



Exam : 070-297

Title : Designing a Microsoft Windows Server 2003  
Active Directory and Network Infrastructure

Ver : 11-14-2008

## **Topic 1, A. Datum Corporation, Scenario**

### **Overview**

A. Datum Corporation is a company that provides technical classes at locations across North America. The company primarily offers instructor-led courses, on a Monday-through-Friday schedule.

### **Physical Locations**

The company's main office is located in Atlanta. The company has three branch offices in the following locations:

1. Chicago
2. Dallas
3. Seattle

In Addition to the main office in Atlanta, there are also two satellite offices: Atlanta East and Atlanta West. There is no IT staff in the satellite offices

### **Planned Changes**

The company has evolved into a single business unit from four separate technical schools in each of the cities where the company's offices are currently located.

The company recognizes that a cohesive administrative structure will better serve its employees and better secure critical resources.

Recently, the company has begun to offer classes from Atlanta that is available online via the Internet. The company wants to begin offering online content from all offices, not just from Atlanta.

### **Business Process**

Currently, the offices of A. Datum Corporation operates as four independent business units: Atlanta, Chicago, Dallas, and Seattle.

The IT staff in each office functions independently. Network resource access is primarily localized to each office with the exception of the student records database and the current online courseware, which are hosted on servers in Atlanta only.

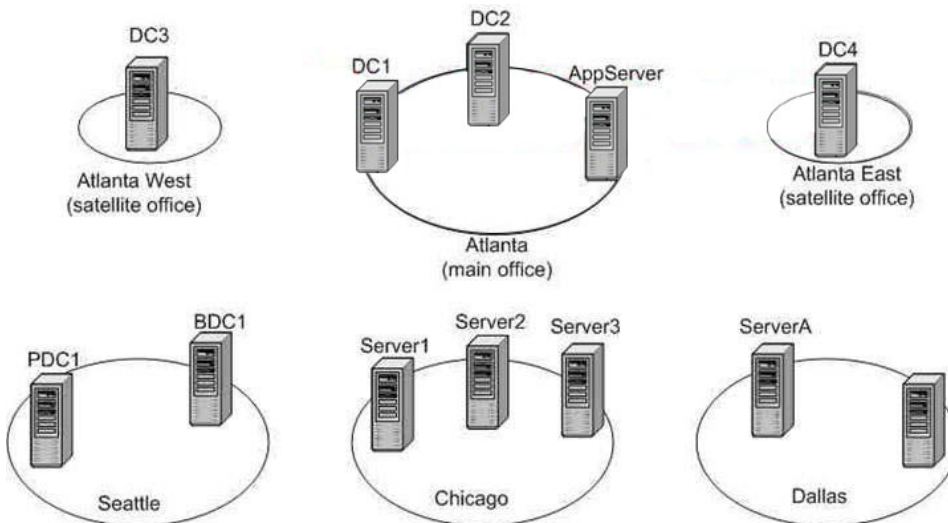
The student records database contains students' personal data and their transcripts.

Currently, the branch offices e-mail the students' enrollment and transcript information to the Atlanta office for entry into the student records database. The admissions department enters personal student data and the registrar's department enters grades. The student records database currently cannot be updated from any other location.

The online course content is already developed and in use.

### **Directory Services**

The servers are configured as shown in the Available Servers exhibit.

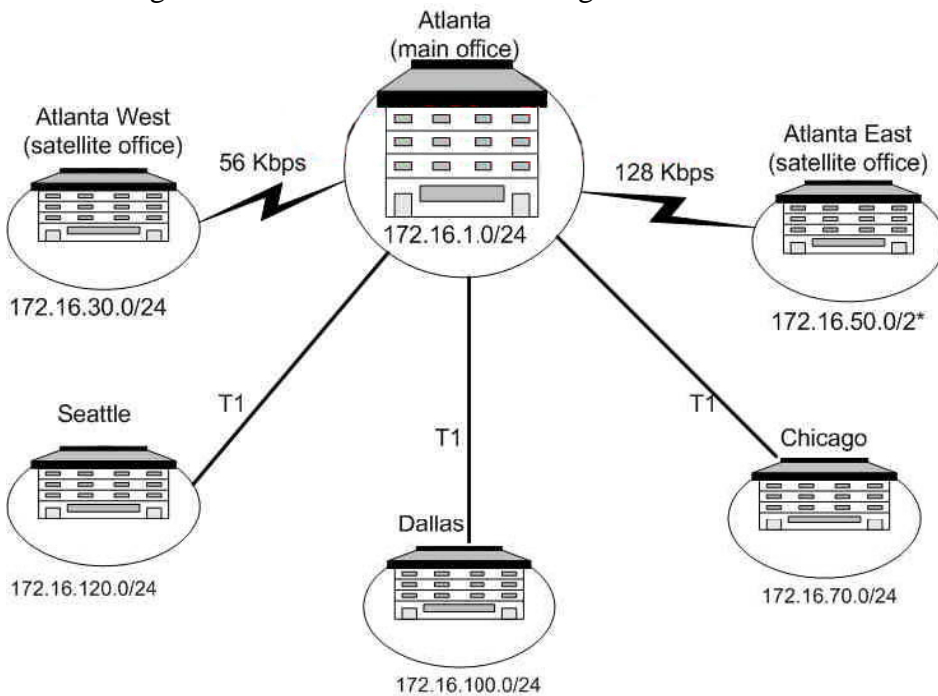


The Atlanta office currently has a Windows 2000 Active Directory domain. The Chicago and Dallas branch offices are both running in workgroup configurations.

Each office manages its own users and groups.

### Network Infrastructure

The existing network is shown in the Existing Network Infrastructure exhibit.



Wan connections between the Atlanta main office and Atlanta East can be unreliable.

There are DHCP servers in Atlanta and the branch offices.

All servers are Pentium III 550-MHz or greater processors with at least 512 MB of memory.

All of the offices run various client operating systems, which include Windows 98, Windows NT Workstation 4.0, Windows 2000 Professional, Windows XP

Professional, and UNIX.

The instructors run either Windows 2000 Professional or Windows XP Professional on their desktop computers at the office. UNIX instructors use a UNIX client computer to access the network when working from home.

### **Problem Statements**

The following business problems must be considered:

1. The company recognizes that its biggest security vulnerability is the methodology that it uses to update the student records database in Atlanta. In the past, there have been problems with students gaining access to and altering their student records.
2. There has been reason to suspect that courseware has been compromised because of weak passwords on instructors' computers.

### **Chief Executive Officer**

I am pleased with the performance of our staff at

A. Datum Corporation. However,

I am concerned about protecting our intellectual property. Both our online curriculum and the student records database need protection. Our primary focus must be that no one outside of the organization can view or modify this information.

### **Chief Information Officer**

We need to provide an adequate security structure for our network environment. It is important that we create a centralized network operations team. I am confident in the ability of our IT staff in Atlanta to take a lead administrative role in our envisioned environment.

The practice of sending student information through e-mail must stop. I think our strategy of a single, centralized student records database is valid. We need to make this database directory-aware so that users who have the responsibility for updating the student records will need only a single set of credentials to make the necessary changes.

Additionally, instructors are not receiving updated teaching schedule information on a timely basis. The issue should be addressed by ensuring that our new scheduling program is installed on all instructor computers, including the computers that the instructors use when accessing our network remotely.

### **Registrar, Atlanta Office**

I am concerned about the network changes. The good news is that they will tell me that I will need only one logon name. However, the other news I am hearing is not good. I am told that the password I use cannot be a word. How am I going to remember a password that is not a word? I have a hard time remembering passwords as it is.

My other major concern is that I am being told that the instructors in each location will be able to enter grades. Recording grades should be my job exclusively.

### **Business Drivers**

The following business requirements must be considered:

1. For its Web site,  
A. Datum Corporation is using the registered domain name adatum.com.
2. The company anticipates more focus on the online course offerings in the future.

### **Organizational Goals**

The following organizational requirements must be considered:

1. The student records database must be available to all offices from Atlanta during the hours of 9:00 A.M. to 8:00 P.M. Eastern Time, Monday through Friday.
2. The online courseware must be available 24 hours a day, seven days a week.

### **Security**

The following security requirements must be considered:

1. The student records database server must be secured to allow only those with the appropriate authorization to modify or add data. These authorized personnel include both instructors and staff in each of the company's offices.
2. Instructors will require the necessary permissions to modify the content for the online courseware for which they are responsible.
3. Instructors are required to make changes to the online courseware and post grades from the LAN only.

### **Customer Requirements**

The following customer requirements must be considered:

1. Remote access will be required for all instructors when they need to access their business offices from home. Some instructors will use UNIX client computers for remote access.
2. Instructors will need the new scheduling application to be installed both on their office and home computers that are members of the domain, even if using a dial-up connection.
3. Windows 98 is currently the operating system on the sales representatives' computers. These computers will not be upgraded in the near future. However, the Active Directory client will be installed on these computers. There are sales representatives in all of the company's offices.
4. Web access to the online curriculum is required by the students enrolled in the online classes, and must be limited to enrolled students only.

### **Active Directory**

The following Active Directory requirements must be considered:

1. The goals of the new Active Directory structure are to provide a centralized method of service administration for supporting the administrative staff and provide secure access to student records.
2. Administration of the Active Directory service will be in Atlanta. Resource administration will occur in Atlanta and the branch offices.
3. Students must not have any permission to any resource other than the online courses.

### **Network Infrastructure**

The following infrastructure requirements must be considered:

1. Because the company has a limited budget, it will need to continue working with the existing physical network.
2. For updating student grades, authorized computers in the registrar's office will require smart card support.
3. The Atlanta, Chicago, Dallas, and Seattle offices will each host DNS subdomains to support the online courseware.
4. The amount of DNS zone transfer or replication must be minimized.

5. Unauthorized updates of DNS records must be prevented.
6. All computers, including client computers, must have host (A) resource records in DNS.
7. UNIX instructors require support of pointer (PTR) resource records for several applications used from their home computers.
8. Network traffic needs to be minimized across the WAN links.
9. Remote access policies for Atlanta, Chicago, Dallas, and Seattle should be centralized.

### Topic 1, A. Datum Corporation (10 Questions)

---

#### QUESTION 1

##### DRAG DROP

You are designing the new forest structure and migration strategy to meet the business and technical requirements. What should you do?

To answer, move the appropriate actions from the list of actions to the answer area, and arrange them in the appropriate order. (Use only actions that apply)

Actions	Answer Area
Upgrade the Seattle domain.	<i>Place first step here</i>
Upgrade the Atlanta domain	<i>Place second step, if any, here</i>
Use ADMT to migrate accounts from the Seattle domain to the Atlanta domain.	<i>Place third step, if any, here</i>
Restructure the Seattle domain.	<i>Place fourth step, if any, here</i>
Restructure the Atlanta domain.	<i>Place 5th step, if any, here</i>

Answer:

Actions	Answer Area
Upgrade the Seattle domain.	Upgrade the Atlanta domain.
	Use ADMT to migrate accounts from the Seattle domain to the Atlanta domain.
Restructure the Atlanta domain.	Restructure the Seattle domain.
	<i>Place fourth step, if any, here</i>
	<i>Place 5th step, if any, here</i>

Explanation:



The correct order of operations would be to

1. Upgrade the Atlanta Domain,
2. Restructure the Atlanta Domain,
3. Use ADMT to migrate accounts.

The Atlanta domain is currently a Windows 2000 domain, so it must be upgraded; this is a Server 2003 environment, after all. It must be restructured to include OUs for the branch offices including Seattle. Finally, since Seattle will not be a separate Domain, the objects must be migrated to the new domain using ADMT.

Active Directory Migration Tool (ADMT) 2.0 allows migration of users and passwords from Windows NT 4.0 domains or Windows 2000 domains to Windows 2003 domains.

Reference:

Lisa Donald, Suzan Sage London, and James Chellis; MCSA/MCSE: Windows (r) Server 2003 Environment Management and Maintenance Study Guide, Sybex, Chapter 1, pp. 3.

---

## **QUESTION 2**

You are designing a DNS strategy to meet the business and technical requirements. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

- A. Create a dynamic reverse lookup zone for each subnet.
- B. Create a dynamic forward lookup for each domain.
- C. Install caching-only DNS servers in the branch offices.
- D. Enable the BIND secondaries option for each DNS server.

Answer: A, B

Explanation:

The scenario states: "UNIX instructors require support of pointer (PTR) resource records for several applications used from their home computers." It also says: "The company anticipates more focus on the online course offerings in the future."

A reverse lookup zone is a database which stores a mapping of IP address to friendly DNS domain names. In DNS Manager, reverse lookup zones are based on the in-addr.arpa domain name and typically hold pointer (PTR) resource records..

A forward lookup zone is a name-to-address database that helps computers translate DNS names into IP addresses and provides information about available resources.

Incorrect options:

C: Caching-only servers do not host any zones and are not authoritative for any particular domain.

D: Windows DNS zone files can contain RRs that can cause problems for BIND secondaries. These records include those that use an underscore in the host or domain name and the WINS and WINS-R records. On some versions of BIND, notably BIND 8.0, the presence of these records can cause the zone to fail to load.

Reference:

James Chellis, Paul Robichaux, and Matthew Sheltz; MCSA/MCSE: Windows (r) Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, Sybex, Glossary, pp. 470 and 477,

J. C. Mackin, and Ian McLean; MCSA/MCSE self-paced training kit (exam 70-291): implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Chapter 4, pp. 4-31.

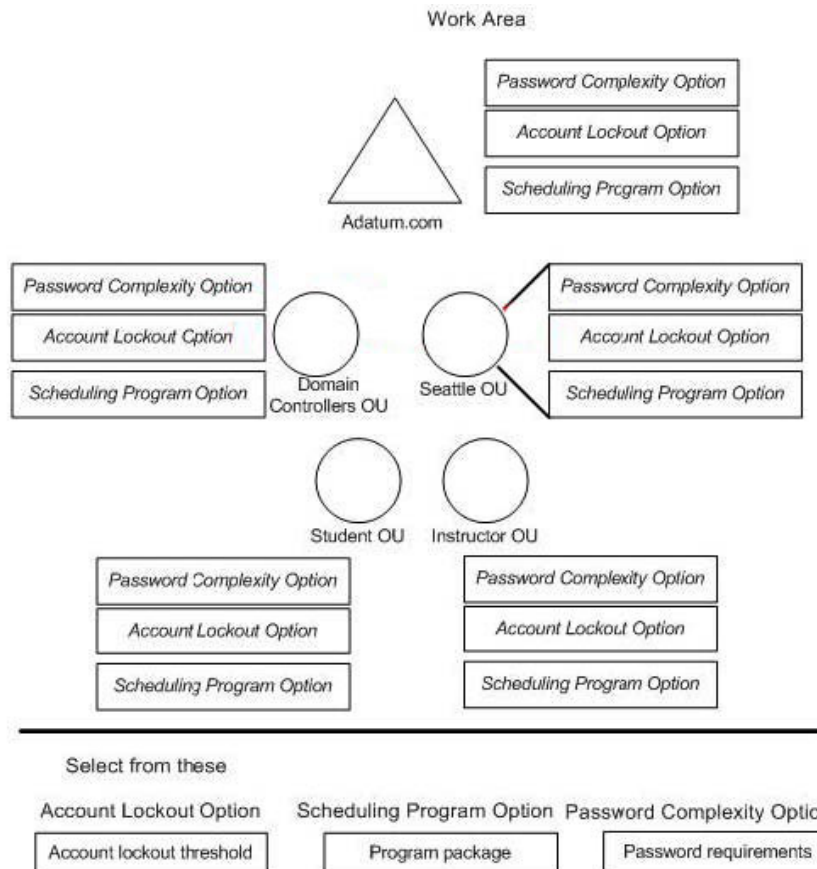
Martin Grasdahl, Laura E. Hunter, and Michael Cross; MCSE Planning and Maintaining a Windows Server 2003 Network Infrastructure: Exam 70-293 Study Guide & DVD Training System, Chapter 6, pp. 396.

### QUESTION 3

#### DRAG DROP

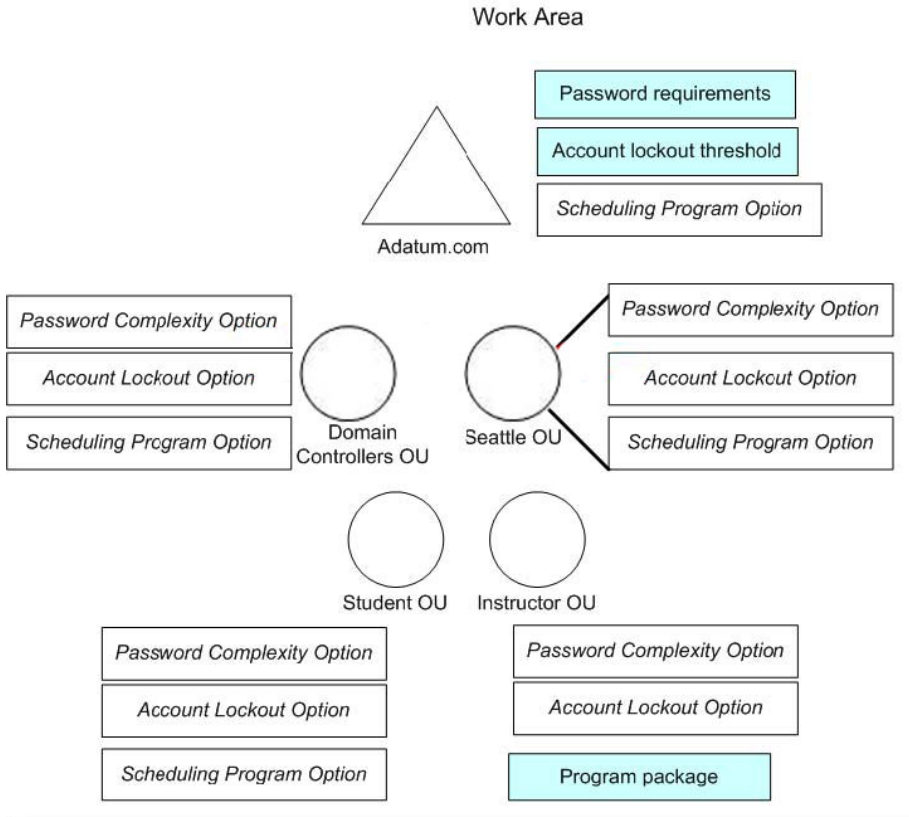
You are designing the Group Policy settings to meet the business and technical requirements. You are reviewing a possible logical structure for the company as shown in the diagram in the work area. The Domain Controllers OU and the Seattle OU are created at the domain level. The Instructor OU and Student OU are children of the Seattle OU. The diagram does not cover all organizational requirements. Based on this diagram, how should you design the Group Policy settings?

To answer, drag the appropriate Group Policy object (GPO) option or options to the correct location or locations in the work area.



Answer:





Select from these

Account Lockout Option    Scheduling Program Option    Password Complexity Option

#### Explanation:

Account Lockout threshold and Password Requirements are both Account Policies and must be placed at the domain level. "The account policy must be defined in the Default Domain Policy or in a new policy that is linked to the root of the domain and given precedence over the Default Domain Policy, which is enforced by the domain controllers that make up the domain."

The case states: "Instructors will need the new scheduling application to be installed both on their office and home computers that are members of the domain." This tells us that the scheduling program must be assigned to "their" computers not all computers that they use or login into. "Their" computers would be members of the domain and would be placed into "Instructor OU" within the domain. Question 6 also verifies this.

Reference:

<http://www.microsoft.com/technet/security/guidance/secmod49.mspx#EQAA>

#### **QUESTION 4**

You need to ensure that only authorized personnel are able to modify student grades.

Which desktop environment or environments should you use? (Choose all that apply)

A. Windows XP Professional

- B. Windows 2000 Professional
- C. Windows 98 with Active Directory client installed
- D. Windows NT Workstation 4.0 with the latest service pack and Active Directory client installed

Answer: A, B

Explanation:

In order for authentication to occur from a centralized point, you need to apply group policies. The desktop environments that support these features are, Windows XP Professional and Windows 2000 Professional.

Incorrect options:

C and D: These desktop environments do not support group policies.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 4, pp. 4-38 to 4-39.

---

### **QUESTION 5**

You need to ensure that the sales representatives are provided with adequate NetBIOS name resolution.  
What should you do?

- A. Install WINS on the PDC emulator.
- B. Install WINS on servers in Atlanta and Seattle.
- C. Enable WINS lookup on the DNS server in Atlanta.
- D. Enable WINS on one domain controller in each office.

Answer: D

Explanation:

As the sales representatives are currently using Windows 98 computers, they need NetBIOS name resolution which is provided for by WINS. In the scenario they also say that there are sales representatives in all offices, which means domain controllers in each office has to be WINS enabled, because they control all activities on the domain.

Reference:

J. C. Mackin, and Ian McLean; MCSA/MCSE self-paced training kit (exam 70-291): implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Chapter 4, pp. 4-7 to 4-6.  
Elias N. Khnaser, Susan Snedak, Chris Peiris, and Rob Amini; MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 2.

---

### **QUESTION 6**

You are designing a strategy to install the new scheduling application.  
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

- A. Assign the scheduling application package to the Instructor OU.
- B. Publish the scheduling application package to the Instructor OU.
- C. Ensure that the scheduling application can install across slow WAN links.
- D. Prevent the scheduling application from installing across slow WAN links.

Answer: A, C

Explanation:

The scenario states: "Additionally, instructors are not receiving updated teaching schedule information on a timely basis. The issue should be addressed by ensuring that our new scheduling program is installed on all instructor computers, including the computers that the instructors use when accessing our network remotely."

All instructor computers form part of the Instructor OU, so by assigning the application to this OU ensures that the package will be installed with minimum administrative effort. The need for ensuring that the scheduling application can install across slow WAN links is due to the network having connections with different speeds.

---

### **QUESTION 7**

You are designing a VPN authentication strategy to meet the business and technical requirements.

What should you do?

- A. Implement the RADIUS service in Atlanta.
- B. Implement the RADIUS service in each branch office.
- C. Configure network address translation (NAT) on all VPN servers.
- D. Configure the Connection Manager Administration Kit (CMAC) on the PDC.

Answer: A

Explanation:

Remote Authentication Dial-In User Service (RADIUS) is a widely used protocol that enables centralized accounting, authentication, and authorization for remote network access. With RADIUS, you can manage network access for VPN, dial-up, and wireless networks. Since the online course content is already developed and in use in the Atlanta office, which is also the main office, it is viable to implement RADIUS there.

Incorrect Options:

B: The online course content is already developed and in use in the Atlanta office.

C: Network Address Translation (NAT) is a technology that enables a local-area network (LAN) to use one set of Internet Protocol (IP) addresses for internal traffic and a second set of addresses for external traffic.

D: This is used to Automate VPN client installation.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris, and Rob Amini; MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 10

Roberta Bragg; MCSE Self-Paced Training Kit (Exam 70-298): Designing Security for a Microsoft Windows Server 2003 Network, Chapter 7, pp. 7-62.

---

**QUESTION 8**

You are designing a DHCP strategy for the new Active Directory environment. Which two groups have the necessary rights to authorize the DHCP servers? (Each correct answer presents part of the solution. Choose two)

- A. IT staff in Atlanta
- B. IT staff in Seattle
- C. DHCP administrators in all offices
- D. DHCP administrators in Atlanta only
- E. Members of the Enterprise Admins group

Answer: A, E

Explanation:

This question is about DHCP Authorization. Only Enterprise Admins have the ability to authorize DHCP servers. An administrator in the Root Domain of the Forest would simultaneously be a member of the Enterprise Admins Group. The fact that they are going to have full administrative privilege for the domain, as well as being admins in the root domain, makes them Enterprise Admins. According to the scenario, the Atlanta office will deal with the administration of active directory. Therefore the IT staff in Atlanta is the correct answer, and "B" is incorrect..

Incorrect Options:

C and D: DHCP Administrator is a built-in group in AD that does not have the ability to authorize DHCP.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder; Exam 70-290: MCSA/MCSE, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing, Inc., Chapter 3, pp. 257.

---

**QUESTION 9**

You are designing the placement of operations master roles in the new environment. In which location or locations should a PDC emulator be designated? (Choose all that apply)

- A. Atlanta
- B. Chicago
- C. Dallas
- D. Seattle

Answer: A

Explanation:

Seeing that the Atlanta office is responsible for the administration of Active Directory, it must be where the Forrest Root domain is located. So if this is true, then the PDC Emulator should be designated to them.

The Primary Domain Controller (PDC) is the first domain controller created in the domain, while all other domain controllers are considered backup domain controllers (BDCs). Therefore, B, C and D are incorrect.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder; Exam 70-290: MCSA/MCSE, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing, Inc, Chapter 1, pp. 19.

---

### **QUESTION 10**

You are designing a DNS and DHCP implementation strategy to support the new environment.

What should you do?

- A. Create a WINS resource record in the Active Directory DNS zone.
- B. Create a WINS referral zone in the DNS zone that supports Active Directory.
- C. Configure a DNS domain name on the DHCP server.
- D. Configure the DHCP server to update DNS for DHCP clients that do not support dynamic updates.

Answer: D

Explanation:

One of the dynamic update settings you can configure on the DNS tab of the DHCP server properties dialog box determines whether the DHCP server should provide dynamic DNS update service on behalf of DHCP clients not capable of performing dynamic updates, such as computers running Microsoft Windows NT 4. By default, Windows Server 2003 DHCP servers do not attempt to perform dynamic updates on behalf of these clients.

Incorrect Options:

- A: The WINS resource record instructs the DNS service to use WINS to look up and forward queries for host names not found in the zone database.
- B: You should configure a WINS referral zone to provide a means of organizing and distinguishing between WINS and DNS records.
- C: An option that specifies the domain name that DHCP clients should use when resolving unqualified names during DNS domain name resolution. This option also allows clients to perform dynamic DNS updates.

Reference:

J. C. Mackin, and Ian McLean; MCSA/MCSE self-paced training kit (exam 70-291): implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Chapter 7, pp. 7-13 and 7-41.

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 6, pp. 6-14.

Martin Grasdahl, Laura E. Hunter, and Michael Cross; MCSE Planning and Maintaining a Windows Server 2003 Network Infrastructure: Exam 70-293 Study Guide & DVD Training System, Chapter 6, pp. 403.

## **Topic 2, City Power & Light, Scenario**

### **Overview**

City Power & Light is a large provider of electrical services for residential and business customers throughout Europe.

The company purchases electricity from large power-producing companies, as well as from small wind-energy providers, such as local farmers and ranchers.

### **Physical Locations**

The company's main office is located in Amsterdam. The company has three branch offices in the following locations:

1. Berlin
2. Brussels
3. Paris

Each branch office has two or more satellite offices in the region. The number of satellite offices and the number of users in each office is shown in the following table.

Office	Number of satellite offices	Total number of users, including satellite offices
Amsterdam	0	800
Berlin	4	150
Brussels	2	70
Paris	5	120

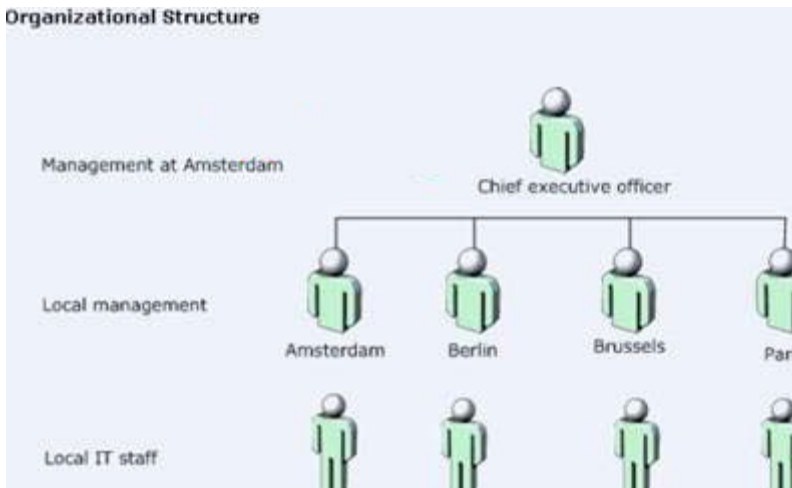
### **Planned Changes**

The company has experienced rapid growth in the past 12 months, and continued growth is anticipated. It is critical to business that the company provides reliable, uninterrupted service 24 hours a day, seven days a week. To meet these demands, the company wants to implement a Windows Server 2003 environment.

### **Business Processes**

The organizational structure of the company is shown in the Organizational Structure exhibit.





The Amsterdam office and each branch office have its own IT staff. The majority of the IT staff is at the Amsterdam office. There is no IT staff at the satellite offices. The IT staff at the branch offices support their respective satellite offices. Regional customer support is provided by the branch offices and satellite offices. The company uses a mission-critical application named App1 that monitors the power network and detects any failures. When failures are detected, App1 automatically sends detailed information about the power failure to the nearest available field technicians. All users within the company have access to App1. App1 logs on to the App1 database by using a shared user account. The App1 database handles security within the database.

### Directory Services

App1 runs on UNIX servers at the Amsterdam office and the branch offices. Each UNIX server has its own security accounts database.

Each office uses a standard user account and password for all servers in that office.

Network administrators in each office know the user account and password combination. Network administrators in each office work independently, but company-wide decisions are made at the Amsterdam office.

Currently, the company does not use Windows domain structure.

### Network Infrastructure

Each office uses a switched 100-Mbps Ethernet network. All client computers run Windows XP Professional.

The company uses its own private leased lines to connect the branch offices and most of the satellite offices. Some satellite offices are connected to the nearest branch office by using ISDN lines. The company wants to reduce telephone costs of these satellite offices by minimizing network traffic through the ISDN lines. The company uses VPN connections over the Internet as a backup to connect the different offices.

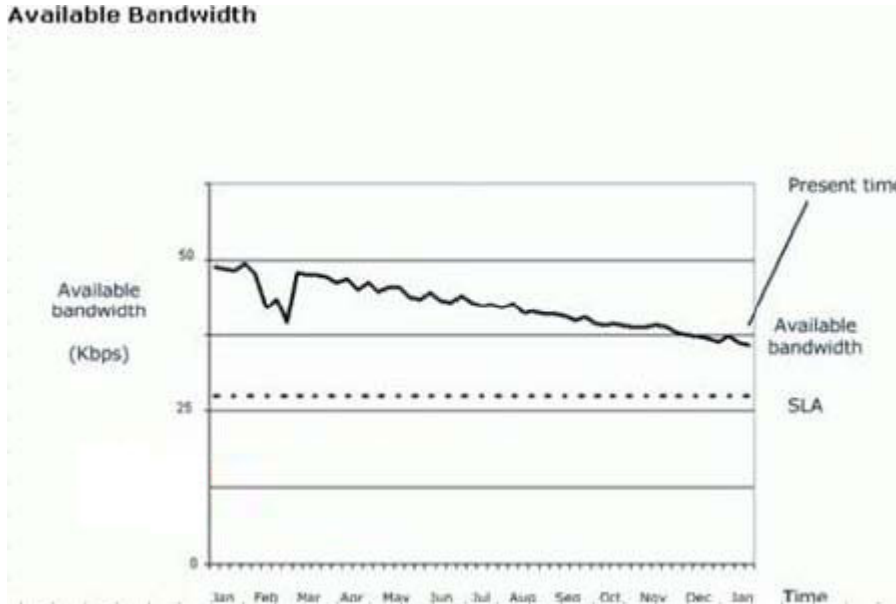
### Problem Statements

The following business problems must be considered:

1. A service-level agreement states that the company must resolve power failures within one day. Currently, the company cannot guarantee this requirement. Last year, there were more than 30 power failures that could not be resolved within one day. The primary cause of the delay in resolution was that the company could not

identify where the problem occurred.

