Review Questions

1. Answer: a, b. Fine-grained password and account lockout policies are available when you raise the domain functional level to Windows Server 2008. You can't raise the domain functional level to Windows Server 2008 until all of the domain controllers are running Windows Server 2008. It's not necessary to raise the forest functional level to support multiple account lockout policies. It's not necessary to upgrade member servers to raise the domain functional level; only domain controllers need to be upgraded.

2. Answer: a. You can reduce the three-domain forest to a one-domain forest. You'd first need to upgrade all domain controllers to Windows Server 2008 and then upgrade the domain functional level to Windows Server 2008. Next, you could create fine-grained policies for the users in the two-child domains, use the Active Directory Migration Tool (ADMT) to migrate all the accounts to the root domain, and delete the child domains. Because the domains were created just to support additional password policies, it's not necessary to keep them once you have upgraded to Windows Server 2008 and implemented fine-grained password policies. Creating a new forest does not reduce the number of domains and is not required.

3. Answer: d. You can reduce the two-domain forest to a one-domain forest. You'd first need to upgrade all domain controllers to Windows Server 2008 and then upgrade the domain functional level to Windows Server 2008. Next, you could create fine-grained account lockout policies for the original users in the child domain, use the Active Directory Migration Tool (ADMT) to migrate all the accounts to the root domain, and delete the child domains. Because the child domain was created just to support additional password policies, it's not necessary to keep the child domains once you have upgraded to Windows Server 2008. You can't delete the root domain without removing the forest. Fine-grained password policies are used in a single domain, not in multiple domains. Creating a new forest does not reduce the number of domains and is not required.

4. Answer: b. A Windows Server 2003 server cannot be promoted to a domain controller if the domain functional level is greater than Windows Server 2003. Because the forest functional level is Windows Server 2008, the domain functional level of all domains in the forest is also at least Windows Server 2008. Member servers can be promoted to domain controllers. Forest functional levels (and domain functional levels) cannot be demoted.

5. Answer: a. RODCs require the forest functional level to be at least Windows Server 2003. Because the forest functional level is already Windows Server 2003, the functional level does not need to be modified. It's not necessary to raise the domain functional level or the forest functional level. Also, you can't raise the forest functional level to Windows Server 2008 without raising the domain functional level to Windows Server 2008.

6. Answer: c. A forest trust is needed, but it cannot be created until the forest functional level is raised to at least Windows Server 2003 in both forests. Because the other forest is in the Windows Server 2000 forest functional level, it must be raised first. A User Principal Name (UPN) is another logon name that individual users can use, but it would not help in this scenario. It's not necessary to raise both forests to Windows Server 2008.

7. Answer: b. You should create two single-domain forests and raise the forest functional level of both to at least Windows Server 2003 so that a forest trust can be created between them. Replication traffic between the two headquarters offices will be minimized by keeping separate forests. A forest trust between the two forests will ensure that administrators can grant users access to resources in any of the domains. A single-domain forest would require extensive replication between the main offices. Leaving the design with six domains doesn't minimize the number of domains as much as possible.

8. Answer: b. A two-domain forest with a child domain for the subsidiary provides service autonomy for the subsidiary because it can manage its domain independently. A single domain with an OU for the subsidiary will provide data autonomy but not service autonomy. Separate forests will provide isolation, but only autonomy is desired, not isolation.

9. Answer: c. The forest should be reduced to two domains: Cengage.com and Contracting.Cengage.com. Because Contracting.Cengage.com requires service autonomy, it must be a separate domain. The RnD domain needs separate password and account lockout policies, which can be supported with fine-grained policies in the same domain. Data autonomy is required by NW.Cengage.com, which can be achieved with an OU in the Cengage.com domain. It's not possible to keep the RnD.NW.Cengage.com domain without the parent NW.Cengage.com (even if it were desirable to do so).

10. Answer: c. The Active Directory Migration Tool (ADMT) is used to migrate accounts from one domain to another or

even from one forest to another. Active Directory Users and Computers (ADUC) can be used to move users within the domain, either with the Move command or by dragging and dropping with the mouse, but you can't use ADUC to move users between domains. ADPrep is used to prepare the domain or forest for new functionality, not to move users.

11. Answer: b. A forest trust with selective authentication should be used. A forest trust is transitive, but an external trust is not. Forest-wide authentication will allow any users to be granted access, while selective authentication allows you to limit which users or groups are granted access.

12. Answer: a. A one-way forest trust should be created so that Cengage trusts CourseTech to allow users in CourseTech to access resources in Cengage. Selective authentication should be used so that access can be restricted to a specific server to only the G_PartnerProject group; grant this group the Allowed to Authenticate permission on that server.

13. Answer: d. The design should include two separate forests to allow each business to completely manage its own Active Directory infrastructure. This is also known as isolation. If both businesses are in the same forest, neither will be able to completely manage its own Active Directory infrastructure. Additionally, anyone in the Enterprise Admins group will have access to both businesses.

14. Answer: d. Because the forest trust is configured with selective authentication, the Allowed to Authenticate permission must be granted in Active Directory for FS1. If the forest trust is changed to an external trust, it will only create a trust relationship for a single domain instead of all the domains in the other forest. If forest-wide authentication is used, there is a danger that other users in the partner organization will be granted access to any server in your organization.

