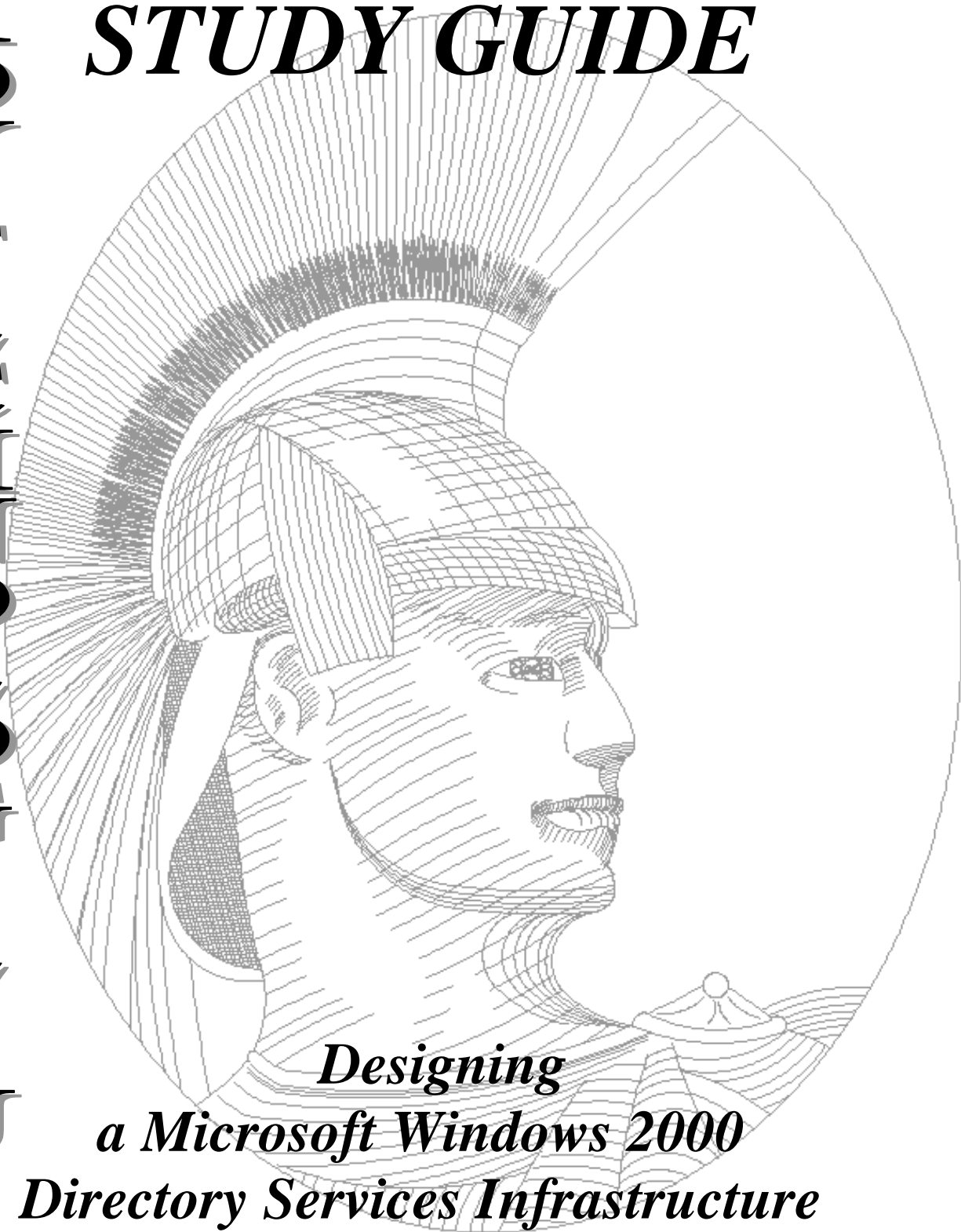


FOR THE  
TECHNICAL  
SPECIALIST

# *MCSE STUDY GUIDE*



*Designing  
a Microsoft Windows 2000  
Directory Services Infrastructure  
Exam 70-219*

Edition 1

## Congratulations!!

You have purchased a ***Troy Technologies USA*** Study Guide.

This study guide is a selection of questions and answers similar to the ones you will find on the official Designing a Microsoft Windows 2000 Directory Services Infrastructure MCSE exam. Study and memorize the following concepts, questions and answers for approximately 10 to 12 hours and you will be prepared to take the exams. We guarantee it!

Remember, average study time is 10 to 12 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:

Troy Technologies USA  
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.

*This material is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this material, or any portion thereof, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.*

© Copyright 2000 Troy Technologies USA. All Rights Reserved.  
<http://www.troytec.com>

## Table of Contents

Analyzing Business Requirements .....	1
ANALYSIS OF THE BUSINESS MODEL .....	1
ANALYSIS OF THE COMPANY MODEL AND THE GEOGRAPHICAL SCOPE ....	1
ANALYSIS OF COMPANY PROCESSES .....	2
Information Flow.....	2
Communication Flow .....	2
Service and Product Life Cycles .....	2
Decision-Making Process .....	2
ANALYSIS OF THE ORGANIZATIONAL STRUCTURE .....	2
Management Model.....	2
Company Organization.....	2
Vendor, Partner and Customer Relationships .....	3
Acquisition Plans.....	3
FACTORS INFLUENCING COMPANY STRATEGIES .....	3
Company Priorities .....	3
Projected Growth and Growth Strategy .....	3
Relevant Laws and Regulations .....	3
Identifying Tolerance for Risk .....	3
Risk Identification .....	4
Risk Analysis.....	4
Risk Action Planning.....	4
Risk Tracking .....	4
Risk Control .....	4
Identifying Total Cost of Operations.....	4
ANALYSIS OF IT MANAGEMENT STRUCTURE .....	4
Administration Type.....	5
Funding Model .....	5
Outsourcing .....	5
Decision-making process.....	5
Change Management.....	6
Analyzing Technical Requirements .....	6
EVALUATING THE EXISTING AND PLANNED TECHNICAL ENVIRONMENT..	6
Analyzing Company Size and User and Resource Distribution.....	7
Assessing Available Connectivity and Bandwidth.....	7
Performance Requirements .....	7
Analyzing Data and System Access Patterns .....	7
Analyzing Network Roles and Responsibilities .....	8
Analyzing Security Considerations .....	8
ANALYZING THE IMPACT OF ACTIVE DIRECTORY .....	8
Assessing Existing Systems and Applications .....	8
Identifying Upgrades and Rollouts.....	8
Analyzing the Technical Support Structure .....	9
Analyzing Network and Systems Management .....	9

ANALYZING REQUIREMENTS FOR CLIENT COMPUTER DESKTOP MANAGEMENT .....	9
Analyzing End-User Needs .....	9
Identifying Technical Support Needs .....	9
Establishing the Required Client Computer Environment .....	9
Designing a Directory Service Architecture.....	10
AD Database Overview .....	10
Forest and Trees .....	10
Sites .....	10
Dynamic Domain Name System (DDNS).....	10
Organizational Units (OUs).....	11
Global Catalog.....	11
Domain Controllers .....	11
Replication.....	11
Sites .....	12
Site Links.....	12
Site Link Bridge .....	12
DESIGNING AN ACTIVE DIRECTORY FOREST AND DOMAIN STRUCTURE..	12
Designing a Forest and Schema Structure.....	12
Designing a Domain Structure .....	12
DESIGNING AN ACTIVE DIRECTORY NAMING STRATEGY.....	13
Establishing the Scope of AD.....	13
Designing the Namespace .....	13
Planning DNS Strategy.....	13
DESIGNING AND PLANNING THE STRUCTURE OF ORGANIZATIONAL UNITS .....	13
Developing an OU Delegation Plan .....	13
Planning Group Policy Object Management.....	13
Creating a Group Policy Object (GPO).....	14
Linking an Existing GPO .....	14
Delegating Administrative Control of Group Policy.....	15
Modifying Group Policy Inheritance.....	15
Exceptions to Inheritance Order .....	15
Filtering Group Policy Settings by Associating Security Groups to GPOs .....	15
Removing and Deleting GPOs .....	15
Managing and Troubleshooting User Environments by Using Group Policy.....	15
PLANNING FOR THE COEXISTENCE OF ACTIVE DIRECTORY .....	16
DESIGNING AN ACTIVE DIRECTORY SITE TOPOLOGY .....	16
Designing a Replication Strategy .....	16
Managing Intrasite Replication .....	16
Defining Site Boundaries .....	17
DESIGNING A SCHEMA MODIFICATION POLICY .....	17
DESIGNING AN ACTIVE DIRECTORY IMPLEMENTATION PLAN.....	17
Designing Service Locations.....	17
DESIGNING THE PLACEMENT OF OPERATIONS MASTERS .....	17
DESIGNING THE PLACEMENT OF GLOBAL CATALOG SERVERS .....	18

Creating Global Catalog Servers.....	18
DESIGNING THE PLACEMENT OF DOMAIN CONTROLLERS .....	18
DESIGNING THE PLACEMENT OF DNS SERVERS .....	19
Interoperability with Existing DNS.....	19
Configuring Zones for Dynamic DNS (DDNS) Updates.....	19
Managing Replication of DNS Data.....	19

## **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 organiza-

tional 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 limitations. 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 obtained 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. troytec.com and support.troytec.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.troytec.com, marketing.troytec.com, and troytec.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 troytec.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 through 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 troytec.com. These domains can contain child domains which are split into zones, support.troytec.com, and shipping.troytec.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 your 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 settings 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 Policies 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**

Troy Research

### **Windows 2000 Upgrade Project:**

Your company is asked to provide consulting, development and integration services for a company named Troy Research. As a part of this project you will implement Windows 2000. All client computers that currently run Windows will be upgraded to Windows 2000 Professional. Wherever possible, the Windows NT 4.0 domain controller environment will be fully upgraded to Windows 2000 Server.

