Managing, Monitoring, and Troubleshooting the Exchange Organization

Terms you'll need to understand:

- ✓ Back-end server
- ✓ Child folder
- ✓ Default public folder tree
- ✓ Front-end server
- ✓ General-purpose public folder tree
- ✓ Internet Protocol Security (IPSec)
- ✓ Outlook Web Access (OWA)
- ✓ Parent folder
- ✓ Public folder
- ✓ Public folder tree
- ✓ Replication
- ✓ Top-level folder
- ✓ Virtual server

Techniques you'll need to master:

- ✓ Creating and managing public folders
- ✓ Troubleshooting public folder issues
- ✓ Configuring and managing virtual servers
- ✓ Configuring and managing front-end and back-end servers
- ✓ Troubleshooting front-end and back-end servers

Introduction to Public Folders

In the chapters prior to this, we've mentioned the term public folder several times and we've even examined how to configure policies for them, but we've not really introduced public folders or their purpose in the Exchange infrastructure. If you've used Usenet newsgroups, you've got a basic idea of one type of data that can be stored in public folders—but Exchange provides much more than just newsgroups in its public folders!

Public folders are basically a storage location that can be used to store various types of information, such as email, documents, multimedia files, and so on, for sharing with many users. Users can access Exchange public folders natively within the organization using the Outlook client. In addition, public folders can be accessed via Hypertext Transfer Protocol (HTTP) and the venerable Network News Transfer Protocol (NNTP) by users who might be located outside of your organization's network.

As you might well suspect by now, public folders are created and located in public folder stores on Exchange servers. Public folders are mail-enabled and exist as objects within Active Directory. Public folders are arranged hierarchically in a tree structure known appropriately enough as the *public folder tree*. *Parent folders* contain *child folders*, and the folders that exist directly under the root of the public folder tree are called *top-level folders*. One of the more unique, and potentially troublesome, things about public folders is that they can actually be created and configured from within Outlook. We examine this more later in this chapter.

As mentioned previously, public folders can be accessed by both internal and external clients—assuming that you've configured the public folder permissions for such. Internal clients connect to the public folders using Messaging Application Programming Interface (MAPI)–compliant Outlook, HTTP, or NNTP, as previously discussed. Now that you have a basic idea of what a public folder is, you might be wondering what the need for public folders is. Public folders have virtually endless possible uses and are only limited by your imagination. Perhaps the most common uses for public folders are hosting Usenet newsgroups for internal clients, hosting Usenet newsgroups for external clients (such as `microsoft.public.cert.mcse`), providing a storage location for Outlook forms, and providing a discussion area for internal users similar to a newsgroup.

Public folders in Exchange Server 2003 have some nice features of which you should be aware:

- Users can post email messages directly to public folders, such as to participate in an ongoing discussion.
- Users can send email messages to the email address of the public folder, thus allowing the message to be posted in the folder.
- Public folders can be stored in multiple public folder trees via replication to increase their availability and reduce wide area network (WAN) link usage.
- Public folders can be accessed using a uniform resource locator (URL).
- Like mailbox stores, public folders can also be full-text indexed to make searches against them more efficient for the user.

Public Folder Trees

As mentioned previously, public folders are located in public folder trees, which are located on Exchange servers. When the Exchange installation is performed on a server, one default public folder store and public folder tree are created. The default public folder tree is thus replicated to all public folder servers by default. You can, however, create additional public folder trees as your organization might require. In the next paragraphs, we examine the specifics of *default public folder trees* and *general-purpose public folder trees*.

The Default Public Folder Tree

As mentioned previously, the default public folder tree is created automatically with the Exchange installation and is configured to automatically replicate to all public folder servers by default. This is the public folder tree that you will see listed in the Exchange System Manager as "Public Folders" and in Outlook as "All Public Folders."

Clients can access the default public folder tree using MAPI, HTTP, or NNTP. There can be only one public folder tree that can be accessed via MAPI, and that is the default public folder tree. As we discuss in the next section, all general-purpose public folder trees are accessed by using HTTP or NNTP. The default public folder tree contains the listing of all public folders located within that tree—but does not contain the content of these folders. The content remains in its original location and is only referenced by the default public folder tree—an important distinction to remember.

General-Purpose Public Folder Trees

General-purpose public folder trees are typically created to house custom applications and data that might be pertinent to only one department within

your organization. As an example, you might create one public folder tree to store various information that will be used by the Accounting department for research and other data. You could then create another public folder tree for your Engineering department to provide a centralized location to store research and development information for ongoing projects.

General-purpose public folder trees can be configured to replicate to any selected Exchange 2000 Server or Exchange Server 2003 public folder server, thus allowing you granular control over where they are stored. Access to these public folder trees is via HTTP or NNTP only, thus you need to configure your Outlook clients to access them using the Folder Home Page feature. In addition, to allow users to access the general-purpose public folder trees, you need to create and configure an HTTP virtual server or virtual directory. We discuss both of these items later in this chapter.

Public Folder Permissions

You can configure permissions on most every object within Active Directory (with a few notable exceptions), and public folders are no exception. Like other directory objects, a public folder inherits its permissions from its parent object. A top-level public folder gets its default permissions from the administrative group to which it belongs, whereas a child folder inherits its permissions from the parent folder under which it is located in the public folder tree.

Like NTFS permissions, public folder permissions are assigned by administrators (and public folder creators) to specify which users or security groups are allowed to perform specified actions in that public folder. Public folder permissions vary from NTFS permissions, however, in that you can assign both client access permissions and administrative permissions to a public folder.

Although at time of creation, a public folder inherits the permissions of its parent object, changes made subsequently to the parent object are not automatically propagated to the child object. You can force the permissions on the parent object to be propagated to the child object by manually propagating the permissions from the parent object. Note that this process overwrites the existing permissions configured on the child object.

The three categories of public folder permissions are detailed in Table 6.1.