2. Another service-level agreement states that the IT department must guarantee an available bandwidth of 28 Kbps to ensure adequate bandwidth for App1. Currently, the available bandwidth decreases every month, and it is uncertain how long the company can continue to guarantee this requirement. The available bandwidth is shown in the Available Bandwidth exhibit.



\* The company is experiencing problems with the confidentiality of customer information. This is occurring because the data is not centrally managed and the security settings are inadequate.

#### **Chief Executive Officer**

To ensure that customers of City Power & Light receive the most reliable service possible, we want to invest in upgrading App1 to a new application named NewApp. Power failures are inevitable, but if we quickly detect the problem and identify the source, we can restore power more quickly.

#### **Chief Information Officer**

Data from App1 is now saved in different locations. I am concerned about who has access to the data and how to reconstruct the data in the event of a disaster.

#### **Network Administrator**

Currently, we perform our own administration at each office. All network administrators will work together to replace App1 with NewApp. Because NewApp will be centralized, we are concerned that a failure at the Amsterdam office will affect the availability of our monitoring infrastructure.

Most important to us is the ability to monitor the state of the power network. When a failure occurs in the power network, we must detect it immediately.

#### **Customer Service Representative**

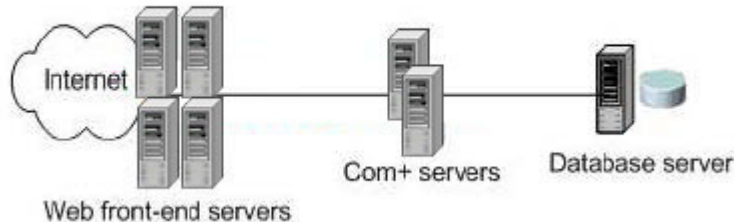
Sometimes customers call in to report a power failure two or three times for the same failure. Each time we have to ask the customer for the same information about the power failure. I want to be able to view what the customer reported the first time, and not have to ask for the same information each time the customer calls in.

#### **Business Drivers**

The following business requirements must be considered:

- \* As City Power & Light changes its infrastructure, all offices must share a common namespace: cpandl.com.
- \* Availability of the monitoring infrastructure and customer support must be improved.
- \* The company will replace App1 with a new application named NewApp. NewApp is a multitier application as shown in the NewApp Architecture exhibit.

NewApp Architecture



1. The company wants customers to be able to receive detailed information about power failures by using the telephone. Customer service representatives need to have detailed real-time information about the power failures, so they can inform customers about the duration of power failures.
2. Each branch office must be able to maintain account policies that meet its unique national legal requirements.

### Organizational Goals

The following organizational requirements must be considered:

1. Upgrades of bandwidth are discouraged. However, upgrades of bandwidth can be permitted if justified.
2. There are no plans to open more offices in the near future. However, the new environment must allow for future company growth.
3. The company anticipates a 50-percent increase in the number of customers over the next two years.

### Security

The following security requirements must be considered:

1. Security of NewApp must be Active Directory integrated.
2. DNS servers will be administered only by network administrators from the Amsterdam office.
3. Network administrators must have Full Control permissions for NewApp.
4. Internal users must be able to access information about customers and power failures. Customers must be allowed to access only public information.
5. A complete power failure in one location must not affect other locations.
6. Network administrators should only be allowed to access NewApp database servers by using smart card authentication. However, network administrators must be able to log on to users' computers to fix problems without using a smart card.
7. Computers that have smart card readers installed must automatically get the NewApp management tools installed.

### Customer Requirements

The following customer requirements must be considered:

1. NewApp must be available 24 hours a day, seven days a week.
2. Client applications that connect directly to NewApp must use the NetBIOS name

of NewApp.

3. To minimize WAN traffic, the branch offices need to use their local resources as much as possible.

4. Wind-energy providers must be able to see how much electricity they have delivered. These providers should be able to connect to NewApp by using the Internet.

### **Active Directory**

The following Active Directory requirements must be considered:

1. City Power & Light must achieve better control of resources.
2. The company must ensure that data can be recovered in the event of a disaster.
3. Replication latency between sites must be minimized.

### **Network Infrastructure**

The following infrastructure requirements must be considered:

1. To improve customer service, information from App1 databases in all locations must be consolidated in the NewApp database.
2. The number of services at the satellite offices must be kept to the absolute minimum.
3. Client computers must always obtain a valid IP address, even when a DHCP server is not available for 24 hours.
4. Field technicians must be able to connect directly to the NewApp database from their portable computers by using a remote connection. They will connect to the nearest branch office when they have to make a remote connection.

### **Users**

The following user requirements must be considered:

1. All users must have Microsoft Office and NewApp automatically deployed on their desktop computers. Network administrators at the branch offices must be able to decide which components of Office get installed at their locations.
2. Resetting user passwords will be delegated to each user's manager. All customer service representatives need to be able to reset the passwords of the wind-energy providers.

## **Topic 2, City Power & Light (9 Questions)**

---

### **QUESTION 11**

You need to evaluate whether the currently available network bandwidth is adequate to run NewApp.

Which three actions should you perform? (Each correct answer presents part of the solution. Choose three)

- A. Use a debug version of NewApp to collect information about NewApp.
- B. Use Performance Monitor to collect data about the saturation of each WAN link.
- C. Use Network Monitor to analyze the data that is transmitted over the network for App1.
- D. Install SNMP on all computers that are connected to App1 to obtain information about App1.
- E. Build a test environment for NewApp to analyze how much bandwidth is required for

NewApp.

Answer: B, C, E

Explanation:

Performance Monitor, which is replaced by System Monitor in Windows Server 2003, allows us to obtain stats on total bandwidth used. The System Monitor is designed for real-time reporting of data to a console interface, and can be reported in graph, histogram, or numeric form.

SNMP allows for the monitoring the status of network components.

A test environment would be ideal in this case to prevent disruption of the active network.

Reference:

Dan Holme, and Orin Thomas; MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, Chapter 12, pp. 12-18.

Craig Zacker; MCSE Self-Paced Training Kit (Exam 70-293): Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Glossary, G-50.

---

### **QUESTION 12**

You need to ensure that there is adequate bandwidth available to meet the service-level agreement requirements.

Which action or actions should you perform? (Choose all that apply)

- A. Upgrade all WAN lines in six months.
  - B. Upgrade all WAN lines prior to implementing NewApp.
  - C. Analyze the cause of a peak in network usage in February.
  - D. Analyze network usage characteristics for NewApp.
- Based on these results, create an upgrade plan for the WAN lines.

Answer: C, D

Explanation:

This option allows you to obtain a baseline of the network usage.

The case study stated that they would only upgrade the WAN links if justified. Keeping a running report on the effects of NewApp would allow this.

Incorrect Options:

A and B: These options are invalid, since the case study stated that they would only upgrade the WAN links if justified.

---

### **QUESTION 13**

You need to ensure that the network administrators are able to administer the NewApp database servers.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

- A. Create an organizational unit (OU) for all users who log on to any of the NewApp servers.
- B. Create an organizational unit (OU) named NewApp Users for the NewApp users.
- C. Create an organizational unit (OU) named NewApp Servers for the NewApp servers.
- D. Create a Group Policy object (GPO) for the NewApp Users OU to enforce the use of IPSec.
- E. Create a global group for all NewApp servers. Add this group to the NewApp Servers OU.
- F. Create a Group Policy object (GPO) for the NewApp Servers OU to enforce the use of smart cards.
- G. Use the account properties to force all users who have to log on to the NewApp servers to use smart cards.

Answer: C, F

Explanation:

The case study says "Network Administrators should only be allowed to access NewApp database server by using smart card authentication. However, network administrator must be able to log on to users computers to fix problems without using a smart card".

Answer C and F combined would create the OU for the NewApp servers and then force anyone logging into the server directly (network administrators) to use smart cards. Since customers and users will be using the web based NewApp they will not be logging on interactively so the GPO won't apply to them

An organizational unit (OU) is an Active Directory container object used within a domain. An OU is a logical container into which you can place users, groups, computers, and other OUs. It can contain objects only from its parent domain. An OU is the smallest scope to which you can apply a Group Policy or delegate authority.

Smart Card Is Required For Interactive Logon - is an option used to designate that the user

must use a smart card during the authentication process, which is found in Account Properties by clicking the account tab. Smart cards are portable, tamper-resistant hardware devices that store unique identification information for a user. They are inserted into a card reader attached to a computer and provide an additional physical identification component to the authentication process.

Incorrect Options:

G: Turning this setting on would require smart card logon to all computers not just the app servers because it is tied with the user account not the server account.

Reference:

Dan Holme, and Orin Thomas; MCSA/MCSE Self-Paced Training Kit: Upgrading Your Certification to Microsoft Windows Server 2003: Managing, Maintaining, Planning, and Implementing a Microsoft Windows Server 2003 environment: Exams 70-292 and 70-296, Chapter, pp. 44-6 to 44-8.

---

## **QUESTION 14**

You are designing a strategy for migrating the UNIX user accounts to Active



Directory.

Which three actions should you perform? (Each correct answer presents part of the solution. Choose three)

- A. Import the user accounts as inetOrgPerson objects.
- B. Import the user accounts into Active Directory by using the Ldifde command-line tool.
- C. Export all user accounts from the UNIX servers to a text file.
- D. Export all user accounts and their passwords from the UNIX servers to a text file. Encrypt this file to achieve extra security.
- E. Assign random passwords to each user object, and securely distribute the password to the users.
- F. Create the same strong password for each user object, and require users to change their passwords at first logon.
- G. Instruct users to use the same name and password as they used on the UNIX servers.

Answer: B, C, F

Explanation:

The LDIFDE tool can be used to import user accounts into AD, so it is correct to export the accounts to a text file and then import them using LDIFDE. However, passwords cannot be added using LDIFDE upon object creation. Passwords can be modified by using the following command:

```
ldifde -i -f chPwd.ldif -t 636 -s dcname -b username domain password
```

Here's the line in the MS doc that refers to that:

The password attribute used by Active Directory is "unicodePwd." This attribute can be written under restricted conditions, but cannot be read. This attribute can only be modified, not added on object creation or read by a search.

A strong password is a password that provides an effective defense against unauthorized access to a resource.

Incorrect Options:

A: InetOrgPerson is an object-similar to a user object-that is used to migrate users from other Lightweight Directory Access Protocol (LDAP) directory services to Active Directory, not from one OS to another.

D: Passwords cannot be added using LDIFDE upon object creation.

E:

G: This cannot be done, since the password attribute for UNIX and Active Directory is different.

Reference:

For more info, see the following web page for Knowledge Base article 263991:

<http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q263/9/91AS>

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Glossary, pp. G-6.

**QUESTION 15**

You are designing a site topology to meet the business and technical requirements. What should you do?

- A. Increase the replication interval between sites,
- B. Use SMTP as the transport protocol for replication.
- C. Create site links to represent the physical topology.
- D. Disable the Knowledge Consistency Checker (KCC) and manually configure site replication.

Answer: C

Explanation:

A site link is an Active Directory object that represents the physical connectivity between two or more sites. For replication to occur between sites, you must establish a link between the sites. There are two components to this link: the actual physical connection between the sites (usually a WAN link) and a site link object. The site link object determines the protocol used for transferring replication traffic (IP or SMTP) and governs when replication is scheduled to occur.

Incorrect Options:

A: The scenario states: "Replication latency between sites must be minimized." This option reduces the amount of traffic over the WAN, but also increases replication latency.

B: SMTP can be used for replication between sites that are not connected with permanent connections (which are required for RPCs).

D: Knowledge Consistency Checker (KCC) is a built-in service that runs on all domain controllers and automatically establishes replication connections between domain controllers in the same site and between bridgehead servers in different sites.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 5, pp. 5-23 to 5-27, and Glossary, pp. G-7.

---

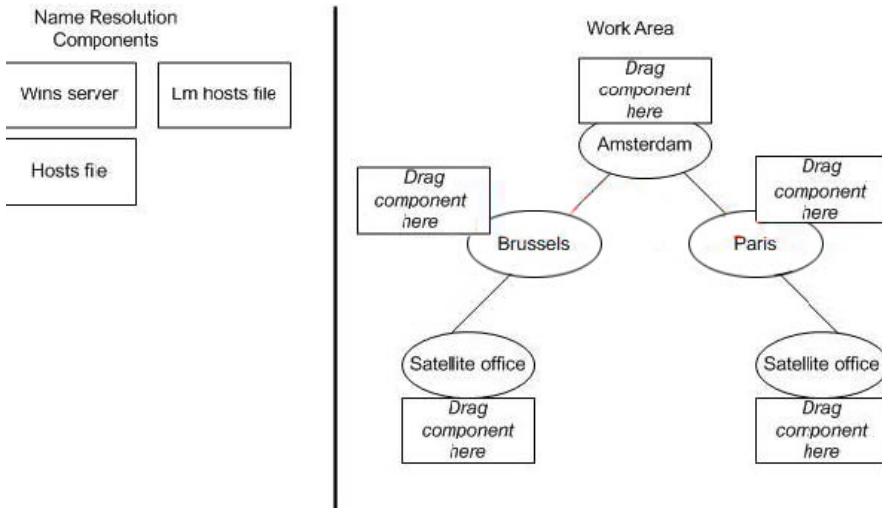
**QUESTION 16**

**DRAG DROP**

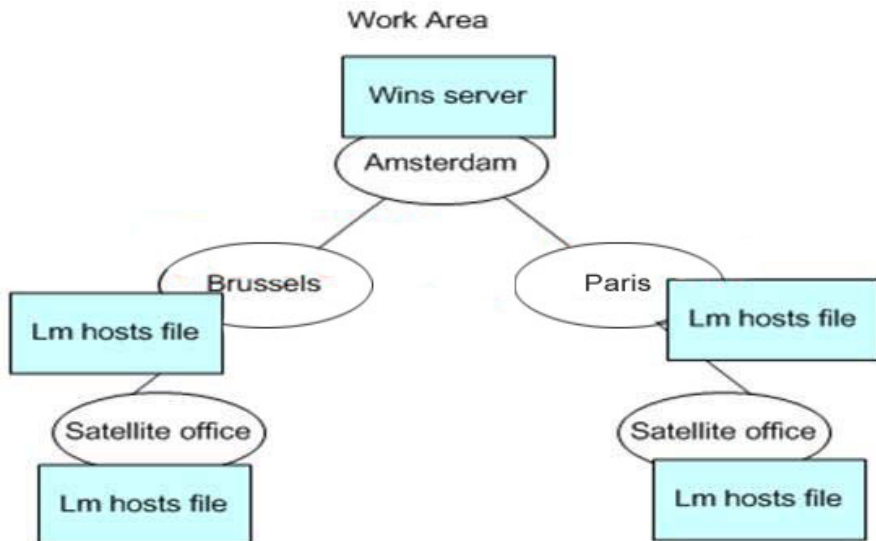
You are designing a NetBIOS name resolution strategy for all computers in all offices.

What should you do?

To answer, drag the appropriate name resolution component or components to the correct location or locations in the work area.



Answer:



Explanation:

The question says that "You are designing a NetBIOS name resolution strategy for all computers in all offices." WINS Server provides computer name resolution by translating NetBIOS names to IP addresses. For applications that depend on NetBIOS name resolution, will need WINS to support these applications in a routed environment.

Reference:

William Boswell; Inside Windows Server 2003, Addison Wesley, Chapter 4.

### QUESTION 17

You are designing a strategy to optimize the DNS name resolution for the satellite offices that connect to the branch offices by using ISDN lines.

What should you do?

- A. Use caching-only DNS servers at these satellite offices.
- B. Configure a Hosts file for all client computers at these satellite offices.
- C. Configure a DNS server to use WINS forward lookup at these satellite offices.

D. Place a DNS server with secondary zones of all domains at these satellite offices.

Answer: A

Explanation:

A caching-only server, as its name implies, caches the answers to queries and returns the results. This saves time and reduces network traffic because calls to multiple DNS servers are not required.

Incorrect Options:

B: HOSTS files, still in use on some networks, are a predecessor to DNS and are files with static mappings of hostnames to IP addresses.

C: You use the WINS tab or the WINS-R tab in reverse lookup zones-to configure Windows Internet Name Service (WINS) servers to aid in name resolution for a given zone after DNS servers have failed to resolve a queried name.

D: This kind of zone is an authoritative backup zone for the primary zone or for other secondary zones.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 6, pp.6-6, and Chapter 1, pp. 1-19.

J. C. Mackin, and Ian McLean; MCSA/MCSE self-paced training kit (exam 70-291): implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Chapter 5, pp. 5-34, and Chapter 4, pp. 4-29.

---

### **QUESTION 18**

You are designing the Active Directory infrastructure to meet the business and technical requirements. You run ADSizer, and find that it provides a solution that contains only one domain controller for Amsterdam.

What should you do?

A. Place at least two domain controllers in Amsterdam.

B. Configure the domain controller as a bridgehead server.

C. Configure the domain controller as a global catalog server.

D. Distribute the users among sites in ADSizer and recalculate the number of domain controllers.

Answer: A

Explanation:

This question may be ambiguous, but it does only speak about the Amsterdam office. Presumably, other offices have also been assigned Domain Controllers.

The problem is not to distribute the users in the Amsterdam office among sites; rather AD Sizer believes that one DC can handle the logon requests. The case study states the need for 24-7 availability, and two domain controllers in a site would allow for this as it increases fault tolerance.

Incorrect Options:

B: A bridgehead server is a server that is responsible for transferring directory replication information between sites.

C: A global catalog server is a domain controller that stores a read-only copy of all Active Directory objects in a forest, with the exception of objects stored in application directory partitions. Global catalog servers are used to store universal group membership information, authenticate users who log on using a UPN, and facilitate searches for objects across the entire forest.

Reference:

---

### **QUESTION 19**

You are designing a DHCP solution to meet the business and technical requirements.

What should you do?

- A. Increase the default lease time on all DHCP servers.
- B. Split all address ranges across multiple DHCP servers.
- C. Configure duplicate scopes on at least two DHCP servers.
- D. Force client computers to obtain an IP address from Automatic Private IP Addressing (APIPA).

Answer: B

Explanation:

We need the users to receive an IP address from the DHCP server even if it is not available for 24 hours. Configuring 2 DHCP servers, with split address ranges, would add redundancy.

Incorrect Options:

A: It is a best practice not to set your lease duration too high, because other DHCP clients on your network may be unable to obtain an IP address lease if all addresses are used up before current leases expire.

C: Scopes provide the essential means for the server to manage distribution and assignment of IP addresses and of any related configuration parameters to clients on the network. This means that duplicating it would cause conflict in the IP addressing.

D: If you do not have a DHCP server, the new interface will obtain a network address using Automatic Private IP Addressing (APIPA).

Reference:

Deborah Littlejohn Shinder, and Dr. Thomas W. Shinder; MCSA/MCSE Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Chapter 3, pp. 164.

William Boswell; Inside Windows Server 2003, Addison Wesley, Chapter 3.

## **Topic 3, Coho Vineyard, Scenario**

### **Overview**

Coho Vineyard is an importer and distributor of fine wines from around the world.

### **Physical Locations**

The company's main office is located in Los Angeles. The company has two branch

offices in the following locations:

1. Paris
2. Sydney

The company plans to open two additional branch offices within the next year.

These offices will be located in Barcelona and Lisbon.

### **Planned Changes**

To reduce costs and streamline business processes, the company wants to implement a Windows Server 2003 Active Directory environment.

### **Business Processes**

Coho Vineyard consists of the following departments:

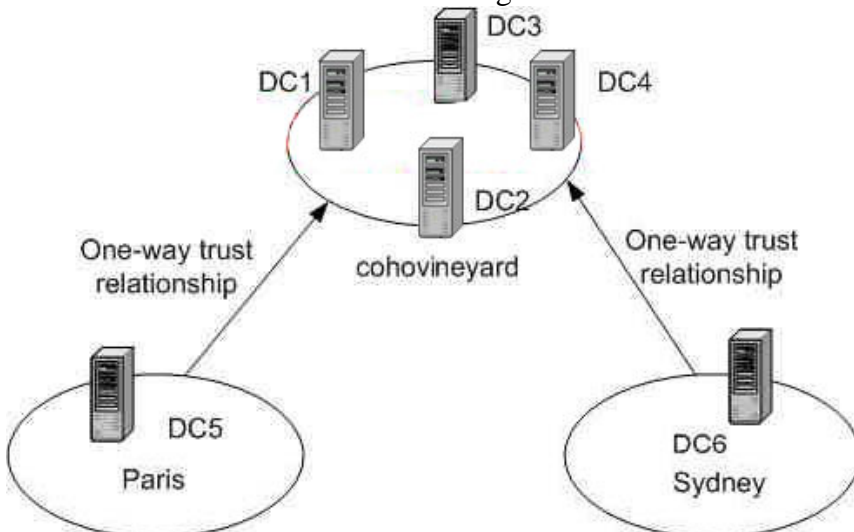
1. Accounting
2. Distribution
3. Human resources (HR)
4. Information technology (IT)
5. Marketing
6. Purchasing
7. Sales

The IT department maintains all internal servers and resources. Currently, the company outsources its e-mail infrastructure to an ISP in Los Angeles.

A Windows NT Server 4.0 computer named Server1 in the Los Angeles office hosts a mission-critical application. This application is accessed by users from all departments and offices in the company. The application vendor currently does not support running other than Windows NT Server 4.0. this application on any operating system

### **Directory Services**

The company has three Windows NT 4.0 domains configured in a single master domain model as shown in the Existing Domain Model exhibit.



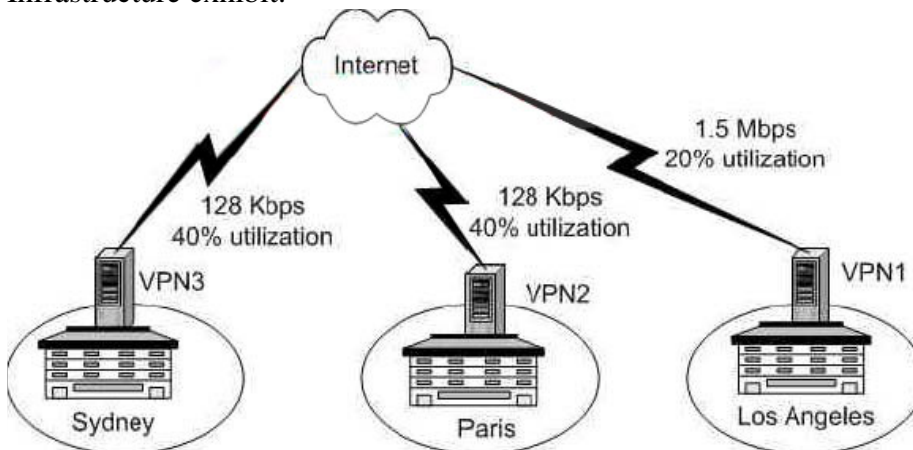
All user accounts are maintained in the cohovineyard domain. Client computer accounts are managed locally in each regional domain.

IT responsibilities for the company are shown in the following table.



Job title	Office	Responsibilities
Chief information officer	Los Angeles	Oversees all IT operations for all offices.
Network Administrator	Los Angeles	Manages all aspects of the network for all offices.
Help desk staff	Los Angeles	Supports all users in all offices. Performs tasks such as resetting user account passwords.
Regional network administrator, Los Angeles	Los Angeles	Manages user and computer accounts for the Los Angeles office.
Regional network administrator, Paris	Paris	Manages user and computer accounts for the Paris office.
Regional network administrator, Sydney	Sydney	Manages and maintains user and computer accounts for the Sydney office.

The existing network infrastructure is shown in the Existing Network Infrastructure exhibit.



Currently, all offices connect to the Internet directly through Windows 2000 Server computers that perform network address translation (NAT). These servers also provide a PPTP tunnel between all offices.

The existing server hardware is shown in the following table.

Server name	Role	Domain	Location	Operating system	Processor	Description and additional functions
DC1	PDC	cohovineyard	Los Angeles	Windows NT Server 4.0	Pentium III 866 MHz	
DC2	BDC	cohovineyard	Los Angeles	Windows NT Server 4.0	Pentium III 866 MHz	WINS, DHCP
DC3	BDC	cohovineyard	Paris	Windows NT Server 4.0	Pentium III 800 MHz	WINS, DHCP
DC4	BDC	cohovineyard	Sydney	Windows NT Server 4.0	Pentium III 800 MHz	WINS, DHCP
DC5	PDC	Paris	Paris	Windows NT Server 4.0	Dual RISC 250 MHz	File server for Paris
DC6	PDC	Sydney	Sydney	Windows NT Server 4.0	RISC 250 MHz	File server for Sydney
Server1	Member server	cohovineyard	Los Angeles	Windows NT Server 4.0	Dual RISC 250 MHz	Mission-critical application server

### Client Computers and Users

The current user population for each office and department is shown in the following table.

Department	Los Angeles	Paris	Sydney	Total
Accounting	10	2	2	14
Distribution	50	5	5	60
HR	5	1	1	7
IT	5	2	2	9
Marketing	10	1	1	12
Purchasing	30	20	20	70
Sales	50	5	5	60
<b>Total number of users</b>	160	36	36	232

The current operating systems installed on the client computers are shown in the following table.

Operating system	Los Angeles	Paris	Sydney	Total
Windows NT 4.0 Workstation, with latest service pack	100	0	0	100
Windows 2000 Professional	20	25	29	74
Windows XP Professional	30	5	1	36
<b>Total client computers</b>	150	30	30	210

### Problem Statements

The following business problems must be considered:

1. Because of security limitations of Windows NT Server 4.0, all IT staff has been added to the Administrators group of the cohovineyard domain. IT staff should be allowed administrative rights only to their specific areas of responsibility.
2. Lack of control over IT procedures and processes have made the current environment costly to maintain.

### Chief Executive Officer

The current IT infrastructure at Coho Vineyard is negatively affecting business operations. IT operations need to be streamlined to accommodate the anticipated growth.

### Chief Information Officer

The current IT environment needs to be reorganized. Corporate standards need to be implemented. Users currently install unauthorized and unlicensed software. These installations need to be implemented. Administrative roles have been clearly defined, but now need to be enforced.

The IT budget for the next year has already been allocated. No new server hardware is to be purchased for the existing offices. New server hardware has been budgeted for the new offices.

After the deployment of Active Directory is complete, e-mail services will be implemented by using Microsoft Exchange Server 2003. The Exchange Server 2003 infrastructure will be maintained by the internal IT staff.

Also we want to provide all users VPN access to the network.

### Network Administrator

There is a need to provide standardized settings for all users and computers. The current IT administration practices need to be reevaluated, and new practices that

are more effective need to be enforced.

### **Office Worker**

The current environment is difficult to use. Information is scattered on the network, making it difficult to find. There does not seem to be any clear definition as to who is responsible for responding to network and computer problems. Because of this confusion, most users manage their own computers.

Also, we want to be able to connect to the network when working remotely.

### **Business Drivers**

The following business requirements must be considered:

1. The current namespace used for the externally hosted e-mail infrastructure is cohovineyard.com. This namespace will be used when e-mail services are implemented internally.
2. The new environment must provide fault tolerance in the event of a single domain controller failure.
3. The ISP provides extremely reliable service for each location. No plans are being made to provide for redundant links. The current level of network outages caused by WAN link failures is considered to be acceptable.
4. To improve network support, Windows Server 2003 will become the corporate standard for all server computers wherever possible. Client computers will be standardized over the next two years to run Windows XP Professional.

### **Organizational Goals**

The following organizational requirements must be considered:

1. Branch offices in Lisbon and Barcelona will be implemented in the next year. The Lisbon branch office is expected to have 65 users and client computers. The Barcelona branch office will have no more than 10 users and client computers.
2. Because of the small size of the Barcelona branch office, it will have no IT staff and no servers. The Lisbon IT staff will manage users and computers for both the Lisbon and Barcelona branch offices.
3. Two servers have been purchased for the Lisbon branch office. One will be designated as a domain controller. The other server will be a VPN server and will also provide NAT services.

### **Security**

The following security requirements must be considered:

1. Regional network administrators must have only limited control over the Active Directory service. They will be responsible for managing user and computer accounts for their regions. They will also manage local servers.
2. The network administrator in the Los Angeles office will manage all domain controllers, configure sites, and perform other high-level administrative tasks.
3. Users will have limited access to their computers. They will be allowed to modify only certain desktop settings, and they will not be allowed to install unauthorized applications.
4. Some users currently have blank passwords. Password security standards must be implemented.
5. Security auditing must be implemented to track all unauthorized logon attempts to the domain. Auditing must not be enabled on any client computers.

### **Active Directory**

The following Active Directory requirements must be considered:

1. Centralized control over Active Directory must be maintained by the network administrator in the Los Angeles office. Limited access to Active Directory will be given to the help desk staff and the regional network administrators.
2. Although bandwidth is not currently an issue, incremental increase in bandwidth usage is anticipated. To accommodate this projected growth, all designs should minimize WAN traffic.
3. Departments within Coho Vineyard have their own unique needs, which include, but are not limited to, specialized departmental applications.

#### **Network Infrastructure**

The following infrastructure requirements must be considered:

1. Remote access security and restrictions for all offices must be implemented and managed centrally by the network administrator in the Los Angeles office. Only one set of remote access policies must exist for the company.
2. A domain-naming strategy must be identified that reduces administrative complexity and is intuitive to the users.
3. One domain controller in each of the current offices will have the DNS service installed. DNS name resolution traffic must be minimized over all WAN links.

### **Topic 3, Coho Vineyard (13 Questions)**

---

#### **QUESTION 20**

As part of your design, you are evaluating whether to upgrade all domains to Windows Server 2003.

Based on current configurations, which server or servers prevent you from achieving this goal? (Choose all that apply)

- A. DC2
- B. DC3
- C. DC4
- D. DC5
- E. DC6
- F. Server1

Answer: D, E

Explanation:

The question asks what is preventing you from upgrading the DOMAINS to Windows Server 2003. The correct answer is D and E. Both these servers are PDC in their domain. The problem is that they are RISC servers. There is no RISC version of Windows 2003 so the domain cannot be upgraded.

Incorrect Options:

A, B and C: These BDC's are running Pentium processors which do support Windows Server 2003. Furthermore, BDC's can be upgraded from Windows NT Server 4.0 domains to Windows Server 2003 domains.

F: The case study says that Server1 is currently hosting a mission critical application,

and that the application vendor does not support running this application on any operating system other than Windows NT Server 4.0.

Reference:

Jerry Honeycutt; Introducing Microsoft Windows Server 2003, Microsoft Press, Chapter 16.

---

**QUESTION 21**

You are designing the Windows Server 2003 Active Directory forest structure to meet the business and technical requirements.

Which forest structure should you use?

- A. One Active Directory forest with one domain.
- B. One Active Directory forest with three domains.
- C. One Active Directory forest with four domains.
- D. Two Active Directory forests with one domain in each forest.
- E. Three Active Directory forests with one domain in each forest.