### **Background:**

Troy Research is a military research company that operates from several locations in the United States. Most of the company's business comes from the contracts from the United States government and military. Its headquarters and primary IT center is in Washington, D.C. The company is distributed as follows:

- Research Facilities
  - Boston, Massachusetts
  - Denver, Colorado
  - San Diego, California
  - San Francisco, California
  - Seattle, Washington
  - St. Petersburg, Florida
  - Washington, D.C.

The Denver, San Diego, San Francisco and Seattle facilities were originally a separate company named Parelli Aerospace. These facilities became a part of Troy Research when they were purchased in 1997. These facilities still use the Parelli Aerospace name and Parelli Aerospace still maintains its identity as a separate company. Troy Research is likely to acquire another company in the near future.

### **Problem Statement:**

#### **Chief Executive Officer (CEO):**

Because we are primarily a military research contractor working on a variety of classified projects, our primary concern is security. We purchased Parelli Aerospace in 1997, but in many respects it still operates as a separate company. We are attempting to eliminate duplicate work within the two companies as much as possible. We are also in the process of developing common operating practices.

For purposes of shared research, we allow government and military customers to access some of our data.

When we bought Parelli Aerospace we needed to restructure our entire security network structure. We need to be able to support our growth plans without needing to perform this type of restructuring again.

#### **Chief Information Officer (CIO):**

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

Rather than built more than one directory service, we want an integrated directory service. To work towards accomplishing the goal, we will be migrating Microsoft Exchange Server 5.5 to Exchange 2000 Server.

All account administration currently needs to be performed from our IT centers. We want to remove this limitation. We also want a security infrastructure that will not be need to be restructured when the accounts database reaches 40 MB.

Our current arrangement of trust relationship is cumbersome to manage. The current Windows NE 4.0 domain structure requires several domains for delegation of administration. We eventually want to have a global IT facility that uses the common software, standards, and procedures. The consolidation will begin during the Windows 2000 upgrade but we do not expect to complete it during the upgrade. We want the IT facilities to be controlled from one location as necessary. However, we also want to be able to delegate certain tasks without necessarily needing to create domains for them.

We are concerned that MS Windows 95 and Windows 98 do not offer security at the client computer level. We want to increase our control and continue to standardize our client computers and applications in all departments.

We want to standardize our security and management environment throughout the company as much as possible.

We must minimize the disruption caused by Windows 2000 upgrade, and the upgrade must not compromise our security.

#### **History:**

Troy Research has a diverse server environment. The company uses mainframe, UNIX, Novell, Macintosh, Banyan VINES and Microsoft servers.

The current Windows NT domain structure was configured in 1997, after the purchase of Parelli Aerospace, in an attempt to integrate the IT structures of the two companies. The network based on Windows NT was configured as a coexisting server structure, and mi-

gration and interoperability were gradually implemented. Since then, all service packs up to Service Pack 7 have been applied to Windows NT 4.0. The goal of this migration is to finally remove all of the remaining Banyan VINES and Novell servers.

### **Existing IT Environment:**

#### **General:**

The Troy Research uses 25,000 personal computers.

The distribution of users is shown below:

Boston	2,900
Denver	4,200
San Diego	1,900
San Francisco	3,600
Seattle	2,400
St. Petersburg	2,600
Washington, D.C.	7,400

There are currently two Windows NT account domains. All user accounts are in these domains. There is one resource domain in each of the seven geographic locations. There are account domains in Washington, D.C., and San Francisco. BDCs are distributed throughout the company as needed. At the Washington, D.C., location, there are two domain controllers running custom applications that will not run on Windows 2000. During the upgrade process, these domain controllers will remain on computers that run Windows NT Server 4.0. These domain controllers will be migrated at a later date.

#### **Network Infrastructure:**

There is a 44.736-Mbps line from San Francisco to the primary IT center in Washington, D.C. This line is used primarily for business applications. The 44.736-Mbps line has an average available bandwidth of 35 percent. There are 1.544-Mbps lines from Washington, D.C., to Denver, Boston, St. Petersburg, Seattle and San Diego. There are also 1.544-Mbps lines from San Francisco to San Diego, Denver and Seattle. The WAN links will be upgraded if more bandwidth is needed.

Each location has one internal DNS server to manage the current UNIX environment. The current internal implementation of DNS does not support SRV records, dynamic update, Unicode characters, or incremental zone transfer. The IT staff members who currently maintain DNS servers manage both the UNIX environment and Windows NT Server environment. The external DNS systems for both the Troy Research Web site and the Parelli Aerospace Web site are currently hosted on third-party ISP servers. The DNS modifications required for Windows 2000 will be designed to use the existing internal DNS structure.

## **IT Structure:**

The primary IT center is in Washington, D.C. There is also a major IT center in San Francisco. In many ways, the San Francisco research facility operates as an independent business unit. Since 1997, the IT department has been creating an increasingly centralized IT structure. All account management is performed in Washington, D.C., and San Francisco. All Windows 2000 operations masters will remain in their default locations. The departments that must be supported by the IT infrastructure include the following:

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

Policies and application specifications are defined at the Washington, D.C., and San Francisco IT centers. These two locations also provide telephone support for each department. Additionally, there is an IT department at each geographic location. These local IT departments report directly to the global technical support center. At the local offices, the IT staff is divided by departments and departmental responsibilities.

## **Security:**

Currently, the two domains have different security policies for password length and complexity, and for account lockout. These policies will not be changed after the Windows 2000 upgrade project is completed. Accounts will be created at the Washington, D.C., and San Francisco facilities. The rights for resetting passwords and changing attributes will be delegated to local IT administrators.

IT administrators give these users rights by adding global groups to local groups. There will be four levels of administrators for day-to-day operations:

- Enterprise administrators will be a small group contained in a separate top-level domain to manage the entire organization.
- Domain administrators will be granted rights to the entire domain.
- Branch administrators will be granted rights for operations at the physical locations.

- Departmental administrators will have localized rights based on their specific roles.

The departmental and branch administrators of resource domains are not granted administrative rights for the corresponding account domains.

**Group Policy Goals:**

Group Policy will be centrally managed from Washington, D.C., as much as possible. Initially, Group Policy will be designed to redirect folders to minimize logon time, to define logon scripts, to set security, and to allow specific software to be made available for installation in departments where users have the ability to install software.

## Troy Research Practice Questions

### 1. Which upgrade plan should you use for Troy Research?

*A: Create a root domain.*

*Upgrade the two account domains to Windows 2000, upgrade the resource domains, and then consolidate the resource domains into the account domains.*

### 2. You need to design the group policy hierarchy that should be applied to a user in the human resources department for technical staff at the Boston research facility. In which order should you apply the Group Policy objects (GPOs)?

*A: Boston site GPO, domain GPO, Boston OU GPO, human resources GPO.*

### 3. How should you implement the administration of group policy?

*A: Enable 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.*

*Enable departmental administrators at each location to edit GPOs that apply to their departmental OUs.*

### 4. You must decide how many domains to create for Troy Research. What is the most important factor that you should consider when deciding whether to create more than one domain?

