The MCSE™ Windows® 2000 Network Cram Sheet

This Cram Sheet contains the distilled, key facts about the MCSE Implementing and Administering a Microsoft Windows 2000 Network Infrastructure 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 a blank piece of paper before beginning the exam.

DHCP

1. The lease process consists of four different messages:
   - IP request
   - IP offer
   - IP selection
   - IP acknowledgement
2. *Automatic Private Internet Protocol Addressing (APIPA)* is a client-side feature of Windows 98/2000 DHCP-enabled computers. The client receives an IP address from the 169.254.0.0/16 address range if a DHCP server is not reached.
3. A *DHCP scope* is a range of IP addresses allocated to DHCP-enabled clients on the network. Other components of the scope include:
   - *Scope options*—Additional IP configurations for the clients within the scope.
   - *Exclusions*—Ranges within the scope of IP addresses that are removed from the allocation to clients.
   - *Reservations*—Individual IP addresses within the scope that are reserved for a particular network card address on the network.
   - *Lease duration*—The allotted amount of time the client can use the IP address without renewing the lease.
4. BOOTP scopes and clients are supported along with BOOTP lease durations.
5. DHCP options take three different forms:
   - *Server options*—Effective for all scopes configured for the DHCP server.
   - *Scope options*—Only apply to the scope they are configured for.
   - *Reservation options*—Only applied to the specified computer.
6. All DHCP options have *class* and *vendor* options that can be configured.
7. *Superscopes* and *multicast scopes* are supported types of scopes.
8. Windows 2000 DHCP servers need to be authorized with Active Directory before they can allocate IP addresses to DHCP-enabled clients.
9. The *DHCP relay agent* is a computer that helps DHCP-enabled clients obtain an IP address from a DHCP server on another segment.
10. DHCP is integrated with DNS for dynamically updating both A and PTR records:
    - This task is always done on Windows 2000 clients.
    - This task may be configured for legacy Windows clients.
11. The **ipconfig** command is used to control the IP configuration for the client.

REMOTE ACCESS

12. The two different types of remote access are:
    - *Dial-up access*—Uses standard telephone lines or ISDN connections.
    - *Virtual private network (VPN)*—Uses a common internetwork to link two disparate networks.
13. Remote access must either have a static pool of IP addresses or use DHCP.
14. The DHCP relay agent is a critical component of the remote access configuration. It gives the connecting client access to the DHCP server.
15. *Dial-up services* support PPP for incoming connections.
16. *VPN services* support PPTP and L2TP for connections.
17. L2TP enables the use of IPSec for securing the payload between client and server.
18. Supported PPP configurations are:
    - *Multilink*—The ability to aggregate physical connection links.
    - *BAP*—Dynamically controls the multilink connection for optimized bandwidth utilization.
    - *LCP*—Supports the additional features of callback and Caller ID.
19. *Remote access policies* control the communication abilities and configuration between the server and client.
20. *Conditions* are the initial portion of the remote access policy that the connecting client must meet to have the policy apply.
21. The *remote access policy profile* determines what the connecting client configuration must be for communication to be successful. Configurations include:
    - Dial-in constraints
    - IP settings
    - Multilink settings
    - Authentication settings
    - Encryption settings
    - Advanced settings for IAS and RADIUS configurations
22. Authentication options include:
    - PAP
    - SPAP
    - CHAP
    - MS-CHAP v1 and v2
    - EAP
23. Data encryption is available via MPPE and the basic and strong encryption methods.
24. IAS uses the RADIUS protocol to centralize authorization, authentication, and accounting for the remote access servers in the enterprise.

