

Index

Note to the reader: Throughout this index **boldfaced** page numbers indicate primary discussions of a topic. *Italicized* page numbers indicate illustrations.

A

- access tier in network access hierarchy, 307–308, 308
- account/discretionary access control list (A/DAACL), 241
- account domains
 - migration strategies, 172–173, 173
 - in Windows NT 4, 63
- account group/discretionary access control list (AG/DAACL), 241–242
- account group/resource group (AG/RG), 242–245, 243
- account lockout restrictions, 194
- account policy to manage, 236, 238–239
 - domain control, 116
- Account Operators group
 - group creation by, 246
 - in Windows NT 4, 172
- account OUs, 168–170
- account policies, 236–240
 - for single domain, 116
- accounting department, 3
- accounts. *See also* user accounts
 - authentication policy, 236–240
 - exam essentials, 251
 - for external partners, 325
 - local, 116
 - planning, 228–240
 - identifying current structure, 229–230
 - naming strategy, 229, 230–235
 - types, 228–229
- Accounts—Global
 - group—Domain Local
 - group—permissions (AGDLP), 244, 244–245
- Accounts—Global
 - group—(Global group)—Universal group—Domain Local group—permissions (AGUDLP), 245, 245
- Accounts -- Global group -- Local
 - group -- permissions (AGLP), 243, 243–244
- Active Directory
 - advanced install, 286
 - business structure and, 2, 18–20
 - containers, 207
 - design
 - for centralized/centralized administration model, 10
 - decentralized
 - administration, 11
 - organization chart and, 4
 - DHCP server authorization, 331
 - and DNS, 351
 - hiding folders from searches, 167
 - migration strategies, 132–140
 - domain names definition, 138–139
 - forest root domain, 139–140
 - restructuring considerations, 133–134
 - upgrade considerations, 133
 - from Windows 2000, 137–138
 - from Windows NT 4, 134–137
 - name selection, 47
 - namespace, 138
 - reasons for implementing, 47–48
 - replication of objects, 323–324
 - site design to support, 269–272
 - Active Directory Application Mode (ADAM), 94
 - Active Directory-enabled applications, object classes and attributes for, 100
 - Active Directory—integrated zones, 363–364
 - Active Directory Migration Tool (ADMT), 133–134
 - Active Directory Services Interface (ADSI) scripting, 116
 - ADAM (Active Directory Application Mode), 94
 - address records, in stub zone, 362
 - address translation servers, 307
 - administration models, 8–14
 - centralized, 8–11
 - centralized/centralized, 9, 9–10
 - centralized/decentralized, 10, 10–11
 - decentralized, 11, 12
 - exam essentials, 25
 - hybrid, 12–13
 - for control of corporate standards, 14
 - for delegation of remote resources, 13
 - identification, design scenario, 15
 - outsourced, 13–14, 15
 - administrative control
 - of domain controllers, and placement, 280
 - as organizational requirement, 51–52
 - of resources, documenting current, 65
 - restrictions, and system design, 49–51
 - in structure design, 84
 - Administrative Control table sample, 52
 - Administrative delegation, 65
 - administrative overhead, 136
 - administrative structure of Active Directory
 - design, 20–23
 - exam essentials, 25
 - administrative structure of business
 - Active Directory impact on, 18–20
 - analyzing existing, 16–18
 - design scenario, 15
 - determining needs, design scenario, 52–53
 - real world scenario, 17
 - ADMT. *See also* Active Directory Migration Tool (ADMT)
 - ADPREP utility, 137–138
 - alternate IP addressing, 331
 - American National Standards Institute (ANSI), 359
 - APIPA (automatic private IP address), 331
 - application support
 - Active Directory implementation for, 47
 - and site design, 272, 273
 - Asynchronous Transfer Mode (ATM), 60
 - attributes, 47
 - schema for definitions, 100
 - auditing, account changes in forest root, 101
 - Authenticated Users group, GPO applied to, 203
 - authentication. *See also* passwords; trust relationships
 - design scenario, 240
 - for remote access, 315–316
 - selective, 132
 - authentication policy for
 - accounts, 236–240
 - lockout restrictions, 238–239
 - log-on options, 239–240
 - passwords, 236–238
 - authoritative zone transfers (AXFRs), 362

410 automatic private IP address (APIPA) – DHCP

automatic private IP address (APIPA), 331
 automation tools, for remote administration, 11
 autonomous administration, 88–90, 89
 flowchart to determine, 99
 autonomy, 86–90
 multiple domains for, 123, 127
 of objects, 163
 real world scenario, 21
 availability of network, 309–311
 AXFRs (authoritative zone transfers), 362