*A: The requirement that different companies have different account lockout policies.*

### 5. You upgrade the Troy Research client computers and domain controllers to Windows 2000 as planned. You must now choose the locations for the server services. Move each service to the appropriate location or locations. (Use all the server services. You might need to reuse server services)

North American Troy Research Locations	Server Services
Washington, D.C. Boston San Francisco	global catalog DNS RID master schema operations master infrastructure operations master PDC emulator domain naming master

*A: Washington, D.C.; RID master, schema operations master, infrastructure operation master, domain naming master, PDC emulator, global catalog. Boston; DNS.*

*San Francisco; global catalog, PDC emulator, RID master, infrastructure operations master.*

- 6. You need to grant permissions to a set of resources that are managed on three domain controllers the Washington, D.C., facility. You need to grant these permissions to users at all facilities. What should you do?**

*A: Create a domain local group in the local domain, and grant this group access to the resources. Create one global group in the appropriate domain or domains, and add to this group the users who need access to the resources. Add the global groups to domain local group.*

- 7. Which change must you make to DNS to prepare for the implementation of Windows 2000?**

*A: Provide DNS services that will support SRV records.*

- 8. How should you implement DNS naming strategy for Troy Research?**

*A: Upgrade the existing DNS infrastructure.  
Use three domains named troyresearch.com, corp.troyresearch.com, and parelli-aerospace.troyresearch.com.*

- 9. How should you design the DNS for Troy Research?**

*A: Upgrade the existing UNIX DNS service.  
On this service, configure the zones required for Windows 2000.*



## Highabove Toys

### **Background:**

Highabove Toys is a medium-sized manufacturer of corporate marketing products. The company designs personalized clothing, glasses, hats, and many other marketing products. It specializes in manufacturing unique items for large companies.

The company is acquiring one of its clothing suppliers. The supplier is named Worldwide Importers. The supplier is well known and has an Internet presence on its own domain. This domain is named [worldwideimporters.com](http://worldwideimporters.com). Worldwide Importers will operate independently of Highabove Toys.

### **Problem Statement:**

Highabove Toys reports that there is too many IT administrators in the domain. Main-frame administrators with minimal experience have administrator rights to the domain. The company wants to decrease technical support cost by performing all technical support at an IT center in Detroit.

### **Organization:**

#### **Headquarters:**

Highabove Toys headquarters is located in Detroit. There are two separate locations in Detroit, one for IT, one for the corporate offices. The IT center has 100 employees and the corporate offices have 2000 employees.

#### **Manufacturing Facilities:**

The company employs 20,000 people in nine manufacturing facilities in the United States and in two facilities in Canada. Of these 20,000 employees, 8,000 use computers. Manufacturing facilities are also being built in Europe and Mexico.

### **Geography:**

The company is divided among the following regions:

#### **EAST – 3,000 users:**

- Boston, Massachusetts - regional headquarters
- New York, New York
- Pittsburgh, Pennsylvania

#### **MIDWEST – 3,000 users:**

- Chicago, Illinois – regional headquarters
- Cincinnati, Ohio

- Cleveland, Ohio

**WEST - 2,000 users:**

- Oklahoma City, Oklahoma - regional headquarters
- Los Angeles, Nevada
- San Francisco, California

**CANADA – 1,000 users:**

- Montreal, Quebec
- Toronto, Ontario - regional headquarters

The Montreal office will be permanently closed in near future. Many of the users from this office will be transferred to Toronto. Although the Montreal office is scheduled to close during the Windows 2000 implementation, it might not close until after the implementation is complete.

Highabove Toys is opening offices in Europe. A sales office was recently opened in Frankfurt, Germany. Manufacturing facilities are also being built in Mexico. These facilities can be used by all the sales regions. The company is also planning to open manufacturing facilities in Europe.

**Existing IT Environment:**

**WAN:**

Pittsburgh and New York 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 Cleveland connect to Chicago by means of a 56-Kbps line.

Chicago connects to IT center by means of a 1.544-Mbps line.

San Francisco and Las Vegas connect to Oklahoma City by means of a 56-Kbps line.

Oklahoma City 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.

Detroit 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 of the desktop client computers run Windows NT Workstation 4.0. The portable computers run either Microsoft Windows 95 or Windows 98.

**Network:**

There are three Windows NT 4.0 domains; HANA, HAEU and HAENG. All locations in Canada, Mexico, and the United States are in HANA, Frankfurt is in HAEU. There is a two-way trust between HANA and HAEU. All locations use Windows NT Server 4.0 for DHCP, WINS, and DNS. Each location also has a BDC and a separate application server. However, Frankfurt has a PDC and a BDC for only HAEU domain. There is not a HAEU BDC in North America.

Because of the security concerns, users in the Engineering department have their own domain. This domain is named HAENG. The Engineering department also provides administration for the domain. They administer all the user accounts and resources. HANA trusts the HAENG domain.

On the HANA domain, passwords expire after 45 days. All the HAEU domain, passwords expire after 30 days.

Each manufacturing facility currently uses a mainframe computer to process orders and quotes that must be processed quickly. The mainframe computer uses only TCP/IP.

**Network Roles:**

Each of the regional headquarters has a technical support staff. The office in Mexico is managed from the IT center in Detroit. The locations without the network administrators have mainframe administrators. These mainframe administrators also help with domain administration. The mainframe administrators respond to support calls for basic issues and add and remove user accounts. However, their knowledge is usually limited to basic account administration.

**Envisioned IT Environment:****WAN:**

Before the Windows 2000 implementation, the 56-Kbps connection will be replaced with a 1.544-Mbps line.

However, there is no plan to upgrade the 56-Kbps connection to Canada and Mexico.

Worldwide Importers will connect to the Highabove Toys by means of a 256-Kbps line. Highabove Toys wants to continue using the existing IT administrative structure and security policies for Europe and North America.

**Network Roles:**

Highabove Toys will create two new technical support centers: a North American support center and European support center. Each region will have a small IT staff that will be responsible for basic support such as password resets and account lockout resets. Tasks that require higher levels of administrative access or more advanced skills will be performed by the European or North American support centers. Support for Europe that takes place after European business hours will be performed by the North American support center.

Each support center will also be responsible for granting the staff at each region access to resources as needed.

However, the North American and European support centers want complete control of their own resources. The engineering department will remove its domain during the Windows 2000 implementation. The users and resources in this department will be integrated into Active Directory as normal users and resources.

**Software:**

A software development company is in the process of creating human resources software for Highabove Toys. This software will be integrated with Active Directory, and it will enable employee management for all of Highabove Toys. This software will add additional attributes to user objects.

Worldwide Importers is also developing similar software. Both software solutions will be implemented independently.

**Internet:**

Highabove Toys has registered highabovetoys.com, Worldwide Importers have registered as WideWorldImporters.com.

**Client Computers:**

Client Computers will be upgraded to Windows 2000 Professional.

**Policies:**

Each region should be created in Active Directory as a separate entity. Group Policy can vary among regions and locations. Technical support staff in each region need to have the ability to change policies at each location.

## Highabove Toys Practice Questions

- You must decide how your Active Directory will be affected by factors that influence Highabove Toys business strategies. Move each business factor to the Active Directory design component that it most influences. (Use all the business factors. Use business factors only once.)**

Active Directory Design Components	Business Factors
Site design Domain design OU design Forest design	Manufacturing facilities are being built in Germany. Highabove Toys acquiring Worldwide importers. 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.

- A: 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: Highabove Toys is acquiring Wide World Importers.*
- Domain design: The European offices will operate independently of the North American offices.*

- You must design the site topology for the Highabove Toys. Which factors should have the most influence on your design? (Choose all that apply.)**

- A: Number of locations.  
 Available WAN bandwidth*

- You must integrate Europe and North America in Active Directory. What should you do?**

- A: Create one forest for Highabove Toys.  
 Create one domain for Europe and one domain for North America.*

- After the Windows 2000 implementation is complete, which domain name or names should you use in the internal DNS for Highabove Toys? (Choose all that apply.)**

- A: europe.highabovetoys.com  
 northamerica.highabovetoys.com*

- Which server roles should you implement for Highabove Toys?**

*A: One schema operations master, one domain naming master, two RID masters, two PDC emulators, and two infrastructure operations masters.*

- 6. Engineering users want to be able to continue to administer their own resources after the Windows 2000 implementation. What should you do?**

*A: Create a separate Organizational Unit for the engineering department.  
Locate this OU in the North America domain.  
Grant the engineering department complete administrative control of its Organizational Unit.  
Move computer and user objects into the OU.*

- 7. You must decide whether to place Europe in Active Directory as a domain or as an Organizational Unit. Which factors should most influence your decision?**

*A: The current and proposed IT administrative structures and security policies in Europe.*

- 8. After the Montreal office is permanently closed, how many sites should you use for the highabovetoys.com domain tree?**

*A: 14*

- 9. What should you do to prepare for the transfer of employees from the Montreal office to the Toronto office?**

*A: Create separate OUs for Montreal and Toronto.  
Move the user accounts to the Toronto OU when the Montreal OU is removed.*

- 10. Which factor or factors should you consider when designing the domain naming strategy for Highabove Toys? (Choose all that apply.)**

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

- 11. Which strategy should you use to integrate Worldwide Importers to Highabove Toys in Active Structure?**

*A: Create a forest for HiabuvToys.com. Create a second forest for WideWorldImporters.com.*

## Business Consultants (BC)

### **Background:**

Business Consultants is an international company that specializes in developing equipment for ticketing and access control for ski resorts. The company's turnstile-gate technology uses smart-card reading units. These units can unobtrusively access information from smart cards to authenticate users. The units can also add or subtract values from the cards. For example, the unit can track the number of times a user skis a particular ski run. The units can read the cards from a distance, so that users can simply pass by the units with the cards. Monetary amounts can also be added to or subtracted from the smart-card accounts, so that the card can be used to purchase items.