ROUTING

25. *Static routes* update the routing table for network communication.
26. Static routes across demand-dial interfaces support *default routes* or *auto-static routes*.
27. *Demand-dial routing* has the following characteristics and options:
    - On-demand or persistent connection types
    - One-way or two-way demand-dial connections
    - Demand-dial filtering to allow or deny connectivity
    - Dial-out hours set to control the connection and peak time bandwidth
    - Support for static or dynamic routing
28. Demand-dial user account details include:
    - Password expiration should be turned off.
    - Change Password At Next Logon should be turned off.
    - The username needs to be the same as the demand-dial interface name.
29. OSPF terminology:
    - *Area*—A segment of like subnets that reduces intra-area traffic.
    - *Area border router (ABR)*—An OSPF router that links an area to the backbone area.
    - *Autonomous system (AS)*—A collection of networks with a common administrative authority.
    - *Backbone area*—A high-bandwidth network.
    - *Virtual link*—A connection to a new or changing area that is not directly connected to the backbone area. These connections should be avoided!
30. RIP has three options:
    - RIP v1 is chatty and supports no peer security.
    - RIP v2 supports multicast announcements, password authentication, CIDR, and VLSM.
    - RIP Listener processes announcements only (Windows 2000 Professional).
31. RIP and SAP for IPX is supported.
32. ICS supports the following characteristics:
    - Single IP address from an ISP
    - Utilizes the 192.168.0.0/24 network on the internal interface
    - Limited configuration of applications and services
    - Automatically configures a static route
33. NAT supports the following characteristics:
    - Built-in DHCP allocator or use of network DHCP server
    - Multiple Internet IP address support
    - Inbound and outbound application configuration
34. IGMP proxy and IGMP router are supported for both forwarding and multicasting

NETWORK PROTOCOLS

35. Windows 2000 supports the following protocols:
    - TCP/IP
    - NWLink
    - NetBEUI
    - AppleTalk
36. The *OSI reference model* is divided into seven layers:
    - *Application layer*—Responsible for the way network applications interact with the network.
    - *Presentation layer*—Responsible for the way network information is formatted. Also responsible for compression.
    - *Session layer*—Responsible for establishing and breaking network communications between hosts.
    - *Transport layer*—Responsible for ensuring error-free delivery of network packets.
    - *Network layer*—Responsible for addressing network packets and the route they take to their destination.
    - *Data Link layer*—Responsible for taking raw data bits and packaging them into frames.
    - *Physical layer*—Responsible for taking electric impulses off network media and putting raw data onto network media in the form of electric impulses.

37. *TCP/IP* is a 32-bit addressing scheme represented in dotted decimal notation (W.X.Y.Z) where each letter represents an *octet*. A 32-bit number called a *subnet mask* accompanies the IP address. It masks a portion of the IP address to distinguish which part of the address is the host ID and which part is the network ID. Four classes of IP addresses are supported in Windows 2000:
    - *Class A*—Contains addresses where the first octet ranges from 1 to 126.
    - *Class B*—Contains addresses where the first octet ranges from 128 to 191.
    - *Class C*—Contains addresses where the first octet ranges from 192 to 223.
    - *Class D*—Contains addresses where the first octet ranges from 224-239.
38. *Binding order* is the order by which network protocols are used in client/server communication. The most frequently used protocols should be placed toward the top of the list.
39. You install network protocols in the Local Area Connections Properties dialog box in Network and Dial-up Connections.
40. *Packet filtering* is the ability to define what traffic is allowed into and out of each NIC based on what filters are defined.

IPSEC

41. The purpose of IPSec, not to be confused with digital certificates, is to secure TCP/IP packet communication by:
    - Protecting the integrity of the packet while en route
    - Ensuring the confidentiality of the packet
    - Authenticating credentials for established entities in the secured conversation
    - Protecting computers against network protocol attacks
42. The ESP protocol provides data privacy by encrypting the IP packets.
43. *Cryptography-based keys* create a digital checksum for each IP packet. Any modifications to the packet data alter the checksum, which indicates to the receiving computer that the packet was modified in transit.
44. *Mutual verification* (authentication headers, or AH) is used to establish trust between the communicating systems; only trusted systems can communicate with each other. IPSec combines mutual authentication with shared, cryptography-based keys.
45. *Packet filtering* determines whether communication is allowed, secured, or blocked according to IP address ranges, protocols, or specific protocol ports.
46. *IPSec filters* control how packets are processed before the client sends them and before the server processes them.
47. *Internet Key Exchange (IKE)* is performed if matching filters exist on the client and server to force secure communication.
48. *Security associations (SA)* have control of the negotiating and processing of communications between client and server.
49. An SA negotiates in two phases. Phase I handles the initial negotiations and secure encryption of the packets:
    - Policy negotiation, where encryption (such as DES) and hashing (such as MD5) of the packet occur
    - DH exchange of public values
    - Authentication
50. Phase II of the SA handles the next-level processing of communications between client and server:
    - Policy negotiation: the IPSec protocol (AH or ESP)
    - The hash algorithm for integrity and authentication (MD5 or SHA)
    - The algorithm for encryption, if requested (3DES or DES)
    - Session key refresh or exchange
51. Two SAs are created, one for outbound communication and one for inbound.
52. IPSec can be used either standalone or tunneled. Tunneling adds no IPSec security levels but adds outer headers to the packet for secure transmission between routers.
53. AH provides for authentication security.
54. When IPSec is tunneled, ESP should be applied first, then AH.
55. IPSec filters specify what types of packets are allowed to be processed by a receiving computer: source port, source address, or protocol used in transport.

