INDEX

Numerics

3DES, 118
802.1Q standard, 33

A

access control, 127
    authentication, 127–128
    authorization, 129
    defending against IP spoofing, 104
    mitigating IP spoofing threats, 104
access VPNs, 115–117
accounting management, 182
administrative requirements for SLAs, 228
agents, 195
ANS.1 (Abstract Syntax Negotiation One), 193
APM (Application Performance Monitor), 233
application characterization, performing, 164
application layer attacks, 108
application servers, 13
ARPANET, 3
ASA (Adaptive Security Algorithm), 113
ASICs (Application Specific Integrated Circuits), 31
    reducing latency from load balancing, 36
assessing QoS policy needs, 162–163
    defining service levels, 164–165
    performing application characterization, 164
    performing network characterization, 163
asymmetric encryption, 119
attacks
    application layer, 108
    detecting with IDS, 44–45
    DoS, 104, 106
    IP spoofing, 103
        defense mechanisms, 104
    man-in-the-middle, 107
    network reconnaissance, 109
    packet sniffers, 102
        defense mechanisms, 103
    password, 106–107
    port redirection, 110
    Trojan horse, 110
    trust exploitation, 109
    unauthorized access, 110
    viruses, 110
authentication, 127
    biometrics, 128
    defending against packet sniffers, 103
    OTP, 128
    username/password, 128
authorization, 129
automatic paging, 187
availability, 27. *See also* high availability systems
    downtime, 75
    five nines, 75
    with Cisco Internet Systems Architecture, 63
AVVID (Architecture for Voice, Video, and Integrated Data)
    customer care service integration, 10
    QoS, 160

B

backend World Wide Web applications, 13
bandwidth, capacity, 28
best practices for maintaining high availability, 88
biometrics, 128
bottleneck points in Q-Tip architecture, 143
brute-force attacks, 106
buffering techniques, 30
building
    Cisco SAFE architecture, 129
        Corporate Internet module, 134–135
        E-Commerce module, 137–138
        Enterprise module, 130–131
        Management module, 131, 133
        Remote Access VPN module, 136–137
        Server module, 133–134
    service level model, 224
bundles, 210
bus architecture fabric, 32
business application servers, 13
business solutions
    customer care, 7
        IPCC, 9–10
        Land's End, 8–9
        service integration, 8

e-commerce, 11
World Wide Web service components, 12–13
e-learning, 15–17
case study, Genuity, 17–18
e-publishing, 20–21
supply chain management, 14
workforce optimization, 19–20
business synchronization, 222
reporting, 224
SLA expectations, setting, 223

C

CAs (certification authorities), 119
caching, transparent, 154
CANI (Constant and Neverending Improvement), 98
capacity, 28, 62
CCS (Cisco Content Smart Switches), 36
CDM (Content Distribution Manager), 53, 151–152
CDNs (Content Delivery Networks), 51, 53–54, 143
components, 144–145
CDM, 151–152
Content Edge Delivery, 150
Content Routing, 151
Content Switching, 145–149
Intelligent Network Services, 145
E-CDN, 155
e-learning solutions, 17
transparent caching, 154
central storage growth (Internet), 141
CERT (Computer Emergency Response Team), 105
CIS (Customer Interaction Suite), Lands' End customer care solution, 8
Cisco AVVID (Architecture for Voice, Video and Integrated Data)
customer care service integration, 10
QoS, 160
Cisco CSS 11000 series content service switches, 147
Cisco e-CDNs (enterprise CDNs), e-learning solutions, 17
Cisco host-based IDSs, features of, 126
Cisco Internet Reference Architecture
content engines, 46, 49–54
Content Routers, 55, 60
content switches, 34–37, 40
firewalls, 41–43
IDS, 44–45
Layer 3 switches, 28–29
redundancy, 32–34
sizing, 30–32
perimeter routers, 26–27
Cisco Internet System Architecture
connectivity, types of, 29
Cisco Internet Systems Architecture
benefits of using, 61
availability, 63
capacity, 62
connectivity, 62
manageability, 64
QoS, 63–64
security, 63
server placement, 60
Cisco IOS
QoS tools, 170–172
SAA (Service Assurance Agent), 232
Cisco IPM (Internetwork Performance Monitor), 234–235
Cisco network management solutions, 209
CiscoWorks2000 bundles, 210–216
CNR (Cisco Network Registrar), 216
QPM, 216
Cisco network-based IDS, features, 125
Cisco PIX firewall, exclusive features, 112–117
application awareness, 113
DoS Guards, 113
FragGuard, 114
intrustion detection, 114
NAT options, 115
redundancy, 116
site-to-site VPNs, 115–116
standards-based IPSec, 115
stateful inspection, 113
TCP intercept, 114
Virtual Reassembly, 114
VPN acceleration, 116
Cisco QPM (QoS Policy Manager), 235–236
Cisco SAFE architecture, 95, 129
Corporate Internet module, 134–135
E-Commerce module, 137–138
Enterprise module, 130–131
Management module, 131–133

