

Index

A

- Access control
 - process 396–397
 - Windows 2000 security model 383
- Access control entries (ACEs)
 - components 341
 - delegating administration 298
 - inheritance 298, 305
 - moved objects 305
- Access control lists (ACLs)
 - access control granularity 397
 - access control process 396–397
 - allowing access to resources 397
 - associated objects 397
 - certificate template access 459–460
 - components 341
 - default resource permissions 397
 - delegating administration 298–299
 - Everyone security group 397
 - implementing 397–398
 - moved security principals
 - adding new SIDs to ACLs 364
 - changed SIDs 362–364
 - computer accounts 369–370
 - member servers 370
 - setting resource permissions 396
 - viewing 397
 - Windows 2000 security model 383, 386
- Access tokens 341, 345
- Accessibility options
 - Accessibility Reset 1080
 - Active Accessibility 866, 1075, 1076
 - Active Desktop 1080–1081
 - configuration methods
 - Accessibility Wizard 1080, 1083
 - Control Panel 1080, 1084
 - Group Policy 867, 1078, 1079
 - Remote OS Installation 1078
 - unattended setup 1078
 - Accessibility options (*continued*)
 - configuration methods (*continued*)
 - user profiles 1079
 - Windows Installer 1079
 - definition 1073
 - FilterKeys 1089
 - high-contrast color schemes 1094
 - hot keys 1089
 - installing 1075–1076, 1078
 - keyboard shortcuts 1088
 - Magnifier 1092
 - mapping features to needs
 - cognitive disabilities 1084–1085
 - common difficulties 1081–1083
 - hearing impairments 1085–1086
 - physical disabilities 1087–1090
 - seizure sensitivity 1090–1091
 - visual impairments 1091–1094
 - Microsoft Accessibility Web page 1077
 - mouse options 1090
 - mouse pointers 1094
 - Narrator 1092
 - new features 1073–1075
 - overview 865
 - ShowSounds 1086
 - sound schemes 1085, 1091
 - Sound Sentry 1086
 - StickyKeys 1089
 - Synchronized Accessible Media Interchange 1086
 - testing 1075
 - third-party products 866, 1076–1078
 - ToggleKeys 1089, 1092
 - Utility Manager 1081
 - volume control 1086
- Account domains
 - guidelines for upgrading 342–343
 - multiple-master domain example 331
 - SAM database size 334, 342, 360
 - upgrading after resource domains 342
- Account lockout policy 269, 415
- Account Operators group 400
- ACEs *See* Access control entries

Index

- ACLs *See* Access control lists
- Active Accessibility 866, 1075, 1076
- Active Desktop 1080–1081
- Active Directory
 - disk space requirements 328
 - feature overview 253–257
 - installing
 - on upgraded PDC 338
 - order of 255
 - non-Windows 2000 client software 804
 - printer objects 570
 - structure planning
 - design principles 260
 - documenting current architecture 170–171
 - domains *See* Active Directory domain structure
 - example scenario 45–48
 - forests *See* Active Directory forest structure
 - OUs *See* Active Directory organizational units
 - planning process 257–259
 - site topology *See* Active Directory site topology
 - structure components 261
 - technology interdependencies 63
- Active Directory Client
 - domain controller directory writes 339
 - finding network users 736
 - installing 804
- Active Directory Connector (ADC)
 - acute administration capabilities 734–735
 - ADC Connection Agreement Plan 762
 - ADC policy 743
 - backing out of synchronization process 765–766
 - bridgehead servers 739, 741
 - canceling synchronization 765–766
 - connection agreements
 - administering objects 748–750
 - described 736–737
 - designing 752–753
 - Global Catalog searches 742
 - mapping containers to OUs 751–752
 - minimum number of 752
 - multiple, described 737
 - planning worksheets 1014–1018
 - scheduling 763–765
 - stopping synchronization in progress 765–766
 - testing 762–763
 - connection models
 - connection agreement design 752–753
 - multiple Windows domains 756–761
 - single Windows domain 753–756
- Active Directory Connector (ADC) (*continued*)
 - data backup and recovery
 - authoritative restore 765, 766
 - backups 765
 - planning for 765
 - populating Active Directory with new objects 766
 - populating attributes 766
 - delegation capabilities 734–735
 - deployment best practices 741
 - Exchange Server integration considerations 63–64
 - Exchange sites
 - identifying Active Directory objects 739
 - identifying topology 738
 - in multiple forests 753
 - managing user permissions 734–735
 - mapping containers to OUs 750–752
 - populating new Active Directory 734
 - synchronizing entire site 742
 - third-party e-mail directories 731, 735
 - versions supported 736
 - finding network users 736
 - Global Catalog searches 742
 - hub-and-spoke networks 739, 741
 - identifying current network structure 738
 - installing 738, 742–743
 - management tools 733
 - object-level updating 733
 - one-way synchronization
 - administering from Active Directory 748
 - administering from Exchange 749
 - overview
 - features 733–736
 - network user directories 736
 - planning process 737–738
 - planning task list 767
 - single source administration 734
 - synchronization process 731–732
 - preparing network for deployment 739–743
 - schema modifications 743, 767
 - selective attribute selection 733
 - single source administration 734
 - stopping synchronization 765–766
 - synchronization schedule 763–765
 - system requirements 740–741
 - third-party e-mail directories 731, 735
 - two-way synchronization
 - ADC features 733
 - administering objects 749–750

- Active Directory Connector (ADC) *(continued)*
 - two-way synchronization *(continued)*
 - examples 753–761
 - third-party e-mail directories 735
 - user objects
 - administering from Active Directory 748, 749–750
 - administering from Exchange 748, 749–750
 - attribute mapping 743–748
 - defining for synchronization 750–752
 - deleted 748
 - managing permissions 734–735
 - mapping containers to OUs 750–752
 - object-level synchronization 733
- Active Directory Connector Management snap-in 752, 753
- Active Directory domain structure
 - creating domain controllers 482, 485
 - DNS domain names
 - computer names 287
 - determining number of trees 285
 - DNS server deployment 287–291
 - duplicate names 285
 - example deployment scenario 45, 47
 - Internet standard characters 284
 - multiple-tree environments 283–284
 - naming guidelines 284–286
 - NetBIOS considerations 282, 286
 - single-tree environments 282–283
 - tree root domain 282, 283
 - used to locate domain controllers 270, 282
 - domain user security policy 269, 272
 - example deployment scenario 45–48
 - forests
 - authentication between 392
 - change control policy 267–268
 - forest database 268
 - merging 268
 - migration considerations 333
 - moving objects between 268
 - multiple-forest environments 263–267
 - overview 261–263
 - partitioning 276–279
 - planning process 257–259, 263
 - restructuring 268
 - root domain 281, 333
 - schema change policy 267
 - Schema container 269
 - schema design 261
- Active Directory domain structure *(continued)*
 - forests *(continued)*
 - single-forest environments 263
 - unique namespace 332, 333
 - multiple-domain environments
 - cost considerations 279–280
 - forest root domain 281
 - moving domains between forests 268
 - optimizing replication traffic 272
 - separate domain administration 272
 - separate security policies 272
 - when to use 271
 - Windows NT domains 271, 272
 - overview 268–270
 - partitioning domains
 - assigning domain controllers 276–279
 - network topology diagram 273–274
 - optimizing replication traffic 272
 - partitioning process 273
 - placing domain controllers in sites 274–276
 - strategies 277–278
 - planning process 257–259, 270
 - renaming domains 294
 - restructuring 268, 293–294
 - single-domain environments 270
 - site topology *See* Active Directory site topology
 - trust relationships *See* Trust relationships
- Active Directory Domains and Trusts snap-in
 - native-mode switch 348
 - setting explicit trusts between forests 405
- Active Directory Knowledge Consistency Checker 306
- Active Directory organizational units
 - associated access control lists 397, 398
 - consolidating resource domains 373–375
 - delegating administration
 - access control lists 298–299
 - built-in delegation permissions 427
 - delegation models 271, 297–298
 - full control 300–301
 - Group Policy objects *See* Group Policy, delegating client administration
 - of computers and users 428
 - of sites and services 427
 - OU structure 299–300
 - per-object class control 302–303
 - security considerations 426–427
 - two-tiered delegation 299
 - upgrading resource domains 334–335, 360
 - disk space requirements 297

Index

- Active Directory organizational units (*continued*)
 - Group Policy considerations 304
 - hiding objects 304
 - mixed-mode domains 336
 - overview 295–297
 - restructuring 305
 - structure planning 257–259, 297
- Active Directory Service Interfaces (ADSI) 256
- Active Directory site topology
 - account replication
 - changes to 307
 - creating replication connections 306
 - inter-site vs. intra-site 306
 - Knowledge Consistency Checker (KCC) 306
 - locator record lookup 314
 - optimizing traffic 272
 - replicating or splitting domains 277–278
 - replication interval 306, 309, 311
 - schedule 305, 309, 311
 - site link cost value 305, 310, 311
 - transport 306, 310, 311
 - client connections 306, 308
 - Configuration container *See* Configuration container
 - DNS client configuration 314
 - overview 305–307
 - partitioning domains *See* Active Directory domain structure
 - planning process 257–259, 307
 - planning task list 315
 - restructuring after deployment 315
 - servers
 - adding domain controllers 312
 - DNS servers 313–314
 - Global Catalog servers 313
 - location 312
 - sites without domain controllers 308
 - sites
 - connecting 309–311
 - creating 308–309
 - defining 308
 - definition 305
 - diagramming links 273–274
 - names, example 311
 - naming 308
 - site link parameters 305
 - subnets 308
- Active Directory Sites and Services snap-in
 - delegating control of sites and services 427
 - modifying certificate ACLs 459
- Active Directory Users and Computers snap-in
 - adding users to security groups 400
 - configuring Remote Installation 883
 - delegating control of computers and users 428
 - enabling remote access 395
 - opening user accounts 388
 - security settings, built-in groups 427
 - viewing Group Policy security settings 413
 - viewing OU access control lists 398
- Active Directory Users and Groups snap-in 298
- Active Server Pages (ASP) security 425
- Ad hoc labs 103–104, 106
- ADC *See* Active Directory Connector
- Add/Remove Programs
 - applications in Terminal Services 613
 - applications installed using ZAP files 891
 - component services 572
 - published applications 894
 - removing applications 895, 900
- Administrators group
 - default permissions 400
 - default permissions in Terminal Services 605–606
 - default rights in security templates 419–421
- ADSI (Active Directory Service Interfaces) 256
- ADSL (Asymmetric DSL) 225
- Advertising applications
 - MMC snap-in *See* Software Installation snap-in
 - SMS *See* Systems Management Server software distribution
- Analyzing network infrastructure *See* Systems Management Server
- Answer files
 - [GuiRunOnce] section
 - creating domain controller 482, 485
 - installing client applications 940–943
 - installing server applications 489–491
 - running Sysprep 497, 503, 950, 956
 - client setup
 - bootable CD answer file 960
 - creating answer files 933–935
 - ExtendOEMPartition parameter 936–937
 - installing applications 940–943
 - installing HALs 926, 930
 - installing mass storage devices 926, 928
 - installing NTFS 937
 - installing Plug and Play devices 929, 930, 931

- Answer files (*continued*)
 - client setup (*continued*)
 - multiple answer files 923
 - naming answer files 932
 - OEMFILESPATH key 926
 - OemPnPDriversPath parameter 927
 - overview 932
 - setting passwords 935–936
 - Setup Manager 933
 - Sysprep.inf *See* Sysprep client imaging
 - Unattend.doc 926
 - Unattend.txt 932
 - Windows 2000 enhancements 945–946
 - default 1037, 1040–1042
 - examples
 - installing Internet Explorer 1044–1048
 - installing Network Load Balancing 1050–1054
 - installing Professional from CD 1042–1044
 - installing two network adapters 1048–1050
 - installing Windows Clustering 1054–1058
 - on CD 480, 932
 - Sysprep.inf 498–499, 952–953
 - Unattend.txt 1040–1042
 - file format 1039
 - key and value formats 1039
 - local copy 936
 - server setup
 - bootable CD answer file 507
 - creating answer files 481–483
 - creating domain controllers 482, 485
 - ExtendOEMPartition parameter 484
 - installing applications 489–491
 - installing HALs 474, 478
 - installing mass storage devices 474, 476
 - installing NTFS 484
 - installing Plug and Play devices 477, 478, 479
 - local copy 484
 - multiple answer files 471
 - naming answer files 480
 - OEMFILESPATH key 474
 - OemPnPDriversPath parameter 475
 - overview 480–481
 - setting passwords 483–484
 - Setup Manager 481
 - Sysprep.inf *See* Sysprep server imaging
 - Unattend.doc 474
 - Unattend.txt 480
 - Windows 2000 enhancements 492–493
- Answer files (*continued*)
 - SMS software distribution
 - enabling unattend mode 525
 - multiple answer files 524
 - omitting name in Setup command 525
 - security 528
 - specifying answer file to use 523
 - user input considerations 524–525
 - Windows 95 or Windows 98 upgrade domain settings 527–528
 - Windows NT upgrades 528
 - specifying in Setup command 481, 932
 - Uniqueness Database file, specifying 1034, 1036
- Antivirus software 182, 183, 786
- APIPA (Automatic Private IP Addressing) 193, 815
- APIs, monitoring using ApiMon 790
- AppleTalk protocol
 - loading 568
 - routing structure 215
 - Services for Macintosh 802
 - Windows servers in AppleTalk zones 809
- Application servers
 - See also* Member servers
 - installing Windows 2000 571–573
- Application Specification for Windows 2000
 - accessibility standards 1077
 - certification for compatible applications 13, 784
 - desktop and distributed applications 784
 - directory of compatible applications 784–785
 - Microsoft test plan 786
 - Web site 786
 - Windows 2000 Compatibility Guide 790
- Applications
 - antivirus compatibility 182, 183
 - backup domain controllers
 - avoiding pass-through authentication 347
 - incompatible applications on 326
 - client configuration standards
 - configuration management technologies 871–872
 - defining 78–79, 829–830
 - enforcing 250–251, 897–900
 - overview 908–910
 - planning task list 916
 - planning worksheets 1025–1026
 - SMS tools 876–878
 - support standards 832–833, 835, 871
 - version control 251

Index

Applications (*continued*)

- compatibility testing
 - accessibility options 1077
 - antivirus software 182, 183, 786
 - applications, definition 773
 - certified compatible 13, 784–785
 - commercial applications 785–786
 - custom applications 786
 - deployment tests 786–788
 - domain migration issues 326–327
 - inventorying *See* Software inventory
 - lab *See* Test labs
 - list of compatible applications 784–785
 - managing tests 771–775
 - Microsoft specification *See* Application Specification for Windows 200
 - migration DLLs 787
 - overview 771–774
 - pass-fail criteria 783
 - planning worksheets 1019–1020
 - prioritizing applications 775, 778–779
 - resolving incompatibilities 794–795
 - results, reporting 794
 - results, tracking 791–794
 - scenarios 134–135, 786–789
 - Setup Check Upgrade Only 785
 - SMS product compliance database 244–247
 - test plan 131–134, 779–784
 - testing process 774, 795–796
 - tools for testing 785, 789–790
 - Windows 2000 Compatibility Guide 790
 - Windows compatibility issues 182–183, 561, 790–791
- debugging
 - ApiMon tool 790
 - Dependency Walker tool 789
- deployment planning tips 66, 67
- deployment testing 786–788
- digital certificates
 - Authenticode 422–423
 - public key cryptography *See* Public key infrastructure
- directory-aware 256, 261
- life cycle 897–899
- line-of-business
 - documenting 169
 - Terminal Services 588–589
- migration DLLs 787
- redundant 777

Applications (*continued*)

