INDEX

Numerics

32-bit signed integer values, converting to IP addresses, 420–422
802.1Q tunneling
  disabling, 185
  dropping frames, 196
802.1x Ethernet port authentication, 170–174

A

AAA, 436–437
  accounting, 444
  authorization, 442–444
  protocol selection, 437
  restricting access, 439–440
    RADIUS configuration, 440–442
    TACACS+ configuration, 440
AAR (automated alternate routing), 66–69
  configuring, 67–69
AccessXX.log application log, 355
accounting (AAA)
  configuring, 444
  using CDR data, 394
AD (Active Directory), directory integration
  planning, 375–377
  preparing the directory, 377–382
  User Creation Base, 383–387
adapter teaming, 96
adding hard drives to servers, 22
adds, moves, and changes for unsupported CallManager operations, 390
adjusting bandwidth consumption on WANs, 58–59
administrative control traffic, encrypting, 168
administrative operations, 388–389
administrator account modifications, caveats, 104
administrator training, 25–27
advanced services, 316
Alert Log format, 485
Alerting Timeout parameter (CallManager service), 320
alerts (RTMT), preconfigured, 477–478
  CallProcessingNodeCpuPegging, 478
  CodeRedEntry, 478
  CodeYellowEntry, 478
  CriticalServiceDown, 479
  DirectoryConnectionFailed, 479
  DirectoryReplicationFailed, 479
  ExcessiveVoiceQualityReports, 479
  LowAvailableDiskSpace, 480
  LowAvailableMemory, 480
  LowCallManagerHeartbeatRate, 480
  LowTcdServerHeartbeatRate, 480
  LowTFTPServerHeartbeatRate, 480
  MaliciousCallTrace, 480
  MediaListExhausted, 476, 480
  MgcpDChannelOutOfService, 481
  NonCallProcessingNodeCpuPegging, 481
  NumberOfRegisteredGatewaysDecreased, 481
  NumberOfRegisteredGatewaysIncreased, 481
  NumberOfRegisteredMediaDevicesDecreased, 481
  NumberOfRegisteredMediaDevicesIncreased, 481
  NumberOfRegisteredPhonesDropped, 481
  recipients, selecting, 475
  RouteListExhausted, 482
allocating IP addresses, 190–191
Alpha clusters, creating, 140
analyzers (syslog), 457
Annunciator, 497
application layer, 7
applications, CDR-related third-party, 428
assessing current data infrastructure, 5
  availability, 6–7
  documentation, 8
  security, 7–8
assigning privileges to functional groups, 359
ATM (Asynchronous Transfer Mode), WAN deployment architecture, 46–47
authenticating
  HSRP, 192–193
  routing protocol traffic, 191–192

authorization (AAA), configuring, 442–444
Automated Alternate Routing Enabled parameter, 322
AutoSecure feature (IOS routers), 166
availability, maintaining, 6–7
avoiding single points of failure, 161–163
AVVID Partner Program, CDR partners, 428–429

B

backup servers, versus backup target, 118
backup strategies, 112
    backing up CallManager servers, 113
    backing up Cisco Unity messaging repository, 115
    backing up frequently stored files, 114
    backing up gateways, 115–116
    backing up log files, 114
    backing up MOH sources, 114
    backing up router/switch configurations, 116
    backing up Subscriber, 113–114
    maintaining consistent private password phrases, 123–124
    mitigating misconfiguration disasters, 116–117
    performing backups with BARS, 119
        checking log files for errors, 122
        default backup targets, 120–121
        moving backup files, 122
    planning, 117
    scheduling backups, 118
    selecting appropriate backup server, 117
    staging, ensuring backup space, 123
bandwidth consumption, adjusting on WANs, 58–59
Barge enhancements for release 4.0(1), 503
BARS (Backup and Restore System), 113
    checking log files for errors, 122
    ensuring backup space, 123
    moving backup files, 122
    performing backups, 119
        default backup targets, 120–121
    Restore Wizard, 126
    restoring files, 125
baselining CDR data for jitter and latency, 415
BAT (Bulk Administration Tool), release 4.0 enhancements, 512
B-Channels, removing from service for maintenance, 324–325
billing, CDR data, 394
    collecting, 318
BPDU Guard, preventing BPDU Spanning-Tree attacks, 181–182
broadcast storm control, disabling, 186

C

CAC (Call Admission Control)
    locations-based, configuring, 62–65
    oversubscription, preventing, 60–65
call join feature (release 4.0), 502–503
Call Log format, 487–489
call park, customizing, 326
Call Park Display Timer parameter, 326
Call Park Reversion Timer parameter, 327
callingPartyLoginUserID field (CDR), 406
callingPartyNumber field (CDR), 409
callingPartyNumberPartition field (CDR), 409
CallManager service
    CDR data, collecting, 318
    parameters
        Automated Alternate Routing Enabled, 322
        Call Park Reversion Timer, 327
        Digit Analysis Complexity, 319
        Forward Maximum Hop Count, 321
        Forward No Answer Timer, 321
        International Number Prefix, 325
        Locations Trace Details Enabled, 319
        Max Forward Hops to DN, 322
        Maximum Number of Registered Devices, 320
        Maximum Phone Fallback Queue Depth, 320
        Offhook to First Digit Timer, 321
        Speed Dial Await Further Digits, 323
        Statistics Enabled, 322
        Status Enquiry Poll Flag, 319