Remote Access VPN module, 136–137
Server module, 133–134
Cisco Secure Policy Manager, 123
CiscoWorks 2000 SMS, 231–232
classification tools (QoS), 170–171
CLTs (Control List Technicians), 156
Comer, Gary C., 8
commands (SNMP), 196
comparing redundant and non-redundant topologies, 81–83
components
of Cisco Internet Reference Architecture
content engines, 46–54
Content Routers, 55, 60
content switches, 34–40
firewalls, 41–43
IDS, 44–45
Layer 3 switches, 28–34
perimeter routers, 26–27
of Internet system architecture, 25
Computer Associates, Inc., Unicenter TNG, 209
confidentiality, 96
congestion avoidance
buffering traffic, 30
Cisco IOS QoS tools, 171
connectivity
types of, 29
with Cisco Internet Systems Architecture, 62
Content Edge Delivery, 150
content engines, 46, 49, 51, 53–54
CDM, 53
CDNs, 51
content routers, 55, 60, 151
content switches, 34–40, 145–146
CSM, 147–149
maintaining session state, 40
control plane, 36
Corporate Internet module, Cisco SAFE architecture, 134–135
corporate training, e-learning solutions, 15–17
Genuity case study, 17–18
correlation rules, 199
cost-benefit analysis, total cost of ownership model, 72–74
creating SLAs, 225
crossbar switch fabric, 32
cryptography, defending against packet sniffers, 103
CSM (Cisco Content Switch Module), 147–149
customer care solutions, 7
Land's End, 8–9
service integration, 8–10

D

data encryption, 118–121
data traffic, QoS requirements, 161
DDoS (distributed denial-of-service) attacks, 105
decision-making process, Layer 3 switching, 31
decryption, 118–119, 121
defending against IP spoofing attacks, 104
defining
objectives for high availability systems, 76–77
security polices, 98–99
service levels (QoS), 164–165
delay, 162
Deming, Edward, 7
deploying large-scale QoS implementation, 166
with Modular QoS CLI, 167–168
with QoS Device Manager, 170
with QPM, 166–167
DES (Data Encryption Standard), 118
designing
highly available systems
defining objectives, 76–77
development road map, 78
EtherChannel, 86
failover mechanisms, 87–88
HSRP, 86–87
load balancers, 84
recovery procedures, 89–91
Spanning Tree, 85–86
top-down approach, 77
verifying design, 79
VRRP, 86–87
Internet system architecture. guidelines, 28
SLM solutions, integrating components from various vendors, 230
detecting
attacks with IDS, 44–45
failed components, 91
development road map, achieving high availability objectives, 78