Answer: A

Explanation:

In the security section of the case study it states: "Regional network administrators must have only limited control over the Active Directory Service. They will be responsible for managing user and computer accounts for their regions. Therefore, the locations will become OU's and we will delegate control."

The network administrator in the Los Angeles office will manage all domain controllers, configure sites and perform other high-level administrative tasks. This would then be the Root of the forest. There was no reason in the case study given that would state the requirement of a multi domain model such as different passwords or schema. It is for this reason that B, C, D and E are incorrect.

---

**QUESTION 22**

You are designing the top-level organizational unit (OU) structure to meet the business and technical requirements. Your design must accommodate the anticipated growth of the company.

Which top-level OU structure should you use?

- A. Paris OU, Sydney OU, Los Angeles OU, Lisbon-Barcelona OU
- B. IT Administration OU, All CohoVineyard Departments OU, All CohoVineyard Offices OU
- C. Sales OU, Purchasing OU, Marketing OU, Accounting OU, Distribution OU, Human Resources OU
- D. CohoVineyard Users OU, CohoVineyard Computers OU, CohoVineyard Servers OU, CohoVineyard Applications OU

Answer: A

Explanation:

In the security section of the case study it states: "Regional network administrators must have only limited control over the Active Directory Service. They will be responsible for managing user and computer accounts for their regions".

Under the Organizational Roles section it states: "Because of the small size of the Barcelona branch office, it will have no IT staff and no servers. The Lisbon IT staff will manage users and computers for both the Lisbon and Barcelona branch offices". This justifies the creation of the "Lisbon-Barcelona" OU

Although you should not create separate OUs based on geographic locations just because it's an obvious dividing point for structure, there are times when it is an appropriate decision. When the network is dispersed over a wide area and connected by slower wide area network (WAN) links, you can make it easier to design site boundaries by creating a separate OU for each location and then creating nested OUs that delegate administrative control.

Sites in Active Directory provide a way to abstract the logical organization of the directory structure (the forest, domain, and organizational unit [OU] structure) from the physical layout of the network. Sites take the responsibility for representing the physical layout within Active Directory. Because sites are independent of the domain structure, a single domain can include multiple sites or a single site can include multiple domains.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 4, pp. 4-4, and Chapter 5, pp. 5-3 to 5-4.

---

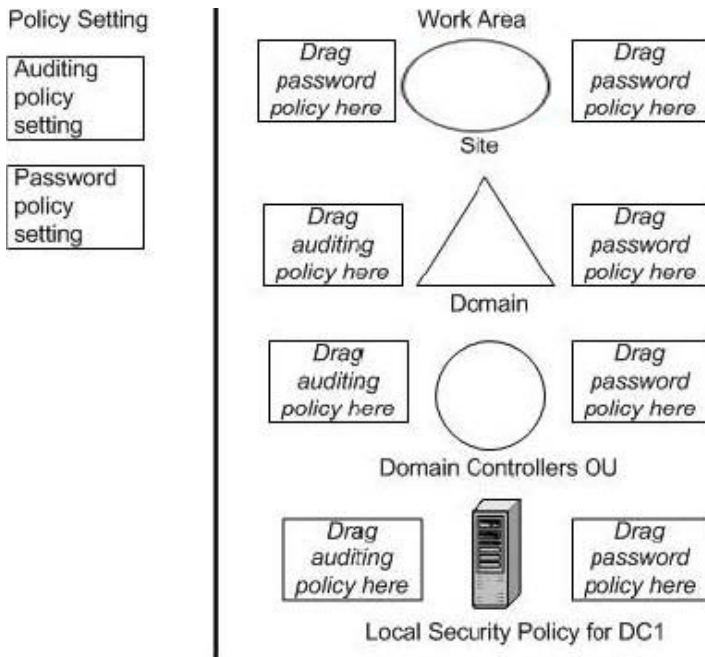
**QUESTION 23**

**DRAG DROP**

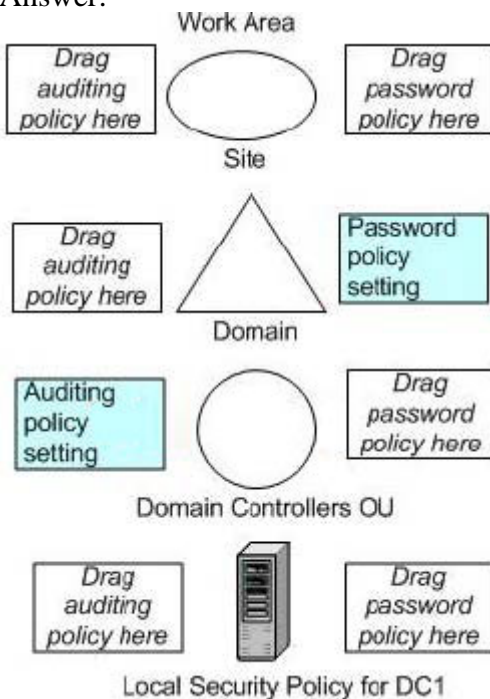
You are designing a plan for applying the security policy settings to meet the business and technical requirements. Where should you implement the auditing password policy settings?

To answer, drag the appropriate policy setting or settings to the correct location or locations in the work area.





Answer:



Explanation:

Account Logon events take place on the domain controllers. Password policies always go to the domain.

Audit Account Logon Events is a policy that audits each instance of user logon that involves domain controller authentication. For domain controllers, this policy is defined in the Default Domain Controllers GPO.

The domain password policies enable you to protect your network against password compromise by enforcing best-practice password management techniques.

Reference:

Dan Holme, and Orin Thomas; MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment , Chapter 3, pp. 3-39, and 3-42 to 3-43.

---

**QUESTION 24**

As part of your design, you are evaluating whether a second-level organizational unit (OU) structure is required.

Which factor necessitates the need for a second-level OU structure?

- A. Audit policy settings
- B. Software deployment needs
- C. Client operating systems in use
- D. Delegation of administrative authority

Answer: B

Explanation:

The Active Directory Section states: "Departments within Coho Vineyard have thier own unique needs, which include but are not limited to, specialized departmental applications." This would justify a 2nd level OU structure by Departments.

Creating OUs based on software management needs allows you to target applications to the appropriate set of users.

Incorrect Options:

A: Audit policy settings is an administrative tool, and "D" says: "rules for OU placement at lower levels of the domain are based more on user and computer management than delegating administrative privileges."

C: There are no organizational requirements specific to either Windows Workstation 4.0 or Windows XP Professional. In addition, all workstations are to be standardized to Windows XP.

D: The rules for OU placement at lower levels of the domain are based more on user and computer management than delegating administrative privileges.

Reference:

Jill Spealman, Kurt Hudson, and Melissa Craft; MCSE Self-Paced Training Kit (Exam 70-294); Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Chapter 12, pp. 12-14.

William Boswell; Inside Windows(r) Server 2003, Addison Wesley, Chapter 8.

---

**QUESTION 25**

You are designing a DNS name resolution strategy to meet the business and technical requirements.

Which action or actions should you perform? (Choose all that apply)

- A. Create an Active Directory-integrated zone named cohovineyard.com on a domain controller in Los Angeles.
- B. Create an Active Directory-integrated zone named paris.cohovineyard.com on a domain controller in Paris.

- C. Create an Active Directory-integrated zone named sydney.cohovineyard.com on a domain controller in Sydney.
- D. On a domain controller in Los Angeles, delegate paris.cohovineyard.com to a domain controller in Paris.
- E. On a domain controller in Los Angeles, delegate sydney.cohovineyard.com to a domain controller in Sydney.

Answer: A

Explanation:

We only have a single domain, and the Network Infrastructure section states: "A domain-naming strategy must be identified that reduces administrative complexity and is intuitive to other users." You can't get anymore simple than a Single Active Directory Domain.

In this type of zone, the DNS database is stored within Active Directory. All DNS servers in an Active Directory-integrated zone are considered primary servers because the DNS information actually becomes part of the Active Directory database; any DNS server can be updated and any of them can resolve client requests. Active Directory is responsible for replicating zone information between DNS servers, often making replication quicker and making it a part of Active Directory management instead of a separate management practice

The Active Directory section states: "Centralized control over Active Directory must be maintained by the network administrator in the Los Angeles office."

Therefore, B,C, D and E are incorrect.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 1, pp. 1-24.

---

### **QUESTION 26**

You are designing a plan for maintaining the WINS infrastructure on the new Windows Server 2003 Active Directory environment.

Which factor or factors necessitate the need to maintain the WINS infrastructure?

(Choose all that apply)

- A. Client operating systems in use.
- B. Server operating systems in use.
- C. VPN client access by using PPTP.
- D. Installation of Active Directory client software.

Answer: A, B

Explanation:

Server1 will not be upgraded due to the mission critical application. Until the upgrade of the client computers to Windows XP Pro takes place, there are still several that are running pre-Windows 2000 operating systems.

As long as there are computers running versions of Windows older than Windows 2000,

there will be a need for WINS.

Incorrect Options:

C: Point-to-Point Tunneling Protocol (PPTP) is a data-link layer protocol used to provide secured communications for virtual private network (VPN) connections.

D: In environments that include any combination of Windows 95, Windows 98, Windows Me, and Windows NT 4.0, the Active Directory client software will need to be installed on these systems in order to participate in an Active Directory domain.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 7, pp. 7-2.  
Dan Holme, and Orin Thomas; MCSA/MCSE Self-Paced Training Kit: Upgrading Your Certification to Microsoft Windows Server 2003: Managing, Maintaining, Planning, and Implementing a Microsoft Windows Server 2003 environment: Exams 70-292 and 70-296, Chapter 4, pp. 4-53.

---

### **QUESTION 27**

You are designing a DNS implementation strategy for the Paris office.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

- A. Create an Active Directory-integrated zone named cohovineyard.com.
- B. Create an Active Directory-integrated zone named paris.cohovineyard.com.
- C. Create a standard primary zone named paris.cohovineyard.com.
- D. Configure all computers in Paris to use DC3 as their DNS server.
- E. Configure all computers in Paris to use DC6 as their DNS server.

Answer: A, D

Explanation:

In the Network Infrastructure Section it states: "One domain controller in each of the current offices will have the DNS service installed. DNS name resolution traffic must be minimized over all WAN links".

The local server for Paris is DC3, which is also a domain controller. Also, seeing as how DC3 is a local server, it would minimize traffic over its WAN link.

Incorrect Options:

B: paris.cohovineyard.com is not a valid domain name.

C: The master copy of the DNS database resides in a standard ASCII text file, in this zone. Only this primary zone can be directly modified.

E: DC6 is located in Sydney, so this option would increase traffic on the WAN lines.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 1, pp. 1-24.

---

### **QUESTION 28**

You are designing a strategy for implementing Internet Authentication Service (IAS) to meet the business and technical requirements.

What should you do?

- A. Install IAS on VPN1, VPN2, and VPN3.
- B. Install IAS, on VPN1.  
Configure VPN2 and VPN3 as RADIUS clients.
- C. Install IAS on VPN1.  
Configure VPN1, VPN2, and VPN3 as RADIUS clients.
- D. Install IAS on DC1.  
Configure VPN2 and VPN3 as RADIUS clients.  
Create all remote access policies on VPN1.
- E. Install IAS on DC2.  
Configure VPN2 and VPN3 as RADIUS clients.  
Configure remote access logging on VPN1.

Answer: C

Explanation:

Internet Authentication Service (IAS) Server is Microsoft's implementation of Remote Authentication Dial-In User Service (RADIUS). A RADIUS server is a server that authenticates, authorizes, and performs accounting functions when a connection attempt is made from a remote access client. It is also a network access server (NAS) that is running IAS. A RADIUS client can be a dial-up server, VPN server, or a wireless access point (AP).

"C" is the most likely answer because it conforms to the above rule, except that the policies have not been included.

Incorrect Options:

- A: Only one IAS server is required.
- B: All VPN servers have to be IAS clients.
- D and E: Policies are created on the IAS server.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 10, pp. 10-38.

---

### **QUESTION 29**

You are designing a DNS infrastructure to meet the Internet name resolution requirements.

What should you do?

- A. Create a standard primary zone named "." on all DNS servers.
- B. Create an Active Directory-integrated zone named "." on a DNS server on Los Angeles.
- C. Configure all DNS servers to use forwarders. Specify the IP address of the DNS server at the local ISP.
- D. Enable default root hints on all DNS servers.
- E. Disable recursion on all DNS servers.

Answer: C

Explanation:

Since all clients will use their local DNS servers for name resolution, they will need to have Forwarders enabled on the DNS servers for Internet Host Name resolution.

If your organization is connected to the Internet by means of a slow wide area link, you can optimize name resolution performance by channeling all DNS queries through a forwarder.

Reference:

J. C. Mackin, and Ian McLean; MCSA/MCSE self-paced training kit (exam 70-291): implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Chapter 5, pp. 5-3 to 5-7.

---

**QUESTION 30**

You are designing the placement of the PDC emulator role to meet the business and technical requirements.

In which location should you place the PDC emulator role? (Choose all that apply)

- A. Los Angeles
- B. Paris
- C. Sydney
- D. Lisbon
- E. Barcelona

Answer: A

Explanation:

When upgrading Windows NT 4.0 and earlier domains, only one domain controller running Windows Server 2003 can create security principals (users, groups, and computer accounts). This single domain controller is configured as a PDC emulator master. The PDC emulator master emulates a Windows NT 4.0 and earlier PDC.

Los Angeles has the most NT 4.0 users, so placing it there would minimize traffic over the WAN lines.

Therefore, B, C, D and E are incorrect.

Reference:

Jerry Honeycutt; Introducing Microsoft Windows Server 2003, Microsoft Press, Chapter 16.

---

**QUESTION 31**

You are designing the IP addressing scheme for the new Barcelona office.

Which network address or addresses are valid for your design? (Choose all that apply)

- A. 10.10.10.0/28
- B. 10.10.255.0/24

- C. 131.15.0.0/24
- D. 151.10.10.0/24
- E. 192.168.11.0/25

Answer: A, B, E

Explanation:

Private addresses are confined to specific ranges that can be used by any private network but that cannot be seen on the public Internet. For example, a user connecting computers in a home TCP/IP network does not need to assign a public IP address to each host. The user instead can take advantage of the address ranges shown in the table to provide addresses for hosts on the network.

Table of Private Address Ranges

Starting Address	Ending Address
10.0.0.0	10.255.255.254
172.16.0.0	172.31.255.254
192.168.0.0	192.168.255.254

Incorrect Options:

C and D: The case study says that the IT staff in the Lisbon office will manage users in the Barcelona office because Barcelona will not have any servers installed. It also says that a VPN server will provide NAT services, which enables a local-area network (LAN) to use one set of Internet Protocol (IP) addresses for internal traffic and a second set of addresses for external traffic.

Reference:

J. C. Mackin, and Ian McLean; MCSA/MCSE self-paced training kit (exam 70-291): implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Chapter 2, pp. 2-7 to 2-8.

Dan Holme, and Orin Thomas; MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment , Glossary, pp. G-14.

---

## QUESTION 32

### DRAG DROP

You are designing the migration strategy to meet the business and technical requirements. You need to identify the actions that you should perform to achieve this goal. What should you do?

Move the appropriate actions from the list of actions to the answer area, and arrange them in the appropriate order.



**Actions, select from these**

Create an empty forest root domain
Restructure the cohovineyard domain
Restructure the Paris domain
Restructure the Sydney domain
Upgrade the cohovineyard domain
Upgrade the Paris domain
Upgrade the Sydney domain

**Steps, place here**

Place first step here
Place second step, if any, here
Place third step, if any, here
Place fourth step, if any, here
Place 5th step, if any, here
Place 6th step, if any, here
Place 7th step, if any, here
Place 8th step, if any, here

Answer: >

**Actions, select from these**

Create an empty forest root domain
Restructure the cohovineyard domain
Upgrade the Paris domain
Upgrade the Sydney domain

**Steps, place here**

Upgrade the cohovineyard domain
Restructure the Paris domain
Restructure the Sydney domain
Place fourth step, if any, here
Place 5th step, if any, here
Place 6th step, if any, here
Place 7th step, if any, here
Place 8th step, if any, here

Explanation:

Incorrect Answer:

Upgrade cohovineyard, restructure cohovineyard, upgrade paris

This has to be incorrect, because once you upgrade, you don't need to restructure.

Restructure causes one to use migration tools such as ADMT. Also, if you upgrade Paris, you will end up with a child domain which is incorrect because this case study is a single forest with one domain.

## Topic 4, Litware, Scenario

## Overview

Litware, Inc., is a corporate management company that manages the internal operations for its business customers.

Internal operations include sales, accounting, and payroll.

## Physical Locations

Litware, Inc., has two main offices in the following locations:

1. New York

2. Chicago

Each office has approximately 300 users.

The New York office has a branch office in Boston. The Boston office has approximately 100 users.

Staff in the Boston exclusively office work on projects for customers in the New York office. The Boston office has no customers of its own.

## Planned Changes

As part of its initiative to streamline the IT environment and increase network security, the company has decided to implement a Windows Server 2003 Active Directory environment.

The New York office is currently in negotiations to secure Contoso, Ltd., as a new customer.

## Business Processes

Litware, Inc., manages the business operations for eight business customers. For each customer, Litware, Inc. has a dedicated staff that works exclusively with that customer.

Users require access only to project data for the customers to which they have been directly assigned. The New York and Chicago offices are responsible for their own customers and maintain them separately. Each individual customer project is listed in the following table.

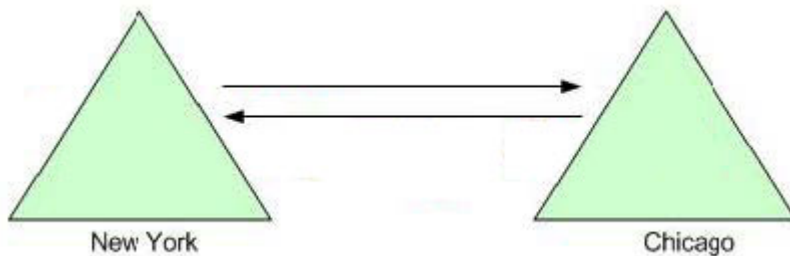
Customers name	Managed by
Alpine Ski House	New York
Baldwin Museum of Science	Chicago
Coho Vineyard	New York
Fabrikam, Inc.	New York
Humongous Insurance	Chicago
Lucerne Publishing	New York
Wingtip Toys	Chicago
Woodgrove Bank	Chicago

The chief information officer is the only person who is authorized to implement any changes that will impact the entire company. Roles and responsibilities in the IT department are shown in the following table.

Job title	Responsibilities	Office
Chief information officer	Approves all major IT decisions, manages the IT budget, functions as liaison between network administrators in the New York and Chicago offices.	New York
Network administrator, New York	Manages the day-to-day operations of the New York and Boston networks. Installs and manages servers and domain controllers	New York
Network administrator, Chicago	Manages the day-to-day operations of the Chicago network. Installs and manages servers and domain controllers.	Chicago
IT support	Provides day-to-day troubleshooting and maintenance of the network. This includes the installation of operating systems for end users and some server configuration. Each office has its own IT support staff	New York, Chicago, Boston
Help desk	Provides telephone support for all users in all offices.	New York

### Directory Services

Currently, Litware, Inc., has two Windows NT 4.0 domains configured as shown in the Existing Domain Model exhibit.

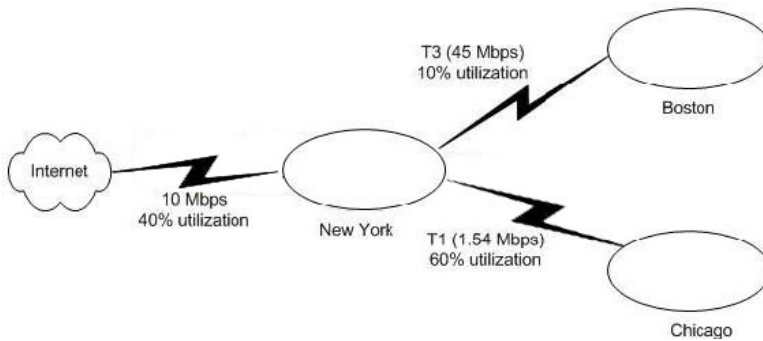


The New York domain contains user and computer accounts for both the New York and Boston offices. The Chicago domain contains user and computer accounts for the Chicago office.

Litware, Inc., users require access only to project data for the customers to which they have been directly assigned. They also require access to internal company resources, such as a time-building application that is hosted in the New York office. Accounting auditors and executives require access to data from all customer projects to perform quarterly reports, account reviews, and billing verifications. Account auditors and executives are located in both New York and Chicago offices, and frequently travel between offices.

### Network Infrastructure

The existing network infrastructure is shown in the Existing Network Infrastructure exhibit.



All Internet access is provided through a proxy server located in the New York office. The proxy server provides Internet name resolution on behalf of the client computers.

Currently, all servers run Windows NT Server 4.0 with the latest service pack installed. A time-billing application is installed on a Microsoft SQL Server computer named SQL1. SQL1 is managed by the network administrators in the New York office, and is accessed by all Litware, Inc., users.

The company's servers, including their domain membership, physical locations, and network functions, are shown in the following table.

Server name	Domain	Office	Functions
DC1	New York	New York	PDC, DHCP server
DC2	New York	New York	BDC, WINS server
DC3	New York	Boston	BDC, DHCP server, WINS server
Fileserver1	New York	New York	Member server, DHCP server, file server
Fileserver2	New York	New York	Member server, WINS server, file server
Fileserver3	Chicago	Chicago	Member server, DHCP server, file server
Fileserver4	Chicago	Chicago	Member server, WINS server, file server
SQL1	New York	New York	Member server, SQL Server computer, time-billing application server

Most required network resources are available locally.

All client computers in the company run Windows 2000 Professional.

### Problem Statements

The following business problems must be considered:

1. Contoso, Ltd., requires that the new Active Directory infrastructure is completely

in place prior to obtaining the contract.

2. Administrative authority for network administrators in the New York and Chicago offices must remain equal.

#### **Chief Executive Officer**

The addition of Contoso, Ltd., as a customer will likely increase annual revenue by 50 percent. Additional funds and resources have been allocated to secure this contract. All efforts should be made to demonstrate to the Contoso, Ltd., representatives that we will address all of their security concerns. This will be done on part though a migration to the Windows Server 2003 Active Directory environment.

Any short-term costs associated with a technology deployment are acceptable if they allow for growth and flexibility in the future.

#### **Chief Information Officer**

A Web-based interface for the time-billing application will be implemented in the near future. The current network administrators in the New York and Chicago offices perform their jobs well.

To reduce the burden on IT staff, trusted individuals within the organization should be identified to help reduce the IT administrative burden.

#### **Office Worker**

We want to be able to access the internal network from our home computers.

#### **Business Drivers**

The following business requirements must be considered:

1. The company wants access to the network to remain easy and intuitive. A company policy now states that user logon names and e-mail addresses should be identical. Currently, each user has an e-mail address made up of that user's first initial and last name, and an additional domain name indicating the region that manages that user's account. For example, the user Nicole Caron from the New York office has the e-mail address of ncaron@ny.litwareinc.com. The user Luis Bonifaz from Chicago has the e-mail address of lbonifaz@chi.litwareinc.com.
2. The domain name litwareinc.com has been registered.
3. To ensure reliability in the event of a single WAN link failure, users should continue to authenticate on the network. Additionally, all domains should be fault tolerant in the event of a single domain controller failure.
4. VPN access will be provided to enable user access to customer data outside of regular business hours. VPN connections will be assigned through the New York office.

#### **Organizational Goals**

The following organizational requirements must be considered:

1. As part of the negotiations between Contoso, Ltd., and the New York office, Litware, Inc., has agreed to ensure that all users who require access to Contoso, Ltd., data must have complex passwords that are a minimum of 10 characters in length.
2. The company has also agreed that management of Contoso, Ltd., data must be completely isolated from all other Litware, Inc., data. This included the ability to manage security of Contoso, Ltd., resources. There will be no exceptions.
3. Planning for other aspects of how Contoso, Ltd., will integrate with the Litware,

Inc., environment is premature at this point. However, a quick migration solution for the existing environment must be identified to allow for this anticipated growth.

4. Litware, Inc., account auditors and executives from the New York and Chicago offices will require limited access to Contoso, Ltd., data.

### **Security**

The following security requirements must be considered:

1. A new Web-based interface will be implemented for the time-billing application running on SQL1. This application will use IIS, and will require the use of IP filtering that uses computer host names for security purposes.
2. Only authorized computers within the internal Litware, Inc., network will be given access to the time-billing application.

### **Active Directory**

The following Active Directory requirements must be considered:

1. The network administrators in the Chicago and New York offices will retain their current responsibilities, such as the management of user accounts, servers, and domain controllers for their regions. There should be no overlap between their administrative authority.
2. There is a need to allow trusted individuals responsible for each customer project to manage user account information. Responsibilities will include the ability to reset passwords and define personal user information on user accounts, such as phone numbers and addresses. The trusted individuals will be allowed to manage only user accounts within the customer project to which they have been assigned.

### **Network Infrastructure**

The following infrastructure requirements must be considered:

1. Users in the Chicago office access Internet-based resources frequently. This Internet-related traffic accounts for most of the bandwidth used between the Chicago and New York offices. Bandwidth utilization between these two offices is currently a cause for concern. Network traffic between the Chicago and New York offices must be minimized whenever possible.
2. Because of the Boston office's data access requirements, a high level of availability and reduced latency between the New York and Boston offices is required. Bandwidth utilization between the Boston and New York offices is minimal and is not a concern in the foreseeable future.
3. A Windows Server 2003 computer will provide VPN access to the network by using both L2TP and PPTP. Usage statistics will be gathered over time to identify which users establish VPN connections to the network, and the duration of their connections. These usage statistics will help the company track trends and plan for future growth.
4. The network administrator in Chicago has extensive knowledge of DNS, and will manage the implementation of the DNS infrastructure for the Litware, Inc., network.
5. The DNS structure must be secured against any unauthorized modifications, but also must be easy to maintain and manage.

## **Topic 4, Litware(9 Questions)**

---



**QUESTION 33**

You are designing a forest and domain structure to address the concerns of Contoso, Ltd., and to meet the business and technical requirements. You want to use the minimum number of domains and forests that are required.

Which domain structure should you use?

- A. One forest and two domains.
- B. One forest and three domains.
- C. One forest and four domains.
- D. Two forests and three domains.
- E. Two forests and four domains.

Answer: E

Explanation:

This question address a concept Microsoft has recently adopted for Windows 2003: isolation vs. autonomy.

The "Organizational Goals" section of the case states:

The company has also agreed that management of Contoso, Ltd. data must be completely isolated from all other Litware, Inc. data. This included the ability to manage security of Contoso, Ltd. resources. There will be no exceptions.

The key phrases in the case are "data must be completely isolated" and "included the ability to manage security". If Contoso becomes a sub-domain or OU in the Litware forest, there will always be higher level administrators (non-client related) who can assign themselves rights to Contoso data. The security boundary for isolation is the forest, and the answer should reflect that.

Use multiple forests when you need to provide support for multiple distinct companies or when you need to provide autonomy or isolation to a unit within a company.

Incorrect Options:

A and C: To provide autonomy or isolation to a unit within a company, you need multiple forests.

B: This option only provides for data autonomy for Contoso, which does not address the case.

D:

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 3, pp. 3-2 to 3-15.

---

**QUESTION 34**

You are designing the top-level organization unit (OU) structure to meet the administrative requirements. What should you do?

- A. Create a top-level OU named New York.  
Place all user and computer accounts from New York in the New York OU.
- B. Create a top-level OU named Chicago.



Place all user and computer accounts from Chicago in the Chicago OU.

C. Create a top-level OU named Coho.

Place all user and computer accounts that are assigned to the Coho Vineyard customer project in the Coho OU.

D. Create a top-level OU named Sales.

Place all user and computer accounts from the sales department in the Sales OU.

Answer: C

Explanation:

The case study states: "To reduce the burden on IT staff, trusted individuals within the organization should be identified to help reduce the IT administrative burden."

In the Active Directory section of the case study it states: "The trusted individuals will be allowed to manage only user accounts within the customer project to which they have been assigned." So we would create OU's for each project and Delegate Authority.

It is for this reason that A, B and D are incorrect.

---

### **QUESTION 35**

You are designing a security group strategy to meet the business and technical requirements.

What should you do?

A. Create one global group named G\_Executives.

Make all executives user accounts members of that group.

B. Create two global groups named G\_Executives and one universal group named U\_Executives.

Make the two global members of U\_Executives.

Make the executive user accounts members of the appropriate global group.

C. Create three global groups named G\_NY\_Executives and G\_Chi\_Executives and G\_Executives.

Make G\_NY\_Executives and G\_Chi\_Executives members of G\_Executives.

Make the executive user accounts members of the appropriate global group.

D. Create one domain local group named DL\_Executives.

Make all executive user accounts members of that group.

Answer: B

Explanation:

Global groups are used to gather users that have similar permissions requirements. One of its characteristics is they can be assigned permissions or be added to local groups in any domain in a forest. We have already established the need for two forests, so we also need two global groups because each forest can have only one global group.

Universal groups are normally used to assign permissions to related resources in multiple domains. Universal groups share the following characteristics:

1. Universal groups are available only when the forest functional level is set to Windows 2000 native or Windows Server 2003.

2. Universal groups exist outside the boundaries of any particular domain and are managed by Global Catalog servers.

1. Universal groups are used to assign permissions to related resources in multiple domains.

2. Universal groups can contain users, global groups, and other universal groups from any domain in a forest.

3. You can grant permissions for a universal group to any resource in any domain.

Incorrect Options:

A and C: Global groups cannot be applied across forests.

D: Domain local groups exist on domain controllers and are used to control access to resources located on domain controllers in the local domain.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 4, pp. 4-27 to 4-28.

---

### **QUESTION 36**

You are designing an Active Directory implementation strategy to present to executives from your company and from Contoso, Ltd.

Which implementation strategy should you use?

A. Upgrade the New York domain.

Upgrade the Chicago domain.

Create a pristine forest for Contoso, Ltd.

B. Create a pristine forest.

Upgrade the New York domain.

Upgrade the Chicago domain.

Do nothing further.

C. Create pristine forest.

Upgrade the New York domain.

Upgrade the Chicago domain.

Create a pristine forest for Contoso, Ltd.

D. Create a pristine forest.

Upgrade the New York domain.

Upgrade the Chicago domain.

Create a new child domain for Contoso, Ltd.

Answer: C

Explanation:

The case study states: "...the company has decided to implement a Windows Server 2003 Active Directory environment." It also says that "Currently, Litware, Inc. has two Windows NT 4.0 domains..."

The Active Directory Installation Wizard simplifies upgrading a Windows NT domain to Windows Server 2003 Active Directory. The Active Directory Installation Wizard installs and configures domain controllers, which provide network users and computers

access to the Active Directory directory service. Any member server (except those with restrictive license agreements) can be promoted to domain controllers using the Active Directory Installation Wizard. During this process you will define one of the following roles for the new domain controller:

1. New forest (also a new domain)
2. New child domain
3. New domain tree in an existing forest
4. Additional domain controller in an existing domain

By creating two new forests, you are providing isolation and. This satisfies the organizational requirements.

Incorrect Options:

A and D: To provide autonomy or isolation to a unit within a company, you need multiple forests.

