HTTP, 309
    request header, 347–348
      CONNECT, 351
      DELETE, 351
      GET, 349
      HEAD, 349
      OPTION, 348
      POST, 349
      PUT, 350
      TRACE, 351
  URLs, 316
metrics
  performance, 934–935
  firewalls, 938
  load balancers, 939–945
  multilayer switches, 936–937
  SSL offloaders, 946, 948–949
  testing, 950–957
tuning
  EIGRP, 553–554
  OSPF, 547, 856
MHSRP, 818
MIBs (Management Information Bases), 698
  platform flexibility, 702
  RMON, 699
Microsoft .NET, 92
middleware, 76, 91–92
  components, 93
  traffic patterns, 94–95
MIME format, 323–324
  character sets, 326
  HTTP comparison, 326
  media types, 327–328
Min Connections parameter, 694–695
MJPEG (Motion JPEG), 450
MLS (Multilayer Switching)
architectures, 809
CEF-based, 821
flow-based, 820
switching paths, 809
mod_session, session-tracking case study, 740–741
modifying TCP keepalive defaults, 55
monitoring TCP connections, 67
motion estimation, 989
MPEG (Motion Pictures Experts Group), 990–991
macroblocks, 991
MPEG1, 450
MPEG2, 450
slices, 991
MSS (maximum segment size), 44, 283–284
MST, 823, 831
MTU (Maximum Transmission Unit), 488
mtu command, defining nonstandard frame size, 497
multicast addresses, mapping, 486
multicast packets, 471
multicast streaming, 24
multilayer switches, performance metrics, 936–937
latency, 937
throughput, 936
multimedia streaming, TCP versus UDP, 445–446
multimedia transport formats, 454
RTCP, 457–459
RTP, 454
multiple-tier designs, 133, 135
collapsed multitier design, 137–138
expanded multitier design, 135–136
multiplexing, 257
multiprocess application servers, 53
multiprocess servers, 53
multitier architecture application environment, 12
MX (Mail Exchange) records, 404

N
Nagle algorithm, 46, 281–282
name servers, 418
name-based virtual hosting, 61
namespace, URNs, 321
naming relative URIs, 314–315
NAT (Network Address Translation), 556–558, 663
application support, 559–560
IOS NAT, 561–562
load balancers, 565–566
PIX firewalls, 563–564
native VLANs, 503
NAU (network addressable unit), 571
NBMA (nonbroadcast multiaccess), 542
NCP (Network Control Program), 570
negative caching, 421
neighbor router authentication, 876
Netscape
introduction of cookies, 735
JavaScript, 1013
netstat –a command, 37
network infrastructure trends, 152–157
network management security
SNMPv3, 649
SSH, 647
network security infrastructure, 169
ACLS, 169–171
firewalls, 173
hybrid, 176–177
limitations, 178
packet-filtering, 174
proxy, 175
statefull, 175
IDSs, 178
anomaly-based versus
signature-based, 181
host-based, 180
network-based, 179
responses, 182
signatures, 181
Layer 2, 183
802.1Q tag all, 187
ARP inspection, 184
port security, 183
private VLANs, 185
private VLANs with firewalls, 187
network-based IDSs, 179, 891
networks
campus core, security, 884
Data Centers
roles of, 7
SP environment, 9
designing, multitier design (case study), 108–111
Internet edge security, 869–882
intranet server farms
design alternatives, 896–906
security, 885–895
management network security, 908–914
security, implications for application integration, 104–107
traffic patterns, 923
VLANs, 502
access ports, 520
creating trunks, 505–506
designing, 505
PVIDs, 503
trunks, 503
NICs (network interface cards), 32–33
autonegotiation, 490
Ethernet driver, 36
interrupt coalescing, 63
server multihoming, 33
NIDs (namespace IDs), 321
Nimda, 165
NIST (National Institute of Standards and Technology), 609
NNs (network nodes), 572
gnode types (APPN), 579–580
nonbroadcast multiaccess (NBMA), 542
nonedge ports, 829, 840
nonprintable ASCII character sets, 963–964
nonrepudiation, 189
NS (Name Server) records, 403, 423–425
NSAPI, 88
NSF, 835–837
NSSAs (not-so-stubby areas), 543
n-Tier model, 11
database access, 95–96
Java, 96
markup languages, 79–83
middleware, 91–92
components, 93
traffic patterns, 94–95
server-side programming, 87–89
case study, 90–91
user agents, 84
browsers, 84
client-side programming, 85
helpers and plug-ins, 85
web servers, 86
object middleware, 91
OIDs (object identifiers), 697
on-demand caching, 472
operating systems
LPAR, 570
mainframe-based, 570
UNIX, system calls, 39–40
optimizing server performance, 62
interrupt processing, 62–63
load balancing, 65
preventing server overload, 65–67
reverse proxy caching, 63
SSL, 384–385
OPTION method (request header), 348
options field, 255–256
TCP header, 266–267
OSA (open system adapters), 576
OSI reference model, 241–243
application layer, 244
OSPF, 541–542, 852
advertising the local subnets, 854
area assignment and summarization, 853
areas, 543
convergence time, 856
default advertisement, 551
failure detection, 545
LSAs, 544
metric tuning, 547, 856
neighbor states, 542
redistribution, 547–549
stub areas, 854
summarization and filtering, 550
topology, 852
OTPs (one-time passwords), 641
OUI (organizationally unique identifier) format, 486
out-of-band probes, 707–708
application layer, 713
DNS probes, 717
FTP probes, 717
HTTP probes, 714
IMAP4 probes, 718
POP3 probes, 718
SMTP probes, 718
SSL probes, 716
ICMP, 711
TCP, 711
UDP, 712
outside global addresses, 558
outside local addresses, 558
overloaded servers, 65–67