devices, 44
availability, 27
CDN components, 144–145
CDM (Content Distribution Manager), 151–152
Content Edge Delivery, 150
Content Routing, 151
Content Switching, 145–149
Intelligent Network Services, 145
Cisco Internet Reference Architecture components
content engines, 46–54
Content Routers, 55, 60
content switches, 34–37, 40
firewalls, 41–43
IDS, 44–45
Layer 3 switches, 28–34
perimeter routers, 26–27
fault tolerant, building highly available systems, 80
hitless upgrades, 26
shadow routers, 234
VPN access support, 122
Digital IDs, 119
digital signatures, 121
director console (IDS), 45
disclosure (SNMP), 196
distributed switching, 31
DMZ (demilitarized zone), 43
DNS Guard feature (Cisco PIX firewall), 113
DNS mode (Content Routers), 56
request processing, 57, 60
documentation
network policies, 76
security policies, 98
defining, 98–99
implementing, 100
improving, 101
monitoring, 100
testing, 100
DoS attacks, 104–106
downtime, 75
MTBF, 80
outages, tracking causes of, 78
dumbbell architecture, 143
bottleneck points, 143
ISPs, 143
Dynamic NAT translation, 115

E

e-business solutions
customer care, 7
IPCC, 9–10
Land's End, 8–9
service integration, 8
e-commerce, 11
World Wide Web service components, 12–13
e-learning, 15–17
Genuity case study, , 17–18
e-publishing, 20–21
supply chain management, 14
workforce optimization, 19–20
E-CDN (Enterprise CDN), 155
E-Commerce architecture
non-redundant design, 83
redundant design, 83
E-Commerce module, Cisco SAFE architecture, 137–138
e-commerce solutions, 11
World Wide Web service components, 12–13
ECS (event correlation system), 199
e-learning solutions, 15, 17
Genuity case study, 17–18
employee training, e-learning solutions, 15–17
encryption, 118–119, 121
public keys, 120
VPN access, Cisco device support, 122
Enterprise module (Cisco SAFE architecture), 130–131
entitlement engines, 13
e-publishing solutions, 20–21
EtherChannel, 86
impact on bandwidth, 33
event correlation engine, 199
events
handling, 186–187
SNMP, 197–199

examples of external SLAs, 227–228
exclusive Cisco PIX features
application awareness, 113
DoS Guards, 113
FragGuard, 114
intrusion detection, 114
NAT options, 115
redundancy, 116
site-to-site VPNs, 115–116
standards-based IPSec, 115
TCP intercept, 114
Virtual Reassembly, 114
VPN acceleration, 116
external connections of World Wide Web, 13
external SLAs, 226
example, 227–228
extranet VPNs, 118

F

failover mechanisms, 87–88
failover mode (Cisco PIX firewall), 116–117
failure analysis, 89
failure detection, 91
fault management
event handling, 186–187
necessity of, 188
placing systems, 188
status polling, 185
troubleshooting, 189
fault tolerance
designing highly available systems, 80
in highly available systems, 89
FCAPS (Fault, Configuration, Accounting, Performance, and Security) model, 177
accounting management, 182
configuration management, 178–181
description, 180
process, 181
results, 181
tools, 181
fault management, 178
performance management, 183
security management, 183
feasibility of five nines availability, 75
features of Cisco IDSs
host-based, 126
network-based, 125
FIB (forwarding information base), 31
FIFO queuing, 159
filtering URLs, content filtering, 155–156
financial considerations of redundant systems, 72–74
firewalls, 41–43, 111
Cisco PIX, 112
exclusive features, 112–117
DMZ, 43
packet filtering, 111
stateful, 42, 112
five nines availability, 75
fixed-size buffers, 30
Flood Defender feature (Cisco PIX firewall), 113
flow-based switching, 31
FragGuard (Cisco PIX), 114
fragmentation of customer care services, 7
front end World Wide Web applications, 12
functional dependencies of SLAs, 229
functionality of perimeter routers, 27

