Managing A Windows® 2000 Network Environment Exam Cram

This Cram Sheet contains the distilled, key facts about the Managing a Microsoft Windows 2000 Network Environment exam. Review this information last thing before entering the test room, paying special attention to those areas where you feel you need the most review. You can transfer any of the facts onto the provided blank piece of paper before beginning the exam.

NETWORKING PROTOCOLS

1. Addressing protocols: AppleTalk, Internet Protocol (IP), Internet Packet Exchange (IPX), NetBIOS Enhanced User Interface (NetBEUI).
2. TCP/IP Suite: FTP, HTTP, IP, POP3, PPP, PPTP, SLIP, SMTP, SNMP, TCP, Telnet, UDP.
3. IP addressing: network address, host address, subnet mask, CIDR notation *(<IP Address>/<mask bits>)*.
4. Host identification: FQDN (myserver.mycorp.com), IP (128.46.197.101), MAC (AF-04-2B-11-69-43), NetBIOS (myserver).
5. Address classes: A (001–126.0.0.0/255.0.0.0), B (128–191.x.0.0/255.255.0.0), C (192–223.x.x.0/255.255.255.0), Reserved: D (224–239), E (240–255), localhost (127.0.0.1). Private network ranges: 10.0.0.0/8, 172.16.0.0/16,192.168.0.0/24 (a zero in the host address refers to a complete subnet).
6. Subnetting means to take an available block of addresses and designate additional network address bits in order to create smaller, contiguous numerical groupings. The remaining bits provide available host addresses within a subnet, from which one gateway and one broadcast address are unavailable for host identification. If the network addresses match, then the two IP addresses are in the same subnet.

ACTIVE DIRECTORY STRUCTURE

7. Active Directory is a multimaster hierarchical structure composed of one or more contiguous namespaces, also called *trees*.
8. Global Catalog is a distributed multimaster database containing information and settings for references to objects such as users, computers, groups, and shared resources.
9. Flexible Single Master Operation (FSMO) roles: Domain Naming Master, Infrastructure Master (not on Global Catalog Server), PDC Emulator, RID Master, Schema Master.
10. Trusts are logical connections between domains. They can be one-way or two-way, and transitive or nontransitive (Windows 2000 default: two-way transitive).
11. Forests contain one or more trees; trees contain one or more domains sharing a hierarchical name space; domains contain users, computers, groups, and organizational units (OUs); OUs contain users, computers, groups, and other OUs.
12. Groups allow inheritance of permissions by members. OUs allow granting of subdomain administrative capability.
13. Sites are made up of one or more IP subnets closely connected using dependable connections. Intersite replication is accomplished through a bridgehead server, and may be scheduled manually for off-peak times.

NAME RESOLUTION

14. FQDN name resolution: Hierarchical naming resolved using DNS or HOSTS file (located in %SystemRoot%\WINNT\System32\drivers\etc). HOSTS entries look like this: 128.167.244.10 myserver.mycorp.com.
15. NetBIOS: Flat namespace resolved using WINS or LMHOSTS file. LMHOSTS entries look like this: 128.167.244.10 myserver #PRE (#PRE designates a preload into cache at boot).
16. Lightweight Directory Access Protocol (LDAP) is used to browse the directory. Objects are listed using a distinguished name (CN=myserver,OU=sales,DC=mycorp,DC=com) whose relative distinguished name is the most unique portion (CN=myserver).
17. WINS static mapping types: domain name, group, Internet group, multihomed, and unique.
18. WINS replication can be push, pull, or push/pull.
19. DNS servers can be primary, secondary (read-only copy), or cache-only.
20. DNS querying can be iterative or recursive.
21. Zones can be forward lookup (name to IP) or reverse lookup (IP to name), and can be Active Directory integrated (Win2K domain controllers only), standard (file-based), primary, or secondary.
22. DNS resource record types: A (HOST), CNAME (alias), MX (mail exchanger), NS (name server), PTR (pointer for reverse lookup), SOA (start of authority), or SRV (service).