B

back-to-back firewalls, 320, 320
 backbone, 305
 backup
 of GPOs, 212
 system state, 286
 Backup domain controller (BDC), 64
 bandwidth
 cost examples for available, 275
 defining requirements, 314
 for remote access, 304
 replication requirements, 266
 and schema changes, 102
 baseline, 57
 bastion host, 318, 319
 Block Inheritance option, 202–203
 blocking of inheritance, 172
 bridgehead servers, globally unique ID (GUID) for, 267
 brute-force attack, 194
 business models, 2–8
 cost center model, 6–7
 departmental model, 3–4, 4
 exam essentials, 25
 identification, design scenario, 8
 product/service-based model, 6, 7
 project-based model, 4–6, 5

C

caching, universal group membership, 281–282
 centralized administration models, 8–11
 centralized/centralized, 9, 9–10
 centralized/decentralized, 10, 10–11
 single domain for, 117
 change management procedures, 210–212

Citrix MetaFrame XP, 16
 class options, for DHCP server, 332
 clustering services, 92
 coerced administrator, 115
 collaboration, 86–90
 collaborative administration, 86–88, 87
 company objectives, and Group Policy Objects, 193–196
 security, 193–194
 software installation, 194–195
 user restrictions, 196
 computer accounts, 229
 naming strategy, 232–233, 358–359
 Computers container, 207
 connection objects, creation for replication path, 267
 Connection Type form, 61
 connections
 between offices, 59–60. *See also* remote site connectivity
 guaranteeing, 311
 outside U.S., 314
 for remote access, 313–314
 consultants, 45
 contact accounts, 228
 naming strategy, 230–231
 control delegation
 and organizational units (OUs), 166–172
 account and resource, 168–170
 delegation methods, 167–168
 inheritance, 170–172
 core tier in network access hierarchy, 305, 306
 corporate offices
 connections, 52, 59–60. *See also* remote site connectivity
 guaranteeing, 311
 outside U.S., 314
 corporate standards
 and Group Policy development, 197
 linking in Group Policy hierarchy, 201, 202
 cost center business model, 6–7
 OU tree for, 160
 cryptographic export laws, in United States, 50
 custom software, identifying current requirements, 55

D

data administrators, 85–86
 in collaborative administration, 87
 data autonomy, 89
 multiple domains for, 123

data isolation, multiple forests for, 94
 data modification DNS attack, 375
 database, size calculation, 279
 dcgpofix.exe utility, 197, 205
 DHCP (Dynamic Host Configuration Protocol), 330–331
 dcpromo /adv switch, 286
 decentralized administration models, 11, 12
 with Active Directory, 19, 19
 for autonomy, 95, 96
 single domain for, 118, 118–119
 dedicated forest root domain, 140
 Default Domain Controller Policy, utility to re-create, 205
 Default Domain Policy, 196, 205
 and corporate standards, 197
 lockout settings, 238
 password policy options, 236–237, 237
 Default Group Policy Restore command, 197
 DEFAULTIPSITELINK, 273
 Delegation of Control Wizard, 168, 246
 delegation record, 365
 demilitarized zone, 320
 denial-of-service attacks, 375
 departmental business model, 3–4, 4
 organization-based forest for, 95
 Description field for accounts, 229
 design, 47. *See also* schema
 autonomy, collaboration and isolation, 86–90
 autonomous administration, 88–90, 89
 collaborative administration, 86–88, 87
 isolated administration, 90, 90
 criteria identification, 84–86
 data administrators, 85–86
 service administrators, 85
 exam essentials, 103
 forest structure, 93–99
 organization-based forest, 95, 96
 resource forest, 97, 97
 restricted-access forest, 97–99, 98
 owner identification, design scenario, 91
 priorities, 91–92
 design scenario, 93
 Desktop, restrictions on user, 196
 DHCP (Dynamic Host Configuration Protocol), 58, 330–331