G

general-purpose application servers, 13
Genuity, e-learning case study, 17–18
Get requests (SNMP), 194
GetBulk operation (SNMP), 196
GetNext requests (SNMP), 194
goals
of Internet system architecture, 5
service level definitions, 224
growth of Internet technologies, 3
Guard features of Cisco PIX, 113
guidelines of network management, 203–207

H

hash algorithms, 118
head of line blocking, 30
Hewlett Packard Openview, 208
HIDS (Host-based IDS), 108

high availability systems, 72
E-Commerce architecture
non-redundant design, 83
redundant design, 83
EtherChannel, 86
designing
defining objectives, 76–77
design verification, 79
development road map, 78
top-down approach, 77
failover mechanisms, 87–88
five nines, 76
HSRP, 86–87
implementing
with fault tolerant devices, 80
with redundant topologies, 80, 83
load balancers, 84
MTBF, 80
non-network considerations
operational best practices, 88
power consumption, 89
server fault tolerance, 89
Spanning Tree, 85–86
VRRP, 86–87
hitless upgrades, 26
Host Sensor 2.0, 126
host-based IDS features, 126
HSRP (Hot-Standby Routing Protocol), 86–87
HTTP requests, load balancing, 37

I

IBM Tivoli, 208
IDEA (International Data Encryption Algorithm), 119
IDSs (Intrusion Detection Systems), 44–45, 122–123
director console, 45
features
host-based, 126
network-based, 125
sensors, 123–124
placement, 125
implementing
high availability systems
with fault tolerant devices, 80
with redundant topologies, 80–83
large-scale QoS deployment, 166
business synchronization, 222–224
service level definitions, 224
with Modular QoS CLI, 167–168
with QoS Device Manager, 170
with QPM, 166–167
security policies, 100–101
improving security policies, 101
infrastructure of ISP networks, 143
input queuing, 30
integrating
customer care services
benefits of, 8
IPCC, 9–10
SLM components from various vendors, 230
integrity, 96
Intelligent Network Services, 145
interaction enablers, 13
internal SLAs, 226
Internet, central storage growth, 141
Internet Systems Architecture, 3–5, 25
benefits of using, 61
availability, 63
capacity, 62
connectivity, 62
manageability, 64
QoS, 63–64
security, 63
goal of, 5
server placement, 60
intranet VPNs, 118
intrusion detection (Cisco PIX), 114
IP spoofing, 103
defense mechanisms, 104
IPCC (Cisco IP Contact Center), 9–10
IPM (Internetwork Performance Monitor), 234–235
ISO (International Standards Organization), FCAPS model, 177
ISP's, network infrastructure, 143

J

jitter, 162
job training, e-learning solutions, 15–17

K

KAIZEN, 19
Kiwi Syslog Deamon, 197
Knowledge Bases, 80

L

Land's End, customer care services, 8–9
large-scale QoS deployment, 166
    with Modular QoS CLI, 167–168
    with QoS Device Manager, 170
    with QPM, 166–167
latency, load balancing induced, 36
Layer 3 switches, 28–29
    redundancy, 32, 34
    sizing, 30, 32
        queuing model, 30
        switch fabric, 32
        switching implementation, 31
life cycle model of security, 99
link efficiency mechanisms, 172
LMS (LAN Management Solution), 210–213
load balancers
load balancing, 84
    content switches, 34, 36–37, 40
    HTTP requests, 37
    latency, 36
logical network maps, 180