DHCP CONFIGURATION

23. DHCP lease process: discovery, offer, client request, and acknowledgement.
24. Default lease duration is eight days—longer for mobile users, shorter for rapid reuse.
25. DHCP servers must be authorized to provide addresses for domain members.
26. A scope must be set up for each subnet supported, with an address pool, reservations, and any scope parameters (start and end IP address, exclusion range, lease duration, subnet mask, gateway, domain name, DNS, and WINS). Scopes must be activated to become available.

ACTIVE DIRECTORY ADMINISTRATION

27. Access permissions can be explicitly allowed, explicitly denied, or implicitly denied (default). Explicit denial overrides any allowal grants.
28. Access permissions are inherited from containers, so group membership can simplify mass-assignment and rapid change.
29. The Delegation Of Authority Wizard allows delegation of basic administrative tasks.
30. MMC consoles can be created and distributed with snap-ins, along with the adminpak.msi file from the Windows 2000 Server CD, to allow local administrators access to customized interfaces.
31. Taskpads are user-friendly versions of the MMC that hide administrative complexity behind simple task shortcuts.

GROUP POLICY

32. Group policies specify settings, configuration information, and software deployment packages for users and computers to centralize management and configuration of large networks based on container-level assignment at the site, domain, and OU level.
33. Group policy objects are made up of the group policy container, which is an Active Directory object, and the group policy template, which is a hierarchical folder structure located in %SystemRoot%\WINNT\SYSVOL\sysvol\<domain>\Policies\.
34. Group Policy setting types: Administrative Templates, Folder Redirection, Internet Explorer Maintenance, Remote Installation Services, Scripts, Security Settings, and Software Installation.
35. Multiple group policies can be linked to each container, and each group policy can be linked to multiple containers. Resolution is handled from the highest-level container to lowest, with same-container resolution handled in list order from bottom to top.
36. Block inheritance prevents all inheritance from above, except settings configured with the No Override option. You can filter by group by removing the Read and Apply Group Policy permissions on the group policy link.
37. Group policy can identify a slow network as one communicating under 500Kbps, limiting evaluation to Administrative Templates, Security, and Encrypted File System settings only.
38. Administrative template types: Control Panel, Desktop, Network, Printers, Start Menu & Taskbar, System, and Windows Components. Settings can be configured as Disabled, Enabled, or Not Configured.
39. Default security templates are provided for basic, secure, and high security configurations.
40. Account policies can be configured for specific password and account lockout settings. All three of the account lockout policies must be configured to work.
41. Password policy settings include: Enforce History, Maximum Age, Minimum Age, Minimum Length, Must Meet Complexity Requirements, and Whether To Store Using A Reversible Encryption.
42. Account lockout policies include: Duration, Threshold, and Reset Counter After.
43. Scripting allows multiple commands to be enacted at logon/logoff (users) or startup/shutdown (computers). Scripts are placed within the Group Policy template under the appropriate GPO_GUID and object type (user or computer).
44. Folder redirection applies to Application Data, Desktop, My Documents, My Pictures, and Start Menu, and may be applied the same way to all, differently by group, or specifically to a user using the ***%username%*** variable.

45. Software life cycle:
    a. Preparation of the MSI Windows Installer Package using third-party software.
    b. Deployment of the package using Group Policy to publish or assign packages.
    c. Maintenance of the package using Group Policy to publish or assign updates.
    d. Removal of the package using forced or optional removal via Group Policy.

RESOURCE MANAGEMENT

46. Publishing a resource creates a reference to the object within the Global Catalog. A resource can have several published links, each with its own DACL.
47. Location specification for published resources has a maximum of 260 characters, with a 32-character limit for each name: general/less general/more precise/.
48. Shared folders have the Change, Read, and Full Control access permissions. Those without the Read permission will not be able to see the published resource when browsing the catalog.
49. When resolving access permissions, share permissions are evaluated for the most favorable combination, NTFS permissions are evaluated for the most favorable combination, and then the results of both are evaluated for the least favorable combination. A denial will override all access allowal grants.
50. Shared printer options: Connect (allows installation), Move, Open (allows job management), and Properties (driver and print queue management).