- removing 787, 900
 - secure
 - access permissions to run 420–421
 - Authenticode 422–423
 - Microsoft certification security standards 421
 - security considerations 421–422
 - server configuration standards 78
 - service packs and patches 899
 - site-licensed, managing 778
 - unauthorized 778
 - version control 791, 251
 - Windows 2000 Application Specification 786
 - certification for compatible applications 784
 - desktop and distributed applications 784
 - Windows Logo Application Certification
 - vendor testing 784
 - ARP servers 224, 226
 - ASP (Active Server Pages) security 425
 - Asymmetric DSL (ADSL) 225
 - Asynchronous Transfer Mode (ATM)
 - benefits of 222
 - Call Manager 222
 - client connectivity 809–810
 - components 225
 - drivers 177
 - Infrared Data Association protocol 810
 - IP over ATM services 224, 226, 810
 - LAN Emulation
 - client connectivity 809
 - configuring connections 800
 - default ELAN 223, 226
 - example 223
 - preparing clients for upgrade 226
 - Multicast and Address Resolution Service 224, 226
 - NDIS ATM network adapter support 223
 - PPP over ATM 225
- ### Auditing
- audit logs 428–430
 - audit policy 416
 - disk space 429
 - events affecting the registry 418
 - events to audit 430
 - failed and successful events 417
 - file and folder events 418, 429
 - implementing 429
 - overview 387
 - process 428

- Auditing (*continued*)
 - System Services policy 417
 - viewing log file 429
 - Authenticated Users group 396, 397
 - Authentication
 - Active Directory domain database 269
 - avoiding pass-through 347
 - best practices 389–390
 - computers 389
 - definition of 385
 - delegating network connections 389, 390
 - IAS *See* Internet Authentication Service
 - Kerberos *See* Kerberos authentication
 - mutual 389
 - NTLM *See* NTLM authentication
 - optimizing with shortcut trusts 292
 - overview 388–389
 - remote client *See* Remote access authentication
 - services 389
 - single logon process feature 385, 388, 390
 - smart cards *See* Smart cards
 - two-factor 385, 389
 - user accounts 388
 - Web site security 425
 - Windows 2000 security model 383
 - Authenticode 422–423
 - Autoexec.nt 561
 - Automated client installation
 - benefits and features 944–946
 - examples 966–970
 - installing applications
 - available methods 939
 - using answer files 940–943
 - using Cmdlines.txt *See* Cmdlines.txt
 - using Windows Installer *See* Windows Installer
 - installing Windows 2000 Professional
 - Syspart 947–949
 - using bootable CD *See* Bootable CD
 - using Remote OS Installation *See* Remote Operating System Installation
 - using SMS *See* Systems Management Server
 - software distribution
 - using Sysprep *See* Sysprep client imaging
 - planning worksheets 1027–1028
 - process 921–922, 945
 - task list 971
 - technologies 939, 946–947
 - Automated client installation (*continued*)
 - upgrade vs. clean install
 - determining best method 919–921
 - installation method capabilities 921, 939
 - what you can install 944
 - Automated server installation
 - automated installation features 491–493
 - examples 508–512
 - installing applications
 - available methods 487
 - technologies 487
 - using answer files 489–491
 - using Cmdlines.txt *See* Cmdlines.txt
 - using Windows Installer *See* Windows Installer
 - installing Windows 2000 Server
 - Syspart 494–495
 - using bootable CD *See* Bootable CD
 - using SMS *See* Systems Management Server
 - software distribution
 - using Sysprep *See* Sysprep server imaging
 - planning worksheets 999–1000
 - process 469–470, 492
 - task list 512
 - technologies 493–494
 - upgrade vs. clean install
 - determining best method 467–469
 - installation method capabilities 469, 487
 - what you can install 492
 - Automatic Private IP Addressing (APIPA) 193, 815
 - Autonomous systems, OSPF networks 210–211
 - Availability *See* Windows Clustering
 - Availability planning worksheet 986–988
- ## B
- Backup domain controllers
 - application servers 347
 - mixed mode 348
 - PDC emulator replication 339
 - physical security 348
 - upgrading 179
 - Windows 2000 incompatible applications 326
 - Windows 2000 native-mode domains 322, 337
 - Backup program 724
 - Back-ups *See* Data backup and recovery
 - Bandwidth Allocation Protocol 198
 - Bandwidth control, QoS 227
 - Basic security template 420
 - Basic storage disks 705–706

Index

- BIND service 168
- Bootable CD
 - client installation
 - answer file requirements 960
 - answer files *See* Answer files
 - automated installation enhancements 945–946
 - automated installation methods 946–947
 - BIOS boot order 959
 - distribution folders *See* Distribution folders
 - El Torito No Emulation support 960
 - installation process 921–922, 960
 - Uniqueness Database Files 960
 - when to use 959
 - server installation
 - answer file requirements 507
 - answer files *See* Answer files
 - automated installation enhancements 492–493
 - automated installation methods 493–494
 - BIOS boot order 507
 - distribution folders *See* Distribution folders
 - El Torito No Emulation support 507
 - installation process 469–470, 508
 - Uniqueness Database Files 508
 - when to use 507
- Bootstrap protocol 219
- C**
- Capacity planning 85–86
- CD-ROM devices, Removable Storage system 709
- Certificates snap-in 438
- Certification authorities *See* Public key infrastructure
- Certification Authority snap-in
 - configuring revocation lists 460
 - importing certificate requests 457
 - managing local certificate authorities 438
 - specifying certificate types 459
- Certified applications
 - Authenticode certificates 422–423
 - Microsoft certification security standards 421
 - public key cryptography *See* Public key infrastructure
 - software signing 422–423
- Certified for Windows 2000 program
 - accessibility requirements 1077
 - compatibility issues 561
 - directory of compatible applications 784–785
 - vendor testing 784
 - Web site 13
- CGI (Common Gateway Interface) 425
- Challenge Handshake Authentication Protocol (CHAP) 198, 638
- Change management labs
 - post-deployment testing 137
 - return on investment 104–105
 - role of the lab 137–139
 - vs. ad hoc labs 106
- Child domains
 - incorrectly joined 333
 - multiple-tree environments 283–284, 292
 - single-tree environments 282–283
 - upgrading 343–344
- CIDR (Classless Interdomain Routing)
 - custom subnetting 195
 - RIP for IP networks 208, 209
- CIFS (Common Internet File System) protocol 806, 808
- Classless interdomain notation 195
- Classless Interdomain Routing (CIDR)
 - custom subnetting 195
 - RIP for IP networks 208, 209
- Clean install vs. upgrade decision
 - example deployment scenario 48
 - Windows 2000 Professional
 - determining best method 919–921
 - installation method capabilities 921, 939
 - Windows 2000 Server
 - determining best method 467–469
 - installation method capabilities 469, 487
- Client configuration plan
 - applications *See* Applications, client configuration standards
 - client administration plan 839–840
 - configuration management plan 908–910
 - configuration recovery 873
 - deployment scenario 60–62
 - hardware configuration *See* Hardware overview 823–827, 869–872
 - planning tasks 868, 916
 - planning worksheets 980–982, 1021–1026
 - strategies for different users 910–915
 - support plan
 - current support issues 832–833, 871
 - IT administration model 833–835
 - managed environments 835
 - unmanaged environments 835

- Client configuration plan (*continued*)
 - user interface
 - accessibility 865–867
 - defining standards 853–855
 - multilingual 859–864
 - user types, defining 827–829
- Client connectivity *See* Network connectivity
- Client Installation wizard 1078, 1079
- Client Service for NetWare 213, 804, 805
- Clock setting, Kerberos authentication 391
- ClonePrincipal utility 371, 376–377
- Cloning computers
 - definition of 47
 - RIS images *See* Remote OS Installation
 - Sysprep *See* Sysprep client imaging; Sysprep server imaging
- Cluster servers, NetBIOS 353
- Cluster service
 - applications on server clusters 672–673
 - backup and recovery strategy
 - cluster backup and restore 695–696
 - cluster remapping 693
 - emergency repair disk 695
 - backup server 671
 - deploying 690–691
 - deployment planning tasks 671–672, 696–697
 - IPX protocol 672
 - limitations 689–690
 - NetBEUI protocol 672
 - planning for availability
 - downtime costs 649–651
 - hardware compatibility 657–658
 - identifying network risks 656–657, 673–674
 - needs assessment 655–657
 - planning tasks 652–653
 - planning team 654–655
 - RAID considerations 674, 690
 - Removable Storage devices 689
 - resource groups
 - dependency tree 687–688
 - failover policies 674–675
 - fallback policies 675
 - placing resources in groups 684–688
 - server capacity requirements 688–689
 - server cluster models
 - dedicated secondary node 677–679
 - high availability configuration 679–684
 - single node server cluster 676–677
 - server clusters, described 671
- Cluster service (*continued*)
 - server roles 675–676
 - Terminal Services 690
 - testing server capacity 693–695
- Cluster, definition 653
- Clustering, Windows *See* Windows Clustering
- Cmdlines.txt
 - client applications 939–940, 956
 - server applications 487–488, 502
- Code signing
 - authenticating code downloaded from Internet 386
 - Authenticode 422–423
 - public key cryptography *See* Public key infrastructure
- Common Gateway Interface (CGI) 425
- Common Internet File System (CIFS) protocol 806, 808
- Communications planning worksheet 988–990
- Compatible security template 420
- Component services
 - adding 572
 - planning worksheet 985–986
- Computer accounts
 - See also* Security principals
 - authentication 389
 - managing using Netdom 371, 377
 - moving to restructure domains 369–370
 - trusted for delegation 389, 390
- Computer local groups 399
- Computer Management snap-in
 - remote access policies 394–395
 - viewing migrated Macintosh volume 566
- Computer names 287
- Config.nt 561
- Configuration container
 - autonomous domain administration 272
 - definition 261
 - directory-aware applications 261
 - Enterprise Administrators group 261
 - located on domain controllers 269
 - replicated to domain controllers 307
 - trust relationships 405
- Conflict resolution, multiple-master replication 340
- Conflict resolution, security groups and account replication 402
- Connection Manager 201
- Connectivity *See* Network connectivity
- Consolidating domains *See* Domain restructure
- CryptoAPI 453

Index

- Custom application compatibility issues 786
 - Custom Policy modules, create using CryptoAPI 453
 - Custom subnet masks 195–196
- ## D
- Data backup and recovery
 - Active Directory/Exchange Server synchronization
 - authoritative restore 765, 766
 - backups 765
 - planning for 765
 - populating Active Directory with new objects 766
 - populating attributes 766
 - stopping synchronization in progress 765–766
 - backing up and restoring license servers 598
 - backing up servers before upgrading 563
 - backup policies 726–727
 - Backup program 724
 - certification authority failures 452–453
 - client configuration recovery 873
 - clusters
 - backup and restore 695–696
 - cluster remapping 693
 - emergency repair disk 695
 - fault tolerance 692
 - hardware RAID 692
 - transaction logging and recovery 693
 - data protection strategies 725
 - disaster recovery planning
 - backup policies 726–727
 - documenting recovery procedures 729
 - needs assessment 727–728
 - off-site storage policies 727
 - preparing for system failures 725–726
 - testing 728–729
 - domain migration recovery plan 332–333
 - recovering files encrypted using EFS 408
 - Data confidentiality
 - definition of 386
 - Encrypting File System (EFS) 407
 - IPSec (Internet Protocol security) 410
 - smart cards 392
 - Data integrity
 - definition of 386
 - IPSec (Internet Protocol security) 410
 - secure e-mail 424
 - signing data packets *See* Public key infrastructure
 - smart cards 392
 - Data management
 - clustering *See* Windows Clustering
 - Indexing Service 720–722
 - storage *See* Storage management
 - user data *See* IntelliMirror user data management
 - Data packets, signing *See* Public key infrastructure
 - Data protection technologies 406
 - Database application servers 573
 - Debugging applications
 - ApiMon tool 790
 - Dependency Walker tool 789
 - Default subnet masks 309
 - Defragmenting disks 708
 - Delegating administration
 - access control lists 298
 - built-in group delegation permissions 427
 - delegation models 271, 297–298
 - full control 300–301
 - Group Policy objects
 - Active Directory namespace design 839–840
 - associated Active Directory containers 839
 - delegating administration of Group Policy 840–842
 - directory service control 840
 - links to Active Directory containers 840
 - Microsoft Management Console 842
 - object access permissions 841
 - of computers and users 428
 - of sites and services 427
 - OU structure 299–300
 - per-object class control 302–303
 - principle of least privilege 427
 - security considerations 426–427
 - security groups 427
 - two-tiered delegation 299
 - upgrading resource domains 334–335
 - Delegating network connections 389, 390
 - Demand-dial connections, VPN 201
 - Demilitarized zone (DMZ)
 - designing 190–191, 632–633
 - example 203–204
 - Dependency Walker 789
 - Deployment project plan
 - Active Directory design
 - corporate structure 64
 - Exchange Server integration 63–64
 - sample deployment scenario 45–48
 - technology dependencies 63
 - capacity planning 85–86

- Deployment project plan (*continued*)
 - configuration standards and guidelines 78–79
 - deployment best practices 64–67
 - deployment phases 39–40, 65
 - deployment planning tasks 68, 92
 - deployment scenarios 45–62
 - Active Directory design 45–48
 - client deployment process 60–62
 - computer cloning 47
 - deployment teams 45–46
 - DNS root name 45, 47
 - domain design 45–48
 - evaluating Windows 2000 features 49
 - feature design case studies 15–24
 - pilot project 50
 - roaming users 51
 - server deployment process 52–59
 - test lab 50
 - upgrade vs. migration considerations 48
 - Windows 2000 infrastructure design 55–57
 - deployment schedule 89–90
 - deployment teams
 - client team scenario 52, 60–62
 - communication strategies 84–85
 - example scenarios 45–46, 73–74
 - management roles 75–77
 - organizing 72–77
 - server team scenario 52–59
 - documenting current environment 77–78
 - feature design phase
 - example case studies 15–24
 - functional design specification 41–42, 83
 - mapping features to needs 12–14, 24–34
 - planning process 8
 - technology dependencies 62–64
 - gap analysis 79
 - getting started 3–8
 - goals and objectives phase 40–41, 71–72
 - international installations 66
 - migration plan, example scenarios 51–62
 - overview 37–40
 - pilot phase 42–43, 80–81
 - See also* Pilot project
 - planning documents, types of 81–83
 - planning worksheets
 - component application services 985–986
 - desktop management solutions 980–982
 - information publishing and sharing 984
 - management infrastructure worksheet 978–980
- Deployment project plan (*continued*)
 - planning worksheets (*continued*)
 - networking and communications 988–990
 - scalability and availability 986–988
 - security features 982–984
 - storage management 990–992
 - production rollout phase 44, 90–91
 - project management process 39–40
 - project scope 71
 - risk management planning 86–90
 - tasks for creating 37, 34
 - test plan 80–81
 - user education 85
- Deployment tools 1059–1070
- Designing labs *See* Test labs, designing
- Desktop applications specification 784
- Desktop management planning worksheet 980–982
- Device drivers, incompatible 183
- Device support enhancements 9
- Dfs (Distributed file system) 716–720, 565–566
- DHCP (Dynamic Host Configuration Protocol)
 - benefits of 218
 - bootstrap protocol support 219
 - centralized design 220–221
 - client connectivity 802–803
 - DHCP Manager 218, 220
 - distributed design 220–221
 - DNS integration 178, 219
 - dynamic assignment of IP addresses 217
 - multicast address allocation 218
 - new features 218–220
 - Remote Installation servers 962–964, 966
 - server placement 178
 - unauthorized server detection 219
 - WINS (Windows Internet Name Service) 196
- Diagramming
 - physical and logical networks 165–167, 187–188
 - test lab 122–125
- Dial-up connections
 - dial-up profiles
 - and remote access policy 199
 - creating 818
 - VPN connections 201, 640, 916
 - direct to remote access server 811, 818
 - Network and Dial-up Connections folder 800
 - Network Connection wizard 810–811, 817
 - on-demand router-to-router VPN example 203
 - security risks 638
 - slow link processing options 845