T301, 320
T302, 321
CallManager Serviceability
Alarm Facility
configuring, 448
SNMP traps, 465
restarting services, 314
starting/stopping services, 313
CallProcessingNodeCpuPegging alert, 478
calls, diverting to voice mail, 504–505
CAR (CDR Analysis and Reporting Tool), 422
installing, caveats, 424
load settings, configuring, 422–423
quality of service, tracking, 426
reports
standard, 424–425
utilization, 425–426
users, tracking, 426
CatOS devices
CoS settings, ignoring, 174
OOB management, implementing, 167–168
cause codes
ITU Q.850, 410–413
MLPP, 406–407
cBarge, 503
CBR (constant bit rate), 46
CCM Directory Manager account, permissions, 381
CCM trace data, customizing with service parameters, 319
CCMAdministrator user account, 353
tracing logins, 361–362
ccmCallManagerFailed trap, 463
ccmGatewayFailed trap, 464
ccmGatewayLayer2Change trap, 464
ccmMaliciousCall trap, 465
ccmMediaResourceListExhausted trap, 464
ccmPhoneFailed trap, 463
ccmPhoneStatusUpdate trap, 463
ccmQualityReport trap, 465
ccmRouteListExhausted trap, 464
CDR data
32-bit signed integer values, converting to IP addresses, 420–422
collecting, 394–395
limiting entries, 395–396
method of, documenting, 15
service parameters, 395
enterprise parameters, 396–397
examples
of normal calls, 414–415
of unsuccessful calls, 416
exporting, 418–419
fields, 399–403
most commonly used, 409–410
updates for Release 4.0, 404–407
for billing, 394
jitter, baselining, 415
latency, baselining, 415
querying SQL database, 417
third-party applications, 428
time stamps, converting to human-readable form, 419–420
CDR UNC Path enterprise parameter, 345
centralized CallManager architecture, gateway selection, 85–87
centralized deployment
AAR, 66, 68–69
with ATM, 46
with Frame Relay, 45
with leased lines, 44–45
with MPLS, 47–48
with V3PN, 48
changing
service parameters, 316
service status, 312
Cisco CallManager Attendant Console enhancements (release 4.0), 514
Cisco CDR Insert service, 338
Cisco Customer Directory Configuration Plugin, 374
Cisco Extended Functions service, 339–340
Cisco Extension Mobility service, 342
Cisco IOS Software, AutoSecure feature, 166
Cisco Secure ACS, configuring for DC Directory communication, 437–439
Cisco Security Agent, hardening CallManager and voice application servers, 200–202
Cisco Serviceability Reporter service, 340, 484
Cisco Telephony Call Dispatcher service, 335
Cisco Unity messaging repository, backing up, 115
Cisco VT Advantage, 499
ciscoatGUID attribute (User object), 372
ciscoatUserProfile attribute (User Object), 372
ciscoatUserProfileString attribute (User object), 372

CiscoWorks syslog servers, 454–456
classes of service, documenting, 15–16
Cluster Security Mode enterprise parameter, 345
clusters
  backing up CallManager servers, 113
  backup server, selecting, 117
  CDR data collection
    enabling, 395
    limiting entries, 395–396
  Publisher, attempting MLA configuration changes while down, 355
  service parameters, 316
  Subscribers, 111
    backing up, 113–114
    duplicating, 126
    reinstalling, 126
CMI (Cisco Messaging Interface) service, 331–333
CMRs
  examples of normal calls, 414–415
  fields, 399–404
codecs, centralized region configuration, 60–61
CodeRedEntry alert, 478
CodeYellowEntry alert, 478
collecting CDR data, 318, 394–395
  limiting entries, 395–396
  service parameters, 395
commands
  copy running-config, 116
  NBSTAT, 132
comment field (CDR), 405
community strings, 459
  selecting, 460–461
comparing Event Viewer and syslog, 458
compartmentalizing services, 203
conferencing cause codes (MLPP), 407
conferencing infrastructure enhancements (release 4.0), 508
configuring
  AAR, 67–69
  accounting, 444
  authorization, 442– 444
  CallManager Serviceability Alarm, 448
  CAR, load settings, 422–423
  Cisco Secure ACS for DC Directory communication, 437–439
  directory access, 370, 372
  LFI with traffic shaping, 58
  LLQ, 52–55
  locations-based CAC, 62–65
  Region setting in CallManager Administration, 60–61
  RTMT, 473– 474
    alerts, 475
    polling interval, 476
  SNMP traps, 462– 465
  SRST, 71, 73
  syslog, multiple server configuration, 456–457
  WINS addresses, 129
connectivity
  restricting with PVLANs, 174– 175
  verifying before installation, 95
consistent use of private password phrases, 123–124
contract number, verifying, 97
converting
  32-bit signed integer values to IP addresses, 420–422
  CDR time stamps to human-readable form, 419–420
copy running-config command, 116
creating
  Alpha clusters, 140
  custom functional groups in MLA, 357
  custom reports from RISDC data, 484
    Alert Log format, 485
    Call Log format, 487–489
    Device Log format, 489–490
    Perfmon Log format, 490–491
    Server Log format, 485– 487
  custom user groups in MLA, 358
  feature inventory database, 9–14
  security policies, 161
  training curriculum, 24–26
    for administrators, 26–28
  user information packets, 34
  user-specific accounts in MLA, 357
CriticalServiceDown alert, 479
cron, 456
cRTP (Compressed Real-Time Transport Protocol), adjusting bandwidth consumption, 58
CSA (Cisco Security Agent), 107
CTIManager service, 334
CTL (Cisco Certificate Trust List) Provider service, 338–339
current voice applications, assessing, 18–20
custom functional groups, creating in MLA, 357

custom reports
Alert Log format, 485
Call Log format, 487–489
creating from RISDC data, 484
Device Log format, 489–490
Perfmon Log format, 490–491
Server Log format, 485
Service Log format, 486–487
custom user groups, creating in MLA, 358
customizing
call park, 326
CCM trace data with service parameters, 319
cutover method, establishing, 31–33

D

DAI (Dynamic ARP Inspection), enabling, 176–179
daily system monitoring, importance of, 436
Data Collection Enabled parameter (RIS Data Collector service), 337
data link layer. *See* Layer 2 security
data retention. *See* backup strategies
Database Layer Monitor service, 338
database synchronization, verifying, 105
dateTimeConnect field (CDR), 410
dateTimeDisconnect field (CDR), 410
dateTimeOrigination field (CDR), 410
dateTimeStamp field (CDR), 410
DC Directory, communicating with Cisco Secure ACS, 437–439
decimal call clearing cause codes (ITU Q.850), 410–413
dedicated servers, 303
TFTP, 329
Default MOH Volume Level parameter (MOH Audio Translator service), 336
Default Network Locale enterprise parameter, 345
Default User Locale enterprise parameter, 345
dependencies among services, 301–302
deploying
SRST, 73–76
WANs
with ATM, 46–47
with Frame Relay, 45
with leased lines, 43, 45
with MPLS, 47–48
with V3PN, 48
desktop video telephony, 498–501
destCause_value field (CDR), 404, 410
destIpAddr field (CDR), 410
destIpPort field (CDR), 404
destPrecedenceLevel field (CDR), 404
destVideoCap_Codec field (CDR), 404
destVideoCap_Resolution field (CDR), 405
destVideoTransportAddress_IP field (CDR), 405
destVideoTransportAddress_Port field (CDR), 405
Device Log format, 489– 490
Device Search feature (RTMT), 483
Device Security Mode enterprise parameter, 345
devices
memory requirements, 22
selecting, 21
device-to-CallManager authentication, 514
DHCP snooping, 176
dial plan, documenting, 14–15
dial tone, selecting for OnNet and OffNet calls, 328
Digit Analysis Complexity parameter, 319
DirAndUIXX.log application log, 354
directory access, 367–369
configuring, 370–372
directory integration, 367–368, 372–373
planning, 375–377
preparing the directory, 377–382
User Creation Base, 383–387
DirectoryConnectionFailed alert, 479
directoryNumPartition field (CDR), 409
DirectoryReplicationFailed alert, 479
DirTrfr (direct transfer), 506
disabling
802.1Q tunneling, 185
broadcast storm control, 186
DTP, 184
IIS on CallManager servers, 363

