Numerics

1-out-of-N sampling, 115
64-bit high-capacity counters, 240

A

AAA, accounting, 405. See also RADIUS accounting. See also accounting management; accounting MIBs
AAA, 405
application monitoring and profiling scenario, 26–30
billing scenarios, 43–45, 47–49
connection-based, 55
content-based, 55
destination-sensitive, 50–51
QoS billing, 53–54
source-sensitive, 52–53
VoIP billing, 55–57
volume-based, 49–50
capacity planning scenario, 31
link capacity planning, 31–32
network-wide capacity planning, 32–34
NetFlow, customer applications, 320–321
network monitoring scenario, 22–24
peering agreements, 37–43
RADIUS
Acct-Session-Id field, 423–424
VSAs, 419–422
security analysis, 57–61
time stamps, 602
traffic engineering scenario, 34–37
types of, 405
user monitoring and profiling scenario, 24–25
versus billing, 599
voice services, 573
standards and technologies, 573–576
with CDRs, 575
accounting management, 181–182
defining, 11–13
TMN/FCAPS model, 176
versus performance management, 17–20
accounting MIBs, 239, 247
CISCO-FRAME-RELAY-MIB, 247–249
for IPv6, 251–252
for multicast
IF-MIB, 253
RMON-MIB, 253
for telephony, 257–258
CISCO-CALL-HISTORY-MIB, 261–262
CISCO-VOICE-COMMON-DIAL-CONTROL-MIB, 261
CISCO-VOICE-DIAL-CONTROL-MIB, 260–261
Dial Control Management MIB, 259
SIP MIB, 262–265
for VLANs, 253–255
MPLS LSR MIB, 249–250
MPLS Traffic Engineering MIB, 250
traffic management and control
CISCO-CAR-MIB, 255
CISCO-CLASS-BASED-QOS-MIB, 256–257
Acct-Delay-Time AVP, 414
Acct-Session-Id field, RADIUS accounting, 423
versus VSAs, 424
accuracy of measured metrics (Cisco IP SLA), 455
active monitoring, 120–128
active voice performance measurement, 565
aggregation, 87
aggregators, 344
aging mechanism for NetFlow flows
on Catalyst switches, 328–329
on Cisco IOS routers, 327–328
APM (Application Performance Measurement) MIB, 289–291
application monitoring, 534–536
application traffic classification
Citrix ICA traffic, 437
NBAR classification, 435–436
subport classification, 436–437
application metrics, linking, 456
application-wide SMI data types, 195
applying performance management and accounting techniques, 74–80
Arbor’s Peakflow SP anomaly-detection system, 585
ART (Application Response Time) MIB, 289–291
ASN.1 (Abstract Syntax Notation 1), 228
ATM operation (Cisco IP SLA), 475–476
attacks
DoS, 580
postmortem, performing, 594–596
source of, tracing, 591–592
attributes of RADIUS, 409–414
VSAs, 418–422
authentication, RADIUS, 408
authNoPriv SNMP example configuration, 233–235
authorization, RADIUS, 408
authPriv SNMP example configuration, 235
average triggers (Cisco IP SLA), 497
AVPs (attribute/value pairs), 409, 411–414
Acct-Delay-Time, 414

volume-based, 603
peering agreements, 604–606
residential broadband access, 603–604
transit agreements, 604–606
billing agreements, 604, 606
black holes, 593
blocking security attacks, 59–60
BML (Business Management Layer), 178
business traffic class, 119
B-RAS (broadband remote access server), 404