Table 6.1 Examining the Various Exchange Public Folder Permissions

Permission Type	Description
Client permissions	Used to specify which clients (users) are to have access to the public folder. For example, you can specify which users are allowed to have read permissions and which users are allowed to have read/write permissions.
Directory rights	Used to specify which users are allowed to perform configuration on the mail-enabled public folder object in Active Directory.
Administrative rights	Used to specify administrative rights to public folders to control which administrators are allowed to exercise administrative control over a specific public folder.

We examine each type of public folder permission in more detail in the following sections.

Client Permissions

The client permissions on a public folder are a bit different than what you might typically be familiar with when configuring NTFS permissions. As you can see in Figure 6.1, client permissions revolve around roles.

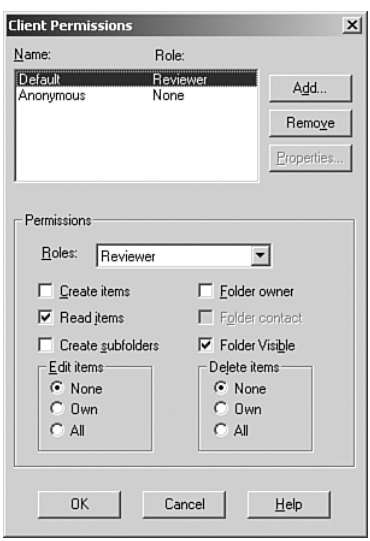

Figure 6.1 Examining public folder client permissions.

You can choose from the following roles:

- *Owner*—The user has full permissions on the public folder and can create, read, modify, and delete all items contained in the public folder. The user can also create new child folders and can change permissions on child folders.
- *Publishing Editor*—The user has permission to create, read, modify, and delete all items within the public folder. The user can also create new child folders within the public folder.
- *Editor*—The user has permission to create, read, modify, and delete all items in the public folder.
- *Publishing Author*—The user has permission to create and read items in the public folder. The user can also modify and delete items they have created as well as create new child folders within the public folder.
- *Author*—The user has permission to create and read items in the public folder. The user can also modify and delete items they have created within the public folder.
- *Nonediting Author*—The user has permission to create and read items in the public folder.
- *Reviewer*—The user has permission only to read items in the public folder.
- *Contributor*—The user has permission to create new items in the public folder but cannot view the contents of the folder.
- *None*—The user has no permissions configured for the public folder.

Directory Rights

By configuring the directory rights on a public folder, you can configure the standard NTFS permissions that you might be familiar with from the public folder object within Active Directory. The Directory Rights dialog box with a sample public folder is shown in Figure 6.2.

When configuring directory rights, you should be aware of the default status of the following groups:

- *Domain Admins*—Members of the Domain Admins group are responsible for all administrative tasks within their domain. They can manage user accounts, contacts, groups, mailboxes, client computers, and servers within their domains. Although members of the Domain Admins group have a fair amount of control over Exchange servers, they do not have full control.

➤ *Enterprise Admins*—Members of the Enterprise Admins group are the highest level of administrators within an enterprise and can manage any Active Directory object in the entire enterprise. Members of the Enterprise Admins group have full control over Exchange servers and can, thus, perform any configuration or management task they choose.

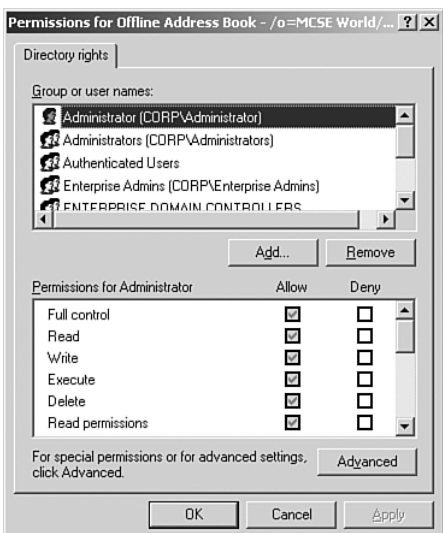

Figure 6.2 Directory rights allow you to control who can configure permissions on a public folder.

Administrative Rights

The final type of public folder permission is administrative rights. Administrative rights allow you to configure who will be able to actually administrate the public folder—something that client permissions and directory rights do not do for you. The Administrative Rights dialog box for an example public folder is shown in Figure 6.3.

The rights you can configure from this area are different than those granted by the Owner client permission. These rights deal with the system configuration of the public folder, not with the user permissions associated with the public folder.

Public Folder Replication

By default, any newly created public folders are not replicated to other Exchange servers—only one copy, the original copy, exists. For many reasons, you might want to configure your public folders to replicate to other public folder servers, thus creating replicas on these servers. Having replicas

of public folders helps to evenly distribute the load caused by an abundance of client access to public folders as well as provides a form of redundancy in the event one or more public folder servers becomes unavailable. Just like Active Directory, Exchange public folder replicas exist in a multimaster environment in which no one public folder is the master copy. All replicas of a given public folder are identical (after replication has completed) and a change made to any replica is then replicated to all other replicas, including the original public folder.

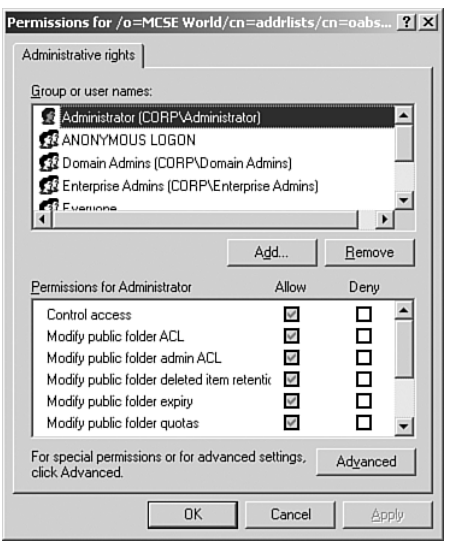

Figure 6.3 Administrative rights allow you to configure who can administer the public folder.