Business Consultants now wants to expand its scope to serve the informational needs of ski facilities and all of its customers that it serves.

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

Business Consultants will customize its services to meet specific needs of each resort by promoting each independently. However, BC will also provide a benefit known as the Passport that any member can use any resort served by the BC infrastructure. The Passport will provide many services to the members. BC also intend to use its membership list to promote products.

### **Problem Statement:**

Business Consultants currently has only one turnstile smart-card tracking equipment located at ski resorts. The company must acquire the technical expertise to develop new IT system that will support its new mission. It has concluded that Windows 2000 and Active Directory will be important components of its success.

Business Consultants plans to implement its goals in three phases:

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

Phase 2 will occur during the following year. During phase 2, BC plans to add 14 more resort locations and achieve a total membership of more than one million.

Phase 3 will occur during the following year. During this phase, the company plans to double the number of resort locations and members.

Business Consultants intends to gain recognition in the market by using the newest technologies. The company is willing to take risks if the ideas are feasible and will provide services that will promote customer loyalty and company recognition.

### **Business Goals:**

Members will be able to purchase tickets for ski lifts and reserve rental equipment from their home computers or at the resorts. Individual user details will be stored so that ski sizes, the quality of equipment, and other details will need to be added only once. When customers arrive at the resort, they will need not to wait. All equipment will be prepared and stored in the locker. Provisions will also be made for the storage and transport of customer-owned equipment to any resort served by BC.

Business Consultants does not want its customers to have to wait for any services at any ski resorts. Customers will also be able to purchase tickets for ski lifts online from kiosks. As a part of a membership, BC will issue smart cards attached to the stretchable cords. At the ski resorts members, will be able to use cards to open their lockers. They will also use the cards to gain access to ski lifts and to make restaurant reservations. Members who are staying at resorts will use cards as key to their rooms and will not need to register with the resort. Points will also be accumulated for services that are purchased. These points will be used to earn gifts and awards. Members using the smart card to purchase at the ski lodge or store will enjoy discounts. Three memberships classifications will be available: Premier, Active Skier, and Standard. Higher membership levels will receive increased discounts.

Members will also have voice mail and e-mail services. Computers for the services will be located in each room and at many locations in the lodge and on the slopes. When members pass the ski lift turnstile, it will make a sound if they have any new e-mail or voice mail messages. At the top of the lift, they can retrieve their messages. This service will provide a convenient way for members to locate other skiers and communicate with them. Additionally, family and friends at home who know a member's account ID will be able to send e-mails/voice mails to that member.

Reports of the current ski lift usage will be broadcast on the Web sites and on displays in the lodges. Resorts will have the option of instituting a premium classification for access to the lifts. Members in the classification will never need to wait to get on the lifts.

Members who share account IDs will be able to add the IDs to their family lists or friend list. This will make it convenient for members of a household to make reservations for the entire family, or for the individuals to see which of the friends are skiing on any given day.



Members will be eligible for the discount packages, and will be able to use their smart cards at any of the resorts served by BC. Members will also have the ability to add medical information to their cards. All ski patrol teams members will have wireless smart-card readers.

### **Envisioned IT Environment:**

Business Consultants will design and construct the global services to support two inter-related components. One component will be for members, and the other component will be for resorts. Members will be able to access the member component from the Internet or any resort. The resort component will be used to support each resort and its unique internal business and employee needs.

The company headquarters is located at Denver, Colorado. The headquarters employs 56 people. The company has installed a high-speed connection to its IT center San Jose, California. The IT center is connected to the Internet by means of 45-Mbps DS-3 lines. BC does not intend to create a separate employee domain.

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

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

New members will be able to enroll for BC services at each resort. They will also be able to complete application forms on the Internet. The member will be affiliated with one resort, but will be able to use services from any other.

The LANs at the resort will be upgraded to the highest feasible bandwidth. Each resort will have a connection to the Internet. The connection speeds will vary depending upon services available. Each resort will have a Virtual Private Network tunnel to the servers located in San Jose.

During the phase 2, Business Consultants will open a European office to manage the resorts in Europe.

As the company grows during phase 3, it is anticipated that BC will have businesses and IT management centers in each country in which participating resorts are located.

### **Interviews:**

**BC Chief Information Officer (CIO):**

There are two major components of our plan: members and resorts. These components will be constructed at the same time. The members component will provide services to the skiers. The resort component will provide services to the resort businesses and employees. Active Directory will be crucial to both components of the plan.

The schema for the directory serving to the members will need to be modified so that the new functionality will be supported. For development and security, the server hosting the member schema master will be located at our headquarters in Denver. Member accessing BC services from any other resort will have the same functionality.

To achieve the fastest response time, all logon requests must avoid using WAN line. So even if the members travel from one resort to the another, their logon processes will be performed locally and will not require a WAN transmission. Local resort employees will be able to update the members records registered only at their own resort. Requests for changes to records of the members of other resorts will be sent to BC staff. Consequently, it needs to be easy to move a member user object from one resort to another.

In case of possible server failure, a fault-tolerance design will be implemented at each resort so that local service will continue to run even if one servers fail. We must avoid performing directory replication during times of peak usage.

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

Both the member and resort network must support wired and wireless devices. These devices can be connected and automatically assigned IP addresses. For security, other applications must be able to access the devices by means of their DNS names. To help each resort automate its internal operations, we will provide turnkey system that integrates Active Directory and advanced Windows 2000 functionality into each location. The design will ensure that employee information for one resort will not be visible to the other.

**Resort Manager:**

The design for the BC resort infrastructure will provide some great services to employees at my resort. Our employees will access the system for services that include e-mail, human resources information, training and safety programs, the purchase of supplies, equipment inventory and maintenance, and staff scheduling. Employees will be able to access the system from a variety on client computers and kiosks. The kiosks will be computers that run Windows 2000 Professional and have touch-screen plays. Both smart-card authentication and password authentication will be used for employee security authentication. Specific employees will be assigned the responsibility of issuing smart cards and updating member records.

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

The resort is organized into five departments: hotel, restaurant, operations, maintenance, and business administration.

Because each resort is independently owned and managed, each one will want to be able to add applications that might uniquely change the directory schema. In addition, the resorts do not want any external companies or any other resort to have the authority to change user permissions for their employees. Nor do we need to have our internal domain replicated by means of our WAN line. Our e-mail addresses need to be unique for each resort.

Currently each resort has its own Web site. Each resort Web site is registered under its own domain. The DNS services for our top-level DNS domain will continue to be managed by our external Web presence provider. We do not want our internal-operations Active Directory to remain on our external DNS server. The home page of our resort's Web site will include a variety of information related to our resort. We will provide a link from our Web site for members who want to update their records. This link will take our members to a member Web site that is hosted by [businessconsultants.com](http://businessconsultants.com).

## Business Consultants Practice Questions

- You must decide how your Active Directory design will be affected by the factors that influence the business strategies of Business Consultants. Move each business factor to the appropriate component in you active directory design (Use all business factors. Use each business factor only once.)**

Active Directory Design Components	Business Factors
Forests Sites Number of domains OU Security groups membership	Each resort must have independent control. Directory replication cannot be scheduled during times of peak usage. Resort administrative control is divided among five departments. 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. All member logon requests must avoid using the WAN line.