B
backup options for SCTP, 341
bandwidth, capacity planning. See capacity planning
baselining, 68–70, 583
basic NBAR configuration example, 445–446
Bell, Alexander Graham, 559
BER (Basic Encoding Rule), 228
best-effort traffic class, 119
BGP AS Path, classifying, 91–93
BGP next-hop key-field, 362–363
BGP passive peer feature (NetFlow), collecting core traffic matrix, 554–555
BGP Policy Accounting, collecting core traffic matrix, 555
billing
destination-sensitive, 606
equipment departmental charge back, 608
flat rate, 609
for peer-to-peer traffic, 557
network blueprint, 600
service-based, 607–608
time- and distance-based, 606
time-based, 602
dial-in, 603
pWLANs, 602
versus accounting, 599
Cisco Catalyst switches
  RMON groups, configuring, 279–280
  Statistics and History group, configuring, 282
Cisco CNS NetFlow Collection Engine, 344–345
Cisco IOS NetFlow. See NetFlow
Cisco IOS Software
  Cisco IP SLA support, 501–502
  DSMON MIB support, 286
  IP Accounting
    Layer 3, supported IOS versions, 299
    MAC address support, 309
  NBAR support, 438–439
  NetFlow. See NetFlow
  RMON support, 277–278
  SMON MIB support, 288
  SNMP support, 229
Cisco IP SLA, 127
  ATM operation, 475–476
  CLI operations, 480–482
  CPU utilization, effect on accuracy, 504–506
  deploying, 507
  DHCP operation, 471
  distribution of statistics feature, 492–494
  DLSw+ operation, 479
  DNS operation, 471–472
  Enhanced Object Tracking, 499–501
  error statistics, 464
  features, 451
  Frame Relay operation, 473–475
  FTP operation, 470
  history collection feature, 494–495
  HTTP operation, 472
  ICMP operations, 464
    ICMP Echo operation, 465
    ICMP Path Echo operation, 465–466
    ICMP Path Jitter operation, 467
  IP SLA Responder, 459–462
  time-stamping, 461
  measured metrics, 453
    accuracy of, 455
    DHCP response time, 456
    DNS response time, 456
    HTTP response time, 456
    jitter, 454
  network delay, 454
  metrics
    frequency parameter, 457
  interpacket interval parameter, 458
  lifetime parameter, 459
  measuring, 457
  number of packets parameter, 458
  packet size parameter, 458
  start time parameter, 459
  timeout parameter, 458
  MPLS VPN awareness, 459
  network connectivity monitoring, 530–531, 534
  non-IP SLA responder-based operations, 463
  operational statistics, 464
  operations, 453
    configuring with CISCO-RTTMON-MIB, 482–483
    multiple operations, scheduling, 490–491
    random operations, scheduling, 491
    scheduling, 488–489
  summary table, 511–513
  verifying router support for, 483–486
  performance impact on devices, 503–504
  placement of, 508, 511
  responder-based operations, 463
  RTP-based VoIP operation, 477–479
  security considerations, 506–507
  supported devices and IOS versions, 501–502
  TCP Connect operation, 470
  threshold monitoring, 495–499
  threshold violation triggers, 497–498
  UDP operations
    UDP Echo operation, 468
    UDP Jitter operation, 468–469
    VoIP UDP Jitter operation, 469–470
  VoIP Call Setup Monitoring operation, 477
  VoIP Gatekeeper Registration Delay Monitoring operation, 476
  VoIP operations, example, 486–488
Cisco Network Planning Solution, 547
Cisco routers
  NetFlow version 8, 332–333
  non-TOS aggregation schemes, 334–335
  TOS aggregation schemes, 334–336
  RMON support, 279
CISCO-CALL-HISTORY-MIB, 261–262
CISCO-CAR-MIB, 255
CISCO-CLASS-BASED-QOS-MIB, 256–257
CISCO-DATA-COLLECTION-MIB, 244–246
CISCO-ENVMON-MIB, 244
CISCO-HEALTH-MONITOR-MIB, 244
CISCO-IF-EXTENSION-MIB, 241
CISCO-MEMORY-POOL-MIB, 244
CISCO-NETFLOW-MIB MIB
NetFlow SNMP operations, 346
CiscoPingCompleted trap, 242
CISCO-PING-MIB, 241
read-only objects, 242
read-write objects, 241
CISCO-PROCESS-MIB, 242
objects, 242–244
CISCO-RTTMON-MIB, configuring Cisco IP
SLA operations, 482–483
CISCO-VOICE-COMMON-DIAL-CONTROL-
MIB, 261
CISCO-VOICE-DIAL-CONTROL-MIB,
260–261
CiscoWorks Unified Operations Manager,
measuring voice performance, 572
Citrix ICA traffic classification (NBAR), 437
classification phase of six-stage security
operations model, 587–590
classifying application traffic
NBAR, 435–436
subport classification, 436–437
clear counters command, 309
clear ip accounting command, 300–302, 305–307
CLI operations
Cisco IP SLA, 480–482
Flexible NetFlow, 377–379
CMIP (Common Management Information
Protocol), 218–219
CMISE (Common Management Information
Service Element), 218
CMRs (call management records), 565
fields, 567–568
collecting
core traffic matrix
 pull model, 555
 push model, 551–555
NetFlow records, 585
collection monitoring
IP Accounting ACL, 306–308
IP Accounting (Layer 3), 302–303
IP Accounting MAC Address, 311–312
IP Accounting Precedence, 315–317
collection servers
placement, 154–56
real-time requirements, 156–157
columnar objects, 228
command accounting, 406
commands
Cisco IP SLA, enabling, 481–482
clear counters, 309
clear ip accounting, 300–302, 305–307
for IP Accounting (Layer 3), 299–300
for IP Accounting ACL, 304–305
for IP Accounting MAC Address, 309
for IP Accounting Precedence, 314
for NBAR configuration, 443
for NetFlow configuration, 345–346
for RADIUS, 415–416
for VoIP accounting with RADIUS, 425–428
ip nbar custom, 443
show commands, NBAR-related, 443–445
show ip accounting, 300, 305
show ip accounting access violations, 307
show ip accounting output-packets, 307
show ip cache flow, 325, 589
show ip cache verbose flow, 326
show ip nbar, 444
show ip sla application, 483–486
show rmon stats, 284
show snmp, 231
show snmp group, 233
show snmp view, 234
community string indexing, 254
comparing
active and passive monitoring, 103
data collection MIBs, 517–521
features of IP Accounting, 317
MIB functional areas, 238–239
Netflow information elements on different
export protocol versions, 338–339
network monitoring applications, 292–293
original NetFlow and Flexible NetFlow,
375–377
RADIUS accounting, Acct-Session-Id field
versus VSAs, 424
RADIUS and Diameter characteristics,
429–430
RADIUS and TACACS+, 406–407
configuration management, 181
configuring
Cisco Catalyst switches
  RMON groups, 279–280
  Statistics and History group, 282
Cisco IP SLA operations, CISCO-RTTMON-MIB, 482–483
IP Accounting (Layer 3), 302
IP Accounting ACL, 305–306
IP Accounting MAC Address, 311
IP Accounting Precedence, 315
MPLS-Aware NetFlow, 360–362
multicast egress accounting, example configuration, 363
multicast ingress accounting, example configuration, 363–365
NBAR
  basic NBAR configuration example, 445–446
  related commands, 443
NetFlow
  commands, 345–346
  on Catalyst switch, example configuration, 348–349
  version 5, example configuration, 347
  version 8, example configuration, 350
  version 9, example configuration, 350–351
NetFlow Input Filters, example configuration, 359–360
NetFlow Top Talkers, example configuration, 368–370
Sampled NetFlow, example configuration, 354–356
SNMPv2c, 230
SNMPv3, 231–233
  with user authentication, 235
  without user authentication, 233–235
connection accounting, 405
collection-oriented flows, 325
core traffic matrix
classifying, 98–99
collecting
  with pull model, 555
  with push model, 551–555
data collection. See also data collection protocols
categories of data, 94
event-based model, 145–146
export protocols
  FTP, 150–151
  NetFlow, 149–150
  SNMP, 148–149
MIBs, comparing, 517–521
NBAR summary, 449
push versus pull model, 144–145
required data, 93
data collection protocols
CMIP, 218–219
CMISE, 218
Diameter, 216–217
IPDR, 218
IPFIX, 208
  charter objectives, 211
  export protocol, 209–210
  RFCs, 211
metering methods, 102
  active monitoring, 103, 120–128
  passive monitoring, 104–120
NetFlow, 201
  export protocol, 204
  FlowSets, 204–205
  NetFlow version 9 export protocol, 202
template management, 205–206
template mechanism, 203
network design considerations, 151–152
PSAMP
  protocol specifications, 212–213
RFCs, 213–214
RADIUS, 214–215
RFCs, 215
TACACS+, 216
Data FlowSets, 204
data groups, 246
data integrity, ensuring, 168–169
data models, 190
DATA-COLLECTION-MIB, 529
de facto standards, 174
defining granularity of core traffic matrix, 548
delay metric, 454
deleting conceptual rows, 281
deploying
  Cisco IP SLA, 507
  NetFlow, 385–386
destination-sensitive billing, 606
deterministic sampling, 108–114
development from normal, 73
device-level architecture (NetFlow), 342
devices
  availability, testing, 121
  NBAR-supported, 438–439
  network elements, performance monitoring, 63–64
  performance monitoring, 526
  MIBs, 527–530
  RMON-supported, 277–278
  servers, performance monitoring, 64–65
DHCP operation (Cisco IP SLA), 471
DHCP response time, 456
Dial Control Management MIB, 259
dial-in services, time-based billing, 603
 Diameter, 216, 407, 428
  base protocol structure, 428
  intermediary agents, 428
RFCs, 217
discrete thresholds, 71
displaying
  NetFlow cache entries, 325
  SNMPv2c statistics, 231
distribution of statistics feature (Cisco IP SLA), 492–494
DLSw+ operation (Cisco IP SLA), 479
DNBAR (Distributed NBAR), 435
DNS operation (Cisco IP SLA), 471–472
DNS response time, 456
DoS attacks, 169, 580
DSCP data, classifying, 89–91
DSMON MIB, 284
  MIB object groups, 286
  principles, 286
  supported devices and IOS versions, 286