Index

- Dial-up connections (*continued*)
 - software installation and maintenance 896
 - Terminal Services
 - bandwidth considerations 592, 608
 - print jobs 616
 - Windows-based terminals 611
 - to virtual private networks 812, 818
 - user authentication *See* Remote access authentication
- Digital certificates
 - Authenticode software signing 422–423
 - public key cryptography *See* Public key infrastructure
- Digital subscriber lines, PPP over ATM 225
- Directory of Window-compatible applications 784–785
- Directory synchronization, Exchange Server *See* Active Directory Connector
- Directory-aware applications 256, 261
- Disaster recovery
 - backing up data *See* Data backup and recovery
 - Backup program 724
 - certification authority failures 452–453
 - client configuration recovery 873
 - clusters
 - backup and restore 695–696
 - cluster remapping 693
 - emergency repair disk 695
 - fault tolerance 692
 - hardware RAID 692
 - data protection strategies 725
 - disaster recovery planning
 - backup policies 726–727
 - documenting recovery procedures 729
 - domain migration recovery plan 332–333
 - needs assessment 727–728
 - off-site storage policies 727
 - preparing for system failures 725–726
 - testing 728–729
 - fault tolerance *See* Fault-tolerant systems
 - risk management planning 86–90
- Disk Defragmenter 708
- Disk imaging
 - RIS images *See* Remote Operating System Installation
 - Sysprep *See* Sysprep client imaging; Sysprep server imaging
- Disk management
 - See also* Storage management
 - fault tolerance *See* Fault-tolerant systems
 - MMC snap-in *See* Disk Management snap-in
 - quota management *See* Disk quotas
 - Remote Storage system 710–712
 - Removable Storage system 709–711
 - Windows features 699, 704
- Disk Management snap-in
 - basic storage 705–706
 - Disk Defragmenter 708
 - disk quotas 715
 - dynamic storage 705–706, 708
 - initializing disks 706
 - Logical Disk Manager 707
 - managing basic and dynamic disks 706
 - online disk management 704
 - overview 704–705
 - remote disk management 704
 - volume management 707
 - volume mount points 707–708
- Disk quotas
 - default 715
 - Disk Management snap-in 715
 - file ownership 715
 - guidelines for setting 907
 - NTFS file system 716
 - setting 715–716
 - storage management features 716
- Disk space
 - Active Directory objects 297, 328
 - certificate databases 455
 - Cluster services requirements 689
 - event log 429
 - managing using Remote Storage 710–712
 - MultiLanguage version 916
 - Network Load Balancing component 670
 - print servers 569
 - server requirements, estimating 180, 238, 560
 - shared disk space quotas *See* Disk quotas
 - Terminal Services client requirements 611
 - user accounts database 560
- Distance-vector routing protocol 208
- Distributed applications specification 784
- Distributed file system (Dfs) 716–720, 565–566
- Distributed security planning *See* Security strategies

- Distribution folders
 - client installations
 - \SOEM\$ subfolder 926–927
 - \SOEM\$\$ subfolder 927
 - \SOEM\$1 subfolder 927
 - \SOEM\$1\pnprvrs subfolder 927, 930
 - \SOEM\$1\Sysprep subfolder 927, 939
 - \SOEM\$drive_letter subfolder 927
 - \SOEM\$textmode subfolder 926, 928, 930
 - %systemdrive% variable 927
 - %systemroot% variable 927
 - %windir% variable 927
 - Cmdlines.txt location 939
 - creating 923–924
 - distribution servers, multiple 923
 - distribution servers, specifying path 938
 - distribution share root 926
 - file names, converting long 927, 931–932
 - file names, short file names required 927
 - hardware abstraction layer setup 926, 929–930
 - i386 folder 924, 926
 - mass storage devices 926, 928–929
 - naming root folder 924
 - Plug and Play devices 927, 930–931
 - structure 924–927
 - Txtsetup.oem 926, 928, 929
 - Unattend.doc 926
 - server installations
 - \SOEM\$ subfolder 474
 - \SOEM\$\$ subfolder 475
 - \SOEM\$1 subfolder 475
 - \SOEM\$1\pnprvrs subfolder 475, 478
 - \SOEM\$1\Sysprep subfolder 475, 487
 - \SOEM\$drive_letter subfolder 475
 - \SOEM\$textmode subfolder 474, 476, 478
 - %systemdrive% variable 475
 - %systemroot% variable 475
 - %windir% variable 475
 - Cmdlines.txt location 487
 - creating 471–472
 - distribution servers, multiple 471
 - distribution servers, specifying path 487
 - distribution share root 473, 474
 - file names, converting long 475, 479–480
 - file names, short filenames required 475
 - hardware abstraction layer setup 474, 477–478
 - i386 folder 472, 473
 - mass storage devices 474, 476–477
 - naming root folder 472
- Distribution folders (*continued*)
 - server installations (*continued*)
 - Plug and Play devices 475, 478–479
 - structure 472–475
 - Txtsetup.oem 474, 476, 477
 - Unattend.doc 474
 - SMS packages 521
 - Distribution groups 398
 - DLLs (dynamic-link libraries)
 - inventorying 240
 - migration DLLs 787, 528
 - DMZ (demilitarized zone)
 - designing 190–191, 632–633
 - example 203–204
 - DNS (Domain Name System)
 - client configuration 314
 - client connectivity 802–803
 - delegation points 288–289
 - DHCP integration 219
 - DNS database 288
 - dynamic registration support 168
 - dynamic synchronization with DHCP 178
 - Exchange Server integration 63
 - forest namespace 332, 333
 - locator records 289, 314
 - multihoming 206–207
 - naming domains *See* Active Directory domain
 - structure, DNS domain names
 - naming sites 308
 - resource records 288
 - reverse lookup zones 289
 - round robin DNS 667–668
 - servers authoritative for domain names
 - corresponding locator records 289
 - identifying 287–289
 - server requirements 290–291
 - servers, site topology 313–314
 - Service (SRV) resource record support 168
 - technology dependencies 63
 - Terminal Services load balancing 599
 - Windows Internet Name Service integration 196
 - zones 288–289, 314
 - Domain administrator account, security 426
 - Domain Administrators group
 - autonomous domain administration 272
 - control over objects in domain 300
 - dedicated domains 281
 - Group Policy object permissions 840–841
 - member of local administrators group 402

Index

- Domain Administrators group (*continued*)
 - monitoring membership 279
 - overview 269
- Domain controllers
 - assigning domains to 276–277, 278–279
 - Configuration container
 - autonomous domain administration 272
 - definition of 261
 - directory-aware applications 261
 - located on domain controller 269
 - replicated to domain controller 307
 - consolidating domains *See* Domain restructure
 - designating as Global Catalog Server 313
 - documenting current structure
 - administration model 170–171
 - logical network diagram 167
 - physical network diagram 165–166
 - domain database 269
 - PDC emulation
 - conflict resolution 340
 - overview 339
 - properties 340
 - physical security 275
 - placing in domains 312
 - placing in sites 274–276
 - preparing for upgrade 177–178
 - promoting servers to 482, 485
 - Schema container 269
 - site topology *See* Active Directory site topology
 - sites without domain controllers 275, 308
 - upgrading 179
- Domain local groups
 - domain migration 349
 - group expansion 352
 - mixed mode 399
 - nested security groups 351
 - properties 350
 - when to use 399
 - Windows NT 3.51 327
- Domain Master browser 339
- Domain Name System *See* DNS
- Domain restructure
 - child domain incorrectly joined 333
 - consolidating resource domains 373–375
 - definition of 323
 - domain migration basic utilities 359
 - example scenarios 371–375
 - incremental migration 371–373
 - migration goals 321–322
- Domain restructure (*continued*)
 - migration planning phases 319–321
 - moving computers 369–370
 - moving domain controllers 361
 - moving member servers 370
 - moving users and groups 361–369
 - planning task list 378
 - reasons to restructure 325–326, 359–360
 - two-phase migration 325
 - when to restructure 326, 329, 360–361
- Domain upgrade
 - access control components 340–341
 - account domains 342–343
 - Active Directory disk space requirements 328
 - Active Directory namespace 317
 - application compatibility 326–327
 - backup domain controllers
 - application servers 347
 - incompatible applications on 326
 - mixed mode 348
 - native mode 322, 337
 - PDC emulator replication 339
 - physical security 348
 - upgrading 179
 - definition of 322, 329
 - designing Windows 2000 domains *See* Active Directory domain structure
 - domain controllers 179
 - examining existing structure 331–332
 - FRS *See* File Replication Service
 - interoperability, defining requirements 327–328
 - Kerberos *See* Kerberos authentication
 - LAN Manager *See* LAN Manager Replication Service
 - mean time between failures 321, 322
 - migration goals 321–322
 - mixed mode *See* Mixed mode
 - multiple-master domains
 - conflict resolution 340
 - domain model 331
 - explicit trusts 331, 334
 - mixed mode 336
 - native mode 337
 - PDC emulation 339
 - native mode
 - backup domain controllers 322, 337
 - definition of 337
 - irreversible switch 338, 347
 - Netlogon synchronization disabled 337

- Domain upgrade (*continued*)
 - native mode (*continued*)
 - PDC emulation enabled 337
 - reasons for switching to 348
 - running applications 326
 - security groups 349–352
 - switching to 336, 337–338, 348
 - transition from mixed mode 337
 - trusts in child domains 343–344
 - when to switch to 322, 325
 - Windows 2000 features in 335–336
 - NetBIOS 353–354
 - Netlogon synchronization 337
 - non-Microsoft operating systems 328
 - order of upgrading
 - account domains 342
 - Active Directory 255
 - clients and member servers 323–324, 325, 330
 - domain controllers 325, 179
 - domains 325
 - resource domains 342
 - RRAS servers 327, 358
 - PDC emulation
 - conflict resolution 340
 - native-mode switch 337
 - overview 339
 - properties 340
 - phases 319–321
 - planning worksheets 996–998
 - primary domain controller
 - Active Directory installation 338
 - emulating *See* PDC emulation
 - order of upgrading 325
 - upgrading 338
 - recovery plan 332–333
 - resource domains 334–335, 342, 343
 - RRAS servers 327, 358–359
 - SAM database size 334, 342, 360
 - security groups
 - ClonePrincipal utility 376–377
 - upgrading Windows NT 349–352
 - Windows 2000 349
 - task lists 330, 378
 - trust relationships
 - determining explicit 331
 - Kerberos authentication 336
 - master domains 334
 - multiple-master domains 262, 331, 334
 - Netdom utility 371, 377
 - Domain upgrade (*continued*)
 - trust relationships (*continued*)
 - NTLM authentication 345
 - primary domain controllers 338
 - resource domain in new tree 335
 - upgraded child domains 343–344
 - upgrade paths 319, 330
 - upgrade process 329–330
 - upgrading member servers *See* Member servers
 - user account passwords maintained 329
 - versus restructuring 324–325
 - Windows NT browser service 339
 - Windows NT interoperability 329
 - Dual-boot systems 715
 - DVD-ROM devices, Removable Storage system 709
 - Dynamic data storage, Cluster service 689
 - Dynamic Host Configuration Protocol *See* DHCP
 - Dynamic storage disks 705–706, 708
 - Dynamic-link libraries (DLLs)
 - inventorying 240
 - migration DLLs 787, 528
- ## E
- EAP (Extensible Authentication Protocol)
 - extensions for PPP 395
 - L2TP user authentication 204
 - preventing user name interception 638
 - EAP Transport Layer Security authentication 396, 638
 - EFS *See* Encrypting File System
 - E-mail security
 - planning considerations 424–425
 - public key cryptography *See* Public key
 - infrastructure
 - S/MIME standard 424
 - security risks 424
 - Emergency repair disk 695
 - Encrypting File System (EFS)
 - Data Recovery policy 408
 - encryption keys 407
 - implementing 407
 - overview 406–407
 - public key cryptography *See* Public key
 - infrastructure
 - recovery agents 407, 408
 - recovery strategies 408
 - shared servers 408
 - specifying recovery account 460

Index

- Enterprise Administrators group
 - configuration change policy 268
 - Configuration container 261
 - forest root domain 281
 - Group Policy object permissions 840–841
 - security considerations 426
 - Enumerating domain trusts 371
 - Escalation plans 131
 - Event logging 428–430
 - audit policy 416
 - disk space 429
 - Event Log policies 416
 - events affecting the registry 418
 - events to audit 430
 - failed and successful events 417
 - file and folder events 418, 429
 - implementing 429
 - overview 387
 - process 428
 - System Services policy 417
 - viewing log file 429
 - Event Viewer
 - overwriting old log entries 429
 - viewing log file 429
 - Everyone group
 - default permissions 400
 - restricting access to network shares 397
 - Example deployment planning worksheets *See* planning worksheets
 - Example deployment scenarios 45–62
 - Active Directory design 45–48
 - client deployment process 60–62
 - computer cloning 47
 - deployment planning teams 45
 - DNS root name 45, 47
 - domain design 45–48
 - evaluating Windows 2000 features 49
 - pilot project 50
 - roaming users 51
 - server deployment process 52–59
 - test lab 50
 - upgrade vs. migration considerations 48
 - Windows 2000 infrastructure design 55–57
 - Exchange Server
 - integration considerations 63–64
 - synchronization *See* Active Directory Connector
 - Executable files, inventorying 240
 - Explicit trusts *See* Trust relationships
 - Extensible Authentication Protocol (EAP)
 - extensions for PPP 395
 - L2TP user authentication 204
 - preventing user name interception 638
 - Extranet, definition of 646
- ## F
- Failover
 - application data location 673
 - cluster-aware applications 673
 - cluster-unaware applications 673
 - definition of 654
 - described 712
 - failover policies 674–675
 - fallback policies 675
 - FAT file systems
 - converting to NTFS 714
 - defragmenting disks 708
 - supported in Windows 2000 714
 - Fault-tolerant systems
 - designing 725
 - error recovery 693
 - hardware RAID 692
 - overview 723
 - RAID configurations 723–724
 - transaction logging and recovery 693
 - Fibre Channel 32, 709
 - File and Print Services for NetWare 568, 805, 806
 - File filter compatibility issues
 - Windows 2000 I/O 791
 - Windows 95 and Windows 98 183
 - Windows NT 182, 786
 - File permissions, Group Policy 852
 - File Replication Service (FRS)
 - bridge to LAN Manager replication 356–358
 - replication process 355–356
 - transition from LAN Manager replication 354–358
 - File servers
 - See also* Member servers
 - accessing NetWare 804–807
 - computer local group permissions 399
 - Macintosh access 802
 - upgrading 565–568
 - File System policies 418
 - File systems
 - Distributed file system (Dfs) 716–720, 565–566
 - EFS *See* Encrypting File System

- File systems (*continued*)
 - NTFS *See* NTFS file system
 - supported in Windows 2000 714
 - Finding files using Indexing Service 720–722
 - Firewalls
 - demilitarized zone 632
 - IAS server location 644
 - Microsoft Proxy Server 633
 - monitoring server activity 430
 - Terminal Services servers 591, 598, 608
 - virtual private networks 641–642
 - Folder redirection
 - disk quota 901, 907
 - enabling IntelliMirror user data management 902
 - implementing 904–905
 - overview 901
 - Font enumeration 791
 - Forests *See* Active Directory domain structure
 - FORTEZZA Crypto Cards 449
 - FRS *See* File Replication Service
 - Full-text indexing *See* Indexing Service
- G**
- Gateway Service for NetWare 213, 804–805, 807
 - Generic QoS 224
 - Global address book 388
 - Global Catalog
 - Active Directory objects in 262
 - Global Catalog server placement 313
 - multiple-forest environments 264, 265
 - search interface 262
 - search scope 262
 - single-forest environments 263
 - universal group updates 401
 - universal groups listed in 350
 - validating user principal names 263
 - Global groups
 - See also* Security principals
 - group expansion 352
 - members of universal groups 399
 - moving 367
 - nested security groups 351
 - properties 351
 - Restricted Groups policy 417
 - when to use 399
 - Windows NT 349
 - Group Policy
 - Active Directory
 - associated containers 412, 839
 - multiple domains 269
 - namespace design 414, 839–840
 - restructuring organizational units 305
 - delegating client administration
 - See also* delegating administration
 - Active Directory namespace design 839–840
 - directory service control 840
 - Group Policy object access permissions 841
 - implementing 840–842
 - links to Active Directory containers 840
 - MMC Consoles 842
 - folder redirection
 - disk space quota 901, 907
 - enabling IntelliMirror 902
 - implementing 904–905
 - overview 901
 - implementing 413–414
 - inheritance 413, 414
 - kiosk environments 851
 - linking objects to containers 413, 840
 - local 848–851
 - multiple-domain environments 280
 - objects, definition 837
 - offline file management 906–907
 - overview 836–837
 - planning worksheets 1023–1025
 - processing options
 - asynchronous processing 846
 - background processing 847
 - Block Policy options 844
 - client-side extensions 846–848
 - loopback options 844
 - network performance 842
 - No Override (Enforce) option 844
 - periodic refresh 846, 848
 - slow links 845, 847, 859
 - synchronous processing 846
 - public key policy
 - assigning trust lists to objects 446–447
 - automatic certificate enrollment 461
 - certificate trust lists 461
 - domain-wide scope 415
 - EFS recovery agents 460
 - root certificate trust 461
 - setting 439
 - Remote OS Installation options 886