- integrating DNS with, 374
 - scope options, 332
 - server placement, 333
 - Digital Subscriber Line (DSL), 59
 - directory service infrastructure, 47
 - examining current, 63–66
 - for Windows 2000 Active Directory, 66
 - for Windows NT 4, 63–65, 64
 - software requirements, 66, 68
 - disk imaging utility, 195
 - distance vector routing, 317
 - distribution groups, 233, 240–241
 - distribution tier in network access hierarchy, 306–307, 307
 - DNS namespace, and Active Directory namespace, 138
 - documenting
 - domain design, real world scenario, 128
 - nested groups, 230
 - workstations, naming strategy, 233
 - documenting current system implementation, 45, 46–63
 - current directory service
 - Windows 2000 Active Directory, 66
 - for Windows NT 4, 63–65
 - current hardware requirements, 56–57
 - current software requirements, 54–56
 - exam essentials, 69–70
 - format, 60–63
 - Administrative Control table sample, 52
 - Administrative delegation, 65
 - Connection Type form, 61
 - Subnet Allocation form, 62
 - Windows 2000 Active Directory administration, 67
 - network requirements, 58–60, 68–69
 - organizational requirements, 46–54
 - administrative control, 51–52
 - reasons for Active Directory implementation, 47–48
 - special requirements, 48–51
 - software requirements, 66, 68
 - domain accounts, password policy for, 236
 - Domain Admins group, 86
 - for changing Schema Admins group, 101
 - group creation by, 246
 - rights and permissions, 85
 - domain controllers
 - configuration for RPC ports, 325
 - creation options, 284–286
 - documenting current system implementation, 64
 - Global Catalog placement, 281–282
 - how to build, real world scenario, 285
 - Master Operations placement, 282–286
 - network infrastructure requirements, 278
 - reliable systems for, 92
 - replication, 266, 267
 - specifications and placement, 277–286
 - domain level, linking group policies at, 205
 - Domain Local group, 248
 - account group/discretionary access control list (AG/DACL) strategies using, 242
 - Domain Name System (DNS), 56, 351
 - delegation options, 365–366
 - exam essentials, 381–382
 - infrastructure design, 366–367
 - integration options, 359–361
 - with DHCP, 374
 - with WINS, 374–375
 - migration options, 364–365
 - name selection, 47
 - namespace design, 353–366
 - internal and external requirements, 354–357
 - naming standards, 357–359
 - root domain requirements, 356–357
 - server security, 378–379
 - static IP addressing for server, 330
 - zones, 361–366
 - delegation options, 365–366
 - migration options, 364–365
 - propagation methods, 362–364
 - types, 361–362
 - Domain Naming Master, 139, 283
 - domain owners, and administrative control, 115
 - domains, 84. *See also* forest root domain
 - account policies settings, 210
 - Active Directory implementation for restructuring, 47
 - administrative structure with multiple domains, 122–124
 - administrative structure with multiple trees, 124, 125
 - administrative structure with single domain, 115–127, 116–121
 - for centralized administration, 117, 117–118
 - for decentralized administration, 118, 118–119
 - hybrid administration, 119–120, 120
 - outsourced administration, 121, 121
 - creation considerations, 126–127
 - design selection, design scenario, 125
 - exam essentials, 141–142
 - functional levels, 127
 - name selection, 138–139
 - real world scenario, 140
 - security concerns, 126
 - trust relationships, 127–132
 - authentication, 132
 - design scenario, 131
 - external and realm trusts, 130–131
 - with forest trust, 128–129
 - with SID filtering, 131–132
 - with trusts between domains, 129–131
 - in Windows NT 4, 63
 - drive space, for domain controllers, 278
 - DSL (Digital Subscriber Line), 59
 - duration of account lockout, 239
 - Dynamic Host Configuration Protocol (DHCP), 58, 330–331
 - integrating DNS with, 374
 - scope options, 332
 - server placement, 333
 - dynamic routes, 317
-
- ## E
- E-Carrier line, 59–60
 - e-mail software, distribution groups for, 233
 - empty forest root, 134–135, 135
 - encryption, reversible, for password storage, 237
 - Enforce Password History setting, 236
 - Enterprise Admins group, 19–20, 85, 86, 139
 - for changing Schema Admins group, 101
 - group creation by, 246

412 exam coverage – IANA (Internet Assigned Numbers Authority)

exam coverage
 assumptions for NetBEUI protocol, 56
 case studies, 46
 Exchange Server
 additions to Active Directory, 100
 and Global Catalog server, 281
 extendable database, Active Directory as, 47
 external namespace, 357–358
 external trusts, 130–131
 extranet, 325

F

fault tolerance, 310
 for replication of WINS, 372
 file replication service (FRS), 273
 filtering
 in GPOs, 203
 WMI, 200, 201
 firewalls, 305, 307
 real world scenario, 323
 and remote access, 319
 for forest, 320–322
 options, 318–320
 secure replication through, 322–324
 and replication traffic, 276
 and VPN server, 326
 folders, hiding from Active Directory searches, 167
 footprinting, 376
 forest root domain, 139–140, 280
 when upgrading multiple MUDs, 134
 forest trust, 95, 96, 128–129
 forests
 administrative collaboration, 88
 and firewalls, 320–322
 multiple, 20, 22
 reasons for, 93–94
 Operations Masters in multiple domain, 283–284
 Operations Masters in single domain, 282
 planning and testing, 101
 resource access design for, 247
 as security boundary, 86
 structure, 93–99
 organization-based forest, 95, 96
 resource forest, 97, 97, 136
 restricted-access forest, 97–99, 98
 Frame Relay, 60
 FRS (file replication service), 273
 Full Control permission, for organization units, 156