Layer 2 control protocols, 179–185
VTP, 183
displaying
service parameters for every server, 317
service status, 312
distinctive rings, enabling for OnNet and OffNet calls, 325
diverting calls to voice mail, 504–505
DNA (Cisco Dialed Number Analyzer), customizing data with service parameters, 319
documenting
CallManager upgrades, 150–151
CDR method, 16
classes of service, 15–16
current infrastructure, 8
dial plan, 14–15
existing hardware, 20–21
server characteristics, pre-installation checklist, 93–94
domains (Window), CallManger server participation, 100
DoS (denial of service) as security threat, 159
downloading
CallManager maintenance releases, 144
Remote Desktop Client, 468
Windows OS upgrades, 144
downtime, surviving with SRST, 69–71, 73–76
PSTN calling during fallback, 82– 84
voice mail during fallback, 78– 80
dropping
802.1q frames on IP Phones, 196
parties from Ad Hoc conferences, 505
DTP, disabling, 184
dual phone and flash cut migration method, 33
duplicating Subscribers, 126

E

Enable Dependency Records enterprise parameter, 344
enabling
Access log file for MLA, 356
CDR data collection, 394–395
time synchronization, 398–399
trace logs for MLA, 355
encrypting administrative control traffic, 168
endpoint provisioning, 207
endpoint image authentication, 208
enrollment, 208–215
operation, 215–218
ensuring
adequate backup space, 123
CallManager upgrade version compatibility with Windows OS, 141–142
enterprise-related CDR parameters, 396–397
Epoch time, converting to human-readable form, 419–420
escalation plans, 35
establishing
escalation plans, 35
operations procedures, 36–38
problem reporting methods, 35
rollout plan, 28
adding phones, 28–30
cutover method, 31–33
second-day support centers, 34–35
Ethernet port authentication, 170–174
Event Viewer, 457–458
examples of CDRs
for normal calls, 414–415
for unsuccessful calls, 416
ExcessiveVoiceQualityReports alert, 479
exporting CDR data, 418–419

F

failed Subscribers, reinstalling, 126
feature inventory database, creating, 8–11, 13
feature list for release 4.0(1), 493
Ad Hoc conference party drop, 505
annunciator, 497
BAT enhancements, 512
call join, 502–503
cBarge, 503
Cisco CallManager Attendant Console enhancements, 514
conferencing infrastructure enhancements, 508
desktop video telephony, 498–501
DirTrfr, 506
display of configurable call forward information, 505–506

hunt group ehancements, 508, 510
iDivert, 504–505
IPMA enhancements, 506–507
management and monitoring enhancements, 513
MCID, 510–511
MLA enhancements, 513
MLPP, 494–496
multiple calls per line appearance, 502
privacy, 504
published API enhancements, 511–512
Q.SIG enhancements, 496-497
security enhancements, 514–515
Service URL, 505
SIP trunk signaling interface, 497–498
fields
of CDR data, 399–403
frequently searched fields, 409–410
updates for release 4.0, 404–407
of CMRs, 403–404
of syslog messages, 447
FIFO (first in, first out) queuing, 49
filtering network traffic, 187–190
with NBAR, 189-190
with PACLs, 188
finalCalledPartyLoginUserID field (CDR), 406
finalCalledPartyNumber field (CDR), 409
finalCalledPartyNumberPartition field (CDR), 409
First Digit Timeout parameter (CallManager service), 321
flash cut, 31
forcing NetBIOS name lookups, 128
Forward Maximum Hop Count parameter, 321
Forward No Answer Timer parameter, 321
fractional PRI, 325
Frame Relay
jitter, reducing with LFI, 57
WAN deployment architecture, 45
frequently stored files, backing up, 114
functional groups
creating custom groups in MLA, 357
permissions, 349–352
overlapping, managing, 359–360
privileges
assigning, 359
user groups, 349

G-H

GARP, ignoring on IP Phones, 194–195
gateways
backing up, 115–116
selecting for centralized CallManager architecture, 85–87
generating
CAR utilization reports, 425–426
privileges report in MLA, 356
globalCallID_callId field (CDR), 409

H323 FastStart Inbound parameter, 326
hard drives, adding to servers, 22
hardening
access via IP phones, 194–196
CallManager and Voice application servers, 197
Cisco-provided hardening, 197
services, compartmentalizing, 203
with account/password policies, 204–207
with Cisco Security Agent, 200–202
with patches and updates, 197, 199
with Secure Remote Administration, 202–203
with virus protection software, 200
routers and switches, 165–167
hardware, documenting, 20–21
host-based monitoring, 434
HP Insight Agents, 462–463
HR, updating personnel changes in MLA, 362
HSRP (Hot Standby Routing Protocol), authenticating, 192–193
hunt group enhancements (release 4.0), 508–510