Public folder replication occurs through SMTP. Don't let this throw you for a loop though. Consider the obvious benefits—this allows for public folder replication to occur using the same protocols and connectors you've already got installed in your Exchange organization. Because of this, replicas can exist on public folder servers that might actually be located on a different physical network or subnet, again providing a load-balancing effect for client access.

Public folder replication is actually a somewhat complex process that is controlled by two different services.

- *Exchange Information Store Service*—Responsible for the actual replication of public folder trees. This service is also responsible for the replication of the actual public folder content itself, which includes message body, message header, and any attachments.

- *Active Directory*—Responsible for the replication of mail-enabled objects within the public folder. These objects are replicated to domain controllers and global catalog servers, just as user accounts and groups are.

As much sense as creating replicas of public folders makes, there are actually times when you might not want to configure a replica for a public folder. For example, if your public folder is used to hold Usenet newsgroups, the extra traffic due to replication is probably not worth any benefit you might reap. You would be better off, in this instance, to simply configure multiple public folder servers to independently provide this service, if required.

Another instance in which you might not want to configure replication to occur is if you must maintain absolute version control over the contents of the public folder and ensure it is always 100% up to date. In this situation, you would be better off to ensure that all clients, local and remote, have adequate access to the single public folder location. These are two somewhat extreme cases, however. In the vast majority of public folder instances, you need to give consideration to configuring multiple replicas to increase availability and provide load balancing as discussed previously.

Now that we've discussed public folder replication in general terms, we need to examine exactly how it works. The public folder replication process breaks down nicely into four distinctly different processes:

- *Hierarchy replication*—During this stage of the public folder replication process, public folder trees are replicated to all of the associated public folder stores within your Exchange organization.
- *Content replication*—During this stage of public folder replication, the actual data contained within the public folder is replicated between all associated public folder stores. When changes are made to this data, messages are triggered that replicate these changes to all of the other replicas.
- *Backfill replication*—During this stage of public folder replication, stores receive any missing updates that they need to be fully synchronized with all other stores. Backfill replication typically occurs when a public folder store has become out of synchronization.
- *Content conflict resolution*—During this final stage of public folder replication, more of an error mechanism than anything else, content conflict resolution occurs. A content conflict generally occurs when the same item has been modified by more than one user at the same time using different public folder servers. As you might suspect, two different types of conflicts can occur: message edit conflicts and folder edit conflicts. In

the event of a message edit conflict, a message is sent to the public folder contact (responsible person) who determines which version to retain. In the event of a folder edit conflict, the most recently saved version is kept.

Public Folder Referral

The final topic we must cover here is that of *public folder referral*—or how clients actually make connections to public folders. The public folder to which the user wants to make a connection might be located in the same routing group as that user or perhaps on a server in another routing group. Recall that Exchange routing groups are similar to IP sites in that they are groups of servers that are connected by high-quality, permanent links.

If a user is attempting to connect to a public folder that has a replica in the same routing group as the client (the routing group that contains the user's mailbox store), the client first attempts to connect to the replica using the default public store that is associated with the mailbox store for that user account. Recall from Chapter 5, "Managing Address Lists and Exchange Policies," the discussion on configuring mailbox store policies in which you could configure a default public folder store for a mailbox store. In the event that the replica in question does not exist on the default public folder store, the client then makes a connection to a randomly selected replica within the client's routing group. The process continues until the client either locates the desired replica or runs out of local replicas. In the event that the desired replica is not found locally (within the client's routing group), the client needs to gain access to a replica located in another (remote) routing group—herein lies the act of public folder referral.

Routing groups are connected to each other using group connectors. Routing group connectors have a cost value (think metric) associated with them that determines the flow of traffic out of that routing group. Cost values range from a low value of 1 to a high value of 100, with the lower values being the more preferred routes out of the routing group. When a client needs to connect to a remote routing group to access a public folder replica, the lowest cost connection is used. However, one more issue must be kept in mind in this situation—whether public folder referrals are allowed across that routing group connector. By default, public folder referrals are allowed on routing group connectors. In addition, both routing group connectors in both routing groups must be configured to allow public folder referrals. As an alternative (and you knew there had to be one), you can actually configure a referral list directly on a public folder store, thus forcing clients seeking a referral to choose a store from the list.

Creating, Managing, and Troubleshooting Public Folders

With our introduction to public folders out of the way, we can now move forward and examine some of the more common tasks that you should be prepared to manage, and troubleshoot public folders within your Exchange organization. These tasks include, but are not limited to, the following:

- Creating general-purpose public folder trees
- Configuring client permissions for public folders
- Managing public folder replication
- Managing public folder referral
- Managing public folder full-text indexing
- Troubleshooting public folder replication issues
- Troubleshooting other public folder issues

We briefly examine each of these tasks in the following sections.

Creating General-Purpose Public Folder Trees

You might need to create new general-purpose public folder trees for any number of reasons. Some of the more common reasons include hosting Usenet newsgroups and providing departmental public folder stores.

To create a new general-purpose public folder tree, perform the following steps:

1. Open the Exchange System Manager.
2. Expand the administrative group within which you want to create the new public folder tree.
3. Right-click the Folders container and select New, Public Folder Tree from the context menu, as shown in Figure 6.4.
4. The public folder tree Properties dialog box opens to the General tab. Enter a descriptive name for the new public folder tree. Click OK to close the Properties dialog box. The new public folder tree appears in the Folders container.

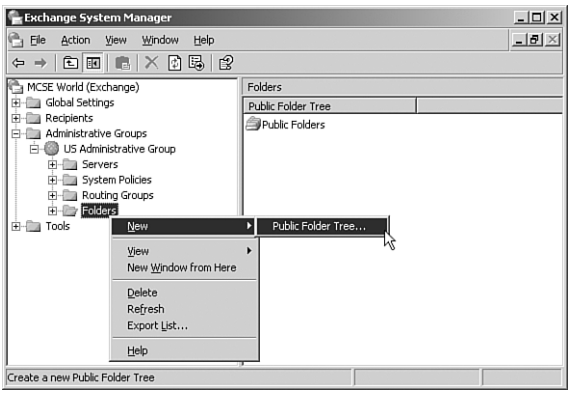

Figure 6.4 New public folder trees are created at the administrative group level.