M

maintaining
    high availability, operational best practices, 88
    session state, 40
    SLAs, 225
manageability, Cisco Internet Systems Architecture, 64
managed devices, 194
Management module (Cisco SAFE architecture), 131–133
management protocols
    RMON, 201–202
    SNMP, 192–193
        Get requests, 194
        GetNext requests, 194
        Set operations, 194
        traps, 194
        versions, 195
    syslog, 202
    Telnet, 192
manager/agent model, 192
man-in-the-middle attacks, 107
marking tools (QoS), 170–171
masquerading, 196
measuring
    high availability, MTBF, 80
    service level performance, 232–233
media streams, link efficiency mechanisms, 172
message digest algorithms, 119
MIBs (Management Information Bases), 201
mission-critical data, QoS requirements, 161
mitigating security threats
    application layer attacks, 108
    DoS attacks, 106
    IP spoofing, 104
    network reconnaissance, 109
    packet sniffers, 103
    password attacks, 107
    unauthorized access, 110
modification of information, 196
Modular QoS CLI, large-scale QoS deployment, 167–168
monitoring
    security policies, 100
    SLAs, 191
monitoring tools, failure detection, 91
MTBF (meantime between failure), 80
MTTR (meantime to repair), 80
multi-switch deployment with EtherChannel, 34

N

NAT options (Cisco PIX), 115
network analysis tools, 164
network availability metrics (SLAs), 229
network characterization, performing, 163
network management
  FCAPS model, 177
    accounting management, 182
    configuration management, 178–181
    fault management, 178
    performance management, 183
    security management, 183
  guidelines, 203–204, 206–207
  policy documentation, 76
  RMON, 201–202
network performance metrics (SLAs), 229
network reconnaissance, 109
network response time thresholds, troubleshooting, 235
network-based IDS
  features, 125
  sensors, 123–124
NIDS (Network-based IDS), 108
NMSs (Network Management Systems)
  Cisco solutions, 209
    CiscoWorks 2000 bundles, 210–216
    CNR, 216
    QPM, 216
  fault management
    event handling, 186–187
    necessity of, 188
    placing systems, 188
    status polling, 185
    troubleshooting, 189
  performance management, 190–191
  RMON, 201–202
  SNMP, 192–193
    commands, 196
    disclosure, 196
    events, 197, 199
    Get requests, 194
    GetNext requests, 194
    MIBs, 201
    modification of information, 196
    Set operations, 194
    syslog messages, 197
    traps, 194
    versions, 195
  Telnet, 192
non-redundant design (E-Commerce architecture), 83
n-tier model, 25

O

Object Identifiers, 201
objectives for high availability systems, defining, 76–77
Old World system architecture, 3
online services
  customer care, 7–8
    IPCC, 9–10
    Land's End, 8–9
  e-commerce, 11
    World Wide Web service components, 12–13
  e-learning solutions, 15, 17
    Genuity case study, 17–18
  e-publishing solutions, 20–21
  supply chain management solutions, 14
  workforce optimization solutions, 19–20
Openview (Hewlett Packard), 208
operation level metrics (SLAs), 229
operational best practices, maintaining high availability, 88
OTPs (one-time passwords), 103
  authentication, 128
outages, tracking causes of, 78
output queuing, 30

P

packet filtering, 111
packet sniffers, 102
  defense mechanisms, 103
password attacks, 106–107
PAT (Port Address Translation), 115
peering points, 143

performance
capacity, 28, 62
of service levels, measuring, 232–233
SLA metrics, 229
troubleshooting with IPM, 234
performance management, 183, 190–191
performing
application characterization, 164
network characterization, 163
QoS policy needs assessment, 162–163
perimeter routers, 26–27
physical network maps, 180
placement
of fault management systems, 188
of IDS sensors, 125
of servers, Cisco Internet Systems Architecture, 60
policies
documenting, 76
QoS
defining service level, 164–165
performing application characterization, 164
performing needs assessment, 162–163
performing network characterization, 163
testing, 165
SLAs, 77
port redirection, 110
power consumption in highly available systems, 89
proactive management, 190
probes (RMON), 202
productivity, KAIZEN, 19
programs, 123
promiscuous mode (packet sniffers), 102
public key encryption, 118
CAs, 119
certificates, 120
publishing, e-publishing solutions, 20–21