I

iDivert, 504–505
ignoring
  CoS settings on CatOS devices, 174
  GARP on IP Phones, 194–195
IIS, disabling on CallManager servers, 363
implementing, OOB management on IOS/CatOS devices, 167–168
infrastructure
  security feature checklist, 164–165
  documenting, 8
installing CallManager, 91
  adapter teaming, 96
  consistent server passwords, creating, 101
  contract number, verifying, 97
  installation media, preparing, 94
  LMHOSTS file, updating, 100
  locating key directories and files, 98–99
  logistics checklist, 92–93
  network connectivity, verifying, 95
  post-installation tasks
    adding Cisco virus protection software, 107
    caveats against unsupported software, 103
    double-checking pre-installation checklist, 102
    maintaining current user accounts, 104
    maintaining OS parameters, 103
    patching, 104
    verifying database synchronization, 105
    verifying optimal NIC settings, 105–106
  power supply connections, verifying , 95
  reading release notes, 97–98
  server characteristics, documenting, 93–94
  service releases, 152–155
  VNC, 470–471
  Windows domain participation, avoiding, 100
installing CAR, caveats, 424
integrity, violations of, 160
Interdigit Timeout parameter (CallManager service), 321
International Number Prefix parameter, 325
inventory database, creating, 9–14
IOS routers, implementing OOB management, 167–168
IOS-based gateways, backing up, 115–116
IP addresses
  allocating, 190–191
  converting from, 32-bit signed integer values, 420–422
IP Manager Assistant service, 341
IP phones
  802.1Q frames, dropping, 196
  directory access, configuring, 370–372
  GARP, ignoring, 194–195
IP RTP priority, minimizing latency on WANs, 50–52
IP Voice Media Streaming App service, 333–334
IPMA enhancements (release 4.0), 506–507
IPSec, securing interserver communication, 219
ISAPI (Internet Service API) filter, 353
ISAPIFilterXXXXXX.txt application log, 354
ITU Q.850, cause codes, 410–413

J–L

jitter
  CDR data, baselining, 415
  reducing on WANs, 56
    with LFI, 56–57

labeling backup tapes, 117
lastRedirectDnPartition field (CDR), 409
lastRedirectRedirectOnBehalfOf field (CDR), 405
lastRedirectRedirectReason field (CDR), 406
latency, baselining CDR data, 415
Layer 2 security
  802.1Q tunneling, disabling, 185
  broadcast storm control, disabling, 186
  connectivity, restricting, 174–175
  control protocols, disabling, 179–184
  CoS settings, restricting, 174
  DAI, enabling, 177–179
  DHCP replies, denying, 175
  DHCP snooping, 176
  Ethernet port access, restricting with Ethernet port authentication, 170–174
  HSRP, authenticating, 193
  IP addresses, allocating, 191
  MAC addresses, restricting on switch ports, 169
  network traffic, filtering, 187

on IP Phones
dropping, 802.1Q frames, 196–197
ignoring GARP, 194–195
voice traffic, prioritizing, 186–187
Layer 3 security
HSRP, authenticating, 192
IP addresses, allocating, 190
network traffic, filtering, 188–190
routing protocol traffic, authenticating, 191–192
layers of OSI reference model, 163
LDAP (Lightweight Directory Access Protocol), 353
leased lines, WAN deployment architecture, 43–45
LFI
reducing jitter on Frame Relay networks, 57
reducing jitter on point-to-point links, 56
limiting
CDR database entries, 395–396
DHCP responses with Option, 82, 175
Linux-based syslog servers, configuring, 451–454
LLP, minimizing latency on WANs, 52–55
LLQ, minimizing latency on WANs, 50
LMHOSTS file
name resolution, 129–131
updating, 100
load settings (CAR), configuring, 422–423
LocalNetPriority, 377
locating key directories and files for installation, 98–99
locations-based CAC, configuring, 62, 64–65
Locations Trace Details Enabled parameter, 319
Lock-and-Key security, 469
log files
backing up, 114
for release 4.x, 354
logistics checklist, CallManger installation, 92– 93
LowAvailableDiskSpace alert, 480
LowAvailableMemory alert, 480
LowCallManagerHeartbeatRate alert, 480
LowTcdServerHeartbeatRate alert, 480
LowTFTPServerHeartbeatRate alert, 480

M

MAC addresses, restricting on switch ports, 169–170
maintaining
availability, 6–7
password consistency across servers, 101
maintenance releases, downloading, 144
MaliciousCallTrace alert, 480
management and monitoring enhancements (release 4.0), 513
managing
overlapping permissions in MLA, 359–360
trace facility file sizes, 467–468
mandatory services, 302–305
mass storage media, labeling, 117
master file (Windows), reading, 152
Max CDR Records parameter (Database Layer Monitor service), 338
Max Forward Hops to DN parameter, 322
Maximum Ad Hoc Conference parameter, 327
Maximum Login Time parameter (Cisco Extension Mobility service), 342
Maximum MeetMe Conference Unicast parameter, 327
Maximum Number of Registered Devices parameter, 320
Maximum Phone Fallback Queue Depth parameter, 320
MCID (malicious call identification), 510–511
MCSs (Media Convergence Servers), 111
MediaListExhausted alert, 476, 480
messages, syslog
CallManager Serviceability Alarm, 448
format, 447
router logging, 449–451
severity levels, 446
severity levels, selecting, 448
MgcpDChannelOutOfService alert, 481
MIBs, 459
Microsoft Excel, converting UTC and IP addresses, 421–422
Microsoft Performance, 466
migration, methods of, 31
flash cut, 31
PBX migration, 31–33