- A: 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:*  
*OU: Resort administrative control is divided among five departments.*  
*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.*

- You must decide how many Windows 2000 Server computers you need to host the domain controllers and global catalog servers for phase 1 of the implementation plan. What is the minimum number of servers that you should use?**

*A: 27*

- Which BC business needs should you implement by using Group Policy objects? (Choose all that apply.)**

*A: Configuring the desktop settings for resort employees.*  
*Updating the software on the kiosks.*

- How should you design the domain and forest structure for the members?**

*A: Use businessconsultants.com for the forest root and single domain.*

- 5. You need to design a DNS, domain, and forest structure that meets the internal needs of the resorts. What should you do?**

*A: Create a DNS zone named ad as a subdomain of the resort's existing Internet domain name.*

*Assign this domain name to the Active Directory forest root.*

- 6. You must decide how many forests BC should use. Which business as technical factor should influence your decision? (Choose all that apply.)**

*A: 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 BC or any other resort to have any authority to change user permissions for their employees.*

- 7. You need to choose the top-level organizational unit that will support a resort's internal business requirements. Which top-level OU should you use?**

*A: Departments*

- 8. Resort employees must be able to update member records. Which trust relationship should you configure between the member domain and each resort domain?**

*A: A one-way trust, where member trusts resort.*

- 9. You need to configure replication for Business Consultants. Which two steps should you take? (Choose two)**

*A: 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 a.m. to 6 a.m. local time at each resort.*

- 10. You must implement DNS services for one of the resorts. Which sets of steps should you perform? (Choose all that apply.)**

*A: Install MS DNS Server on two servers.*

*Configure a subdomain of the resort's Internet domain.*

*Migrate the resort's top-level domain to DNS Server.*

- 11. How many forests should you create for phase one of BC implementation plan?**

*A: 7*

**12. You are deciding how should you support the requirements of Business Consultants members, resort employees and resort departments. You need to decide which properties are most appropriate to meet the requirements of each group. Move each technology to most appropriate groups (Use all technologies. Use each technology only once.)**

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

A: Resort employees: *intrasite replication*  
 Members: *intersite replication*  
 Resort Departments: *unique schema*  
*delegated administrative rights*

## Electrik Corporation

### **Background:**

Electrik Corporation manufactures various silicon components that are used in consumer electronics. Design teams are located at six offices that are dispersed worldwide. These teams collaborate to create, test, and modify new and existing component design. This collaboration requires creating, accessing, and modifying a variety of documents and document formats that are on the servers located throughout the company.

### **Geography:**

The headquarters for Electrik Corporation is located in New York. Branch offices are located in San Jose, London, New Delhi, Bangkok and Sidney. Component designers work in all offices. The San Jose and Bangkok offices are manufacturing facilities. The New York and Sidney offices have 2,500 employees each. Each other office has 500 employees.

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

- Western Region
  - New York, New York.
  - San Jose, California.
  - London, England.
- Eastern Region
  - Sydney, Australia
  - Bangkok, Thailand
  - New Delhi, India

### **Network Infrastructure:**

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

The connection between the New York and London offices is heavily utilized during New York's business hours. The connection between Sydney and Bangkok is heavily utilized during Sydney's business hours.

All locations have a 155-Mbps ATM backbone. All client computers are connected 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. Our employees must be able to collaborate with each other 24 hours per day, and we can not allow anything to interfere with this capability.

During the next one to two years, we anticipate a series of mergers, partnerships, and acquisitions. We need to be ready to assimilate these new entities into our organizational and managerial structure, and into our infrastructure. We must be able to easily restructure our organization, administration, and online data to take advantage of new resources without interrupting the design and manufacturing processes. We might begin selling parts of business during the next one to two years.

### **Chief Information Officer (CIO):**

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

To maintain control, we have divided between the New York and Sidney offices the responsibilities of all IT operations and IT infrastructure management. However, New York office makes final decisions regarding the infrastructure designs. The New York office is responsible for the Western Region, and the Sidney office is responsible for the Eastern Region.

This division of control should not hinder the performance or availability of computer based services when users access network resources, these resources should be presented quickly. We can not afford to have any computer down time our computer. Our mission for the next year is to have all services available and for those to start as quickly as possible.

### **Security Officer:**

We have seen an increase in attempts to breach the security of our network. We do not know whether these attempts are being made by individuals who are simply testing their skills or whether they are attempts at organized industrial espionage. But, we are not taking risks. Security must be one of the primary considerations in design of all operating systems and services.

We are implementing strict security policies and procedures at all facilities. The Eastern and Western regions will individually manage policies. Because of an existing security policy, and to ensure that the users are minimally affected, the Eastern Region will require password resets every 30 days and a minimum password length of four characters.



The Western Region will require password resets every 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 work hard to associate Elektrik Corporation's name with a highly recognizable and positive image. Although our e-commerce business is successful, we might sell that portion of the business. Because it will possible that we will sell the name with a portion of the business, we need to take actions to ensure that the sale of the name will not effect internal operations. If we sell the e-commerce business, [www.elektrik.com](http://www.elektrik.com) will be included as a part of the sale.

**Existing IT Environment:**

All locations have three Windows NT 4.0 domains: one account domain and two resources domains. The Western Region locations use Windows NT 4.0 DNS Server for name resolution. The Eastern Region currently uses a UNIX-based DNS service that supports the use of SRV records but that does not support dynamic updates.

Each facility has several Windows NT 4.0 computers.

## Electrik Corporation Practice Questions

1. Which two Electrik Corporation business factors should influence your Active Directory naming strategy?

*A: Organizational Unit hierarchy.  
Possible sale of Electrik Corporation name.*

2. Which Electrik Corporation business factor necessitates a multiple domain Active Directory design?

*A: Individual infrastructure management control at the New York and Sydney offices.*

3. You are designing Electrik Corporation's OU hierarchy. Which business factors should have the most influence on your design?

*A: Departments.*

4. Electrik Corporation is considering using the domain names listed below in a design that uses only the default Windows 2000 Trusts. Identify the Kerberos referral path that is traversed when a user in newyork.west.electrik.com accesses resources located in sydney.east.electrik.com. Move the appropriate domain names to the trust path list and arrange them in correct order. (Use only domain names that apply.)

Trust Path List	Possible Domain Names
	1. electrik.com 2. west.electrik.com 3. east.electrik.com 4. newyork.west.electrik.com 5. london.west.electrik.com 6. sanjose.west.electrik.com 7. sydney.east.electrik.com 8. bangkok.east.electrik.com 9. newdehli.east.electrik.com

*A: The Trust Path List should include the following numbered tasks in this order: 2, 3, 7.*

5. You are considering the following domain hierarchy for Elektrik Corporation:

elektrik.com  
east.elektrik.com  
west.elektrik.com  
bangkok.east.elektrik.com  
newdelhi.east.elektrik.com  
newyork.west.elektrik.com  
london.west.elektrik.com  
sanjose.west.elektrik.com  
sydney.east.elektrik.com

There is a one-to-one relationship between sites and locations. A domain associated with only one location. Additionally, elektrik.com and west.elektrik.com will be managed in the New York location. How should you design the server services at the New York location?

*A: One schema operations master, one domain naming master, six domain controllers, two global catalog servers and three PDC emulators.*

6. Elektrik Corporation decides to enter into a joint venture with one of the vendors. This venture will result in the creation of a third company that will require its own Internet presence. Systems administration duties for the new company will be shared equally by Elektrik Corporation and vendor. Elektrik Corporation and vendor currently have separate Active Directory forests. Which modifications should you make to Active Directory to support the joint venture requirements?

*A: Create a new tree for the new company.  
Create this tree in Elektrik Corporation's forest.*

7. A proposed design for Elektrik Corporation is shown below:

San Jose Site	New York Site
sj1 west.elektrik.com	ny1 west.elektrik.com
sj2 west.elektrik.com	ny2 west.elektrik.com
sj3 west.elektrik.com	ny3 west.elektrik.com

The servers are named SJ1, SJ2, SJ3 and NY1, NY2 and NY3. SJ3 and NY3 are bridgehead servers. You want to create a new user on NY1. You must identify the steps for default replication of that user to every domain controller in the New York and San Jose sites. Given this proposed design, move the replication steps needed to achieve this goal to the list of steps and arrange them in correct order. (Choose only replication steps that apply.)

Ordered List of Replication Steps	Possible Replication Steps
	<ol style="list-style-type: none"> <li>1. Create the user.</li> <li>2. NY1 notifies its replication partner or partners.</li> <li>3. NY1 sends data to SJ3.</li> <li>4. NY1 and NY3 begin pull replication from NY1.</li> <li>5. NY3 notifies its replication partner or partners.</li> <li>6. NY3 sends data to SJ3.</li> <li>7. SJ1 and SJ2 begin pull replication from NY3.</li> <li>8. SJ3 notifies its replication partner or partners.</li> </ol>

*A: The Replication Steps should include the following numbered tasks in this order:  
1, 2, 4, 5, 8, 9, 7.*

Facade, Inc.

### **Windows 2000 Upgrade Project:**

Your company is asked to provide consulting, development and integration services for a company named Facade, Inc. As a part of this project you will implement Windows 2000. All client computers that currently run Windows 95 will be upgraded to Windows 2000 Professional. The domain controller environment will be fully upgraded to Windows 2000 Server.