P

packet filters, 890
packet processing, 35–36
packet-filtering firewalls, 174
packetization, 453
packets
directed mode processing, 661
Ethernet, 482
filtering, ACLs, 25
header rewrites, 656
multicast, 471
RMI, 94
unicast, 471
PAgP (Port Aggregation Protocol), 501
parallel Sysplex, 585–588
partial URIs, 311
passive state, 552
passwords, OTPs, 641
paths, switching, 806
PAUSE frames, 492
PAWS, 295
PCI (Peripheral Component Interface), 34
PCI-X bus architecture, 35
performance metrics, 934–935
firewalls, 938
HTTP
attribute comparison, 341
compression, 342–343
version differences, 340
implications of SSL, 379–380
improving in SSL transactions, 384–385
load balancers, 671–672, 939–941
CC metric, 943
CPS metric, 942
latency, 942–944
PPS metric, 944
response time, 945
multilayer switches, 936–937
SSL offloaders, 946
CPS metric, 948
latency, 949
PPS metric, 949
testing, 950
hardware, 953
selecting data mix, 956–957
software, 952
test environment, 954–955
tools, 951
persistence, 749
cookies, 728–729
  active, 775
  match, 771–773
  passive, 769
HTTP sessions, 339, 374, 754, 757
  redirection, 784
load balancers, 754, 789
multi-port protocols, 755–756
proxy servers, 758
  clustered proxies, 759
session sharing servers, 761
source IP hash, 768
source IP stickiness, 765
  mega proxies, 766–767
SSL, 755, 790–791
  stickiness, 785–789
streaming protocols, 757
URL cookies, 776–778, 794–796
URL hash, 780–781
URL match, 779
P-frames, 451, 991
PHP, 88
physical layers
  10-GigE, 495
  Ethernet, 493
Fast Ethernet, 494
Gigabit Ethernet, 495
ping of death (PoD) attacks, 163
pipelining, 340
PIX Firewalls
  election process, 905
  failure detection, 906
NAT, 563–564
pixels
  chroma subsampling, 989
  DCT, 988
PKCS (Public Key Cryptography Standards), 388
PKI (public key infrastructure), 388–389, 612
  CAs, 619
    certificates, 621
    deployment options, 623
    enrollment, 624
    key exchange, 620
    revocation, 625
digital certificates, 615
  extensions, 619
  formats, 617
standards, 614
placement
  of DNS servers
    forwarders, 427–428
    split namespace, 428, 430
  of switches in redundant Data Centers with
    services, 148
plug-ins, 85
PMTUD (path MTU discovery), 284–287
  black-hole problem, 287–288
  enabling on Linux, 291–292
  enabling on Solaris 2, 291
  enabling on Windows 2000/Windows NT, 289–290
  enabling on Windows 95/98, 290
point-to-point links, 829
POP3 probes, 718
port mappings, 105
port remapping, 667
port security, 183, 894
Port VLAN IDs (PVIDs), 503
portal applications, 72
port-based virtual hosting, 60
PortFast, 828, 839
portmapper, 94
ports
  802.1w, 829
    logical ports, 517–518
    putting into a permanent trunk, 841
    roles and states, 511
    switch ports, 505
POST metric (request header), 349
PPS metric, 933
  load balancers, 944
  SSL offloaders, 949
Pragma field (HTTP general header), 346
precedence bits, 249
predictors, 761
  cache farm load-balancing, 683–685
  fastest, 680
  hash address, 681
  least connections, 678
  round-robin, 676
source IP, 681
URL and hash URL, 681
URL hash, 780–781
weighted least connections, 679
weighted round-robin, 677
preemption, 851
presentation tier, 77
preventing server overload, 65–67
printable ASCII character sets, 964–965
private VLANs
  in conjunction with firewalls, 187
  security, 185
probes, 690
  comparing and selecting, 709
  DNS, 713
in-band health checks, 703–705
  HTTP return code checks, 706
  server recovery, 706
out-of-band probes, 707–708
  application layer, 713–718
  ICMP, 711
  TCP, 711
  UDP, 712
server failure detection, 700–701
probing, 162
process switching, 807
processes, 51–53
  channels, 569
  configuring on web servers, 57
  multiprocess application servers, 53
programming
  client-side, 85
  server-side, 87–91
progressive playback. See HTTP streaming
protocol field, 252–254
protocols
  ARP, 525–526
  authentication, 640
  control, 466
  EIGRP, 551
    default advertisement, 555
    failure detection, 552
    metric tuning, 553–554
    redistribution, 554
    summarization and filtering, 555
  GLBP, 536
    active/standby election, 537
    failure detection, 538–539
    load distribution, 540
  HSRP, 528
    failure detection, 531
    groups, 530
    preempt option, 529
    tracking, 533
Internet traffic patterns, 922
Layer 2, STP, 508–520
NAT, 556–558
  application support, 559–560
  IOS NAT on routers, 561–562
  load balancers, 565–566
  PIX firewalls, 563–564
OSPF, 541–542
  areas, 543
  default advertisement, 551
  failure detection, 545
  LSAs, 544
  metric tuning, 547
  neighbor states, 542
  redistribution, 547–549
  summarization and filtering, 550
  routing, securing, 875–876
  streaming, 441–442
VRRP
  failure detection, 535
  master/backup election, 534
  wire format, 474
proxies, mega proxies, 766
proxy firewalls, 175
proxy servers
  load balancing, 760
  persistence, 758–759
Proxy-Authorization field (HTTP header), 982
PTR (Pointer Resource Records) records, 404, 408
PU Type 2.1, 579
public key encryption, 191, 379. See also
  asymmetric cryptography
punt adjacencies, 808
PUs (physical units), 571
PUT method (request header), 350
PVID (Port VLAN ID), 503
PVST+ (Per VLAN Spanning-Tree Plus), 501
  convergence, 828
  rapid PVST+, 514
  configuring, 518
  VLAN support, 518

