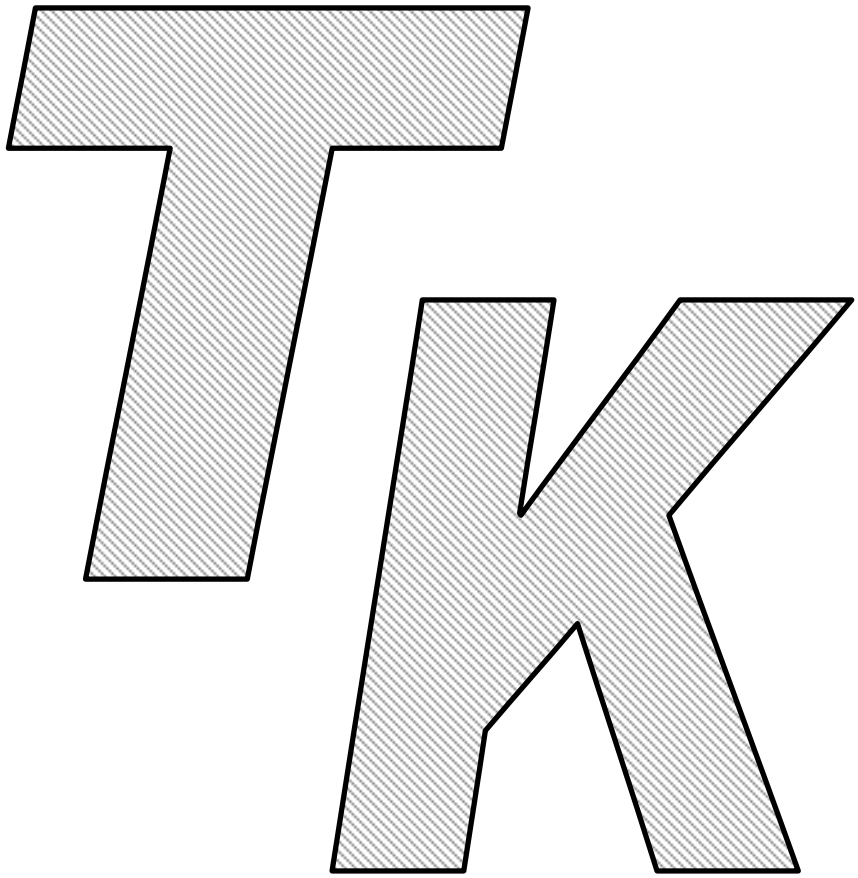
TESTKILLER

MCSE STUDY GUIDE



Designing Microsoft Windows 2000 Directory Services Infrastructure 70-219

Edition 2

Congratulations!!

You have purchased a ***TestKiller, Ltd.*** Study Guide.

This study guide is a selection of questions and answers similar to the ones you will find on the official Designing Microsoft Windows 2000 Directory Services Infrastructure MCSE 70-219 exam. Study and memorize the following concepts, questions and answers for approximately 15 to 20 hours and you will be prepared to take the exams. We guarantee it!

Remember, average study time is 15 to 20 hours and then you are ready!!!

GOOD LUCK!

Guarantee

If you use this study guide correctly and still fail the exam, send your official score notice and mailing address to:

TestKiller, Ltd
8200 Pat Booker Rd. #368
San Antonio, TX 78233

We will gladly refund the cost of this study guide. However, you will not need this guarantee if you follow the above instructions.

Table of Contents

It is important that you read and study the "Key-point Concepts" portion of this guide. We have identified important "KEYPOINTS" in this section that you will have to know to successfully pass the exam. Please ensure that you absolutely know and understand these. You will find them in double lined boxes throughout the text.

Designing a Microsoft Windows 2000 Directory Services Infrastructure Concepts

Analyzing Business Requirements

ANALYSIS OF THE BUSINESS MODEL

To analyze the business model, you must perform an analysis of the company model and its corresponding geographical scope. Models can include branch office, subsidiaries, regional, national, and sometimes international offices. The process of analyzing the business model begins with understanding the dynamic decision-making processes, business information flow, communication flow, and service and product life cycles.

To accomplish a thorough analysis of the existing and planned organizational structures, you should take into consideration the management model; the company's organizational structure; relationships with third-party vendors and partners, and customer relationships.

Both the existing model and any planned changes must be taken into consideration. This includes future planned acquisitions. Business models refer to the ways in which a company conducts its business. You must understand both information and communication flow, and the mechanism these flows rely on (e.g. e-mail, web sites, printed or verbal communication).

ANALYSIS OF THE COMPANY MODEL AND THE GEOGRAPHICAL SCOPE

In your analysis, you must determine where the company's resources are located and how are they distributed among the locations. The scope of operations may include international, national, regional, subsidiary, and branch offices. You must take into account where remote offices are located, and the relationship of those offices to each other and to the company headquarters.

International operations occur when a company has a global presence in the business community. Business is conducted in more than one country, and often, remote offices are located in different countries. International regulations and laws play an important factor in international operations.

National operations occur when the company does business within a country, and rarely conducts business outside the national boundaries. In most cases, you do not need to worry about things such as international translations, and currency.

Regional operations occur when the company operates within a state or a specific region of the country.

Subsidiary operations will require the approval for any propositions or solutions of the parent company.

Many organizations are relatively local, in which all or most business comes from members of the community, or within a city.

ANALYSIS OF COMPANY PROCESSES

Information Flow

Information flow normally follows the company's organizational chart. Geographic separation can interrupt or disrupt information flow.

Communication Flow

Communication flow often lacks formal structure. It generally results from daily contact with peers, third-party vendors, customers, etc.

Service and Product Life Cycles

The life span must be considered for each product or service the company produces. The cycle a product endures from conception to delivery may be very dynamic. Similar products or services may remain constant for years. Technological advancements often necessitate the redesign of a portion, or all of the product's life cycle.

Decision-Making Process

The decision-making process can be very formal, or decentralized, according to the strengths of the company's employees, and the delegation power of management. Analysis of the decision-making process is critical.

ANALYSIS OF THE ORGANIZATIONAL STRUCTURE

Consideration of the organizational structure should include the management model, the company organization, vendor, partner, and customer relationships, and potential acquisition plans. This analysis must include both the current existing, and future planned structure.

Management Model

You must determine the chain-of-command within the company. As different risk models are associated with different management models, you must determine the dynamics of the management model. The management style may be based on the organizational structure, or on the management style. Management can dictate rules and regulations, or it can adopt a team-oriented approach. Companies can include family-owned enterprises, privately held businesses, or large public entities. The management model will often determine the scope and planning structure that is put into place.

Company Organization

Organizations are divided in many different ways. Some organizations divide their operations by products, geographic location, or services. Remote offices may or may not include each division of the company's organization.

Vendor, Partner and Customer Relationships

You must know contractual agreements, third-party partnerships, liability limits, and the dynamics of the company's relationship with their customers. Key contact points should be indicated in the analysis. Many companies offer more advanced methods of doing business such as offering a web presence on an Internet, Intranet, or Extranet basis.

Acquisition Plans

Planning for the future is critical in analyzing the organizational structure. The company may be either seeking an acquisition, or conversely, they may be the potential target of an acquisition.

FACTORS INFLUENCING COMPANY STRATEGIES

A great many factors influence company strategies. These are identified during the information gathering and analysis stages of the planning process. Some common factors include:

Company Priorities

Priorities change with management philosophy, employee dynamics, technology advancements, and even market shifts of product sales. Priorities should be outlined based on current, and projected growth, organizational structure, and corporate philosophy.

Projected Growth and Growth Strategy

You need to analyze how is expansion for your company is accomplished. This can be accomplished by many different avenues; acquisition, divestiture, franchises, etc.

Relevant Laws and Regulations

Laws and regulations are subject to change not only by country, but also over time. Many companies dedicate a portion of their staff to keeping an eye out on changing regulations, and how it will impact their products and services. The geographic scope will affect the necessity to review local laws, state laws, regional laws and even international laws. When designing your Active Directory structure, you may have to create multiple domains to apply differing sets of rules for sites.

Identifying Tolerance for Risk

Risk to an implementation can take many forms, not all of them technical or commercial. The possibility of suffering loss in the form of having a lower quality system than anticipated, exceeding budgetary constraints, or the failure to have satisfied the business requirements are consequences of

inadequate analysis and planning. Risk management involves continuous assessment of potential risks and critical decisions to define and implement strategies to counter them.

Risk to an Active Directory program can take two forms: Risk to the implementation project or its schedule, and Risk to its efficient running after implementation. Risk management solution involves five steps: Risk Identification, Risk Analysis, Risk Action Planning, Risk Tracking, and Risk Control. Risk management involves evaluating both the risks and the opportunities.

Risk Identification

The first step in risk management must be to identify the risk, both the originating condition and the projected consequence.

Risk Analysis

The next step is to analyze the risk to outline proposals for countering action. This involves identifying the risk probability, risk impact, and risk exposure.

Risk Action Planning

The risk action planning stage is comprised of formulating strategies for risk management and contingency planning. There are four areas of risk action planning: Research, Acceptance, Manage, and Avoidance.

Risk Tracking

Tracking involves the continuous monitoring of known risks and the continuing effects of any countering actions taken.

Risk Control

This step involves setting up procedures for monitoring and controlling risk action plans, documenting and compensating for variations, and responding to warnings.

Identifying Total Cost of Operations

This must take into account all the factors related to any factor that will end up costing money. There may be obvious costs, such as software and licensing, and there may be less obvious costs. These additional costs may include the need for new hardware, administrator and end-user training, resources and implementation costs. By establishing a baseline, you can acquire reliable data regarding how costs are being incurred, conduct research into budget figures against actual figures, and identify unbudgeted expenses. You then need to develop a plan of how costs can be brought under closer control, and how they can be reduced. Common recommendations include:

- Introducing a system of checks, such as firewalls, that do not allow access to unknown and untrusted web sites.

- Imposing policies to reduce the control that users have over their own desktops.
- Changing IT management structures to reduce local autonomy.

ANALYSIS OF IT MANAGEMENT STRUCTURE

It is important to consider the network administrative structure. You must identify if the structure is centralized in one IT department or is administrative authority distributed throughout the organization based on geographic location, department, or other divisions of responsibility. You need to consider the type of administration, the funding model, outsourcing requirements, the decision-making process, and the change-management process.

Administration Type

Administration types can be either centralized or decentralized. An example of a centralized administration type is the U.S. postal system. Administrators are centrally located in one city, where the main post office branch is located, while branch offices exist throughout the United States. With a decentralized model, an administrator is stationed at each branch office to handle the needs at that office.

Funding Model

You should build a cost into each stage of any planned implementation. From that, you will be able to identify all of the stages where capital or other costs are going to occur. You can then plan for costs and have them approved in principle before you incur them. Funding will not run out before completion. Occasionally, there will be a funding model that divides responsibility for funding between several departments or divisions. You may have to deal with more than one executive sponsor. You should also, if possible, agree on a backup funding source as a fallback for your worst-case scenario taking place.

Outsourcing

Outsourcing occurs when a company employs another company, usually a specialist in one area, to run certain aspects of a corporation's affairs. This frees up resources allowing the company to concentrate on their core business. Outsourcing can include anything from accounting to IT functions. Any service that cannot be performed internally without great cost should be outsourced. When outsourcing, you must consider:

- Any or all personnel within a division or department may actually be working for another company.
- You may have to adjust your OU structure to reflect the outsourcing. It may seem logical for members of a team to report to a particular manager, but if the manager is employed by an outsourcing company, it may be practical to remove that manager from the hierarchy.

- Security considerations are heightened. You may have to rethink your views on security, and on rights and permissions in Active Directory.

Decision-making process

In most instances, decisions come from the top in a pyramid-shaped hierarchy. This may not always be the case, so you must know exactly where they are made, versus where they seem to be made. You must determine whether all decisions are made in the same place, or whether certain types of decisions are delegated to specialists. You need to establish the decision-making hierarchy, and any deviations from it, to allow you to decide where organizational and reporting boundaries can be drawn. You should create a minimum number of OUs to support the organizational structure. The fewer OUs you have, the more flexible the structure will be.