function. *See* job function
 "funny money", 7

G

Global Catalog server, 272
 drive space for, 278–279
 placement, 281–282
 Global group, account group/
 discretionary access control list (AG/DACL) strategies using, 242
 globally unique ID (GUID), for bridgehead servers, 267
 government defense contracts division isolation for, 9
 forest for isolation, 98, 99
 GPMC. *See* Group Policy Management Console (GPMC)
 group accounts, 229
 naming strategy, 233–235
 Group Policy, 48
 administration training methodology, 209–210
 control, real world scenario, 211
 corporate objectives and, 193–196
 design, 196–206
 for inheritance, 201–205
 interoperability issues, 199, 201
 user requirements, 197–198
 hierarchy, 197
 linking options, 205, 207
 minimizing logon time, real world scenario, 200
 overview, 190–191
 Group Policy change approval committee, 211
 Group Policy Management Console (GPMC), 190–191
 for backup and restore, 212
 Delegation tab for OU, 209
 Group Policy Objects (GPOs) in, 192
 Group Policy Modeling, 192
 Group Policy Modeling Wizard, 208
 Group Policy Objects (GPOs)
 administration, 120
 and administrative load, 117
 backup and restoring, 212
 change management, 210–212
 defining, design scenario, 206
 disabling part, 199
 exam essentials, 213–214
 minimizing, 198–199
 permissions, identifying required, 210
 groups
 creation options, 246–247
 creation strategy, 247–249

access level requirements, 248–249
 nesting efficiency, 249
 resource access needs, 248
 documenting nested, 230
 exam essentials, 251
 requirements for resource access
 account/discretionary access control list (A/DACL), 241
 account group/
 discretionary access control list (AG/DACL), 241–242
 account group/resource group (AG/RG), 242–245, 243
 user membership in, 249
 and log-on time requirements, 249
 growth, plans for, 51
 GUID (globally unique ID), for bridgehead servers, 267

H

hard drives for domain controllers, 278
 hardware
 identifying current requirements, 56–57
 static IP addressing requirements, 330
 testing current load, 57
 hiding
 folders from Active Directory searches, 167
 service accounts, 231
 high-availability solutions, 92
 high-level DNS security policy, 377
 hostnames, 358–359
 hub-and-spoke method of replication, 370, 371
 multi-level, 372
 human resources department, 3
 hybrid administration models, 12–13
 for control of corporate standards, 14
 for delegation of remote resources, 13
 single domain for, 119–120, 120
 user changes to GPOs, 208–209

I

IANA (Internet Assigned Numbers Authority), 331

IAS. *See* Internet Authentication Service (IAS)

ICANN (Internet Corporation for Assigned Names and Numbers), 47

incremental zone transfers (IXFRs), 362

Identity Integration Services, 88

InetOrgPerson account, 228

naming strategy, 230–231

information technology department, 3

in cost center model, 6–7

infrastructure design, responsibility for, 45

infrastructure master, 283–284

inheritance, 170–172

Group Policy design for, 201–205

installation of software, GPOs for, 194–195

Integrated Services Digital Network (ISDN), 59

IntelliMirror, 195

internal DNS root, 356

internal users, security, 304–305

Internet

- access to, 311–312
- domain name registration for, 139, 357–358
- name selection, 357

Internet Assigned Numbers Authority (IANA), 331

Internet Authentication Service (IAS), 315

Internet Corporation for Assigned Names and Numbers (ICANN), 47

Internet protocol security (IPSec) policies, 194, 309

for replication, 324

Internet Service Provider (ISP), 351–352

intersite connection objects, 267

Intersite Topology Generator (ISTG), 267

interviews, open ended questions in, 17

IP addressing, 327–333

- allocation, 328, 329–331
 - with alternate IP addressing, 331
 - with APIPA, 331
 - with DHCP, 330–331
 - with static addressing, 330
- DHCP server locations, 333
- resolution. *See* Domain Name System (DNS); Windows Internet Name Service (WINS)
- scope options, 332

IP (Internet protocol), for replication, 273

IP spoofing, 375

IPSec. *See* Internet protocol security (IPSec) policies

IPX/SPX protocol, 59

ISA Server, Enterprise Edition, additions to Active Directory, 100

ISDN (Integrated Services Digital Network), 59

isolated administration, 90, 90

flowchart to determine, 99

isolation, 86–90

- of domain, 115
- forest to allow for, 140
- multiple trees and, 124
- real world scenario, 98