B: This option only provides for data autonomy for Contoso, which does not address the case.

Reference:

Jerry Honeycutt; Introducing Microsoft Windows Server 2003, Microsoft Press, Chapter 16.

---

### **QUESTION 37**

You are designing the DNS infrastructure to meet the business and technical requirements.

What should you do?

- A. Create an Active Directory-integrated zone on DC4.  
Set the replication scope to all DNS servers in the domain.
- B. Create an Active Directory-integrated zone on DC5.  
Set the replications scope to all DNS servers in the forest.
- C. Create an Active Directory-integrated zone on any domain controller in the forest root domain.  
Set the replication scope to all domain controllers in the domain.
- D. Create a standard primary zone on DC4
- E. Create a standard primary zone on any domain controller in the forest root domain.

Answer: B

Explanation:

The answers refer to a DC4 and DC5 which do not exist in the scenario - a diagram or chart of some kind is missing. However, answer C does not make any sense. Typically you will store the root domain DNS info in AD (AD-I zone) and set the replication to Forest DNS Zones, i.e., to all DCs with DNS in the forest, especially the msdcs subdomain, found in the root domain. Based on that simple fact, the answer is B, assuming that DC5 is in the root domain of the forest.

You can control the replication scope of Domain Name System (DNS) zone data stored in Active Directory so that only specific domain controllers in the forest participate in DNS zone replication.

Reference:

Jerry Honeycutt; Introducing Microsoft Windows Server 2003, Microsoft Press, Chapter 16.

---

**QUESTION 38**

You are designing a DNS implementation strategy for the network.

Which two zone types should you use? (Each correct answer presents part of the solution. Choose two)

- A. Reverse lookup zones
- B. Standard primary zones
- C. Standard secondary zones
- D. Active Directory-integrated zones

Answer: A, D

Explanation:

Reverse lookup zones provide IP and Hostname restrictions for IIS.

Active Directory-integrated zones are fault tolerant and secure.

Incorrect Options:

C: This zone type is usually implemented when there is UNIX or older DNS systems in place.

D: Secondary zones can increase fault tolerance and availability, but zone transfer traffic can consume unacceptable amounts of bandwidth in some circumstances.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 6, pp. 6-15.

Martin Grasdahl, Laura E. Hunter, and Michael Cross; Planning and Maintaining a Windows Server 2003 Network Infrastructure: Exam 70-293 Study Guide & DVD Training System, Syngress, Chapter 6, pp. 469.

---

**QUESTION 39**

You are designing a strategy to upgrade the DHCP servers after the new Active Directory structure is in place.

Who can authorize the DHCP servers? (Choose all that apply)

- A. Chief information officer
- B. IT support staff in Boston
- C. IT support staff in New York
- D. Network administrator in Chicago
- E. Network administrator in New York

Answer: A

The case study states: "The chief information officer is the only person who is authorized to implement any changes that will impact the entire company."

---

**QUESTION 40**

You are designing the placement of the global catalog servers. You want to use the minimum number of global catalog servers that are required.

Which design should you use?

- A. One global catalog server in New York.
- B. Two global catalog servers in New York.
- C. One global catalog server in Chicago and one global catalog server in New York.
- D. Two global catalog servers in Chicago and two global catalog servers in New York.
- E. One global catalog server in Chicago, one global catalog server in New York, and one global catalog server in Boston.

Answer: E

Explanation:

The "Network Infrastructure" section of the case states that Boston requires high availability and reduced latency. The only way to achieve these goals is to give them their own GC which would process logons locally (universal group membership needs to be checked during logon), instead of contacting a GC in the NY office. An argument could be made that a DC in the Boston office could have universal group membership caching enabled, thus removing the requirement for a local GC, but this was not an option in the answer matrix.

---

**QUESTION 41**

You are designing an IP addressing strategy for your VPN solution.

How many public addresses should you use?

- A. 1
- B. 25
- C. 50
- D. 255

Answer: A

Explanation:

VPN connections will be assigned through the New York office.

## **Topic 5, Certkiller .com, Scenario**

### **Overview**

Certkiller .com is a new Government-funded organization, established to consolidate medical research performed at universities in to a single electronic library.

The Company has been allocated a large budget to start the project, and more funds will be made available as more universities integrate their research with Certkiller .com.

### **Physical Location**

The Company has one office located in Dallas. The Office currently has 100 users.

### **Planned Changes**

A New Office in Seattle will be opened soon. The Seattle office will have 100 users when it opens. An additional 100 users will be hired in the Dallas office over the next year. The number of users is expected to grow by 60 percent over the next five years.

An external Network will be established to allow universities to share medical research. At launch, the user population will be minimal. It is expected that the external network will have more than 10,000 active users in the next two years.

### **Business Processes**

Certkiller .com will reorganize its internal staff to include the following departments:

1. Accounting
2. Administration
3. Information Technology(IT)
4. Knowledge Management
5. Marketing
6. Projects

The Project department will work directly with universities to help them integrate data with Certkiller .com.

A separate project team will be dedicated to each university that partners with the Company. This project team is in charge of making external security available, creating user accounts, and establishing security for the university whose resources are made available through the Company's external network.

The Company has a small internal IT staff that manages internal resources for internal users. The internal IT staff includes a network administrator and technical support team.

The external network will have its own IT staff. This IT staff will include a network administrator, a technical support team, and a development team. External and internal resources will be managed independently.

Internal users will require access to data located on both the internal network and the external network. External users and partners from universities will have access only to external resources. Under no circumstances will external users be given access to internal resources. This includes the external IT staff.

### **Infrastructure**

#### **Directory Services**

To provide a quick solution to allow for information sharing, an unplanned Windows 2000 network was established when the company was first established.

A Windows 2000 Active Directory Environment was implemented with the domain name of research.com and the NetBIOS domain name of research. The domain name research.com has been registered by another organization and this name is not available to the company. The domain contains two domain controllers. A single file server exists on the network to store shared data for the internal users.

#### **Network Infrastructure**

The company has a 10-Mbps Internet connection. The use of the Internet connection is minimal at present, but is expected to grow once external resources are made available to universities.

### **Problem Statements**

The Following business problem must be considered:

1. The Current internal network was not properly planned and need to be completely redesigned.
2. Information such as user accounts must be migrated from the current environment to a new Windows Server 2003 Active Directory Environment.
3. A clean separation must exist between external and internal resources.

#### **Chief Executive Officer**

Funding for Certkiller .com has been finalized and it is time to move forward with the design and implementation of the internal and external network. A stable environment that has the ability to grow is of at most importance for the external network.

#### **Chief Information Officer**

The internal and external networks will have very different needs and audiences. For that reason, we have decided to have a separate IT staff to manage each network. Access to internal resources will be made available to internal users only. Planned VPN access will allow internal users access to internal data while traveling. A Microsoft Exchange server 2003 deployment will be implemented for internal users with a dedicated Exchange Server 2003 computer in each office. To avoid confusion, all internal users need to be able to gain access to both internal & external resources by using a single set of credentials. Internal users should not be prompted for alternate credentials when accessing external resources.

During the migration, internal users must have access to resources in the existing domain. We do not want to manually redefine the security on existing resources.

#### **Network Administrator**

I will manage server deployment and configuration for all external resources. Technology decisions and implementation done for the internal network should not affect me.

My technical support team will manage day-to-day server maintenance. The development team will deploy a knowledge management patrol to streamline information sharing with external partners.

Project teams for the internal network will help in the management of security and will be given strict security areas in which they will be able to manage security for their specific university. The project teams will manage the data security and create user accounts for the university they are managing.

#### **Business Requirements**

##### **Business Drivers**

The following business requirements must be considered:

1. Certkiller .com has registered the domain name treyresearch.com. Internal and External naming needs to be intuitive and easy to manage. Internal and external naming will be managed independently.
2. No new domain names will be registered, and naming decisions must not cause conflicts with any Internet hosts.
3. The naming strategy for the external resources must be as short as possible to make it easy for external partners to access.
4. The company already has a small web site accessible at [www.treyresearch.com](http://www.treyresearch.com)
5. The company will require two domain controllers in each office. A single domain



controller failure or WAN link failure between the Dallas and Seattle offices must not affect the operations of the Exchange Server 2003 environment.

### **Organizational Goals**

The following Organizational requirements must be considered:

1. External users will only require access to a server named web1. Web1 will provide a web interface to the external users and retrieve resources from other external servers. External resources for universities will be provided by using HTTPS.
2. All external users who require access to resources will require a username and password to gain access to the external resources.
3. Web1 will also host the interface for the public web site. Anonymous access will be provided for the public web site.
4. Internal users will be granted VPN access by connecting to VPN1.
5. Domain based DFS servers will be implemented in the Dallas and Seattle offices. DFS replication must not occur during regular business operation. DFS replication must occur between the hours of 9:00 P.M. and 5:00 A.M Central Time.
6. Users in each office should automatically be redirected to the DFS server in their current physical location. In the event of a single DFS server failure, users should be automatically redirected to an available DFS server.

### **Security**

The following security requirements must be considered:

1. To maintain the security of both the internal network and the external network, only traffic that is required by the company to meet its goal will be allowed to pass through the perimeter firewall.
2. All other traffic must be blocked.

### **Technical Requirements**

#### **Active Directory**

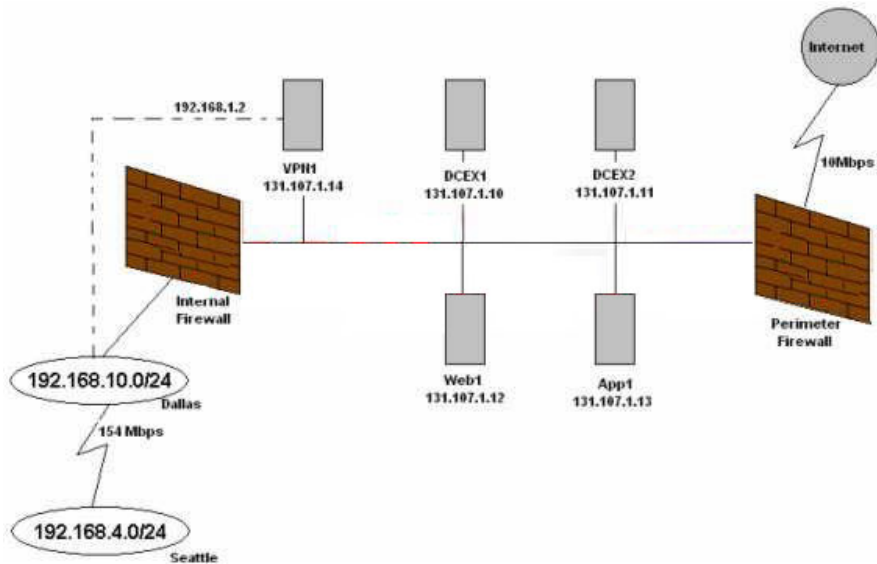
The following Active Directory requirements must be considered:

1. External and Internal resources must be managed independently. This includes high-level modifications to the directory service, such as the installation of Exchange Server 2003 or other directory aware applications.
2. During the first two years, many new users will be added to the network. To provide a consistent environment, the replication of internal domain user accounts must occur within a maximum time delay of one hour between the Dallas and Seattle offices.

#### **Network Infrastructure**

The following infrastructure requirements must be considered:

The network infrastructure will be configured as shown in the planned network infrastructure exhibit.



1. The internal DNS structure must be secured to prevent unauthorized systems from registering their names with DNS.
2. To reduce the impact that name resolution of Internet based resources might have on WAN links, a solution must be identified that allows name resolution to occur without generating excessive and unnecessary traffic. A single domain controller in each office will be configured as a DNS server.
3. A single DHCP server will be present at each office. The DHCP server will configure local client computers to have the appropriate IP settings, including the address of a local DNS server. All users accessing the internal network must receive their IP configurations from one of these DHCP servers.
4. An external DNS server will be required to perform only name resolution for the namespace treyresearch.com. It will not be allowed to resolve any other name for external users, including names of other Internet based hosts.

### Topic 5, Certkiller .com (14 Questions)

#### QUESTION 42

You need to identify the features that will be available immediately after the domain migration to the new environment is complete. Which feature or features will be available? (Choose all that apply)

- A. Global group nesting.
- B. Universal group nesting.
- C. Domain local group nesting.
- D. Universal security groups.
- E. Sid history attributes.

Answer: A, B, C, D, E  
They all will be available.

**QUESTION 43**

You are designing a NetBIOS naming strategy for the internal domain. What are two possible NetBIOS domain names you can use to achieve your goal? (Each correct answer presents a complete solution.) (Choose two)

- A. ad
- B. dallas
- C. internal
- D. external
- E. Research

Answer: A, C

Explanation:

Internal is an appropriate name for an internal domain. "A" ad makes as much sense as "C".

Incorrect Options:

B: Dallas would not correctly represent the internal name since it refers to a location rather than a domain .

D: The question says you are designing a NetBIOS naming strategy for the INTERNAL domain. So an internal domain name of external is very misleading.

E: Research as we know from the case study is already registered by a different company, and MS does not recommend creating an internal domain name with someone else's registered domain name.

---

**QUESTION 44**

**DRAG DROP**

You are designing a strategy for performing the migration of the internal network. You need to identify the actions that you should perform to achieve this goal. What should you do?

To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the appropriate order. (Use only actions that apply.)

Select from these

Steps, place here

- Create a Pristine forest
- Create a new child domain
- Change the Domain functional level
- Migrate User Accounts
- Migrate Computer Accounts
- Establish an external trust relationship

Place first step here

Place second step, if any, here

Place third step, if any, here

Place fourth step, if any, here

Place 5th step, if any, here

Place 6th step, if any, here

Answer:

**Steps, place here**

Create a Pristine forest

Establish an external trust relationship

Change the Domain functional level

Migrate Computer Accounts

Migrate User Accounts

*Place 6th step, if any, here*

Explanation:

A migration is accomplished by creating a new pristine Active Directory on a new server. Then, you use a migration tool to copy the domain information from your old domain to your new one. Here are some of the advantages of this method:

1. Migration is gradual. You can migrate one department at a time.
2. Accounts are copied rather than moved, so you can return to the old domain if necessary.
3. You avoid the complexity of taking existing database bugs and moving them into your new Active Directory.
4. You can re-evaluate your existing domain structure and consolidate or expand your domains, as you deem necessary.

Reference:

Michael Cross, Jeffery

A. Martin, and Todd

A. Walls: MCSE: Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory Infrastructure Study Guide & DVD Training System, Syngress, Chapter 7, pp. 501.

---

### **QUESTION 45**

You are designing the site topology for the internal domain. Which action or actions should you perform? (Choose all that apply.)

- A. Create a Single Site.
- B. Create a site for each physical location.
- C. Set the replication interval on the default IP site link to 60 Minutes.
- D. Configure the schedule of the default IP site link to only allow replication between the hours of 9:00 P.M and 5:00 A.M
- E. Configure the schedule of the default IP site link to only allow replication between the hours of 3:00 A.M and 11:00 A.M

Answer: B, D

Explanation:

The "How DFS Works - Storage Services: Windows Server 2003" white paper states the

following:

The DFS object stores the DFS metadata for a domain-based namespace. The DFS object is created in Active Directory when you create a domain -based root, and Active Directory replicates the entire DFS object to all domain controllers in a domain.

One of the goals in the case study says: "DFS replication must occur between the hours of 9:00 PM and 5:00 AM."

And since DFS is replicated with AD, you can't set the replication interval to every 60 minutes.

---

**QUESTION 46**

You are designing the DNS name resolution strategy for the internal network. What should you do?

- A. Configure all internal DNS servers to use the default root hints.
- B. Disable recursion on the DNS server in Seattle. Configure the Seattle DNS to use Dallas DNS server as a forwarder.
- C. Create a root zone on the DNS server in Dallas. Configure the Seattle DNS server to use the Dallas DNS server as a forwarder.
- D. Create a root zone on the DNS server in both Dallas and Seattle.

Answer: B

Explanation:

When forwarders are configured this way in combination with disabling recursion, the local DNS server is known as a slave server because in these cases, it is completely dependent on the forwarder for queries that it cannot resolve locally.

When to Use Forwarders

In some cases, network administrators might not want DNS servers to communicate directly with external servers. For example, if your organization is connected to the Internet by means of a slow wide area link, you can optimize name resolution performance by channeling all DNS queries through one forwarder. Through this method, the server cache of the DNS forwarder has the maximum potential to grow and reduce the need for external queries.

Reference:

J.C. Mackin, and Ian McLean: MCSA/MCSE self-paced training kit (exam 70-291):implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Microsoft, Chapter 5, pp. 5-3 to 5-7.

---

**QUESTION 47**

You are designing a strategy to allow users to gain VPN access to the internal network. What should you do?

- A. Allow all inbound VPN traffic to pass through the internal firewall and the perimeter firewall.
- B. Allow all inbound VPN traffic to pass through the perimeter firewall only.
- C. Allow all VPN traffic from the source IP address of 131.107.1.14 to pass through the

internal firewall.

D. Allow all VPN traffic from the source IP address of 191.168.1.0/24 to pass through the perimeter firewall.

Answer: B

Explanation:

The case study states: "Planned VPN access will allow internal users access to internal data while traveling." It also states: "Internal users will be granted VPN access by connecting to VPN1." According to the planned network infrastructure exhibit, VPN1 is located inside the perimeter firewall and outside the internal firewall. So, for the internal users to access VPN1 while traveling, VPN traffic has to be allowed through the perimeter firewall only.

---

**QUESTION 48**

You are designing a strategy to allow internal users in Dallas to resolve domain names. What are three possible ways to achieve the goal? (Each correct answer presents a complete solution. Choose three)

- A. Configure the internal DNS server to have a root zone.
- B. Configure the Dallas DNS server to use the default root hints.
- C. Configure the Dallas DNS server to forward all request for the external namespace to the external DNS server.
- D. Create a caching-only DNS server on the perimeter network.
- E. Create a stub zone for the external namespace on the Dallas DNS server.

Answer: B, C, E

Explanation:

To perform recursion properly, the DNS server first needs to know where to begin searching for names in the DNS domain namespace. This information is provided in the form of root hints, a list of preliminary resource records used by the DNS service to locate servers authoritative for the root of the DNS domain namespace tree.

A common use of forwarding is to allow DNS clients and servers inside a firewall to resolve external names securely. When an internal DNS server or client communicates with external DNS servers by making iterative queries, normally the ports used for DNS communication with all external servers must be left open to the outside world through the firewall. However, by configuring a DNS server inside a firewall to forward external queries to a single DNS forwarder outside your firewall, and by then opening ports only to this one forwarder, you can resolve names without exposing your network to outside servers.

A stub zone is a copy of a zone that contains only the resource records needed to identify an authoritative DNS server. An authoritative DNS server is a server that hosts resource records for a particular DNS zone. Rather than a DNS server having to query the Internet to locate an authoritative DNS server, the DNS server can simply refer to the list of name servers (NS resource records) in the stub zone. Distributing a list of authoritative DNS

servers for a zone can be implemented by using stub zones. Unlike secondary zones, which primarily are used for redundancy and load-balancing reasons, stub zones are used to improve name resolution performance.

Reference:

J.C. Mackin, and Ian McLean: MCSA/MCSE self-paced training kit (exam 70-291): implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Microsoft, Chapter 4, pp. 4-19, and Chapter 5, pp. 5-6.

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 6, pp. 6-26.

---

**QUESTION 49**

You are designing the IP address assignment strategy for the VPN users. Which two actions should you perform.(Each correct answer presents part of the solution.  
(Choose two)

- A. Configure VPN1 as a DHCP Relay Agent.
- B. Configure VPN1 to assign IP Address by using DHCP server.
- C. Configure VPN1 to have a static pool of IP Address from the network address of 131.107.1.0/24.
- D. Configure VPN1 to have a static pool of IP Address from the network address of 192.168.1.0/24.
- E. Configure the perimeter firewall to allow inbound DHCP traffic to be passed to VPN1.
- F. Configure the interval firewall to allow DHCP broadcasts to be forwarded from the external network to the internal network.

Answer: A, B

Explanation:

DHCP Relay Agent is a routing protocol configured in Routing and Remote Access that allows DHCP clients to obtain an IP configuration from a DHCP server on a remote subnet.

Reference:

J.C. Mackin, and Ian McLean: MCSA/MCSE self-paced training kit (exam 70-291):implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Microsoft, Chapter 9.

---

**QUESTION 50**

You are designing the configuration of the external DNS server to meet the business and technical requirements. What should you do?

- A. Configure a root zone on the external DNS server.
- B. Configure a stub zone for.com on the external dns server.
- C. Configure the external DNS server to use the default root hints.
- D. Configure the External DNS server to use the ISP'S DNS server as a forwarder.

Answer: A



---

**QUESTION 51**

You need to identify the types of inbound traffic that should pass through the perimeter firewall while maintaining the security of the network. Which inbound traffic should be allowed? (Choose all that apply?)

- A. VPN Traffic
- B. DNS Traffic
- C. LDAP Traffic
- D. HTTP Traffic
- E. HTTPS Traffic
- F. Traffic from the network address of 192.168.10/24

Answer: A, C, D, E

Explanation:

The case study states: "Planned VPN access will allow internal users access to internal data while traveling." It also states: "Internal users will be granted VPN access by connecting to VPN1." According to the planned network infrastructure exhibit, VPN1 is located inside the perimeter firewall and outside the internal firewall. So, for the internal users to access VPN1 while traveling, VPN traffic has to be allowed through the perimeter firewall only.

Lightweight Directory Access Protocol (LDAP) is the primary access protocol for Active Directory. LDAP is an industry-standard protocol, established by the Internet Engineering Task Force (IETF), which allows users to query and update information in a directory service. Active Directory supports both LDAP version 2 and LDAP version 3. Hypertext Transfer Protocol (HTTP) is the method by which Web pages are transferred over the network.

Reference:

J.C. Mackin, and Ian McLean: MCSA/MCSE self-paced training kit (exam 70-291):implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Microsoft, Glossary, pp. G-20.

Dan Holme, and Orin Thomas: MCSA/MCSE Self-Paced Training Kit (Exam 70-290):Managing and Maintaining a Microsoft Windows Server 2003 Environment, Microsoft, Glossary, pp. G-10.

---

**QUESTION 52**

You are designing a strategy to ensure that VPN users are able to access all internal resources. What should you do?

- A. Specify a static routing table entry on VPN1 for the Dallas network.
- B. Specify a static routing table entry on VPN1 for the Seattle network.
- C. Implement Internet Authentication Service (IAS) on VPN1.
- D. Define a User Class option for Routing & Remote Access Clients on the DHCP Server.

Answer: C

Explanation:

Internet Authentication Service (IAS) is the Microsoft implementation of a Remote Authentication Dial-In User Service (RADIUS) server and proxy in Microsoft (r) and Windows Server 2003; Datacenter Edition. As a RADIUS server, IAS performs centralized connection authentication, authorization, accounting, and auditing (AAAA) for many types of network access, including wireless, authenticating switch, dial-up and virtual private network (VPN) remote access, and router-to-router connections. As a RADIUS proxy, IAS forwards authentication and accounting messages to other RADIUS servers. IAS supports the Internet Engineering Task Force (IETF) standards for RADIUS described in RFC 2865 and RFC 2866.

Since both Dallas and Seattle will be in the same domain and utilize the same DNS server there is nothing special that needs to be done to allow VPN users (once authenticated via IAS) access to all internal resources.

Reference:

<http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/techref/en-us/Default.asp?url=/Resources/Docu>

---

### **QUESTION 53**

You are designing a strategy to migrate user accounts. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. Change the functional level.
- B. Create an external trust relationship.
- C. Run adprep to prepare the research.com forest.
- D. Run adprep to prepare the research.com domain.

Answer: A, B

Explanation:

The target domain must be running in either Windows 2000 Native or Windows Server 2003 functional level. This is required because SID History cannot be stored in a classic SAM, so all BDCs must be off the wire.

In this case, we are migrating from Windows 2000 to Windows Server 2003.

The source domain must trust the target domain. This ensures that the ADMT agent has the proper security context.

Incorrect Options:

C and D: adprep is used for in-place upgrades.

Reference:

William Boswell: Inside Windows(r) Server 2003, Addison Wesley, Chapter 9.

---

### **QUESTION 54**

**DRAG DROP**

You are designing a naming strategy for the new internal and external domains.

You need to identify the appropriate domain name for each domain. What should

you do?

To answer, drag the appropriate domain name or names to the correct location or locations in the work area.

Domain name, select from these

research.com

ad.research.com

certkiller.com

ad.certkiller.com

Internal Windows Server 2003 domain

External Windows Server 2003 domain

Place here

Place here

Answer:

Domain name, select from these

research.com

ad.research.com

certkiller.com

ad.certkiller.com

Internal Windows Server 2003 domain

External Windows Server 2003 domain

research.com

certkiller.com

Explanation:

The case states: "A Clean separation must exist between external and internal resources." As well as, "Under no circumstances will external users be given access to internal resources. This includes the external IT staff."

This would indicate Isolation separate forest is the security boundary, therefore separate root domains are a must as is stated in the deployment guide.

The case also states: "During the migration, internal users must have access to resources in the existing domain. We do not want to manually redefine the security on existing resources."

Therefore we must maintain research.com. Providing access for internal users to external resources can be done with external trusts.

[http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dssbc\\_logi\\_lcbx.asp](http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dssbc_logi_lcbx.asp)

---

### QUESTION 55

You are designing the top-level OU structure for the external domain. On which factor/s should you base the top-level OU structure?

- A. Physical locations
- B. External partners and universities
- C. The company's internal departments
- D. The company's software deployment needs

Answer: B

Explanation:

The case study states: "External users and partners from universities will have access only to external resources."

## **Topic 6, Fourth Coffee, Scenario**

### **Overview**

Fourth Coffee is company that specializes in the retail sale of packaged coffee. The Company has more than 500 retail outlets throughout the United States.

### **Physical Location**

The Company's main office is located in Atlanta. The Company has six branch offices in the following locations:

1. Boston
2. Chicago
3. Dallas
4. Denver
5. Los-Angeles
6. Seattle

Each Branch office manages at least 60 retail outlets.

### **Planned Changes**

The company plans to upgrade the network to make provision for future expansion of the company product line. This will be the first upgrade in six years.

### **Business Processes**

The Atlanta office manages the six branch offices, as well as the retail outlets in the Atlanta area. The branch offices manage the retail outlets in their respective cities and regions. Some of the very large retail outlets have managers who are responsible for daily reporting. Each of those managers has a desktop computer for the purpose of creating reports.

A single group of network administrators, located in the Atlanta office, controls all network resources and access. Two employees per branch office have been trained to assist the administrative group by performing tasks from the branch office whenever necessary.

In each branch office a point-of-sale application, named the retail outlet employees of sale application, is installed on servers that run Windows NT 4.0 Terminal Server Edition. The Retail outlet employees currently do not have access to any other applications.

Employees in the Atlanta office and the branch offices work between the hours of 8:00 A.M and 5:00 P.M, Monday through Friday. The network administrators are required to work on weekends to support the retail outlets. Employees in the retail outlets work in two shifts between the hours of 6:00 A.M and 11.00 P.M.

## Infrastructure

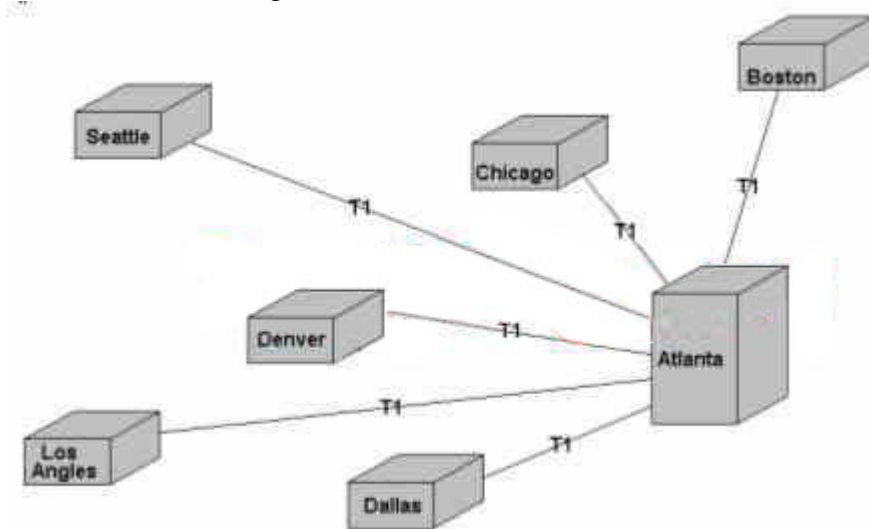
### Directory Services

The network consists of a single Windows NT 4.0 Domain named Fourth coffee. One PDC and Three BDC's are located in the Atlanta Office.

Each branch office has a BDC. The Domain Controllers are not used for any other network service. Each group has been named for the function of the Group. For example, the group name of the users in the finance department of the Atlanta office is Atlanta Finance Users.

### Network Infrastructure

The network connections between the Atlanta office and the branch offices are shown in the Existing Network Infrastructure exhibit



The Atlanta office and the branch offices have 100-Mbps Ethernet networks. Each retail outlet connects to the associated branch office by using a fractional T1 line with a committed rate of 256 kbps or greater.

All WAN links are reliable. There is an agreement between Fourth Coffee and its telecommunications provider to have any WAN failure resolved within one hour. The amount of bandwidth currently seems to be sufficient during business hours. The Atlanta office and the branch offices have servers running Windows NT Server 4.0, Terminal Server Edition. The number of servers per office is based on the number of retail outlets that connect to the Atlanta office or branch offices, and the number of terminals at the retail outlets. The distribution of servers is shown in the following table.

Office	Number of Users	Number of Outlets	Number of Terminal Services	Number of Terminals	Number of File and Print Servers
Atlanta	300	90	7	172	3
Boston	100	80	6	153	1
Chicago	100	60	4	115	1
Dallas	100	60	4	115	1
Denver	180	75	5	144	1
Los Angeles	150	75	5	144	1
Seattle	180	65	5	125	1

Only one of the terminal servers in Atlanta, running Windows NT Server 4.0, is dedicated to the finance department.

The other six terminal servers are available to be used by the retail outlets. No

other servers or operating systems are in use. All company software has been successfully tested on computers that run Windows Server 2003 and Windows XP Professional.

The Company's existing hardware is shown in the following table.

Computer	Processor	Memory	Harddisk Drive
Domain Controller	Pentium 133	64 MB	1.2 G.B
Terminal Server	Pentium 133	96 MB	Two 2.0 G.B
Client Computer	Pentium 90 Or Pentium 100	32 MB	1.0 GB

### **Problem Statements**

The following business problems must be considered:

1. Employees in the branch offices often log on to install software by using local computer accounts rather than domain accounts.
2. IP addresses are configured manually. This leads to incorrectly configured or duplicate addresses on the network.
3. Employees in the retail outlets have been reporting that network performance is slow.
4. Employees with desktop computers do not want to lose their installed application, data and profiles during the changeover.

### **Executives**

#### **Chief Executive Officer**

Fourth Coffee's Expansion will occur as a phased process over the next three years, and we need to use some of our accumulated profits to achieve this.

A new company policy must be enforced to ensure that all company employees have access to similar network services when they are at work.