minimizing latency on WANs, 49–50
with IP RTP, 50–52
with LLP, 52–55
misconfigurations, mitigating disaster with backup strategy, 116–117
mismatched SQLSvc passwords, troubleshooting, 134
mitigating security threats
routers and switches, hardening,165–167
on CallManager and voice application servers, 197–207
on IOS/CatOS devices, 168
on Layer 2
802.1Q tunneling, disabling, 185
broadcast storm control, disabling, 186
connectivity, restricting, 174–175
control protocols, disabling, 179–185
DAI, enabling, 176, 178–179
default native VLAN value, reassigning, 184
DHCP snooping, 176
dropping 802.1Q frames on IP phones, 196–197
DTP, disabling, 184
ignoring CoS settings on CatOS devices, 174
ignoring GARP on IP Phones, 194–195
limiting DHCP responses, 175
network traffic, filtering, 187–190
voice traffic, prioritizing, 186–187
VTP, disabling, 183
with Ethernet port authentication, 170–174
with port security, 169–170
on Layer 3
HSRP, authenticating, 192–193
IP addresses, allocating, 190–191
routing protocol traffic, authenticating, 191–192
MLA (multilevel administration), 349, 458
Access file, monitoring, 356, 360
access, restricting, 362
application logs, 354
attempting configuration changes while Publisher is down, 355
CCMAdministrator user account, 353
tracing logins, 361–362
custom functional groups, creating, 357
custom user groups, creating, 358
enabling for release 4.x, 355
enhancements to release 4.0, 513
functional groups, 349
assigning privileges, 359
permissions, 349–352
overlapping permissions, managing, 359–360
privileges report, generating, 356
security audits, 364
standard user groups, permissions, 350–352
super user, 349
trace logs, enabling, 355
unauthorized web browser access, preventing, 363
updates from previous release, 353
backup and restore operations, 354
disabled features, 353
log file location, 354
user-specific accounts
checking against HR, 362
creating, 357
MLPP (Multilevel Precedence and Preemption), 494–495
cause codes, 406–407
conferencing cause codes, 407
precedence calls to another network, 496
precedence calls withing cluster, 496
precedence values, 407
modifying
administrator account, caveats against, 104
OS parameters, caveats against, 103
MOH Audio Translator service, 335–336
Default MOH Volume Level parameter, 336
MOH sources, backing up, 114
monitoring
CAR, 424–426
media resouces with RTMT
media resouces
monitoring with RTMT, 475
MLA Access log file, 356, 360
trunk utilization with RTMT, 476
utilization reports, 425–426
monitoring tools, 435
AAA, 436–437
accounting, configuring, 444
authorization, configuring, 442– 444

protocol selection, 437
restricting access, 439–442
daily monitoring, 436
Microsoft Performance, 466
SNMP, 459–460
community strings, 460–461
traps, 462– 465
SRA, 466
syslog, 445
analyzers, 457
CallManager Serviceability Alarm, 448
CiscoWorks syslog server, 454–456
cron, 456
Event Viewer, 457–458
facilities, 446
Linux-based server configuration, 451–454
message format, 447
message severity levels, 446
multiple server configuration, 456–457
router logging, 449–451
severity level, selecting, 448
Terminal Services, 468
security vulnerabilities, 469–470
unsupported agents, 435
versus host-based monitoring, 434
moving system into production, 152
MPLS (Multiprotocol Label Switching), WAN deployment architecture, 47–48
Multiple Login Behavior parameter (Cisco Extension Mobility service), 343
multiple syslog server configuration, 456–457
multiple-domain AD forest, placing User Creation Base, 383

N

name resolution
LMHOSTS file, 129–131
WINS, configuring, 129
National Number Prefix parameter, 325
native VLAN value, reassigning, 184
NBAR (Network-Based Application Recognition), filtering network traffic, 189–190
NBTSTAT command, 132
NetBIOS
forcing name lookups, 128
name resolution issues, troubleshooting, 128
resolving names with LMHOSTS file, 129–132
network layer. *See* Layer 3 security
network traffic, filtering, 187–190
with NBAR, 189–190
with PACLs, 188
NICs (Network Interface Cards)
adapter teaming, 96
optimal settings, verifying, 105–106
no answer ring duration, 321
NonCallProcessingNodeCpuPegging alert, 481
nonrepudiation, violation of, 160
NTP (Network Time Protocol), enabling time synchronization, 398–399
NumberOfRegisteredGatewaysDecreased alert, 481
NumberOfRegisteredGatewaysIncreased alert, 481
NumberOfRegisteredMediaDevicesDecreased alert, 481
NumberOfRegisteredMediaDevicesIncreased alert, 481
NumberOfRegisteredPhonesDropped alert, 481

O

obtaining CallManager upgrade media, 143
Offhook to First Digit Timer parameter, 321
OffNet calls, selecting dial tone, 328
one-time passwords, implementing, 168
OnNet calls, selecting dial tone, 328
OOB (out-of-band) management, implementing on IOS/CatOS devices, 167–168
operations procedures, establishing, 35, 37
optional services, 302–305
recommendations for 500+ user systems, 305–306
recommendations for 1500+ user systems, 306–307
recommendations for 10,000+ user systems, 307–308
recommendations for 20,000+ user systems, 309–312
origCalledPartyRedirectedOnBehalfOf field (CDR), 405
origCalledPartyRedirectReason field (CDR), 406

origCause_value field (CDR), 404, 410
originalCalledPartyNumber field (CDR), 409
originalCalledPartyNumberPartition field (CDR), 409
origIpAddr field (CDR), 410
origIpPort field (CDR), 403–404
origPrecedenceLevel field (CDR), 404
origVideoCap_Codec field (CDR), 404
origVideoCap_Resolution field (CDR), 404
origVideoTransportAddress_IP field (CDR), 405
origVideoTransportAddress_Port field (CDR), 405
OSI reference model, layers of, 163
overlapping permissions, managing in MLA, 359–360
oversubscription
  monitoring with weekly voice messaging utilization reports, 426
  preventing with CAC, 60–65

P

PACLs (port access control lists), filtering network traffic, 188
parameters
  CallManager service
    Call Park Display timer, 326
    H323 FastStart Inbound, 326
    Maximum Ad Hoc Conference, 327
    Maximum MeetMe Conference Unicast, 327
    National Number Prefix, 325
    Party Entrance Tone, 327
    Preferred G711 Millisecond Packet Size, 328
    Preferred G723 Millisecond Packet Size, 328
    Preferred G729 Millisecond Packet Size, 328
    Preferred GSM EFR Millisecond Packet Size, 328
    Silence Suppression for Gateways, 328
    Speed Dial Await Further Digits, 323
    Strip G.729 Annex B from Capabilities, 328
    Subscriber Number Prefix, 325
    Suppress MOH to Conference Bridge, 327
  changing, 316
  customizing CCM traces and DNA data, 319
  displaying for every server, 317
  enterprise parameters, 343–345
  Unknown Caller ID Text parameter, specifying, 322
Party Entrance Tone parameter, 327
passwords
  consistent use of, 101, 123–124
  for CCMAdministrator user account, changing, 353
  SQL mismatches, troubleshooting, 134
patches, 104
  installing, 152, 154–155
  versus upgrades, 138–139
PerfMon, 466
Perfmon Log format, 490–491
performance counters, setting threshold triggers, 482
performing backups with BARS, 119
  checking log files for errors, 122
  default backup targets, 120–121
  moving backup files, 122
permissions
  for CCM Directory Manager account, 381
  for functional groups, 349–352
  for standard user groups, 350–352
PermissionsXXXXXX.txt application log, 354
personnel changes, updating through HR department, 362
planning
  backup strategies, 117
    consistent password phrases, 123–124
    ensuring backup space, 123
    default backup targets, 120–121
    moving backup files, 122
    performing backups with BARS, 119–122
    scheduling backups, 118
    selecting appropriate backup server, 117
  directory integration, 375–377
plugins, Cisco Customer Directory Configuration Plugin, 374
point-to-point links, reducing jitter with LFI, 56
polling interval, configuring on RTMT, 476