### **Background:**

Facade, Inc. manufactures and supplies plastic containers to manufactures of personal grooming products. The company has three offices in southern United States. These offices are located in Dallas, Atlanta and Phoenix. The company headquarters is in Dallas. The following departments are located in Dallas. The following departments are located in Dallas office:

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

In both Phoenix and Atlanta there are offices for the following departments:

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

The company currently operates two eight-hour shifts for manufacturing and one shift for administrative and clerical functions.

### **Problem Statement:**

#### **Chief Executive Officer (CEO):**

The benefits derived from IT administration are not worth the money that we spend on it.

Our suppliers and customers want to be able to link to our network for inventory updates, pricing, and billing.

Currently, many of the processes are paper based. This practice causes all the associated difficulties related to paper handling and data entry. Another consequence of this practice is that our data is not as current as we want it to be. We want to automate and consolidate the sites that employees need to access to find employee information and to input information.

### **Chief Information Officer (CIO):**

Currently, all account administration must be performed in Dallas. With the exception of account administration, there is no centralized management of client computers. Internet mail is not currently available within the company. The existing Windows NT domain 4.0 structure necessitates several domains for the delegation of administration.

We want to create accounts at headquarters. However, we want departmental IT staff members at the Phoenix and Atlanta locations to be able to reset passwords and make other modifications to the accounts. We do not want to give Phoenix or Atlanta full administrative control.

We are concerned that Microsoft Windows 95 does not offer enough security at the client computer level. The amount of traffic on the existing WAN connections between Atlanta and Dallas and between Phoenix and Dallas averages 75 percent saturation during business hours. All IT maintenance will be performed during a four-hour period during non-business hours. We try to schedule traffic during the evening hours whenever possible.

I need to justify cost of every improvement we make to the IT infrastructure.

### **History:**

The Windows environment was most recently upgraded in early 1997. It was upgraded to Windows NT 4.0 and Microsoft Windows 95 from NetWare 3.12 and Windows 3.1. All service packs were applied to Windows NT 4.0 when they were released. The upgrade in 1997 caused several problems with connectivity, validation, and permissions. Because of these problems, some employees were not able to work. These problems were associated with the specific consulting organization that performed the upgrade. Nevertheless, employees still remember the problems and recall them whenever upgrades are suggested. Consequently, company is sensitive about the duration of downtime during the upgrades.

### **Existing IT Environment:**

#### **General:**

Facade Inc employs approximately 10,000 people. The company uses approximately 5,000 computers. Of these computers, 3,750 are in Dallas, 750 are in Atlanta and 500 are in Phoenix.

The existing manufacturing environment is controlled by UNIX-based computers. There are currently four Windows NT 4 domains: a global account domain in Dallas that controls all user accounts, and resource domains in Dallas, Phoenix and Atlanta.

### **Network Infrastructure:**

There are 56-Kbps lines from Dallas to both Phoenix and Atlanta. IT administrators are concerned about the amount of available bandwidth but can not justify upgrading the links at this time. Because of these concerns, traffic is scheduling for evening hours whenever possible. SAP is used for inventory management. The SAP server is located in Dallas.

The existing Web site is hosted by a third party. The facade.com domain is registered. It is hosted by third party Web servers, but it does not host any interactive Web pages. At each location, there is an internal BIND DNS server to manage the UNIX environment. The UNIX DNS structure is completely self-contained and functions as its own root. The Windows 2000 support staff must easily be able to gain access to the DNS that supports Windows 2000.

The company currently has no connection to the Internet.

### **Client Computer Environment:**

Employees in the manufacturing design department use Unix-based computers for design processes. For e-mail and Web processing, they use Windows computers. The computers used by the manufacturing department use a terminal-emulation program to communicate with the system that control the manufacturing processes.

Most of the employees use the computers that run Windows 95. Most the Windows 95 computers run on Pentium 166-MHz MMX hardware platforms that have 16 MB of RAM and 2.1-GB hard disks. Facade, Inc., uses Microsoft Office 97 as its standard office suite. Department-specific applications are installed locally by on-site administrators.

Each of the manufacturing department's computers is used by more than one employee. The company wants server-stored profiles and documents to be available from local servers to each manufacturing department user at each of the manufacturing department's computers.

### **IT Infrastructure:**

The primary IT center is in Dallas. IT management is performed in Dallas whenever possible. The sales and marketing, manufacturing, human resources, purchasing, administration, quality control and maintenance departments each use unique software. The technical support staff needs specific expertise to supply support to each of these departments. Consequently, each department has its own technical support staff. The IT policy for each

department is defined and managed in Dallas. Most of the departmental support staff is located in Dallas, although some of the support staff members at the local offices report directly to departmental IT managers in Dallas. The departmental support staff at the local offices will need delegated authority to perform basic administration.

**Security:**

In the master account domain, grouping of users for resource access is performed by means of global groups. This grouping is performed by the IT administrators in Dallas. For local resource access, local groups are created on local servers. These groups are created by the local IT administrators. Administrators grant these user rights by adding global groups to local groups.

Local administrators of resource domains are not granted administrator rights for the Dallas domain.

**Group Policy Goals:**

Group policy will be managed for Dallas with the both company-wide policy and departmental policy. Initially, Group policy will be designed to redirect folders, to define logon scripts that will be customized for each department at each location, to minimize the logon time, to define the desktop settings, and to allow department-specific software to be made available. Security groups will not filter Group Policy objects, with the exception that most Group Policy will not apply to technical support staff.



## Facade, Inc. Practice Questions

**1. Which goal is accomplished as a direct result of the upgrade to Windows 2000 Active Directory?**

*A: Increased control and increased capability to standardize applications and configurations throughout the company.*

**2. How should you design the sites and site links for Facade, Inc.?**

*A: Create one site each for Atlanta, Dallas and Phoenix. Create IP site links between Atlanta and Dallas and between Dallas and Phoenix. Between Atlanta and Dallas and between Dallas and Phoenix, schedule the links to replicate from 2:00 a.m. to 4:00 a.m., Dallas local time.*

**3. Which upgrade paths should you use for Facade, Inc?**

*A: Upgrade the Dallas 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.*

**4. Where should you locate the server services for Windows 2000?**

*A: In Dallas, locate a schema operations master, a domain naming master, an infrastructure operations master, a RID master, a PDC emulator and a global catalog. Locate one global catalog in Atlanta and one global catalog in Phoenix.*

**5. Which Windows 2000 site design should you implement for Facade, Inc?**

*A: Continue using the existing WAN lines.  
Create one site each for Dallas, Atlanta and Phoenix.*

**6. How should you design DNS to support Windows 2000 for Facade, Inc?**

*A: Install Microsoft DNS server on Windows 2000 computers, and integrate DNS into Active Directory.*

**7. You want to implement Windows 2000 to minimize the impact of replication on WAN traffic for Facade, Inc. What should you do?**

*A: Use IP site links for replication.  
Optimize the replication schedule.*

**8. You need to create a design that will allow you to grant permissions to a set of resources that are on three servers in the Dallas office. You need to grant these**

**permissions to users throughout the entire company after the upgrade. What should you do?**

*A: Create a domain local group in the domain in which the resources exist, and grant this group access to the resources. Create one global group for the domain or domains, and add the members who need to gain access to the resources. Add the global groups to the domain local group.*

**9. How many domains should Facade, Inc., have at the end of upgrade project?**

*A: One domain for the entire company.*

**10. The database administrator for the human resources department attempts to upgrade the SAP applications that will integrate with active directory and new classes in installation phase. What is the most likely cause of this failure?**

*A: The administrator trying to install application is not in the Schema Administrators group.*

## Proposal Corporation

### **Background:**

### **Overview:**

Proposal Corporation was founded in 1990 as an employment agency for temporary employees. The company supports media companies' needs for freelance writers, reporters and graphic artists.

In 1998, Proposal Corporation expanded its scope to include a broader range of information workers (IWs) and to support a broader range of companies. Proposal Corporation's new mission is twofold. This mission is to become a leader in supporting the individual needs of highly qualified freelance IWs and to provide the best service to the corporate customers seeking temporary employs.

### **Information Workers (IWs) Service:**

Proposal Corporation recruits consultants, freelance workers and independent contractors worldwide. The company refers to these individuals as information workers (IWs). The company provides the IWs with personal and GroupWare tools such as e-mail, discussion groups, and scheduling resources to help make them more productive. Next, the company evaluates and markets their skills. Then, finally the company helps them work with the employers that help them by making it easy to share information with these employers. If an IW is assigned to a position with an employer who has network connectivity to Proposal Corporation, special access to shared resources is granted. This special access allows IWs to conveniently share work with employees of the companies that employ them.

### **Corporate Customer Services:**

Proposal Corporation works with a group of leading technology and services companies that need temporary employees. Proposal Corporation makes it easy for companies to browse to its online list of workers and find the right worker for the job. In addition, Proposal Corporation makes it easy for its corporate customers to initiate contract processes and for the employees of the corporate customers to conveniently share information with temporary employees.