Change Management

Change management is a process intended to provide a level of corporate fault tolerance by allowing you to backtrack after a mistake, or after an erroneous decision. Change control should encompass all aspects of the Active Directory implementation, including creating, renaming, moving, or deleting objects, adding new hardware to the network, and revising the Active Directory organizational structure. You should designate one source as a permission-granting authority, and require permission to be granted before a change. This will ensure that changes by people, who are not aware of the big picture, will not be made. The permission-granting authority allows you to schedule changes to be made at the most appropriate times. All appropriate personnel need to be told of the change to limit the risk of applying a crucial change at a moment when it will conflict with another process. This will allow you to coordinate changes and schedule them at a specific time to limit downtime.

All changes should be documented, and should include recording the time and date of any changes, the people informed, and identifying the person making the change.

Analyzing Technical Requirements

You must assess how directory services will impact the technical aspects of the network infrastructure. These aspects include performance and stability. You should evaluate the company's existing and planned technical environment. After you assess the existing systems and applications and identify existing and planned software and hardware upgrades and rollouts, you should attempt to predict the impact of the Active Directory design on the existing and planned technical environment. The following factors are critical:

- Available connectivity between the geographic locations of sites
- Available network bandwidth and latency
- Company size

- Existing and planned network and systems management
- Existing methods for accessing data and systems
- Network roles and responsibilities
- Performance requirements
- Technical support structure
- User and resource distribution

EVALUATING THE EXISTING AND PLANNED TECHNICAL ENVIRONMENT

Areas you will want to consider in assessing the existing technical environment and developing a plan for the transition to Windows 2000 include:

- Proactive training of users before the rollout of the new operating system.
- Training of all technical personnel on the new operating system and how to use the directory services.
- Written documentation to aid in assisting users with common problems, and documenting reported problems.

Analyzing Company Size and User and Resource Distribution

The geographic scope plays an important part of designing your Directory Services. You must take into account the size and geographic location of all parts of the company. Analysis should also include the size and distribution of users, both internal and external. Resource allocation for peripherals and server access must be determined. Connectivity issues across geographic locations and within sites must also be documented. Identify if users are connecting for authentication only or for the entire session as with a Terminal Server.

Assessing Available Connectivity and Bandwidth

You must work closely with the network operations team to assess network connectivity and performance based on reliability, capacity, and latency. Reliability is how dependable the network link is. Capacity is the ability of the connection to transfer data packets. Bandwidth is the theoretical capacity of the network connection. Throughput, or actual capacity, is the capacity of the link, minus overhead caused by administrative data needing to flow over the link. Latency, or delay, is the delay of how long it takes to get data from one point to another.

Performance Requirements

To obtain peak performance, you must assess performance requirements, and create a baseline from which to judge future modifications. You must determine peak utilization, the type of circuits used, application requirements, and resource conflicts. During this analysis, identify any bottlenecks or potential performance hazards.

Analyzing Data and System Access Patterns

In your analysis, you need to determine if all resources are centralized or remotely disbursed. Frequently used resources should be across a highly reliable connection. You must determine if users should go through a firewall, or if they need to use encryption. If encryption is used, you need to clarify if the password, data, or both should be encrypted.

Authentication can be accomplished through the use of the following:

CHAP	Challenge Handshake Authentication Protocol. Does not use clear-text passwords.
EAP	Extensible Authentication Protocol. The client and the server negotiate the protocol that will be used. Protocols include one-time passwords, username / password combinations, or access tokens.
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol. Requires the client to be using a Microsoft Operating System (Version 2), or other compatible OSs (Version 1).
PAP	Password Authentication Protocol. Uses a plain-text password authentication method and should only be used if clients cannot handle encryption.
SPAP	Shiva Password Authentication Protocol. For backward-compatibility and is not favored for new installations.

Analyzing Network Roles and Responsibilities

Administrative roles are predefined by the operating system with additional responsibilities above the normal user. Administrative type roles include Backup Operator, Server Operator, Print Operator, and Account Operator. Service roles run as services, without user interaction, in the operating system. User roles include the right to logon and use network resources. Other roles include being an application, a group, or owner.

Analyzing Security Considerations

The most effective means of implementing security with Windows 2000 clients is through the use of Group Policies. You must analyze security considerations and provide information about access to data and resources, password policies, security protocols (IPSec), disaster recover, and authentication. You must analyze what are the needs of the organization, and what operating systems does the organization support. Determine the optimum protocol, and assess the security features that are compatible with that protocol. Determine if the existing technical structure will allow the user of Kerberos, RADIUS, or Encrypting File System. In the analysis, ensure that all potential solutions will not conflict with existing third-party tools and applications.

ANALYZING THE IMPACT OF ACTIVE DIRECTORY

Assessing Existing Systems and Applications

To understand the impact Windows 2000, and Active Directory will have on your existing network, you must analyze how the current network operates. You must identify abilities and limita-

tions. Compatibility and testing play an important role in the design and implementation of Active Directory. All existing applications must current, with the latest service pack installed. You must identify any network issues and problems including network connectivity and LAN and WAN media speeds. Protocols and addressing must be compatible with Windows 2000 and Active Directory's dependence on TCP/IP. DNS is the choice for resolution because of the foundational use of TCP/IP and the mirroring of Internet processes by Windows 2000.

Identifying Upgrades and Rollouts

You must identify planned upgrades and rollouts of new applications, and assess the impact Active Directory will have on them. Consider all compatibility issues with Active Directory, and plan accordingly.

Analyzing the Technical Support Structure

Currently, most technical support is comprised of third-party products for logging user calls, generating trouble tickets, and remote access of systems for problem resolution. Windows 2000 and Active Directory provide many auditing, and security log features which will enhance troubleshooting efforts. These features include Microsoft Management Console (MMC), Group Policy Objects (GPOs), and Terminal Services.

Analyzing Network and Systems Management

There are a number of ways to proactively analyze network and systems management. Tools available to determine the health of individual systems, WANs, and LANs include network monitoring software, server management and monitoring software, and software distribution methods such as Systems Management Server (SMS). Windows Management Instrumentation (WMI) allows you to control and monitor the hardware on your local workstations. It allows you to provide information and notification to Windows 2000 Server.

ANALYZING REQUIREMENTS FOR CLIENT COMPUTER DESKTOP MANAGEMENT

Analyzing End-User Needs

Analysis of business and technical requirements for client computer desktop management involves analyzing user work needs in addition to technical support needs. The baseline developed will allow you to establish the most productive use of network and directory services in the client computer environment. In planning the deployment of Windows 2000 and designing your network infrastructure in the most effective way, you must determine the needs of those who use the network. This information can be obtain through personal interview to determine features and functionality to increase productivity, surveys to determine increased usability, personal observation, and time studies. Software distribution methods can be assigned to a user, or to a computer. The three stages of software deployment are: Testing and Development, Pilot Deployment, and Production Deployment. You must identify whether a roaming user profile is needed for individuals who use more than one desktop. Users can be limited in their scope through the use of lockdowns using Group Policy Objects and disk quotas.

Identifying Technical Support Needs
Users must be properly trained on any new application or operating system installed. Properly trained end-users have a higher productivity rate, and log fewer trouble calls. The use of WMI allows client computers to communicate with Windows 2000 Server. Remote access to resolve issues can be implemented, power-management settings can be centralized, and WMI can restart failed services, run a specific program, or reboot a system.

Establishing the Required Client Computer Environment
The life an application can be broken down into four stages: Preparation, Deployment, Maintenance and Removal. These stages can be managed through the use of Group Policies. Users should be instructed on how to access needed applications, and problem resolution methods.

Designing a Directory Service Architecture

Active Directory's naming scheme follows the path of Forest, Tree(s), and Domains. A forest can consist of a single domain, or multiple domains. A tree is a contiguous namespace, meaning the child has the parent as part of its name (e.g. testkiller.com and support.testkiller.com). Each tree has its own identity within the forest. Active Directory names are equivalent to DNS names and use the SRV records of DNS to store information about services. The first division of DNS is into domains. The InterNIC (Internet Network Information Center) controls top-level domains (e.g. .com is commercial organizations, .gov is non-military government organizations).

AD Database Overview
Forest and Trees
The AD database contains all information about objects in all the domains from logon authentication to objects in the directory. A hierarchical structure made up of multiple domains that trust each other is called a tree. A set of object definitions and their associated attributes is called a schema. All domains in a tree will share the same schema and will have a contiguous namespace. A namespace is a collection of domains that share a common root name. An example of this is support.testkiller.com, marketing.testkiller.com, and testkiller.com. A disjointed namespace contains domains that are interrelated, but don't share common root name. This might occur when a company merges with another company. An example of this is testkiller.com, and abc.com. A forest is one or more domain trees that have separate contiguous namespaces. All the trees in a forest share a common schema and trust one another because of transitive trusts. If you have multiple forests, you must set up an explicit trust between them.

Sites
Use the Active Directory Sites And Services Microsoft Management Console (MMC) snap-in to configure sites. To create a site, add the subnets the domain controllers are in to the site object. A site object is a collection of subnet addresses that usually share a geographic location. Sites can span domains, and domains can span sites. If the subnet address of a client or domain controller

has not been included in any site, it is assigned to the initial site container created by AD, named Default-First-Site. If a subnet requires fast access to the directory, it should be configured as a site. In every site, at least one global catalog server should be installed for fast directory access, and at least one domain controller should be installed.

Dynamic Domain Name System (DDNS)
AD requires Dynamic Domain Name System (DDNS) for name resolution of objects. The records in the DNS database are automatically updated instead of the normal DNS manual methods.

Organizational Units (OUs)
An Organizational Unit is a container object that can hold users, groups, printers, and other objects, as long as these objects are members of the same domain as the OU. You can organize the domain into logical administrative groups using OUs. OUs allow you to delegate the management of the objects in the OU to other users. You can assign separate sets of permissions over the objects in the OU, other than the permissions in your domain. The Active Directory Users And Computers MMC snap-in is used to create and manage OUs. To delegate the control of an OU, use the Delegation of Control Wizard.

Global Catalog
A global catalog contains all the objects in the AD, with only a subset of their attributes. This allows you to find object quickly even in a large multi-domain environment. The global catalog serves as an index to the entire structure of all domains and trees in a forest. It is also used for user authentication, so a user can log on at any location without having to perform a lookup back to the user's home domain. The first server installed in a tree is called the global catalog server. Additional global catalog servers will improve the response time of queries for AD objects. Use the Active Directory Sites And Services MMC snap-in to create additional global catalog servers.

Domain Controllers
All domain controllers in a Windows 2000 domain have a writeable copy of the AD database. All changes performed on any domain controller are replicated to all the other domain controllers within the domain via multimaster replication. Multimaster replication occurs when there is no master domain controllers, and all domain controls are considered equal. Domain controllers are not required to replicate directly with each other. Domain controllers that are in close proximity to each other can replicate with each other, and then one of them can send all the changes to a remote domain controller.

Replication
A connection object is a connection that AD uses for replication. Connection objects are fault tolerant. When a communication fails, AD will automatically reconfigure itself to use another route to continue replication. The process that creates connection objects is called Knowledge Consistency Checker (KCC). It runs on all domain controllers every 15 minutes by default. It creates connection objects that provide the most favorable route for replication at the time of replication. KCC uses the network model that has been defined to determine connectivity between sites, but it

will configure the links between domain controllers in the same site without assistance. Changes that need to be replicated are based on the update sequence number (USN). Each domain controller maintains a table of its own USNs, which is updated whenever it makes a change to an AD object. The USN is written to the AD database with the attribute that has changed. Other domain controllers use this USN to determine whether a change has occurred on a replication partner. To reduce network traffic, only the changed attribute will be transferred. After a domain controller fails, it attempts to replicate with all of the domain controllers when brought back online. It only requests updates with USNs greater than the last USN that was applied.