ISP (Internet Service Provider), 351–352

ISTG (Intersite Topology Generator), 267

IXFRs (incremental zone transfers), 362

J

job function

- as basis for OU design, 158, 159, 160
- and Group Policy development, 198

K

Kerberos service authentication, 239

- policy control at domain level, 116

Knowledge Consistency Checker (KCC), 267

L

Layer Two Tunneling Protocol (L2TP), 60, 315

leases for IP addresses, 330

length of password, 237, 238

line-of-business applications, 48

linear replication model, 371

link-state routing, 317

linking options

- GPOs within Active Directory, 212
- group policies, 205, 207

load balancing, 311

local accounts, 116

Local groups, account group/discretionary access control list (AG/DAACL) strategies using, 242

LocalService account, 231

location

- as basis for OU design, 157, 158

- with organization, 160, 161, 162
- domains based on, 123–124

lockout restrictions, 194

- account policy to manage, 236, 238–239
- domain control, 116

logon

- minimizing time requirement, 200
- domain controller placement for, 280
- group memberships and, 249
- options, 239–240

loopback, for Group Policy Objects, 203–205

low-level DNS security policy, 376

M

marketing department, 3

Master Operations, placement, 282–286

Master User Domains (MUDs), 134, 172

- updating to Active Directory, 134–136, 135

Maximum Password Age, 237

mean time between failures (MTBF), 310

mean time to recovery (MTTR), 310

memory for domain controllers, 278

Microsoft Management Console snap-ins, 11

mid-level DNS security policy, 377

migration strategies, 132–140

- domain names definition, 138–139
- forest root domain, 139–140
- restructuring considerations, 133–134
- upgrade considerations, 133
- from Windows 2000, 137–138
- from Windows NT 4, 134–137
- organizational units (OUs), 172–175

Minimum Password Age, 237

modem, 59

most-restrictive/most-inclusive strategy, for nested groups, 249, 250

MTBF (mean time between failures), 310

MTTR (mean time to recovery), 310

MUDs. *See* Master User Domains (MUDs)

multifactor authentication, 240

414 name resolution – perimeter network**N**

- name resolution. *See also* Domain Name System (DNS); Windows Internet Name Service (WINS)
 exam essentials, 381–382
 infrastructure
 examining current, 351–353
 security, 374–380
 integrating services, 374–375
 name server record, in stub zone, 362
 namespaces
 for DNS
 internal and external requirements, 354–357, 355
 separating, 364
 for tree, 124
 naming strategy
 for accounts, 229, 230–235
 computer accounts, 232–233
 group accounts, 233–235
 security group, 234–235
 servers, 232–233
 service accounts, 231
 studying current, 230
 user accounts, 230–231
 workstations, 232
 real world scenario, 235
 for sites, 269
 nested groups, 243–245
 documenting, 230
 efficiency in creating, 249
 most-restrictive/
 most-inclusive strategy, 249, 250
 NetBEUI, and Windows Server 2003. *See* Windows Internet Name Service (WINS)
 NetBIOS names, 359
 resolution, 352
 network access, 304–312. *See also* remote access
 hierarchy, 305–308, 306
 access tier, 307–308, 308
 core tier, 305, 306
 distribution tier, 306–307, 307
 improving availability, 309–311
 Internet access, 311–312
 security considerations, 309
 network addresses, 58–59
 network administrators, 45
 network infrastructure
 documenting current system implementation, 68–69
 hardware capabilities, 57
 and site topology design, 268
 network map, 268, 269
 multiple domain, 270
 Network Monitor, 58
 NetworkService account, 231
 nontransitive trust relationships, 64
-
- O**
- object-based delegation, 167
 objectives of company, and
 Group Policy Objects, 193–196
 security, 193–194
 software installation, 194–195
 user restrictions, 196
 obsolescence, planned, 47–48
 offices, connections, 52, 59–60.
 See also remote site
 connectivity
 guaranteeing, 311
 outside U.S., 314
 Open Shortest Path First (OSPF), 317
 operating systems
 Group Policy interoperability, 199, 201
 loss of support for legacy, 47–48
 Operations Masters, 92
 organization
 analyzing existing requirements, 49–50
 as basis for OU design, 158, 159
 with location, 160, 161, 162
 name selection, 47
 organization-based forest, 95, 96
 organization chart, and Active Directory design, 4
 organizational units (OUs), 48
 basics, 156–157
 and control delegation, 166–172
 account and resource, 168–170
 delegation methods, 167–168
 inheritance, 170–172
 design criteria, 162–166
 object autonomy, 163
 object visibility, 164–166, 166
 design options, 157–161
 for administrative purposes, 165
 best approach selection, 161
 function as basis, 158, 159, 160
 location and organization as basis, 160, 161, 162
 location as basis, 157, 158
 organization as basis, 158, 159
 for hybrid administration, 120
 linking group policies at, 205
 migration from NT 4.0, 172–175
 account domains, 172–173, 173
 design scenario, 174
 resource domains, 173–175
 organizing for inheritance, 201, 202
 for outsourced administration, 121
 redirecting new accounts to, 207
 structure, 169
 administrative requirements, 208–210
 after permissions delegated, 171
 creation, 207–212
 OSPF (Open Shortest Path First), 317
 OU administrators, 157
 object control by, 168
 OU owners, 164
 control, 168
 training in delegation, 167
 user accounts as, 156
 OUs. *See* organizational units (OUs)
 outsourcing
 single domain for, 121, 121
 thin client, real world scenario, 16
 owner identification, design scenario, 91
-
- P**
- packaged software, identifying current requirements, 55
 partners, resource access by, 325
 passwords
 account policy to manage, 236–238
 change
 PDC emulator as clearinghouse for, 284
 requiring, 116
 user authentication before, 194
 policies for, 116
 strong, 193–194, 236
 enforcement, 237
 peak usage times, in hardware monitoring, 57
 Performance Logs and Alerts, 57, 66
 Performance Monitor, 57
 perimeter network, 320
 DNS servers on, 378, 378
 real world scenario, 323