E

EML (Element Management Layer), 178
  enabling NetFlow, 385–386
Enhanced Object Tracking feature (Cisco IP SLA), 499–501
enterprise departmental charge back, 608
enterprise networks
  capacity planning, 544–545
  monitoring, 525
  optimized routing, 536–538
error statistics, Cisco IP SLA, 464
estimating core traffic matrix, 556
eTOM (enhanced Telecom Operations Map) model, 185
eTOM model, 185, 188
  FAB, 188
  OPS, 186
event-based data collection model, 145–146
EVENT-MIB, 268
element configurations
  authNoPriv SNMP, 233–235
  authPriv SNMP, 235
  multicast egress accounting, 363
  multicast ingress accounting, 363–365
  NetFlow
    on Catalyst switch, 348–349
    version 5 on router, 347
    version 8, 350
    version 9, 350–351
  NetFlow Input Filters, 359–360
  NetFlow Top Talkers, 368–370
  Sampled NetFlow, 354–356
  SNMPv2, 230
examples
  of basic NBAR configuration, 445–446
  of EXPRESSION-MIB, 266–268
  of Flexible NetFlow applications, 379–385
  of NBAR custom application, 446–447
  of NetFlow version 9 export protocol, 206–208
  of VoIP operations, 486–488
EXEC accounting, 406
export protocols (NetFlow), 204, 340
  FTP, 150–151
  NetFlow, 149–150
  SCTP, 341
  SNMP, 148–149
EXPRESSION-MIB, 265–268
external core matrix, 40
generating, 549–550

F
FAB (Fulfullment, Assurance, and Billing) model, 186–188
failover mode (SCTP), 342
fault management, 70, 74, 180
tresholds, 71–72
FCAPS (Fault, Configuration, Accounting, Performance, and Security) model, 174, 179–180
  accounting management, 181–182
  configuration management, 181
  fault management, 180
  performance management, 182–183
  security management, 183
features
  of Cisco IP SLA, 451
  of NBAR application classification, 436
  of NetFlow, 351–353
    Layer 2 and Security Monitoring Exports feature, 365–366
    Top Talkers, 366–368
fields
  of CDRs, 566
  of CMRs, 567–568
filtering, 105–106, 118–120
flat rate billing, 47, 609
Flexible NetFlow, 324, 370–371
  CLI operations, 377–379
  core traffic matrix, collecting, 552–553
  example applications of, 379–385
  Flow Caches, 374–375
  Flow Monitors, 371
  key-fields, 372–374
  packet sections feature, 374
  versus original NetFlow, 375–377
Flow Caches in Flexible NetFlow, 374–375
flow keys, 323
flow mask, 324
Flow Monitors, 371
flow sampling, 109
flow values, 323
flow-based Sampled NetFlow, 356–357
flows, 322
  aging mechanism
    on Catalyst switches, 328–329
    on Cisco IOS routers, 327–328
  connection-oriented, 325
  key-fields, 323–324
    BGP next-hop, 362–363
FlowSets, 204–205
formal languages, 190
Frame Relay, CISCO-FRAME-RELAY-MIB, 247–249
Frame Relay operation (Cisco IP SLA), 473–475
frequency parameter of metric measurement, 457
FTP operation (Cisco IP SLA), 470
full-mesh design, 508
full collection, 104–105
fundamentals of NetFlow, 322

G
general-purpose MIBs, 237
    for accounting and performance, 239
generating core traffic matrix, 548
    external versus internal core traffic matrix, 549–550
    granularity, defining, 548
GetBulk operations (SNMP), 197
GetNext operations (SNMP), snmpwalk utility, 236
Gnutella, limiting peer-to-peer traffic, 447
granularity of core traffic matrix, defining, 548
gavity model, estimating core traffic matrix, 556
groups
configuring on Cisco Catalyst switches, 279–280
in DSMON MIB, 286
in SMON MIB, 288–289
NAM-supported, 279
RMON 1, 275
RMON 2, 276