Sites

AD uses sites to control replication traffic over a WAN. A site is a group of domain controllers joined by a fast connection. Intrasite replication traffic can consume a large amount of bandwidth. Intersite traffic is compressed at a rate of 10:1.

Site Links

Site links are created using either Remote Procedure Call (RPC), or Simple Mail Transfer Protocol (SMTP) after sites are created. These links facilitate the replication between sites. If not created, domain controllers will not be able to send or receive directory updates. Replication availability, cost, and replication frequency can be configured for greater efficiency. The KCC uses settings from the site links to determine which connection objects to create to replicate directory data. SMTP transport is generally used for connections that are intermittent, such as dial-up links. Replication can be set up for a specific schedule by specifying when replication over that site link cannot take place, or by default, which allows replication to occur at any time. The default replication time is every three hours. Cost value determines which link to use when there are multiple links between sites. AD always uses the lowest cost path available. You can designate a domain controller as a bridgehead server to act as a replication gateway. It accepts all replication data from other sites via slow links and distributes it to other domain controllers in the site via fast links. Bridgehead servers are commonly used when sites are separated by firewalls, proxy servers, or Virtual Private Networks (VPNs).

Site Link Bridge

A site link bridge specifies a preferred route for replication traffic. It is the process of building a connection between two links. It is not needed in a fully routed IP network. If you set up site link bridges, you must turn off the default option to bridge all site links automatically.

DESIGNING AN ACTIVE DIRECTORY FOREST AND DOMAIN STRUCTURE

Designing a Forest and Schema Structure

Within the forest, you need to design a domain structure. The domain structure should include a domain tree consisting of a root domain and (optional) child domains, all of which share a contiguous namespace. You must analyze and optimize the trust relationships between domains, when you have devised the domain structure.

Designing a Domain Structure

As administrative privileges do not extend past domain boundaries, a domain is an administrative as well as security boundary. A simple network consists of a single domain. Creating additional domains allows you to retain existing NT domain structures, manage replication traffic, support and manage decentralized administration, support international boundaries, and support more than one domain policy.

DESIGNING AN ACTIVE DIRECTORY NAMING STRATEGY

Establishing the Scope of AD

You need to clearly outline the specific use of components. AD can be used as a central employee database to manage user accounts, mailboxes, and other databases. AD can be used in conjunction with other applications to eliminate administrative overhead in managing personnel. AD is able to synchronize changes with multiple databases though replication.

Designing the Namespace

The hierarchy of the forest must be decided upon before designing the AD namespace. You must designate which domain will be the root domain, and assign its Domain Name System (DNS) name. Each additional domain should be designated as a child or subdomain of the root, or a new tree root. Use trees sparingly to avoid confusion. Use unique domain names even if those domains are not physically connected. Use names that are descriptive and distinct, but short enough to remember.

Planning DNS Strategy

DNS is a distributed database that provides host IP address resolution to client machines. DNS is comprised of three parts: domains, zones, and DNS servers. Domains are top-level DNS names like testkiller.com. These domains can contain child domains which are split into zones, support.testkiller.com, and shipping.testkiller.com. If your organization does not have existing DNS servers, or if you use them only to browse the Internet, you can use Windows 2000 DNS. But if you have UNIX DNS servers, you may have to forward all non-local requests to the corporate UNIX DNS server for resolution, create an A record for the Windows 2000 server that will host the Windows 2000 DNS server, or create an NS record on you UNIX DNS database.

DESIGNING AND PLANNING THE STRUCTURE OF ORGANIZATIONAL UNITS

Developing an OU Delegation Plan

Organizational Units (OUs) allow administrators to delegate authority on a granular basis. You must consider many factors in designing an OU plan, including the administrative policies, geographic distribution and company structure, as well as existing resource domains. An Organizational Unit (OU) is a container for organizing objects within a domain into logical sub-groupings. Creating OUs allows you to create group policy objects, control access to resources, to delegate administration if needed, to group common objects, and to establish boundaries for application of Group Policy.

Planning Group Policy Object Management
Group policies are collections of computer and user configuration settings that are linked to domains, sites, computers, and organizational units. When applied, a Group Policy affects all users and computers within a container. Group Policy settings define what controls, freedoms, or restrictions are placed over an OU. Group Policy Objects can contain seven types of settings:

Setting	Description
Administrative Templates	Defines application and desktop configurations via Registry controls.
Security	Controls access and security (account policies, lockout policies, audit policies, user rights, etc.)
Software Installation	Controls installation, update, and removal of software.
Scripts	Controls when Windows 2000 will execute specific scripts.
Remote Installation Services	Controls options when Client Installation Wizard is used by RIS.
Internet Explorer Maintenance	Manages and customizes Internet Explorer.
Folder Redirection	Defines folder redirection for user profile home directories and folders.

User configuration settings apply group policies to users, regardless of what computer they have logged on to. Settings are only applied at time of logon and removed when the user logs off. Computer configuration setting*s* apply group policies to computers, regardless of what user logs on to them. Settings are applied when Windows initializes.

Creating a Group Policy Object (GPO)
A GPO is stored in two locations; a Group Policy template (GPT), and a Group Policy container (GPC). Local GPOs are created using the Group Policy snap-in for the MMC. Site GPOs are created by Start | Programs | Administrative Tools | AD Sites And Services. Right-click the Site folder, and choose Properties, Group Policy tab. Each Windows 2000 computer can have one local GPO. Local GPOs can have their settings overridden by non-local GPOs when used in conjunction with AD. In a peer-to-peer environment, local GPOs are not overwritten by non-local GPOs. Domain/OU GPOs are created by Start | Programs | Administrative Tools | AD Users And Computers. Right-click domain or OU, and choose Properties, Group Policy tab.

Linking an Existing GPO
GPOs are linked with a container. It's through the container that GPOs are applied to individual users and computers. GPOs cannot be tied directly to users or computers. A single GPO can be linked to multiple OUs, or multiple GPOs can be linked to a single OU. Only Domain Admins and Enterprise Admins have the ability to link GPOs to domains, OUs, or sites. To link a GPO to an existing, domain or OU, use Administrative Tools | AD Users And Computers | Right-click domain or OU, and choose Properties, Group Policy tab. Click Add then choose the policy and click OK.

To link a GPO to an existing, site use Administrative Tools | AD Sites And Services | Right-click domain or OU, and choose Properties, Group Policy tab. Click Add then choose the policy and click OK.

Delegating Administrative Control of Group Policy
Delegating a GPO to a user grants that user control over the GPO, not the container to which the GPO applies. GPO management delegation includes; GPO links to sites, domains and OUs, creating GPOs, and editing GPOs. The default permissions are:

Security Group	Default Settings
Authenticated users	Read, Apply Group Policy, Special Permissions
Creator Owner	Special Permissions
Domain Admins	Read, Write, Create All Child Objects, Delete All Child Objects, Special Permissions
Enterprise Admins	Read, Write, Create All Child Objects, Delete All Child Objects, Special Permissions
System	Read, Write, Create All Child Objects, Delete All Child Objects, Special Permissions

Modifying Group Policy Inheritance
When multiple Group Polices apply to an object, the inheritance rules (order in which applied) of Group Policy apply. The order is Local GPO, Site GPO, Domain GPO, and OU GPO. Each previous GPO is overwritten by the next in line. When several GPOs are linked to a single OU, they are processed synchronously, in the order specified by the administrator.

Exceptions to Inheritance Order
Any site, domain or OU can block inheritance of group policy from above, except when an administrator has set No Override to the GPO link. No override can be set so that none of its policies will be overridden by a child container it is linked to. Loopback setting is used to merge or replace modes.

Filtering Group Policy Settings by Associating Security Groups to GPOs
By default, a GPO is applied to all members of its linked container. Filtering grants or restricts Read access to the GPO. If a user/group has Read access, the GPO can be applied; if not, it has been filtered. To apply the GPO to specific uses, modify the GPO's Access Control List (ACL). To prevent a GPO from applying to a listed group, remove the Allow setting for the Apply Group Policy setting from the Security tab. To prevent a GPO from applying to a specific user within a listed group, add the user to the list of names and then select the Deny setting for the Apply Group Policy setting.

Removing and Deleting GPOs
Deleting a GPO removes it from any sites, domains or OUs it was linked to. When a GPO link is removed, it is no longer applied, but still exists.

Managing and Troubleshooting User Environments by Using Group Policy
Group policies can be used to control the abilities of a user to perform tasks or access portions of the operating system or network. System Policies are a collection of user environment settings that are enforced by the operating system and cannot be modified by the user. User profiles refers to the environment settings that users can change. Environment control takes place via Administrative Templates. Administrative Templates control a system through editing or overwriting portions of the Registry.

PLANNING FOR THE COEXISTENCE OF ACTIVE DIRECTORY
The Active Directory can coexist and interact with other directory services, such as the DNS database and other LDAP compatible directory services that are in use on your network.

DESIGNING AN ACTIVE DIRECTORY SITE TOPOLOGY
Active Directory sites are IP subnets or groups of subnets that are connected by high performance links. Establish sites to control Active Directory replication between sites to optimize the use of network bandwidth. Bandwidth usage can be optimized by setting the interval period or by scheduling replication to occur during off-peak usage hours.

Designing a Replication Strategy
Replication takes place for domain controllers between sites (intersite replication) based upon a schedule, the amount of network traffic, and costs. The replication schedule, defined by site link and connection objects, is used to define the time that replication is allowed to occur. The replication interval is used to define how often replication should occur during a "window of opportunity" based on the schedule. Bridgehead servers are computers with additional hardware or network capacity that are specified as preferred recipients for intersite replication. The bridgehead server subsequently replicates its AD information to its replication partners. Using bridgehead servers improves replication performance between sites. When using a firewall proxy server, you must establish it as a bridgehead server and allow it to replicate AD information to other domain controllers outside the firewall.

Managing Intrasite Replication
Replication takes place between domain controllers within a site (intrasite replication) as needed without regard to cost or schedules. Domain controllers in the same site replicate using notification. When one domain controller has changes, it notifies its partners. The partners then request the changes and the replication occurs.

Urgent replication triggers:
Events replicated immediately in native-mode domains:

- changing an LSA secret
- newly locked-out account
- RID manager state changes

Events replicated immediately in mixed-mode domains:

- changes to account lockout policy
- changes to domain password policy
- changing an LSA secret
- changing the password on a machine account
- inter-domain trust password changes
- newly locked-out account
- RID manager state changes

Defining Site Boundaries

Prior to defining sites and site boundaries, you must know where all computers will be located, and how they connect to your network. Replication plans an important factor in site boundaries. Computers within a site should have a fast and reliable connection. When planning a site structure, consider load balance and fault tolerance. You must determine the need for a domain controller, the location of any domain controllers, and the location of global catalog servers. Windows 2000 will always look first for a domain controller within the same site boundary when a user tries to log in.

DESIGNING A SCHEMA MODIFICATION POLICY

An Active Directory schema is a description of the object classes and attributes stored in Active Directory. The schema defines the attributes an object class must have, the additional attributes it may have, and the object class that can be its parent for each object class. Authorized users can modify the Active Directory schema, or it can be updated dynamically. Any changes to the schema are global in nature and schema extensions are not reversible.

DESIGNING AN ACTIVE DIRECTORY IMPLEMENTATION PLAN

Your Active Directory implementation plan should be based on the existing Windows NT network and its domain structure. This plan should take into account the need to merge existing resource domains into one domain and using organizational units for the administrative delegation purposes formerly served by separate domains.

Designing Service Locations

Service locations are the placement of servers performing different functions throughout the network.