post-installation tasks
caveats when using unsupported software, 103
database synchronization, verifying, 105
double-checking pre-installation checklist, 102
existing user accounts, maintaining, 104
optimal NIC settings, verifying, 105–107
OS parameters, maintaining, 103
patching, 104
power supplies, verifying connections before installation, 95
precautions, observing while installing service releases, 154–155
precedence values (MLPP), 407
preconfigured RTMT alerts, 477–478
CallProcessingNodeCpuPegging, 478
CodeRedEntry, 478
CodeYellowEntry, 478
CriticalServiceDown, 479
DirectoryConnectionFailed, 479
DirectoryReplicationFailed, 479
ExcessiveVoiceQualityReports, 479
LowAvailableDiskSpace, 480
LowAvailableMemory, 480
LowCallManagerHeartbeatRate, 480
LowTcdServerHeartbeatRate, 480
LowTFTPServerHeartbeatRate, 480
MaliciousCallTrace, 480
MediaListExhausted, 480
MgcpDChannelOutOfService, 481
NonCallProcessingNodeCpuPegging, 481
NumberOfRegisteredGatewaysDecreased, 481
NumberOfRegisteredGatewaysIncreased, 481
NumberOfRegisteredMediaDevices-Decreased, 481
NumberOfRegisteredMediaDevices-Increased, 481
NumberOfRegisteredPhonesDropped, 481
RouteListExhausted, 482
Preferred G711 Millisecond Packet Size parameter, 328
Preferred G723 Millisecond Packet Size parameter, 328
Preferred G729 Millisecond Packet Size parameter, 328
Preferred GSM EFR Millisecond Packet Size parameter, 328
pre-installation tasks
adapter teaming, 96
contract number, verifying, 97
documenting server characteristics, 93–94
double-checking, 102
logistics checklist, 92
network connectivity, verifying, 95
power supply connections, verifying, 95
preparing installation media, 94
reading release notes, 97–98
preparing
CallManager upgrade checklist, 142–143
for directory integration, 377–382
installation media, 94
preventing
BPDU Spanning-Tree attacks with BPDU Guard, 181–182
oversubscription with CAC, 60
location-based CAC, 62–65
unathorized web browser access, 363
PRI fractional, 325
prioritizing voice traffic, 186–187
privacy
ehancements for release 4.0(1), 504
violations of, 160
private password phrases, consistent use of, 123–124
privileges, assigning to functional groups, 359
privileges report (MLA), generating, 356
problem reporting methods, establishing, 35
provisioning endpoints, 207
endpoing image authentication, 208
enrollment, 208–215
PSTN (public-switched telephone network), 69
published API enhancements (release 4.0), 511–512
Publisher, 111
attempting MLA configuration changes while down, 355
PUT (Product Upgrade Tool), 143

Q

Q.SIG enhancements, 496–497
QoS (quality of service)
bandwidth consumption, adjusting on WANs, 58–59
jitter, minimizing on WANs, 56–57

latency, minimizing on WANs, 49–55
tracking via CAR, 426
Query Builder, querying known CDR values, 417
queuing
FIFO, 49
IP RTP priority, minimizing latency on WANs, 50–52
LLP, minimizing latency on WANs, 52–55
LLQ, minimizing latency on WANs, 50

R

RADIUS (Remote-Access Dial-In User Service) authentication, configuring, 440–442
RAID (redundant array of inexpensive disks)
implementing staging environments for CallManager upgrades, 140
remirroring with spare drive, 150
README files, 152
reassigning default native VLAN value, 184
recipients to alerts (RTMT), selecting, 475
redundancy, backup strategies, 112
backing up CallManager servers, 113
backing up Cisco Unity messaging repository, 115
backing up frequently stored files, 114
backing up gateways, 115–116
backing up log files, 114
backing up MOH sources, 114
backing up router/switch configurations, 116
backing up Subscriber, 113–114
reestablishing RAID mirroring, 150
Region setting (CallManager Administration), configuring, 60–61
reinstalling Subscribers, 126
release 4.0(1)
feature list, 493
Ad Hoc conference party drop, 505
annunciator, 497
BAT enhancements, 512
call join, 502–503
cBarge, 503
Cisco CallManager Attendant Console enhancements, 514
conferencing infrastructure enhancements, 508
desktop video telephony, 498–501
DirTrfr, 506
display of configurable call forward information, 505–506
hunt group enhancements, 508–510
iDivert, 504–505
IPMA enhancements, 506–507
management and monitoring enhancements, 513
MCID, 510–511
MLA enhancements, 513
MLPP, 494–495
precedence calls to another network, 496
precedence calls within cluster, 496
multiple calls per line appearance, 502
privacy, 504
published API enhancements, 511–512
Q.SIG enhancements, 496–497
security enhancements, 514–515
Service URL, 505
SIP trunk signaling interface, 497–498
updated CDR fields, 404– 406
codec values, 407
MLPP cause codes, 406
MLPP precedence values, 407
redirect reason codes, 408-409
video resolution values, 408
release 4.x
MLA, enabling, 355
updates from previous release, 353–354
release notes, reading, 97–98
release timeline of CallManager components, 139
Remember the Last User Logged In parameter (Cisco Extension Mobility service), 343
Remote Desktop Client, downloading, 468
remote upgrades, VNC, 470–471
replication (SQL), troubleshooting, 133–134
reports (CAR), 424–425
utilization, 425–426
rerouting calls with AAR, 66, 68– 69
resolving NetBIOS names with LMHOSTS file, 129–132
restarting services in CallManager Serviceability, 314

