This Cram Sheet contains the distilled, key facts about the Designing a Windows 2000 Directory Services Design 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.

Business Analysis and Requirements

1. Consider the following points when assessing the business:
    * Scope of the rollout
    * Organizational model
        * Centralized
        * Decentralized
        * Centralized-decentralized
    * Business priorities
    * Client computing requirements
    * LAN/WAN connectivity
        * Speed
        * Available bandwidth
    * Server and workstation distribution
    * Security requirements
    * Performance requirements

Active Directory Design Elements

Forests

2. In its most basic form, a *forest* is a single domain but can contain multiple domains depending on the requirements of the business.
3. The first domain installed becomes the *forest root domain*. This domain cannot be renamed without reinstalling Active Directory.
4. Each domain added to the forest inherits a portion of its namespace from its parent domain.
5. All domains within a single forest share the following items:
    * Schema
    * Schema Admin
    * Configuration Container
    * Enterprise Admin
    * Global Catalog
6. When you're planning a forest structure, a single-forest environment is recommended. However, here are some of the business requirements that may require the creation of multiple forests:
    * Limited trusts with subsidiaries
    * Separate Global Catalogs

* Separate schema

7. Two-way transitive trusts are automatically established between all parent and child domains within the same forest.
8. An explicit one-way trust must be defined between two forests.

Trees

9. Domains within the same tree share a contiguous namespace (that is, a child domain will inherit a portion of its namespace from its parent domain).
10. Domains requiring a unique namespace can be established as a new tree within a forest.
11. Subsidiaries within a business requiring their own Internet presence can be established as a new tree within the forest; this will allow them to still have access to forest-wide resources and information.
12. Two-way transitive trusts are automatically established between any new trees established within the forest and the forest root domain; this creates a trust path throughout the forest, making resources available forest wide.

Domains

13. Domains have the following characteristics:
    * Domains determine both the security and administrative boundaries within Active Directory.
    * Domain controllers within a domain use the multi-master replication model.
    * Domains can be nested within one another (parent –child relationship).
    * Two-way transitive trusts established between parent domains and child domains within the same tree.
14. When at all possible a single domain structure is recommended but any business having any of the following requirements may result in a multiple domain structure.
    * Decentralized administration
    * Distinct administrative boundaries
    * Separate security policies
    * Separate and distinct namespaces
    * Slow physical links
15. Table 1 summarizes the security groups available in Windows 2000.

Table 1 Windows 2000 security groups.

Group Type	Membership	Scope
Local	Can contain user accounts on the local computer.	Local groups are used to assign user permissions on a local computer.
Global	Can contain user accounts from the local domain.	Global groups are used to assign user permissions to resources throughout the forest.
Domain local	Can contain user accounts and global groups from any domain within the forest.	Domain local groups are used to assign permissions to resources within the domain where the group is created.
Universal	Can contain other universal groups, global groups, or user accounts from any domain in the forest.	Universal groups are used to assign permissions to resources throughout the forest.

Organizational Units

16. Organizational Units (OUs) are container objects used to organize objects within a domain.

17. The OU structure that's designed should be based on the business' current administrative model. This way, the business can continue to delegate authority in such a way that meets its needs.

Sites

18. Sites are created within Active Directory to optimize replication.
19. Sites are groups of IP subnets connected by high-speed reliable links; a thorough assessment of the physical network will determine which IP subnets should be grouped together.

20. Sites are used to control the following traffic-generating events:

    * User authentication
    * Controlled replication
    * Site-aware applications

21. Keep the following points in mind when planning site boundaries:

    * Create a site for each group of subnets connected by a fast, reliable link.
    * A single site is usually recommended for a single-LAN environment.
    * Create separate sites for those IP subnets connected by slow, unreliable, heavily used links.

22. Site links are created between sites. The site links are transitive by default; therefore, if a site link is defined between sites A and B as well as between sites B and C, it is assumed that sites A and C can communicate.
23. For those networks that are not fully routable, the transitiveness of site links can be turned off and site link bridges can be created to establish a replication path.
24. Several configurable options are available for site links. Table 2 summarizes the options used to control replication.

Table 2

Option	Description
Transport	This is the method for transferring data between two sites. RPC or SMTP can be used.
Schedule	This specifies the time when replication can occur over the link.
Cost	This is the value assigned to the link. When multiple links exist, the link with the lowest cost is tried first.
Interval	This specifies how often during the scheduled times a site link can be used to check for updates within another site.

25. When planning sites, you'll need to select an intersite transport. Keep in mind the points shown in Tables 3 and 4 when selecting an intersite transport. These tables summarize the advantages and disadvantages of RPC and SMTP.

Table 3 Advantages and disadvantages of RPC.

Advantages	Disadvantages
Faster than SMTP.	A direct connection is required with the destination server.
Can be used for intersite replication between DCs in same domains.	Can only be used in a TCP/IP-based network.
Uses the schedules set on the site links.	Can only have one outstanding connection at one time.

Table 4 Advantages and disadvantages of SMTP.

Advantages	Disadvantages
Uses store-and-forward messaging.	Generally slower than RPC.
Multiple messages can be sent at one time.	The format of the message increases network traffic.
Because information is in the form of an email message, it can be routed.	Can only be used for intersite replication.