permissions

- assignment from parent to child, 170–172
- for GPOs, identifying required, 210
- groups to organize, 233
- managing, task vs. object level, 168
- for users, 309
 - group creation and, 248

Personal Identification Number (PIN), 240

planned obsolescence, 47–48

Point-to-Point Tunneling Protocol (PPTP), 60, 315

political boundaries, restrictions on information crossing, 50

ports, for replication with IPsec, 324

PPTP (Point-to-Point Tunneling Protocol), 60, 315

Primary domain controller (PDC), 64

primary domain controller (PDC) emulator, 284

primary zones in DNS, 361–362

printers, groups to administer, 246

privacy laws, 50–51

processing priority for Group Policy Objects, 203

processors for domain controllers, 278

product/service-based business model, 6, 7

- organization-based forest for, 95
- OU tree for, 160

production department, 3

project-based business model, 4–6, 5

- OU tree for, 160

projects in progress, and system design, 46

protocols

- determining software requirements, 55–56
- for replication, 273–274
- proxy servers, 312
- pull replication in WINS, 370
- push/pull replication in WINS, 370
- push replication in WINS, 370

Q

questions in interviews, 17

R

RADIUS. *See* Remote Authentication Dial-In User Service (RADIUS)

RAM (random access memory), for domain controllers, 278

realm trusts, 130–131

redircmp.exe utility, 207

redirection attack, 376

redirsur.exe utility, 207

redundancy, 310

- for replication of WINS, 372
- for WINS servers, 369

regional domain model, 123, 123

registration of domain namespace, 139, 352

regulations, and system design, 49–51

relative identifier (RID) master, 283

reliable systems, as design priority, 91–92

remote access, 312–316

- bandwidth, 304
- connection options, 313–315
- identifying considerations, 312–313
- risks, 312
- user authentication and accounting guidelines, 315–316

remote administration, 11

Remote Authentication Dial-In User Service (RADIUS), 315–316

- client and server placement, 327

Remote Desktop, workstation names for, 233

Remote Procedure Calls (RPC), 273, 324

- opening ports, 324

remote site connectivity, 316–327

- connectivity needs, 317
- exam essentials, 334–335
- extranet options, 325
- firewalls, 319
 - for forest, 320–322
 - options, 318–320
- secure replication through, 322–324
- server placement, 325–327

replication

- Active Directory, 363–364
- through firewalls, 322–324
- multimaster technology, 266
- multiple domains and, 124
- network resources
 - consumption, 271, 285
 - of schema changes, 100
 - site links for, 273
 - WINS, 353, 370–374
- research and development, autonomy, real world scenario, 21
- reserved client options, for DHCP server, 332
- reserving IP address on DHCP server, 330
- Reset Account Lockout Counter After setting, 239
- resource administrators, 168
- resource domains, 136–137
- migration strategies, 173–175
- in Windows NT 4, 63, 134

resource forest, 97, 97, 136

Resource group, 242–245

resource OUs, 168–170

resource records, 366

resources

- access design for forests, 247
- access needs in group creation, 248
- administration of, 157
- administrative control, 51–52
 - documenting current, 65
- group requirements for access, 240–247
 - account/discretionary access control list (A/DACL), 241
 - account group/discretionary access control list (AG/DACL), 241–242
 - account group/resource group (AG/RG), 242–245, 243
- OUs for autonomy over, 127
- restricting user access, 309
- security group to access, 234