Q
QoS policies, 24
quantization, 988
queries (DNS)
  communication flows, 420
  resolution process, 412
QuickTime, 460, 474
  Real Video, 451

R
RADIUS servers, 74
Range field (HTTP request header), 355
Rapid PVST+, 823–825
  convergence, 829–830
rapid PVST+, 514
  configuring, 518
RCs, 602
RDT stream delivered on HTTP, 466
real-time streaming, 442–444
  bandwidth, 444
  HTTP tunneling, 461
Real-Time Streaming Protocol, 467–470
  realtime-streaming, 443
RealVideo, 460, 474
reassembler module, 453
  reassigning connections, 704
  receive window (TCP), 47
  records, 375
  A records, 425
  glue records, 415
  NS records, 423–424
  recursive queries, 404, 409
  recursive queries (DNS), resolution process, 417
  redirection status codes (HTTP response header), 359
redistribution
   EIGRP, 554
   OSPF, 547–549
redundancy, 448, 833
   EtherChannels, 507
   gateways, 849–851
   high availability, 226–228
       active-active load balancing, 229–230
       active-standby load balancing, 228
   NSF, 835–837
   spanning trees, 842
   supervisor redundancy, 834–835
redundant firewall server-farm design, 905–906
redundant Layer 2/Layer 3 designs, 139
   access layer, 141–146
   application architecture trends, 150–151
   network infrastructure trends, 152–157
   services, 146–150
redundant links, 815–817
Referer field (HTTP request header), 355
referrals (DNS), resolution process, 414–417
reflexive ACLs, 172–173
registered informal namespaces, 321
registries, 94
relative URIs, 311
   naming, 314–315
relative URLs, 316
reliability, 257
Remote Network Monitoring, 699
removing, temporal redundancy, 987, 989
request header, 347
   fields, 352
      Accept field, 353
      Accept-Charset field, 353
      Accept-Encoding field, 354
      Authorization field, 354
      Host field, 354
      If-Modified-Since field, 355
      Max-Forwardst field, 355
Range field, 355
Refrer field, 355
User-Agent field, 356
methods, 348
   CONNECT, 351
   DELETE, 351
   GET, 349
   HEAD, 349
   OPTION, 348
   POST, 349
   PUT, 350
   TRACE, 351
request URI, 351
request URI, 351
Rescorla, Eric, 379
reserved characters, 318
residual macroblock, 989
resolving DNS names, 404–406, 411
   caching, 420
      client applications, 422–423
      TTL values, 421
   DNS proxy, 409
      caching-only servers, 411
      forwarders, 410
   DNS servers, 407
      iterative queries, 417
      queries, 412
      recursive queries, 417
      referrals, 414–417
      root hints, 413–414
resources (HTTP), 309
   URNs, 320
response header
   fields, 362–363
Status-Codes, 356
   client error status codes, 360
   informational status codes, 357
   redirection status codes, 359
   server error status codes, 362
   success status codes, 358
response time
load balancers, 945
SSL offloaders, 949
retransmission, 276
reverse proxy caching. See RPC
reverse zones, 402
RFC 1738, 315
RFC 1918 filtering, 870
RFC 2827 filtering, 870
RFCs (requests for comments), 310
RHI (Route Health Injection), 846
RMI, passing through firewalls, 106
RMON (Remote Network Monitoring), 699
root DNS servers, 407
root hints (DNS), resolution process, 413–414
root port (RP), 512
root ports (RPs), 829
root switches, setting priority, 511
round-robin predictors, 676
route filters, 876
Route Health Injection (RHI), 846
router ACLs (RACLs), 170
routing, 655
between core and aggregation routers, 846, 849
NAT, 557, 561–562
neighbor router authentication, 876
OSPF, 853
passive states, 552
process overview, 655
routing protocol security, 875–876
RP (root port), 512
RPC (reverse proxy caching), 683
optimizing server performance, 63
RPR+, 835
RRs (resource records), 402–403
TTL values, 421
RSA (Rivest, Shamir, and Adelman), ephemeral
RSA, 631
RTP (Real-time Transport Protocol), 454
load balancing, 472
payload types, 455
QuickTime, 460
RTSP (Real-Time Streaming Protocol), 467–470

S
SACK, 292–293
SANs (storage-area networks), connecting storage
device to servers, 19
scalability
in Data Center design, 117
EtherChannels, 815
spanning-tree algorithm, 824
scanning, 162
scripting, 88
ASP, 1022
CGI, 1019
secondary root switches, 511
secret-key algorithms, 190
SSL, 378
security
AAA, 197
attacks
buffer overflow, 167
DDoS, 164
DoS, 163
eavesdropping, 165
Internet infrastructure attacks, 166
Layer 2, 167–168
scanning/probing, 162
session hijacking, 167
trust exploitation, 166
unauthorized access, 165
viruses and worms, 165
1054 security