WINS

56. Name resolution is the process by which a host determines the IP or MAC address of another host. There are two major types of name resolution:
    - *NetBIOS name resolution*—There are four nodes of NetBIOS name resolution:
        - *B-node*—Uses a local broadcast.
        - *P-node*—Uses a WINS server.
        - *M-node*—Uses a local broadcast and then a WINS server.
        - *H-node*—Uses a WINS server and then a broadcast.
    - *Hostname resolution*—For clients that cannot use NBNS for name resolution. Uses DNS and HOSTS files as its primary method of resolving FQDNs (fully qualified domain names) to IP addresses.
57. The *LMHOSTS file* is a text file containing a table that is stored on a host and used to resolve NetBIOS names to IP addresses. Options for an LMHOSTS file include:
    - **#PRE**
    - **#DOM:<*domain_name*>**
    - **#INCLUDE <*path to file*>**
    - **#BEGIN_ALTERNATE**
    - **#END_ALTERNATE**
    - **#NOFNR**
    - **#MH**
58. The *HOSTS* text file is a table that is stored on a host and used to resolve FQDNs to IP addresses.
59. *WINS proxy* is used when a client cannot register its name with a WINS server. To configure a Windows 2000 computer as a WINS proxy, you must add the **EnableProxy** value (set to 1) to the following Registry key:

    ```
    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
       Services\NetBt\Parameters
    ```

60. *Manual tombstoning* prevents WINS servers from sending deleted records back to other WINS servers.
61. *WINS name registration* includes not only the name, but also the workstation service, the server service, the messenger service, the workgroup or domain that the computer pertains to, and the user who was logged on to the client when it registered its name.
62. *WINS name renewal*—When a client computer registers its name with the WINS server, the server returns a TTL value to the client.
63. *WINS name release*—Names are released when a client shuts down, when a client fails to renew its name within the TTL value, or when the WINS server marks it for extinction by giving it an extinction interval.

DNS

64. DNS services provide name-to-TCP/IP address resolution in forward lookup zones and TCP/IP address-to-name resolution in reverse lookup zones.
65. *Standalone primary zones* write information to the DNS database. *Standalone secondary zones* receive information from the primary zone master through zone transfers.
66. *Active Directory integrated zones* are replicated to all domain controllers, which then can receive writes to their respective databases, which then replicate through the normal Active Directory replication topology.
67. To enable secure dynamic updates of the database, you must be using Active Directory integrated zones.
68. Caching-only servers do not write to their databases, nor do they replicate.
69. Additional domain name suffixes on the client allow for multiple namespace searches for similarly named hosts.
70. If additional name servers outside of the member domain need to be searched, add those entries to the root hints file, and then configure the DNS to read that file on boot rather than consult the Active Directory exclusively.

CERTIFICATE SERVICES

71. Certificate Services must be installed for Active Directory to issue certificates for the domain.
72. If external certificate authorities (CAs) are to be used, they must be trusted by the domain in which they will be valid.
73. Enterprise certificate authorities can only issue, validate, and revoke certificates for members (objects) of that domain.
74. For external certificate issue, validation, or revocation, create a standalone certificate authority rather than an enterprise.
75. Subordinate authorities can be established for load balancing of certificate services.
76. Certificate Revocation Lists (CRLs) are used to rescind and invalidate certificates previously issued.
77. SSL is for Web and Internet services, not for domain user or machine certificates.
78. Public keys encrypt; private keys decrypt.
79. The Encrypting File System (EFS) encrypts files on a user basis, and only that user can open the file once encrypted. You can recover the file by the domain (or OU) recovery agent, but that is a separate process.
80. CA names are bound to their certificates and cannot be changed.

CORIOLIS™
Certification Insider Press
© 2000 The Coriolis Group. All rights reserved.