Index

Group Policy (*continued*)
 security group filtering
 faster Group Policy processing 837
 implementing 842–843
 local Group Policy 851
 security policies
 account lockout policy 415
 Account policies 415, 415–416
 applying 412–413
 audit logging 416, 428–430
 authenticating computers and services 389
 based on domain user accounts 388
 certificate auto-enrollment policy 205
 changing 413
 computer policy 389
 Data Recovery policy 408
 delegating network connections 389, 390
 directory database 383
 enabling remote access 395
 Event Log policies 416
 File System policies 418, 852
 Internet Explorer policies 423
 Internet Protocol policies 410
 IPSec 418
 Kerberos authentication 391, 415–416
 Local Computer policies 416
 opening user accounts 388
 password policy 415
 planning considerations 414
 Registry policies 418
 remote access *See* Remote access policies
 Restricted Groups policies 417
 scope 415
 security templates 419–421
 single logon process within forest 388
 System Services policies 417
 viewing 413
 Windows 2000 security components 384
 software distribution options
 assigning applications 893–895
 distribution phase 892
 IntelliMirror technology 873–874, 878–879
 mobile users 896
 publishing applications 893–895
 roaming users 895
 shared computers 896
Terminal Services
 access to applications 602
 conflicting policies 602

Group Policy (*continued*)
 Terminal Services (*continued*)
 deploying applications 613
 installing applications 602
 remote application installation 580
 user language 614
 user interface configuration
 accessibility options 865–867, 1078, 1079
 custom logon and logoff 855
 disabling Control Panel 856
 disabling registry editors 856
 MultiLanguage policy 864
 optimizing desktop 856–858
 planning 826–827, 835, 853–855
 remote computers 858–859
 restricting user changes 856–858
 Start menu 857–858
 user profiles 854
 Windows NT system policies
 compared to Group Policy 835–836
 transferring 837–839

H

HAL *See* Hardware abstraction layers
Hardware
 adding to SMS product compliance database 244–245
 client configuration
 defining standards 830–832
 file system 852
 hardware profiles 852–853
 support standards 832–833, 835
 defining configuration standards 78–79
 Windows 2000 compatibility
 checking using Setup 116
 estimating hardware requirements 238–240
 hardware components to check 237
 member server requirements 559–560
 physical network infrastructure 176–177
 print server requirements 569
 Windows 2000 Hardware Compatibility List (HCL) 237, 562
Hardware abstraction layers (HALs)
 client installation distribution folder 926
 installing on clients 929–930
 installing on servers 477–478
 server distribution folder 474
 unique 885

- Hardware Compatibility List (HCL) 562
 - Hardware inventory
 - extracting SMS inventory data 244, 248
 - member servers 559
 - physical network diagram 165–167
 - running SMS inventory 238–240
 - selecting computers for upgrade 520, 538–540
 - SMS reports 242–244
 - SMS version 1.2 considerations 234
 - Windows NT network data 164
 - Heterogeneous environments 183, 327–328
 - See also* Mixed mode
 - High Secure security template 421
 - High-capacity disk drives 709
 - HTTP (Hypertext Transfer Protocol) 425
 - Hyberfil.sys 503, 957
 - Hypertext Transfer Protocol (HTTP) 425
- I**
- I2O (intelligent I/O) 30, 709
 - I386 distribution folder 472, 473, 924, 926
 - IANA (Internet Assigned Numbers Authority) 195
 - IAS *See* Internet Authentication Service
 - ICS (Internet Connection Sharing) 198, 813–814
 - IDE interfaces 709
 - IEEE 1394 709
 - IGMP (Internet Group Management Protocol) 215–216
 - IIS (Internet Information Services)
 - Internet Services Manager 573
 - Network Load Balancing 664
 - security features 425
 - Indexing Service 720–722
 - Information publishing and sharing worksheet 984
 - Infrared Data Association (IrDA) protocol 810
 - Installer *See* Windows Installer
 - Installing applications
 - available methods 487, 939
 - available technologies 871–874, 878–879
 - best practices 66, 67
 - using Add/Remove Programs *See* Add/Remove Programs
 - using answer files
 - See also* Answer files
 - client applications 940–943
 - server applications 489–491
 - using Cmdlines.txt *See* Cmdlines.txt
 - using IntelliMirror *See* IntelliMirror software distribution
 - Installing applications (*continued*)
 - using Remote OS Installation *See* Remote OS Installation
 - using SMS *See* Systems Management Server software distribution
 - using Software Installation *See* Software Installation snap-in
 - using Windows Installer *See* Windows Installer ZAP configuration files 891
 - Installing Windows 2000 Professional
 - automated installation features 944–946
 - available methods 946–947
 - deployment plan *See* Deployment project plan
 - estimating hardware requirements 238–240
 - example installation configurations 966–970
 - upgrade paths 330, 181
 - upgrade vs. clean install
 - determining best method 919–921
 - installation method capabilities 921, 939
 - using CD *See* Bootable CD
 - using Remote OS Installation *See* Remote OS Installation
 - using SMS *See* Systems Management Server software distribution
 - using Syspart *See* Syspart
 - using Sysprep *See* Sysprep client imaging
 - Installing Windows 2000 Server 330
 - automated installation features 491–493
 - available methods 493–494
 - deployment plan *See* Deployment project plan
 - example installation configurations 508–512
 - hardware requirements, estimating 238, 559–560
 - installation disk 564–565
 - late-breaking release notes 562
 - member servers *See* Member servers
 - upgrade vs. clean install
 - determining best method 467–469
 - installation method capabilities 469, 487
 - using CD *See* Bootable CD
 - using SMS *See* Systems Management Server software distribution
 - using Syspart *See* Syspart
 - using Sysprep *See* Sysprep server imaging
 - Instrumentation services 25
 - Integrated device electronics (IDE) interfaces 709
 - Integration tests 130–131
 - Intelligent I/O (I2O) 30, 709

Index

- IntelliMirror software distribution
 - Add/Remove Programs
 - applications installed using ZAP files 891
 - published applications 894
 - removing applications 895, 900
 - assigning applications 893–895
 - client configuration recovery 873
 - configuration management planning
 - planning worksheets 1021–1026
 - process 887–889
 - software deployment planning 878–879
 - strategies for different users 908–915
 - task list 916
 - distribution phase 892
 - IntelliMirror technology components 871–875
 - mobile users 896, 912
 - preparing applications 889–892
 - See also* Windows Installer
 - repackaging 890–891
 - setup programs 889, 891
 - transforms 891
 - ZAP files 891
 - publishing applications 893–895
 - removing software 891, 893, 900
 - roaming users 895
 - service packs and patches 899
 - shared computers 896
 - SMS configuration management tools 876–878
 - software life cycle 897–899
 - targeting software 893
 - Terminal Services clients 874
 - upgrading software 899–900
- IntelliMirror user data management
 - client configuration recovery 873
 - configuration plan *See* Client configuration planning
 - enabling 901–902
 - folder redirection
 - disk space quota 901, 907
 - implementing 904–905
 - overview 901
 - IntelliMirror technology components 871–875
 - network data storage quota 901, 907
 - offline files
 - configuring folder for offline use 906
 - disk space quota 901, 907
 - Group Policy options 906–907
 - overview 901
 - Synchronization Manager 905–906
 - IntelliMirror user data management (*continued*)
 - roaming user profiles 901, 903
 - SMS data management tools 876–878
- IntelliMirror user settings management
 - client configuration recovery 873
 - configuration plan *See* Client configuration planning
 - enabling 901–902
 - IntelliMirror technology components 871–875
 - planning task list 916
 - roaming user profiles 901, 903
 - SMS configuration management tools 876–878
 - strategies for different users 908–915
- Internet Assigned Numbers Authority (IANA) 195
- Internet Authentication Service (IAS)
 - account authorization 644
 - example configuration 637
 - features 205–206
 - IAS server location 644
 - installing 644
 - protocol support 206
 - RADIUS protocol 644
 - redirected Routing and Remote Access requests 644
 - remote access policies on IAS servers 206
 - Routing and Remote Access configuration 637
- Internet Connection Sharing (ICS) 198, 813–814
- Internet Explorer
 - enabling Authenticode 423
 - Group Policy settings 423, 836
 - viewing certificates 438
- Internet Group Management Protocol (IGMP) 215–216
- Internet Information Services (IIS)
 - Internet Services Manager 573
 - Network Load Balancing 664
 - security features 425
- Internet Protocol security *See* IPSec
- Internet Services Manager snap-in 573
- Internetwork Packet Exchange *See* IPX routing
- Inventory
 - hardware *See* Systems Management Server
 - SMS tools *See* Systems Management Server, inventory
 - software *See* Software inventory
- IP addressing
 - DHCP *See* DHCP
 - IP over ATM 224
 - IPX network ID 214
 - Multicast and Address Resolution Service 224
 - multihoming 206–207

- IP addressing (*continued*)
 - network address translation 216–217, 814–815
 - OSPF networks 212
 - remote access clients
 - DHCP 199
 - IPX network ID 199
 - static IP address pool 199
 - RIP for IP networks 209
 - TCP/IP *See* TCP/IP protocol
 - Terminal Services
 - client applications 916
 - Cluster service 580
 - firewalls 608
 - Network Load Balancing 599
 - preparing network 591
 - round-robin DNS 599
 - WINS (Windows Internet Name Service) 353, 196, 802
 - IP over ATM services 224, 226, 810
 - IP routing infrastructure
 - AppleTalk routing 215
 - configurations 207
 - IPX routing
 - Cluster service 672
 - IPX network ID 214
 - NetWare server interoperability 213
 - network design 214–215
 - RIP for IPX support 213
 - SAP for IPX support 213, 215
 - Terminal Services 591
 - multicast support 215–216
 - network address translation 216–217, 814–815
 - OSPF networks
 - area design 211–213
 - autonomous systems 210–211
 - features 210
 - IP addressing 212
 - link-state routing protocol 210
 - network size 209
 - RIP for IP protocol 208–209
 - static routed networks 207–208
 - IP Security Policy Management snap-in 410
 - IP Telephony 32
 - IPCONFIG diagnostic tool 575
 - IPSec (Internet Protocol security)
 - acceleration cards, security issues 411
 - authenticating clients using certificates 459
 - communication process 409–410
 - computer certificates *See* Public key infrastructure
 - IPSec (Internet Protocol security) (*continued*)
 - data protection considerations 406
 - deploying in demilitarized zone 916
 - implementing 410–412
 - Internet Key Exchange (IKE) protocol 409
 - network performance impact 411
 - remote access security policy 412
 - security policies 410, 418
 - exempt protocols 641
 - filters 641
 - rules 641
 - security policy options 411
 - VPNs *See* L2TP over IPSec VPNs
 - IPX network client connectivity 804–807
 - IPX routing
 - Cluster service 672
 - IPX network ID 214
 - NetWare server interoperability 213
 - network design 214–215
 - remote access client network ID 199
 - RIP for IPX support 213
 - SAP for IPX support 213, 215
 - Terminal Services 591
 - IrDA (Infrared Data Association) protocol 810
- J**
- Just-in-time application installation 890
- K**
- KCC (Knowledge Consistency Checker) 306
 - Kerberos authentication
 - authentication process 346–347, 390
 - default authentication protocol 346
 - Group Policy security settings 391, 415–416
 - implementing 391
 - interoperability 391, 328
 - Kerberos ticket policy 269
 - Key Distribution Center (KDC) 346
 - MIT Kerberos v5 realms 403, 404
 - mixed mode 336
 - multiple forests 392
 - optimizing cross-domain referrals 391
 - security group member expansion 352
 - single logon process 385, 388, 390
 - system time 391
 - trusts 391–392
 - Knowledge Consistency Checker (KCC) 306

L

L2TP over IPSec VPNs
 compared to Point-to-Point Tunneling Protocol 640
 computer certificates
 See also Public key infrastructure
 authentication process 201
 default settings 204
 example configuration 205
 trust relationships 205
 Connection Manager 201, 643
 demand-dial connections 201
 deploying IPSec 203–205
 on-demand router-to-router connection 203
 overview 201
 packet filtering 204
 persistent connection router-to-router 202
 policy for securing tunnel traffic 201
 trust relationships 205
 user authorization 201
 User Datagram Protocol 204

Labs *See* Test labs

LAN emulation
 client connectivity 809
 configuring connections 800
 default ELAN 226
 overview 223
 preparing clients for upgrade 226

LAN Manager Replication Service
 L-bridge.cmd script 356, 357
 mixed environment domains 356–358
 not supported in Windows 2000 354
 replication process 354–355
 transition to File Replication Service 354

Language options *See* MultiLanguage version

Layer 2 Tunneling Protocol *See* L2TP over IPSec
 VPNs

LDAP (Lightweight Directory Access Protocol) 733

LDM (Logical Disk Manager) 707

Lightweight Directory Access Protocol (LDAP) 733

Line-of-business applications
 documenting 169
 Terminal Services 588–589

Link-state routing protocol 210

Load balancing
 definition of 654
 round-robin DNS in Terminal Services 599
 Windows 2000 *See* Network Load Balancing

Local Computer Group Policy 416

Local groups
 See also Security principals
 mixed mode domains 349
 native mode domains 349
 nested security groups 351
 properties 350
 Restricted Groups policy 417
 upgrading Windows NT 349
 Windows NT 3.51 327

Localized Windows 2000 *See* MultiLanguage version

Locator records, DNS 289, 314

Logical diagrams of test lab 122–123

Logical Disk Manager 707

Logical network diagram 165, 167

Logo-compliant applications
 accessibility requirements 1077
 compatibility issues 561
 directory of compatible applications 784–785
 Microsoft Logo program Web site 13
 vendor testing 784

Logoff, Group Policy options 855

Logon
 authenticating *See* Authentication; Remote access
 authentication
 number failed logon attempts allowed 415
 passwords *See* Passwords
 PDC emulation logon server 340
 security options 416
 Terminal Services
 auto-logon 606–607
 logon scripts 607
 user rights 605
 user interface options 855
 user principal names 262–263, 266

M

Macintosh
 AppleTalk routing 215
 file server access 802
 multiprotocol remote access 192
 print services 569
 Services for Macintosh 566, 569, 802
 upgrading Macintosh volumes 566–568
 Windows servers in AppleTalk zones 809

Magneto-optic discs 709

Mailing lists 398

Managed volumes 710

- Management infrastructure planning worksheet 978–980
- MARS (Multicast and Address Resolution Service) 224, 226
- Mass storage devices
 - automated client installation 926, 928–929
 - automated server installation 474, 476–477
- Media pools, creating 709
- Member servers
 - accessing NetWare 804–807
 - definition of 555
 - documenting current 169
 - domain migration
 - benefits of upgrading 323–324
 - moving servers 370
 - order of upgrading 323, 325, 330
 - installing Windows 2000
 - application servers 571–573
 - clean installation procedure 564
 - file servers 565–568
 - incrementally 558
 - Microsoft Proxy Server 574
 - planning task list 577
 - print servers 569–571
 - upgrade procedure 564
 - Web servers 573–574
 - performance tuning 575–576
 - post-installation testing
 - file shares 568
 - network connectivity 575
 - print shares 570–571
 - preparing for Windows 2000
 - backups 563
 - event log errors 563
 - Hardware Compatibility List (HCL) 562
 - hardware inventory 559
 - hardware requirements 180, 559–560, 569
 - pre-upgrade checklist 563–564
 - software compatibility 562–563
 - software compliance, third-party 561
 - UPS devices 564
 - promoting to domain controllers 482, 485
 - system administration tools 576
 - upgrade and installation plan
 - guidelines for creating 557
 - planning process 556
 - planning worksheets 1001–1007
 - schedule 557–558
- Memory
 - Advanced Server memory support 652, 658
 - Windows robust heap checking 790
- MetaFrame Terminal Services add-on 584
- Metering software 234, 241, 251
- Microsoft Base Cryptographic Provider 437
- Microsoft Certificate Services
 - Authenticode certificates 422
 - certificate enrollment and renewal 450–451
 - certificate security settings 442
 - creating certification authorities 443
 - custom applications for 443
 - designing public key infrastructures 440
 - Encrypting File System certificates 408
 - enrollment and renewal Web pages 453
 - installing 457
- Microsoft CryptoAPI 453
- Microsoft Management Console (MMC)
 - Active Directory Connector Administrator snap-in 752
 - Active Directory Connector Management snap-in 753
 - Active Directory Domains and Trusts snap-in 405, 348
 - Active Directory Sites and Services snap-in 427
 - Active Directory Users and Groups snap-in 298
 - ADC Administrator snap-in 743
 - Certificates snap-in 438
 - Certification Authority *See* Certification Authority snap-in
 - Cluster Administrator snap-in 713
 - Computer Management snap-in 395, 566
 - delegating administration 842
 - Disk Management *See* Disk Management snap-in
 - Group Policy snap-in *See* Group Policy
 - Internet Services Manager snap-in 573
 - IP Security Policy Management snap-in 410
 - Remote Storage Manager snap-in 710–712
 - Security Configuration and Analysis snap-in 384, 419
 - Server System Monitor snap-in 575
 - Software Installation *See* Software Installation snap-in
 - system administration tools 576
 - Users and Computers *See* Active Directory Users and Computers snap-in
- Microsoft Official Curriculum (MOC) 85