With the new public folder tree created, you now must create a public folder store with which to associate it. Without a public folder store, the public folder tree is inaccessible to clients.

To create a new public folder store, perform the following steps:

1. Open the Exchange System Manager.
2. Locate the administrative group in which you just created the new public folder tree. Expand the Servers node and locate the server and storage group within which you want to create the new public folder store.
3. Right-click the selected store group, and select New, Public Store from the context menu, as shown in Figure 6.5.

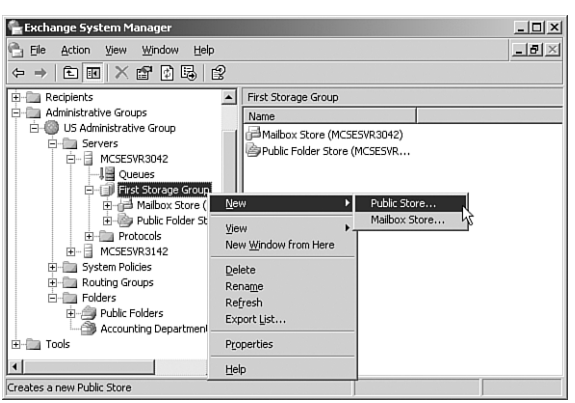

Figure 6.5 You must create a new public folder store to house the new public folder tree.

4. The public folder store Properties dialog box opens to the General tab. Enter a descriptive name for the new public folder store.
5. Click the Browse button to open the Select a Public Folder Tree dialog box, as shown in Figure 6.6. Select the applicable public folder tree (the one created in the preceding exercise), and click OK.

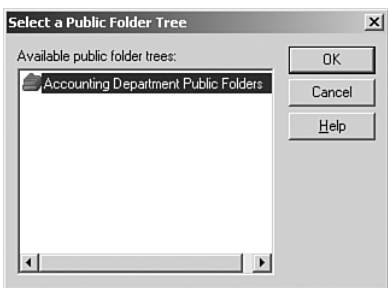

Figure 6.6 After you create the new public folder store, you need to associate it with a public folder tree.

6. Click OK to close the public folder store Properties dialog box.
7. When prompted to mount the public folder store, click Yes—this makes it available immediately to clients.
8. Click OK to acknowledge the public folder store was successfully mounted.

Configuring Client Permissions for Public Folders

As discussed previously in the "Client Permissions" section of this chapter, public folders have a somewhat unusual assortment of permissions that can be applied to them. Recall that client permissions are used to assign users roles that define what they are capable of doing within a public folder. By default, all users have the Author role, which allows the user to create and read items in the public folder. The user can also modify and delete items they have created within the public folder.

Client permissions are also unique because they can be modified from two distinctly different locations: from the Exchange System Manager and from within Outlook. Outlook has the limitation of not being able to access general-purpose folder trees, thus you can only use Outlook to configure the client permissions on the default public folder tree. Client permissions for

general-purpose folder trees can only be configured using the Exchange System Manager.

When working with client permissions, keep the following points in mind about how they are applied to users:

- Client permissions that are explicitly (directly) granted to a user are the only ones that will be applied to that user.
- When a user is a member of a single security group that has client permissions configured for the public folder, the user's net permissions are the least restrictive of the group permissions or the implicit (default) permissions of the public folder. Note that this is in direct contrast to the typical behavior of NTFS permissions.
- When a user is a member of multiple security groups that have client permissions configured for the public folder, the user's net permissions are the least restrictive of the implicit (default) public folder permissions or the most restrictive of all permissions configured on the security groups of which the user is a member.

To configure public folder client permissions from within the Exchange System Manager, perform the following steps:

1. Open the Exchange System Manager.
2. Locate the public folder (not public folder tree) for which you want to configure the client permissions, as shown in Figure 6.7. Right-click the public folder and select Properties from the context menu.

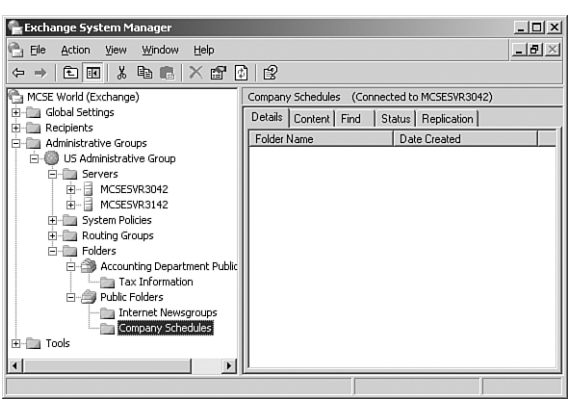

Figure 6.7 You configure client permissions for a public folder, not for a public folder tree.

3. The public folder Properties dialog box opens. Switch to the Permissions tab and click the Client Permissions button.

4. The Permissions dialog box opens (refer back to Figure 6.1).
5. Configure the public folder client permissions as required.

To configure public folder client permissions from within Outlook, perform the following steps:

1. Open Outlook.
2. In the folder list, locate the public folder for which you want to configure client permissions.
3. Right-click the public folder and select Properties from the context menu.
4. The Properties dialog box opens, as shown in Figure 6.8. Switch to the Permissions tab and configure the desired client permissions.

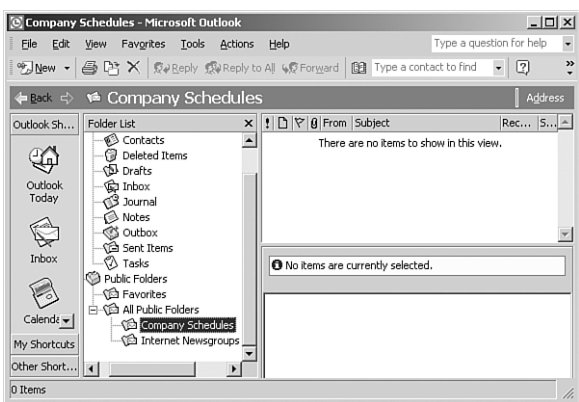

Figure 6.8 You can configure client permissions for the default public folder tree from within Outlook.