A market survey has shown that we need to establish a web presence to remain competitive. We need to provide information about what we do, where we are located and what our business hours are.

#### **Chief Information Officer**

The existing network was designed and implemented almost six years ago. Only minor changes have taken place since that time, the only thing that has changed is an upgrade to our WAN links last year. This upgrade did not solve the performance problems experienced by the retail outlets. It has since been established that the performance problems are related to hardware.

With the changes in our product line, we anticipate a growth in the number of customers. This ensures that terminals must be upgraded to provide for the increased connection to our servers from the retail outlets. We do not expect to add a vast number of terminals.

Substantial funds are available for this project. We hope to once again have a network that will last six years without major changes.

#### **Network Administrator**

We have noticed in System Monitor that most servers are running high processor and memory utilization. We currently instruct the retail outlets on which terminal server to connect to, to achieve manual load balancing.

The individual users in the retail outlets must have access to personal data in the new environment. We currently do not have any DNS servers or Internet access available.

Even though I am a newly appointed network administrator, I found that the current management of our groups is incorrect. We use only local groups for the assignment of permissions. This is done by using groups that contain all the users located in the branch offices. Sometimes we may be more specific and focus on the function of the group within the office. Users can also be managed very easily, because we know that almost all of the passwords are "password". Only a few users change their passwords. Complex passwords need to be implemented.

The users at the retail outlets sometimes leave the terminal connected to the application for weeks without disconnecting. This results in failed backups of the application data. All of the users in the branch offices also leave their computers on for long periods of time.

We plan to implement a naming strategy that will identify users by first name, followed by the first character of their surname. Group names will indicate the department, as well as "GG" for global groups or "UG" for universal groups. Domain local groups will be identified by the type of access they will receive.

### **Retail Manager**

We have noticed that the network is gradually becoming slower. No one in the retail outlets has access to e-mail and we do not have Internet access.

All employees in our retail outlet use the same username and password to connect to the terminal server. As a result, we do not have any privacy and cannot even have our own desktop background. Employees in the branch offices have very nice games and other software on their computers that we are not able to access.

### **Business Requirements**

#### **Business Drivers**

The following business requirements must be considered:

1. A Web site, named [www.fourthcoffee.com](http://www.fourthcoffee.com), must be established to enable customers to search for the retail outlet nearest to them.
2. An online ordering system must be established, which will allow customers to order company merchandise online.

#### **Organizational Goals**

The following organizational requirements must be considered:

1. Retail outlets will be expanded over the next three years to provide seating and to allow for increased business. Future expansion might include providing customers with Internet access while they are having their coffee in the store.
2. A manager will be appointed in each retail outlet with the task of improving customer service. The manager's desktop computer will be used by other staff members to access the Internet and their e-mail by using their own usernames and passwords.

#### **Security**

The following security requirements must be considered:

1. All security settings must be equal to or more restrictive than the default Windows Server 2003 settings.
2. As a part of these requirements, all users must be forced to change their passwords at least once a month.
3. Users with desktop computers should no longer be allowed to log on to the local computer as an administrator.



4. The duration of logon hours must be strictly enforced.
5. Users must not be allowed to shutdown the terminal servers.

### **Technical Requirements**

#### **Active Directory**

The following active directory requirements must be considered:

1. The Active Directory design must specify how the management of user and group permissions will be established and maintained.
2. The new design must overcome the existing performance issues and also provide all employees with e-mail and Internet access. Employees in the retail outlets will be allowed to use these services only while they are on their lunch or coffee breaks. Employees will be able to use only their own user accounts for network access.
3. The design must also facilitate the use of Group Policy to control all user accounts within a branch office. Group Policy settings for users in the branch offices must be different from the Group Policy settings for users in the retail outlets.
4. User accounts for users in the finance department must be managed separately.

#### **Network Infrastructure**

The following network infrastructure requirements must be considered:

1. A new T1 WAN link from the Atlanta office to the ISP will be installed.
2. All server computers must have Windows Server 2003 installed. All desktop computers must have Windows XP professional installed. This must be achieved as quickly as possible.
3. All terminal servers in a single office must be configured to use Network Load Balancing. All users must use roaming profiles to ensure that they have a consistent desktop appearance and access to applications. Terminal server user profiles must be stored on a network shared folder. Redundancy for all other servers is required.

### **Topic 6, Fourth Coffee (11 Questions)**

---

#### **QUESTION 56**

You are designing a strategy for configuring a newly installed Windows Server 2003 computer to meet the Active Directory DNS requirements. How should you configure the computer?

- A. As a caching-only DNS servers
- B. As the primary DNS server for the fourthcoffee.com DNS zone
- C. With a stub zone for the fourthcoffee.com DNS zone hosted by the ISP
- D. As a secondary DNS server for the fourthcoffee.com DNS zone hosted by the ISP

Answer: B

Explanation:

Primary DNS servers store original source data for zones. With Windows Server 2003, you can implement primary zones in one of two ways: as standard primary zones, in which zone data is stored in a text file, or as an Active Directory-integrated zone, in which zone data is stored in the Active Directory database

Incorrect Options:

A: A caching-only server does not host a zone, its only purpose is to cache queries so that future requests for the same resource record are done instantly because the results of the previous query are already in cache.

C: A stub zone is a copy of a zone that contains only the resource records needed to identify an authoritative DNS server.

D: Secondary DNS servers are authoritative backup servers for the primary server. The servers from which secondary servers acquire zone information are called masters. A master can be the primary server or another secondary server.

Reference:

Dan Holme, and Orin Thomas: MCSA/MCSE Self-Paced Training Kit: Upgrading Your Certification to Microsoft Windows Server 2003: Managing, Maintaining, Planning, and Implementing a Microsoft Windows Server 2003 environment: Exams 70-292 and 70-296, Microsoft, Chapter 8, pp. 8-25.

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 6, pp. 6-26 and 6-31.

---

**QUESTION 57**

You are designing the forest and domain structure to meet the business and technical requirements.

Which structure should you use?

- A. A single forest with one tree, and one domain
- B. A single forest with one tree two domain
- C. A single forest with two trees, each with a single domain
- D. Two forests, each with a single tree and a single domain
- E. Two forests, each with two trees, with a single domain in each tree.

Answer: A

Explanation:

The case study states: "All security settings must be equal to or more restrictive than the default Windows Server 2003 settings." It also states: "...users must be forced to change their passwords at least once a month."

In a single-domain model, all objects are located within the same security boundaries, so you won't have to worry about planning trust relationships with other domains or implementing cross-domain authentication and permissions. When using a single-domain model, user and group planning is simpler, as is the implementation of group policy. In fact, almost all management functions are simpler-and simpler means less planning, less administration, less troubleshooting, and a lower total cost in the end. Active Directory domains are scalable and can grow much larger than Windows NT domains, which removes a significant obstacle that prevented the use of single-domain networks in structures based on Windows NT, in which the Security Accounts Manager (SAM) could support only up to 40,000 objects in a domain. By contrast, an Active Directory domain can hold more than one million objects.

Incorrect Options:

A: Multiple domains are necessary when you need to implement different domain-level security policies. Certain policies can only be controlled at the domain level. For example, one department may enforce tighter password policies or account lockout policies than another department.

C and D: You might need to implement multiple forests in situations where you are linking two existing separate organizations, creating an autonomous unit or creating an isolated unit.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 3, pp. 3-2 to 3-12.

---

**QUESTION 58**

You are designing a group management strategy for users in the finance department. You need to identify the appropriate changes that need to be made to the current group management strategy. You want to accomplish this goal by using the minimum number of groups. What should you do?

- A. Add the finance users to the financeData group to which the necessary permissions have been assigned.
- B. Add the finance users to the financeGG group to which the necessary permissions have been assigned.
- C. Add the finance users to the financeGG group. Then add the financeGG group to the financeData group to which the necessary permissions have been assigned.
- D. Add the finance users to the financeGG group. Add the financeGG group to the financeUG group to the financeDat group to which the necessary permissions have been assigned.

Answer: B

Explanation:

The question specifies that the minimum number of groups must be used to accomplish this goal, and "B" conforms to it.

---

**QUESTION 59**

You are designing a strategy of enforce the corporate security policy. Which action or actions should you perform? (Choose all that apply.)

- A. Configure a password policy that requires strong passwords
- B. Configure a password policy that requires all users to change their passwords once a month.
- C. Allow users in the branch offices to log on between the hours of 8:00 A.M and 5:00 P.M., Monday through Friday.
- D. Allow users in the retail outlets to log on between the hours of 6:00 A.M and 11:00 P.M., daily.

E. Enable a policy that forces users to log off when their logon hours expire.

Answer: A B, C, D, E

Explanation:

The case study asks for complex passwords to be implemented, and in the process of designing a strong password policy you can select the "Require the use of complex passwords" option.

According to the case study, users must be forced to change their passwords at least once a month.

The case study says: "The users at the retail outlets sometimes leave the terminal connected to the application for weeks without disconnecting. This results in failed backups of the application data. All of the users in the branch offices also leave their computers on for long periods of time."

It also says "The duration of logon hours must be strictly enforced."

Therefore, all actions should be performed.

---

### **QUESTION 60**

You are designing a migration strategy to meet the business and technical requirements. What should you do?

A. Upgrade the fourthcoffee BDC to Windows Server 2003. Then upgrade the PDC to Windows Server 2003

B. Upgrade an existing domain controller to Windows Server 2003. Establish a two-way trust relationship with the fourthcoffee domain.

C. Install and configure a new Windows NT 4.0 BDC. Promote the BDC to a PDC. Then upgrade the PDC to Windows Server 2003

D.

Create a new Windows 2000 Server Active Directory domain. Establish a two-way trust relationship with the fourthcoffee domain. Use the Active Directory Migration Tool (ADMT) to migrate all user and computer accounts.

Answer: C

Explanation:

First, spec out the hardware for a server that is adequate for your domain controller needs. Do a test installation of Windows Server 2003 on this server just to make sure you have no compatibility issues. Make sure you test all the SCSI channels and drives that you will eventually use to store Active Directory files.

Now, wipe the operating system drive on the new server and install NT4 as a BDC in your existing NT domain. Make sure you verify that you get steady replication between this server and the PDC. Leave the new server on the wire for a day or two to check for complications prior to upgrading.

Promote the new server to PDC with User Manager. This automatically demotes the existing PDC to a BDC. Again, let the system bake for a couple of days to make sure everything works as you would expect.

When you're ready to upgrade the domain, start by upgrading the new PDC to Windows Server 2003.

Reference:

William Boswell: Inside Windows(r) Server 2003, Addison Wesley, Chapter 9.

---

**QUESTION 61**

You are designing for implementing Group Policy objects (GPOs) to meet the business and technical requirement. What should you do?

- A. Create one new GPO to enforce software restriction policies. Link this GPO to the domain.
- B. Create one new GPO to enforce software restriction policies. Link this GPO to the appropriate organizational unit (OU).
- C. Create one new GPO to enforce software restriction policies. Link this GPO to all organizational units (OUs).
- D. Create new GPOs to match the number of organizational units (OUs).configure these GPOs to enforce software restriction policies. Link this GPO to its respective OU.

Answer: A

Explanation:

In the problem statements, it states: "Employees in the branch offices often log on to install software by using local computer accounts rather than domain accounts."

Microsoft uses the term Group Policy Object as an umbrella to identify the two components of a group policy: the Group Policy Container and the Group Policy Template. Container objects in Active Directory such as sites, domains, and organizational units (OUs) can be linked to a GPO. This applies the GPO settings to user and computer objects under that container.

A GPC is an Active Directory object that lists the names of the GPTs associated with a particular GPO. Windows clients use the information in a GPC to determine which GPTs to download and process. (Microsoft documentation sometimes uses the terms GPO and GPC interchangeably.)

A GPT is the set of instructions that implements a set of policies. For example, policies that update the Registry are stored in a GPT file called Registry.pol. File-based GPTs are stored in policy folders under the Sysvol folder on each domain controller.

Reference:

William Boswell: Inside Windows(r) Server 2003, Addison Wesley, Chapter 12.

---

**QUESTION 62**

You are designing a DNS name resolution strategy to allow all users access to internal and external web sites. What should you do?

- A. Allow zone transfers to any DNS server.
- B. Create a new stub zone for the DNS zone on the DNS server.
- C. Configure the DNS server to forward all unanswered queries to a DNS server located at the ISP

D. Add the DNS server located at the ISP to the list of name servers for the fourthcoffee.com DNS zone

Answer: C

Explanation:

The question states: "...allow all users access to internal and external web sites."

When a DNS server receives a query, it will first check to see whether it can answer the query authoritatively-that is, on the basis of information contained in a locally configured zone on the server. If it cannot, it will query other DNS servers on the network. In this case it will be a DNS server at the ISP, which is authoritative for external queries.

The process of a DNS server querying other DNS servers on behalf of an original querying client is known as recursion.

Reference:

J.C. Mackin, and Ian McLean: MCSA/MCSE self-paced training kit (exam 70-291):implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Microsoft, Chapter 4, pp. 4-19 to 4-16.

---

### **QUESTION 63**

You are designing a strategy to assign the IP addresses to meet the business and technical requirement. Which two actions should you perform? (Each correct answer presents part of the solution. choose two)

- A. Install and Configure one DHCP server in Atlanta and one DHCP server in each branch office.
- B. Install and Configure two DHCP servers in Atlanta and two DHCP servers in each branch office.
- C. Create one scope on each DHCP server. Specify one DHCP server to always update DNS records. Configure the scope to assign half of the IP addresses available to each office.
- D. Create two scopes on each DHCP server. Specify one DHCP server to update DNS records only for client computers that request it. Specify a second DHCP server to never update DNS records.

Answer: B, C

Explanation:

Dynamic Host Configuration Protocol (DHCP) is an industry standard protocol that lets a server automatically assign IP addresses to clients. This would be one of the problem statements, which says: "IP addresses are configured manually. This leads to incorrectly configured or duplicate addresses on the network."

When you install Windows Server 2003 DHCP service, you can enable the DHCP server to perform updates on behalf of DHCP clients to any DNS server that supports dynamic updates. In other words, DHCP can register the A (host) records and PTR records for all DHCP-enabled clients. DHCP clients can provide their FQDN to the DHCP server, as well as instructions on how it would like the server to process DNS dynamic updates.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 1, pp. 1-39, 6-13.

---

**QUESTION 64**

You are designing a name resolution strategy for the retail outlets to ensure that the existing bandwidth is used efficiently. Which three actions should you perform? (Each correct answer presents part of the solution. Choose three.)

- A. Configure the DNS server service on the terminal servers as caching-only servers.
- B. Configure multiple sites to have site links and set up a specific replication schedule.
- C. Configure the default site to have the subnets of Atlanta and the branch offices.
- D. Create a new DNS zone and configure zone transfers to name servers only.
- E. Create an application partition to be used for DNS
- F. Specify the scope of replication to be used for DNS

Answer: D, E, F

Explanation:

In an incremental zone transfer (IXFR), servers keep track of, and transfer only, changes that are made to resource records in a particular zone, the advantage being that less traffic is sent over the network.

The application partition can be configured to replicate objects to any set of domain controllers in the forest, not necessarily all in the same domain. This partition provides the capability to host data in Active Directory without significantly impacting network performance by providing control over the scope of replication and placement of replicas. Therefore, dynamic data from network services such as Remote Access Service (RAS), RADIUS, Dynamic Host Configuration Protocol (DHCP), and Common Open Policy Service (COPS) can reside in a directory, allowing applications to access them uniformly with one access methodology.

Reference:

Jill Spealman, Kurt Hudson, and Melissa Craft: MCSE Self-Paced Training Kit (Exam 70-294); Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Chapter 5, pp. 5-4.

---

**QUESTION 65**

You are designing a strategy for installing Windows server 2003 on the new domain controllers. Which method should you use?

- A. Unattended installation
- B. Remote Installation Services (RIS)
- C. Automated Deployment Services (ADS)
- D. Microsoft Systems Management Server (SMS)

Answer: A



Explanation:

Examining Plans for Domain Controllers

Special considerations apply if you intend to create domain controllers by using an automated installation method. You cannot configure a Sysprep master computer as a domain controller. You need to first configure a master computer as a stand-alone server, and then install Active Directory by using the Active Directory Installation Wizard (Dcpromo.exe) after the disk image is copied onto a destination computer. However, you can script Dcpromo.exe with an answer file, and you can use the GuiRunOnce entry in your answer file to automatically start it at the end of an Unattended Setup. This is, therefore, a more efficient choice for installing preconfigured domain controllers.

---

**QUESTION 66**

You are designing a strategy to ensure that all employees have Internet access. For each branch office, what should you do?

- A. Configure a DNS server to function as caching-only servers
- B. Configure Internet Connection sharing on terminal servers.
- C. Install and configure an Internet Security and Acceleration (ISA) Server Computer
- D. Install and configure a server running Routing and Remote Access to function as a VPN server

Answer: C

Explanation:

Proxy servers, such as ISA Server 2000, client computers can access Internet resources through the proxy server, which will perform name resolution on their behalf. The proxy server and computers that cannot use the proxy client software need to be configured to use separate, internal DNS forwarders or other DNS servers for Internet name resolution. A proxy server is a firewall component that manages Internet traffic to and from a local area network (LAN) and that can provide other features, such as document caching and access control. A proxy server can improve performance by supplying frequently requested data, such as a popular Web page, and it can filter and discard requests that the owner does not consider appropriate, such as requests for unauthorized access to proprietary files.

Reference:

J. C. Mackin, Ian McLean: MCSA/MCSE self-paced training kit (exam 70-291): implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Microsoft, Glossary, pp. G-26.

## **Topic 7, Consolidated Messenger, Scenario**

### **Overview**

Consolidated Messenger is a transportation and express delivery company serving the continental United States.

The company maintains a commitment to its customers to expedite deliveries within contracted guidelines and offers a 100 percent refund to the customers if the

contract is not fulfilled.

### **Physical Locations**

The company's main office is in Chicago. The company has two branch offices in the following locations:

1. Boston
2. San Diego

### **Planned Changes**

The company is expanding its business into the Asian market by acquiring Contoso, Ltd., which is an Asian import company located in San Francisco. Contoso, Ltd has established relationships with shipping companies and various retail firms in China. Furthermore, Contoso, Ltd. has a strong background in working with the governmental trade protocol in china.

Consolidated Messenger is also planning changes to enable the office and the branch office to work together more effectively.

### **Business Processes**

Consolidated Messenger consists of the following primary departments:

1. Accounting
2. Customer service
3. Delivery
4. Human Resources (HR)
5. Information Technology (IT)
6. Management

The company has a decentralized IT structure. The Chicago office and each branch office have its own IT staff.

Each office maintains its resources separately. Each office is using the same delivery tracking database, named Deliveries, but information is not shared between the three offices.

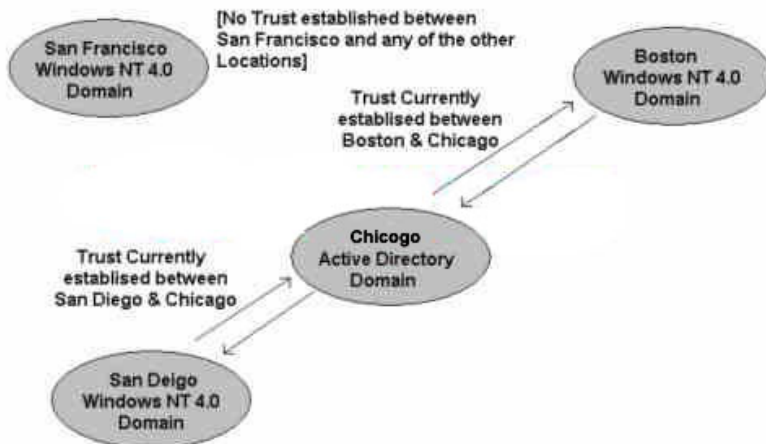
Each office uses an application named TrackingApp to update the tracking database.

Every morning, delivery personnel receive a printed list of deliveries to be made for the day. They can contact the appropriate office for additional information, as needed.

### **Infrastructure**

#### **Directory Services**

The existing domain model is shown in the Existing Domain Model exhibit.



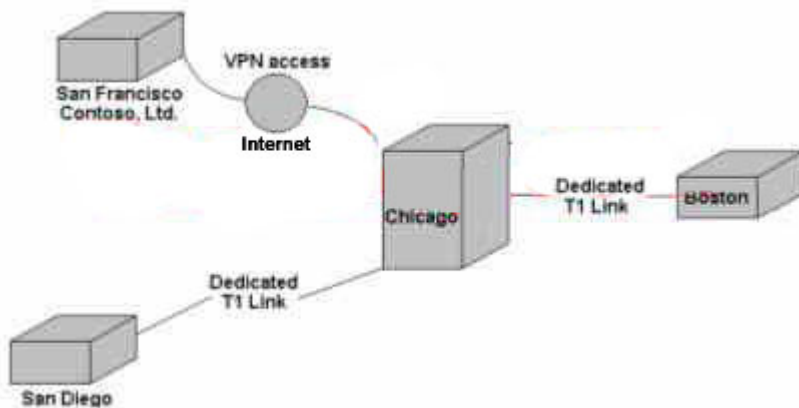
Consolidated Messenger has Windows NT 4.0 domains in the branch offices. The Chicago office has a Windows 2000 Active Directory domain named `ad.consolidatedmessenger.com`

The domain for the Chicago office contains four toplevel organizational units (OUs) named Accounting, Customer Service, Human Resources, and Delivery. The network consists of a single Active Directory site.

Contoso, Ltd., has a Windows NT4.0 domain in its San Francisco office.

#### **Network Infrastructure:**

The company's existing network infrastructure is shown in the Existing Network Infrastructure exhibit.

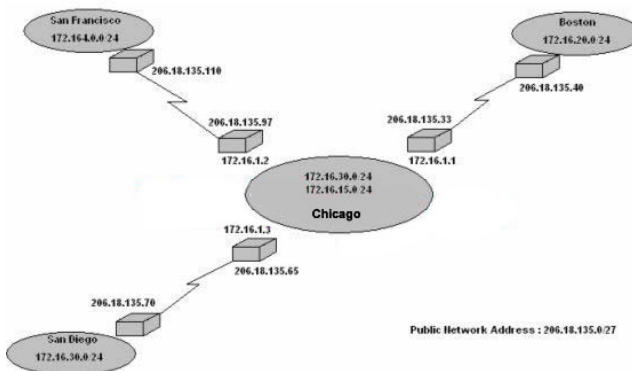


Client computers in the accounting, IT and management departments, at Consolidated Messenger, run either Windows 2000 professional or Windows XP professional. Client computers in the customer service department run windows 98. Client computers at Contoso, Ltd runs either Windows 98 or Windows NT workstation 4.0.

Consolidated Messenger has a web site hosted by an ISP in Chicago. The web site, named `www.consolidatedmessenger.com`, is available for Internet customers to place orders or track deliveries.

Contoso, Ltd., also has a web site, named `www.contoso.com`, which provides information to users about Contoso, Ltd. It is hosted by an ISP in San Francisco. The ISP in San Francisco has DNS on a Unix Server.

The IP address in use for Consolidated Messenger is shown in the Network addresses exhibit.



## Problem Statements

The following business problems must be considered:

1. Consolidated Messenger needs to create a better delivery tracking mechanism for the existing offices. Currently, each office provides point-to-point delivery as orders come in.
  1. They are functioning adequately, but there is room for improved operational efficiency. For example, the Chicago office sometimes delivers into the northeast, which overlaps with the territory of the Boston office. Both the Chicago office and the Boston office might deliver to the west coast, which is the territory of the San Diego office. A centralized database is required to make tracking delivers more efficient.
2. When Consolidated Messenger implements a centralized version of the Delivers database, there must be a way to ensure continuous access to up to date delivery data, regardless of WAN status.
3. Consolidated Messenger wants to provide a better solution for delivery personnel to access information about scheduled deliveries, than printed delivery lists.
4. Consolidated Messenger will need to bring Contoso, Ltd, up to its technology standards. Contoso, Ltd., does not use much technology. Although there is a Windows NT 4.0 domain present, there is a network administrator and there has been a great deal of turnover in this job. As a result, there is not adequate security for its computers. It does not adequately track Shipments, Inventory, Payable, or Receivable. Although Contoso, Ltd. uses a spreadsheet application for its inventory listings it is still primarily a paperbased company.

## Chief Executive Office

With the acquisition of Contoso, Ltd., by Consolidated Messenger, I am concerned that it should be a part of our overall business model, yet remain separate because it is a new venture. This is a positive addition to our current line of business. I want to be sure that have a method for clearly tracking the contributions that Contoso, Ltd., makes to our business.

## Chief Information Officer

I have two major goals for our Deliveries database. First, I want a method for integrating the data between the offices. Second, I want a directory services structure that provides a more straight forward model for maintenance.

I also want an improved user experience when accessing centralized resources in the Chicago office. Additionally, I have strong reservations regarding the inexperience of the new IT staff to be hired in the San Francisco office. I want to make sure that

we are monitoring their activities.

I foresee substantial expenditure for upgrading desktop computers, and salaries for a new IT staff in the Contoso, Ltd., division. We need to provide sufficient access to Contoso, Ltd.; however, we need to spend only the money necessary to achieve this goal.

### **Managers, Contoso, Ltd**

I am unsure if the restrictions imposed by our new parent company will benefit the business of Contoso, Ltd. On the other hand, I fully recognize that being part of a larger company can provide us with more financial stability.

### **Business Requirements**

The following business requirement must be considered:

1. Contoso, Ltd., will be a separate division within Consolidated Messenger, maintaining its line of business because Contoso Ltd., is a new endeavor, Consolidated Messenger has elected to keep the namespace separate so that the internal staff will not be confused.
2. The duplication of effort in maintaining the Deliveries database between Consolidated Messenger branch offices must be reduced.
3. Contoso needs to replace spreadsheets. The database, to be named Inventory, will be created and administered in the Chicago office. The IT staff in the Chicago office will be responsible for the maintenance of this database, and will be replicated from the San Francisco office to the Chicago office. It is anticipated that database replication will exceed the available bandwidth provided by the VPN connection between the San Francisco office and the Chicago office.

### **Organizational Goals**

The following organizational requirements must be considered:

1. Integrating the separate database into a single nationwide database is extremely important to the business.
2. Delivery workers will begin using PDAs to download delivery information from the Deliveries database. As a result, they will discontinue telephone check in for delivery information. As each delivery is completed, the customer will sign the PDA. At the end of each day, the delivery information will be batch uploaded from each PDA to the Deliveries database either from a company office or, if delivery personnel are too far away from a company office, a remote connection.
3. Each office must support wireless access for PDAs

### **Security**

The following security requirements must be considered:

1. Appropriate permissions to trackingapp, the Deliveries database, and other resources will need to be established for users based on that user's job function. Job functions include customer service, delivery personnel, accounting, and management.
2. The IT staff in the Chicago office will audit administrative activity in all domains, particularly in Contoso,Ltd., domain, this includes interactive logons; shutdowns and restarts of domain controllers; changes to security logging; and changes to user and group accounts.

### **Technical Requirements**

#### **Active Directory**

The following Active Directory requirements must be considered:

1. Enterprise Active Directory administration will take place in the Chicago office. Additionally, the IT staff in the Chicago office has the primary responsibilities for administration of the Deliveries database.
2. Each current Consolidated Messenger domain will undergo an in place upgrade. Contoso, Ltd., will be added to the forest, but will maintain its separate namespace. The Contoso, Ltd., domain will be named ad.contoso.com. There will be a single forest design with a minimum number of domains.
3. Upgrading the Windows NT 4.0 domains in the Boston and San Diego offices must be optimized to reduce the need for network administrators to travel between offices.
4. Permissions must be maintained. Additional groups can be created for the Deliveries database, as needed.
5. User and group accounts for Contoso, Ltd. will be recreated. However, desktop settings for Contoso, Ltd., users must be preserved.

#### **Network Infrastructure**

The following Infrastructure requirements must be considered:

1. All Contoso, Ltd., client computers will run Windows XP Professional. Consolidated Messenger has decided to migrate the user settings from the existing Contoso, Ltd., client computers to ease the transition.
2. The Deliveries database is a missioncritical resource for Consolidated Messenger. Database access for the Deliveries databases must be maintained in the event that WAN connectivity is lost.
3. All domain controllers will be configured as DNS servers. Client computers will be configured to point to the local DNS server.
4. DNS zones must be secured.
5. VPNs will be implemented in all locations to support remote access for wireless devices.
6. Remote access policies will be centralized.
7. A single DHCP server will be configured in each office. In the event of a DHCP server failure, client computers must be able to obtain an IP address.

#### **Topic 7, Consolidated Messenger (9 Questions)**

---

##### **QUESTION 67**

You are designing the DNS zone to support the Active Directory domain for Contoso.Ltd. Which two actions should you perform? (Each Correct answer presents part of the solution. Choose two).

- A. Create ad.contoso.com as a standard primary DNS Zone.
- B. Create ad.contoso.com as an Active DirectoryIntegrated DNS Zone.
- C. Enable only authorized client computers to update DNS.
- D. Configure a zone transfer between the DNS server at the ISP and the DNS servers at Contoso.Ltd.

Answer: B, C

**Explanation:**

The case study specifically states that all Domain Controllers are DNS servers and that zones must be secured.

When you are running the DNS server service on a computer that is an Active Directory domain controller and you select the Store The Zone In Active Directory (Available Only If DNS Server Is A Domain Controller) check box while creating a zone in the New Zone Wizard, the server does not create a zone database file. Instead, the server stores the DNS resource records for the zone in the Active Directory database. Storing the DNS database in Active Directory provides a number of advantages, including ease of administration, conservation of network bandwidth, and increased security.

Note: D does not make any sense.

**Incorrect Options:**

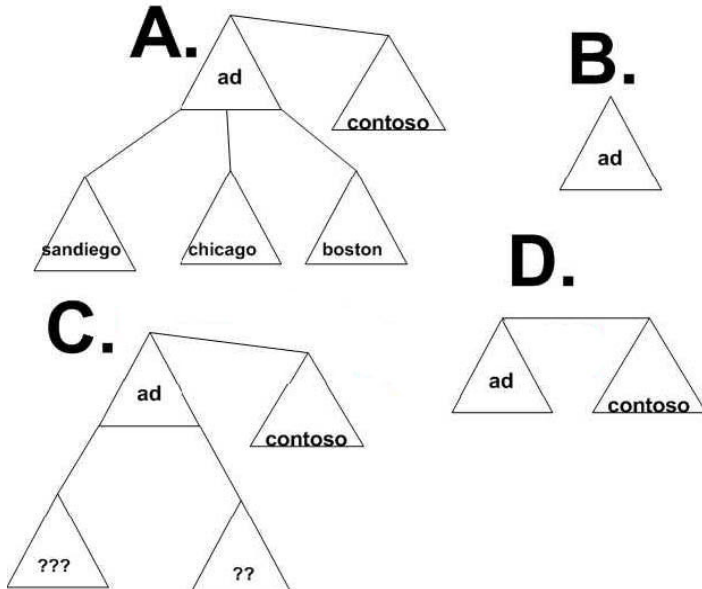
A: This type of zone can be modified, which is not secure.

C: The question speaks about designing a zone, not updates.

**Reference:**

Walter Glenn, and Michael T. Simpson; MCSE 70297 Training Kit Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 1, pp. 124.