Q

QoS (quality of service), 160
application characterization, performing, 164
business synchronization, 222
reporting, 224
setting SLA expectations, 223
Cisco IOS tools, 170–172
large-scale deployment procedures, 166–168, 170
link efficiency mechanisms, 172
necessity of, 159–160
network characterization, performing, 163
policies
needs assessment, 163
testing, 165
requirements for traffic types, 161
service levels, defining, 164–165
SLAs
administrative requirements, 228
cost, 229
creating, 225
external, 226–228
functional dependencies, 229
internal, 226
network availability metrics, 229
network performance metrics, 229
operation level metrics, 229
technical dependencies, 228
traffic conditioning, 172
with Cisco Internet Systems Architecture, 63–64
QoS Device Manager, large-scale QoS deployment, 170
QPM (QoS Policy Manager), 166, 216, 235–236
large-scale QoS deployment, 166–167
Q-Tip architecture, 143
bottleneck points, 143
ISPs, 143
quality assurance, Edward Deming, 7
queuing, 30, 159

R

reactive performance management, 190
read command (SNMP), 196
recovery procedures, implementing, 89–91
redundancy. *See also* high availability systems
E-Commerce architecture, designing, 83
highly available systems, designing, 80, 83
impact on total cost of ownership, 72–74

Layer 3 switches, 29–34
single point of failure, 83
VRRP, 86–87
Remote Access VPN module (Cisco SAFE architecture), 136–137
request/response model, 192
requirements of service level objectives, 221
retail services
Land's End customer care solution, 8
supply chain management solutions, 14
retrieving static Web server content, content engines, 49–54
revenue loss from security downtime, 97
RFC 2196, security policies, 97
RMON (Remote Monitor), 201–202
RSA Data Security, Inc, 119
RWAN (Routed WAN Management) solution, 213–214

S

SAA (Cisco IOS Service Assurance Agent), 232–233
SAFE architecture. *See* Cisco SAFE architecture
scalability, 28
security
access control, 127
attacks
application layer, 108
DoS, 104–106
IP spoofing, 103–104
man-in-the-middle, 107
network reconnaissance, 109
packet sniffers, 102–103
password, 106–107
port redirection, 110
Trojan horse, 110
trust exploitation, 109
unauthorized access, 110
viruses, 110
Cisco SAFE architecture, building, 129–138
Cisco Internet Systems Architecture, 63
confidentiality, 96
effect on revenue, 97
firewalls, 41–43, 111
Cisco PIX, 112–117
DMZ, 43
packet filtering, 111
stateful, 42
stateful inspection, 112
IDSs, 44–45, 122–123
director console, 45
host-based, 126
network-based, 125
sensors, 123–124
integrity, 96
life cycle model, 99
perimeter router functionality, 27
policies, 97–98
defining, 98–99
implementing, 100
improving, 101
monitoring, 100
testing, 100
update notification system, 45
VPNs, 117
Cisco device support, 122
data encryption, 118–119, 121
security management, 183
selecting QoS policies
defining service level, 164–165
performing application characterization, 164
performing needs assessment, 162–163
performing network characterization, 163
validation, 165
sensors
host-based, attack recognition database, 126–127
IDS, 45, 123–125
Server module (Cisco SAFE architecture), 133–134
servers
fault tolerance, 89
placement using Cisco Internet Systems Architecture, 60
service level definitions, 164–165, 224
service level objectives, 221
session state, maintaining, 40
Set operation (SNMP), 192–194
shadow routers, 234
shared-memory fabric, 32

