This Cram Sheet contains the distilled, key facts about the Designing a Windows 2000 Network Infrastructure exam. Review this information immediately before entering the test room, paying special attention to those areas in which you feel you need the most review. Remember, you can transfer any of these facts that you've crammed into your short-term memory onto a blank piece of paper before beginning the exam.

TCP/IP

1. The Transmission Control Protocol/ Internet Protocol is required with Windows 2000. The Windows 2000 implementation of the TCP/IP suite has been enhanced to support several new features, which include:
   * Increased window size
   * TCP selective acknowledgement (SACK)
   * Internet Control Message Protocol (ICMP)
   * Disabling NetBIOS over IP
2. Along with these new features, Windows TCP/IP includes support for IPSec, which can improve the security of your network. IPSec allows administrators to encrypt TCP/IP communications between hosts. Although Windows 2000 hosts support this feature with no additional software requirements, Windows 9x hosts require third-party software to participate in secured communications. IPSec has three predefined security policies.
   * Client
   * Server
   * Secured Server
3. QoS is a routing mechanism that can guarantee data delivery for a certain application. Paths for traffic flows are determined based on some knowledge of resource availability in the network, as well as the QoS requirements (needed amount of bandwidth) for the flows. QoS-based routing allows the determination of a path that has a good chance of accommodating the requested QoS.

DHCP

4. DHCP is used to assign IP addresses to client computers.
5. DHCP can assign the following items:
   * IP address
   * Subnet mask
   * Default gateway
   * DNS servers
   * WINS server
6. DHCP can specify different configurations for:
   * Hardware vendors
   * Operating system (Windows 98 or Windows 2000)
   * Group of users
7. DHCP Server or Relay Agent is required on each subnet that does not have direct access to a DHCP server.
8. Multicast addressing is used to simultaneously send a multicast session to multiple people.
9. DHCP can be integrated with the following:
   * DNS (so DHCP clients are automatically updated in the DNS table)
   * Active Directory (to authorize a DHCP server). Without authorization, a DHCP server could not start the DHCP services.
   * RRAS servers (to allow automatic IP addressing of remote users)
10. DHCP Relay Agent is not required if all routers are BOOTP enabled.
11. DHCP servers can be clustered for redundancy.
12. Multiple DHCP servers can use a portion of each other's scopes for redundancy

DNS

13. Place one DNS server per LAN location, unless special circumstances warrant a different arrangement.
14. DNS is a required service when implementing Active Directory.
15. The three types of zones are standard primary, standard secondary, and Active Directory-integrated.
16. Use forwarders to control which DNS servers perform iterative queries on the Internet.
17. The best solution is to use the same namespace for the DNS and Active Directory services. Active Directory services can be implemented as a subdomain of a preexisting DNS namespace.
18. Standard primary and secondary zones are interoperable with other DNS services. Active Directory-integrated zones are not.
19. By default, Windows 2000 DNS clients will update their own A records in the DNS database, and the DHCP server will update the PTR record. For secure dynamic updates, the DHCP server needs to be set to update both the A and PTR records for the clients.

WINS

20. Evaluate the necessity of WINS based on the number of NetBIOS clients
21. NetBIOS can be turned off, eliminating the need for WINS in an all Windows 2000 environment
22. It is not necessary to place one WINS server at each LAN location. Use as few WINS servers as possible.
23, Do not build in redundancy into the WINS service unless it is specifically requested.

NAT

24. NAT can be used on only a nonrouted network.
25. NAT is used to hide a company's private addressing schemes from public networks.
26. NAT is installed under Routing and Remote Access.
27. NAT changes the IP address in the packet header.
28. NAT has the following requirements:
    * DHCP services are disabled.
    * DNS resolution occurs through the NAT server.
    * NAT supports only TCP/IP.
    * NAT cannot translate the following protocols:
    * SNMP
    * COM/DCOM
    * LDAP
29. The NAT server should be located between the public and private network.