### **Organization:**

Currently, Proposal Corporation has approximately 300 full-time employees. They are evenly distributed among its four offices in New York, Chicago, Atlanta and Los Angeles. The Chicago office is the company headquarters.

Proposal Corporation has the following departments:

- Business Administration

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

The consulting department provides management and communication services to the corporate customers. In the consulting department, experts are assigned to support each IW occupational role. These experts hire the IWs, evaluate their skills, manage their security certification clearances, and monitor their assignments with corporate customers. Corporate customers occasionally hire these consultants for temporary assignments.

Proposal Corporation organizes its information into the following groups: employee, recruiting, IW, accounting, corporate customers, and projects.

The company provides services to more than 20,000 IW. Approximately 20 percent of these workers are currently employed in temporary positions acquired by Proposal Corporation.

Proposal Corporation wants to increase the number of its full time employees to 450 during the next two years. During the next two years, the company also wants to double the number of IWs and increase the percentage of IWs that are actively employed.

### **Existing IT Environment:**

The internal WAN consists of 1.544-Mbps lines that connect New York, Atlanta and Los Angeles to the headquarters in Chicago. The connection to network operates at 30 percent utilization, the connection to Atlanta operates at 20 percent utilization, and the connection to Los Angeles operates at 50 percent utilization. The connection to Internet is in Chicago. The company's external Web site is hosted by a third party.

The network consists of one master domain and one separate resource domain at each of the company's four locations. The master domain contains all employee user accounts and is named PW\_Master. PW\_Master has its PDC and a BDC in Chicago and BDCs located in New York, Los Angeles and Atlanta. Each location has a resource domain. The PDCs and BDCs for these resources domains are located at associated offices. Each location also has a second BDC located at the Chicago office. The resource domains are CH\_RES, NY\_RES, LA\_RES and AT\_RES. The PW\_MASTER and LA\_RES PDCs also run WINS. Currently, there are no DNS or DHCP services running.

Currently, the information workers (IWs) want to access the internal WAN. The IWs only access resources on the Windows NT and UNIX Web servers that are hosted by the ISP. E-mail service for IWs is hosted by a UNIX POP3 server.

**Proposed Corporate-Customer Connectivity:**

Currently, 50 percent of Proposal Corporation's IWs are working at approximately 20 large companies. Proposal Corporation has at least one full-time employee permanently located at ten of these companies to manage IWs services. Two corporate customers are willing to configure trust relationships between their own WANs and the Proposal Corporation WAN. Therefore, approved IWs will be able to place files in the Proposal Corporation servers, and employees of these two corporate customers will be able to access the files conveniently.

**Project Goals:****Information Worker Management:**

Proposal Corporation wants corporate customers to be able to directly acquire and manage information workers (IWs). The IT system will need to feature highly flexible tools for searching, scheduling, estimating costs, and deploying resources.

**Establishing Trust:**

Many of the services that information workers (IWs) will provide to Proposal Corporation's corporate customers will be performed remotely. Because little or no personal contacts will occur, establishing trust will be difficult. In an attempt to solve this problem, Proposal Corporation will use video conferencing whenever possible. The company will provide membership access to national video conference centers. When bandwidth allows, the company will also provide support for video conferencing from IW home offices. To further increase trust, IWs enrolled in the Virtual Office service will be granted a higher level of security clearance.

**Information Worker (IW) Virtual Office:**

Proposal Corporation currently provides Web-based administrative tools such as time-sheet reporting, invoicing, and payroll services. It also offers the deluxe services to its information workers:

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

As a part of this project, Proposal Corporation will offer a premium service level named Virtual Office. IWs will pay an additional charge for this service level. This level will provide 50 MB of file storage, project team rooms, personal scheduling tools, contact management, access to discussion groups and advertisement space on the Proposal Corporation Web site, with links to personal portfolios. Proposal Corporation intends to use Public Key Infrastructure (PKI), Microsoft Outlook 2000, and Microsoft Exchange 2000 to support this functionality.

Each IW is classified as one of the following occupational roles:

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

The support the corporate customer's need for confidentiality, IWs will be classified into one of the several levels of security clearance. Depending upon work history and credentials, they can attain higher security levels.

### **Project Requirements:**

Proposal Corporation intends to upgrade the client computers of all permanent employees to Windows 2000. The company will hire external workers to perform the upgrade. The company also wants to consolidate and upgrade the existing Windows NT domains, implement Active Directory, and upgrade Microsoft Exchange 5.5 to Exchange 2000.

Each Proposal Corporation office currently operates at a small independent business. However, most information sharing is contained within each department, regardless of the location. The administration of user account resources should be restructured to support this organizational system.

For security management, the company wants the root of its internal forest namespace to be subdomain of its public domain. This domain is named proposal.com. For fault tolerance, at least two servers host domain controllers in each domain.

In addition to internal network, Proposal Corporation intends to use Public Key Infrastructure, Active Directory, and Exchange 2000 to implement the information worker (IW) Virtual Office service. Permission changes made to IW resources should not need to be replicated to other Proposal Corporation offices, although all employees need to be able to search the complete global catalog containing employees and IWs.

Initially, all 20,000 IWs will be imported into Active Directory as contacts. When IWs subscribe to the Virtual Office service, they will be supplied with Microsoft Outlook 2000, migrated to Exchange 2000, and entered into Active Directory as users. IW users will access Proposal Corporation's internal network to the Chicago Internet connection by means of VPN. To support the anticipated high security levels, IWs subscribing to the Virtual Office service will require stronger password policies than Proposal Corporation employees. These policies include longer passwords and PKI certificates. The design must support smart cards and consistent logon procedures regardless of domains. All users will use username@proposal.com for authentication.

Proposal Corporation also wants to create extranet connections and trusts. Initially, Proposal Corporation will configure the extranet connections and trust with two of its corporate customers. IWs with appropriate credentials will be able to store documents on servers at Proposal Corporation. Corporate customer employees will be able to access these documents easily. The two corporate customers who are configuring trust relations with the Proposal Corporation WAN have already installed Active Directory domains. Users at these companies will want to be able to view appropriate Proposal Corporation file shares in their own global catalogs. These two corporate customers do not want IW user accounts to appear on any of the access control list in their forest.

### **Chief Information Officer (CIO) Interview:**

There are a lots of creative individuals in the IT field. They will install the services just to see how the services work. Because of this tendency, we often have many more services running than we need. I want to regain top-level administrative control. I also want to be able to delegate administrative tasks. Because I want to keep our initial design as simple as possible, I want to use only services absolutely necessary. Because we will use video conferencing, I want to be able to control the quality of service provided to specific users. I also want to be able to control domain replication. In addition, because we might lose a WAN link to our remote locations, employee logon processes should not require the WAN connection.

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

The IT support staff at each location will be responsible for all of the normal daily work, including the daily administration of users, resources, and permissions. I have better things to do with the resources I have. I want the new design to be structured so that this work is delegated to individuals in each department.

## Proposal Corporation Practice Questions

- 1. Which task or tasks must you perform to implement the required Windows 2000 design for Proposal Corporation? (Choose all that apply.)**

*A: Create two explicit one-way trust relationships. Configure these trusts so that Proposal Corporation IWs domain trusts a domain in each of the two corporate customer forests.*

*Request that Proposal Corporation file share objects be added to the corporate customers' global catalogs.*

*Install domain controllers in New York, Atlanta and Los Angeles.*

*Configure DNS and global catalog services in New York, Atlanta and Los Angeles.*

- 2. Which requirements should affect your domain migration strategy?**

*A: Maintaining employee accounts and passwords.*

- 3. How many forests and domains should you create for Proposal Corporation?**

*A: One forest and three domains.*

- 4. How many sites should you create for Proposal Corporation?**

*A: 4*

- 5. Which Proposal Corporation planned upgrade will require you to modify the schema?**

*A: Microsoft Exchange Server 5.5 will be upgraded to Exchange Server 2000.*

- 6. Which steps should you take to design DNS infrastructure and Active Directory domains? (Choose all that apply.)**

*A: Create a forest root named corp.proposal.com.*

*Create a subzone for any necessary child domains of the corp.proposal.com tree.*

- 7. You need to migrate Proposal Corporation's existing Windows NT domains into Active Directory. Move the tasks needed to achieve this goal, and arrange them in the correct order. (Use only tasks that apply.)**



Migration Plan	Possible Tasks
	1. Move users from the PW_MASTER domain to the resource domain at their location. Upgrade the PW_MASTER PDC to Windows 2000, and create the Active Directory root domain. Upgrade each resource domain's PDC to Windows 2000, creating a separate child domain for each location.
	2. Upgrade the Windows NT 4.0 resource domain PDCs to Windows 2000, designating each as a child domain of the employee domain. Create new OUs in the employee domain. Move the computer security groups and other security groups into the new OUs. Decommission the child domains.
	3. Upgrade all of the BDCs of each Windows NT 4.0 domain to Windows 2000 domain controllers.
	4. Upgrade the PW_MASTER PDC to Windows 2000, creating a Windows 2000 domain containing all employee user accounts. Attach this domain to the root domain.
	5. Use a clean install to create an Active Directory root domain.
	6. Create a new Windows NT 4.0 domain and add to this domain user accounts for each IW. Migrate the Windows NT domain to Windows 2000. Create an explicit transitive trust relationship between the employee domain and the corporate customer domains.