shared-memory queues, 31
shunning, 45
single point of failure, 83
  eliminating, 91
site-to-site VPNs, 115–116
sizing Layer 3 switches
  queuing model, 30
  switch fabric, 32
  switching implementation, 31
SLAs (service-level agreements), 77
  administrative requirements, 228
  business synchronization, 222
    reporting, 224
    setting expectations, 223
  cost, 229
  creating, 225
  external, 226
    example, 227–228
  functional dependencies, 229
  internal, 226
  network availability metrics, 229
  network performance metrics, 229
  operation level metrics, 229
  service level objectives, 221
  service levels
    defining, 164–165
  technical dependencies, 228
SLM (service-levelmanagement)
  design integration, 230
  tools, 231
    CiscoWorks 2000 SMS, 231–232
    IPM, 234–235
    QPM, 235–236
SmartFilter, 156
SMS (Service Management Solution), 215
SNMP (Simple Network Management Protocol), 187, 192–193
  commands, 196
  disclosure, 196
  events, 197, 199
  Get requests, 194
  GetNext requests, 194
  masquerading, 196
  MIBs, 201
  modification of information, 196
  Set operations, 194
  syslog messages, 197
  traps, 194
  versions, 195
SODA (Self Organizing Distributed Architecture), 155
Spanning Tree, 85–86
splintered customer care services, 7
standards-based IPSec (Cisco PIX), 115
stateful failover, 116
stateful firewalls, 42
stateful inspection, 112–113
stateless failover, 116
static NAT translation, 115
status polling, 185
stickiness, maintaining session state, 38–40
supply chain management solutions, 14
switch fabric, 32
switching implementation, 31
symmetric-key encryption, 118
SYN attacks, 39
syslog, 202
syslog messages, 187, 197

T

TCP intercept (Cisco PIX), 114
technical dependencies of SLAs, 228
Telnet, 192
testing
  QoS policies, 165
  security policies, 100
third-party network management tools, 207
  Openview (Hewlett Packard), 208
  Tivoli (IBM), 208
  Unicenter TNG (Computer Associates), 209
thresholds, troubleshooting network response time, 235
throughput, 42
Tivoli (IBM), 208
TLI (Transport Layer Interface), 191
TMN (Telecommunications Management Network) Architecture, FCAPS model, 177–178
  accounting management, 182
  configuration management, 178–181

fault management, 178
performance management, 183
security management, 183
tools
Cisco IOS QoS, 170–172
configuration management, 181
network analysis, 164
SLM, 231
CiscoWorks 2000 SMS, 231–232
IPM, 234–235
QPM, 235–236
third-party network management, 207
Openview (Hewlett Packard), 208
Tivoli (IBM), 208
Unicenter TNG (Computer Associates), 209
top-down approach, high availability system design, 77
topologies, redundant versus non-redundant, 81–83
total cost of ownership, 72, 74
traffic
load balancing, 84
content switches, 34–40
QoS, 160–161
traffic conditioning, Cisco IOS QoS tools, 172
training employees, e-learning solutions, 15–18
transparent caching, 150, 154
trap command (SNMP), 194–196
traversal command (SNMP), 196
Trojan horse attacks, 110
troubleshooting
fault management systems, 189
with IPM, 234
trust exploitation, 109
tunneling, 117
Cisco device support, 122
data encryption, 118–119, 121
two-factor authentication, 103

U

unauthorized access, 110
unavailbility. *See* downtime
Unicenter TNG (Computer Associates), 209
Unified Internet system architecture, 5
update notification systems, 45
upgrades, hitless, 26
URLs, filtering, 155–156
user management, 13
username/password authentication, 128
utilization, 28

V

validating QoS policies, 165
variable-size buffers, 30
verifying high availability design, 79
Vesperman, Ann, 8
video traffic
link efficiency mechanisms, 172
QoS requirements, 161
Virtual Reassembly (Cisco PIX), 114
viruses, 110
VMS (VPN/Security Management Solution), 215
voice traffic
link efficiency mechanisms, 172
QoS requirements, 161
VPNs, 117
acceleration, 116
Cisco device support, 122
data encryption, 118–121
VRRP (Virtual Router Redundancy Protocol), 86–87
vulnerable network locations, IDS sensor placement, 125

W-Z

WCCP (Web Cache Communication Protocol), 154
Web servers
content engines, 46–54
Content Routers, 55, 60
placement, 60
workforce optimization solutions, 19–20
World Wide Web
cental storage growth, 141
services, 12
WRED (Weighted Random Early Detection), 162, 171
write command (SNMP), 196