Index

- Microsoft Proxy Server
 - See also* Proxy servers
 - client configuration 634
 - Microsoft Security Advisor link 634
 - security logging 634
 - upgrading 574, 633
 - Migration DLLs 787, 528
 - MIME standard 424
 - Mirrored volumes 705, 723, 563
 - MIT Kerberos v5 realms 404
 - Mixed mode
 - account replication 179
 - authentication 179
 - backup domain controllers 348
 - defining interoperability requirements 327–328
 - definition of 335
 - interoperability features 329
 - NTFS file system 179
 - NTLM authentication 345
 - PDC emulation
 - conflict resolution 340
 - native-mode switch 337
 - overview 339
 - properties 340
 - reasons for using 347–348
 - RRAS servers 358–359
 - security groups 349–352
 - transition to native mode 337
 - trusts in child domains 343–344, 345
 - Windows 2000 features available in 335–336
 - MMC *See* Microsoft Management Console
 - Mobile users
 - client configuration planning 827
 - data and settings management 912–913
 - software distribution methods 896, 912–913
 - MOC (Microsoft Official Curriculum) 85
 - Monitoring APIs 790
 - Monitoring networks (SMS Network Monitor) 248–250
 - Monitoring software usage (SMS) 241
 - Multicast and Address Resolution Service (MARS) 224, 226
 - Multicast traffic
 - DHCP IP addressing 218
 - IGMP 215–216
 - IGMP Version 2 198
 - MARS servers 224, 226
 - Network Load Balancing 670
 - Multihoming 206–207
 - MultiLanguage version
 - deployment planning 66
 - disk space 863
 - features 861
 - installation 862–864
 - language groups 862–864
 - multiple language considerations 859–860
 - restricting using Group Policy 864
 - Terminal Services 614
 - upgrade path 861–862
 - Multiple-master domains
 - conflict resolution 340
 - domain model 331
 - mixed mode 336
 - native mode 337
 - PDC emulation 339
 - trust relationships
 - compared to Active Directory trusts 261–262
 - explicit 331, 334
- ## N
- Narrator 1092
 - NAT (network address translation) 216–217, 814–815
 - Native mode domains *See* Domain upgrade, native mode
 - NDIS ATM network adapter support 223
 - NetBEUI protocol
 - Cluster service 672
 - virtual private networks 640
 - NetBIOS
 - Active Directory domain names 282, 286
 - clients, support 178
 - discontinuing 353
 - domain migration considerations 353–354
 - name resolution 196
 - NetBIOS over IPX broadcasts 214
 - Windows NT domain locator 282
 - Netdom utility 371, 377
 - Netlogon synchronization, native mode 337
 - NetMeeting 14
 - NetWare
 - accessing NetWare resources 804–807
 - Client Service for NetWare 213, 804, 805
 - Common Internet File System protocol 806
 - File and Print Services for NetWare 805, 806
 - Gateway Service for NetWare 213, 804–805, 807
 - IPX routing 213–215
 - Microsoft File and Print Services for NetWare 568

- NetWare (*continued*)
 - NetWare Core Protocol 806
 - Novell Distributed Print Services 807
 - NWLink 213, 802
- Network address translation (NAT) 216–217, 814–815
- Network addressing *See* IP addressing
- Network and Dial-Up Connections folder
 - configuring multiple LAN adapters 801
 - configuring network components 801
 - creating dial-up profile 818
 - local area network connections 800, 801
- Network basic input/output system *See* NetBIOS
- Network Connection wizard 810–811, 817
- Network connectivity
 - Asynchronous Transfer Mode *See* Asynchronous Transfer Mode
 - client connectivity
 - See also* Remote client connectivity
 - accessing NetWare resources 804–807
 - Active Directory, non-Windows 2000
 - clients 804
 - ATM (Asynchronous Transfer Mode) 809–810
 - configuring connection components 801
 - DHCP 802–803
 - dial-up connections 800, 810–812, 817–818
 - DNS (Domain Name Service) 802–803
 - external clients, definition 799
 - Infrared Data Association protocol 810
 - installing network devices 801
 - installing protocols 802
 - internal clients, definition 799
 - IP over ATM services 810
 - LAN adapters, configuring 801
 - LAN connections 800–801
 - medium-to-large network example 819–821
 - Network Connection wizard 810–811, 817
 - planning task list 821
 - protocols 802–804
 - remote client considerations 191
 - static addresses 804
 - strategy planning process 799–800
 - technologies based on network size 819
 - UNIX clients 808–809
 - viewing connection status 801
 - virtual private network connections 811–812, 818
 - Windows servers in AppleTalk zones 809
- Network connectivity (*continued*)
 - demilitarized zone
 - designing 190–191, 632–633
 - example 203–204
 - diagramming current network 187–188
 - Dynamic Host Configuration Protocol *See* DHCP
 - planning process 188–190
 - planning task list 228
 - planning worksheets 988–990, 995–996
 - Quality of Service (QoS) 224, 227
 - remote access *See* Routing and Remote Access
 - remote client considerations 192
 - routing infrastructure *See* IP routing infrastructure
 - secure network connections *See* Security strategies
 - site connectivity media 191–192
 - site topology *See* Active Directory site topology
 - SOHO networks *See* SOHO networks
 - TCP/IP *See* TCP/IP protocol
 - testing after server upgrade 575
 - VPNs *See* Virtual private networks
- Network data packets, signing *See* Public key infrastructure
- Network diagrams, physical and logical networks 165–167, 187–188
- Network downtime, minimizing during upgrade 557, 558
- Network infrastructure
 - analyzing *See* Systems Management Server
 - connectivity *See* Network connectivity
 - documenting current
 - ATM configurations 168
 - bandwidth utilization 168–169
 - BIND service 168
 - DHCP service servers 168
 - diagnostic tools 163, 164
 - directory services 170
 - DNS namespace 171
 - domain structure 170–171
 - dynamic registration 168
 - example documents 995–996
 - hardware inventory *See* Hardware inventory
 - IP addressing methods 168
 - line-of-business applications 169
 - logical network diagram 165, 167
 - member servers 169
 - name resolution services 168
 - overview 163
 - physical network diagram 165–167
 - protocols 164

Index

- Network infrastructure (*continued*)
 - documenting current (*continued*)
 - remote access configurations 168
 - security 171–173
 - SMS *See* Systems Management Server,
analyzing network infrastructure
 - software inventory *See* Software inventory
 - trust relationships 170
 - Windows NT network settings 164
 - preparing for Windows 2000
 - clients 181–183
 - domain controllers 179
 - heterogeneous environments 183
 - infrastructure servers 177–178
 - labs *See* Test labs
 - member servers 180
 - physical infrastructure 176–177
 - preparation tasks 173–175
 - protocols 175–176, 182, 183
 - security infrastructure 180–181
 - stabilizing network 175
 - task list 184
 - routing infrastructure *See* IP routing infrastructure
- Network Load Balancing
- capacity planning
 - adding clusters 668
 - cluster size 667
 - server capacity 668–669, 670
 - Cluster service on same server 690
 - cluster, definition 653
 - Component Services application servers 664–666
 - deploying using Terminal Services 662–664
 - deployment planning tasks 696
 - deployment planning worksheets 1007–1014
 - disaster recovery
 - cluster backup and restore 695–696
 - cluster remapping 693
 - emergency repair disk 695
 - error recovery 693
 - fault tolerance planning 692
 - hardware RAID 692
 - transaction logging and recovery 693
 - host failures 659
 - IIS servers 664–666
 - implementation planning process 660
 - load balanced applications
 - application failures 660
 - data synchronization 661
- Network Load Balancing (*continued*)
- load balanced applications (*continued*)
 - licenses 662
 - requirements 669–670
 - load balancing, definition 654
 - multicast mode 670
 - optimizing clusters 669, 691–692
 - planning for availability
 - downtime costs 649–651
 - hardware compatibility 657–658
 - identifying network risks 656–657, 666–667
 - needs assessment 655–657
 - overview 658–660
 - planning tasks 652–653
 - planning team 654–655
 - port rules 661
 - round robin DNS 667–668
 - routers 670
 - streaming media servers 662
 - switches 668, 669
 - Terminal Services servers 599
 - testing server capacity 693–695
 - unicast mode 670
 - virtual private network servers 662
- Network Monitor (SMS) 248–250
- Network Monitor (Windows) 250
- Network security plan *See* Security strategies
- Networking and communications planning
 - worksheet 988–990
- Nonrepudiation
 - definition of 386
 - IPSec (Internet Protocol security) 410
 - smart cards 392
- Nontransitive trusts, definition 404
- Novell
 - accessing NetWare resources 804–807
 - Client Service for NetWare 213, 804, 805
 - Common Internet File System protocol 806
 - File and Print Services for NetWare 805, 806
 - Gateway Service for NetWare 213, 804–805, 807
 - IPX routing 213–215
 - Microsoft File and Print Services for NetWare 568
 - NetWare Core Protocol 806
 - Novell Distributed Print Services 807
 - NWLink 213, 802

NTFS file system
 - Cluster service considerations 689
 - compared to FAT system 714–715
 - converting FAT volumes 714

- NTFS file system (*continued*)
 - defragmenting disks 708
 - disk quota support 715, 901, 907
 - dual-boot systems 715
 - file systems supported in Windows 2000 714
 - Group Policy file security options 852
 - mixed mode 179
 - Terminal Services servers 604
 - transaction logging and recovery 693
 - unattended installation 484, 937
 - volume mount points 707
 - NTLM authentication
 - access tokens 341
 - backward compatibility 392
 - between forests 392
 - mixed mode 345
 - RRAS servers 358–359
 - trust relationships 403
 - NULL session, RRAS servers 358
 - NWLink 213, 802
- O**
- Offline files
 - configuring folder for offline use 906
 - disk quota 901, 907
 - enabling IntelliMirror user data management 902
 - Group Policy options 906–907
 - overview 901
 - Synchronization Manager 905–906
 - Off-site storage policies 727
 - One-way trusts, definition 403–404
 - Open Shortest Path First *See* OSPF networks
 - Open standards support 256
 - organizational units *See* Active Directory
 - organizational units
 - OSPF networks
 - area design 211–213
 - autonomous systems 210–211
 - features 210
 - IP addressing 212
 - large networks 209
 - link-state routing protocol 210
- P**
- Pagefile.sys 503, 957
 - Partition table, backing up 563
 - Pass-through authentication 347
 - Passwords
 - authenticating users *See* Authentication
 - creating secure passwords 416
 - delegating network connections 389, 390
 - domain security policy 269
 - Group Policy password policy 415
 - managing using PDC emulation 339
 - retained after upgrade 329
 - secure 389
 - setting in answer file 483–484, 935–936
 - single logon process 385, 388, 390
 - PDC emulation
 - conflict resolution 340
 - overview 339
 - properties 340
 - Permanent labs *See* Change management labs
 - Permanent virtual circuits 222
 - Permissions
 - See also* Access control lists; Security groups
 - assigning *See* Security groups
 - default 400
 - file system permissions 397
 - hiding objects 304
 - managing 396–397
 - network share permissions 397
 - resources outside of forest 264
 - setting 396
 - Physical network diagram 165–167
 - Physical test lab diagram 124–125
 - Pilot project
 - deploying 155–156
 - deployment project phases 42–43
 - evaluating 156
 - example deployment scenario 50
 - feedback 145, 157
 - monitoring 156
 - objectives 145, 149
 - overview 80–81, 143–145
 - phases
 - dry run 155
 - IT pilot 147
 - production pilot 147
 - risk management 145
 - pilot plan 147–148
 - planning task list 158
 - process for conducting 146
 - rollback procedure 152
 - rollout procedures 155
 - schedule 152–153

Index

- Pilot project (*continued*)
 - scope 148
 - site preparation 153
 - users
 - communication process 151, 154
 - selecting 149–150
 - support 151
 - training 150–151, 154
 - validating backups 156
- PING diagnostic tool 575
- PKI *See* Public key infrastructure
- Planning worksheets
 - application and service availability 1007–1014
 - application compatibility testing 1019–1020
 - automated client installation 1027–1028
 - automated server installation 999–1000
 - change and configuration management 1025–1026
 - client administration and configuration standards 1021–1025
 - component application services 985–986
 - desktop management solutions 980–982
 - directory service synchronization 1014–1018
 - distributed security 998–999
 - domain migration strategies 996–998
 - information publishing and sharing 984
 - management infrastructure worksheet 978–980
 - network infrastructure 995–996
 - networking and communications 988–990
 - scalability and availability 986–988
 - security features 982–984
 - storage management 990–992
 - test lab documents 992–994
 - upgrading and installing member servers 1001–1007
- Plug and Play devices
 - automated client installation 927, 930–931
 - automated server installation 475, 478–479
 - third-party 182, 183
- Point-to-Point Encryption 638
- Point-to-Point Protocol (PPP) 395, 198, 225
- Point-to-Point Tunneling Protocol (PPTP) 176, 200, 640
- Power Users group
 - default permissions 400
 - default rights in security templates 419–421
 - rights to run applications 420
- PPP over ATM networks 225
- Prefix notation, IP addressing 195
- Primary domain controller
 - PDC emulation
 - conflict resolution 340
 - overview 339
 - properties 340
 - upgrading domains *See* Domain upgrade
- Print Operators group 400
- Print servers
 - See also* Member servers
 - accessing NetWare 804–807
 - Active Directory 570
 - configuring network environment 570
 - Terminal Services print jobs 614–616
 - testing printer shares 570–571
 - upgrading 569, 571
 - Windows 2000 system requirements 569
- Prioritizing applications for testing 775, 778–779
- Product compliance database (SMS) 244–247
- Profiles, hardware 852–853
- Proxy servers
 - See also* Member servers
 - Microsoft Proxy Server
 - client configuration 634
 - Microsoft Security Advisor Web page 634
 - security logging 634
 - upgrading 633
 - monitoring network security 634
 - multiple 634
 - network demilitarized zone 632
 - public network security issues 632, 633
 - testing 634, 635
 - upgrading 574
- Public key infrastructure (PKI)
 - capacity planning 454–455
 - certificate enrollment
 - access control 459–460
 - automatic 450, 461
 - Automatic Certificate Request wizard 450
 - Certificate Request wizard 451
 - Certificates snap-in 438
 - configuring before deployment 462
 - defining enrollment process 450–451
 - Microsoft Enrollment Control 450
 - template 442
 - Web-based 439, 451, 453
 - certificate life cycle 448–450
 - certificate policies 443–444
 - certificate security requirements 441
 - certificate templates 442–443, 459–460