Craig Zacker; MCSE SelfPaced Training Kit (Exam 70293): Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Chapter 4, pp. 436.

**QUESTION 68****Exhibit**

You are designing the Active Directory Infrastructure for the new forest to meet the business and technical requirements. What should you do?

- A. Choose forest model A.
- B. Choose forest model B.
- C. Choose forest model C.
- D. Choose forest model D.



Answer: C

Explanation:

According to the Active directory section of the case study Contoso, Ltd., will be added to the forest, but will maintain its separate namespace. This means that the Contoso domain is a domain tree in the single Active Directory forest.

The other two represents the Sandiego and Boston domains.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70297 Training Kit Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 3, pp. 38.

---

**QUESTION 69**

You are designing a strategy for adding the additional hardware necessary to support Contoso, Ltd. What should you do?

- A. Add a T1 Wan Link Between Chicago and San Francisco.
- B. Add a T3 Wan Link Between Chicago and San Francisco.
- C. Add a Basic ISDN Connection between Chicago and San Francisco.
- D. Configure HighSpeed modems in Chicago and San Francisco to support demand-dial routing.

Answer: A

---

**QUESTION 70**

You are designing a client computer upgrade strategy for Contoso.Ltd. What should you do?

- A. Use the ldifde command to migrate user settings.
- B. Use the User State Migration Tool (USMT) to Migrate user settings.
- C. Create trust relationships between the Chicago domain and the San Francisco domain. Use the Active Directory Migration Tool (ADMT) to migrate user settings.
- D. Create trust relationships between the forest root domain and the San Francisco domain. Use the Active Directory Migration Tool (ADMT) to migrate user settings.

Answer: B

Explanation:

This command line tool is used to collect a user's documents and settings before an operating system migration to Windows XP from an earlier version of Windows and to restore them after the installation.

Incorrect Options:

A: This command line tool facilitates the importing and exporting of larger numbers of security principals, including groups.

C, and D: Active Directory Migration Tool (ADMT) 2.0, which allows migration of users and passwords from Windows NT 4.0 domains or Windows 2000 domains to

Windows 2003 domains.

Reference:

William Gruber, Sandra Faucett, Greg Gille, Jim Bevan, Deborah R. Jay, and Chris McKitterick; Microsoft(r) Windows(r) Server 2003 Deployment Kit Automating and Customizing Installations, A Resource Kit Publication, Chapter 5, pp. 321.

---

**QUESTION 71**

You are designing a DNS Name resolution strategy for the client computer in the customer service department. What are the two possible ways to achieve the goal? (Each Correct answer presents a complete solution. (Choose two)

- A. Create a reverse lookup zone in DNS for each new Domain.
- B. Add a WINS lookup record to the DNS forward lookup zone.
- C. Add a WINS reverse record to the DNS reverse lookup zone.
- D. Enable Dynamic updates for DownLevel client computers on each DHCP server.
- E. Install the Active Directory Client on All Computers in the Customer service department.

Answer: B, D

Explanation:

The WINS resource record instructs the DNS service to use WINS to look up and forward queries for host names not found in the zone database.

"...the Dynamically update DNS A and PTR records for DHCP clients that do not request updates (for example, clients running Windows NT 4.0) check box must also be selected before DHCP will update the A and PTR records for these clients automatically. The check box is not checked by default.

Incorrect Options:

A: The reverse lookup zone will handle those few queries where the client knows the IP address and wants a host name. You can get by without creating reverse lookup zones

C: A WINS reverse lookup zone is of no use.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70297 Training Kit Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 6, pp.614. Deborah Littlejohn Shinder, and Dr. Thomas W. Shinder; Exam 70291: MCSA/MCSE Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress, Chapter 3 2, pp. 17. William Boswell; Inside Windows(r) Server 2003, Addison Wesley, Chapter 5.

---

**QUESTION 72**

You are designing DNS implemetation Strategy for the new Infrastruce. Which two actions should you perform? (Each correct answer represents part of the solution. Choose two).

- A. Create a Stub Zone in each domain of the root zone.
- B. Create a \_msdcs subdomain in a new zone on the root domain.

- C. Replicate the \_msdcs subdomain across the roor domain.
- D. Replicate the \_msdcs subdomain to the ForestDNS zone applciation partition.
- E. Configure a zone transfer of the \_msdcs subdomain to secondary zone on all DNS servers in the forest.

Answer: B, D

---

**QUESTION 73**

You are designing a remote access strategy to meet the business and technical Requirement. What should you do?

- A. Configure each server running Routing and Remote Access as a RADIUS Client.
- B. Add a Remote Access policy to each server running Routing and Remote Access. Configure the Access method as VPN access.
- C. Add a Remote Access policy to each server running Routing and Remote Access. Configure the Access method as dialup access.
- D. Add a Remote Access policy to each server running Routing and Remote Access. Configure the Access method as wireless access.

Answer: A.

Explanation:

IAS is the Microsoft implementation of a RADIUS server and proxy.

The basic purpose of a RADIUS server is to centralize remote access authentication, authorization, and logging. RADIUS is useful, for example, in large organizations such as ISPs that need to manage many remote access connections to separate remote access servers.

For basic RADIUS scenarios in which no RADIUS proxy is implemented, deploying IAS as a RADIUS server requires configuration both at the client running Routing And Remote Access and at the server running IAS.

Incorrect Options:

B, C and D: The case study specifies that Remote Access policies will be centralized.

Reference:

J. C. Mackin, and Ian McLean; MCSA/MCSE selfpaced training kit (exam 70291): implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Chapter 10, pp. 1069 to 1074.

---

**QUESTION 74**

You are designing a DNS implementing strategy to meet the business and technical requirement. Which type of zone should you use?

- A. Sub Zones
- B. Standard Primary Zones
- C. Secondary Zones
- D. Active DirectoryIntegrated Zones

Answer: D

Explanation:

The case study specifically states that all Domain Controllers are DNS servers and that zones must be secured.

When you are running the DNS server service on a computer that is an Active Directory domain controller and you select the Store The Zone In Active Directory (Available Only If DNS Server Is A Domain Controller) check box while creating a zone in the New Zone Wizard, the server does not create a zone database file. Instead, the server stores the DNS resource records for the zone in the Active Directory database. Storing the DNS database in Active Directory provides a number of advantages, including ease of administration, conservation of network bandwidth, and increased security.

Incorrect Options:

A: Stub zones are most frequently used to keep track of the name servers authoritative for delegated zones.

B: For standard primary zones, only a single server can host and load the master copy of the zone. If you create a zone and keep it as a standard primary zone, no additional primary servers for the zone are permitted.

C: Secondary zones can increase fault tolerance and availability, but zone transfer traffic can consume unacceptable amounts of bandwidth in some circumstances.

Reference:

J. C. Mackin, and Ian McLean; MCSA/MCSE selfpaced training kit (exam 70291): implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Chapter 4, pp. 430, 566.

Craig Zacker; MCSE SelfPaced Training Kit (Exam 70293): Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Chapter 4, pp. 436.

---

### **QUESTION 75**

You are designing a strategy to perform inplace upgrade of domain controller in Boston and San Diego. Which method should you use?

- A. adprep
- B. sysprep
- C. Answer File
- D. Remote Installtion Services (RIS)

Answer: C.

Explanation:

An inplace domain upgrade is useful in the following circumstances:

1. The current domain structure translates well to Windows Server 2003.
2. You are limited in the amount of design and deployment time you are given.
3. You want to minimize changes to the current administrative structure or flow of information on the network.
4. You want to minimize the effect that users and administrators experience during the migration.

Incorrect: answer:

A: Prepares Windows 2000 domains and forests for an upgrade to Windows Server 2003.  
We have Windows NT 4.0 domains, not Windows 2000 domains.

B: Sysprep is used for clean installations not upgrades.

D: RIS cannot perform domain controller upgrades

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70297 Training Kit Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure, Chapter 5, pp. 534.

## **Topic 8, WoodgroveBank, Scenario**

### **Overview**

Woodgrove Bank is a financial institution that operates in the Netherlands. The company's primary business is providing residential and commercial mortgages. The Company wants to offer its customers secure Internet access to a mortgage management application.

### **Physical Location**

The Company's main office is located in Amsterdam. The Company has two branch offices in the following Locations:

1. Utrecht
2. The Hague

The Company has 200 local banks that are located throughout the Netherlands. The number of users in each location is shown in the following table:

<b>Location</b>	<b>Number of Users</b>
1.	Amsterdam 2,500
2.	Utrecht 650
3.	The Hague 800
4.	Each Local Bank 10-100

### **Planned Changes**

The Company wants to convert its mortgage management application to a multitier application named NewApp.

To support this new environment, the company will upgrade its servers to Windows Server 2003.

### **Business Processes**

The Amsterdam office and each branch office has its own IT staff in addition, most of the larger local banks have their own IT staff.

Currently, Local bank employees have access to their local resources and to resources at the Amsterdam office. Each office uses its own instance of a business-critical mortgage application.

The IT staff at the Amsterdam office includes a development team. The development team is responsible for developing and testing NewApp.

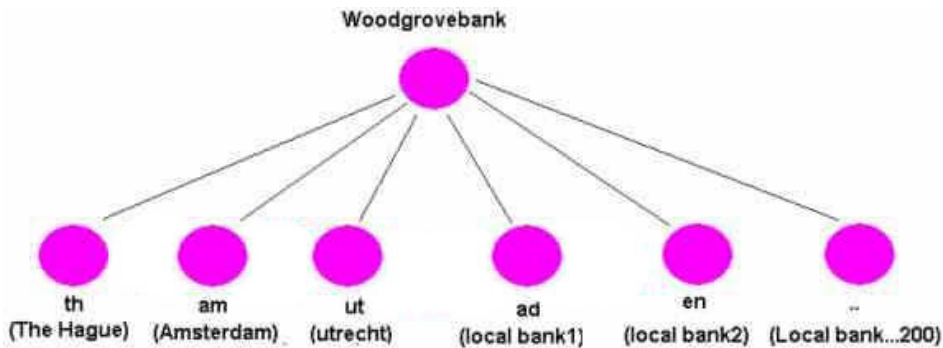
### **Infrastructure**

#### **Directory Services**

The Relevant portion of current domain structure is shown in the Existing Domain

#### **Model exhibit**

#### **Existing Domain Model Exhibits**



The Company has a Windows NT 4.0 environment that has more than 200 domains; each domain has a two-way trust relationship with the domain at Amsterdam office. Currently, Domain administrators manage their own domains. Each Location that has a local administrator currently manages its own users and resources. In addition, these administrators share responsibility for administering ring locations that do not have an IT staff.

#### Network Infrastructure

The Relevant portion of the existing network infrastructure exhibit

**\*\* MISSING \*\***

Domain Controllers vary from single processor servers at 700Mhz to processor Quad server at 1.5 GHz.

Client Computers run Windows 98, Windows NT Workstation 4.0 and Windows 2000 professional. There are also some Unix Client Computers.

Managers are issued portable Computers that contain confidential business information. These portable computers are equipped with smart card readers.

Managers use portable computers to establish VPN connections to the Amsterdam office when they travel.

#### Problem Statements

The following business problems must be considered:

Employees at local banks are often unable to serve customers because of failure of the mortgage application. The failure sometimes lasts many hours because there is nobody available to fix it.

The Development team has access to the occasionally, unapproved changes that are made to the application, resulting in unnecessary downtime.

Deployment of new operating systems takes a long time because network administrators have to each local bank.

#### Chief Executive Officer

I want Woodgrove bank to be visible on the Internet. I want NewApp to be easily accessible to our customers by using the Internet.

The newly designed environment will help to minimize the amount of administrative effort for all IT-related operational tasks.

For business reasons, I will not allow domain upgrades.

#### Officer Worker

Currently, it is sometimes difficult to access the information I need. For different information, I have to remember different passwords. In the new environment, I want to have one account and one password.

#### Business Requirements

### **Business Drivers**

The following business requirements must be considered:

Woodgroove Bank wants their company name to be visible on the Internet with.

Customers must be able to access mortgage information 24 hours a day, seven days a week.

The Company wants to reduce the costs of managing branch offices.

### **Organizational Goals**

The following organizational requirement must be considered

Bank employees need to be able to make a secure connection from their homes to the corporate network.

The company currently has 1 million customers. About half of them have mortgages. In the next 5 years, the infrastructure must be able to accommodate at least 2 million customers, with about 1 million customers having mortgages.

### **Security**

The following security requirement must be considered

Bank employees must have access to resources at the Amsterdam office, their local banks, and NewApp.

The Company must ensure that servers can be easily restored when one or more servers fail, with minimum loss of data and minimum downtime.

The Company needs the highest possible secure authentication method for all computers that contain confidential information.

### **NewApp Requirements**

The following NewApp requirement must be considered

NewApp is a web-based application that contains tools that are used by customers and tools that are used by employees.

Employees from all locations will connect to the web servers to access NewApp.

NewApp stores customer information in Active Directory by using custom classes and attributes.

NewApp stores mortgage information in the NewApp database.

Developers need to be able to test the NewApp schema modifications without affecting any other servers.

NewApp must be available 24 hours a day, seven days a week.

Because of national legal requirements, the server that contains mortgage information requires several security settings that are different from those on the NewApp application servers.

### **Technical Requirements**

#### **Active Directory**

The following Active Directory requirement must be considered

Active Directory must be deployed to support NewApp.

All domain controllers in the new environment must run Windows Server 2003.

Administration of Active Directory will not be performed at the local banks.

Each user should be authenticated locally when possible.

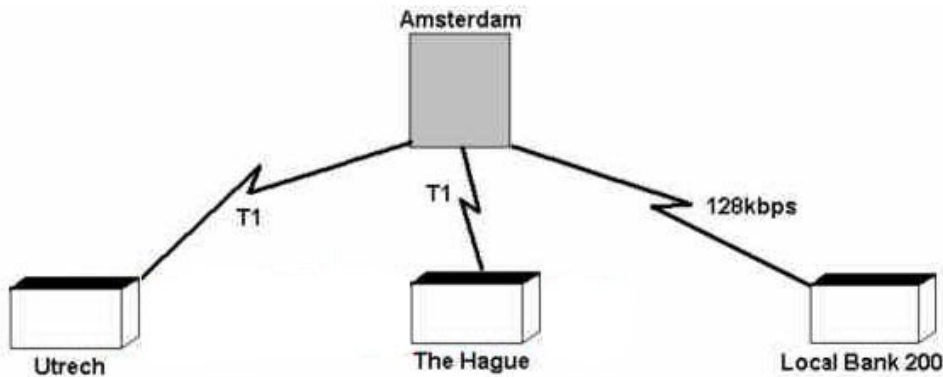
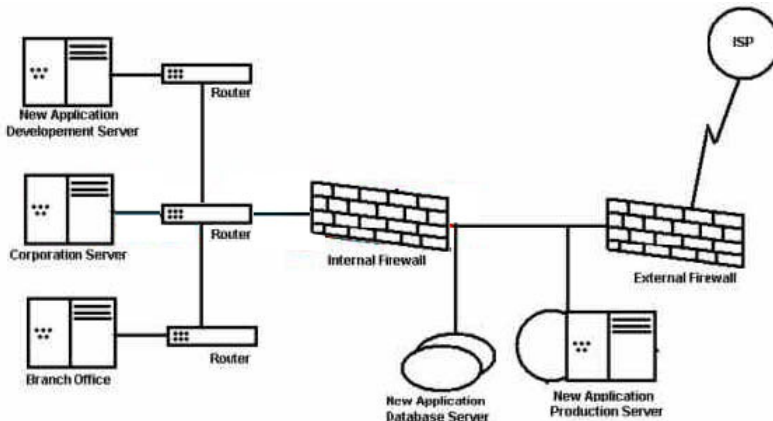
Domain Controllers will be placed in all locations that support more than 50 users.

#### **Network Infrastructure**

The following Network Infrastructure requirement must be considered

The planned network is shown in the planned Network Infrastructure exhibit.



**Network Infrastructure Exhibit:****Planned Exhibit:**

Bandwidth between the Amsterdam office and the branch offices is not an issue.

However, some local banks report that there are slow response times to the branch offices or to the Amsterdam office.

The company uses some legacy applications that are heavily dependent on NetBios name resolution. These applications will also be used after the migration.

The Company needs to use the smallest subnets possible in each location because of planned future expansion to include many additional branch offices.

VPN servers will be placed at the Amsterdam office only.

It is crucial to ensure 24-hour availability of the VPN servers.

Dial-up servers exist in each branch office to allow network administrators to administer each branch office in the event of WAN link failure.

Management of all remote access must be centralized.

**Topic 8, WoodgroveBank (9 Questions)****QUESTION 76**

You are designing a forest structure to meet the business and technical requirements. How many forests should you create?

- A. One
- B. Two
- C. Three
- D. Four

Answer: B

Explanation:

Using more than one forest requires administrators to maintain multiple schemas, configuration containers, global catalogs, and trusts, and requires users to take complex steps to use the directory. However, you might need to consider using multiple forests in the following situations:

1. Network administration is separated into autonomous groups that do not trust each other.
2. Business units are politically separated into autonomous groups.
3. Business units must be maintained separately.
4. There is a need to isolate the schema, configuration container, or global catalog.
5. There is a need to limit the scope of the trust relationship between domains or domain trees.

The case states: "Developers need to be able to test the NewApp schema modifications without affecting any other servers." For this reason you would need a different forest.

Reference:

Jill Spealman, Kurt Hudson, and Melissa Craft; MCSE Self-Paced Training Kit (Exam 70-294); Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Chapter 1, pp. 1-38 to pp. 1-39.

---

### **QUESTION 77**

You are designing an organizational unit (OU) structure to manage the New App servers. What should you do?

- A. Create one OU that includes both the web servers and the database servers.
- B. Create one OU that includes the web servers and one OU that includes the database servers.
- C. Create one OU that includes the web servers. Then Place the database servers in the Computer Containers.
- D. Place the web server and the database servers in the Domain Controller OU.

Answer: B

Explanation:

Organizational Units (OUs) provide a way to create administrative boundaries within a domain. Primarily, this allows you to delegate administrative tasks within the domain. OUs serve as containers into which the resources of a domain can be placed. You can then assign administrative permissions on the OU itself.

OUs are containers within a domain that allow you to group objects that share common administration or configuration.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 1, pp. 1-10.

Dan Holme, and Orin Thomas; MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, Chapter 1.pp. 1-12.

---

**QUESTION 78**

You are designing a new NETBIOS naming strategy for the corporate environment. Which domain name should you use?

- A. ad
- B. woodgrovead
- C. woodgrovebank
- D. woodgrovebank.com

Answer: B

The name "woodgrovead" conforms to the NetBIOS domain naming rules.

Incorrect Answers:

A: The name "ad" is not descriptive enough

C: The company already has 200 Windows NT 4.0 domains. The possibility that woodgrovebank is already in use is thus high.

D: A NetBIOS name can only be 15 characters long. Woodgrovebank.com is 17 characters long and is therefore not valid. In addition, the use of a dot in the NetBIOS name is not recommended.

---

**QUESTION 79**

You need to configure the security settings for the new app servers. Which two actions should you perform? (Each correct answer presents part of the solutions. Choose two)

- A. Create a Group policy object (GPO) for the web servers.
- B. Create a Group policy object (GPO) for the database servers.
- C. Modify the Default Domain Policy.
- D. Modify the Default Domain Controllers Policy.

Answer: A, B

---

**QUESTION 80**

You are designing an Active Directory site infrastructure to meet the business and technical requirements. What should you do?

- A. Create one site for each office and each local bank.
- B. Create one site for all offices. Create one site for all local banks.
- C. Create one site for Amsterdam. Create one site for all branch office and all local banks.
- D. Create one site for Amsterdam. Create one site for the Utrecht branch office. Create one site for that Hague branch office. Place half the local banks in the Utrecht site and half the local banks in the Hague site.

E. Create one site for Amsterdam. Create one site for the Utercht brach office. Create one site for each local bank that has more than 50 users. Place all the other local banks in the Amsterdam Site.

Answer: E

Explanation:

For the Main and branch office you should create a site for each one, since the number of user on each is mandatory to do so, and you need local authentication. You should also create a site for each local bank that has more than 50 users, since you need to do local validation (Technical Requirements : "Domain controllers will be placed in all locations that supports more than 50 users"). Regarding the rest of local bank locations, since they do not have so many users, you should point all of them to the Amsterdam site. The network topology is in a "star mode", so all the communications have a central point which is Amsterdam.

---

### **QUESTION 81**

You are designing a strategy to ensure that DNS queries always take the most efficient route to get resolved. Which action or actions should you perform? (Choose all that apply)

- A. Configure conditional forwarding on the corporate DNS servers to point the development DNS servers.
- B. Configure conditional forwarding on the development DNS servers to point the corporate DNS servers.
- C. Configure conditional forwarding on the perimeter network DNS servers to point the corporate and development DNS servers.
- D. Configure forwarding on the corporate and development DNS servers to point the perimeter network DNS servers.
- E. Disable root hints on the perimeter network DNS Servers.

Answer: A, B, D

Explanation:

Since you have created two separate forest infrastructures, you should configure forwarding on the Development DNS Servers to point to corporate DNS Servers, since these are the ones that would be in the production environment. You should also configure forwarding on the corporate and development DNS servers to point to the perimeter network DNS servers, since this should be the ones that would communicate with the internet.

The Forwarders tab allows you to forward DNS queries received by the local DNS server to upstream DNS servers, called forwarders. Using this tab, you can specify the IP addresses of the upstream forwarders, and you can specify the domain names of queries that should be forwarded. The process of forwarding selected queries in this way is known as conditional forwarding.

Reference:

J. C. Mackin, and Ian McLean; MCSA/MCSE self-paced training kit (exam 70-291): implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Chapter 5, pp. 5-4.

---

**QUESTION 82**

You are designing a remote access strategy to meet the business & technical requirements. Which authentication mechanism should you use?

- A. MS-CHAP v2.
- B. Internet Authentication service (IAS).
- C. Multilink & Bandwidth Allocation Protocol (BAP).
- D. Remote access policies on all servers running Routing & Remote Access.

Answer: B

Explanation:

IAS performs the following for dial-up, VPN, and wireless connections:

1. Centralized accounting: IAS collects usage or accounting information from all network access servers.
2. Centralized authentication: IAS supports many of the standard authentication methods such as Challenge Handshake Authentication Protocol (CHAP), Microsoft Challenge Handshake Authentication Protocol (MS-CHAP versions 1 and 2), and Extensible Authentication Protocol (EAP). IAS interoperates with network access devices from different vendors regardless of the access method used. If IAS is configured as a member of an Active Directory domain, the user account database is used to authenticate and authorize access to the network.
3. Centralized auditing: IAS logs all authentication Accepts and Rejects, as well as usage information such as logon and logoff records.

Instead of having your dial-up server or VPN server performing these tasks and storing accounting and auditing information, you can configure them to be RADIUS clients, each forwarding all connection requests to your IAS server. Any remote access policies stored on these RADIUS clients are no longer used. Instead, these policies, which are stored on the IAS server, will be used.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 10, pp. 10-28 to 10-29.

---

**QUESTION 83**

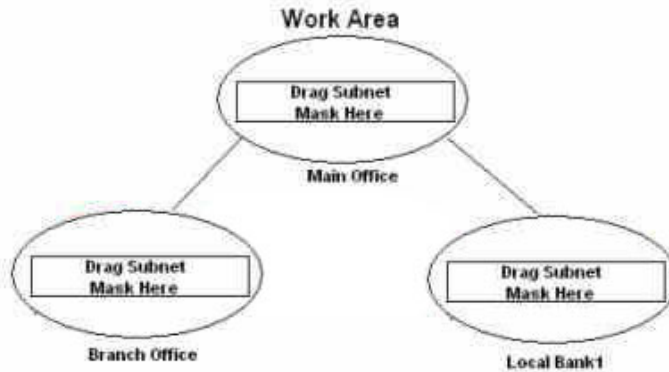
**DRAG DROP**

You are designing the TCP/IP addressing scheme for the company. What should you do?

To Answer, Drag the Appropriate subnet mask or masks to the correct location or locations in the work area.

## Subnet Masks

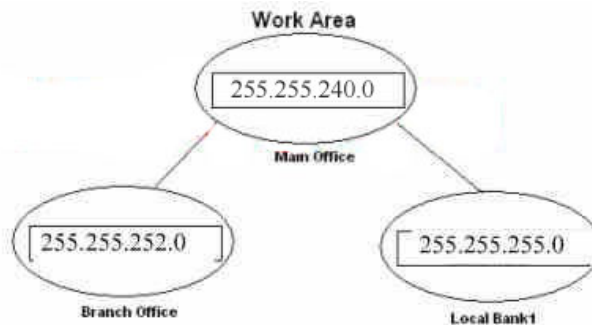
255.255.255.0  
 255.255.252.0  
 255.255.240.0  
 255.255.224.0  
 255.255.128.0



Answer:

## Subnet Masks

255.255.255.0  
 255.255.252.0  
 255.255.240.0  
 255.255.224.0  
 255.255.128.0



Explanation:

The case study states: "The Company needs to use the smallest subnets possible in each location because of planned future expansion to include many additional branch offices."

**QUESTION 84**

You are designing a VPN Server strategy to meet the business and technical requirement. What should you do?

- A. Configure all client computers to point to a VPN server in Amsterdam.
- B. Configure all client computers to use Multilink Bandwidth Allocation Protocol (BAP).
- C. Create a network Load Balancing cluster of VPN servers.
- D. Create a shutdown script for the VPN servers to delete the host(A) resource record of the VPN sever from the DNS database when the VPN server are shutdown.

Answer: C

Explanation:

Clustering is a group of machines acting as a single entity to provide resources and services to the network. In time of failure, a failover will occur to a system in that group that will maintain availability of those resources to the network.

Load balancing is using a device, which can be a server or an appliance, to balance the load of traffic across multiple servers waiting to receive that traffic. The device sends incoming traffic based on an algorithm to the most underused machine or spreads the traffic out evenly among all machines that are on at the time.

High Availability

is the essence of mission-critical applications being provided quickly and reliably to

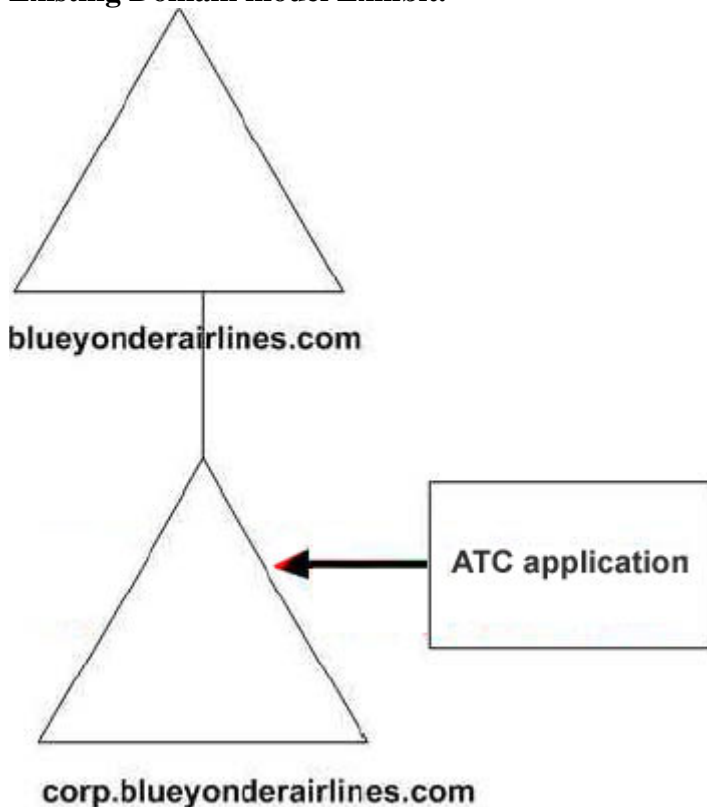
clients looking for your services. Five Nines is the term for saying a service or system will be up almost 100 percent of the time. To achieve this level of availability, you need to deploy systems that can survive failure. The ways to perform this are through clustering and load balancing.

Reference:

Robert J. Shimonski; Windows Server 2003 Clustering & Load Balancing, Osborne/McGraw-Hill, Chapter 1.

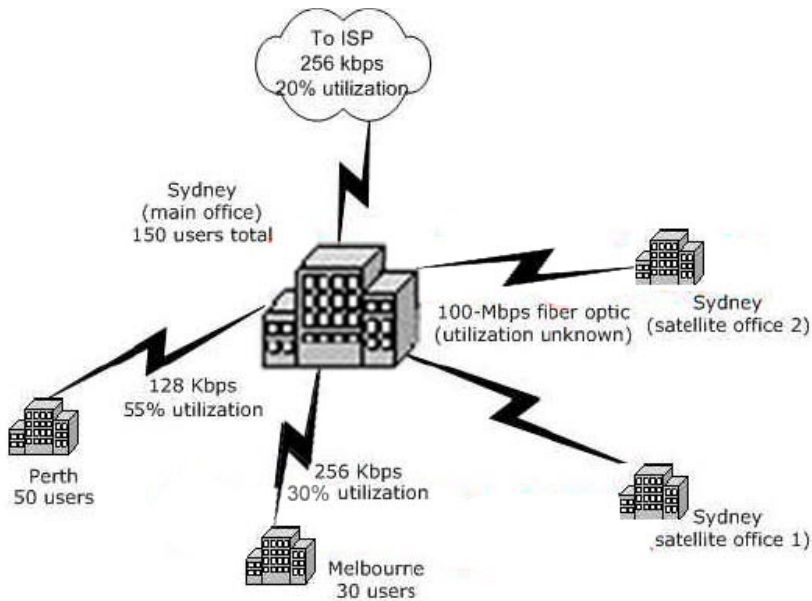
## **Topic 9, Blue Yonder Airlines, Scenario**

**Existing Domain model Exhibit.**

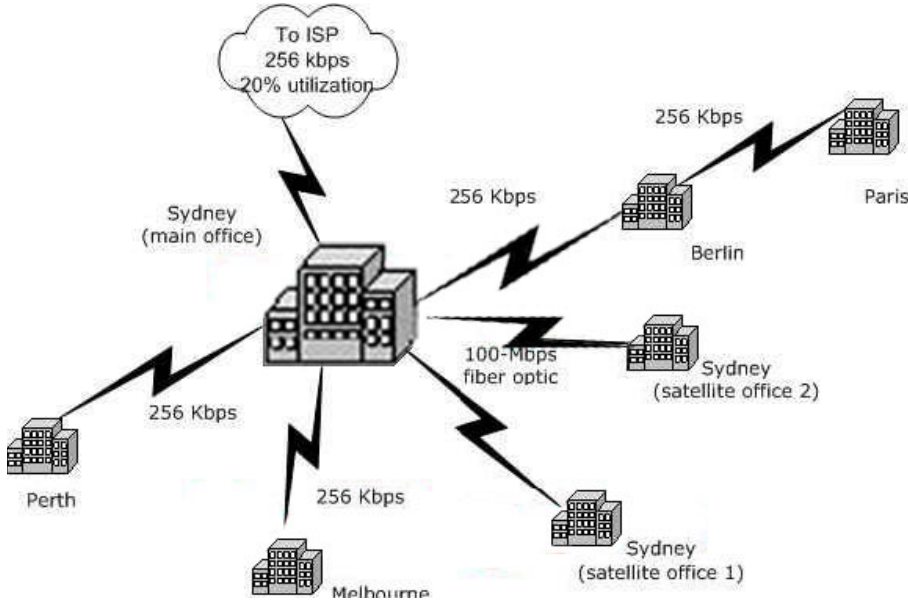


**Existing Network Infrastructure Exhibit.**





### Planned Network Infrastructure Exhibit.



### Overview

Blue Yonder Airlines provides air transportation services to locations throughout Australia. Services include executive-class travel and cargo delivery.