H
HC-RMON, 276
Headquarters OER configuration, 538
HIDSs, 591
history collection feature (Cisco IP SLA), 494–495
honeypots, 590
hot-potato routing, 141, 549
HTTP, subport classification, 436–437
HTTP operation (Cisco IP SLA), 472
HTTP requests, payload inspection, 447–448
HTTP response time, 456
hysteresis function (Cisco IP SLA), 495

I
IANA (Internet Assigned Numbers Authority)
assigned protocol numbers, 94
well-known ports, 95
ICMP operations (Cisco IP SLA), 464
ICMP Echo operation, 465
ICMP Path Echo operation, 465–466
ICMP Path Jitter operation, 467
ICPIF (Impairment/Calculated Planning Impairment Factor)
calculating, 564
voice performance, measuring, 563
Idd (Delay Impairment Factor), 563
identification phase of six-stage security operations model, 584–586
IIDSs, 590
Ie (Equipment Impairment Factor), 563
IETF RFCs
Diameter, 217
IPFIX-related, 211
obtaining, 269
PSAMP-related, 213–214
RADIUS, 215
RFC 2924, Accounting Attributes and Record Formats, 189
RFC 2975, Introduction to Accounting Management, 189–190
SMI-related, 199
SNMP-related, 200–201
IETF PSAMP working group, 338
IF-MIB, 253
ifTable, 236
ILMI (Interim Local Management Interface), 234
immediate Cache Flows, 375
immediate triggers (Cisco IP SLA), 497
impact
of Cisco IP SLA CPU utilization on accuracy, 504–506
of Cisco IP SLA on device performance, 503–504
include parameter (show ip cache flow command), 589
in-depth flow inspection, 587
Inform operation (SNMP), 197
information elements (NetFlow), comparing on different export protocol versions, 338–339
information modeling, 176, 190–191
Input Filters (NetFlow), 358
test configuration, 359–360
inspecting HTTP requests payload, 447–448
interfaces supported on NetFlow, 339
internal core matrix, 40
Internet management model, 191
interpacket interval parameter of metric measurement, 458
intranet as security threat, 582
intrusion attacks, 580
IP Accounting, 297
features, comparing, 317
IP Accounting (Layer 3), 298
collection monitoring, 302–303
configuring, 302
principles, 298
related IOS commands, 299–300
SNMP operations, 300
supported devices, 299
supported IOS versions, 299
IP Accounting ACL, 303
collection monitoring, 306–308
commands, 304–305
configuring, 305–306
principles, 304
SNMP operations, 305
supported devices, 304
supported IOS versions, 304

IP Accounting MAC Address, 308
collection monitoring, 311–312
commands, 309
configuring, 311
MIBs, 310–311
principles, 308
supported devices, 309
supported IOS versions, 309

IP Accounting Precedence, 312
collection monitoring, 315–317
commands, 314
configuring, 315
MIBs, 314–315
principles, 313
supported IOS versions, 313

NBAR PD MIB features, 440–441

IP Accounting (Layer 3), 298
collection monitoring, 302–303
configuring, 302
principles, 298
related IOS commands, 299
SNMP operations, 300
supported devices, 299
supported IOS versions, 299

IP Accounting ACL, 303
collection monitoring, 306–308
commands, 304–305
configuring, 305–306
principles, 304
SNMP operations, 305
supported devices, 304
supported IOS versions, 304

IP Accounting MAC Address, 308
collection monitoring, 311–312
commands, 309
configuring, 311
MIBs, 310–311
principles, 308
supported devices, 309
supported IOS versions, 309

IP telephony
metering sources, 561
network blueprint, 560–561
voice performance, measuring, 561
active measurement, 565
ICPFF, 563
MOS, 562
passive measurement, 564
standards and technology, 561
with CCM, 565, 568
with CiscoWorks Unified Operations Manager, 572
with NAM, 571

IPDR (Internet Protocol Data Record), 604
IPDR (Internet Protocol Detail Record), 217, 404
IPDR.org website, 218
IPDV (IP Packet Delay Variation), 454
IPFIX (IP Flow Information eXport), 208–209, 321
charter objectives, 211
export protocol, 209–210
RFCs, 211

IPM (CiscoWorks Internet Performance Monitor), 531

IPPM (IETF IP Performance Metric), 221
RFCs, 222
IPv4 multicast routing MIB, 253
IPv6 MIBs, 251–252

ITU-T recommendations
M.3010, 178, 184
M.3400, FCAPS, 179–180
accounting management, 181–182
configuration management, 181
fault management, 180
performance management, 182–183
security management, 183
ITU-T specification Y.1541, Network
Performance Objectives for IP-Based Services, 221
ITU-T standards, measuring voice performance, 561

J-K

jitter, 454
ICMP Path Jitter operation, 467
UDP Jitter operation, 468–469
key-fields, 89, 323–324
BGP next-hop, 362–363
in Flexible NetFlow, 372–374

L

Lakhina, Anukool, 549
Layer 2 and Security Monitoring Exports feature
(NetFlow), 365–366
lifetime parameter of metric measurement, 459
limiting peer-to-peer traffic with NBAR, 447
link capacity planning, 541, 543
linking metrics to applications, 456
links, performance monitoring, 526
MIBs, 527–530
LLA (logical layered architecture), 178
load balancing, 122
low-priority processing, 465