Restore Wizard (BARS), 126
restoring from BARS backups, 125
restricting
access with AAA authentication, 439–440
RADIUS configuration, 440–442
TACACS+ configuration, 440
access with MLA, 362
CDR database entries, 395–396
Ethernet port access, 170–174
Layer 2 connectivity, 174–175
MAC addresses on switch ports, 169–170
RIS Data Collector service, 336–337
rollout plan, establishing, 27–32
RouteListExhausted alert, 482
router/switch configurations, backing up, 116
routers
hardening, 165–167
syslog configuration, 449–451
routing protocol traffic, authenticating, 191–192
RTMT (Real-Time Monitoring Tool)
alerts, 475
preconfigured, 477–482
recipients, selecting, 475
changes from previous releases, 474
Cisco Serviceability Reporter service, 483
configuring, 473
counters, setting threshold triggers, 482
custom reports
Alert Log format, 485
Call Log format, 487–489
creating, 484
Device Log format, 489–490
Perfmon Log format, 490–491
Server Log format, 485
Service Log format, 486–487
Device Search feature, 483
media resources, monitoring, 475
polling interval, configuring, 476
trunk utilization, monitoring, 476
running Upgrade Assistant Utility, 145

S

scheduling
backups, 118
change freezes, 147–150
searching CDR SQL database, 417
second-day support centers, establishing, 33–34
Secure Remote Administration, hardening
CallManager and voice application servers, 202–203
security, 7–8
802.1Q tunneling, disabling, 185
administrative control traffic, encrypting, 168
audits, performing, 364
AutoSecure feature (IOS routers), 166
broadcast storm control, disabling, 186
CoS settings, ignoring on CatOS devices, 174
DAI, enabling, 176–179
default native VLAN value, reassigning, 184
DHCP responses, limiting, 175
DHCP snooping, 176
DTP, disabling, 184
endpoint provisioning, 207
endpoint image authentication, 208
enrollment, 208–215
enhancements to release 4.0, 514–515
Ethernet port authentication, 170–174
HSRP, authenticating, 192–193
infrastructure security feature checklist, 164–165
interserver communication, facilitating with IPSec, 219
IP addresses, allocating, 190–191
Layer 2
connectivity, restricting, 174–175
control protocols, disabling, 179–185
MLA, 349
Access file, monitoring, 360
Access log files, monitoring, 356
application logs, 354
attempting configuration changes while Publisher is down, 355
CCMAdministrator account, tracing logins, 361–362

CCMAdministrator user account, 353
custom functional groups, creating, 357
custom user groups, creating, 358
functional groups, 349–352
overlapping permissions, managing, 359–360
privileges report, generating, 356
privileges, assigning to functional groups, 359
restricting access, 362
standard user groups, 350– 352
super user, 349
trace logs, enabling, 355
updates from previous release, 353–354
user-specific accounts, creating, 357
network traffic, filtering, 187–190
on CallManager and voice application servers, hardening, 197–207
on IP Phones
802.1Q frames, dropping, 196
GARP, ignoring, 194–195
one-time passwords, implementing, 168
policies, creating, 161
Port Security, 169–170
routers, hardening, 165–167
routing protocol traffic, authenticating, 191–192
single points of failure, avoiding, 161–163
unauthorized web browser access, preventing, 363
voice traffic, prioritizing, 186–187
VTP, disabling, 183
X.509v3 certificates, 215
endpoint operation, 215–218
selecting
AAA protocol, 437
backup servers, 117
CallManager upgrade version, 141
community strings, 460–461
devices, 21
memory requirements, 22
dial tones for OnNet and OffNet calls, 328
gateways for centralized CallManager architecture, 85– 87
phone types, 23–24
RTMT alert recipients, 475
syslog message severity levels, 448
serialization delay, 56
Server Log format, 485
servers
dedicates, 303
hardware vendor, selecting, 21–22
restoring, 125
Service Log format, 486–487
service releases. *See also* patches
installing, 152–155
Service URL, 505
services, 303, 304–305
advanced, 316
B-Channels, removing from service for maintenance, 324–325
CallManager service
collecting CDR data, 318
parameters, 319–322
Cisco CDR Insert, 338
Cisco Extended Functions, 339–340
Cisco Extension Mobility, 342
Cisco Serviceability Reporter, 340
Cisco Telephony Call Dispatcher, 335
clusterwide parameters, 316
CMI, 331–333
compartmentalizing, 203
CTIManager, 334
CTL Provider, 338–339
Database Layer Monitor, 338
dedicated servers, 303
dependencies, 301–302
enterprise parameters, 343–345
IP Manager Assistant, 341
IP Voice Media Streaming App, 333–334
MOH Audio Translator, 335–336
Default MOH Volume Level parameter, 336
optional
recommendations for 500+ user systems, 305–306
recommendations for 1500+ user systems, 306–307
recommendations for 10,000+ user systems, 307–308
recommendations for 20,000+ user systems, 309–312
parameters
changing, 316
checking for every server, 317