### Physical Locations

The company's main office is located in Sydney. The company has two branch offices in the following locations:

1. Melbourne
2. Perth

The main office location consists of the main office in Sydney and two satellite offices located near the Sydney airport. All three locations are connected by fiber-optic links.

### Planned changes

The company will open European branch offices in the following locations:

1. Berlin
2. Paris

The Berlin office will serve as the regional office for Europe.

In addition, the company plans to establish a new partnership with an application service provider (ASP) named Contoso, Ltd., which will be used to host the company's air traffic control (ATC) application.

The ATC application is an X.500 directory-enabled application that runs on Windows NT Server 4.0 computers in the Sydney office. The company plans to use a new version of the ATC application that will run on a Windows Server 2003 computer hosted by Contoso, Ltd. Only specified users will have access to this application. Users connect to this application by querying DNS for the application's service record. This record is stored on a UNIX DNS server running the latest version of BIND.

Contoso, Ltd., will create the required users in the domain that hosts the application and will provide this information as a file to Blue Yonder Airlines. No other connections to the Contoso, Ltd., network will be allowed except for access to the application itself.

### **Existing Environment**

#### **Business Processes**

Blue Yonder Airlines consists of the following primary departments:

1. Finance
2. Human resources (HR)
3. Information Technology (IT)
4. Air Traffic (ATC)
5. Flight operations

The IT department manages the entire network from the Sydney office or by traveling to the branch offices. All resources are located at the Sydney office and are accessed across the WAN links by users in the branch offices.

Although the ATC department works closely with flight operations, it is still a separate department.

The flight operations department consists of the following groups:

1. Flight officers
2. Manifest
3. Catering

Users in the Manifest group use an application named Manifest. The Manifest application consists of two versions:

1. Passenger Manifest, which contains Passenger information.
2. Cargo Manifest, which contains Cargo information.

Users in the Sydney office use only Passenger Manifest. Users in the branch offices use only Cargo Manifest. Currently, access to the Manifest application is limited only by using NTFS permissions.

Passenger Manifest runs on a server in the Sydney office. The information in Passenger must be current within the hour and must be available at all times to all users in the Manifest group. The information contained in the Passenger Manifest must never become publicly available.

#### **Infrastructure**

## Directory Services

The existing domains and trusts are displayed in the Existing Domain model exhibit. The LAN in each office consists of a 100-Mbps Ethernet network. No server computers are located in the branch offices. All IP addresses are statically configured for computers located in the branch offices.

A Microsoft Exchange Server 2000 environment provides Outlook Web Access (OWA) to all users. A single Exchange Server 2000 front-end server computer in the Sydney office is allocated for OWA.

Currently, the company does not have a public Web site. A Microsoft Internet Security and Acceleration (ISA) Server computer in the Sydney office is configured as a firewall and proxy server. The ISA Server computer is also used for publishing OWA to flight officers who connect to the network from outside the firewall. Flight officers use portable computers to access OWA via an ISP. No other intranet applications are currently available.

Company policy states that client computers should run only Windows 2000 Professional or Windows XP Professional. However, this policy is currently not enforced.

The existing hardware is shown in the following table.

Processor	Hard disk drive	Memory	Roles
Pentium III-800 MHz dual	TWO 9-GB SCSI	256 MB	Two domain controllers for Windows 2000 corporate domain; one domain controller for Windows 2000 root domain
Pentium III-800 MHz	TWO 9-GB SCSI	256 MB	PDC for Windows NT 4.0 domain
Pentium III-750 MHz	TWO 9-GB SCSI	256 MB	Exchange Server 2000 computer as member of Windows 2000 corporate domain

## Problem Statements

The following business problems must be considered:

1. The ATC application uses the inetOrgPerson class when authenticating to the X.500 directory-enabled database that the application uses for authentication.
2. The existing GPOs result in extremely lengthy logon times for users in the branch offices. Members of the Administrators group are currently excluded from the GPO that forces password changes.
3. The current dial-up solution results in expensive long-distance calls and only supports OW  
A. Currently, an on-site user must send the information to flight officers via an e-mail message because the Manifest application requires that users map to drive T to operate.
4. Existing airline security requirements specify that only smart card authentication should be used for the administration of servers by network administration.

## Interviews

### Chief Executive Officer

Blue Yonder Airlines has experienced consistent growth since its startup in 1997. However, this year the market has leveled off and we need to expand our services to Europe. We anticipate substantial growth over the next two years. Our current offices are located near the major airports in Australia. Each office provides all airline-related administrative features for its respective location. The only exception is network administration, which is provided by the Sydney office. If network administrators are needed in one of the branch offices, they are provided

air transportation by our company.

**Chief Information Officer**

Our company plans to establish a Web site named [www.blueyonderairlines.com](http://www.blueyonderairlines.com) that will include an online booking system for our customers.

Blueyonderairlines.com is already registered to the company and is used for e-mail addresses. This must not change.

I am concerned about security risks of the new Web site. Our DNS information must remain secure. The Manifest group must still remain a separate group for security purposes.

All servers must be upgraded to Windows Server 2003 to meet the new airline security requirements and to ease the management concerns we are currently facing. We are planning a hardware refresh within the next year to upgrade all computers to a minimum of 1 GB of RAM and seven SCSI hard disk drivers per server.

I anticipate that 300 new devices will be added to the network in the Sydney office over the next two years.

**Network administrator**

The WAN links are unreliable and can fail for hours at a time. We cannot copy large files because of this, and there are bandwidth problems related to slow links and unreliability.

Fault tolerance for the domains will be required for instances when the WAN links are down or when a single server fails.

We have adequate hardware, but performance for our existing Windows 2000 Server computer is inadequate.

The Exchange 2000 Server computer has excessively high processor utilization once a day. The high utilization lasts for almost an hour and users report that processing is very slow during this time. There cannot be servers in branch offices because of smart card authentication requirement.

A separate network administrator will be appointed to manage the Manifest application. The NetBIOS name of the corp.bloueyonderairlines.com domain is Airlines. Some applications still rely on this NetBIOS name to operate.

Currently, if service packs or new applications need to be installed on computers in the branch offices, a network administrator has to fly to that location. We do this because users do not have permissions to install software on their computers.

**Flight Officer**

Our network is generally performing adequately. However, I frequently have to make long-distance calls to the office to establish a dial-up connection. Often I do not get a connection because of a busy tone, and when I do get a connection I frequently get disconnected.

**Office Worker**

It takes more than five minutes to log on to the network, and when I finally log on to the network, my computer tries to automatically install software that eventually fails. However, I have noticed that my computer seems to respond better after this occurs.

I have to remember too many passwords. Currently, there are three: one for the domain, one for access to the ATC application, and one for access to the Manifest

application.

## **Business requirements**

### **Business Drivers**

The following business requirements must be considered:

1. Blue Yonder Airlines wants to establish a public Web site that is available 24 hours a day, seven days a week. New customers must be able to access this Web site by using a single URL.
2. Internal users must be able to access resources by providing their respective user names and passwords once per session.
3. Managers in the finance department are dissatisfied with the high number of expense claims they receive from flight officers for dial-up connections to the ISP.

### **Organizational Goals**

The following organizational requirements must be considered:

1. The new branch offices will be established in Berlin and Paris.
2. The new offices will connect to each other by means of a permanent WAN link.
3. The new offices will share a new WAN link to the Sydney office.
4. The expected number of new users in these offices is 100.
5. A new European administrative group will be established to manage these users and their resources.

### **Security**

The following security requirements must be considered:

1. Flight officers must be able to access secure data from any company office or from any remote location.
2. Flight officers and users of the Manifest application must be able to access Manifest data.

### **Customer Requirements**

The following customer requirements must be considered

1. User accounts must be created correctly in Active Directory and must be able to use all features of Active Directory and the ATC application simultaneously.
2. Faster name resolution is required when connecting to internal servers and external Web sites.

### **Technical requirements**

#### **Active Directory**

The following Active Directory requirements must be considered:

1. The Manifest application requires administration to meet European legal requirements.
2. Software deployment and security settings are different for users in each department. As users travel between locations, their user information must always be available locally.
3. Each branch office needs to resolve all NetBIOS names even if a WAN link goes down.
4. The browser settings must be distributed to computers by using GPOs.
5. The company's administrative model will change to a decentralized model with the addition of a second administrative group in Europe. Both administrative groups require smart card authentication for server administration.
6. VPN access is required for flight officers only.

## Network infrastructure

The following infrastructure requirements must be considered:

1. The planned network is shown in the Planned Network Infrastructure exhibit.
2. Redundancy for any service must be provided if a single service fails.
3. A WAN link from the newly established Berlin office will connect to the Sydney office. Another WAN link will connect the Paris office with the Berlin office.
4. User's reports of lengthy logon times must be resolved.
5. Daily updates of antivirus software must be executed for all desktop computers.

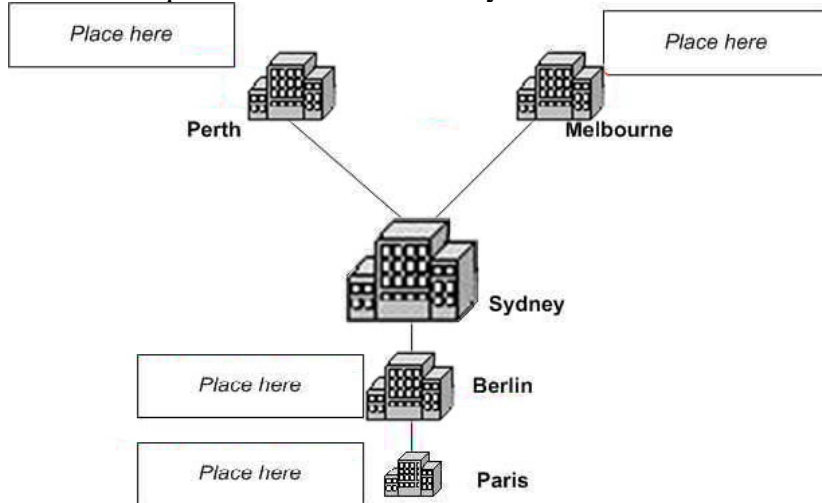
## Topic 9, Blue Yonder Airlines (11 Questions)

---

### QUESTION 85

#### DRAG DROP

You are designing a strategy for the placement of servers to meet the business and technical requirements. What should you do?

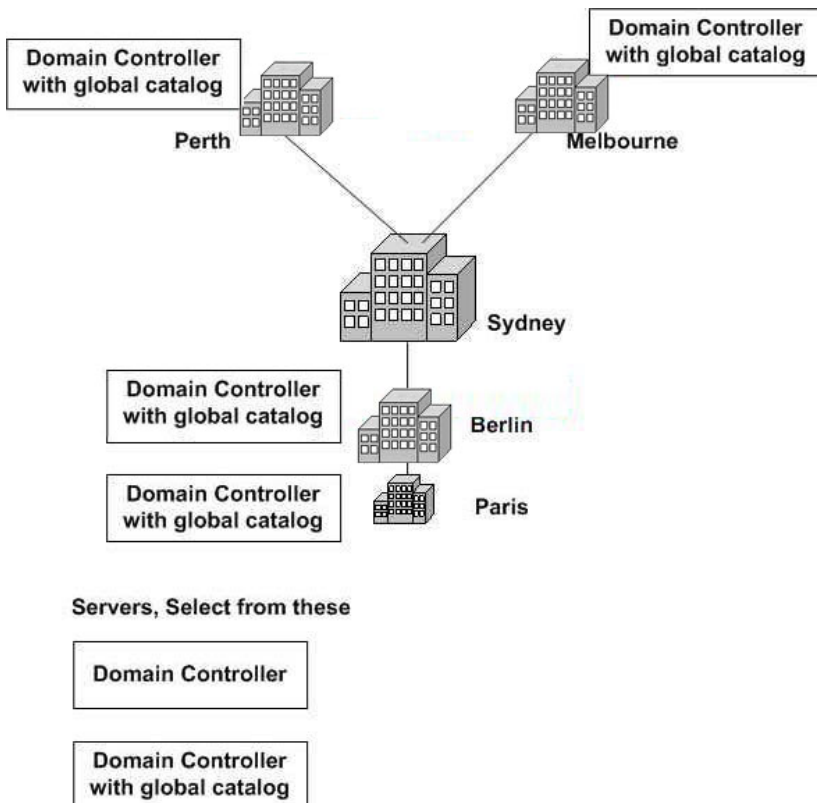


Servers, Select from these

Domain Controller

Domain Controller  
with global catalog

Answer:



Explanation:

A global catalog server is a domain controller that maintains a subset of Active Directory object attributes that are most commonly searched for by users or client computers, such as a user's logon name. Global catalog servers provide two important functions. They allow users to log on to the network, and they allow users to locate Active Directory objects anywhere in a forest without referring to specific domain controllers that store the objects.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 5, pp. 5-15.

---

### **QUESTION 86**

You are designing a top-level OU structure to meet the business and technical requirements. Which top-level OU or OUs should you use? (Choose all that apply.)

- A. ATC
- B. Paris
- C. Berlin
- D. Sydney
- E. Manifest
- F. Human Resources

Answer: A, B

---



**QUESTION 87**

You are designing an authentication solution to meet the security needs of the network administrators. You install an enterprise certification authority (CA). Which three additional actions should you take? (Each correct answer presents part of the solution. Select three).

- A. Enroll each administrative account for a smart card authentication certificate.
- B. Configure autoenrollment for computer authentication certificates.
- C. Install a smart card reader on each server computer.
- D. Install a smart card reader on each network administrator's computer.
- E. Configure each administrative account to require a smart card for interactive logon.
- F. Configure the Default Domain Policy GPO to require smart cards for interactive login.

Answer: A, D, E

Explanation:

The case study states: "Existing airline security requirements specify that only smart card authentication should be used for the administration of servers by network administration."

Enrollment can occur automatically, for example, when an application sends a certificate request to an enterprise CA and immediately receives a certificate in return, or manually, when a user explicitly requests a certificate from a C

A. To send enrollment requests to an enterprise CA, you use the Certificates snap-in for Microsoft Management Console. Because smart card logons are intended only for internal users with access to Active Directory, only enterprise CAs can issue smart card certificates.

A smart card is a credit card-size device used to securely store public and private keys, passwords, and other types of personal information. To use a smart card, you need a smart card reader attached to the computer and a personal identification number for the smart card. In Microsoft Windows Server 2003, smart cards can be used to enable certificate-based authentication and single sign-on to the enterprise.

Smart card is required for interactive logon, found in the Account options section of the Account tab, disables logging on without a smart card.

Reference:

Craig Zacker; MCSE Self-Paced Training Kit (Exam 70-293): Planning and Maintaining a Microsoft

Windows Server 2003 Network Infrastructure, Microsoft Press, Chapter 19, pp. 19-10 and Glossary, pp. G-51.

Deborah Littlejohn Shinder, and Dr. Thomas W. Shinder; MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, Syngress, Chapter 4, pp. 283.

---

**QUESTION 88**

You are designing a domain naming strategy for the new environment. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. Register airlines.com as a new domain name.
- B. Register manifest.airlines.com as a new domain name.
- C. Register manifest.blueyonderairlines.com as a new domain name.
- D. Maintain the existing blueyonderairlines.com registered domain name.
- E. Use the UPN suffix of airlines.com for all new users.
- F. Use the UPN suffix of blueyonderairlines.com for all new users.

Answer: D, F

Explanation:

In the case study, the Chief Information Officer states: "Blueyonderairlines.com is already registered to the company and is used for e-mail addresses. This must not change." It also states that the NetBIOS name of the corp.bloueyonderairlines.com domain is Airlines and that some applications still rely on this NetBIOS name to operate. It goes further, saying: "New customers must be able to access this Web site by using a single URL."

Users logging on using Windows 2000 or later platforms may log on the same way, or they may log on using the more efficient UPN. The UPN takes the format <UserLogonName>@<UPN Suffix>, where the UPN suffix is, by default, the DNS domain name in which the user object resides.

You should plan names that fit both DNS and NetBIOS name requirements.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 3, pp 3-27.

---

### **QUESTION 89**

You are designing a site topology for the new Active Directory environment. What should you do?

- A. Create one site for all offices. Place the subnets for the four branch offices and the Sydney main office in this site.
- B. Create two sites: one site for the four branch offices and one site for the Sydney main office. Place the subnets for the branch offices in one site. Place the subnet for the Sydney main office in the other site.
- C. Create three sites: one site for the four branch offices, one site for the Sydney main office, and one site for the Sydney satellite offices.
- D. Create four sites: one for the Melbourne and Perth branch offices, one site for the Berlin and Paris branch offices, one site for the Sydney main office, and one site for the Sydney satellite offices.
- E. Create five sites; one site for the Melbourne branch office, one site for the Perth branch office, one site for the Berlin branch office, one site for the Paris branch office, and one site for the Sydney main office. Place the subnets for each branch office and the Sydney main office in their respective sites.

Answer: E

Explanation:

The answer should be E since you are deploying a separate DC/GC to a site. Users complain that logon times and GP installation takes forever. If you only create 2 sites (B), then you will continue to have logon problems because site affinity will find any of the remote DC's to authenticate. By having a site in each location, site affinity will use the local DC/GC for authentication and GP processing.

---

**QUESTION 90**

You are designing a strategy to enable the ATC application to successfully resolve computer names. Which name resolution method should you use?

- A. DNS
- B. WINS
- C. Hosts file
- D. Lmhosts file

Answer: A

Explanation:

The case study states: "The ATC application is an X.500 directory-enabled application that runs on Windows NT Server 4.0 computers in the Sydney office. The company plans to use a new version of the ATC application that will run on a Windows Server 2003 computer hosted by Contoso, Ltd. Only specified users will have access to this application. Users connect to this application by querying DNS for the application's service record. This record is stored on a UNIX DNS server running the latest version of BIND."

Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) written and ported to most available versions of the UNIX operating system.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Glossary, pp G-2.

---

**QUESTION 91**

You are designing a DNS implementation strategy to meet the business and technical requirements. What should you do?

- A. Configure a domain controller in each branch office to contain a secondary zone of the contoso.com domain.
- B. Configure the DNS Server service on a domain controller in each office. Configure an Active Directory-integrated zone to replicate to all DNS servers.
- C. Configure an Active Directory-integrated zone on a domain controller in Sydney. Configure this zone to replicate to all domain controllers.
- D. Configure a primary zone for blueyonderairlines.com on a domain controller in Sydney. Configure a secondary zone on another DNS server in Sydney.

Answer: B

Explanation:

When you are running the DNS server service on a computer that is an Active Directory domain controller and you select the Store The Zone In Active Directory (Available Only If DNS Server Is A Domain Controller) check box while creating a zone in the New Zone Wizard, the server does not create a zone database file. Instead, the server stores the DNS resource records for the zone in the Active Directory database. Storing the DNS database in Active Directory provides a number of advantages, including ease of administration, conservation of network bandwidth, and increased security. In Active Directory-integrated zones, the zone database is replicated automatically, along with all other Active Directory data. Active Directory uses a multiple master replication system so that copies of the database are updated on all domain controllers in the domain. You don't have to create secondary zones or manually configure zone transfers, because Active Directory performs the database replication automatically.

This solution satisfies the requirements of the case study, which states: "Our DNS information must remain secure." As well as "Faster name resolution is required when connecting to internal servers and external Web sites".

Furthermore, it also states: "Redundancy for any service must be provided if a single service fails."

Providing redundancy:-For a network that relies heavily on DNS name resolution, having a single DNS server means having a single point of failure. You should deploy a sufficient number of DNS servers so that at least two copies of every zone are always online.

Reference:

Craig Zacker; MCSE Self-Paced Training Kit (Exam 70-293): Planning and Maintaining a Microsoft

Windows Server 2003 Network Infrastructure, Microsoft Press, Chapter 4, pp. 4-28 to 4-37.

---

**QUESTION 92**

You are designing a strategy to meet the security and financial requirements related to the Manifest application.

What should you do?

- A. Configure a VPN server in Sydney.
- B. Configure a VPN server in each branch office.
- C. Configure a dial-up server in Sydney
- D. Configure a dial-up server in each branch office.

Answer: A

Virtual private networking (VPN) provides a way of making a secured, private connection from the client to the server over a public network such as the Internet. Unlike dial-up networking, in which a connection is made directly between client and server, a VPN connection is logical and tunneled through another type of connection. Typically, a

remote user would connect to an Internet service provider (ISP) using a form of dial-up networking (particularly good for users with high-speed connections). The Routing And Remote Access server would also be connected to the Internet (probably via a persistent, or permanent, connection) and would be configured to accept VPN connections. Once the client is connected to the Internet, it then establishes a VPN connection over that dial-up connection to the Routing And Remote Access server.

The reason for configuring it in the Sydney office is that the Passenger Manifest runs on a server in the Sydney office, and the information contained in it must never become publicly available.

Currently, an on-site user must send the information to flight officers via an e-mail message, so VPN would make it easier for the flight officers to access it.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 1, pp. 1-43.

---

**QUESTION 93**

You are designing the placement of the PDC emulator operations master role. In which location or locations should you place the role? (Choose all that apply.)

- A. Sydney
- B. Melbourne
- C. Perth
- D. Berlin
- E. Paris

Answer: A

Explanation:

In a native mode Windows Server 2003 environment, the PDC Emulator receives preference in the replication of user account passwords.

The reason for it being placed in Sydney is, "The IT department manages the entire network from the Sydney office or by traveling to the branch offices. All resources are located at the Sydney office and are accessed across the WAN links by users in the branch offices."

Reference:

Robert Williams, and Mark Walla: The Ultimate Windows Server 2003 System Administrator's Guide, Addison-Wesley, Chapter 5.

---

**QUESTION 94**

You are designing a strategy to improve the performance and reliability of the domain controllers. What should you do?

- A. Create one RAID-5 volume.
- B. Create two RAID-5 volumes.
- C. Create one mirrored volume and two RAID-5 volumes.
- D. Create two mirrored volumes and one RAID-5 volume.

Answer: D

Explanation:

Reference:

A mirrored volume provides good performance along with excellent fault tolerance. Two disks participate in a mirrored volume, and all data is written to both volumes. As with all RAID configurations, use separate controllers (by adding a controller, you create a configuration called "duplexing") for maximum performance.

A RAID-5 volume uses three or more physical disks to provide fault tolerance and excellent read performance while reducing the cost of fault tolerance in terms of disk capacity. Data is written to all but one disk in a RAID-5. That volume receives a chunk of data, called parity, which acts as a checksum and provides fault tolerance for the stripe. The calculation of parity during a write operation means that RAID-5 is quite intensive on the server's processor for a volume that is not read-only. RAID-5 provides improved read performance, however, as data is retrieved from multiple spindles simultaneously.

Reference:

Dan Holme, and Orin Thomas: MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, Microsoft Press, Chapter 11, 11-35 to 11-37.

---

### **QUESTION 95**

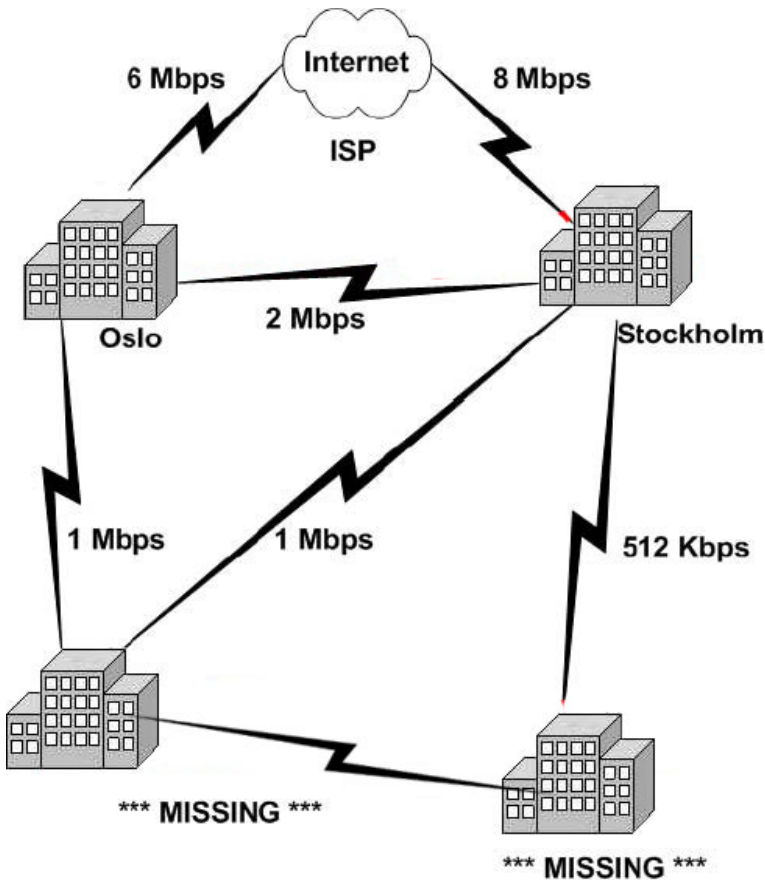
You are designing an IP address management strategy to address the anticipated growth of the company and to meet the business and technical requirements. What should you do?

- A. Install one DHCP server in each branch office and in Sydney. On each server, create duplicate scopes that contain the necessary scope options. Configure the scopes to assign all of the available IP addresses to each office.
- B. Install one DHCP server in each branch office and in Sydney. On each server, create duplicate scopes that contain the necessary scope options. Configure the scopes to assign half of the available IP addresses to each office.
- C. Install two DHCP servers in each branch office and in Sydney. Authorize one server in each office. On each server, create duplicate scopes that contain the necessary scope options. Configure the scope to assign half of the available IP addresses to each office.
- D. Install two DHCP servers in each branch office and in Sydney. Authorize both servers in each office. On each server, create duplicate scopes that contain the necessary scope options. Configure the scope to assign half of the available IP addresses to each office.

Answer: D

## **Topic 10, NorthwindTraders, Scenario**

### **Existing Network Infrastructure Exhibit**



## Overview

### Northwind

Traders is a stockbroker company in Northern Europe. The company provides advice and the resources to buy and sell stocks for individual investors. Currently, the company operates between the hours of 8:00 A.M. and 6:00 P.M. However, with the upcoming changes, business hours will be expanded.

### Physical locations

The company's main office is located in Stockholm. The company has two branch offices in the following locations:

1. Helsinki
2. Copenhagen

The company plans to establish a new branch office in Oslo.

The number of users in each location is shown in the following table.

Location	Number of users
Stockholm	350
Helsinki	100
Copenhagen	150
Oslo	15

### Planned Changes

All stock trading is currently done by telephone or fax.

The company wants to provide a Web site to allow customers to trade directly by using the Internet. It is also providing a new Web application named NewApp to



trade stocks.

To support this new environment, the company will upgrade its servers to Windows Server 2003.

### **Existing Environment**

#### **Business Processes**

Each office of Northwind Traders has its own IT staff.

The company currently hosts a mainframe application that tracks customers' stock traders. Each office uses its own instance of this application.

Stock trades that have been initiated by telephone must be recorded within two hours of the call.

#### **Infrastructure**

##### **Directory Services**

Currently, the company is using a Windows NT 4.0 domain infrastructure consisting of three domains, one for each office. The information about these domains is not well documented.

All links between offices are highly reliable.

All IT staff is members of the Domain Admins group in their own domain.

All domain controllers run Windows NT Server 4.0 with the latest service pack and security fixes installed.

##### **Network Infrastructure**

The existing network infrastructure is shown in the Existing Network Infrastructure Exhibit.

The local network in each office is a 10/100-Mbps Ethernet network.

Client computers run Windows NT Workstation 4.0 and Windows 98. There are also \*\*\* missing \*\*\*

##### **Problem Statements**

The following business problems must be considered:

1. Currently, employees need to remember different user names and password for different computers and offices. The company wants a single sign-on process in the new environment, which will also help to improve security.
2. In the last year, the company had some instances of data being compromised. The company wants to be able to trace which computer used which IP address at the time that the compromise occurred. The company wants to be able to store this information for at least one month.

##### **Chief Executive Officer**

I want customers of Northwind Traders to be able to trade stocks more directly.

Because migration can take months, we need our employees to be able to access both the current environment and the new environment during migration. However, after the migration is completed, employees should not be allowed to log on to the current environment.

##### **Chief Information Officer**

I want to introduce a new application named NewApp. NewApp is multitier application that will run on the Windows Server 2003 computers. NewApp will enable us to provide our customers with a tool to trade stocks online.

NewApp will be hosted on computers in the Stockholm and Oslo offices. The NewApp Web servers will be accessible from the Internet. The NewApp database

servers will be accessible from all sites.

### **Business requirements**

#### **Business Drivers**

The following business requirements must be considered:

1. Northwind Traders will use an Internet Web site hosted as [www.northwindtraders.com](http://www.northwindtraders.com).
2. For the internal DNS name, the company wants to use a contiguous namespace.
3. For internal name resolution, all computers are required to first use a local DNS server.
4. NewApp needs to be highly available. Maximum downtime of this application and its services will be one hour per month.
5. Because the customer transactions are increasing, the company wants to increase productivity and service levels without employing more traders.
6. The company wants to test the disaster recovery model at least once a year.
7. During this test, only the password changes and resource access will be tested.

#### **Organizational Goals**

The following organizational requirements must be considered:

Currently there is no information about how much bandwidth is needed for....

\*\*\* MISSING \*\*\*

#### **Security**

The following security requirements must be considered:

1. Employees need access to customer data. The company needs to secure the customer data.
2. All IT staff is trusted. However, only a selected group of IT staff will have access to customer data.
3. To secure the stock transactions as much as possible, we need all customers to use client certificates for all Web-based stock trading.
4. The company wants to be able to grant and revoke certificates.
5. All NewApp database servers need a common set of security settings.
6. The maximum downtime of NewApp services is specified for one hour. If a downtime of NewApp services in Stockholm of more than one hour is anticipated, administrators must recover NewApp at the disaster recovery location.

#### **Technical requirements**

##### **Active Directory**

The following Active Directory requirements must be considered:

1. Employee accounts and resources must be securely separated from the customer account and resources.
2. Web servers will not be part of a domain.
3. The company will use centralized authentication for Routing and Remote access.
4. IT management has decided to use a common namespace for all domains.
5. To make company-wide Active Directory changes, administrators from both the customer environment and the corporate environment must agree.
6. New hardware will be purchased for all Windows Server 2003 domain controllers.
7. The OU structure must align with the new administrative model.

##### **Network Infrastructure**

The following infrastructure requirements must be considered:

1. Front-end servers of NewApp will be a Network Load Balancing array of single processor servers.
2. Back-end servers of NewApp will be a cluster of eight-way 64-bit servers.
3. The company's ISP does not allow updates to DNS made by customers. The company wants to manage its own namespace.
4. The company has only a limited number of public IP addresses. It can use these addresses only when needed.
5. Logon traffic across WAN links needs to be minimized.
6. All client computers will be upgraded to Windows XP Professional.
7. The company wants to create a disaster recovery location in the Oslo Office.
8. Employees who have remote access will be allowed to access only the NewApp servers when they connect from outside the office. The different remote access requirements are shown in the following table.