Public key infrastructure (PKI) *(continued)*

- Certificates snap-in 438
- certification authorities
 - certification authority practices 443, 444
 - Certification Authority snap-in 438
 - certification process 435
 - compromised 452–453
 - creating local 437–438
 - failures 452
 - installing 457
 - maintenance tasks 451
 - recovery plans 452–453
 - security requirements 448
 - setting certificate types to issue 459
 - trust hierarchies, restoring 453
 - trust hierarchy model 445–446
 - trust hierarchy strategies 447
 - trust lists 445, 446–447
- Certification Authorities Restore wizard 452
- certification process 435
- commonly certified applications 436
- creating custom applications 453
- cryptographic service provider 437
- definition of 433, 435
- disaster recovery 452–453
- Encrypting File System certificates 408
- Group Policy objects
 - assigning trust lists to 446–447
 - automatic certificate enrollment 461
 - certificate trust lists 461
 - EFS recovery agents 460
 - root certificate trust 461
 - setting public key policy 439
- implementation process 436–437
- implementing in stages 181
- IPSec certificates
 - authentication process 201
 - automatic enrollment 205, 461
 - certificate templates 442
 - clients not running Kerberos authentication 439
 - default settings 204
 - example configuration 205
 - L2TP trust relationships 205
 - preparing certificates 436
- issuing certificates 462
- key exchange operation 435
- needs assessment 441–443
- planning process 439–440
- planning tasks 463

Public key infrastructure (PKI) *(continued)*

- private encryption key 435
- production rollout process 455
- public encryption key 435
- renewing certificates
 - automatic 461
 - configuring before deployment 462
 - defining renewal process 450–451
 - key pair 450
 - security considerations 449, 450
 - Web-based 451, 453
- revoking certificates
 - compromised certification authorities 452
 - configuring revocation lists 460
 - publishing revocation lists 451
 - revocation policies 451
- scheduling deployment 456–457
- secure e-mail
 - certificate templates 442
 - encrypting messages 436
 - local certification authority 437
 - production rollout 456
- secure Web sites
 - certificate templates 442
 - certificate types 459
 - local certification authority 437
 - security methods 436
- smart cards
 - certificate templates 442
 - cryptographic service provider 437
 - FORTEZZA Crypto Cards 449
 - local and remote access logon process 436
 - local certification authority 437
 - logon certificates 459
 - production rollout 456
 - security standards 449
 - Smart Card Enrollment station 450, 462
 - storing public or private key on card 449
 - user certificates 459
 - user training phase 462
- software code signing 436, 442
- supporting systems and applications 457–459
- viewing certificates 438

Index

- Publishing applications
 - using IntelliMirror *See* IntelliMirror software distribution
 - using SMS *See* Systems Management Server software distribution
 - using Software Installation *See* Software Installation snap-in

- Q**
- Quality of Service (QoS) 224, 227
- Quota management, disk space *See* Disk quotas

- R**
- RADIUS protocol 205, 644
- RAID volumes
 - basic or dynamic storage on RAID-5 705–706
 - clusters
 - Cluster service considerations 674, 690
 - hardware RAID 692
 - designing fault-tolerant systems 725
 - fault tolerance features 723
 - implementation strategies 724
 - levels supported 723
- RDP *See* Remote Desktop Protocol
- Read1st.txt 562
- Recovering client configuration 873
- Recovering data
 - See also* Data backup and recovery
 - fault tolerance *See* Fault-tolerant systems
 - recovering files encrypted using EFS 408
- Redirecting folders
 - See also* IntelliMirror user data management
 - disk quota 901, 907
 - enabling IntelliMirror user data management 902
 - implementing 904–905
 - overview 901
- Redundant applications 777
- Redundant arrays of independent disks *See* RAID volumes
- Regional options, MultiLanguage Windows *See* MultiLanguage version
- Registry
 - applications that write directly to 791
 - auditing events 418
 - backing up 563
 - disabling registry editors 856
 - font registry keys 791
- Registry (*continued*)
 - Group Policy security settings 418
 - mapping keys using migration DLLs 787, 528
- Relative Identifier (RID) 341
- Relnotes.txt 562
- Remote access *See* Routing and Remote Access
- Remote access authentication
 - Internet Authentication Service
 - protocols 206
 - RADIUS protocol 644
 - redirecting Routing and Remote Access requests 644
- L2TP over IPSec VPNs
 - certificate-based authentication 204
 - example configuration 205
 - VPN server 201
- Routing and Remote Access
 - authentication process 394
 - Challenge Handshake Authentication Protocol 638
 - EAP Transport Layer Security 396, 638
 - enabling remote access for user 395
 - Extensible Authentication Protocol 395, 638
 - mutual authentication 638
 - Point-to-Point Protocol 395
 - protocols 395–396, 638
 - redirecting authentication to IAS 644
 - remote access policies *See* Remote access policies
 - security strategies 396, 637–638
 - virtual private networks 639, 640
- Remote access policies
 - defining 394–395
 - dial-up user profiles 199
 - enabling remote access 395
 - IAS servers 206
 - minimizing number of 643
 - remote access protocols 395–396
 - settings 199, 643
 - users without remote access profiles 394
- Remote Authentication Dial-In User Service (RADIUS) 205, 644
- Remote client connectivity
 - See also* Network connectivity
 - authentication *See* Remote access authentication
 - dial-up connections *See* Dial-up connections
 - direct connections to remote access servers 811
 - installing protocols 802
 - multiprotocol remote access 192

- Remote client connectivity (*continued*)
 - Network and Dial-up Connections folder
 - configuring multiple LAN adapters 801
 - configuring network components 801
 - creating dial-up profile 818
 - local area network connections 800, 801
 - Network Connection wizard 810–811, 817
 - network example 819–821
 - network size 812
 - overview 192
 - planning task list 821
 - remote access service *See* Routing and Remote Access
 - SOHO networks *See* SOHO networks
 - technologies based on network size 819
 - Terminal Services *See* Terminal Services, remote access
 - VPNs *See* virtual private networks
- Remote Desktop Protocol (RDP)
 - client/server connections 592
 - firewalls 591
 - installation directory 612
 - printer redirection 615
 - remote access connections 608
 - Terminal Services Configuration tool 621
- Remote OS Installation
 - Advanced Configuration Power Interface (ACPI) 885
 - automated installation enhancements 945–946
 - clients
 - configuration recovery 873
 - configuring 883–885
 - Preboot Execution Environment (PXE) 960, 874, 881
 - prestaging 964, 965, 883
 - remote-boot media 881
 - system requirements 960
 - configuring 881
 - deployment planning
 - capacity planning 874–875
 - configuration management plan 908–910
 - deployment strategies 878–879
 - strategies for different users 910–915
 - Group Policy 886
 - hardware abstraction layer 885
 - operating system image
 - adding to server 884
 - Client Installation wizard 881
 - client selection 881
- Remote OS Installation (*continued*)
 - operating system image (*continued*)
 - custom installations 885
 - preparing 881, 885–886
 - types of 885
 - overview 879
 - planning process 872
 - Remote Boot ROM 874
 - Remote Installation components 881
 - Remote Installation Preparation wizard 881, 885
 - Remote Installation servers
 - configuring 883–885
 - DHCP service 962–964, 966
 - network load 961
 - optimizing performance 961
 - routers 966
 - server selection 963–966
 - Setup file 881
 - Remote Installation Services Administrator 881
 - restarting setup 886
 - RIS imaging 960
 - Terminal Services clients 874
 - user installation options 884, 885–886
 - when to use 874, 880, 946–947
 - Windows components required 879–880
- Remote server administration, MMC tools 576
- Remote Storage system 710–712
- Remote user type 827, 858–859
- Removable Storage system 709–711
- Replication
 - Conflict resolution 402, 340
 - FRS *See* File Replication Service
 - PDC emulation in mixed-mode networks 339
- Resource domains
 - multiple-master domains 331
 - restructuring into OUs 303, 343
 - See also* delegating administration, 373–375
 - administrator accounts 335
 - delegation models 271
 - SAM database size 334, 342, 360
 - upgrading 334–335, 342, 343
- Restricted Groups policy 417
- Reverse lookup zones 289, 314
- RID (Relative Identifier) 341
- RIP for IP protocol 208–209
- RIP for IPX protocol 213
- RIS (Remote Installation Service) *See* Remote OS Installation
- Risk management planning 86–90

Index

- Roaming user profiles
 - definition of 901
 - implementing 903
 - Terminal Services 600–601, 603
- Roaming users
 - client configuration planning 875, 895, 911–912
 - definition of 827
 - migration scheduling 51
 - planning for, best practices 67
 - Windows 2000 features 14
- Robust heap checking 790
- Round robin DNS 667–668
- Roundtrip Time (RTT), TCP/IP protocol 194
- Routing and Remote Access
 - Bandwidth Allocation Protocol 198
 - Challenge Handshake Authentication Protocol 198
 - enabling remote access for user 395
 - Extensible Authentication Protocol 198
 - Internet Authentication Service configuration 637
 - Internet Connection Sharing (ICS) 198, 813–814
 - multicast support 215–216
 - network address translation 216–217, 814–815
 - Network Connection wizard 810–811, 817
 - network example 819–821
 - network routing concepts 197
 - new features 197–198
 - remote access authentication
 - authentication process 394
 - Challenge Handshake Authentication Protocol 638
 - EAP Transport Layer Security authentication 396, 638
 - Extensible Authentication Protocol 395, 638
 - IAS *See* Internet Authentication Service
 - mutual authentication 638
 - Point-to-Point Protocol 395
 - protocols 395–396, 638
 - redirecting requests to IAS 644
 - remote access policies
 - defining 394–395
 - minimizing number of 643
 - settings 199, 643
 - users without remote access profiles 394
 - remote client addressing
 - DHCP 199
 - IPX network ID 199
 - static IP address pool 199
 - remote client connectivity features 192
 - Routing and Remote Access (*continued*)
 - routers in demilitarized zone 191
 - RRAS server upgrade considerations 327, 358–359
 - security strategies 396, 637–638
 - users without remote access profiles 394
 - Routing infrastructure *See* IP routing infrastructure
 - RRAS *See* Routing and Remote Access
 - RTT (Roundtrip Time), TCP/IP protocol 194
- S**
- S/MIME standard 424
- SAMI (Synchronized Accessible Media Interchange) 1086
- Sample deployment scenarios *See* Example deployment scenarios
- Sample worksheets *See* planning worksheets
- SAP for IPX 213, 215
- Scalability and availability planning worksheet 986–988
- Schema Administrators group
 - forest root domain 281
 - permissions 261
 - schema change policy 267
 - security considerations 426
- Schema container 269
- Scripting services 25
- SCSI drivers
 - automated client installation 926, 928
 - automated server installation 474, 476
 - SCSI adapters 709
- Searching using Indexing Service 720–722
- Secure applications
 - e-mail
 - planning considerations 424–425
 - public key cryptography *See* Public key infrastructure
 - S/MIME standard 424
 - security risks 424
 - Microsoft certification security standards 421
 - minimum security requirements 421–422
 - software downloaded from Internet 422–423
- Secure security template 421
- Secure Sockets Layer (SSL) protocol 425
- Secure Web sites 425–426
- Secure/Multipurpose Internet Mail Extensions (S/MIME) 424

- Security Account Manager (SAM) database
 - copied to Active Directory 338
 - size considerations 334, 342, 360
- Security Configuration and Analysis snap-in
 - analyzing security 384
 - working with security templates 419
- Security event logging
 - audit policy 416
 - available technologies 634
 - disk space 429
 - Event Log policies 416
 - events affecting the registry 418
 - events to audit 430
 - failed and successful events 417
 - file and folder events 418, 429
 - implementing 429
 - overview 387, 634
 - process 428
 - System Services policy 417
 - viewing log file 429
- Security groups
 - access control process 396–397
 - Active Directory Connector 743
 - adding users 400
 - authorization, definition 383, 386
 - ClonePrincipal utility 376–377
 - default permissions 400
 - defining permissions 396–397
 - design considerations 400–402
 - distribution groups 398
 - group expansion 352
 - maximum size 351
 - mixed mode 336, 349–352
 - moving *See* Security principals
 - nesting 401, 402, 351
 - overview 398–402
 - replication conflicts 402
 - Restricted Groups policy 417
 - rights on local computers 416
 - SAM database size 334
 - Terminal Services 605–606
 - types of 399
- Security identifiers (SIDs)
 - access control list components 341
 - access tokens 341
 - definition of 341
 - moved security principals 362–366
 - Relative Identifier (RID) 341
 - user profiles 367–369
- Security principals
 - Active Directory domain database 269
 - creating using PDC emulation 340
 - moving between forests 266
 - moving to restructure domains
 - adding new SIDs to ACLs 364
 - cloning security principals 371, 376–377
 - computer accounts 369–370
 - effect on SIDs 362–366
 - global groups 367
 - member servers 370
 - migrating users incrementally 371
 - SIDHistory 365–366
 - user accounts 367
 - user profiles 367–369
 - multiple-domain environments 280
 - SAM database size 334, 342, 360
- Security risks, network 382–383, 628
- Security strategies
 - developing policies and procedures 630–631
 - distributed security 387–388
 - documenting current standards 171–173
 - identifying security risks 382–383, 628
 - infrastructure planning 180–181
 - Microsoft Security Advisor Web page 634
 - monitoring network security 634
 - network security plan 379–382, 625–627
 - planning process 628–629
 - planning task list 430–432, 648
 - planning worksheets 982–984, 998–999
 - public network access issues 633
 - secure network connection planning
 - deployment plan 630
 - DMZ *See* Demilitarized zone
 - firewalls *See* Firewalls
 - proxy servers *See* Proxy servers
 - strategies for partners 631, 646–647
 - strategies for users 630–632, 635–636, 645–646
 - technology interdependencies 635
 - staff education 630
 - Windows 2000 security model 383–387
- Security templates for Group Policy 419–421
- Selective acknowledgment, TCP/IP protocol 194
- Server administration tools, MMC 576
- Server automated deployment *See* Automated server installation
- Server Gated Cryptography (SGC) 425
- Server Operators group 400
- Server synchronization *See* Active Directory Connector

Index

- Server System Monitor snap-in 575
- Server test labs
 - See also* Test labs
 - designing 111–115
 - documenting
 - lab description 121–122
 - logical diagrams 122–123
 - physical diagrams 124–125
 - domains
 - designing 119–120
 - domain authentication 117
 - user accounts 112
 - test process considerations 119
- Service accounts
 - authentication 389
 - service startup mode 417
 - System Services policies 417
 - trusted for delegation 389, 390
- Service Advertising Protocol (SAP) for IPX 213, 215
- Services for Macintosh 802, 809
- Setup (Windows 2000 Professional)
 - Check Upgrade Only mode 116, 785
 - Client Installation wizard 1078
 - running from bootable CD 959
 - running from installation disk 937
 - unattended
 - See also* Automated client installation
 - answer files *See* Answer files
 - extending disk partitions 936–937, 956–959
 - process 945
 - specifying answer file 932
 - Unattend.doc 932
 - Unattend.txt answer file 932
 - unattended installation switch 932, 937, 938
 - what you can install 944
- Winnt.exe
 - automated installation parameters 932, 937
 - command syntax 1035–1036
 - upgrade vs. clean install capabilities 939
 - when to use 937
- Winnt32.exe
 - automated installation parameters 932, 938
 - command syntax 1031–1034
 - syspart switch 947–949
 - upgrade vs. clean install capabilities 939
 - when to use 937
- Setup (Windows 2000 Server)
 - running from bootable CD 507
 - running from installation disk 485, 564–565
- Setup (Windows 2000 Server) (*continued*)
 - unattended
 - See also* Automated server installation
 - answer files *See* Answer files
 - commands in SMS package definition 525
 - creating domain controllers 482, 485
 - extending disk partitions 484
 - process 492
 - specifying answer file 481
 - Unattend.doc 480
 - Unattend.txt answer file 480
 - unattended installation switch 481, 486
 - what you can install 492
 - Winnt.exe
 - automated installation parameters 481, 486
 - command syntax 1035–1036
 - specifying answer file 481
 - upgrade vs. clean install capabilities 487
 - when to use 485
 - Winnt32.exe
 - automated installation parameters 481, 486
 - command syntax 1031–1034
 - specifying answer file 481
 - syspart switch 494–495
 - upgrade vs. clean install capabilities 487
 - when to use 485
- Setup Manager 481–482, 933–934
- Setupapi.log 503, 957
- SFP (System File Protection) 790
- SGC (Server Gated Cryptography) 425
- Shared system files, protecting 790
- SIDHistory
 - ClonePrincipal utility 376–377
 - moved security principals 365–366
 - Windows NT 3.51 327, 366
- SIDs *See* Security identifiers
- Single logon process 385, 388, 390
- Single subnet networks 193
 - See also* SOHO networks
- Site connectivity media 191–192
- Site topology *See* Active Directory site topology
- Site-licensed applications, managing 778
- Slow links
 - bootable CD software installation 507, 959
 - definition of 273
 - Group Policy options 845, 847, 859
 - Sysprep software installation 496, 949