authentication, 640
AAA protocols, 645–646
challenge/response schemes, 642
digital certificates, 642
HTTP, 364
Kerberos, 644
OTPs, 641
campus core, 884
cryptography, 188–189
asymmetric, 602–606
symmetric, 190, 597–602
Data Center framework
incident response and attack mitigation, 202
secure management framework, 200–201
security life cycle, 198
security policies, 198
defining security zones, 865–868
implications for application integration, 104–107
Internet edge, 869
ACLs, 873
antispoofing filtering, 870
uRPF, 872
IDSs, 880–882
Internet edge design, 882
securing routing protocols, 875–876
stateful firewalls, 878–879
traffic rate limiting, 874
ARP inspection, 895
intranet server farms, 885–886
design alternatives, 896–906
IDSs, 891–893
packet filters, 890
port security, 894
stateful firewalls, 887–888
VLAN features, 895
isolation of management infrastructure, 200
management network, 908
authentication, 911–913
encryption, 910
isolation, 908–910
secure design, 914
need overview, 159
network management
SNMPv3, 649
SSH, 647
network security infrastructure, 169
ACLs, 169–171
firewalls, 173–178
IDSs, 178–182
Layer 2, 183–187
services, 25
terminology, 160
threats, 160
transport security, 626
IPSec, 633–634, 637–639
SGC, 631
SSL, 626–629
SSL cipher suites, 632–633
VLANs, 506
VPNs, 196
vulnerability, 161
out-of-date software, 161
software default settings, 162
servers, 73, 690
clustering
geographical, 101
implications for application integration, 99–104
session persistence, 749
cookies, 728, 732
database, 96
DNS
forwarders, placement of, 427–428
site selectors, 431
split namespace, 428–430
dual-attached, 821
failure detection, 700
probes, 701
SNMP, 701
health management, 224, 689
CISCO-SLB-MIB, 698–699
DFP, 708
graceful shutdown feature, 691
in-band server health, 224, 703–706
load balancing overview, 690
HTTP and HTTPS (case study), 722–723
Max/Min Connections, 694–695
out-of-band server health, 225, 707–718
probe comparison, 709
slowstart feature, 693
SNMP, 697–698
virtual hosting environment (case study), 718–720
XML, 696–697
HTTP, 442
load balancing, 205, 209–210
application integration implications, 98
maximum connections, 682
multihoming, 33
sessions, 727
  persistence, 761
  session tracking, 728
  tracking, 736–740
streaming, 442
URL cookies, 776, 778
vservers, 690
web, 86
server-selection mechanism (load balancers), 653–654
server-side ActiveX, 89
server-side JavaScript, 88
server-side programming, 87–89
  ASP, 1022
  case study, 90–91
  CGI, 1018–1019
  servlets and JSP, 1021
server-specific APIs, 88
services
  Data Centers, 22
    application, 24
      business continuity, 27
      business continuity infrastructure, 26
      IP infrastructure, 23
      security, 25
      storage, 26
    web services, 151
servlet APIs, session-tracking case study, 743–748
servlets, 88, 1021
session affinity, 53
session keys, 616
session negotiation phases (SSL), 376–378
session sharing servers, 761
sessions, 727
  APPN service, 579
  hijacking, 167
  persistence, 219, 673–674, 749
    cookies, 222–223, 769
    e-commerce applications, 790
  HTTP, 754, 757
    multi-port protocols, 755–756
    predictors, 761
    proxy servers, 758–759
    SSL, 755
    sticky groups, 764
    sticky methods, 762
    resuming, 380, 382, 785
    session cookies, 728–729, 769
      matching predictable strings, 773
    session tracking, 728
    SSL, persistence challenges, 787
    tracking, 736
      Apache mod_session (case study), 740–741
      combining methods, 740
      cookies, 731, 739
      form hidden fields, 737
      HTTP sessions with servlets (case study), 743–748
      URL rewriting, 738
SGC, 631
SHA (Secure Hash Algorithm), 608
shared links, 829
short-lived traffic, 925–927
  performance metrics, 933
  SSL connections, 947
show cdp command, output, 501