M

M.3010 recommendation, 178, 184
M.3400 recommendation, FCAPS, 179–180
accounting management, 181–182
configuration management, 181
fault management, 180
performance management, 182–183
security management, 183
managed devices, 192

measuring
metrics, 457
  frequency parameter, 457
  interpacket interval parameter, 458
  lifetime parameter, 459
  number of packets parameter, 458
  operations parameters, 457
  packet size parameter, 458
  start time parameter, 459
  timeout parameter, 458
standards and technology, 561
  with CCM, 565–568
  with CiscoWorks Unified Operations Manager, 572
  with NAM, 571
voice performance, 561, 564
  active measurement, 565
  CCM, 565–568
  CiscoWorks Unified Operations Manager, 572
  ICPiF, 563
  MOS, 562
  NAM, 571

memory consumption of Cisco IP SLA on devices, 503–504
metering devices
  positioning, 130–144
  sources in IP telephony, 561
metrics
  linking to applications, 456
  measuring, 453, 457
    accuracy, 455
    DHCP response time, 456
    DNS response time, 456
    HTTP response time, 456
    jitter, 454
    network delay, 454
MIB table, example data retrieval, 235–237
MIB-II objects, 240
MIBs, 193–194, 228. See also groups
  APM MIB, 289
    suggested default response times, 291
  supported IOS versions and devices, 291
  CISCO-CLASS-BASED-QOS-MIB, traffic classification, 543
  CISCO-DATA-COLLECTION-MIB, 244–246
  CISCO-ENVMON-MIB, 244
  CISCO-HEALTH-MONITOR-MIB, 244
NBAR (Network-Based Application Recognition) 623

CISCO-IF-EXTENSION-MIB, 241
CISCO-NETFLOW-MIB, NetFlow SNMP operations, 346
CISCO-PING-MIB, 241
read-only objects, 242
read-write objects, 241
CISCO-PROCESS-MIB, 242
objects, 243–244
data collection, accounting and performance features, 515–516
DATA-COLLECTION-MIB, 529
DSMON MIB, 284
MIB object groups, 286
principles, 286
supported devices and IOS versions, 286
EVENT-MIB, 268
EXPRESSION-MIB, examples, 266–268
for data collection, comparing, 517–521
for device and link performance monitoring, 527–530
for IP Accounting (Layer 3), 300
for IP Accounting ACL, 305
for IP Accounting MAC Address, 310–311
for IP Accounting Precedence, 314–315
for network connectivity monitoring, 530–531, 534
functional areas, comparing, 238–239
general-purpose, 237–239
Interface-MIB, objects, 240
MEMORY-POOL-MIB, 244
NBAR PD MIB, 439
IP accounting features, 440–441
objects
creating, 265
NBAR PD thresholds, 442–443
obtaining, 269–271
SMI, 194, 196
SMON MIB, 287
groups, 288–289
supported devices and IOS versions, 288
technology-specific accounting and performance MIBs, 247
CISCO-CAR-MIB, 255
CISCO-CLASS-BASED-QOS-MIB, 256–257
CISCO-FRAME-RELAY-MIB, 247–249
for IPv6, 251–252
for multicast, 253
for telephony, 257–265
for VLANs, 253–255
MPLS LSR MIB, 249–250
MPLS Traffic Engineering MIB, 250
transport technology-specific, 237
mini-RMON, 274
configuring on Cisco Catalyst switches, 282–284
MOS (Mean Opinion Score), 221
voice performance, measuring, 562
MPLS LSR MIB, 249–250
MPLS Traffic Engineering MIB, 250
MPLS-Aware NetFlow, 360–361
configuring, 360–362
core traffic matrix, collecting, 553–554
MPLS-Aware NetFlow Top Label Aggregation, 553
MRTG (Multi-Router Traffic Grapher), 86
MTBF (mean time between failure), 62
MTTR (mean time to repair), 62
multicast
egress accounting, example configuration, 363
ingress accounting, example configuration, 363–365
MIBs, 253
Multiple Operation Scheduling feature (Cisco IP SLA), 490–491

N

NAM (Network Analysis Module), 319
attacks, classifying, 589–590
modules, 278
network connectivity monitoring, 532
supported MIB groups, 279
voice performance, measuring, 571
naming conventions for call legs, 417
NAS (Network Access Server), 403
NBAR (Network-Based Application Recognition), 433
application classification, 435–436
attacks, classifying, 589
Citrix ICA traffic classification, 437
configuration commands, 443
configuring, basic NBAR configuration example, 445–446
custom application example, 446–447
inspecting HTTP request payload, 447–448
PD MIB, 439
  IP accounting features, 440–441
PDLMs, 437
peer-to-peer traffic, limiting, 447
Protocol Discovery feature, 434
  thresholds, 442–443
Protocol Discovery statistics group, 440
QoS features, 433
show commands, 443–445
subport classification, 436–437
supported devices, 438–439
supported protocols, 440
Top-N statistics, 441–442
unsupported capabilities, 438
NEL (Network Element Layer), 178
NetFlow, 201–202
  application monitoring, 534–536
  attacks, classifying, 587–589
  cache, 325
    entries, displaying, 325
    entry sizes, 326
    flow record expiry, 327
    parameters, 325
  Cisco CNS NetFlow Collection Engine, 344–345
  configuration commands, 345–346
  core traffic matrix, collecting, 551
  customer applications, 320–321
  deploying, 385–386
  device-level architecture, 342
  example Catalyst switch configuration, 348–349
  export protocols, 204, 340
    SCTP, 341
  Flexible NetFlow, 370–371
    CLI operations, 377–379
    Flow Caches, 374–375
    Flow Monitors, 371
    key-fields, 372–374
    packet sections feature, 374
  flow aging mechanisms
    on Catalyst switches, 328–329
    on Cisco IOS routers, 327–328
  flow mask, 324
  flows
    BGP next-hop key-field, 362–363
    connection-oriented, 325
    key fields, 323
    key-fields, 323
  FlowSets, 204–205
  fundamentals, 322
  information elements, comparing on different
  export protocol versions, 338–339
  Input Filters, 358
    example configuration, 359–360
  IPv6 environment monitoring, 322
  Layer 2 and Security Monitoring Exports
    feature, 365–366
  MPLS-Aware, configuring, 360–362
  NetFlow version 9 export protocol, 202
  Options Template FlowSet, 204
  records, collecting, 585
  router-based aggregation feature, 323
  Sampled NetFlow, 353–354
    example configuration, 354–356
    flow-based, 356–357
  SNMP operations, 346
  supported devices and Cisco IOS versions, 387
  supported interface types, 339
  template management, 205–206
  template mechanism, 203, 336
  Top Talkers feature, 366
    example configuration, 368–370
    match statement options, 367–368
  version 1, 330
  version 5, 330
    example router configuration, 347
  version 7, 330–331
  version 8, 332–333
    example configuration, 350
    non-TOS aggregation schemes, 334–335
    TOS aggregation schemes, 334–336
  version 9, 336
    example configuration, 350–351
    export protocol example, 206–208
    supported features, 351–353
  version 10, 337–338
    versus Flexible NetFlow, 375–377
NetFlow Collector, 344–345
NetFlow Multicast, 363
multicast egress accounting, example configuration, 363
multicast ingress accounting, example configuration, 363–365
net-snmp tools, 229
network accounting, 405
network availability, testing, 122–124
network blueprint
  for capacity planning, 543
  for IP telephony, 560–561
  security, 580
network connectivity, performance monitoring
  MIBs, 530–531, 534
network delay, 454
  versus processing delay, 460
network monitoring applications
  comparing, 292–293
network performance monitoring, 65–66
NFC (NetFlow Collection Engine), 319
  filters, 158
NGOSS (Next-Generation Operations Support Systems), 185
NIDS, 591
NML (Network Management Layer), 178
non-IP SLA responder-based operations, 463
normal Cache Flows, 374
NTP (Network Time Protocol), 405, 455