Speed Dial Await Further Digits, 323
Unknown Caller ID Text parameter, specifying, 322
restarting, 314
RIS Data Collector, 336–337
starting/stopping, 313
status, displaying, 312
TFTP, 328–331
WebDialer, 341
severity levels (syslog messages), selecting, 448
Show Ring Settings enterprise parameter, 345
Silence Suppression for Gateways parameter, 328
single points of failure, avoiding, 161, 163
single-domain AD forest, placing User Creation Base, 383
SIP trunk signaling interface (release 4.0(1)), 497–498
SMDI (simplified message desk interface), CMI service, 331–332
SNMP (Simple Network Management Protocol), 459–460
community strings, 460–461
traps, 462
ccmCallManagerFailed, 463
ccmGatewayFailed, 464
ccmGatewayLayer2Change, 464
ccmMaliciousCall, 465
ccmMediaResourceListExhausted, 464
ccmPhoneFailed, 463
ccmPhoneStatusUpdate, 463
ccmQualityReport, 465
ccmRouteListExhausted, 464
for CallManager Serviceability Alarm facility, 465
HP Insight Agents, 462–463
Speed Dial Await Further Digits parameter, 323
spreadsheets (Microsoft Excel), converting to UTC and IP addresses, 421–422
SQL database (CDR)
exporting CDR data, 418–419
querying known CDR values, 417
replication, troubleshooting, 133–134
SRA (Serviceability Reports Archive), 466
SRST (Survivable Remote Site Telephony), 69, 112
configuring, 71–73
deploying, 73–76
PSTN calling during fallback, 82– 84
user functionality, 70
voicemail during fallback, 78– staging servers, performing CallManager upgrades, 140, 146
staging servers, performing CallManager upgrades, 140, 146
documentation, 150–151
moving system into production, 152
reestablishing RAID mirroring, 150
scheduling change freezes, 147–150
standard functional groups, 349
standard user groups, permissions, 350–352
starting services in CallManager Serviceability, 313
Statistics Enabled parameter, 322
Status Enquiry Poll Flag parameter, 319
storage media, labeling, 117
Strip G.729 Annex B from Capabilities parameter, 328
Subscriber Number Prefix parameter, 325
Subscribers, 111
backing up, 113–114
duplicating, 126
IIS, disabling, 363
reinstalling, 126
super user, 349
Suppress MOH to Conference Bridge parameter, 327
surviving WAN outages with SRST, 69–76
PSTN calling during fallback, 82– 84
voicemail during fallback, 78–80
switches, hardening, 165–167
syslog, 445
analyzers, 457
CallManager Serviceability Alarm, 448
CiscoWorks syslog server, 454–456
cron, 456
Event Viewer, 457–458
facilities, 446
Linux-based server configuration, 451–454
message format, 447
message severity levels, 446–448
multiple server configuration, 456–457
router logging, configuring, 449–451
versus Event Viewer, 458
system performance, managing with service parameters, 320

T

T301 Timer parameter, 320
T302 Timer parameter, 321
TACACS+ (Terminal Access Controller Access Control Server plus), configuring authentication, 440
TAPS (Tool for Auto-Registered Phones Support), 27–28
Terminal Services, 468
  security vulnerabilities, 469–470
TFTP (Trivial File Transfer Protocol) service, 328–331
  dedicated servers, 329
third-party applications
  backup utilities, caveats when using, 121
  CDR-related, 428
threats to security, 159
  mitigating
    hardening routers and switches, 165–167
    on CallManager and voice application servers, 197–207
    on IOS/CatOS devices, 168
    on Layer, 2, 169–190
    on Layer 3, 190–193
  single points of failure, 161–163
time stamps, converting Epoch time to human-readable form, 419–420
time synchronization, enabling, 398–399
tool-based monitoring, 435
trace facility, managing file size, 467–468
tracing
  CCMAdministrator account logins, 361–362
  enabling MLA log files, 355
tracking CAR statistics, 426
training curriculum
  creating, 24– 26
  for administrators, 26–28
traps
  ccmCallManagerFailed, 463
  ccmGatewayFailed, 464
  ccmGatewayLayer2Change, 464
  ccmMaliciousCall, 465
  ccmMediaResourceListExhausted, 464
  ccmPhoneFailed, 463
  ccmPhoneStatusUpdate, 463
  ccmQualityReport, 465
  ccmRouteListExhausted, 464
  configuring, 462
  for CallManager Serviceability Alarm Facility, 465
  HP Insight Agents, 462–463
triggers, setting on performance counters, 482
troubleshooting
  SQL replication problems, 133–134
  using CDR data, 394
  WINS name resolution, 128
troubleshooting reports (CAR), 424–425
trunk utilization, monitoring with RTMT, 476

U

unauthorized access
  as security threat, 159
  to web browser, preventing, 363
Unknown Caller ID Text parameter, specifying, 322
unsuccessful calls, examples of generated CDRs, 416
unsupported administrative CallManager operations, 390
unsupported agents, caveats when using, 435
unsupported software, caveats when adding to CallManager servers, 103
updating LMHOSTS file, 100
Upgrade Assistant Utility, running, 145
upgrading CallManger
  maintenance releases, downloading, 144
  media, obtaining, 143
  preparing upgrade checklist, 142–143
  running Upgrade Assistant Utility, 145
  selecting appropriate version, 141
  version compatibility with Windows OS, ensuring, 141–142
  versus patching, 138–139
  Windows OS upgrades, downloading, 144
  with staging server, 140, 146
    documentation, 150–151
    moving system into production, 152
    RAID-capable servers, 140
    reestablishing RAID mirroring, 150
    scheduling change freezes, 147–150
  with VNC, 470–471
user accounts, CCMAdministrator user account, 353

user classes, 18
User Creation Base, 383–387
user groups, 349
    creating custom groups in MLA, 358
    overlapping privileges, managing, 359–360
user information packets, creating, 34
User object attributes, 372
User Search Base, 380
user training techniques, 25–26
    for administrators, 26–28
user types, selecting appropriate phone types, 23–24
user-specific accounts, creating in MLA, 357
utilization reports, 425–426

V

V3PN (Voice and Video Virtual Private Networking), 193–194
    WAN deployment architecture, 48
VBR (variable bit rate), 46
verifying
    optimal NIC settings, 105–106
    database synchronization, 105
    power supply connections, 95
    pre-installation network connectivity, 95
virus protection software
    adding to new CallManager installations, 107
    hardening CallManager and voice application servers, 200
VNC, 470–471
VNC over SSH, 202–203
voice mail
    diverting calls to, 504–505
    during WAN failure using SRST, 78–80
voice traffic, prioritizing, 186–187
VTP (VLAN Trunking Protocol), disabling, 183

W-X-Y-Z

WANs
    deployment architectures
        ATM, 46–47
        Frame Relay, 45
        leased lines, 43–45
        MPLS, 47–48
        V3PN, 48
    QoS
        bandwidth consumption, adjusting, 58–59
        jitter, reducing, 56–57
        latency, minimizing, 49–55
    SRST, 69
        configuring, 71–73
        deploying, 73–76
        PSTN calling during fallback, 82–84
        user functionality, 70
        voice mail during fallback, 78–80
web browsers
    password lists, 363
    unauthorized access, preventing, 363
WebDialer service, 341
Windows domains, avoiding CallManager server participation,100
Windows Event Viewer, 457–458
Windows 9.x OS
    ensuring compatibility with CallManager upgrade, 141–142
    service releases, installing, 152–155
    update master file, reading, 152
    upgrades, downloading, 144
WINS (Windows Internet Naming Service)
    addresses, configuring, 129
    name resolution, troubleshooting, 128
X.509v3 certificates, 215
    endpoint operation, 215–216, 218