show spanning-tree vlan 10 command, 516
show spanning-tree vlan command, 514
signature-based IDSs, 181
signatures, 105, 181
  digital, 195
  IDSs, 107, 891
  Internet edge IDSs, 881
  Solaris, 894
  Windows, 893
site selection architecture, 430–433
  caching, 436–437
  proximity, 435
  referrals to site selectors, 433–435
  stickiness, 437–438
size (Ethernet), 487–488
slave name servers, 418
slices, 991
sliding windows, 277
slow paths, 933
slow start, 279
slowstart feature, 693
small segments, 46
SMTP probes, 718
smurf attacks, 163
SNA (Systems Network Architecture), 577
  APPN, 579–580
  over TCP/IP, 580
  DLSw, 580–581
  SNAsw, 581–585
subnetwork SNA, 577–579
VTAM, 571
SNAsw (SNA switching), 581
BXN, 583
DLUR/DLUS, 583
EEs, 582–583
TN3270, 584–585
SNMP (Simple Network Management Protocol)
  Management Stations, 697
  OIDs, 697–698
  server failure detection, 700–701
  TRAPs, 700
SNMPv3, 649
SOA (Start of Authority) records, 403
sockets, 39–40
software
  clustering, 100
  default settings (security risk), 162
  load balancing, 98
middleware, 76, 91–92
  components, 93
  traffic patterns, 94–95
  out-of-date (security risk), 161
  performance metric testing, 952
Solaris signatures, 894
Solaris 2, enabling PMTUD, 291
source IP hash, 768
source IP predictor, 681
source IP stickiness, 221, 765–76, 792
spanning trees, 822, 841–843
  client-side VLANs, 826
  selecting algorithms, 823–825
spatial redundancy, 448
  removing, 987–989
specifications, MIME, 323
speed negotiate command, 492
split namespace, 428–430
splitting (stream), 471
spoofing
  ARP, 167
  connection spoofing, 664–667
SQL (Structured Query Language), 96
SQL Slammer, 165
SSH, 647
SSL (Secure Sockets Layer), 626
  authentication, 385–387
  certificates, 629
  client authentication, 642
  connections, 371–372
  connection, 371
  data encryption, 378
  example applications of, 370–371
  handshakes, 374–378
  HTTPS, 372–374
  load balancing, 382–384
offloading, 794–796
  CPS metric, 948
  latency, 949
  performance metrics, 946
  PPS metric, 949
  performance, 379–380
  optimizing, 384–385
  persistence, 755, 791
  probes, 715
  secret keys, 378
  sessions, 372, 380–382
  stickiness, 785
    challenges and concerns, 787–788
    configuring, 786
  TCP/IP layers, 627–628
  traces, analyzing, 391–393
  VPNs, 639
SSLv2, 627
SSLv3, TLS 1.0, 627
SSO, 835
standalone servers, processes, 52
standard ACLs, 170
standard retransmission, 446
standards
  cookies, 735
  PKI, 614
stateful devices, 803
stateful failover, 227, 231
stateful firewalls, 175, 878–879
  intranet server farms, 887–888
stateless failover, 231
static routing, 527
Status-Codes (HTTP response header), 56, 356, 983–985
  client error status codes, 360
  informational status codes, 357
  redirection status codes, 359
  server error status codes, 362
  success status codes, 358
Step-Up, 631
  stickiness, 219, 674
    in site-selection architecture, 437–438
  sticky failover, 231
  sticky groups, 764
  sticky methods, 761–762
  sticky tables, 221
  storage layer, 19
  storage services, 26
  storing cookies, 734–735
STP (Spanning-Tree Protocol), 508
  802.1s configuration, 519–520
  bridge identifiers, 510
  convergence, 827
  failure detection, 513
  logical ports, 517–518
  loop prevention, 832–833
  multiple VLANs, 513–517
  port roles and states, 510–512
  rapid PVST+ configuration, 518
  versions, 509
stream splitting, 471
streaming, 441–442
  applications, session persistence, 757
  congestion, 463
  download rate, 466
  HTTP tuneling, 466
  real-time streaming, 443
  RTSP, 467, 469
  selecting protocol, 445
  servers, 74, 442
    packetizizer module, 453
    unicast/multicast packets, 471
  software products, 473
  streaming rate, 466
  TCP, 462
  transport formats, 454
    RTCP, 457–459
    RTP, 454
TCP (Transport Control Protocol)