Managing Public Folder Replication

Replication is critical for making your public folders available to all clients in all locations, regardless of the routing group or physical location in which they might be located. Replication can also be configured so that only specific routing groups contain a replica of a public folder as a means to limit access to that public folder. Recall that the default public folder tree is automatically configured to replicate to all Exchange servers using the "Public Folder Store" public folder store. General-purpose public folder trees are not automatically configured to replicate.

Three basic steps are involved with configuring public folder replication: creating the replica, configuring the replication schedule, and monitoring the replication process. We briefly examine each of these items in the following paragraphs.

The first two steps to configuring replication of a public folder are to create a replica on another Exchange server and to configure replication to occur. To accomplish these tasks, perform the following steps:

1. Open the Exchange System Manager.
2. Locate the public folder for which you want to create a replica. Right-click the public folder and select Properties from the context menu.
3. The public folder Properties dialog box opens. Switch to the Replication tab, as shown in Figure 6.9.

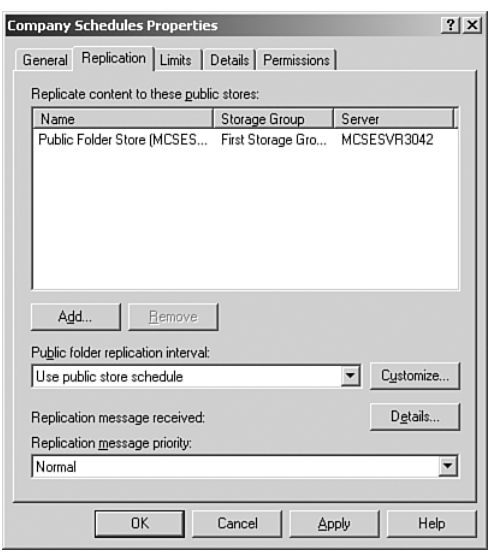

Figure 6.9 You configure replication from the Replication tab of the public folder Properties dialog box.

4. Click the Add button to select another public folder store on which to create a replica of this public folder.
5. Use the Public folder replication interval drop-down list to configure the replication schedule for the public folder.
6. Close the public folder Properties dialog box.

You'll be able to see that the public folder is configured for multiple replicas and also be able to monitor the replication status using the Replication tab of the public folder, as shown in Figure 6.10.

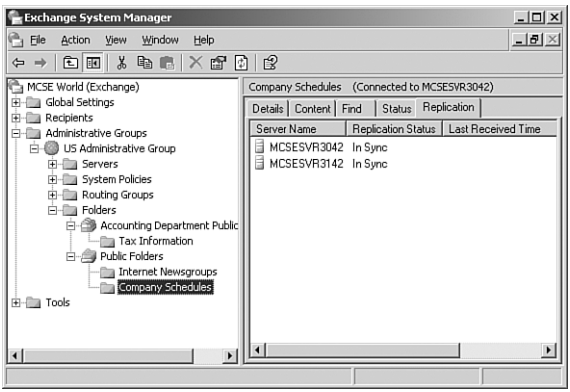

Figure 6.10 You can easily determine which servers house replicas of a selected public folder.

Managing Public Folder Referral

As discussed previously in the "Public Folder Referral" section of this chapter, clients that cannot locate a local (local to their routing group) replica of a public folder need to utilize a public folder referral to locate and access a remote routing group's replica of the public folder. Recall that public folder referral can be controlled in one of the two following locations: on the routing group connector connecting the routing groups in question or directly on the public folder itself. You can use only one method of controlling public folder referral.

To control routing group public folder referrals, open the routing group connector Properties dialog box and select or deselect the Do not allow public folder referrals check box, as shown in Figure 6.11.

Alternatively, you can configure public folder referrals to specific Exchange servers on a server level using the server Properties dialog box. On the Public Folder Referrals tab, shown in Figure 6.12, you can use the drop-down list to change from routing group controlled to custom list controlled. After you've selected Custom List, you can enter servers and the route costs associated with them as needed (think of route costs as route metrics).

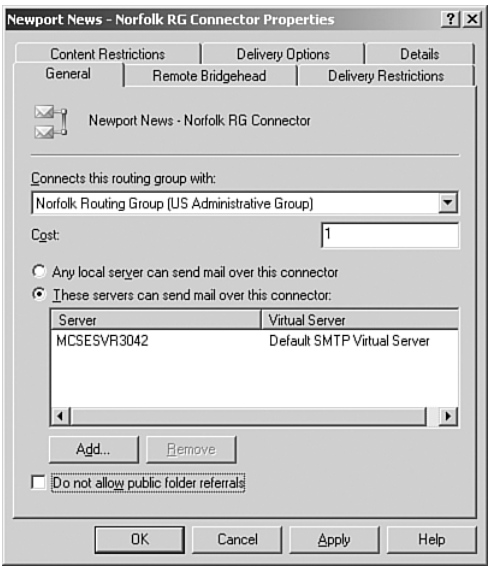

Figure 6.11 You can control public folder referrals over a routing group connector from the routing group connector's Properties dialog box.

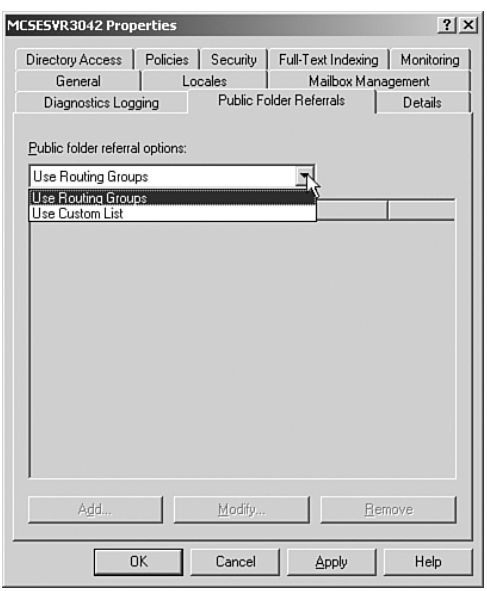

Figure 6.12 You can configure specific Exchange servers to perform public folder referrals to.