DESIGNING THE PLACEMENT OF OPERATIONS MASTERS

AD uses multimaster replication of the directory to make all domain controllers equal. Some operations are impractical to perform in a multimaster environment. In a single-master model, only one DC in the entire directory is allowed to process updates. The Windows 2000 Active Directory has the ability to transfer roles to any domain controller (DC) in the enterprise. Because an Active Directory role is not bound to a single DC, it is referred to as operations masters roles. In designing the plan for assigning operations master roles, consider performance, fault tolerance, functionality, and manageability. Operations Master placement is crucial for load balancing and fault tolerance. There are five operations masters roles:

Role	Description
Domain naming master	Forest-level master that controls adding/deleting of domains to the forest. Responsible for domain name uniqueness.
Infrastructure daemon	Domain-level master that maintains inter-domain consistency.
PDC emulator	Domain-level master that provides support for non-AD compatible clients. Handles the replication of data to Windows NT BDCs.
Relative Identifier (RID) pool operations master	Domain-level master that allocates relative IDs to domain controllers.
Schema master	Forest-level master responsible for write updates and changes to the schema.

DESIGNING THE PLACEMENT OF GLOBAL CATALOG SERVERS

The Global Catalog Server is a domain controller that contains a partial replica of every domain in Active Directory. The global catalog holds a replica of every object in Active Directory. Global Catalog Servers should be placed in locations to reduce traffic and help with load balancing and fault tolerance. Because the global catalog is needed to determine what groups the user belongs to, a user must have access to a global catalog server to successfully log on to the network.

The first Global Catalog Server is created automatically with the first domain controller within the forest. Network performance is increased if the domain controller at a site is also a global catalog server, so it can fulfill queries about all the objects in the entire forest. In areas where bandwidth is at a premium, a GCS can be configured to only receive updates after hours. If too many domain controllers are global catalog servers, replication traffic on your network will increase. For speed reasons, a GCS should be created at each site. Designing the proper placement of global catalog servers requires consideration of issues of fault tolerance, functionality, and manageability.

Creating Global Catalog Servers

There should be at least one global catalog server located in every site. If your network has multiple sites, you may wish to create additional global catalog servers to prevent queries from being performed across slow Wide Area Network (WAN) links. AD creates one global catalog server

per forest by default. To create a global catalog server, go to Start | Programs | Administrative Tools | AD Sites And Services. Open the Site folder, and open the Servers folder, then expand the server object to get to the NTDS Settings. Right-click NTDS Settings, and choose Properties. Select the Global Catalog Server checkbox on the General tab.

DESIGNING THE PLACEMENT OF DOMAIN CONTROLLERS

Planning the placement of domain controllers will require that you first plan the domain structure. Domain controllers should be created for fault tolerance and functionality. As you can't change a server's name when it is a domain controller, you must carefully consider the names you will give to your domain controllers. Considerations in determining where to place domain controllers on the network include: performance (a domain controller at each Active Directory site will optimize logon traffic) and fault tolerance (multiple domain controllers provide for automatic backup of user accounts and other Active Directory information that is replicated from one DC to the others). The Infrastructure master should be placed on a domain controller that is not the global catalog server for load balancing and to separate the burden of each role.

DESIGNING THE PLACEMENT OF DNS SERVERS

You must determine how many DNS servers will be needed, and what role they will play in your Windows 2000 network. You must also consider whether the DNS server will also act as a domain controller or will be a member server. You will also have to decide which of the servers will host primary zone files and which will contain secondary copies. Consider replication traffic and fault tolerance in designing the DNS plan. If you have existing DNS servers, such as UNIX DNS servers on the network, you must plan for interoperability with them. DNS servers can be running Windows 2000, or other operating systems, provided they accept SRV records. When you install Active Directory, you must identify a DNS server. If you cannot do so, the Active Directory Installation Wizard will prompt you to convert the existing machine into a DNS server as well.

Interoperability with Existing DNS

The Domain Name System (DNS) is the Active Directory locator in Windows 2000. Active Directory clients and client tools use DNS to locate domain controllers for administration and logon. You must have a DNS server installed and configured for Active Directory and the associated client software to function correctly. Non-Microsoft DNS servers can be used with AD if they support SRV records and dynamic updates. The DNS server in Windows NT Server 4.0 cannot be used with AD, but BIND versions 8.1.2 and later can. Active Directory Integrated DNS uses the directory for the storage and replication of DNS zone databases. If you use Active Directory Integrated DNS, DNS runs on one or more domain controllers and you do not need to set up a separate DNS replication topology.

Configuring Zones for Dynamic DNS (DDNS) Updates

Zones can be configured for dynamic updates. Resource records will then be updated by the DHCP clients and or server without administrator intervention. The Only Secure Updates option is only available in Active Directory integrated zones. To configure DDNS, from the DNS console,

select the server you want to administer and then select Forward Lookup Zones. Right-click the domain name and choose Properties. Check the Allow Dynamic Updates box on the General tab. You must do the same for the Reverse Lookup Zones. Root or "." zones cannot be configured for dynamic updates.

Managing Replication of DNS Data

Zone Transfer is the duplication of data between DNS servers that do not participate in AD. Zone Replication is the replication of data between DNS servers (on domain controllers) that participate in AD. Zone Replication DNS servers poll AD every 15 minutes for updates. Zone Transfer uses DNS Notification. There are two zone transfer types, full zone transfer (AXFR) and incremental zone transfer (IXFR):

- AXFR*:* When the refresh interval expires on a secondary server it queries its primary using an AXFR query. If serial numbers have changed since the last copy, a new copy of the entire zone database is transferred to the secondary.
- IXFR: Uses serial numbers, but transfers only information that has changed. The server will only transfer the full database if the sum of the changes is larger than the entire zone, the client serial number is lower than the serial number of the old version of the zone on the server or the server responding to the IXFR request doesn't recognize that type of query.

Designing a Microsoft Windows 2000
Directory Services Infrastructure Practice Questions

Mahkent Cryonics

Windows 2000 Upgrade Project:

You have been assigned the task of providing consulting services for a company called Mahkent Cryonics. This project is to include development and integration services for the company's IT. Part of this project will consist of the implementation Windows 2000. Client computers currently running any version of Windows will be upgraded to Windows 2000 Professional. The Windows NT 4.0 domain controller environment should be fully upgraded to Windows 2000 Server whenever possible.

Background:

Mahkent Cryonics is a research firm that began as a cryonics firm but has diversified into other industries. Mahkent Cryonics operates from several locations in the United States, and its headquarters and primary IT center is in Washington, D.C. The bulk of their contracts are with the military. The company is distributed as follows:

Research Facilities

- Amherst, Massachusetts
- Boulder, Colorado
- Berkeley, California
- Pasadena, California
- Seattle, Washington
- Miami, Florida
- Washington, D.C.

The Boulder, Berkeley, Pasadena and Seattle facilities were originally a separate company named Ferris Aircraft. Mahkent Cryonics purchased Ferris Aircraft and took ownership of its facilities in 1996. Ferris Aircraft still maintains its name and facilities as a separate company. Mahkent Cryonics is likely to acquire another company in the near future.

Problem Statement:

Chief Executive Officer (CEO):

Being a military research contractor, we work on a variety of classified projects. Our primary concern is security. Even though we purchased Ferris Aircraft in 1996, it still operates much like as a separate company. We wish to eliminate duplication of effort within the two companies as much as possible, and we are in the process of developing common operating practices.

At times, government and military customers are allowed access to some of our data to coordinate research.

Our purchase of Ferris Aircraft caused us to restructure our entire security network structure. In the future we must be able to support our growth plans without the having to restructure again.

Chief Information Officer (CIO):

In some cases we will use operating systems other than Windows 2000 to avoid the need to replace existing hardware.

We want an integrated directory service to avoid having to build several directory service areas. To this end, we will be migrating our Microsoft Exchange 5.5 organization to Exchange 2000.

Currently all account administration must be performed from our IT centers. We would like to remove this limitation and also would like a security infrastructure that does not require restructuring when the accounts database reaches 40 MB.

The current arrangement of trust relationships is cumbersome to manage. Our Windows NT 4.0 domain structure consists of several domains for delegation of administration. Our goal is to eventually have a global IT facility that will use common software, standards, and procedures. Consolidation will begin with the Windows 2000 upgrade but we do not expect to complete it during the upgrade process. The IT facilities should be controlled from one location as necessary, but we also want to be able to delegate certain tasks without the need to create new domains.

We are unsure if Windows 95 and Windows 98 offer adequate security at the client computer level. We want to increase control while continuing to standardize client computers and applications in all departments.

We also want to standardize the security and management environment throughout the company.

The disruption caused by Windows 2000 upgrade must be minimized. The upgrade cannot be allowed to compromise our security.

History:

Mahkent Cryonics has a diverse server environment that uses mainframe, UNIX, Novell, Macintosh, Banyan VINES and Microsoft servers.

The Windows NT domain structure as it exists today was configured in 1996, shortly after the purchase of Ferris Aircraft. The domain structure was created in an attempt to integrate the IT structures of the two companies. The Windows NT network was configured with a coexisting server structure, with migration and interoperability gradually implemented. Since that time, service packs up to Service Pack 7 have been applied. The eventual removal of the remaining Banyan VINES and Novell servers is the goal of this migration.

Existing IT Environment:

General:

Mahkent Cryonics uses 25,000 personal computers, with the distribution of users shown below:

Amherst	2,900
Boulder	4,200
Berkeley	1,900
Pasadena	3,600
Seattle	2,400
Miami	2,600
Washington, D.C.	7,400

Currently there are two Windows NT account domains, and all user accounts are located in these domains. One resource domain has been created in each of the seven geographic locations and there are account domains in Washington, D.C., and Pasadena, with BDCs distributed throughout the company as needed. The Washington, D.C. location has two domain controllers that run custom applications not compatible with Windows 2000. These domain controllers will remain on computers that run Windows NT Server 4.0 during the upgrade process, and will be migrated at a later date.

Network Infrastructure:

A 44.736-Mbps line connects the Pasadena office to the primary IT center in Washington, D.C., and is used primarily for business applications. The Pasadena-Washington D.C. WAN link has an average available bandwidth of 35 percent. There are 1.544-Mbps lines from Washington, D.C., to Boulder, Amherst, Miami, Seattle and Berkeley. 1.544-Mbps lines also connect Pasadena to Berkeley, Boulder and Seattle. These WAN links will be upgraded if more bandwidth is needed.

There is one internal DNS server at each location that is used to manage the current UNIX environment. The current internal DNS implementation does not support SRV records, Unicode characters, dynamic updates, or incremental zone transfer. IT staff members who maintain DNS servers also currently manage both the UNIX and Windows NT Server environment. The external DNS systems for both the Mahkent Cryonics and Ferris Aircraft web sites are currently being hosted on third-party ISP servers. DNS modifications required for the implementation of Windows 2000 will be designed to use the existing internal DNS structure.

IT Structure:

The Washington D.C. office contains the primary IT center, and there is also a major IT center in Pasadena. The Pasadena research facility operates almost as an independent business unit. Since 1996, the IT structure has been moving toward a more centralized model; with all account management performed from Washington, D.C. and Pasadena. All Windows 2000 operations masters are to remain

in the default locations. The departments that must be supported by the IT infrastructure include the following:

- Administration
- Chemical
- Sales and marketing
- Human resources
- Management
- Public relations
- Biological
- Real estate
- Mechanical
- Information technology (IT)
- Research
- Aerospace
- Electrical
- Financial

The Washington D.C. and Pasadena IT centers define policies and application specifications and also provide telephone support for each department. There are smaller IT departments at each geographic location that report directly to the global technical support center. IT staff in the local offices are divided by department and departmental responsibilities.

Security:

The two domains currently have different security policies for password complexity and length, and for account lockout. These policies will remain the same after the Windows 2000 migration is complete. Accounts will be created at the Washington, D.C., and Pasadena facilities, but the rights for resetting passwords and changing attributes will be delegated to local IT administrators.

IT administrators grant users rights by adding global groups to local groups, and there will be four levels of administrators for day-to-day operations:

- **Enterprise Administrators:** a small group of users contained in a separate top-level domain to manage the entire organization.
- **Domain Administrators:** users granted rights to the entire domain.
- **Branch Administrators:** users granted rights for operations at the physical locations.
- **Departmental Administrators:** users that will have localized rights based on specific role

Branch and departmental administrators of resource domains will not have administrative rights for the corresponding account domains.