UDP, 464–465
video, 447
stub areas, 543, 854
stub resolver (DNS), 405
subdomains, 398
subnetwork SNA, 577–579
success status codes (HTTP response header), 358
summarization
EIGRP, 555, 860
OSPF, 550, 853
supervisor redundancy, 834–835
suppressing broadcasts, 487
SVIs, VLANs, 813
switch fabric, 233–234
switch ports, 505
switching
debounce feature, 831
Ethernet, 498–499
frame size support, 497
MAC address table, 500
failure detection, 513
Layer 3, 807
multilayer, performance metrics, 936–937
operation overview, 654
root, setting priority, 511
switching paths, 806, 933
Cisco IOS, 807–808
MLS, 809
switchport mode trunk command, 506, 841
switchport trunk allowed vlan 10,20 command, 506
switchport trunk encapsulation dot1q command, 506
symmetric cryptography, 597
3DES, 600
DES, 598–600
RCs, 602
symmetric encryption, 190
SYN floods, 163
SYN retransmission mechanism, 55
Sysplex, 585–589
system jumbomtu command, 497

T

tables
ARP, 526
CAM, 526
TACACS+, 645
tagging traffic, 504
TCN (Topology Change Notification) BPDUs, 527
TCP (Transport Control Protocol), 256, 461
ACKs, 48
applications, 41
HTTP, 47
Telnet, 43–46
configuring on web servers, 57
connections, 257, 267
establishment, 268–270
termination, 272–275
data processing, 41
flow control, 257
congestion avoidance, 279
congestion control, 278
delayed ACKs, 280
fast recovery, 280
immediate ACKs, 280
Nagle algorithm, 281–282
retransmission, 276
sliding windows, 277
slow start, 279
half close, 282
header compression, 296–298
header fields, 258–259
acknowledgment number field, 263
checksum field, 266
control flags, 264–266
options field, 266–267
sequence number field, 262
TCP header length field, 264
urgent pointer field, 266
window size field, 266
TCP (Transport Control Protocol)