objects
  for CISCO-FRAME-RELAY-MIB, 247–249
  for CISCO-PING-MIB, 241–242
  for CISCO-PROCESS-MIB, 242–244
  for IPv6 MIBs, 251–252
  for MPLS LSR MIB, 249–250
  for MPLS Traffic Engineering MIB, 250
MIB-II, 240
obtaining
  IETF RFCs, 269
  MIBs, 269–271
OGM (Optimized Edge Routing), 536–538
OIDs (object identifiers), 193, 228
operational statistics (Cisco IP SLA), 464
operations (Cisco IP SLA)
  ATM operation, 475–476
  CLI operations, 480–482
  DHCP operation, 471
  DLSw+ operation, 479
  DNS operation, 471–472
  Frame Relay operation, 473–475
  FTP operation, 470
  HTTP operation, 472
  ICMP operations, 464
    ICMP Echo operation, 465
    ICMP Path Echo operation, 465–466
    ICMP Path Jitter operation, 467
multiple, scheduling, 490–491
placement of, 508, 511
random, scheduling, 491
router support for, verifying, 483–486
RTP-based VoIP operation, 477, 479
scheduling, 488
  Recurring function, 489
summary table, 511, 513
TCP Connect operation, 470
UDP operations
  UDP Echo operation, 468
  UDP Jitter operation, 468–469
  VoIP UDP Jitter operation, 469–470
VoIP Call Setup Monitoring operation, 477
VoIP Gatekeeper Registration Delay Monitoring operation, 476
operations parameters of Cisco IP SLA metric measurement, 457
  frequency, 457
  interpacket interval, 458
  lifetime, 459
  number of packets parameter, 458
  packet size, 458
  start time, 459
timeout, 458
optimized routing on enterprise networks, 536–538
Options Template FlowSet, 204–205
OSR (Operations Support and Readiness), 186
out-of-band-management, 177
OWD analysis, 129
performance management, 182–183
  combining with accounting management, 20–21
defining, 13–17
SLA parameters, 219–221
MIBs, 239
  CISCO-DATA-COLLECTION-MIB, 244–246
  CISCO-ENVMON-MIB, 244
  CISCO-HEALTH-MONITOR-MIB, 244
  CISCO-MEMORY-POOL-MIB, 244
  CISCO-PROCESS-MIB, 242–244
  versus performance monitoring, 14
performance monitoring. See also Cisco IP SLA
device and link performance, 526
MIBs, 527–530
network connectivity MIBs, 530–531, 534
periodic fix-interval sampling, 110
permanent Cache Flows, 375
PFC (Policy Feature Card), 330
ping tests, 126–127, 464
placing Cisco IP SLA operations, 508, 511
polling period, 246
positioning metering devices, 130–131
  edge versus core collection, 132–136
  embedded versus external device collection, 136–138
  flow lookup direction, 140–141
  ingress versus egress collection, 138–140
  technology-dependent special constraints, 141–144
  priority traffic class, 119
postmortem performing on network attacks, 594–596
preparation phase of six-stage security operations model, 583–584
principles
  of DSMON MIB, 286
  of RMON, 277
probabilistic sampling, 116–117
processing data records
  data aggregation, 160–164
  data record correlation, 164
  filtering, 157–159
  flow de-duplication, 165
  formatting, 165–166
  sampling, 159
  threshold monitoring, 159–160
processing delay versus network delay, 460
Protocol Discovery feature (NBAR), 434
  thresholds, 442–443
Protocol Discovery statistics group (NBAR), 440
  protocols supporting NBAR, 440
proxy servers, 263
PSAMP (Packet Sampling) working group, 212
  protocol specifications, 212–213
  RFCs, 213–214
publish and subscribe bus, 152
pull model
  core traffic matrix, collecting with BGP Policy Accounting, 555
  core traffic matrix, generating, 550
push model, 204
  core traffic matrix, collecting
    with BGP passive peer feature, 554–555
    with Flexible NetFlow, 552–553
    with MPLS-Aware NetFlow, 553–554
    with NetFlow, 551
  core traffic matrix, generating, 550
pWLANs, time-based billing, 602