Managing Public Folder Full-text Indexing

As we discussed in previous chapters, full-text indexing on a store allows clients to search for and locate information more quickly. The downsides are increased system utilization during the indexing process and, of course, increased disk space usage as the indexes can grow quite large. For best performance, you should always place your full-text indexes on a separate physical drive or set of physical drives (such as a mirrored set) than the drive on which the operating system, Exchange files, and Exchange databases are located. Indexes are typically 20% as large as the database they have been created from, so a 10GB database will likely yield a 2GB full-text index.

Don't let the amount of space required scare you away from creating full-text indexes. The following benefits are provided as a result of full-text indexing:

- Each store can be configured for indexing independently of every other store. This includes whether or not to have an index, how often to update the index, and where to physically store the index. These options give a great deal of control over how indexing is performed in your organization.
- Searches against the index include related words to the search string for more choices.
- Searches are faster because the search is scanning an index of the database versus scanning the entire database.
- Searching of common attachment types is provided, thus allowing the user to search for information contained not only within a message, but also within its attachments. Only the following file formats can be indexed within: .eml, .txt, .htm, .html, .asp, .doc, .xls, and .ppt.

Of course, as we've already briefly examined, there are some drawbacks to creating and using full-text indexes:

- The disk space required for a full-text index grows quickly. Full-text indexes should be placed on a different physical disk or set of disks than the database they are indexing.
- A significant amount of system time and resources might be consumed creating the index for the first time.
- Search results might be incomplete or inaccurate if clients are using the index before it is fully populated. You can, however, prevent this from occurring by disabling searching of the index during this time.

To implement and configure full-text indexing on a public folder, perform the following steps:

1. Open the Exchange System Manager.
2. Locate the public folder store for which you want to enable full-text indexing, and right-click it. Select Create Full-Text Index from the context menu.
3. You are prompted for the location to place the full-text index, as shown in Figure 6.13. Enter your selection and click OK.

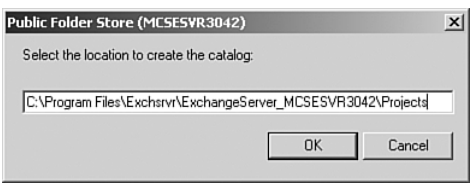

Figure 6.13 You should place the index on a different physical disk than where the database is located.

4. Right-click the public folder store, and select Properties from the context menu. Switch to the Full-Text Indexing tab, shown in Figure 6.14.

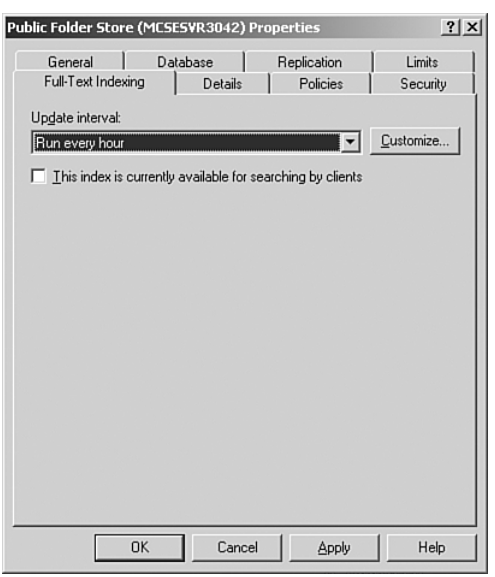

Figure 6.14 You need to configure an indexing schedule.

5. Configure the indexing interval you desire. Note that you can also disable searching of the index as required. Click OK to close the public folder store Properties dialog box.
6. To populate the index, right-click the public folder store and select either Start Incremental Population or Start Full Population from the context menu. These options are discussed in more detail following this exercise.
7. Acknowledge the one (for incremental population) or two (for full population) warning(s) you receive by clicking Yes.

An incremental population event causes only new and modified items to be indexed. During normal scheduled indexing, incremental population occurs to keep the index up-to-date. A full population event causes all items in the public folder store to be indexed or reindexed, regardless of their current state of modification. This results in the entire index being rebuilt, one document at a time, and could take a significant amount of time and system resources to perform. It is not recommended that you perform a full population during normal business hours.

Troubleshooting Public Folder Replication Issues

Public folder replication is an event that typically occurs invisibly to users. Only when it does not work correctly do you hear about it. In Table 6.2, we examine some of the more common replication issues you might experience as well as some suggested courses of action.

Table 6.2 Common Public Folder Replication Problems and Solutions

Problem	Suggested Solution
Replication messages are not being received	Several different problems might result in this situation. Some of the more common include: ➤ *The public folder stores do not have valid email addresses*—Ensure that the Recipient Update Service (RUS) has applied the email address to the public folder store's directory objects. ➤ *Replication messages have no route to follow*—Ensure that normal message traffic is flowing between the servers in question.

(continued)

Table 6.2 Common Public Folder Replication Problems and Solutions *(continued)*	
Problem	**Suggested Solution**
Backfill occurs very slowly	Backfill takes a long time when a new server is installed and the initial status request has been lost or sent to a server that has no knowledge of the public folder hierarchy. To monitor this solution, you can make a hierarchy change on a different server and check to see that it has replicated to the server in question within one to two days.
Backfill does not occur	Check to see if new folders recently added to other servers' replicas have been replicated during the hierarchy replication portion of replication. After the hierarchy has been updated, the replica will deem itself out of synch and complete the backfill synchronization, which might take several days to complete fully.