keepalives, 55
maximum burst size on high-speed networks, 49–50
monitoring connections, 67
MSS, 283–284
multiplexing, 257
offloading, 33
PAWS, 295
PMTUD, 284–287
black-hole problem, 287–288
enabling on Linux, 291–292
enabling on Solaris 2, 291
enabling on Windows 2000/Windows NT, 289–290
enabling on Windows 95/
Windows 98, 290
probes, 711
Real Player, 463
reliability, 257
retransmission, 44
SACK, 292–293
segments, 42
sequence numbers, 257
server failure handling, 54
SYN retransmission, 55
TCP timeouts, 54
server failures, 54
streaming, 462
timestamps, 294
versus UDP, 445–446
well-known port numbers, 260–261
window scale, 295
windows, 47–50
TCP/IP protocol suite, 243
client/server architectures, 37–39
TE field (HTTP header), 982
Telnet
connection establishment, 43
connection termination, 46
delayed ACKs, 45
interactive traffic, 41–43
MSS, 44
Nagle algorithm, 46
TCP retransmission, 44
temporal redundancy, 448
removing, 987–989
temporary cookies, 729
terminating TCP connections, 272, 275
testing performance metrics, 950
hardware, 953
selecting data mix, 956–957
software, 952
test environment, 954–955
tools, 951
thick clients, 9, 83
thin clients, 83
threaded servers versus forking servers, 51, 53
threats (security), 160
three-way handshakes, 268
thresholds, reassigning connections, 705
throughput, multilayer switch metrics, 936
timestamps, 294
TLDs (top-level domains), 399
TN3270 servers, 74, 584–585
topologies
Data Center architecture, 13–14
access layer, 16–18
aggregation layer, 15
layers, 14
storage layer, 19
transport layer, 20–21
EIGRP, 859
fully switched, 804
Layer 2, 818
minimizing changes, 831
OSPF, 852
redundant Layer 2/Layer 3 designs, 139
access layer, 141–146
application architecture trends, 150–151
network infrastructure trends, 152–157
services, 146–150
VLANs, 804
TOS field, 248–250
total length field, 250
totally stubby area, 543
TRACE method (request header), 351
traceroute, 252
tracking
server health, 224
  in-band server health tracking, 224
  out-of-band server health tracking, 225
user sessions, 736
  Apache mod_session (case study), 740–741
  combining methods, 740
  cookies, 739
  form hidden fields, 737
  HTTP sessions with servlets (case study), 743–748
  URL rewriting, 738
traffic
  channeling, 507
  client NAT, 663
  encoding formats, 450–451
  Internet, HTTP, 328
load balancing
  architecture, 232–235
  cache load balancing, 210–211
  connection failover, 231
  connection persistence, 219
  connection tracking, 219
  firewall load balancing, 212–213
  flexibility, 659
  high availability, 226–230
  implications for application integration, 97–98
  Layer 4 load balancing, 216
  Layer 5 load balancing, 217
  process description, 215–216
  server health, 224–225
  server load balancing, 209–210
  session persistence, 219, 222–223
  stateful failover, 231
  stateless failover, 231
  sticky failover, 231
  VPN/IPSec load balancing, 211
multimedia transport formats, 454
  RTCP, 457–459
  RTP, 454
packetization, 453
patterns, 919–920
  Data Centers, 924–933
  Internet, 920–921
  intranets, 923
  load balancers, 939
  protocols, 922
rate limiting, 874
SSL, load balancing, 382–384
switching paths, 806
tagging, ISL, 503
transport rate, 448
traffic mix, 920
Trailer field (HTTP header), 977
Transfer-Encoding field (HTTP general header), 347
transactions
  middleware, 91
  UDP, 301–302, 305
transceivers, 493
  Fast Ethernet, 495
Transfer-Encoding headers, 343
taxtransparent caching, 684
taxtransparent devices, 824–825
taxtransport layer (Data Centers), 20–21
taxtransport protocols, UDP system calls, 40
taxtransport rate, 448
taxtransport security, 626
IPSec, 633
  IKE, 637
  security parameters, 638–639
TCP/IP layers, 634
SGC, 631
SSL, 626
  certificates, 629
  cipher suites, 632–633
  TCP/IP layers, 628
TRAPs, 700
troubleshooting
  DoS attacks, traffic rate limiting, 874
  Ethernet networks, frame size issues, 488
  firewall limitations, 178
  flooding, 831
  loops, 832–833
  server failure detection, 700, 704
    probes, 701
    SNMP, 701
  STP, failure detection, 513
trunks, 503
  configuring, 840
  creating, 505–506
TTL field, 251–252, 421
TTP response header, Status-Codes, 359