Remote access	Idle-timeout	Dial-in schedule	Authentication
**MISSING **	**MISSING **	**MISSING **	**MISSING **

## Topic 10, NorthwindTraders (7 Questions)

---

### QUESTION 96

You are designing a strategy for migrating to the new environment. Which two factions from your current environment will affect your migration strategy? (Each correct answer presents part of the solution. (Choose two.)

- A. Trusts between domains
- B. Number of BDC s in each domain
- C. Users and resources in each domain
- D. Current hardware for domain controllers
- E. Current amount of replication traffic over WAN links

Answer: A, C

---

### QUESTION 97

You are designing an OU structure for IT staff at the branch offices. What should you do?

- A. Create an OU for the NewApp Web servers. Assign the IT staff at the branch offices user rights to this OU.
- B. Create an OU for the NewApp data servers. Assign the IT staff at the branch offices user rights to this OU.
- C. Create an OU for the IT staff at each branch office. Place network administrators at the branch offices in these OUs.
- D. Create an OU for each branch office. Place local servers in the OU for their respective office. Assign the IT staff at the branch offices user rights to these OUs.

Answer: D

Explanation:

The case study states: "Each office of Northwind Traders has its own IT staff."

Organizational Units (OUs) provide a way to create administrative boundaries within a domain. Primarily, this allows you to delegate administrative tasks within the domain. Prior to the introduction of the Active Directory, the domain was the smallest container to which you could assign administrative permissions. This meant that giving a group of administrators administrative control over particular resources was difficult or impossible to do without giving them sweeping permissions throughout the domain. OUs serve as containers into which the resources of a domain can be placed. You can then assign administrative permissions on the OU itself.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Microsoft, Chapter 1, pp. 1-9.

---

**QUESTION 98**

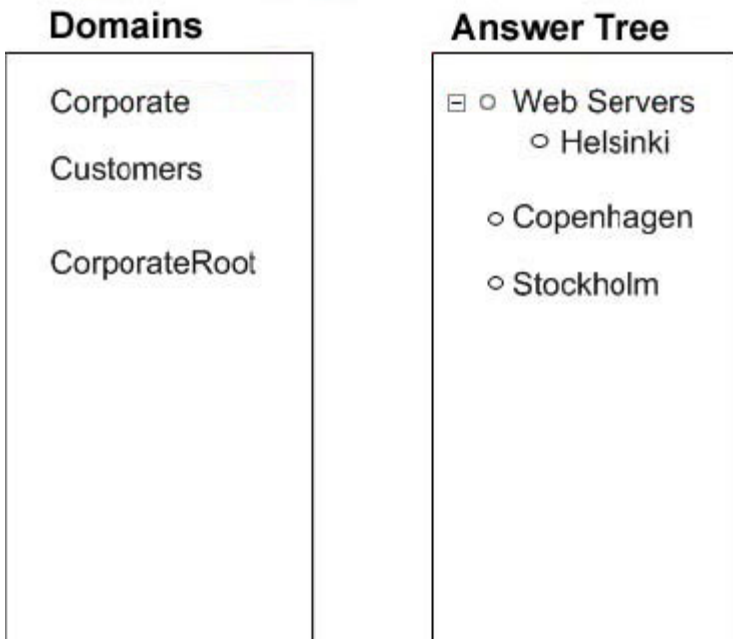
**DRAG DROP**

You are designing the Active Directory domain structure for the company. You need to create a diagram that shows the appropriate structure. What should you do?

Move the appropriate domains to the correction location in the answer tree.

Domains	Answer Tree
Corporate	
Customers	
CorporateRoot	
Copenhagen	
Stockholm	
Helsinki	
Web Servers	

Answer:



Explanation:

Note: Uncertainty

---

**QUESTION 99**

You are designing a migration strategy to create user IDs for all company users in the new environment. What should you do?

- A. Create a script that uses Active Directory Services Interfaces (ADSI) to import all user account into the new environment.
- B. Create new accounts for all users. Create a trust relationship between the existing environment and the new environment to enable access to resources in the existing environment.
- C. Import all user accounts into the new environment by using the Active Directory Migration Tool (ADMT).
- D. Import all user accounts into the new environment. Instruct users to no change their passwords during the migration phase so that they can access resources in the existing environment.

Answer: A

---

**QUESTION 100**

You are designing a security strategy for users who need remote access to the corporate network. What should you do?

- A. Configure Internet Authentication Service (IAS) for accounting.
- B. Configure the server running Routing and Remote Access to support L2TP.
- C. Configure the server running Routing and Remote Access to restrict dial-in traffic to the NewApp servers only.
- D. Create a separate account for remote access users. Configure these accounts to access

the NewApp server only.

Answer: C

Explanation:

Internet Authentication Service (IAS) is the Microsoft implementation of Remote Authentication Dial-In User Service (RADIUS), an authentication and accounting system used by many Internet Service Providers (ISPs). When a user connects to an ISP using a username and password, the information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system.

Reference:

Dan Holme, and Orin Thomas: MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, Microsoft, Glossary, pp. G-11.

---

### QUESTION 101

You need to test your disaster recovery solution. Which role should you transfer to the disaster recovery location during the test?

- A. RID master
- B. Schema master
- C. PDC emulator master
- D. Domain naming master

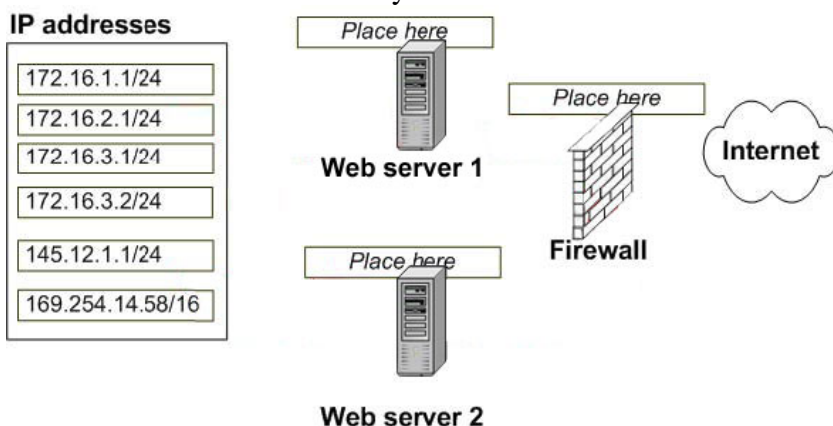
Answer: C

---

### QUESTION 102

DRAG DROP

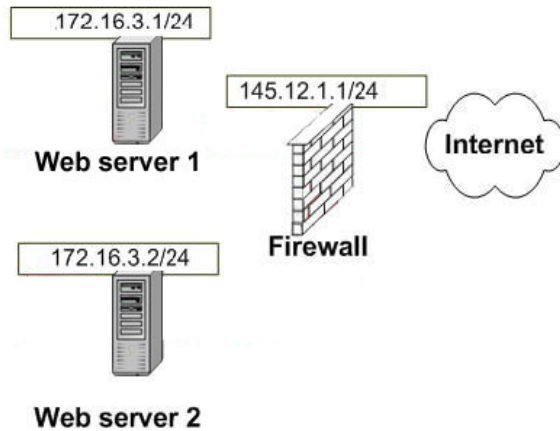
You are designing a strategy to ensure that the Web servers will be accessible from the Internet. You need to identify the appropriate IP configuration components that need to be used. What should you do?



Answer:

**IP addresses**

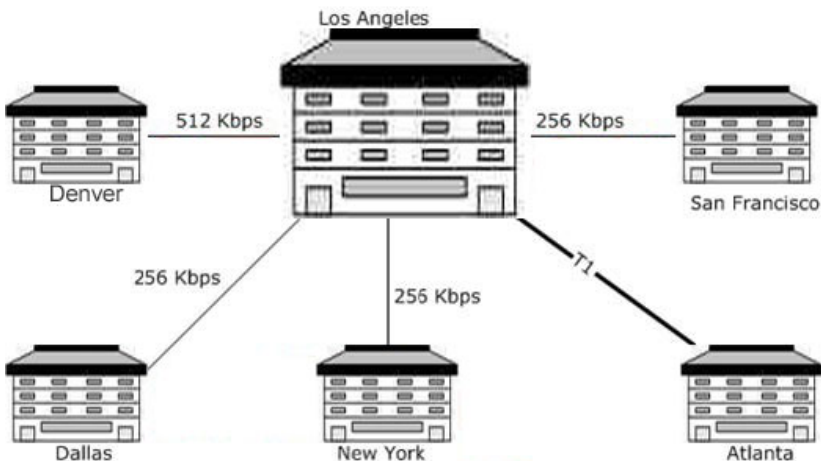
172.16.1.1/24
172.16.2.1/24
172.16.3.1/24
172.16.3.2/24
145.12.1.1/24
169.254.14.58/16



## Topic 11, Graphic Design Institute, Scenario Exhibit, Existing Domain Model



## Exhibit, Existing Network Infrastructure





## Overview

Graphic Design Institute is a graphical design company that creates animated graphics for several advertising companies and movie theaters.

The hours of operation are 8:00 A.M. to 5:00 P.M., Monday through Friday.

## Physical Locations

The company's main office is located in Los Angeles. The company has five branch offices in the following locations:

1. Atlanta
2. Dallas
3. Denver
4. New York
5. San Francisco

The number of users in each office is shown in the following table.

Office	Number of users
Los Angeles	550
Atlanta	300
Dallas	30
Denver	210

## Planned Changes

To meet new security and customer requirements, the company wants to implement a Windows Server 2003 Active Directory environment.

Existing Environment

## Business Processes

Graphic Design Institute consists of the following primary departments:

1. Human Resources (HR)
2. Finance
3. Information Technology (IT)
4. Advertising
5. Movies
6. Animation

The IT department is responsible for all network management.

Users often work on multiple projects at the same time. A strong administrative structure based on each user's office location and department is being used.

## Infrastructure

### Directory Services

The existing domains and trust relationships are shown in the Existing Domain Model exhibit.

The company has one Windows 2000 domain located in the Los Angeles office. The name of the domain is graphicdesigninstitute.com. The domain is a Windows 2000 mixed-mode domain that contains Windows 2000 Server computers configured as domain controllers, Windows NT Server 4.0 computers configured as BDCs, and Windows 2000 Server computers configured as member servers.

Currently, this domain is the only Active Directory domain. The domain consists of the following three top-level OUs:

1. Movies
2. Animation

### 3. Advertising

The default site configuration has been implemented in the existing Active Directory environment.

#### **Problem statements**

The following business problems must be considered:

1. There is currently no enforcement of frequent password changes and logon hours.
2. The ISP can only supply a single subnet, which consists of 32 IP addresses, for the Internet link.
3. It is very difficult to manage users and groups and their necessary permissions.
4. The finance and HR department cannot agree on a mutual security policy to implement.
5. NetBIOS name resolution is saturating the WAN links.

#### **Interviews**

##### **Chief Executive Offices**

Graphic Design Institute has lost a number of contracts due to deadlines that have not been met. Decreasing the amount of time we spend administering the network, along with increasing the amount of time we spend on customers, is my primary reason for requesting the upgrade of the entire network.

Funds are available for critical hardware requirements. I do not want any downtime for users. I also want strict business hours enforced. Employees should not be at the office or work from home outside normal business hours.

##### **Chief Information Officer**

Currently, we have problems as a result of all the merges and acquisitions. I want all the servers to be installed with Windows Server 2003 to resolve these problems. I also want all client computers upgraded to Windows XP Professional over the next two years.

The current IT response level is leading to a lot of lost production hours. Each office will continue to manage its own users and computers, with the exception of the finance and HR departments, which have their own requirements. We need to ensure that no production time is lost as a result of an interruption in the network connectivity.

##### **Network Administrator**

We are currently expected to resolve issues within 24 hours, although this sometimes is not achieved. Because most high-level administrative work can only be done when users are not in the office, network administrators often work after hours or on weekends.

Domain administrators are responsible for managing the private IP addresses of every computer that belongs to their respective domains.

Help desk staff exists in each branch office to assist users with software-related problems, as well as with basic network problems. Each domain has its own help desk staff with personnel located in each office. In the future, the help desk staff will be responsible for resetting passwords if users forget them.

##### **Office Worker**

Only selected users have Internet access. This prevents us from remaining competitive because we cannot perform the necessary research about new technologies or software available.

## **Business Requirements**

### **Business Drivers**

The following business requirements must be considered:

1. A single internal namespace is required to minimize administrative effort.
2. A Web site exists outside the firewall to provide company contact information.

### **Organizational Goals**

The following organizational requirements must be considered:

1. The new design must accommodate the finance and HR departments, which have requirements not addressed by the company's planned password policy.
2. All computers must have the latest service packs and hot fixes installed. In addition, computers in the advertising department must be updated to have the latest versions of graphics and audio drivers installed.

### **Security**

The following security requirements must be considered:

1. Specific security groups must be set up to address security requirements.
2. Security must be based on departments and groups of individuals within the departments.
3. Users in the finance department need access to payroll information on a server named Payroll, which is located in the HR department.

### **Customer Requirements**

The following customer requirements must be considered:

1. A new service-level agreement that requires a response from the IT department to users within one hour must go into effect.
2. Personal information about employees must remain secure.
3. All client computers, regardless of office location, must be able to access all other computers.

## **Technical Requirements**

### **Active Directory**

The following Active Directory requirements must be considered:

1. The company requires a new Active Directory environment that enables the security requirements of various departments to be met. This must be accomplished by installing a Windows Server 2003 on all domain controllers.
2. A completely decentralized administrative approach will be used. Each group of administrators will be responsible for its own departmental environment.
3. Only one operations master role will be allowed per domain controller. This is required for fault tolerance.
4. DNS replication of the forest root domain must be limited to forest domain controllers only.

### **Network Infrastructure**

The following infrastructure requirements must be considered:

1. A new Routing and Remote Access solution must be installed:
2. A DHCP solution that is fault tolerant within each office must be implemented
3. All WAN links must be fault tolerant
4. Name resolution must be localized on the local network

## **Topic 11, Graphic Design Institute (10 Questions)**

---

**QUESTION 103**

You are designing a strategy to address the requirements of the advertising department. What should you do?

- A. Create a GPO and link it to the Denver site.
- B. Create a GPO and link it to the Advertising OU.
- C. Create a GPO and link it to the graphicdesigninstitute.com domain.
- D. Configure the Default Domain Policy to have the No Override option.
- E. Use block inheritance to prevent the GPO from applying to members of the advertising department.

Answer: B

Explanation:

The case study states: "Each group of administrators will be responsible for its own departmental environment."

You can use Group Policy to define user settings such as password restrictions or computer settings. It is much better to create a Group Policy plan that applies GPOs efficiently from the outset, and linking GPOs to OUs provides a way to bring such a plan into effect. Creating GPOs for OUs gives you much better control over the application of Group Policy, because it eliminates the need to filter Group Policy settings.

Incorrect Options:

A: This would apply the GPO to the entire Denver site, but the question refers to the advertising department.

C: This would apply the GPO to the entire graphicdesigninstitute.com domain, but the question refers to the advertising department.

D: The Default Domain Policy applies at the domain level, but the question refers to a department.

E:

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 4, pp. 4-10.

---

**QUESTION 104**

You are deploying a NetBIOS name resolution strategy to meet the business and technical requirements. What should you do?

- A. Install one WINS server in each branch office. Configure the WINS servers to use push/pull replication with the WINS server in Los Angeles. Configure all computers to have the IP address of the local WINS server.
- B. Install two additional WINS servers in Los Angeles. Configure the WINS servers to use push/pull replication. Configure all computers to have the IP addresses of the WINS servers.
- C. Install the DNS Server service on one domain controller on each branch office. Configure the DNS server to forward all unanswered queries to the WINS server.

Configure all computers to have the IP address of the DNS servers.

D. Configure the DNS servers in each branch office to forward all unanswered queries to a local WINS server. Configure all computers to have the IP addresses of the DNS server in graphicdesigninstitute.com forest root.

Answer: A

Explanation:

The question asks for NetBIOS name resolution, which means we must use WINS.

Your goal, when designing a WINS strategy for your network infrastructure, is to have the WINS service available to client workstations when they need it. Availability is at risk when there is only one WINS server configured to support a large number of users. If that server should fail, all of the users will now need to resolve NetBIOS names using one of the other methods, namely: Lmhosts files or broadcasts. In situations in which a slow link exists between two subnets, it is highly recommended that a WINS server be placed in both subnets to maximize performance of client name-resolution requests. It is for this reason that "B" is incorrect.

This is the default configuration of a WINS server. A push of an updated WINS database will occur as discussed previously, and the WINS server is also configured to pull WINS database information from another WINS server at a designated time. This type of configuration is recommended in most cases.

After configuring WINS servers as Push/Pull partners, servers, after replication, will contain NetBIOS records from all subnets. Now, any WINS-enabled client on any subnet can access resources on a different subnet using the NetBIOS name of that resource.

Incorrect Options:

C and D: The question does not ask for DNS resolution.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 7, pp. 7-16 to 7-24.

---

### **QUESTION 105**

You are designing a DHCP strategy to meet the business and technical requirements. What should you do?

- A. Install one DHCP server in each branch office and one DHCP server in Los Angeles.
- B. Install one DHCP server in each branch office and two DHCP servers in Los Angeles.
- C. Install two DHCP servers in each branch office and one DHCP server in Los Angeles.
- D. Install two DHCP servers in each branch office and two DHCP servers in Los Angeles.

Answer: D

Explanation:

The case study states: "A DHCP solution that is fault tolerant within each office must be implemented." Option "D" allows for this to be achieved, by placing two DHCP servers

in each office.

Incorrect Options:

A, B and C: These options do not conform to the requirements because they do not have two servers in each office.

---

**QUESTION 106**

You are designing a DNS strategy to meet the business and technical requirements. What should you do?

- A. Install the DNS Server service on all domain controllers. Create Active Directory-integrated zones. Replicate the zones to all DNS servers in the forest.
- B. Install the DNS Server service on all domain controllers. Create Active Directory-integrated zones. Replicate the zones to all DNS servers in the domain.
- C. Install the DNS Server service on all domain controllers. Create primary zones and secondary zones.
- D. Create application partitions for the different zones on one domain controller. Configure replication to occur on all DNS servers.

Answer: B

Explanation:

The case study states: "...the company wants to implement a Windows Server 2003 Active Directory environment." This environment uses DNS for name resolution. Any domain controller running the DNS Server service can be designated as the primary source for a zone and can update a zone. In other words, there is not one primary DNS server, as in the standard primary zone methodology, which can be a single point of failure for a network. In the Active Directory integrated model, a master copy of the zone is maintained by Active Directory and replicated to all domain controllers.

Incorrect Options:

A: The case study states: "DNS replication of the forest root domain must be limited to forest domain controllers only."

C: For standard primary zones, only a single server can host and load the master copy of the zone. If you create a zone and keep it as a standard primary zone, no additional primary servers for the zone are permitted. The standard primary model implies a single point of failure.

D:

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 6, pp. 6-12 to 6-13.

---

**QUESTION 107**

You need to identify the number of servers that will be used specifically for operations master roles. How many servers should you recommend?

A. 5

- B. 11
- C. 14
- D. 17
- E. 20

Answer: B

---

**QUESTION 108**

You are designing a strategy to provide Internet access to all users. What should you do?

- A. Configure Internet Connection Sharing on all client computers.
- B. Configure Automatic Private IP Addressing (APIPA) on all client computers.
- C. Configure one server as a Routing and Remote Access VPN server.
- D. Configure one server as a Routing and Remote Access NAT router.

Answer: D

Explanation:

Computers running a member of the Windows Server 2003 family now allow you to add the Internal interface as a private interface to the Network Address Translation component of the Routing and Remote Access service. This allows connected remote access clients to access the Internet

Incorrect Options:

- A: Internet Connection Sharing is recommended only for very small networks.
- B: APIPA is an addressing feature for simple networks that consist of a single network segment. Whenever a computer running Windows Server 2003 has been configured to obtain an IP address automatically, and when no DHCP server or alternate configuration is available, the computer uses APIPA to assign itself a private IP address in the range of 169.254.0.1-169.254.255.254.

C:

Reference:

Jerry Honeycutt: Introducing Microsoft Windows Server 2003, Microsoft Press, Chapter 6.

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 9, pp. 9-12.

---

**QUESTION 109**

You are designing an Active Directory forest structure to meet the business and technical requirements. What should you do?

- A. Create a single forest that has one domain. Use OUs to separate the departments.
- B. Create a single forest that has multiple domains to represent every department.
- C. Create a single forest that has three domains: one for finance, one for HR, and one for the remaining departments.
- D. Create multiple forests that have a single domain in each forest to represent the



departments.

Answer: C

Explanation:

The case study states: "The new design must accommodate the finance and HR departments, which have requirements not addressed by the company's planned password policy." It also states: "A completely decentralized administrative approach will be used." This means that they have to have their own domains to which a password policy can be applied to cater for their respective needs.

There are a number of reasons that you might need to define multiple domains. These reasons include the following:

1. You need to implement different domain-level security policies.
2. You need to provide decentralized administration.
3. You need to optimize replication traffic across WAN links more than you can by dividing a domain into multiple sites.
4. You need to provide a different namespace for different locations, departments, or functions.
5. You need to retain an existing Windows NT domain architecture.
6. You want to put the schema master in a different domain than the domains that contain users or other resources.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 3, pp. 3-4 to 3-7.

---

### **QUESTION 110**

You are designing a WAN implementation strategy to meet the business and technical requirements. What should you do?

- A. Configure a demand-dial router.
- B. Create multiple Active Directory site links.
- C. Configure a VPN connection between each branch office.
- D. Install an Internet Authentication Service (IAS) server in each branch office.

Answer: A

Explanation:

Demand-dial connections are used by the Routing and Remote Access service to make point-to-point connections between LANs over which packets are routed.

Reference:

Jerry Honeycutt: Introducing Microsoft Windows Server 2003, Microsoft Press, Chapter 6.

---

### **QUESTION 111**

DRAG DROP

You are designing a strategy to provide the required security for the Payroll server. You need to identify the actions that you should perform to achieve this goal. What should you do?

Move, and arrange the actions in the proper order. Use only actions that apply.

Actions, select from these	Actions, place here
Create a universal group named Payroll, Add users from the movies department to this group.	Place first step here
Create a global group named Finance that contains only the appropriate Finance users.	Place second step, if any, here
Create a domain local group that contains only the appropriate HR users and assign it permissions to the Payroll server.	Place third step, if any, here

Answer:

Actions, select from these	Actions, place here
	Create a domain local group that contains only the appropriate HR users and assign it permissions to the Payroll server.
	Create a global group named Finance that contains only the appropriate Finance users.
	Create a universal group named Payroll, Add users from the movies department to this group.

---

### QUESTION 112

You are designing a password management solution to meet the business and technical requirements. Which two actions should you perform? (Each correct answer presents part of the solution.) (Choose two.)

- A. Delegate the password management controls to the help desk staff.
- B. Delegate the password management controls to the Domain Users group.
- C. Configure the Default Domain Policy to enforce password expiration settings.
- D. Configure the Default Domain Controller Policy to enforce password expiration settings.

Answer: B, D

Explanation:

Security groups are used to group domain users into a single administrative unit. Security groups can be assigned permissions and can also be used as e-mail distribution lists. Users placed into a group inherit the permissions assigned to the group for as long as they remain members of that group. Windows itself uses only security groups.

We have already established that multiple domains must be used when you need to

implement different domain-level security policies. By configuring the Default Domain Controller Policy we apply the settings to that specific domain.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 4 , pp. 4-26.

## **Topic 12, Wide World Importers, Scenario**

**Scenario missing.**

### **Topic 12, Wide World Importers (11 Questions)**

---

#### **QUESTION 113**

You are designing a VPN strategy to meet the business and technical requirements. Based on the current infrastructure, what is the maximum number of VPN connections that can be supported?

- A. 25
- B. 35
- C. 70
- D. 128
- E. 256

Answer: B

---

#### **QUESTION 114**

You are designing a strategy for migrating domain user accounts to the new Windows Server 2003 Active Directory environment. You want to identify the minimum number of trust relationships that need to be manually created to perform this operation. Which design should you use?

- A. one external trust relationship
- B. two external trust relationships
- C. six external trust relationships
- D. twelve external trust relationships
- E. one two-way cross-forest trust relationship

Answer: B

---

#### **QUESTION 115**

You are designing a DNS naming strategy for the proposed Active Directory environment.

Which domain name or names should you use? Select all that apply.

- A. wideworldimporters.com
- B. newyork.wideworldimporters.com
- C. sanfrancisco.wideworldimporters.com

- D. east.wideworldimporters.com
- E. west.wideworldimporters.com
- F. seattle.wideworldimporters.com

Answer: D, E

---

**QUESTION 116**

You are designing the top-level OU structure for the company. Which action or actions should you perform? Select all that apply.

- A. Create an OU named Sales. Place all sales user accounts in the Sales OU.
- B. Create an OU named Montreal. Place all Montreal user accounts in the Montreal OU.
- C. Create an OU named East. Place all user accounts from the East Coast offices in the East OU.
- D. Create an OU named NorthAmerica. Place all user accounts in the NorthAmerica OU.
- E. Create an OU named Servers. Place all server computer accounts in the Servers OU.

Answer: B

---

**QUESTION 117**

You are designing the NetBIOS domain naming strategy for the company. Which NetBIOS domain name or names should you use? Select all that apply.

- A. east
- B. west
- C. quebec
- D. newyork
- E. northamerica
- F. wideworldimporters

Answer: A, B

---

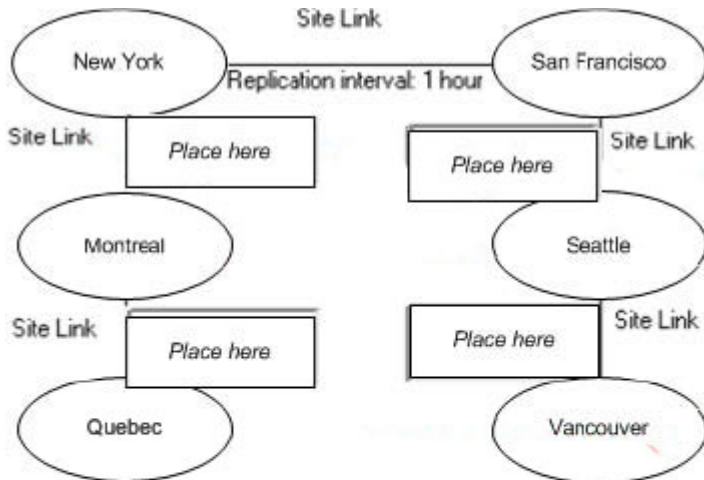
**QUESTION 118**

**DRAG DROP**

You are designing the Active Directory replication topology to meet the business and technical requirements. You need to configure the replication intervals for the site links shown in the diagram. Each site link includes only the two sites it shown between.

What should you do?

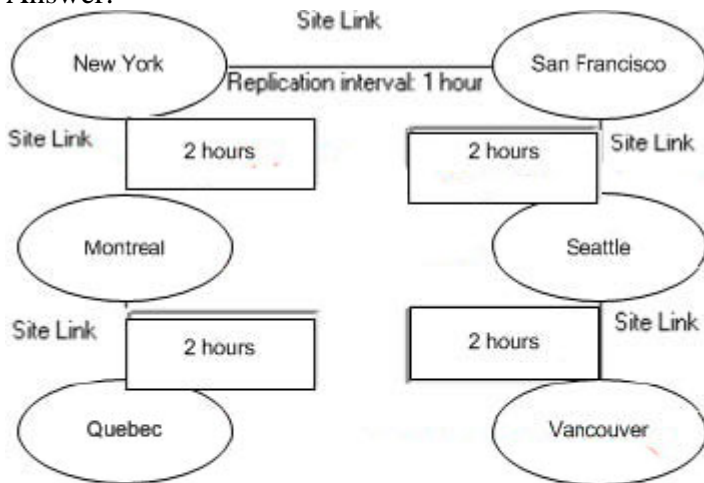
Drag and Drop



**Intervals, select from these**

1 hour	2 hours	4 hours
5 hours		

Answer:



**Intervals, select from these**

1 hour	2 hours	4 hours
5 hours		

### QUESTION 119

You are designing the DNS topology to meet the business and technical requirements.

Which DNS structure should you use?

- A. one primary zone
- B. two primary zones
- C. one Active Directory-integrated zone that has the replication scope set to all DNS servers in the forest.
- D. two Active Directory-integrated zones that have the replication scopes set to all DNS servers in the forest.
- E. one Active Directory-integrated zone that has the replication scope set to all domain controllers in the domain.
- F. two Active Directory-integrated zones that have the replication scopes set to all domain controllers in the domain.

Answer: D

---

**QUESTION 120**

You are designing the security for dial-up remote access to meet the business and technical requirements.

Which two mechanisms should you use? Each correct answer presents part of the solution. Select two.

- A. EAP-TLS authentication
- B. MS-CHAP v2 authentication
- C. a stand-alone certification server
- D. an enterprise certification server
- E. MPPE 56-bit encryption

Answer: A, D

---

**QUESTION 121**

You are designing the Active Directory site topology to meet the business and technical requirements. Which site or sites will require universal group membership caching? Select all that apply.

- A. New York
- B. Montreal
- C. Quebec
- D. San Francisco
- E. Seattle
- F. Vancouver

Answer: C, E, F

---

**QUESTION 122**

You are designing a strategy to allow users to have remote access to internal resources.

Which service or services should you allow on the public interface of the NAT

Server? Select all that apply.

- A. HTTP
- B. LDAP
- C. POP3
- D. SMTP
- E. VPN Gateway

Answer: B

---

**QUESTION 123**

**DRAG DROP**

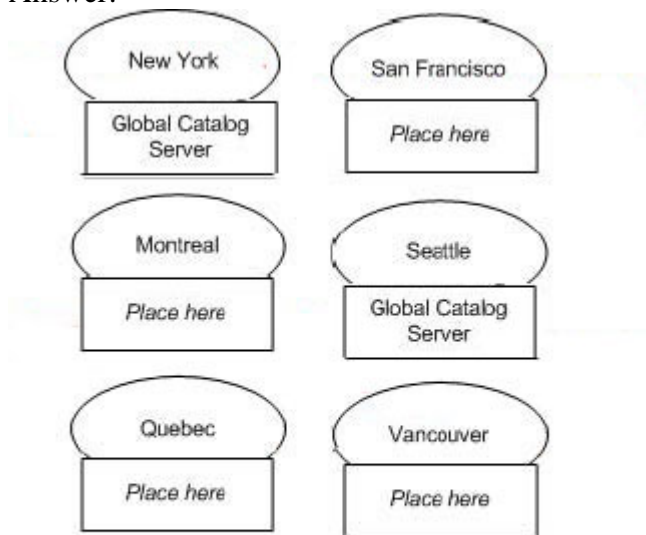
You are designing the placement of global catalog servers to meet the business and technical requirements. You need to identify the sites that require a global catalog server. What should you do?

To answer, drag the global catalog server to the correct site or sites.





Answer:



**Global Catalog server, Select this**

Global Catalbg  
Server