Troubleshooting Other Public Folder Issues

Of course, replication errors are not the only type of error you might encounter with public folders. To that end, some of the other common types of errors you might encounter are presented in Table 6.3.

Table 6.3 Common Public Folder Problems and Solutions	
Problem	**Suggested Solution**
Cannot access permissions on a public folder (Invalid Windows Handle Error)	This problem is commonly caused as a result of an administrator configuring permissions on the M drive (the Exchange Installable File System) on a public folder. Although new installations of Exchange Server 2003 no longer use the M drive, it will still be present in upgrade situations. When permissions are modified through Windows (instead of through the Exchange System Manager), the permissions are modified such that Exchange can no longer convert them into their correct MAPI format. As a result, users can no longer use the dialog boxes in the Exchange System Manager or Outlook to edit public folder permissions. To correct this problem, you need to move the affected public folders into a newly created top-level public folder and force permission propagation to occur. This corrects the problem, but also overwrites all custom permissions entries, resulting in the affected public folders having permissions for only the folder owner (an administrative account), Default users, and Anonymous users.

(continued)

Table 6.3 Common Public Folder Problems and Solutions *(continued)*

Problem	Suggested Solution
Cannot add users to the public folder access list	This problem can occur when a user without a mailbox creates or modifies a public folder resulting in the user having explicit permissions on the public folder. You can correct this problem by creating a mailbox for this user or by removing them from the Client Permissions dialog box listing.
Messages sent to the public folder were not delivered	This problem might occur for a couple of different reasons. Email cannot be delivered to general-purpose public folder trees if the message must travel through an Exchange 5.5 server. In addition, email must make its way to the correct public folder store that houses the replica of the public folder—this process can take some time.
Attachment size exceedsthe limit on the public public folder	This problem can occur when a user attempts to post an attachment to a folder that is larger than 1024KB in size. Users will receive the following message: "This item exceeds the maximum size defined for this folder and cannot be saved. Contact your administrator to have the folder limits increased." The problem is a result of the 1024 KB default size limit on the OWAScratchPad{GUID} system folder. You can increase this size limit by changing the Maximum Item Size (KB) value for the OWAScratchPad folder in the Public Folders folder tree.

Introduction to Virtual Servers

Just as they were in Exchange 2000 Server on Windows 2000 Server, Exchange Server 2003 and IIS 6.0 are tightly integrated to provide a robust messaging solution that is capable of supporting multiple messaging protocols. Exchange Server 2003 supports messaging using the following protocols:

- Post Office Protocol version 3 (POP3) using port 110 default and port 995 by default for POP3 over SSL (Secure Sockets Layer). POP3 is a standard, and fairly limited, email retrieval protocol that remote users can use to access their Exchange mailboxes. Outlook and Outlook Express support POP3.
- Internet Message Access Protocol version 4 (IMAP4) using port 143 by default and port 993 for IMAP4 over SSL. IMAP4 is a newer, and more complex, email retrieval protocol that supports a more advanced feature set than POP3. IMAP4 allows you to organize messages by creating

folders on the server and also allows for message preview by only downloading message headers instead of the entire message. Outlook and Outlook Express support IMAP4.

- Simple Mail Transfer Protocol (SMTP) using port 25 by default and port 25 by default for SMTP over SSL. SMTP is used to send outgoing messages to an Exchange server and also to send messages from one server to another en route to their final destination. Outlook and Outlook Express support SMTP.
- Hypertext Transfer Protocol (HTTP) using port 80 by default and port 443 by default for HTTP over SSL. HTTP is primarily used by Outlook Web Access (OWA) clients to access their Exchange mailboxes and calendars at the URL `http://servername/exchange/`. All mailbox items are referenced by complete URLs, so the inbox can be accessed at `http://servername/exchange/mailbox/inbox`.
- Network News Transfer Protocol (NNTP) using port 119 by default and port 563 by default for NNTP over SSL. NNTP is used by newsreaders to access public folders. Outlook Express supports NNTP.

Recall that because each of these protocols uses its own default port, you only need one IP address to house multiple protocols on a single server. The true magic behind this is the virtual server. By default, Exchange creates a virtual server for each protocol listed previously, as shown in Figure 6.15.

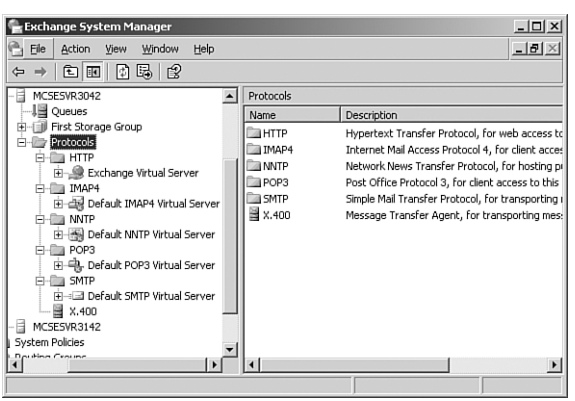

Figure 6.15 Exchange creates multiple virtual servers to facilitate mail transfer.

In a default Exchange organization, only the HTTP and SMTP virtual servers are operational. You can opt to enable the POP3, NNTP, and IMAP4 virtual servers as needed. Alternatively, you might want to remove some virtual servers from one server and re-create them on a different server in an effort to load-balance client access to your Exchange servers.

In larger environments, you might consider placing one protocol on one physical server, further reducing server loading. Alternatively, you might need to create multiple virtual servers for SMTP or NNTP to provide both load balancing and redundancy for client access to these services.

Configuring and Managing Virtual Servers

Unless you are creating an organization with distributed Exchange protocols—one or more servers dedicated to serving one protocol—your exposure to managing virtual servers will likely be very limited. Some of the more common tasks you might find yourself performing for virtual servers include

- Adding a new virtual server
- Starting, stopping, or pausing a virtual server
- Changing virtual server IP addresses and ports
- Limiting inbound connections to virtual servers
- Configuring SMTP relay settings

We examine each of these tasks in the following sections.