UDLD (Unidirectional Link Detection), 501, 832–833
UDP (User Datagram Protocol), 50–51, 299, 461.
  See also TCP
    header compression, 305
    header fields, 299–301
    probes, 712
    server failure handling, 54–55
    server failures, 54
    streaming, 464–465
    system calls, 40
    transactions, 301–302, 305
    versus TCP, 445–446
unicast, 499
unicast flooding, 499
unicast MAC addresses, dummy, 98
unicast packets, 471
Uniform Record Locators. See URLs
Uniform Resource Identifiers. See URIs
Universal Resource Names. See URNs
UNIX, system calls, 39–40
unsafe characters, 318
Upgrade field (HTTP header), 978
upgrading applications, 71
UplinkFast, 827–828
urgent pointer field (TCP), 266
URIs (Uniform Resource Identifiers), 310
  absolute/full, 312
  naming rules, 314–315
  relative/partial, 311
  request URI, 351
  URNs and URLs, 322
URL match, 779
URLs (Uniform Record Locators), 311, 315
  cookies, 776–778, 794–796
  encoding, 316
  hashing, 780–781
  relative and absolute, 316
  reserved characters, 318
  rewriting, 738, 776
  schemes, 316, 319
  stickiness, 776
  unsafe characters, 318
  URIs and URNs, 322
URNs (Universal Resource Names), 311, 320
  encoding, 320
  namespace, 321
  URIs and URLs, 322
uRPF, 872–873
user agents, 84
  browsers, 84
  client-side programming, 85
  helpers and plug-ins, 85
user mode, 35–36
User-Agent field (HTTP request header), 356
V

valuation, 197
Version field, 247
vertical scaling, 206
Via field (HTTP header), 978
video encoding, 987
video on demand (VoD), 445
video streaming, 442, 447
codes
  analog, 448
  comparison of, 452
  MPEG, 990–991
  popular encoding formats, 450–451
  removing spatial and temporal redundancy, 987–989
  slices, 991
redundancy, 448
transport rate, 452
transport formats, 454
  RTCP, 457–459
  RTP, 454
VIPAs (virtual IP addresses), DVIPAs, 587–588
virtual hosting
  configuring on web servers, 58–59
  IP-based, 59
  name-based, 61
  port-based, 60
  server health (case study), 718–720
virtual servers (virtual servers), 690
viruses, 165
VLAN ACLs (VACLs), 170
vlan dot1q tag native command, 506
VLANs, 170, 502, 802
  4096 VLANs, 514
  802.1s, 516
  access ports, 520
  autostate, 814
designing, 505–506
PVIDs, 503

SVIs, 813
topologies, 804
trunks, 503
virtualizing Data Center infrastructures, 810
VoD (video on demand), 445
VPN/IPSec load balancing, 211
VPNs (Virtual Private Networks)
  IPSec versus SSL, 639
  security, 196
VRRP, 527
  failure detection, 535
  master/backup election, 534
vservers (virtual servers), 690
VTAM (virtual telecommunications access method), 571
VTP (VLAN Trunking Protocol), 500, 504
  domains, defining, 504
  modes, 839

W

W3C (World Wide Web Consortium), 151
Warning field (HTTP header), 978
WCCP (Web Cache Control Protocol), 685
Web Cache Control Protocol (WCCP), 685
web servers, 57, 86
  directories, 58
  HTTP applications, 55–56
  inserting cookies, 1010
  server processes, configuring, 57
TCP parameters, configuring, 57
  virtual hosting, configuring, 58–61
web services, 151
weighted least connections predictor, 679
weighted round-robin predictors, 677
well-known port numbers, 260–261
window scale, 295
window size field (TCP), 266
windows, BDP, 50
windows (TCP), 47–48
Windows 95, enabling PMTUD, 290
Windows 98, enabling PMTUD, 290
Windows 2000
    configuring loopback interfaces, 996–998
    enabling PMTUD, 289–290
Windows Media Video, 451, 461
Windows NT
    configuring loopback interfaces, 1002
    enabling PMTUD, 289–290
wire format, 474
WML (Wireless Markup Language), 83
worms, 165
WSA (Web Services Architecture), 21

X–Z

XML (Extensible Markup Language), 79–83,
    696–697

zones (DNS), 400–402
    name servers, 418
    zone transfers, 418–420