- Smart cards
 - authentication process 392
 - drivers 393
 - enterprise certification authority required 393
 - hardware requirements 393
 - hardware supported 393
 - multiple-forest environments 266
 - planning considerations 392–394
 - public key cryptography *See* Public key infrastructure
 - security benefits 392
 - Terminal Services 608
 - two-factor authentication 385
- SMP (symmetric multiprocessing)
 - eight-way (Advanced Server) 11
 - four-way 10
 - scalability 30
- SMS *See* Systems Management Server
- Software applications *See* Applications
- Software distribution
 - automating client *See* Automated client installation
 - automating server *See* Automated server installation
 - using Add/Remove Programs *See* Add/Remove Programs
 - using IntelliMirror *See* IntelliMirror software distribution
 - using Remote OS Installation *See* Remote OS Installation
 - using SMS *See* Systems Management Server software distribution
 - using Software Installation *See* Software Installation snap-in
- Software Installation snap-in
 - application advertisement scripts 893
 - assigning and publishing software 895
 - declared upgrade relationships 900
 - removing software 900
- Software inventory
 - application testing process 774
 - considerations 775–778
 - SMS tools
 - extracting SMS inventory data 244, 248
 - product compliance database 244–247
 - running SMS inventory 240–241
 - SMS reports 242
 - SMS version 1.2 considerations 234
- Windows Management Instrumentation (WMI) 164
- Windows NT network data 164
- Software metering
 - data collected 241
 - SMS 1.2 234
 - software version control 251
- Software signing
 - Authenticode 422–423
 - public key cryptography *See* Public key infrastructure
- SOHO (small office/home office) networks
 - See also* L2TP over IPSec VPNs
 - Automatic Private IP Addressing 193, 815
 - components 813
 - example configurations 815–816
 - Internet Connection Sharing (ICS) 198, 813–814
 - L2TP over IPSec VPNs 201
 - network address translation 216–217, 814–815
 - overview 812–813
 - single subnet network 812
- Spanned volumes 705
- SSL (Secure Sockets Layer) protocol 425
- Standards-based protocol support 256
- Start menu configuration 857–858
- Startup initialization, network performance 66
- Static routed networks 207–208, 804
- Storage management
 - Backup program
 - backup policies 726–727
 - data protection strategies 725
 - using 724
 - clustering *See* Windows Clustering
 - disk management
 - Disk Management snap-in *See* Disk Management snap-in
 - Remote Storage system 710–712
 - Removable Storage system 709–711
 - disk quotas *See* Disk quotas
 - downloading and synchronizing files *See* Synchronizing offline files
 - fault tolerance *See* Fault-tolerant systems
 - file systems *See* File systems
 - Indexing Service 720–722
 - planning
 - budget considerations 703
 - data protection policies 725
 - disaster recovery plan *See* Disaster recovery
 - example worksheet 990–992
 - needs assessment 701–703
 - overview 697–699
 - planning process 700

Index

- Storage management (*continued*)
 - planning (*continued*)
 - storage system models 703–704
 - task list 729
 - Windows features 699, 712
 - user data *See* IntelliMirror user data management
- Striped volumes 705, 723
- Subnet masks 195–196, 309, 193
- Subnet planning, site topology 308
- Switched virtual circuits 222
- Symmetric key encryption 384
- Symmetric multiprocessing (SMP)
 - eight-way (Advanced Server) 11
 - four-way 10
 - scalability 30
- Synchronization Manager 905–906
- Synchronized Accessible Media Interchange 1086
- Synchronizing directories *See* Active Directory Connector
- Synchronizing offline files
 - configuring folders for offline use 906
 - disk space quota 901, 907
 - enabling IntelliMirror user data management 902
 - Group Policy options 906–907
 - overview 901
 - Synchronization Manager 905–906
- Syspart
 - client computer setup
 - answer file *See* Answer files
 - automated installation enhancements 945–946
 - distribution folder *See* Distribution folders
 - installing Windows Professional 921–922, 947–949
 - when to use Syspart 946–947
 - server setup
 - answer file *See* Answer files
 - automated installation enhancements 492–493
 - distribution folder *See* Distribution folders
 - installing Windows Server 469–470, 494–495
 - when to use Syspart 493–494
- Sysprep client imaging
 - administrative password 952
 - automated installation enhancements 945–946
 - Cmdlines.txt 956
 - distribution folder *See* Distribution folders
 - extending disk partitions 936, 937, 956–959
 - Hyberfil.sys 957
 - imaging process 921–922, 950
 - installing Active Directory components 950
- Sysprep client imaging (*continued*)
 - Mini-Setup wizard 953–955
 - Pagefile.sys 957
 - running Sysprep.exe
 - automatically after Setup 956
 - executable file location 950
 - manually 955–956
 - parameters 951
 - quiet mode 951, 956
 - reboot switch 951, 955
 - Setupapi.log 957
 - Setuppl.exe 950, 953
 - Sysprep.inf answer file
 - See also* Answer files
 - administrative password 952
 - ConvertNTFS 957
 - example 952–953
 - file location 951
 - overview 951
 - unattended installation parameters 954
 - system requirements 949
 - when to use 946–947, 949
- Sysprep server imaging
 - administrative password 499
 - automated installation enhancements 492–493
 - Cmdlines.txt 502
 - distribution folder *See* Distribution folders
 - extending disk partitions 484, 503–506
 - Hyberfil.sys 503
 - imaging process 469–470, 497
 - installing Active Directory components 497
 - Mini-Setup wizard 500–501
 - overview 496
 - Pagefile.sys 503
 - running Sysprep.exe
 - automatically after Setup 503
 - executable file location 497
 - manually 501–502
 - parameters 498
 - quiet mode 498, 503
 - reboot switch 498, 501
 - Setupapi.log 503
 - Setuppl.exe 497, 500
 - Sysprep.inf answer file
 - See also* Answer files
 - administrative password 499
 - ConvertNTFS 504
 - example 498–499
 - file location 498

- Sysprep server imaging (*continued*)
 - Sysprep.inf answer file (*continued*)
 - overview 498
 - unattended installation parameters 501
 - system requirements 496
 - when to use 493–494, 496
- System File Protection (SFP) 790
- System policies (Windows NT)
 - compared to Group Policy 835–836
 - transferring 837–839
- System Services policies 417
- Systems Management Server
 - analyzing network infrastructure
 - deployment planning 233–234
 - network infrastructure defined 231
 - process for 231–233, 251
 - SMS 1.2 234–236
 - client configuration management tools 876–878
 - deploying 229
 - inventory
 - estimating hardware requirements 238–240
 - extracting inventory data 244, 248
 - hardware compatibility issues 236–237
 - inventory reports 242–244
 - product compliance database 244–247
 - running inventory component 238–241
 - selecting computers for upgrade 520, 538–540
 - SMS version 1.2 234
 - software header data 240–241
 - Windows 2000 Hardware Compatibility List (HCL) 237
 - Network Monitor 248–250
 - reports
 - inventory 242–244
 - product compliance 246–247
 - software distribution *See* Systems Management Server software distribution
 - software metering
 - data collected 241
 - SMS 1.2 234
 - software version control 251
 - version 1.2 234–236
 - Windows Management Instrumentation (WMI) 876
- Systems Management Server software distribution
 - advertisements
 - client boot passwords 540
 - creating 540–541
 - distribution point security 541–542
 - executing 542–543
- Systems Management Server software distribution (*continued*)
 - advertisements (*continued*)
 - overview 518, 538
 - preparing clients 540
 - scheduling 541, 542
 - Windows 95 or Windows 98 client logon process 540
 - answer files
 - See also* Answer files
 - enabling unattend mode 525
 - multiple 524
 - omitting name in Setup command 525
 - security 528
 - specifying answer file to use 523
 - Windows 95 or Windows 98 domain settings 527–528
 - Windows NT upgrades 528
 - automated installation enhancements 492–493, 945–946
 - distributing packages to distribution sites
 - distributing packages 532–533
 - initial distribution 532
 - overview 529
 - planning 519
 - senders 519, 533–534
 - software distribution process (diagram) 518
 - test site 531–532
 - testing 519, 532, 533
 - distribution folders *See* Distribution folders
 - distribution process
 - phases 519
 - physical diagram 518
 - tasks 515–516, 551
 - domain migration features 549
 - monitoring advertisements
 - overview 544
 - status files 543
 - status reports 546–547
 - System Status subsystem 544
 - troubleshooting 541, 548
 - viewing status information 544–546
 - monitoring package distribution
 - overview 521, 534
 - status information availability 534
 - status reports 537
 - System Status subsystem 534
 - troubleshooting distribution 520, 537–538

Systems Management Server software distribution
(*continued*)

- monitoring package distribution (*continued*)
 - unattended installation error messages 525
 - viewing status information 534–537
- operating system rights
 - distribution points 541–542
 - overview 520
 - SMS version 1.2 550
 - Windows 2000 Server upgrade 526
 - Windows 95 or Windows 98 upgrades 527–528
- preparing distribution sites
 - disk space 519, 529
 - distribution folders *See* Distribution folders
 - distribution point groups 530
 - fan-out distribution 531
 - number of distribution points 530
 - overview 517
 - sender controls 530
 - test site 531–532
- preparing packages
 - distribution folders *See* Distribution folders
 - overview 516–517
 - package definition files 517
 - package source files 516
 - predefined 521
 - SMS programs 516, 521
 - Windows 2000 Advanced Server 526
 - Windows 2000 Professional 521, 526–528
 - Windows 2000 Server 521–524, 525–526
- selecting computers for upgrade 520, 538–540
- senders
 - Courier Sender 533–534
 - overview 519
 - sender controls 530
- unattended
 - See also* Setup
 - /unattend switch 525
 - answer files *See* Answer files
 - error messages 525
 - SMS Installer scripts 517
 - user input considerations 524–525
- version 1.2 differences 550
- when to use 493–494, 507, 946–947, 959

T

- Tape drives, Removable Storage system 709
- Task Manager
 - Network Segment counters 620
 - Physical Memory values 619
 - System Monitor counters 618–619
- Task-based user type 828, 913–914
- TCP/IP protocol
 - client connectivity 802–804
 - configuration testing 575
 - Dynamic Host Configuration Protocol *See* DHCP
 - installing on client 802
 - Internet Protocol security *See* IPSec
- IP addressing
 - Automatic Private IP Addressing 193, 815
 - IP address classes 194–195
 - IP addressing plan 194
 - multihoming 206–207
 - notation 195
 - private addresses 195
 - subnet masks 193, 194, 195–196
 - Windows Internet Name Service 196
- IP over ATM services 224, 226
- large window support 193
- network routing concepts 197
- new features 192–194
- remote access *See* Routing and Remote Access
- Roundtrip Time 194
- selective acknowledgment 194
- subnet masks 308
- subnets 197
- VPNs *See* Virtual private networks
- Terminal Services
 - Active Directory infrastructure 600
 - administrative tools 620–621
 - Application Server mode
 - Cluster service 580
 - default user rights 605
 - overview 580
 - user connections to applications 612
 - Windows Installer 602
 - Client Connection Manager 606
- client devices
 - client requirements 611–612
 - documenting current 592
 - green screen terminals 592
 - terminal emulation 579
 - UNIX terminals 592

- Terminal Services (*continued*)
 - client devices (*continued*)
 - Windows CE-based terminals 610–611
 - Windows-based Terminals 579
 - Cluster service 690
 - current computing environment, documenting 591
 - deployment
 - best practices 67
 - deploying Terminal Services 612
 - planning team 585
 - process 584–585
 - tasks 622
 - upgrade path 612
 - domain structure 600
 - example scenarios
 - central desktop deployment 589–590
 - deployment requirements 590
 - line-of-business applications 588–589
 - remote access 587–588
 - remote administration 586–587
 - external data storage 599
 - Group Policy
 - access to applications 602
 - conflicting policies 602
 - deploying applications 613
 - installing applications 602
 - remote application installation 580
 - user language 614
 - installing applications
 - Add/Remove Programs 613
 - application's setup 613
 - client IP addresses 598
 - execution scripts 593, 604, 607
 - from domain controllers 613–614
 - Install mode 613
 - multimedia applications 593
 - potential problems 593, 598
 - remote installation 580
 - remote session 613
 - scripting 607
 - security rights 606
 - transform files 602, 613
 - Windows Installer 593, 602, 613
 - IntelliMirror software distribution 874
 - Internet Protocol (IP) 591
 - Internetwork Packet Exchange (IPX) 591
 - IP addressing
 - client applications 598
 - Cluster service 916
- Terminal Services (*continued*)
 - IP addressing (*continued*)
 - firewalls 608
 - Network Load Balancing 599
 - preparing network 591
 - round-robin DNS 599
 - license servers
 - activating 595–596, 597
 - backing up 598
 - domain controllers 591, 595
 - domain license servers 594, 595
 - enabling License Service 594, 595
 - enterprise license servers 594, 595
 - installing client licenses 596–597, 597
 - issuing client licenses 596, 597, 598
 - License Server ID 596
 - Licensing administrative tool 597–598
 - licensing process 581–582
 - Licensing Registration wizard 581, 595–596
 - Microsoft Clearinghouse 581, 594, 595
 - overview 581, 594
 - polling 594–595
 - selecting a server 591, 594–595
 - licenses
 - client license key packs 581, 597
 - client licenses, definition of 581
 - licensing process 581–582
 - obtaining 596–597
 - optional 583
 - required 582–583
 - temporary 596, 597, 598
 - Windows 2000 license 583
 - Windows 2000 Server Client Access 582
 - Windows 2000 Server license 582
 - Windows 2000 Terminal Services Client Access 583, 596
 - Windows 2000 Terminal Services Internet Connector 583, 596
 - Work at Home Windows 2000 Terminal Services Client Access 583
 - load balancing 599
 - MetaFrame add-on 584, 612
 - Microsoft Clearinghouse
 - license server registration 594
 - licensing process 582
 - overview 581
 - server Internet connection 595
 - MultiLanguage Version 614
 - Network Load Balancing 662–664

Index

- Terminal Services (*continued*)
 - Novell servers 612
 - overview 577–580
 - performance monitoring
 - CPU performance 618–619
 - establishing baseline 618
 - memory 619
 - network performance 619
 - preparing network connections
 - client/server connections 592, 598, 612
 - Internet access 591
 - wide area networks 591
 - printing 614–616
 - remote access
 - See also* Remote Desktop Protocol
 - example scenario 587–588
 - firewalls 608
 - performance 608
 - security 608
 - via Internet 591–592, 608
 - Windows-based terminals 611
 - Remote Administration mode
 - concurrent connections 580
 - default user rights 605
 - example scenario 586–587
 - licensing 580
 - overview 580
 - Remote Control 620
 - Remote Desktop Protocol (RDP)
 - client/server connections 592
 - firewalls 591
 - installation directory 612
 - printer redirection 615
 - remote access connections 608
 - Terminal Services Configuration tool 621
 - Remote OS Installation 874
 - round-robin DNS 599
 - running applications automatically 606–607
 - SAM database 600
 - scripting 593
 - security
 - Administrators rights 605–606
 - anonymous FTP 608
 - auto-logon 606–607
 - data transfer encryption 607
 - file system 604
 - file system access 606
 - OS/2 applications 608
 - POSIX applications 608
- Terminal Services (*continued*)
 - security (*continued*)
 - remote access connections 608
 - smart cards 608
 - user rights 605
 - Terminal servers
 - CPUs 610
 - definition 581
 - domain controllers 605
 - domain structure 600
 - dump files 609
 - licensing process 581
 - memory 609
 - page files 609
 - polling for license servers 594–595
 - purchasing guidelines 609
 - registry size 610
 - Terminal Services Client Creator 621
 - Terminal Services Configuration tool 605, 621
 - Terminal Services Manager 606, 621
 - test lab environment 617
 - thin client software, definition 579
 - time zones 614
 - User Manager extensions 605
 - user settings
 - application access 602–603, 606–607
 - best practices 616
 - folder redirection 604
 - Group Policy 602
 - home directories 603–604
 - language 614
 - logon 605, 606
 - policy precedence 602
 - system policies 602
 - Terminal Services profiles 605
 - user profiles 600–601, 602, 603
 - UsrLogon.cmd file 607
 - WinFrame 612
 - Test cases 134–135
 - Test labs
 - ad hoc 103–104, 106
 - ADC connection testing 762–763
 - build phase 97, 98, 126–127
 - change management
 - post-deployment testing 137
 - return on investment 104–105
 - role of the lab 137–139
 - vs. ad hoc 106
 - definition of 95