Group Policy Goals:

IT staff in the Washington, D.C. office will be managing Group Policy as much as possible. Group Policy will be designed to:

- Redirect folders to minimize logon time
- Define logon scripts
- Set security
- Allow specific software to be made available for installation in departments where users have the ability to install software.

Mahkent Cryonics Keypoints

Preliminary Network Preparation Keypoints:

The upgrade plan you should use for Mahkent Cryonics should be to first **create a root domain**. Then you should **upgrade the two account domains to Windows 2000, upgrade the resource domains, and then consolidate the resource domains into the account domains**.

To design the group policy hierarchy that should be applied to a user in the human resources department for technical staff at the Amherst research facility, you should apply the Group Policy objects in this order: **Amherst site GPO, domain GPO, Amherst OU GPO, human resources GPO.**

The most important factor that you should consider when deciding whether to create more than one domain is **the requirement that different companies have different account lockout policies.**

You implement the administration of group policy by **enabling domain administrators to create Group Policy objects to link GPOs to sites, domains, and organizational units, and to edit site-level and domain-level GPOs.** You should also **enable departmental administrators at each location to edit GPOs that apply to their departmental OUs.**

Post-upgrade Network Design Keypoints:

After upgrading the Mahkent Cryonics client computers and domain controllers to Windows 2000 as planned, you should then choose the locations for the server services. Given the arrangement below, you should move the following services to the North American locations.

- **Washington, D.C.; RID master, schema operations master, infrastructure operation master, domain naming master, PDC emulator, global catalog, DNS.**
- **Amherst; Global Catalog, DNS.**
- **Pasadena; global catalog, DNS, PDC emulator, RID master, infrastructure operations master.**

North American Mahkent Cryonics Locations	Server Services
Washington, D.C. Amherst Pasadena	global catalog DNS RID master schema operations master infrastructure operations master PDC emulator domain naming master

The resources on three domain controllers the Washington, D.C. office will need to have permissions assigned to them. These permissions must be granted to users at all facilities. To fulfill these require-

ments, you should **create a domain local group in the local domain, and grant this group access to the resources**. **You should then create one global group in the appropriate domain or domains, and add to this group the users who need access to the resources**. Finally, you should Add the global groups to domain local group.

You must provide DNS services that will support SRV records to change the current DNS to prepare for the implementation of Windows 2000.

The DNS naming strategy for Mahkent Cryonics should be implemented by **upgrading the existing DNS infrastructure** and then through the use of **three domains named mahkent-cryonics.com, corp.mahkent-cryonics.com, and ferris-aircraft.mahkent-cryonics.com**.

The DNS for Mahkent Cryonics should be designed by **upgrading the existing UNIX DNS service**. Then **on this service**, you should **configure the zones required for Windows 2000**.

Nelson Novelties

Background:

Nelson Novelties is a medium-sized manufacturer company that designs personalized corporate marketing products for large companies.

Nelson Novelties is acquiring one of its clothing suppliers named Grundy Imports. Grundy Imports is well known and has an Internet presence with its own domain named grundyimports.com. Grundy Imports will continue to operate independently of Nelson Novelties.

Problem Statement:

Nelson Novelties wants to decrease the number of IT administrators in the domain and to decrease technical support cost by performing all technical support at an IT center in Lansing, Michigan.

Organization:

Headquarters:

The Nelson Novelties headquarters located in Lansing, where there are two separate locations, one for IT, and one for the corporate offices. The Lansing has 2100 employees, with 100 employees employed in the IT center and 2000 in the corporate offices.

Manufacturing Facilities:

Nelson Novelties also employs 20,000 people, of these 8,000 use computers. There are currently nine manufacturing facilities in the United States and in two facilities in Canada. Manufacturing facilities are also currently being built in Europe and Mexico.

Geography:

The company is divided among the following regions:

EAST – 3,000 users:

- Boston, Massachusetts - regional headquarters
- Albany, New York
- Scranton, Pennsylvania

MIDWEST – 3,000 users:

- Chicago, Illinois – regional headquarters
- Cincinnati, Ohio
- Columbus, Ohio

WEST - 2,000 users:

- Houston, Texas - regional headquarters
- Reno, Nevada
- Pasadena, California

CANADA – 1,000 users:

- Montreal, Quebec
- Toronto, Ontario - regional headquarters

The Montreal office will soon be permanently closed, and many of its users will be transferred to Toronto. If the current implementation schedule is followed, the Montreal office is scheduled to close during the Windows 2000 phase of implementation, but it might not close until after the implementation is complete.

Nelson Novelties is expanding its operations to Europe, with a sales office recently opened in Berlin, Germany, and further plans to build manufacturing facilities elsewhere in Europe. There are manufacturing facilities currently being built in Mexico as well. The Mexican manufacturing facilities can be used by all sales regions.

Existing IT Environment:

WAN:

- Scranton and Albany connect to Boston by means of a 56-Kbps line.
- Boston connects to IT center by means of a 1.544-Mbps line.
- Cincinnati and Columbus connect to Chicago by means of a 56-Kbps line.
- Chicago connects to IT center by means of a 1.544-Mbps line.
- Pasadena and Reno connect to Houston by means of a 56-Kbps line.
- Houston connects to the IT Center by means of a 1.544-Mbps line.
- Europe, Mexico, and Toronto connect to IT center by means of a 56-Kbps line.
- Lansing headquarters connect to the IT center by means of a 1.544-Mbps line.
- Montreal connects to Toronto by means of 56-Kbps line.
- Bandwidth usage is minimal.

Client Computers:

All desktop client computers run Windows NT Workstation 4.0, and portable computers run either Microsoft Windows 95 or Windows 98.

Network:

There are three Windows NT 4.0 domains; NNNA, NNEU and NNENG. All locations in Canada, Mexico, and the United States are in the NNNA domain and Berlin is in the NNEU domain. A two-way trust exists between NNNA and NNEU. All locations use Windows NT Server 4.0 for DNS, WINS, and DHCP, and each location also has a BDC and a separate application server. The Berlin

office has a PDC and a BDC for only the NNEU domain, and there is not a NNEU BDC in North America.

For security concerns users in the Engineering department have their own domain named NNENG. Engineering department personnel also provide administration for the domain. These personnel administer all the user accounts and resources. The NNNA domain trusts the NNENG domain.

Passwords expire after 45 days on the NNNA domain, and NNEU domain passwords expire after 30 days.

Each manufacturing facility has a mainframe computer to quickly process orders and quotes. The manufacturing facility mainframes use only TCP/IP.

Network Roles:

The regional headquarters each has a technical support staff, and the Mexico office is managed from the IT center in Lansing. Locations without the network administrators have mainframe administrators who also help with domain administration and respond to support calls for basic issues and add and remove user accounts. The mainframe administrators' knowledge is usually limited to basic account administration.

Envisioned IT Environment:

WAN:

Before the Windows 2000 implementation, the 56-Kbps connections will be replaced with a 1.544-Mbps line, but there is no plan to upgrade the 56-Kbps connection to Canada and Mexico.

Grundy Imports will connect to the Nelson Novelties through a 256-Kbps line. Nelson Novelties wishes to continue using the existing IT administrative structure and security policies for Europe and North America.

Network Roles:

Nelson Novelties will create two new technical support centers, one in North America, and one in Europe. The regions will have a small IT staff responsible for basic support like password resets and account lockout resets. Tasks requiring higher levels of administrative access or more advanced skills will be performed by the European or North American support centers. Support for European offices taking place after European business hours will be performed by the North American support center. Each support center will be responsible for granting access to resources as needed.

The North American and European and support centers should have complete control of their own resources. The engineering department's domain will be removed during the Windows 2000 implementation. Users and resources currently in the engineering department will be integrated into Active Directory as normal users and resources.

Software:

A third party software development company is currently creating human resources software for Nelson Novelties. This software will enable employee management for all of Nelson novelties, and will be integrated with Active Directory while adding additional attributes to user objects. Grundy Imports is developing similar software, but both software solutions will be implemented independently.

Internet:

Nelson Novelties has registered nelsonnovelties.com, and Grundy Imports have registered as grundy-imports.com.

Client Computers:

Client Computers are to be upgraded to Windows 2000 Professional.

Policies:

Each region should be created in Active Directory as a separate entity, but group policy can vary among regions and locations. Technical support staff in each region should be able to change policies at each location.

Nelson Novelties Keypoints

Preliminary Network Preparation Keypoints:

The Active Directory will be affected by the following given factors that are influencing Nelson Novelties business strategies.

Active Directory Design Components	Business Factors
Site design Domain design OU design Forest design	• Manufacturing facilities are being built in Germany. • Nelson Novelties acquiring Grundy Imports. • IT support tasks will be performed at American and European Technical support centers. • The Montreal office will be permanently closed. • The European office will operate independently of North American office.

Using all business factors only once the concerns affect design as follows:

- **Site design: The Montreal office will be permanently closed.**
  Manufacturing facilities are being built in Germany.

- **OU design: IT support tasks will be performed at the North American and European technical support centers.**

- **Forest design: Nelson Novelties is acquiring Grundy Imports.**

- **Domain design: European offices will operate independently of the North American offices.**

The factors that should have the most influence on the site topology for the Nelson Novelties should be **number of locations** and **available WAN bandwidth**.

To allow the users in the engineering department to continue to administer their own resources after the Windows 2000 implementation you should **create a separate Organizational Unit for the engineering department** and then **locate this OU in the North America domain**. You should then **Grant the engineering department complete administrative control of its Organizational Unit** and **move computer and user objects into the OU**.

The factors you should consider when designing the domain naming strategy for Nelson Novelties are:

- **The company wants to implement separate security policies for Europe and North America.**
- **The company wants to have an Internet presence.**

Post-upgrade Network Design Keypoints:

To integrate Europe and North America in Active Directory you should **create one forest for Nelson Novelties** and **create one domain for Europe and one domain for North America**.

After the Windows 2000 implementation is complete the domain names that should be used in the internal DNS for Nelson Novelties are **europe.nelsonnovelties.com** and **northamerica.nelsonnovelties.com.**

The server roles that should be implemented are, **one schema operations master, one domain naming master, two RID masters, two PDC emulators, and two infrastructure operations masters**.

The factors that should most influence the decision to place Europe in Active Directory as a domain or as an Organizational Unit should be **the current and proposed IT administrative structures and security policies in Europe**.

After the Montreal office is permanently closed there should be **14** sites used for the nelsonnovelties.com domain tree?

To prepare for the transfer of employees from the Montreal office to the Toronto office you should **create separate OUs for Montreal and Toronto** and **move the user accounts to the Toronto OU when the Montreal OU is removed**.

The strategy to be used to integrate Grundy Imports to Nelson Novelties in Active Directory should be to **create a forest for nelsonnovelties.com** and **create a second forest for grundyimports.com**.

Grant Resort Technology (GRT)

Background:

Grant Resort Technology specializes in developing equipment for ticketing and access control for ski resorts. GRT has a turnstile-gate technology that uses smart-card reading units. The turnstile units can unobtrusively access information from smart cards to authenticate users, and can also add or subtract values from the cards. The turnstile units can read the cards from a distance, which means users need only to pass by the units with the cards. The cards can also be used to purchase items at the resorts, as monetary amounts can also be added to or subtracted from the smart-card accounts.

GRT wishes to expand its role to serving the IT needs of ski facilities and the customers that it serves.

GRT recently acquired a large amount of investment money, which it will use to support an aggressive project to make itself a premier information-service provider to some of the most prestigious ski resorts in the world. The purpose of this project will be to build a large membership of individuals who have common interests and provide them with new and unique services.

GRT plans to customize its services to meet specific needs of each resort through promotion efforts unique to each resort. GRT will also begin a program, which will provide a benefit known as the Passport that any member can use any resort served by GRT. GRT plans to use the membership list that it will create to promote products.