Q

QoS
  CAR, 593
  NBAR features, 433
QRT (Quality Report Tool), 568

R

  accounting
    Acct-Session-Id field, 423–424
    VSAs, 419–422
    attributes, 409–414
    authentication, 408
    authorization, 408
    AVPs, 414
    commands, 415–416
    Diameter, 407, 428
      base protocol structure, 428
      intermediary agents, 428
    packets, 408
  RFC 2866 versus RFC 2865, 407
  RFCs, 215
    voice extensions, 416
      call legs, 416–418
      VSAs, 418–419
    VoIP accounting commands, 425–428
  random sampling, 108, 114–115
  Random Scheduling feature (Cisco IP SLA), 491
  RAS (Reliability, Availability, and Survivability), 180
  reaction stage of six-stage security operations model, 593–594
  reconnaissance attacks, 580
  Recurring function, scheduling Cisco IP SLA operations, 489
  recursive accounting, 38
  redirect servers, 263
  redundant mode (SCTP), 342
  registered ports, 95
  registrars, 263
  Remote Office OER configuration, 538
  responder-based operations (Cisco IP SLA), 463
  retrieving
    MIB table data, example, 235, 237
    SNMPv2c data, 231
  RFC 1213, MIB-II, 240
  RFC 2863, Interface-MIB, 240
  RFC 2865, 409
  RFC 2866, 409
  RFC 2924, Accounting Attributes and Record Formats, 189
  RFC 2975, Introduction to Accounting Management, 189–190
  RFC 3812, MPLS Traffic Engineering MIB, 250
  RFC 3813, MPLS LSR MIB, 249
  RFCs
    Diameter, 217
    IPFIX-related, 211
    obtaining, 269
    PSAMP-related, 213–214
    RADIUS, 215
    SMI-related, 199
    SNMP-related, 200–201
  RM&O (Resource Management & Operations), 188
RMON, 273
  groups, configuring on Cisco Catalyst switches, 279–280
  MIBs, DSMON MIB, 284–286
  NAM modules, 278
  principles, 277
  rows, 280, 282
  supported devices, 277–278
  supported IOS versions, 277–278
RMON 1 groups, 275
RMON 2, 274
  groups, 276
RMON-MIB, 253
  rogue access points, detecting, 61
  round-trip times, measuring, 454
  router-based aggregation, 324
  router-based aggregation feature (NetFlow), 323
  routing optimization, 536–538
  row (RMON), 280–282
RRDtool (Round Robin Database), 86
RSPAN (Remote SPAN), 278–279
RTMP (Real-Time Messaging Protocol), 568
RTP-based VoIP operation (Cisco IP SLA), 477–479
RTR (Response Time Reporter), 451

S

SAA (Service Assurance Agent), 451
SAMIS (Subscriber Account Management Interface Specification), 604
Sampled NetFlow, 353–354
  example configuration, 354–356
  flow-based, 356–357
sampling methods, 107
  deterministic, 109–114
  probabilistic, 116–117
  random, 114–115
  stratified, 117
scalar objects, 228
scenarios
  capacity planning
    for enterprises, 544–545
    for ISPs, 544–545
    link capacity planning, 541–543
for voice networks, 559–560
security-related, 579
scheduling
  Cisco IP SLA operations, 488
    Recurring function, 489
  multiple Cisco IP SLA operations, 490–491
  random Cisco IP SLA operations, 491
SCTP (Stream Control Transport Protocol), 340
  as NetFlow export protocol, 340–341
security. See also security management
  attack postmortem, performing, 594–596
  intrusion attacks, 580
  network blueprint, 580
  reconnaissance attacks, 580
  scenarios, 579
  source authentication, 167–168
  threats from intranet, 582
security management, 183, 582
  six-stage security operations model, 582
    classification stage, 587–590
    identification stage, 584–586
    preparation stage, 583–584
    reaction stage, 593–594
    tracing back source of attack, 591–592
security models and levels (SNMP), 199
  selecting, 175–176
service availability, testing, 124–126
service monitoring, 66–67, 536–538
Serviceability, 568
service-based billing, 607–608
show commands, NBAR-related, 443–445
show ip accounting access violations command, 307
  show ip accounting command, 300, 305
  show ip accounting output-packets command, 307
show ip cache flow command, 325, 589
show ip cache verbose flow command, 326
show ip nbar command, 444
show ip sla application command, 483–486
show rmon stats command, 284
show snmp command, 231
  show snmp group command, 233
  show snmp view command, 234
simple SMI types, 195
simply constructed SMI data types, 196
sinkholes, 590
SIP MIB, 262–265
six-stage security operations model, 582
   classification stage, 587–590
   identification stage, 584–586
   preparation stage, 583–584
   reaction stage, 593–594
   tracing back source of attack, 591–592
size-based flow sampling, 112–114
SLAs, 219
   generic, 68
   monitoring, 99
   network connectivity monitoring, 530–531, 534
parameters, 219–221
SM&O (Service Management & Operations), 188
SMI (Structure of Management Information),
   194–196, 227
   related RFCs, 199
SML (Service Management Layer), 178
SMON MIB, 287
   groups, 288–289
   supported devices and IOS versions, 288
SNMP, 148–149
   ifTable, 236
   managed devices, 192
   message-level security, 198
   MIBs, 193–194
      for data collection, 517–521
      for device and link performance
         monitoring, 527–530
      for IP Accounting (Layer 3), 300
      for IP Accounting ACL, 305
      for IP Accounting MAC Address, 310–311
      for IP Accounting Precedence, 314–315
      for network connectivity monitoring,
         530–531, 534
   NBAR PD MIB, 439–441
   SMI, 194–196
   related RFCs, 200–201
   security models and levels, 199
   traps, ciscoPingCompleted trap, 242
   versions, 196
SNMP operations (NetFlow), 346
   snmpget utility, arguments, 235
   SNMPv1, 196
   SNMPv2, 197
      configuring, 230
      data retrieval, 231
      statistics, displaying, 231
   SNMPv3, 198
      configuring, 231–233
      with user authentication, example
         configuration, 235
      without user authentication, example
         configuration, 233–235
   snmpwalk utility, 236
source of attack, tracing, 591–592
SPAN (Switched Port Analyzer), 278–279
spectrum of test, 457
spoofed source addresses, tracing, 591
SRLG (Shared Risk Link Group), 546
standards, 175–176
   accounting and performance management, 176
   de facto, 174
   for voice service accounting, 573–576
   selection process, 175–176
   voice performance, measuring, 561
start time parameter of metric measurement, 459
stateful inspection, 95
stateful proxy servers, 263
stateless proxy servers, 263
Statistics and History group (RMON 1)
   switch configuration, 282
statistics distribution collection (Cisco IP SLA),
   492–494
statistics for SNMPv2c, displaying, 231
Stewart, John, 582
stratified sampling, 117
Stratum 0, 405
streams, 340
subport classification, 436–437
summary of NBAR data collection criteria, 449
summary table of Cisco IP SLA operations,
   511–513
supported features on NetFlow version 9,
   351–353
suspending conceptual rows, 281
switched network environments, SMON MIB,
   287
   groups, 288–289
   supported devices and IOS versions, 288
syntax for net-snmp tools, 229
system accounting, 406
system clock synchronization, 455