SYSTEM CONFIGURATION

51. Disks can be basic or dynamic. Basic disks have from one to four primary partitions and up to one extended partition on which logical drives can be created. Dynamic disks have one or more volumes, which can be extended, spanned, striped, or mirrored.
52. RAID types supported by Windows 2000:
    - RAID-0 (striping)—Not fault tolerant, but fast access due to simultaneous read/write capability.
    - RAID-1 (mirroring)—Fault tolerant. Inefficient use of storage but faster than RAID-5.
    - RAID-5 (striping with parity)—Fault tolerant. Slower access speed and moderate storage efficiency.
53. The **dcpromo** command allows a member server to be converted to a domain controller, or an existing DC to be reduced to a member server.
54. Domains can be in mixed mode, which allows NT 4 BDCs, or native mode, which requires that all domain controllers be Windows 2000.
55. Computer accounts can be precreated to allow new computers to join into OU containers other than the default Computers container.

INTERNET INFORMATION SERVICES

56. Virtual sites can be identified using one or more unique IP addresses, host headers, or custom ports.
57. Each IIS server can support multiple FTP, Web, NNTP, and SMTP virtual sites. Each site is uniquely identified and addressable using a browser client.
58. Virtual directories create links to folders located outside of the root site folder, but act as if they were located within the site folder hierarchy.
59. The IUSR_*<computername>* account is used for anonymous authentication and the IWAM_*<computername>* account is used to run some Web applications.
60. IIS authentication types: Anonymous (no password or logon), Basic, Digest (W2K Active Directory server and IE5+ only), and Integrated Windows (IE required, and will not function through HTTP proxy connections). FTP sites can only use Anonymous and Basic authentication.
61. Web permissions include General permissions (Directory Browsing, Read, Write, and Script Source Access) and Execute permissions (None, Scripts Only, Scripts And Executables).
62. The Permissions Wizard is used to set both Web and NTFS permissions at once. Two default templates are available: Public Web site and Secure Web site.
63. Access to Web resources is evaluated by first authenticating the user, then Web permissions, and finally NTFS access permissions.
64. Web sites are accessed using port 80 by default; FTP sites use port 21.
65. WebDAV connections allow the use of Web folders, creating remote file shares through port 80.
66. It is sometimes necessary to configure IE to bypass HTTP proxy servers for local intranet addressing.

TROUBLESHOOTING

67. The Advanced Startup Options include: Command Prompt Only, Debugging Mode, Enable VGA Monitor, Last Known Good Configuration (only useful to the last successful logon), Logged, Safe Mode, Safe Mode With Command Prompt, Safe Mode With Networking, and Step-By-Step.
68. The Recovery console can be used after all advanced startup options are unsuccessful, and can recover damaged boot sectors with the **fixboot** command or corrupted master boot records using the **fixmbr** command.
69. System monitoring can be performed using the Task Manager, System Monitor, and Network Monitor.
70. Network diagnostic utilities include the ping, tracert, pathping, ipconfig, netdiag, nbtstat, and nslookup utilities, as well as the **net** commands.
71. Microsoft publishes regular security updates called hotfixes, which are combined with other non-security-related updates into Service Packs. The hfnetchk tool can be used to scan a system or domain for needed hotfixes, and the qchain utility can be used to apply multiple hotfixes at one time.

REMOTE ACCESS

72. A small number of public IP addresses can be shared by a larger number of private addresses using either network address translation (NAT) or Internet connection sharing (ICS). ICS can be configured for on-demand dialing.
73. WAN protocols include: ARAP, RAS, and the Point-to-Point Protocol (PPP). VPNs include LT2P and PPTP.
74. Authentication protocols include: Challenge Handshake Authentication Protocol (CHAP), MS-CHAP, MS-CHAP v2, PAP (low security), and SPAP (medium security). The Extensible Authentication Protocol (EAP) allows the use of smart cards and biometric security devices.
75. Encryption protocols include IPSec, which is used over L2TP connections, and MPPE, which is used over PPTP connections.
76. Remote access settings can be configured on the user account or using Group Policy.
77. Terminal Services provides remote terminal sessions on a central server.
78. The **route add <*IP address*> mask <*mask*> <*gateway*>** command adds a static route to the routing table. The **route delete <*IP address*> mask <*mask*>** command removes it.

SECURITY

79. Auditing allows security-related information to be written to the Security log.
80. Event logs include: Application, Security, System, Directory Service (domain controllers only), and File Replication Service (domain controllers only).