Problem Statement:

Grant Resort Technology currently has only turnstile smart card tracking equipment, so the company must acquire the technical expertise to develop new IT infrastructure to support its plans.

Grant Resort Technology plans to implement its goals in three phases:

Phase 1 will occur during the next year. During phase 1 GRT will build the member web site, and install at one resort location a resort employee IT that will be integrated with this web site. GRT will then test and then install the system at five additional resorts. The goal of phase 1 is to have a global member IT system with six resort IT systems operational within 12 months.

Phase 2 will occur over the following year. In phase 2 GRT plans to add 15 more resort locations. GRT also plans to achieve a total membership of more than one million.

Phase 3 will occur over the following year. In phase 3 GRT plans to double the number of resort locations and members.

Grant Resort Technology intends to gain recognition in the market through the use of the newest technologies. The company is willing to take risks if the ideas are realistic and provide services that will promote customer loyalty and company recognition.

Business Goals:

Members will be able to buy tickets for ski lifts and reserve rental equipment from their home computers or at the resorts, and individual user details will be retained so that sizes, quality, and other details need only to be added only once. When a customer arrive at a resort they will need not to wait as all equipment will be prepared and stored in the locker. There will also be provisions made for storage and transport of customer-owned equipment to any resort served by GRT.

Grant Resort Technology does not want its customers to have to wait for any services at any ski resort serviced by GRT. Customers will be able to purchase tickets for ski lifts online from kiosks. As a part of a membership, GRT will issue smart cards attached to the stretchable cords. At the resorts members, will be able to use the cards to open their lockers, gain access to ski lifts, make restaurant reservations, and as the key to their rooms. Points will be accumulated for services that are purchased, which will be used to earn gifts and awards. Members purchasing goods or services with the smart card at the ski lodge or store will enjoy discounts. There will be three memberships classifications available: Premier, Active Skier, and Standard. Higher membership levels will receive increased discounts.

GRT will also provide members with voice mail and e-mail services. Computers for these services will be located in each room and at various locations at the resort. When members pass the ski lift turnstile the will be notified by a sound if they have any new e-mail or voice mail messages. Members will be able to retrieve their messages at the top of the lift. These services will provide convenient ways for members to locate and communicate with other. Family and friends at home who know a member's account ID will also be able to communicate with that member.

Reports on current ski lift usage will be broadcast on the web site and on displays in the lodges. Resorts will have the option of instituting a premium classification for access to the lifts. Members of the premium classification will not ever need to wait to get on the lifts.

Members can share account IDs and add the IDs to their family or friend lists with the aim of making it easier for members of a household to make reservations for the entire family, or for individuals to see which of their friends are skiing on a given day.

Envisioned IT Environment:

Grant Resort Technology will design and construct global services to support two interrelated components, one for members and one for resorts. Members will be able to access the member component from the Internet or any resort, and the resort component will be used to support the resorts. The resort component will be able to support the unique internal business and employee needs of each resort.

The company headquarters is located at Boulder, Colorado, and employs 56 people. GRT has installed a high-speed connection to the IT center in San Jose, California. The IT center is connects to the Internet through a 45-Mbps DS-3 lines. GRT will not create a separate employee domain.

The design of phase 1 includes the implementation of the member systems and the resort employee systems at the following locations:

- Austria
- California
- Canada
- Colorado
- Switzerland
- Vermont

Customers will be able to enroll for GRT services at each resort, and they will also be able to complete application forms on the Internet. Members are affiliated with one resort but will be able to use services from all resorts.

The resort LANs will be upgraded to the highest feasible bandwidth and each resort will have a connection to the Internet. Connection speeds will vary depending upon the services locally available to each resort. Each resort will have a Virtual Private Network tunnel to the servers at the San Jose IT center.

During phase 2, Grant Resort Technology will open an office in Europe tasked with managing the resorts in Europe.

As the company grows, GRT plans to have business and IT management centers in each country in which it operates.

Interviews:

GRT Chief Information Officer (CIO):

There are two major components of our expansion plans, which will be constructed at the same time: members and resorts. The members component will provide services to the skiers, while the resort component will provide services to the resorts and employees. Active Directory is crucial to both components of our expansion plans.

The schema for the directory that serves members will need to be modified to support the new functionality. In order to facilitate development and security, the server that hosts the member schema master will be placed at the headquarters in Boulder. Member accessing GRT services from any resort will have the same functionality.

All logon requests must avoid using WAN line to achieve the fastest response time. Even if the members travel from one resort to another their logon processes should be performed locally as to not require a WAN transmission. Resort employees must be able to update the members' records registered only at their own resort. Request to change member records from other resorts will be sent to GRT staff, so it should be easy to move member user objects between resorts.

In the case of server failure, we need to implement a fault-tolerance design at each resort so that local service will continue to run even if one server fails. Directory replication must be avoided during times of peak usage.

Servers at the IT center will include one domain controller that contains the infrastructure operations master and one domain controller with a global catalog.

Both member and resort networks must support wired and wireless devices, which can be connected and automatically assigned IP addresses. Other applications must be able to access the devices through the use of DNS names for security reasons. In order to allow each resort to automate its internal operations, we will provide turnkey system that integrates advanced Windows 2000 functionality and Active Directory into each location. The design of these systems will ensure that employee information for one resort will not be visible to the other.

Resort Manager:

The GRT resort infrastructure will provide some great services to employees at the resort. Employees will access the system for various services including e-mail, training and safety programs, the purchase of supplies, equipment inventory and maintenance, human resources information, and staff scheduling. Employees are going be able to access our system from a variety on client computers and kiosks. Kiosks will consist of computers that run Windows 2000 Professional and have touch-screen plays. Smart-card authentication and password authentication should be used for employee security authentication, with specific employees assigned the responsibilities of issuing smart cards and updating member records.

Resorts typically employ people in the following positions: ski patrol member, ski lift operator, maintenance worker, instructor, kitchen worker, restaurant worker, marketing specialist, business administration specialist, front desk attendant, equipment specialist, emergency staff member, and manager. Each position will have different and specific access privileges on our system, and we also want to customize desktop setting for each position.

Resorts are organized into five departments: maintenance, restaurant, operations, hotel, and business administration.

Each resort is independently owned and managed, and each one could require the need to add applications that might uniquely change the directory schema. Also, resorts want to keep any external companies or other resort from changing user permissions for their employees. Resorts also do not need to have their internal domain replicated by means of our WAN line, and e-mail addresses need to be unique for each resort.

Each of the resorts currently has their own web sites, and each resort web site is registered with its own domain. DNS services for our top-level DNS domain are currently and will continue to be managed by an external web presence provider. Our internal-operations Active Directory will remain on the external DNS server. The resorts' web sites will include a variety of information related to each resort. There will be a link on each web site to allow members to update their records, which will take our members to the member web site hosted by granttechnologies.com.

Grant Resort Technology Keypoints

Preliminary Network Preparation Keypoints:

The following business factors influencing the Grant Resort Technologies business strategies will affect the design of Active Directory design in the following ways

- **Forests: Each resort must have independent control.**
- **Sites: Directory replication cannot be scheduled during times of peak usage.**
  All member logon requests must avoid using the WAN line.
- **Number of domains: Resort administrative control is divided among five departments.**
- **OU: It must be easy to move a member's user object from one resort to another resort.**
- **Security groups membership: There are many employee positions at each resort.**

Active Directory Design Components	Business Factors
Number of domains Forests Security groups membership OU Sites	Resort administrative control is divided among five departments. All member logon requests must avoid using the WAN line. There are many employee positions at each resort. It must be easy to move a member's user object from one resort to another resort. Directory replication cannot be scheduled during times of peak usage. Each resort must have independent control.

When deciding how the requirements of Grant Resort Technology members, resort employees and resort departments should be supported, you need to decide which properties are most appropriate to meet the requirements of each group. Using the shown technologies and groups, you should arrange them in the following way:

Resort employees: **intrasite replication**

Members: **intersite replication**

Resort Departments: **unique schema**
delegated administrative rights

Groups	Technology
Resort employees Members Resort departments	unique schema intrasite replication intersite replication delegated administrative rights

You should design the DNS, domain, and forest structure that meets the internal needs of the resorts by **creating a DNS zone named ad as a subdomain of the resort's existing Internet domain name** and **assigning this domain name to the Active Directory forest root**.

There will be a minimum of **27** Windows 2000 Server computers needed to host the domain controllers and global catalog servers for phase 1 of the implementation plan.

You should design the domain and forest structure for the members by **using granttechnologies.com for the forest root and single domain**.

Post-upgrade Network Design Keypoints:

The GRT business needs that you should implement through Group Policy objects are:

- **Configuring the desktop settings for resort employees**
- **Updating the software on the kiosks**

The business or technical factors that should influence the number of forests GRT should use are:

- **Each resort will want to be able to add applications that might uniquely change the directory scheme of internal operating domain.**
- **It will not be necessary for the employees of one resort to access information about employees of another resort.**
- **The resorts do not want GRT or any other resort to have any authority to change user permissions for their employees.**

The top-level organizational unit that you should choose that will support a resort's internal business requirements is **departments.**

The trust relationship that you should configure between the member domain and each resort domain to enable employees to be able to update member records is **a one-way trust, where member trusts resort**.

The two steps that you need to take to configure replication for Grant Resort Technology are:

- **Create intersite links on the member domain controllers that are located at each resort and at the San Jose IT center.**
- **Set the interval to 180 minutes. Set the schedule to 1:00 AM to 6:00 AM local time at each resort.**

The steps that you should perform to implement DNS services for one of the resorts are:

- **Install Microsoft DNS Server on two servers. Configure a subdomain of the resort's Internet domain.**
- **Use these servers for the businessconsultants.com zone that is integrated into AD**

There should be **7** forests created for phase one of GRT implementation plan.

The business or technical factor or factors that should influence your decision as to how many forests Grant Resort Technology should use are.

- **Both smart-card authentication and password authentication will be used for security.**
- **Each resort will want to be able to add applications that might uniquely change the Directory schema of its internal operating domain.**
- **The resorts do not want General Grant Resort Technology or any other resort to have any authority to change user permissions for their employees**
- **It will not be necessary for employees of one resort to access information about employees of another resort.**

Kree Corporation

Background:

The Kree Corporation is a manufacturer of silicon components used in consumer electronics. There are design teams located in six offices worldwide. Design teams collaborate to create, test, and modify the design of new and existing components. Collaboration between the teams requires creating, accessing, and modifying various files and file formats that are on the servers throughout the company.

Geography:

The headquarters for Kree Corporation is located in Albany, New York, and branch offices are located in San Jose, London, New Delhi, Bangkok and Melbourne. There are component designers working in all offices, and the San Jose and Bangkok offices are manufacturing facilities. The Albany and Sidney offices have 2,500 employees each, while each other office has 500 employees.

The six offices are located in one of the two regions defined as follows:

- Western Region
  - Albany, New York
  - San Jose, California
  - London, England

- Eastern Region
  - Melbourne, Australia
  - Bangkok, Thailand
  - New Delhi, India

Network Infrastructure:

The San Jose and Albany offices are connected by means of a 256-Kbps fractional T1 line, and the Albany and the Melbourne offices are connected by means of a 128-Kbps fractional T1 line. There are 64-Kbps fractional T1 lines connections between Albany and London, between London and New Delhi, between New Delhi and Bangkok and between Bangkok and Melbourne.

The Albany-London connection is heavily utilized during Albany's business hours, and the Melbourne-Bangkok connection is heavily utilized during Melbourne's business hours.

All locations have a 155-Mbps ATM backbone, and all client computers connect to their local backbone by means of a switched 10-Mbps or 100-Mbps Ethernet.

Business Plan and Requirements:

Chief Executive Officer (CEO):

The global components market is highly competitive, and our employees must be able to collaborate with each other 24 hours per day. Nothing must be allowed to interfere with this capability.