15. Answer: c. You need to run ADPrep /ForestPrep on the forest schema master, and then run ADPrep /DomainPrep on the infrastructure master in the domain where you want to promote the Windows Server 2008 server. Running only ADPrep /ForestPrep won't adequately prepare the environment for the server to be promoted. It's not possible to run ADPrep /DomainPrep without first running ADPrep /ForestPrep.

16. Answer: c. ADPrep /ForestPrep should be run on the domain controller hosting the schema master operations master role. This is originally the first DC in the root domain, but it can be moved. The domain naming master needs to be contacted when adding or removing domains with DCpromo. The PDC emulator must be hosted on a Windows Server 2008 server to support RODCs, but ADPrep is not run on this DC.

17. Answer: b, c. Two forests should be created, and a forest trust with forest-wide authentication should be used. The two forests allow the changes to the schema in the R&D department to be isolated in the R&D department. The forest trust with forest-wide authentication will allow any of the users in the R&D department to be granted access to resources in the rest of the organization. Because a forest has only one schema, using a two-domain forest does not provide any isolation for the schema, and all users would see all changes. A forest trust with selective authentication would be used if only a limited number of users in the R&D department needed access to the organization's resources, but all of the users in the R&D department needed access to the organization's resources. A parent-child trust is created between domains in a single forest, not between domains in separate forests.

18. Answer: c. You should create two forests. The first forest will have two domains, one for each of the first two business units. The second forest is for the third business unit. Because the third business unit must be completely separate, it requires a separate forest to provide isolation. A forest shares a common global catalog, so the first two units should be in the same forest to accommodate applications that search Active Directory using the Global Catalog; being in separate domains limits the replication between these two domains. A single forest will not provide isolation for the third business unit, which legal requirements dictated must be completely separate. If three forests are used, the global catalog cannot be shared between the first two business units.

19. Answer: d. A one-way forest trust should be created in which Cengage trusts Course Technology. Because access needs to be restricted to specific users, selective authentication should be used. The users are in Course Technology and the resources are in Cengage, so the trust is created as follows:

Resources	---->	Users
Cengage		Course Technology
Trusting domain		Trusted domain

Cengage trusts Course Tech

20. Answer: d. ADMT v3.1 is an upgrade of ADMT v3.0 and needs to be used for Windows Server 2008 migrations. ADMT v3.0 is targeted for Windows Server 2003, and previous domains will not function if either forest is using the forest functional level of Windows Server 2008. It is not possible to reduce a forest functional level. If the forest functional level is 2008, the domain functional level must also be at least Windows Server 2008.

21. Answer: b. SID history must be migrated to allow users to access resources in the source forest using their original SID. If SID filtering is enabled when SID history is used, it will prevent the SIDs included in SID history from being used. The forest functional level is not relevant in this scenario.

22. Answer: b. SID filtering should be disabled in the trust to allow the users to access resources using SIDs included in SID history. If SID filtering is enabled, the SID history can still be migrated, but SIDs included in SID history are not used when accessing resources.

23. Answer: d. The Active Directory Migration Tool (ADMT) can be used to import resources from another domain. You would run ADMT from a DC in the target domain, not the source domain. Active Directory Users and Computers (ADUC) can be used to manage resources in a domain, but it can't migrate resources between forests.

24. Answer: b. You can create an alternative UPN suffix to allow users to log in using a User Principal Name (UPN), which mimics an e-mail address. This UPN suffix can be assigned to the new users. An MX record is created in DNS to locate Microsoft Exchange servers. SID history and SID filtering wouldn't affect how a UPN is used.

25. Answer: d. All of the factors will affect the upgrade. Time should be allotted to do adequate planning and implement a phased upgrade. Resources and funding are needed to accomplish the upgrade. Applications need to be considered to ensure that the upgrade does not affect the business's mission.

Case Projects

Case Project 1-1 Solution: Only one domain is needed. Fine-grained password policies can be used to support different passwords in a single domain. The domain must be raised to Windows Server 2008, meaning that each domain controller must be upgraded to at least Windows Server 2008.

Case Project 1-2 Solution: The domain functional level must be raised to at least Windows Server 2008 to support multiple account lockout policies in a single domain. All domain controllers must be upgraded to at least Windows Server 2008 and the domain must be raised to at least the Windows Server 2008 domain functional level. Member servers do not need to be upgraded to support this plan.

Case Project 1-3 Solution: Merge the two forests into a single forest. Data autonomy allows a business entity independent control over a resource, but not exclusive control over the resource. Course Technology could be merged into a separate domain, or as a separate OU in an existing domain. A separate domain would also allow Course Technology to have service autonomy, while a separate OU would allow them to have only data autonomy. Microsoft has published a relevant TechNet article that can be viewed at *http://technet.microsoft.com/library/cc770331.aspx*.

Case Project 1-4 Solution: Create a two-way forest trust with selective authentication. The current forest functional level of Windows Server 2003 supports a forest trust, so it will not need to be modified. After the trust has been created, you'll need to grant the Allowed to Authenticate permission to groups or users in the other forest for each computer or server they need to access.