- Test labs (*continued*)
 - designing
 - client labs 115–118
 - design phase 97, 98
 - design prerequisites 110–111
 - domains 112, 117, 119–120
 - overview 93–96
 - server labs 111–115
 - test case considerations 111
 - development phases 97–98, 140–141
 - documenting
 - changes to lab 126
 - lab description 121–122
 - logical diagrams 122–123
 - physical diagrams 124–125
 - example deployment scenario 50
 - lab preparation task list 140–141
 - managing 128–129
 - planning worksheets 992–994
 - preliminary 99
 - return on investment
 - change management 104–105
 - considerations 101
 - uses for labs 101–103
 - risk management 96
 - running tests
 - conducting tests 135–136
 - designing test cases 130, 134–135
 - documenting results 136
 - escalation plans 131
 - integration tests 130–131
 - list of tasks 99, 141
 - test plans 131–134
 - test process considerations 119
 - unit tests 130
 - server labs
 - design 111–115
 - domain design 112, 117, 119–120
 - simulating many users 695
 - strategy phase
 - lab development phases 97, 98
 - lab location 107–110
 - lab models 103–106
 - long-term considerations 100
 - return on investment 101–103
 - Terminal Services testing 617
 - uses for 101–103
 - Windows DNA Performance Kit 695
- Test pilot *See* Pilot project
- Test plans 80–81, 131–134, 779–784
- Test processes
 - change management testing 137–139
 - conducting tests 135
 - designing test cases 130, 134–135
 - documenting results 136
 - escalation plans 131
 - integration tests 130–131
 - lab considerations
 - See also* Test labs
 - domain design 119
 - lab design 111
 - restoring after test 119
 - list of tasks 99, 141
 - planning worksheets 992–994
 - proxy servers 634, 635
 - risk management 130
 - test plans 131–134, 779–784
 - testing ADC connections 762–763
 - testing applications *See* Applications, compatibility testing
 - testing cluster servers 693–695
 - testing printer shares 570–571
 - unit tests 130
- Testing applications *See* Applications, compatibility testing
- TGT (Ticket Granting Ticket) 345
- Thin client software
 - definition of 579
 - Windows 2000 *See* Terminal Services
- Ticket Granting Ticket (TGT) 345
- Time setting, Kerberos authentication 391
- Tools, deployment 1059–1070
- Topology plan *See* Active Directory site topology
- Total cost of ownership 9
- Transaction logging and recovery 693
- Transitive trusts, definition 404
- Trust for delegation 389, 390
- Trust relationships
 - Active Directory Domains and Trusts snap-in 405
 - between trees 283–284, 292, 335
 - complete trust model 261–262
 - Configuration container 405
 - default type between domains 261, 283
 - documenting current 167, 170
 - effect of upgrading
 - child domains 343–344
 - multiple-master domains 331

Index

- Trust relationships (*continued*)
 - effect of upgrading (*continued*)
 - primary domain controllers 338
 - resource domains 334–335
 - implementing 405
 - joining domain to tree 403
 - Kerberos 391–392
 - L2TP over IPSec VPNs 205
 - managing using Netdom 371, 377
 - master domains 334
 - mixed mode
 - implementing 405
 - nontransitive trusts 404
 - NTLM authentication 345
 - one-way trusts 404
 - trusts for Kerberos authentication 336
 - upgrading child domains 343–344
 - multiple-forest environments
 - creating explicit trusts 265–266, 404
 - distributed security plan 403
 - limiting scope of trust 264
 - multiple-master domains
 - administrative model 334
 - compared to complete trust 261–262
 - example 331
 - SAM database size limits 334
 - nontransitive, definition 404
 - one-way, definition 403–404
 - planning explicit
 - distributed security plan 403
 - existing Windows NT trusts 331
 - external trusts 403, 170
 - nontransitive trusts 404
 - optimizing trust path 404
 - restructuring domains 360
 - upgraded child domains 344
 - upgraded primary domain controllers 338
 - protocols supported 384, 403
 - shortcut trusts 292
 - single-domain environments 403
 - single-forest environments 263
 - transitive, definition 404
 - trusted domain, definition 403
 - trusting domain, definition 403
 - two-way transitive, definition 404
 - types of 403–404
 - Trusted Root Certification Authority container 439, 445, 461
 - Two-factor authentication 385, 389
 - Two-way transitive trusts, definition 404
 - Txtsetup.oem
 - client installation
 - distribution folder 926
 - installing mass storage devices 929
 - installing SCSI devices 928
 - listing in answer file 926
 - server installation
 - distribution folder 474
 - installing mass storage devices 477
 - installing SCSI devices 476
 - listing in answer file 474
- ## U
- Unattend.doc 480, 932
 - Unattend.txt 480, 1040–1042
 - Unattended Setup *See* Setup, unattended
 - Unauthorized applications 778
 - Uninstalling applications to deploy Windows 787
 - Unit tests 130
 - Universal ADSL 225
 - Universal groups
 - checking membership at logon 313
 - domain migration 350–351
 - Global Catalog 350
 - group expansion 352
 - mixed-mode domains 350
 - nested security groups 401, 351
 - network performance considerations 401
 - properties 351
 - when to use 399
 - UNIX
 - BIND service 168
 - client connectivity 808–809
 - multiprotocol remote access 192
 - Upgrade vs. clean install decision
 - example deployment scenario 48
 - Windows 2000 Professional
 - determining best method 919–921
 - installation method capabilities 921, 939
 - Windows 2000 Server
 - determining best method 467–469
 - installation method capabilities 469, 487
 - User accounts
 - See also* Security principals
 - access control process 396–397
 - account lockout policy 269, 415
 - adding 388

- User accounts (*continued*)
 - auditing *See* Auditing
 - authentication *See* authentication
 - authorization, definition 383, 386
 - creating 400
 - default location 388
 - domain user security policy 269, 272
 - enabling remote access 395
 - global address book 388
 - Kerberos ticket policy 269
 - moving to restructure domain 367
 - password policy 269
 - passwords *See* Passwords
 - preventing delegated connections 390
 - rights on local computers 416
 - SAM database size 334
 - User data management *See* IntelliMirror user data management
 - User education 85
 - User interface
 - accessibility *See* Accessibility options
 - configuration management *See* IntelliMirror settings management
 - User principal names 262–263, 266
 - User profiles
 - accessibility options 1079
 - dial-up profiles
 - and remote access policy 199
 - creating 818
 - VPN connections 201, 640, 916
 - Group Policy precedence 854
 - restructured domains 367–369
 - roaming user profiles
 - definition of 901
 - implementing 903
 - Terminal Services 600–601, 603
 - Terminal Services 600–601, 603, 916
 - User types
 - client configuration scenarios 910–914
 - configuration management strategies 908–915
 - defining 827–829, 1021
 - knowledge workers 828
 - mobile users
 - client configuration needs 912–913
 - definition of 827
 - software distribution issues 896
 - remote users 827, 858–859
 - User types (*continued*)
 - roaming users
 - client configuration needs 911–912
 - definition of 827
 - roaming user profiles 600–601, 603, 901, 903
 - task-based users 828, 913–914
 - Users group
 - default permissions 400
 - default permissions in Terminal Services 605
 - default rights in security templates 419–421
 - file system permissions 397
 - rights to run applications 420
 - UsrLogon.cmd user environment file 607
 - Utilities, deployment 1059–1070
 - Utility Manager 1081
- V**
- Variable Length Subnet Masking (VLSM)
 - custom subnetting 195
 - RIP for IP networks 208, 209
 - Version checking, problems caused by 791
 - Video cards
 - SMS hardware inventory 240
 - Windows compatibility 240
 - Virtual circuits 222
 - Virtual device driver compatibility 183
 - Virtual private networks (VPNs)
 - benefits of 200
 - client connectivity 811–812, 818
 - Connection Manager 643
 - deployment planning 640
 - dial-up connections 812, 817–819
 - example configuration 639
 - firewalls 641–642
 - IPSec protocol *See* IPSec (Internet Protocol Security)
 - network infrastructure planning 177
 - Network Load Balancing 662
 - overview 639–640
 - Point-to-Point Tunneling Protocol 200, 640
 - security protocols 200
 - server capacity 644
 - server location 629–630, 641–642
 - VLSM (Variable Length Subnet Masking)
 - custom subnetting 195
 - RIP for IP networks 208, 209

Index

Volumes

- fault tolerant *See* Fault-tolerant systems
- managing using Disk Management *See* Disk Management snap-in
- managing using Remote Storage 710–712

VPN *See* Virtual private networks

VxD compatibility 183

W

WBEM *See* WMI

Web servers, upgrading 573–574

See also Member servers

Web site security 425–426

Wide-area connection media 191–192

WinDNA Performance Kit 695

Window-based Terminal (WBT), definition 579

Windows 2000 Application Specification

- accessibility standards 1077
- certification for compatible applications 13, 784
- desktop and distributed applications 784
- directory of compatible applications 784–785
- Microsoft test plan 786
- Web site 786
- Windows 2000 Compatibility Guide 790

Windows 2000 Clustering *See* Windows Clustering

Windows 2000 Compatibility Guide 790

Windows 2000 deployment project plan *See*

Deployment project plan

Windows 2000 domains

- Active Directory *See* Active Directory domain structure
- consolidating domains *See* Domain restructure
- upgrading domains *See* Domain upgrade

Windows 2000 Hardware Compatibility List (HCL) 237, 562

Windows 2000 Logo Certification program

- accessibility requirements 1077
- compatibility issues 561
- directory of compatible applications 784–785
- vendor testing 784
- Web site 13

Windows 2000 MultiLanguage Version *See*

MultiLanguage version

Windows 2000 Professional

- features
 - desktop management solutions 26–27
 - device support enhancements 9
 - overview 8–10

Windows 2000 Professional (*continued*)

installing *See* Installing Windows 2000 Professional

total cost of ownership 9, 944

upgrade paths 181

upgrade vs. clean install

- determining best method 919–921
- installation method capabilities 921, 939

Windows 2000 Server

deployment case studies 15–24

features

- Active Directory 10, 13
- administration services 25
- Advanced Server 11
- Application Certification Program 13
- Asynchronous Transfer Mode (ATM) 32
- availability 30–31
- backup enhancements 33
- change and configuration management 14
- Cluster service 30
- communications 31–32
- component application services 28–29
- desktop management solutions 26
- directory services 25
- disk duplication 26
- disk quotas 33
- Distributed file system (Dfs) 33
- DNS dynamic update protocol 31
- dynamic load balancing 29
- enterprise memory architecture 30
- evaluating 24
- Fibre Channel 32
- Group Policy 13, 25
- index services 28
- information publishing and sharing 28
- instrumentation services 25
- integrated Web services 28
- intelligent I/O (I2O) support 30
- IntelliMirror 13, 26, 31
- Internet Protocol security (IPSec) 27
- IP Telephony 32
- Kerberos authentication 27
- management infrastructure services 24–25
- media services 28
- message queuing services 29
- NetMeeting 14
- Network Load Balancing 31
- networking 31–32
- NTFS encryption 27
- NTFS enhancements 33

- Windows 2000 Server (*continued*)
 - features (*continued*)
 - Option Component Manager 26
 - public key infrastructure 27
 - publish and subscribe 29
 - Quality of Service (QoS) 14, 31
 - queued components 29
 - remote installation technologies 13, 26
 - Remote Storage 33
 - Removable Storage 33
 - Resource Reservation Protocol (RSVP) 32
 - roaming user profiles 14, 26
 - scalability 30–31
 - scripting services 25
 - security features 27–28
 - security templates 27
 - smart cards 27
 - Standard Edition 10–11
 - storage management 32–33
 - streaming media services 32
 - symmetric multiprocessing 10, 11, 30
 - Synchronization Manager 14
 - Terminal Services 12, 30
 - transaction services 29
 - Web application services 29
 - Windows 2000 product family 8
 - Windows Installer 26
 - installing *See* Installing Windows 2000 Server
 - total cost of ownership 491
 - upgrade vs. clean install
 - determining best method 467–469
 - installation method capabilities 469, 487
- Windows Clustering
 - Advanced Server features 651–652
 - availability planning worksheets 1007–1014
 - Cluster Administrator snap-in 713
 - cluster environment planning 713
 - Cluster service *See* Cluster service
 - cluster, definition 653
 - failover 712, 713
 - hardware configurations 713
 - load balancing 713, 654
 - NetBIOS required for cluster servers 353
 - Network Load Balancing *See* Network Load Balancing
 - overview 653–654, 712
 - planning for availability
 - downtime costs 649–651
 - hardware compatibility 657–658
- Windows Clustering (*continued*)
 - planning for availability (*continued*)
 - needs assessment 655–657
 - planning tasks 652–653
 - planning team 654–655
 - points of failure 656–657
 - two-node cluster setup 712–713
- Windows DNA Performance Kit 695
- Windows Installer
 - custom installation options 891
 - declared upgrade relationship 900
 - example Windows deployment scenario 48
 - in mixed mode 336
 - just in time installation 890
 - native authored applications 890
 - overview 943–944, 889–890
 - package file 943, 944
 - reinstalling corrupt files 890
 - repackaged applications 890–891
 - service packs and patches 899
 - Terminal servers 593, 602
 - Terminal Services 602, 613
 - terminology 943
 - transforms 891
 - upgrading software 900
 - Windows deployment best practices 64, 66
- Windows Internet Name Service (WINS) 353, 196, 802
- Windows Management Instrumentation (WMI)
 - application scripting support 67
 - SMS inventory 164, 876
- Windows Messaging Service 791
- Windows NT 4.0 system policies 835–836, 837–839
- Windows NT browser service 339
- Windows NT domains, upgrading *See* Domain upgrade
- Windows NT security model
 - access control list (ACL) 341
 - access tokens 341
 - authentication 341
 - creating security principals using PDC
 - emulation 340
 - NTLM authentication 345
 - resource domains 334–335
 - RRAS servers 327, 358–359
 - Security Account Manager database
 - copied to Active Directory 338
 - size 334, 342, 360
 - security descriptors 341
 - security group migration 349–352

Index

- Windows NT security model (*continued*)
 - security identifiers (SIDs)
 - access control list components 341
 - access tokens 341
 - definition of 341
- Windows registry
 - applications that write directly to 791
 - auditing events 418
 - backing up 563
 - disabling registry editors 856
 - font registry keys 791
 - Group Policy security settings 418
 - mapping keys using migration DLLs 787, 528
- Windows Script Host (WSH) 25
- WinInstall LE 890
- Winnt.exe
 - command syntax 1035–1036
 - Windows 2000 Professional
 - See also* Setup (Windows 2000 Professional)
 - automated installation parameters 932, 937
 - upgrade vs. clean install capabilities 939
 - when to use 937
 - Windows 2000 Server
 - See also* Setup (Windows 2000 Server)
 - automated installation parameters 481, 486
 - upgrade vs. clean install capabilities 487
 - when to use 485
- Winnt.sif example answer file 1042–1044
- Winnt32.exe
 - command syntax 1031–1034
 - Windows 2000 Professional
 - See also* Setup (Windows Professional)
 - automated installation parameters 932, 938
 - specifying answer file 932
 - syspart switch 947–949
 - upgrade vs. clean install capabilities 939
 - when to use 937
 - Windows 2000 Server
 - See also* Setup (Windows Server)
 - automated installation parameters 481, 486
 - specifying answer file 481
 - syspart switch 494–495
 - upgrade vs. clean install capabilities 487
 - when to use 485
- WINS (Windows Internet Name Service) 353, 196, 802
- WMI (Windows Management Instrumentation)
 - application scripting support 67
 - SMS inventory 164, 876
- WSH (Windows Script Host) 25

X

xDSL 225

Y

Year 2000 (Y2K) product compliance database 244

Z

ZAP file setup 891