We anticipate a series of mergers, partnerships, and acquisitions over the next two years, and we need to be ready to assimilate these new entities into our organizational and managerial structure, and into our infrastructure. We have to be able to easily restructure our organization, administration, and online data to utilize of new resources as they become available. This must occur without interrupting the design and manufacturing processes. There are several parts of our current business that might be sold during the next one to two years.

Chief Information Officer (CIO):

Our organization will undergo many changes during the next few years. As we acquire new companies, we will be organizing entire divisions, assimilating unknown client and network operating systems and infrastructures, and adding large number of new users.

We have divided the responsibilities of all IT operations and IT infrastructure management between the Albany and Sidney offices. The Albany office will make final decisions regarding infrastructure design. The Sidney office is responsible for the eastern region, and the Albany office is responsible for the western region.

The division of control must not hinder the performance or availability of computer based services when accessing network resources. We must not have any computer down time our system. Our goal for the next 12 months is to have all services available at all times and for those services to start as quickly as possible.

Security Officer:

There has been a dramatic increase in attempts to breach our network security. We are unsure if these attempts are being made by individuals to simply test their skills, or if they are attempts at industrial espionage. We are not taking risks. Security has got to be one of the primary considerations when designing all operating systems and services.

We have begun to implement strict security procedures and policies at all facilities. The Eastern and Western regions will manage policies individually. The Eastern Region will have maximum password lifetimes of 30 days and minimum password length of four characters. The Western Region will have maximum password lifetimes of 45 days and minimum password length of six characters.

Network Operation Officer:

We need to delegate authority for password resets and the management of file and printer resources to our eight major departments: research and development, design, manufacturing, marketing, finance, sales, IT, and human resources. At each branch office, each department's IT staff should have the ability to manage the resources only within that one branch.

Chief Financial Officer (CFO):

We have and continue to work hard to associate the Kree Corporation's name with a highly recognizable and positive image. Despite the success of our online business, we might divest that segment of the business. It is possible that we will sell the name with a portion of the business, so we need to make sure that this sale will not effect internal operations. If we sell the e-commerce business the domain www.kree.com will be included as a part of the sale.

Existing IT Environment:

There are three Windows NT 4.0 domains at all locations. There is one account domain and two resource domains. Locations in the western region use Windows NT 4.0 DNS Server for name resolution, and the eastern region currently uses a UNIX-based DNS service that supports the use of SRV records. The eastern region servers do not support dynamic updates.

There are several Windows NT 4.0 computers at each facility.

Kree Corporation Practice Questions

Preliminary Network Preparation Keypoints:

There is a one-to-one relationship between sites and locations, and a domain is associated with only one location. Kree.com and west.kree.com will be managed in the Albany location, and the following domain hierarchy is being considered for the domain:

Kree.com
east.Kree.com
west.Kree.com
bangkok.east.Kree.com
newdelhi.east.Kree.com
albany.west.Kree.com
london.west.Kree.com
sanjose.west.Kree.com
melbourne.east.Kree.com

The server services at the Albany location should be designed in with **one schema operations master, one domain naming master, six domain controllers, two global catalog servers and three PDC emulators**.

A proposed design for Kree Corporation is shown below:

Servers at the San Jose Site	Servers at the Albany Site
sj1 west.Kree.com	alb1 west.Kree.com
sj2 west.Kree.com	alb2 west.Kree.com
sj3 west.Kree.com	alb3 west.Kree.com

The servers are named SJ1, SJ2, SJ3 and ALB1, ALB2 and ALB3. SJ3 and ALB3 are bridgehead servers. Given the possible replication steps below, when a new user is created on ALB1 the steps for the default replication of that user to every domain controller in the Albany and San Jose sites would be **1, 2, 4, 5, 9, 8, 7**.

Possible Replication Steps
1. Create the user.
2. ALB1 notifies its replication partner or partners.
3. ALB1 sends data to SJ3.
4. ALB2 and ALB3 begin pull replication from ALB1.
5. ALB3 notifies its replication partner or partners.
6. ALB3 sends data to SJ3.
7. SJ1 and SJ2 begin pull replication from SJ3.
8. SJ3 notifies its replication partner or partners.
9. SJ3 begins to pull replication from ALB3.

The business factors that should have the most influence on the design of Kree Corporation's OU hierarchy is **departments**.

The Kree Corporation business factor that necessitates a multiple domain Active Directory design is the **individual infrastructure management control at the Albany and Melbourne offices**.

The two Kree Corporation business factors should influence the Active Directory naming strategy are:

- **Organizational Unit hierarchy**
- **Possible sale of Kree Corporation name**

Post-upgrade Network Design Keypoints:

The Kree Corporation is considering using the domain names listed below in a design that uses only the default Windows 2000 Trusts. Given this table, the Kerberos referral path that is traversed when a user in albany.west.Kree.com accesses resources located in Melbourne.east.Kree.com is **4, 2, 1, 3, 7**.

Possible Domain Names
1. Kree.com
2. west.Kree.com
3. east.Kree.com
4. albany.west.Kree.com
5. london.west.Kree.com
6. sanjose.west.Kree.com
7. Melbourne.east.Kree.com
8. bangkok.east.Kree.com
9. newdehli.east.Kree.com

The Kree Corporation decides to enter into a joint venture with one of its vendors. A third company will be created by this venture that will require its own Internet presence. The system administration duties for the new company will be shared equally between the vendor and the Kree Corporation. The Kree Corporation and vender currently have separate Active Directory forests, and the modifications that should be made to Active Directory to support the joint venture requirements are **create a new forest for the new company** and **assign appropriate trusts between Kree's forest and the new forest**.

Force, Inc.

Windows 2000 Upgrade Project:

You have been asked to provide consulting, development and integration services for Force, Inc. This project will include the implementation of Windows 2000. Client computers that currently running Windows 95 will be upgraded to Windows 2000 Professional, and the domain controller environment will be fully upgraded to Windows 2000 Server.

Background:

Force, Inc. is a manufacturer and supplier of plastic containers to manufactures of personal grooming products. There are three offices in southern United States located in Atlanta and Flagstaff, and the company headquarters is in Houston. The following departments are in the Houston office:

- Quality control
- Maintenance
- Manufacturing
- Graphics
- Administration
- Human resources
- IT administration
- Manufacturing designs
- Purchasing
- Accounting
- Sales and marketing

In Flagstaff and Atlanta there are offices for these departments:

- IT administration
- Manufacturing
- Sales and marketing
- Maintenance
- Quality control

There are currently two eight-hour shifts for manufacturing and one shift for administrative and clerical purposes.

Problem Statement:

Chief Executive Officer (CEO):

We are not receiving benefits from IT administration equal to the money we spend on it. Our suppliers and customers want to connect to our network to be able access to information on inventory updates, pricing, and billing.

Many of our processes are currently paper based, and because of this we have all the associated problems related to paper handling and data entry. Our paper-based system also yields data that is not as current as we want it to be. We wish to automate and consolidate sites that employees access to retrieve and input information.

Chief Information Officer (CIO):

On our network, all account administration must currently be performed in Houston. And, other than account administration, there is no centralized management of our client computers. We have no Internet mail available. We delegate administration in our current Windows NT 4.0 domain structure through the use of several domains.

User accounts should be created at headquarters, and IT staff members at the Flagstaff and Atlanta locations should have the capability to reset passwords and modify accounts. However, neither the Flagstaff nor Atlanta IT staff should have full administrative control.

We have concerns that Microsoft Windows 95 does not offer enough security at the client computer level. The current Atlanta-Houston and Flagstaff-Houston WAN connections average 75 percent saturation during business hours, and all IT maintenance will be performed during non-business hours over a four-hour period. We attempt to schedule traffic during the evening hours whenever possible.

The cost of every improvement made to the IT infrastructure must be justified.

History:

The current Windows environment was most recently upgraded in early 1997 when it was upgraded to Windows NT 4.0 and Microsoft Windows 95 from NetWare 3.12 and Windows 3.1. All service packs have since been applied to Windows NT 4.0 as they have been released. The 1997 upgrade caused several connectivity, validation, and permissions problems, and because of this, some employees were not able to work. The problems experienced were associated with the consulting organization that performed the upgrade. Employees still remember the problems and often recall them when upgrades are suggested therefore the company is sensitive about the duration of downtime during the upgrades.

Existing IT Environment:

General:

Force Inc employs approximately 10,000 people, and the company uses approximately 5,000 computers. There are 3,750 computers in Houston, 750 in Atlanta and 500 in Flagstaff.

UNIX-based computers control the existing manufacturing environment, and there are currently four Windows NT 4.0 domains. There is a global account domain in Houston that controls all user accounts, and resource domains in Houston, Flagstaff and Atlanta.

Network Infrastructure:

There are 56-Kbps lines between Houston and Flagstaff and between Houston and Atlanta. There are concerns about the amount of available bandwidth but the IT administrators cannot justify upgrading the links at this time. Traffic is scheduled for evening hours whenever possible to distribute bandwidth. An SAP server, located in Houston is used for inventory management.

The Force.com domain and web site is registered and hosted by third party web servers, but it hosts no interactive web pages. There is an internal BIND DNS server to mange the UNIX environment at each location. The current UNIX DNS structure is self-contained and functions as its own root, and the Windows 2000 support staff needs to be able to easily gain access to the DNS supporting Windows 2000.

There is currently no connection to the Internet.

Client Computer Environment:

Manufacturing design employees use UNIX-based computers for design processes, but they use Windows-based computers for e-mail and web processing. The manufacturing department's computers use terminal-emulation to communicate with the system that controls the manufacturing processes.

Most employees' computers are running Windows 95, most of which run on Pentium 200-MHz MMX platforms that have 16 MB of RAM and 2.1-GB hard disks. Microsoft Office 97 is the standard office package, and department-specific applications are locally installed by administrators on-site.

There are multiple employees using each of the manufacturing department's computers, and the company wants profiles and documents to be available to each manufacturing department user at any of the computers in the manufacturing department.

IT Infrastructure:

The primary IT center in Houston performs IT management whenever possible. Most internal departments of Force, Inc. use unique software. Our technical support personnel require specific expertise to be able to support to each of these departments, therefore each department has its own technical support staff. IT policy for each department is defined and managed in Houston, and most of the technical support staff from the various departments are located in Houston. Most of the local office technical support staff report directly to departmental IT managers in Houston. There will be no need to delegate authority to support staff at the local offices to perform basic administration.

Security:

In the master account domain, global groups are currently used to group users for resource access. The IT administrators in Houston make the decisions as to how users are grouped. The local IT administrators manage local resource access by creating local groups on the servers located at the remote offices. Administrators grant users access rights by adding global groups to local groups, but local resource domain administrators are not granted administrator rights for the Houston domain.

Group Policy Goals:

The plan is to manage group policy with both company-wide policy and departmental policy. Group policy will initially be designed to define logon scripts customized for each department at each location, redirect folders, define the desktop settings, to minimize the logon time, and to make available department-specific software. Group policy objects will not be filtered by security groups. The only exception to this is that most group policies will not apply to technical support staff.

Force, Inc. Keypoints

Preliminary Network Preparation Keypoints:

The upgrade path that you should use for Force, Inc should be:

- **Upgrade the Houston account domain.**
- **Use this domain as the root domain.**
- **Separately upgrade the three Windows NT 4.0 domains to Windows 2000.**
- **Consolidate these three domains into one domain.**

The Windows 2000 site design should you implement for Force, Inc is to **continue using the existing WAN lines** and to **create one site each for Houston, Atlanta and Flagstaff**.

DNS should be designed to support Windows 2000 for Force, Inc by **installing Microsoft DNS server on Windows 2000 computers, and integrate DNS into Active Directory**.

To implement Windows 2000 to minimize the impact of replication on WAN traffic for Force, Inc. you should **use IP site links for replication**, and **optimize the replication schedule**.

A design must be created that will allow permissions to be granted to a set of resources on three servers in the Houston office. To grant these permissions to users throughout the entire company after the upgrade you should **create a domain local group in the domain in which the resources exist, and grant this group access to the resources**. You should then **create one global group for the domain or domains, and add the members who need to gain access to the resources**. Finally, you should **add the global groups to the domain local group**.