restoring GPOs, 212

restricted-access forest, 97–99, 98

reversible encryption, for password storage, 237

RIP (Routing Information Protocol), 317

roaming users, and Global Catalog server placement, 281

roge administrator, 115

- and SIDHistory attribute, 131–132

roll-out schedule, for schema, 102

root domain requirements, 356–357

routing, 317–318

Routing and Remote Access Server (RRAS), 315, 317

- server placement, 325, 326

Routing Information Protocol (RIP), 317

S

sales department, 3

schema, 100–102

- for forest, 99
- integrated, for multiple trees, 124
- planning and testing, 101
- responsibility for, 101
- roll-out schedule, 102

Schema Admins group, 86, 101, 139

Schema Master, 102, 139

- and domain controller placement, 283

schema modification policy, 100

416 school systems – Terminal Services

- school systems, real world scenario, 24
- scope options, for DHCP server, 332
- searches within Active Directory, hiding folders from, 167
- secondary paths, 310
- secondary zones in DNS, 357, 362
- security
 - breaches, 115
 - as corporate objective, 193–194
 - for DNS servers, 378–379
 - for domain controllers, 280
 - for domains, 126
 - internal namespaces and, 140
 - for name resolution infrastructure, 374–380
 - in network access, 309
 - for outsourcing, 14, 121
 - Windows Internet Name Service (WINS), 379–380
- security boundary, 86
- security groups, 233, 234, 240–241
 - Windows 2000 Native Mode for nesting, 243
- servers
 - address translation, 307
 - bridgehead, globally unique ID (GUID) for, 267
 - Exchange Server
 - additions to Active Directory, 100
 - and Global Catalog server, 281
 - Global Catalog, 272
 - drive space for, 278–279
 - placement, 281–282
 - naming strategy, 232–233
 - proxy, 312
 - reserving IP address on DHCP, 330
 - Routing and Remote Access Server (RRAS), 315, 317
 - server placement, 325, 326
 - Systems Management Server, 195
 - for software inventory, 54
 - Windows Server 2003
 - DNS service migration options, 364–365
 - and Group Policy settings, 199
 - interoperation with DNS, 359–360
 - Network Monitor, 58
 - promoting to domain controller, 286
- service accounts, naming strategy, 231
- service administrators, 85
- service autonomy, domains for, 89
- service identity plan, 231
- service isolation, multiple forests for, 94
- Service Level Agreement (SLA), 198–199
 - and software rollout, 195
- service locator (SRV) record, 271
- shared folders, hiding, 167
- shortcut trusts, 129–130, 130, 280
- SID filtering, 131–132, 322
- SIDHistory attribute, 131–132
- Simple Mail Transfer Protocol (SMTP), for replication, 273–274
- site level, linking GPO at, 205, 210
- site link bridges, 272, 275–276, 276
- site links, 272–275
- site topology, 266–277
 - current network infrastructure, 268
 - design scenario, 277
 - domain controllers
 - creation options, 284–286
 - Global Catalog placement, 281–282
 - Master Operations placement, 282–286
 - specifications and placement, 277–286
 - exam essentials, 287–288
 - site design to support Active Directory, 269–272
 - site link bridges, 272, 275–276, 276
 - site links, 272–275
- sites
 - connector for domain controller replication, 267
 - naming strategy for, 269
 - smart card, for authentication, 240
 - SMTP (Simple Mail Transfer Protocol), for replication, 273–274
 - software
 - identifying current requirements, 54–56
 - packaged vs. home-grown, 55
 - protocol requirements, 55–56
 - installation, GPOs for, 194–195
 - SRV (service locator) record, 271
 - stakeholders, 17
 - information from, 49–50
 - for software inventory, 55
 - and service administrator selection, 85
 - trade-off decisions, 92
 - Start menu, restricting user changes, 196
 - start of authority record, in stub zone, 362
 - static IP addressing, 330
- static routes, 317
- strong passwords, 193–194
 - enforcement, 237
 - user education on, 236
- stub zones in DNS, 362
 - vs. delegation record, 365
- Subnet Allocation form, 62
- system implementation, documenting current, 45, 46–63
 - current directory service
 - Windows 2000 Active Directory, 66
 - for Windows NT 4, 63–65
 - current hardware requirements, 56–57
 - current software requirements, 54–56
 - exam essentials, 69–70
 - format, 60–63
 - Administrative Control table sample, 52
 - Administrative delegation, 65
 - Connection Type form, 61
 - Subnet Allocation form, 62
 - Windows 2000 Active Directory administration, 67
 - network requirements, 58–60, 68–69
 - organizational requirements, 46–54
 - administrative control, 51–52
 - reasons for Active Directory implementation, 47–48
 - special requirements, 48–51
 - software requirements, 66, 68
 - System Policy Editor, 201
 - system state backup, 286
 - Systems Management Server, 195
 - for software inventory, 54
 - Sysvol Group Policy Template, backup, 212