T

TACACS+, 216, 406–407
Taft, Nina, 549
TCP connect, 456
TCP Connect operation (Cisco IP SLA), 470
technology-specific accounting and performance MIBs, 247
  CISCO-FRAME-RELAY-MIB, 247, 249
  for IPv6, 251–252
  for multicast
    IF-MIB, 253
    RMON-MIB, 253
  for telephony, 257–258
    CISCO-CALL-HISTORY-MIB, 261–262
    CISCO-VOICE-COMMON-DIAL-CONTROL-MIB, 261
    CISCO-VOICE-DIAL-CONTROL-MIB, 260–261
  Dial Control Management MIB, 259
  SIP MIB, 262–265
  for traffic management and control
    CISCO-CAR-MIB, 255
    CISCO-CLASS-BASED-QOS-MIB, 256–257
  for VLANs, 253–255
    community string indexing, 254
    MPLS LSR MIB, 249–250
    MPLS Traffic Engineering MIB, 250
Telecommuter OER configuration, 538
telephony, MIBs, 257–258
  CISCO-CALL-HISTORY-MIB, 261–262
  CISCO-VOICE-COMMON-DIAL-CONTROL-MIB, 261
  CISCO-VOICE-DIAL-CONTROL-MIB, 260–261
  Dial Control Management MIB, 259
  SIP MIB, 262–265
Template FlowSets, 204
templates (NetFlow), 203–206, 336
test packets, 452
testing
  device availability, 121
  network availability, 122–124
  service availability, 124–126
threats from intranet, 582
thresholds
  for NBAR Protocol Discovery, 442–443
  monitoring (Cisco IP SLA), 495–499
  violation triggers (Cisco IP SLA), 497–498
time- and distance-based billing, 606
time stamps, 602
time-based billing, 602
time-based flow sampling, configuring, 356–357
timeout parameter of metric measurement, 458
time-stamping, 461
TMF (TeleManagement Forum), eTOM model, 185
  FAB, 188
  OPS, 186
TMN (Telecommunications Management Network), 176
TMN framework, 184
TMN/FCAPS model, 176
TOM (Telecom Operations Map), 185
tools for capacity planning, 546
Top Talkers feature (NetFlow), 366
  example configuration, 368–370
  match statement options, 367–368
top-down accounting and performance management, TM-FCAPS model, 176
Top-N statistics, 441–442
Top-N traffic volume, identifying, 587
TOS aggregation schemes, 335–336
ToS bits, relationship to Precedence and DSCP bits, 95
traceroute, 127
tracing source of attacks, 591–592
traffic classification, CISCO-CLASS-BASED-QOS-MIB, 543
traffic engineering, 548
traffic management and control MIBs
  CISCO-CAR-MIB, 255
  CISCO-CLASS-BASED-QOS-MIB, 256–257
transit agreements, 38–39, 604–606
transport technology-specific MIBs, 237
traps (SNMP), 197
CiscoPingCompleted trap, 242

U

UAC (User Agent Client), 262
UAS (User Agent Server), 262
UDP as NetFlow export protocol, 340
UDP operations (Cisco IP SLA)
  UDP Echo operation, 468
  UDP Jitter operation, 468–469
  VoIP UDP Jitter operation, 469–470
UML (Unified Modeling Language), 190
unicast communication, 152
unsupported NBAR capabilities, 438
users, defining, 100–102
utilities for capacity planning, 546

V

VACM (View-based Access Control Model), 198
verifying router-supported IP SLA operations, 483–486
versions
  of SNMP, 196
  of Cisco IOS Software supporting NBAR, 438–439
VLAN-related MIBs, 253–255
  community string indexing, 254
VoD (video on demand), 608
voice extensions for RADIUS, 416
call legs, 416–418
VSAs, 418
  accounting, 419–422
voice gateways, 416
voice networks
  metering sources, 561
  performance, measuring, 561
    active measurement, 565
    CCM, 565, 568
    CiscoWorks Unified Operations Manager, 572
    ICPF, 563
    MOS, 562
    NAM, 571

passive measurement, 564
standards and technology, 561
scenarios, 559–560
voice quality, MOS, 221
voice service accounting
  standards and technology, 573–576
  with CDRs, 575
VoIP
  accounting with RADIUS, commands, 425–428
  per-call billing, 574
  RTP-based VoIP operation (Cisco IP SLA), 477–479
VoIP Call Setup Monitoring operation (Cisco IP SLA), 477
VoIP Gatekeeper Registration Delay Monitoring operation (Cisco IP SLA), 476
VoIP operations (Cisco IP SLA), example, 486–488
VoIP UDP Jitter operation, 469–470
volume-based billing, 603
  peering agreements, 604–606
  residential broadband access, 603–604
  transit agreements, 604–606
VRF table, 459
VSAs, 418–419
  accounting, 419–422
  RADIUS accounting versus Acct-Session-Id field, 424

W-X-Y-Z

W3C, 175
well-known ports, 95
x of y triggers (Cisco IP SLA), 497