There should be **one domain for the entire company** at the end of upgrade project.

The implementation of Group Policy for the sales department of Force, Inc. should be designed by **creating domain-level Group Policy objects (GPOs) for company-wide policies**. Then **set sales-specific policies in the top-level sales organizational unit**. And finally **use site-level GPOs to set location-specific policies as necessary**.

Post-upgrade Network Design Keypoints:

The goal that is accomplished as a direct result of the upgrade to Windows 2000 Active Directory is **increased control and increased capability to standardize applications and configurations throughout the company.**

The sites and site links for Force, Inc. should be designed by **creating one site each for Atlanta, Houston and Flagstaff**. **Then create IP site links between Atlanta and Houston and between Houston and Flagstaff**. Finally, **schedule the links to replicate between Atlanta and Houston and between Houston and Flagstaff from 2:00 a.m. to 4:00 a.m., Houston local time**.

You should locate the server services for Windows 2000 as follows: **in Houston, locate a schema operations master, a domain naming master, an infrastructure operations master, a RID master, a PDC emulator and a global catalog**, and **locate one global catalog in Atlanta and one global catalog in Flagstaff**.

A database administrator in the human resources department attempts to upgrade SAP applications and fails. The applications will integrate with active directory and create new classes in installation phase. The cause of this failure is that **the administrator trying to install application is not in the Schema Administrators group**.

PowerStaff Corporation

Background:

Overview:

The PowerStaff Corporation was founded in 1992 as an employment agency providing temporary employees to media companies. PowerStaff specializes in freelance writers, reporters and graphic artists.

In 1997 the PowerStaff Corporation widened its scope to include a broader range of workers to support a broader range of companies. PowerStaff added information workers (IWs) as part of the attempt to broaden its skill base and to appeal to more companies. PowerStaff Corporation now has two goals, to provide top-notch service to customers seeking temporary employees, and to become a leader in supporting the needs of highly qualified freelance IWs.

Information Workers (IWs) Service:

PowerStaff Corporation recruits different types of temporary employees worldwide. These employees include consultants, freelance workers and independent contractors. These individuals are referred to as information workers (IWs), and PowerStaff provides their IWs with personal and GroupWare tools such as e-mail, discussion groups, and scheduling resources to increase their productivity. PowerStaff also evaluates and markets their skills, and helps them work with the employers by facilitating information exchange between all three parties. Employers who have network connectivity with PowerStaff can have special access to shared resources. This special access allows IWs to easily collaborate with other employees of companies currently employing them.

Corporate Customer Services:

The PowerStaff Corporation provides a group of leading technology and services companies with temporary employees. PowerStaff allows easy access to companies its online list of workers and provides an interface that facilitates finding the right worker for the job. In addition, PowerStaff facilitates the initiation of contract processes for its corporate customers and collaboration between permanent customer employees and its temporary employees.

Organization:

There are approximately 300 people currently employed by the PowerStaff Corporation on a permanent, full-time basis. These full-time employees are evenly distributed among its four offices. These offices are located in Albany, Chicago, Atlanta and San Jose. The company headquarters is the Chicago office.

PowerStaff Corporation has the following departments:

- Information technology (IT)
- Human resources
- Business Administration
- Marketing
- Consulting

The consulting department supplies communication and management services to corporate customers. In this department there are experts assigned to support the IW individual occupational roles. Experts in the consulting department are responsible for hiring the IWs, evaluating their skills, managing security clearances, and monitoring assignments with corporate customers.

The PowerStaff Corporation organizes information into the following groups

- Employee
- Recruiting,
- IW
- Accounting
- Corporate customers
- Projects.

PowerStaff currently provides services to over 25,000 IWs with approximately 20 percent currently employed in temporary positions.

PowerStaff Corporation will increase their full time employees to 450 over the next two years. PowerStaff also wishes to double the number of IWs and increase the percentage of IWs that are actively employed over this same period.

Existing IT Environment:

The internal WAN consists of 1.544-Mbps lines connecting the headquarters in Chicago to the Albany, Atlanta and San Jose offices. These connections average approximately 35% utilization. The Internet connection is in Chicago, and a third party hosts the company's external web site.

The PowerStaff Corporation's network consists of one master domain and a separate resource domain for each of the company's offices. The master domain, named PS_Master, contains all employee user accounts and has its PDC and a BDC in Chicago and BDCs in Albany, San Jose and Atlanta. The PDCs and BDCs for the four office resource domains are located at their associated offices. There is also a second BDC for each location in the Chicago office. The four office resource domains are named CH_RES, AL_RES, SJ_RES and AT_RES. The PS_MASTER and SJ_RES PDCs also run WINS, but there are no DNS or DHCP services currently running. A UNIX POP3 server currently hosts the e-mail service for the IWs.

Proposed Corporate-Customer Connectivity:

50 percent of PowerStaff's IWs are currently employed at 20 large companies. PowerStaff has at least one full-time employee who coordinates the IWs services permanently located at ten of these companies offices. There are two corporate customers willing to configure trust relationships between the PowerStaff Corporation WAN and their own WANs. When this is accomplished, approved IWs will be able to place files on the PowerStaff Corporation servers and employees of these two corporate customers will be able have convenient access to these.

Project Goals:

Information Worker Management:

The PowerStaff IT system must have tools for estimating costs, scheduling, searching, and deploying resources to enable its corporate customers to be able to directly manage and acquire IWs.

Establishing Trust:

Many of the services that IWs will be providing to PowerStaff's corporate customers will be done remotely, and establishing trust could prove to be difficult. To solve this problem, PowerStaff Corporation will use videoconferencing whenever possible by providing membership access to national videoconference centers. The company will also support videoconferencing from IW home offices when bandwidth is available. In a further attempt to increase trust, IWs will be granted higher security clearances when they are enrolled in the Virtual Office service.

Information Worker Virtual Office:

Web-based administrative tools such as time sheet reporting, invoicing, and payroll services are currently provided by PowerStaff. There are also deluxe services offered to the IWs:

- **Standard-** provides e-mail, 5 MB of file storage, and access to job database. This service is free to the IW.
- **Deluxe**- this level includes all standard services, but also provides group-rate insurance plans and stock options. IWs pay a monthly fee for this service.

A further level of premium service will be offered named Virtual Office. PowerStaff will require an additional charge from the IWs to provide this service level. The Virtual Office service package provides 75 MB of file storage, personal scheduling tools, project team rooms, contact management, access to discussion groups, and links to personal portfolios. To support this functionality, PowerStaff intends to use Public Key Infrastructure, Microsoft Exchange 2000, and Microsoft Outlook 2000.

Each IW is grouped in one of the following occupational roles:

- Information technology (IT)
- Media creation
- Management
- Business
- Sales
- Training

IWs will also be classified into levels of security clearance to support the corporate customer's need for confidentiality. IWs can attain higher levels of security clearance given their work history and credentials.

Project Requirements:

All the client computers of the permanent employees of PowerStaff will be upgraded to Windows 2000, and the company will hire external workers to perform the upgrade. PowerStaff will also consolidate and upgrade the existing Windows NT domains, implement Active Directory, and upgrade Microsoft Exchange 5.5 to Exchange 2000 during this process.

PowerStaff offices currently operate like small independent businesses, but most information sharing is only performed inside each department regardless of the location. Support of this organizational system will require the restructuring of the administration of user account resources.

PowerStaff requires that the root of its internal forest namespace to be a subdomain of its public domain, named powerstaff.com to facilitate security management. For fault tolerance, at least two servers host domain controllers in each domain.

All employees will need to be able to search the entire global catalog containing employees and IWs, but permission changes made to IW resources should not need to be replicated to other PowerStaff offices.

The plan is to initially import all 20,000 IWs into Active Directory as contacts. As IWs subscribe to the Virtual Office service they will be entered into Active Directory as users, migrated to Exchange 2000, and supplied with Microsoft Outlook 2000. Virtual Office IWs will access PowerStaff's internal network by means of a VPN through the Chicago office's Internet connection. Virtual Office IWs will also require greater security in their password policies, including longer passwords, password aging, and PKI certificates to support the anticipated high security levels. Smart cards and consistent logon procedures must also be supported regardless of domain. Users will use username@powerstaff.com for authentication.

PowerStaff also wishes to create extranet connections and trusts, and will initially configure the extranet connections and trust with two corporate customers. IWs with appropriate credentials will be able to store documents on PowerStaff servers and corporate customer employees will be able to easily access these documents. There are Active Directory domains already installed on the two corporate customers who are configuring trust relations with the PowerStaff Corporation WAN. These corporate

users will want to be able to view appropriate PowerStaff Corporation file shares through their own global catalogs, but do not want IW user accounts to appear on any of the access control lists of their forest.

Chief Information Officer (CIO) Interview:

There are many creative individuals in the IT field, and many of them will install the services just to see how they work. This causes problems because we often have far more services running than we need. I need to be able to regain top-level administrative control, and I also have to be able to delegate administrative tasks. I would like to maintain the simplicity of our initial design so I want to use only the services that are absolutely necessary. There must be tight controls on the quality of videoconferencing provided to users. Domain replication must be controlled, and employee logon processes should not require the WAN connection to maintain integrity despite the loss of a WAN link to remote locations,.

I need the ability to control all schema changes, site policies, and additions of new domains. I also require the ability to assign selected individuals to administer employee information worker IW accounts and resources to have full domain rights to these objects.

IT support staff at each location will be responsible for the daily administration of users, resources, and permissions. The new design should be structured so that this work is delegated to individuals in each department.

PowerStaff Corporation Practice Questions

Preliminary Network Preparation Keypoints:

The requirements that should affect your domain migration strategy are **maintaining employee accounts and passwords**.

The tasks you must perform to implement the required Windows 2000 designs for PowerStaff Corporation are:

- **Create two explicit one-way trust relationships,** and **configure these trusts so that PowerStaff Corporation IWs domain trusts a domain in each of the two corporate customer forests.**
- **Request that PowerStaff Corporation file share objects be added to the corporate customers' global catalogs.**
- **Install domain controllers in Albany, Atlanta and San Jose.**
- **Configure DNS and global catalog services in Albany, Atlanta and San Jose.**
- **Integrate DNS into Active Directory.**
- **Create sites and intersite replication schedules for Albany, Atlanta, and San Jose.**

Post-upgrade Network Design Keypoints:

The steps taken to design DNS infrastructure and Active Directory domains are:

- **Create a forest root named corp.powerstaff.com**
- **Create a subzone for any necessary child domains of the corp.PowerStaff.com tree**

Given the following task list, to migrate PowerStaff Corporation's existing Windows NT domains into Active Directory you should use a migration plan that has tasks in this order: 4, 2, 3.

- **Upgrade the PS_MASTER PDC to Windows 2000, creating a Windows 2000 domain containing all employee user accounts. Attach this domain to the root domain.**
- **Upgrade all of the BDCs of each Windows NT 4.0 domain to Windows 2000 domain controllers.**
- **Upgrade the Windows NT 4.0 resource domain PDCs to Windows 2000, designating each as a child domain of the employee domain. Then create new OUs in the employee domain. Move the computer security groups and other security groups into the new OUs. Finally, decommission the child domains.**

Upgrading to Microsoft Exchange 2000 from Exchange 5.5 will require a modification in the PowerStaff's schema.

There should be **one forest and three domains** created for PowerStaff.

There should be **4** sites created for PowerStaff Corporation.

The Active Directory will be affected by factors influencing business strategies of PowerStaff are:

Site structure:	**Existing WAN connectivity and utilization rates**
Domain structure:	**Unique authentication requirements of IWs**
OU structure:	**Division of PowerStaff Corporation into departments**
	Classification of IWs into occupational roles and administration of IWs by PowerStaff Corporation employees
Forest structure:	**Schema modification policy**
Explicit trust:	**Availability of IW shares from the corporate customer domains**

Index