*A: Migration Plan should include the following numbered tasks in this order: 4, 2, 3.*

- 12. You must decide how your Active Directory will be affected by factors that influence the business strategies of Proposal Corporation. Move each business factor to the Active Directory design component that it most influences. (Use all the business factors. Use business factors only once.)**

Active Directory Design Components	Business Factors
Site structure Domain structure OU structure Forest structure Explicit trust relationships	<ol style="list-style-type: none"> <li>1. Unique authentication requirements of IWs.</li> <li>2. Division of Proposal Corporation into departments.</li> <li>3. Classification of IWs into occupational roles and administration of IWs by Proposal Corporation employees.</li> <li>4. Existing WAN connectivity and utilization rates.</li> <li>5. Schema modification policy.</li> <li>6. Availability of IW shares from the corporate customer domains.</li> </ol>

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

## Index

Access Control List.....	15	<i>domain local group</i> .....	27, 53
accessing data .....	6	Domain Name System .....	13
<i>account lockout</i> .....	26	domain naming master .....	17, 33, 46
ACL .....	15	Dynamic Domain Name System.....	10
Acquisition Plans .....	3	dynamic updates.....	19
Active Directory.....	3, 6, 16, 17, 18, 31, 33, 39, 52, 57	EAP .....	7
Active Directory Installation Wizard.....	19	Encrypting File System.....	8
Active Directory Integrated DNS .....	19	Exchange 2000.....	56
Active Directory integrated zone .....	19	explicit trust .....	10
Administration Type .....	5	Extranet.....	3
Administrative Control		fault tolerance.....	17, 18
delegating .....	14	firewall .....	12
Administrative Templates .....	14, 15	firewall proxy server .....	16
Allow Dynamic Updates.....	19	Folder Redirection .....	14
AXFR.....	19	Forest .....	10, 12, 32, 39, 59
bandwidth .....	7, 32	Forward Lookup Zones .....	19
Banyan VINES .....	22, 23	full zone transfer .....	19
BDC .....	23, 30, 55	Funding Model.....	5
bottlenecks .....	7	geographical scope .....	1
branch office .....	1	global .....	22
bridgehead server .....	12, 16	global catalog.....	11
<b>business factors</b> .....	45	Global Catalog Server.....	10, 11, 18, 39, 46
business model.....	1	<i>Global Catalog Services</i> .....	59
Capacity .....	7	global group .....	24, 27, 53
Change Management .....	6	global presence.....	1
CHAP.....	7	GPC.....	14
client computer desktop management.....	9	GPO .....	14, 26
communication.....	1	Linking an existing.....	14
Communication Flow.....	2	local.....	14
Company Organization.....	2	Removing and Deleting.....	15
Company Priorities .....	3	GPT .....	14
Compatibility .....	8	Group Policy .....	8, 13, 14, 25, 31
connection object.....	11, 12	filtering.....	15
connectivity.....	6, 7	Group Policy container .....	14
container .....	14	<b>group policy hierarchy</b> .....	26
contractual agreement .....	3	Group Policy Inheritance	
cost.....	12	Modifying.....	15
Cost of Operations .....	4	Group Policy Object .....	13
customer.....	1	Group Policy objects.....	9, 26, 39, 51
DDNS .....	10, 19	Group Policy Objects.....	9
decision-making process.....	2, 5	Group Policy template .....	14
Default-First-Site .....	10	incremental zone transfer .....	19
Delegation of Control Wizard.....	11	<b>influence</b> .....	32, 39, 40
Deny.....	15	influencing factors.....	3
<i>desktop</i> .....	39	Information Flow .....	2
dial-up links .....	12	Infrastructure daemon .....	17
DNS .....	10, 19, 23, 27, 32, 38, 40, 44, 52, 59	Infrastructure master .....	18
<i>DNS infrastructure</i> .....	27, 59	<i>infrastructure operations masters</i> .....	33
<i>DNS zone</i> .....	40	Inheritance	
Domain .....	10, 12	exceptions.....	15
domain controllers .....	11, 17, 18, 39	inheritance rules .....	15
		international .....	1

Internet .....	3, 31	quotas .....	9
Internet Explorer Maintenance.....	14	RADIUS.....	8
InterNIC .....	10	Read access .....	15
Intranet.....	3	refresh interval .....	19
Intrasite Replication.....	16	regional .....	1
IP subnet .....	16	regulations.....	3
IXFR .....	19	Relative Identifier master.....	18
KCC .....	11	Reliability.....	7
Kerberos.....	8, 45	Remote Installation Services.....	14
Knowledge Consistency Checker .....	11	Remote Procedure Call .....	12
LAN .....	8	replication .....	16, 40, 46, 52
Latency .....	6, 7	availability.....	12
laws .....	3	frequency.....	12
LDAP .....	16	schedule.....	12
Life Cycles.....	2	replication schedule.....	16
load balancing .....	17	replication traffic.....	12
logon .....	19	Resource records.....	19
Loopback .....	15	Reverse Lookup Zones.....	19
LSA secret .....	16	<i>RID masters</i> .....	33
Macintosh .....	22	Risk .....	
management model .....	1, 2	Action Planning.....	3, 4
management philosophy .....	3	Analysis.....	3, 4
Microsoft Management Console.....	9, 10	Control .....	4
<b>migrate</b> .....	59	Identification .....	3
<b>migration strategy</b> .....	59	Management.....	3
MMC.....	9, 10, 11, 14	Tolerance.....	3
MS-CHAP.....	8	Tracking .....	3, 4
multimaster replication .....	11, 17	roles.....	6, 8
namespace.....	10, 13	root.....	13
national .....	1	<i>root domain</i> .....	26
NetWare .....	49	RPC.....	12
network bandwidth .....	6, 16	SAP .....	50, 53
network infrastructure.....	9	schema .....	10, 12, 17, 59
Network Roles .....	30	Schema master .....	18
network traffic.....	11, 16	<i>schema operations master</i> .....	33, 46
Novell .....	22, 23	Security .....	14, 24, 51
Only Secure Updates option .....	19	Security Considerations .....	8
Operations Masters .....	17	Security Group .....	
organizational structure.....	2	Authenticated users .....	15
Organizational Unit.....	11, 13, 33	Creator Owner .....	15
OU .....	11, 13, 26, 33	Domain Admins .....	15
Outlook 2000 .....	56	Enterprise Admins.....	15
Outsourcing.....	5	System.....	15
override.....	15	Service locations .....	17
PAP .....	8	Simple Mail Transfer Protocol.....	12
partner .....	1, 2	site boundaries .....	17
passwords.....	24, 30, 43	Site Link Bridge .....	12
PDC .....	30, 55	site links .....	12, 52
PDC emulator .....	18, 33	site object.....	10
Performance Requirements .....	7	Sites.....	12
permissions .....	11	Sites And Services .....	11, 14
PKI.....	56	SMS .....	9
POP3 .....	55	SMTP.....	12
protocol.....	8	Software Installation .....	14
proxy server .....	12	SPAP .....	8
Public Key Infrastructure.....	56	SRV records.....	10, 19, 23, 27

subnet.....	10	User profile .....	15
subsidiaries .....	1	Users And Computers .....	11, 14
System Access .....	7	USN .....	11
System Policies.....	15	vendors.....	1, 2
Systems Management Server.....	9	Virtual Private Network.....	12
TCP/IP .....	8	WAN.....	8, 32, 37, 38, 49, 52, 56
Technical Requirements		Web site .....	50
Analyzing.....	6	Wide Area Network .....	18
Terminal Services .....	9	Windows 2000 .....	9, 19
training.....	7	Windows 2000 Professional.....	21
Tree.....	10, 46	Windows Management Instrumentation .....	9
<i>trust</i> .....	59	Windows NT .....	17, 21, 44
<b>trust relationship</b> .....	40	WMI.....	9
UNIX .....	19, 22, 23, 27, 44, 50, 55	<i>Zone Replication</i> .....	19
update sequence number.....	11	<i>Zone Transfer</i> .....	19