T

- T-Carrier line, 59
- TCO. *See* total cost of ownership (TCO)
- task-based delegation, 168
- TCP/IP (Transmission Control Protocol/Internet Protocol), 55–56. *See also* IP addressing
- temporary employees, user accounts for, 232
- Terminal Services, 11

testing

- current hardware load, 57
- hardware for domain controller, 278
- thin client, outsourcing, real world scenario, 16
- three-homed firewall, 318, 319, 320
- threshold, for account lockout, 239
- time synchronization, by PDC emulator, 284
- Tivoli, 54
- tombstone lifetime, 286
- total cost of ownership (TCO), 48
 - reduction, 136
- training
 - about passwords, 194
 - on GOP changes, 208
 - OU owners about delegation, 167
- transaction logs, drive space for, 279
- Transmission Control Protocol/Internet Protocol (TCP/IP), 55–56. *See also* IP addressing
- trust relationships
 - for domains, 127–132
 - authentication, 132
 - design scenario, 131
 - external and realm trusts, 130–131
 - with forest trust, 128–129
 - with SID filtering, 131–132
 - with trusts between domains, 129–131
 - and forest firewall, 321–322
 - nontransitive, 64
 - for resource forests, 97
 - in Windows NT 4, 63

U

- United States, cryptographic export laws, 50
- universal group membership caching, 281–282
- Universal Multiple-Octet Coded Character Set (UCS) Transformation Format 8 (UTF-8) naming conventions, 359
- universal security groups, 245
- UPN. *See also* User Principle Name (UPN)
- user account administrators, 168
- user accounts, 228
 - account policy to protect, 236
 - moving between domains, and SID, 133
 - naming strategy, 230–231

- as OU owners, 156
- for temporary employees, 232
- User Principle Name (UPN), 236
 - and password, for log-on option, 239
- username/password log-on option, 239
- users. *See also* training
 - and access tier design, 308
 - group memberships, 249
 - Group Policy design to meet requirements, 197–198
 - internal, security, 304–305
 - restrictions on, 196
- Users container, 207

V

- variable length subnet masks (VLSM), 327
- virtual private network (VPN), 60, 304, 314–315
 - server placement, 325, 326
- visibility of objects, 164–166, 166
- Visio, 52
 - for network diagram, 54

W

- WAN links, 316
 - information on site layout, 271
 - reliability, 281
 - and domain controller placement, 280
- Windows 2000 Active Directory
 - documenting current system implementation, 66
 - forests, 133
 - Windows 2000, migration strategies from, 137–138
- Windows 2000 Mixed functional level, 127
- Windows 2000 Native Mode, 127
 - for security group nesting, 243
- Windows Internet Name Service (WINS), 56, 352
 - infrastructure design, 368–375
 - number of servers, 368–369
 - integrating DNS with, 374–375
 - population determination, design scenario, 369
 - replication options, 370–374
 - design scenario, 373
 - security, 379–380

- Windows Management Instrumentation (WMI) filters, 201
 - for detecting adequate drive space, 200
- Windows NT 4
 - AGLP principle, 230
 - as current directory service, 63–65
 - domain limitations, 132
 - domain restructuring, 133
 - migration strategies
 - for account domains, 172–173, 173
 - design scenario, 174
 - for resource domains, 173–175
 - migration strategies from, 134–137
- Windows Server 2003
 - DNS service, migration options, 364–365
 - and Group Policy settings, 199
 - interoperation with DNS, 359–360
 - Network Monitor, 58
 - promoting to domain controller, 286
- Windows Server 2003 functional level, 127
- Windows Server 2003 Interim functional level, 127
- Windows XP, and Group Policy settings, 199
- WINS. *See* Windows Internet Name Service (WINS)
- WMI. *See* Windows Management Instrumentation (WMI) filters
- workstations
 - connection in access tier, 307, 308
 - naming strategy, 232

X

- X.25 connection, 60

Z

- ZENworks (Novell), 54
- zone transfers, 362–363
 - for footprinting, 376
- zones in DNS, 361–366
 - delegation options, 365–366
 - migration options, 364–365
 - propagation methods, 362–364
 - types, 361–362