26. All intrasite replication is done using RPC.
27. Replication within a site occurs among all domain controllers. Between sites, connections are established between among dedicated computers called *bridgehead servers*.
28. Bridgehead servers are responsible for receiving updates from other sites; once the bridgehead receives updates from another bridgehead in another site, the information is replicated to all domain controllers within the site.
29. Keep in mind that that a bridgehead server is needed for each Domain Naming context within a site.

Planning the Placement of Domain Controllers

30. When planning the placement of domain controllers, you'll need to consider the placement of the following items:
    - Domain controllers
    - Global Catalog servers
    - Operation Masters
        - Schema Master (per forest)
        - Domain Naming Master (per forest)
        - PDC Emulator (per domain)
        - RID Master (per domain)
        - Infrastructure Master (per domain)
    - DNS servers

    Table 5 summaries the placement strategies for the listed items.

Table 5

Server	Placement
Domain Controller	A good rule of thumb is to place at least one domain controller in each site that contains workstations and users.
Global Catalog	Placing a Global Catalog server in each site will increase user response time. In native mode, a Global Catalog is required for successful logon, so consider placing one on each site containing users and workstations.
Operation Masters	The Schema Master should be placed close to the Schema Admin. PDC Emulator, RID Master, and Infrastructure Master should be located centrally within a domain. Designate one server as a "Backup Operations Master".
DNS Server	Ideally, there should be at least one DNS server per site.

DNS

31. The Windows 2000 implementation of DNS now includes the following features:
    * *SRV record support*--SRV records are used to locate services running under Windows 2000.
    * *Dynamic update*--Dynamic DNS allows host computers to automatically update DNS.
    * *Incremental zone transfers*--With incremental zone transfers, only new and updated records are sent to the secondary server.
    * *Active Directory integration*--Zone transfers can be converted to Active Directory so that they follow the Active Directory replication topology.
32. SRV records are required by Windows 2000 because hosts use the service records to locate nearby servers and resources.
33. DNS servers do not have to be upgraded to Windows 2000 DNS; it is possible to use BIND.
34. BIND versions 4.9.7 through 8.2.1 support SRV records; BIND version 8.2.2 or higher supports SRV records as well as dynamic updates.
35. Here are four design options you should keep in mind when planning a DNS naming strategy:
    * Use the same DNS domain name internally as externally.
    * Use existing DNS servers and delegate Active Directory zones.
    * Create a subdomain of the external Internet domain for use internally.
    * Create an internal network name that's different from the external one.

Group Policy

36. Group Policy is a tool that allows administrators to configure and set standards for client computing environments.
37. Group policies can be applied at the site, domain, or OU level (SDOU); the level at which a policy is applied will determine its scope.
38. When group policies are applied at different levels within Active Directory, they are applied in the following order:
    * Local computer policy
    * Site-level policies
    * Domain-level policies
    * OU-level policies
39. If there are multiple policies applied at each level, an administrator will need to specify the order in which they should be processed.
40. Group policies applied at the OU level are passed down from parent OU to child OU.
41. Table 6 summarizes the three ways the scope of a group policy can be configured.

Table 6

Options	**Description**
Filtering	Filtering allows certain security groups to be excluded from the group policy.
Blocking	The inheritance of a group policy can be blocked so it is not passed down from parent to child container.
No Override	Setting the No Override option on any group policies will prevent them from being overwritten by lower-level GPOs.

Delegation

42. Delegation of authority can be assigned to users or groups who will be responsible for administering the GPO that allows an organization to maintain some form of decentralized administration.
43. Delegation of authority eliminates the problem of having one person or group being responsible for all administrative tasks; delegation allows administrative tasks to be distributed among different individuals or groups throughout an organization.
44. It is important to characterize the type of IT organization that a business has implemented, because this will have a direct impact on the model for administration.
45. The model for administration will determine the organization of domains and OUs within the Active Directory structure. Table 7 summarizes the four models for administration.

Table 7

Model	Description
Geographical	The AD structure is organized around the different geographical locations.
Organizational	The AD structure is organized around the different departments or business units.
Functional	The AD structure is organized around the different job roles within a business.
Geographical then organizational (hybrid)	The upper layers of the AD structure are based on geographical location, and the lower layers are based on departments or business units.
Organizational then geographical (hybrid)	The upper layers of the AD structure are based on the different business units or departments, and the lower layers are based on geographical locations.

46. The OU structure that's designed should reflect the business' current delegation plan.
47. Permissions within Active Directory are typically passed down from object to child object.
48. If permissions set on a parent object should not be applied to a child object, the inheritance of permissions can be blocked.

    To block inheritance on a child object, follow these steps:

    1. Open the Active Directory Users and Computers MMC snap-in.
    2. Select the object you want to block inheritance on; then choose Properties from the Action menu.
    3. Select the Security tab from the object's Property dialog box.
    4. To block inheritance, clear the Allow Inheritable Permissions from Parent to Propagate to This Object checkbox.

Trust Relationships

49. Windows 2000 has basically three different types of trust relationships that allow users from one domain to gain access to resources in another domain. These trust types are transitive, shortcut, and external. Table 8 describes each type.

Table 8

Trust	Description
Transitive	This is a two-way transitive trust that is automatically established between parent domains and child domains within the same forest; between the forest root domain and any new trees added to the forest.
Shortcut	This is a two-way transitive trust that must be manually created between two domains to shorten the trust path.

External	This is a one-way trust that must be manually created between domains in separate forests.