30 NAT can be used over a VPN.

Proxy Server

31. All connections from a private network to the Internet or other public network need protection. The NAT, Proxy, or RRAS services can provide this protection.
32. The Proxy Server service is designed for larger networks (even routed networks).
33. Web servers need to be isolated in a screened subnet.
34. For security reasons, the proxy server and the server that provides Web services should not be on the same server.
35. NLB or DNS round-robin entries serve to load balance incoming Web requests from the Internet to a proxy server. Use NLB if the Web server is mission-critical, because NLB automatically adjusts traffic when a server goes down. Use DNS round-robin if resources need to be conserved and overhead is an issue.
36. Proxy arrays provide caching and fault tolerance for internal clients. Arrays cannot help when the bandwidth to the Internet is an issue.
37. CARP is the protocol that a Microsoft proxy server array uses for caching.
38. Caching does not help when content is secured with encryption or when it includes active content. These types of pages cannot be cached.
39. Chaining proxy servers allows client requests to be passed upstream to the proxy server with a connection to the Internet. This helps to increase cache hits, which may reduce requests to the Internet.

RRAS

40. Routers are used to isolate LANs from one another.
41. Broadcasts do not travel through a router (by default), but DHCP broadcasts can if BOOTP is enabled.
42. Routers can provide data encryption between routers.
43. Routers can be authenticated to prevent the use of rogue routers.
44. Routing protocols are RIP and OSPF.
45. IGMP is a membership list of users who are participating in a multicast session.
46. If used in an IPX/SPX network, routers will advertise resource servers to other subnets (SAP).
47. IPSec is used for router authentication and data encryption.
48. Filters can be implemented to specify which packets can pass through a router.
49. VPNs can be established between routers using:
    * PPTP
    * L2TP
    * IPSec
50. For redundancy, RRAS servers should be installed in pairs or clustered.
51. Remote access can be enabled via dial-up clients or through VPNs.
52. Encapsulation is the process of “wrapping” packets of one protocol inside another protocol for transfer over another network, such as the Internet.
53. L2TP allows IP, IPX, or NetBEUI to be encrypted and sent over a PPP connection.
54. SNA tunneling is encapsulating SNA packets inside TCP/IP packets for transfer over a TCP/IP connection.
55. The Remote Access service can be integrated with:
    * DHCP (to assign IP addresses to remote clients)
    * DNS (to dynamically update the DNS tables with DNS names of remote users)
    * WINS (to dynamically update the WINS tables with WINS names of remote users)
    * Active Directory (for central management of remote policies)

DFS

56. DFS acts like a file manager for your network shares. It allows administrators to create a directory tree that appears to be located on one server, when, in actuality, the tree could contain shared folders from several different servers. Common uses for DFS shares include the following:
    * Centralized network file manager
    * Providing a centralized backup point
    * Increasing availability by creating replicas
    * Load balancing of network traffic
58. DFS is integrated with the Active Directory (AD) database and replicates between domain controllers. The AD database is used to store the topology information of the DFS tree. The host domain controller stores the topology information known as the blob (binary large object) and replicates this information to all other DFS-enabled domain controllers.
59. Two types of DFS roots can be created:
    * Domain-based
    * Standalone
60. Domain-based roots can be replicated to other servers, which will allow access to the DFS tree if the server that the root was created on becomes unavailable.

RADIUS

61. RADIUS is used to authenticate remote users on to a network.
62. The Windows 2000 RADIUS can be integrated with other the RADIUS components of other operating systems.
63. The RADIUS server is included in the IAS service in Windows 2000.
64. A RADIUS client is included in the RRAS service in Windows 2000.

Combining Services

65. Combine services to use as few servers as possible.
66. Don’t compromise security when combining services. Proxy, Web, and authentication services for remote users should be on separate servers.
67. WINS, DNS, and DHCP can be combined onto one server.
68. Large applications such as databases and mail or communication servers should not be combined with other services.