We examine more virtual server–related items in our discussion of front-end/back-end server arrangements later in this chapter.

Adding a New Virtual Server

You might need to create a new virtual server for any number of reasons. Typically, you most commonly create an additional SMTP virtual server, and thus we examine this process here. To create a new SMTP virtual server, perform the following steps:

1. Open the Exchange System Manager.
2. Locate the Protocols folder for the physical server for which you want to create a new SMTP virtual server and expand it.
3. Right-click the SMTP folder and select New, SMTP Virtual Server from the context menu.

4. Enter the name of the new SMTP virtual server, and click Next to continue.
5. Select the IP address and click Finish to complete the New SMTP Virtual Server Wizard. If there are no IP address/port conflicts, the new SMTP virtual server starts automatically.
6. If you need to configure additional properties for the new SMTP virtual server, do so by right-clicking on it under the SMTP folder and selecting Properties.

Starting, Stopping, or Pausing a Virtual Server

Should you, for any reason, need to change the operational status of any virtual server, you can do so easily from the context menu. Simply right-click the appropriate virtual server and select the desired action from the context menu.

Changing Virtual Server IP Addresses and Ports

Only one virtual server can be in operation using a specific IP address/port number combination. If you create a new virtual server and your server has only one IP address, the new virtual server cannot start until it has been assigned a unique port number. To change the IP address and/or port number that is assigned to a virtual server, perform the following steps:

1. Open the Exchange System Manager.
2. Locate the Protocols folder for the physical server that houses the virtual server of concern and expand it.
3. Right-click the virtual server of concern, and select Properties from the context menu.
4. The currently configured IP address displays on the General tab, as shown in Figure 6.16.
5. To modify the values, click the Advanced button to open the Advanced dialog box shown in Figure 6.17. From here, you can add, edit, or remove IP address and port combinations as required. Note that you can only use IP addresses that are actually assigned to the server.

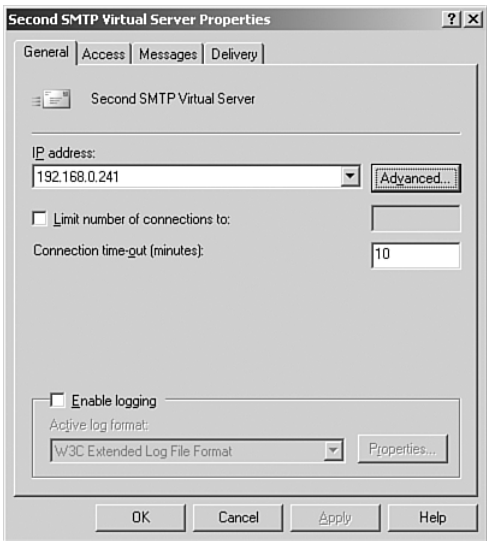

Figure 6.16 You must configure each virtual server with a unique IP address and port number.

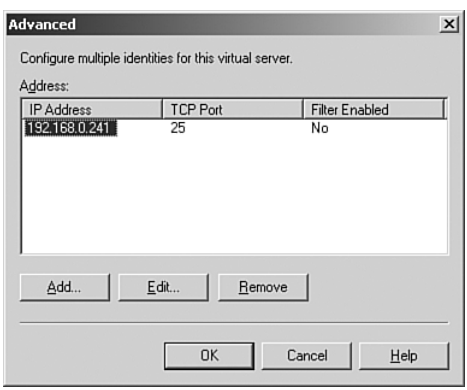

Figure 6.17 You can configure exact IP address/port number combinations for your virtual server.

6. Click OK to close the Advanced dialog box.
7. Click OK to close the virtual server Properties dialog box.

Limiting Inbound Connections to Virtual Servers

Gone are the days when you could blindly allow just anyone to access your email organization. Fortunately, Exchange provides several ways that you can configure your virtual servers to limit inbound connections—and we're

not even to the discussion on configuring SMTP relays! You have the following general options available to you to limit and control inbound connections to your Exchange virtual servers:

- Granting or denying access by IP address, subnet, or domain
- Requiring secure inbound connections
- Requiring authenticated inbound connections
- Restricting multiple concurrent connections and enforcing connection time limits

We briefly examine each of these items in the following sections.

Granting or Denying Access by IP Address, Subnet, or Domain

By default, your Exchange server allows inbound connections from any IP address that can reach it. This is not a very secure configuration, especially for those Exchange servers that might be more susceptible to attack by virtue of their location on the exterior of the protected, internal network.

When you deny access to a virtual server, you prevent all inbound connections from that IP address, subnet, or domain from being made. When you allow access to a virtual server, clients can access the virtual server, but still might not be able to send and receive messages if additional restrictions are in place, such as if inbound authentication is required.

To configure access to a virtual server by IP address, subnet, or domain, perform the following steps:

1. Open the Exchange System Manager.
2. Locate the Protocols folder for the physical server that houses the virtual server of concern and expand it.
3. Right-click the virtual server of concern, and select Properties from the context menu.
4. Switch to the Access tab, and click the Connection button to open the Connection dialog box shown in Figure 6.18.
5. Configure the Connection dialog box as required to allow or deny access to IP addresses or domains.
6. Click OK to close the Connection dialog box.
7. Click OK to close the virtual server Properties dialog box.

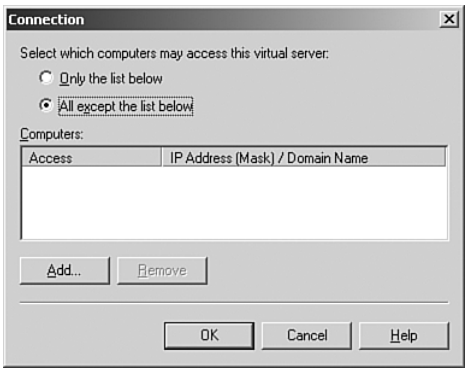

Figure 6.18 You can configure your virtual server to grant or deny access to specified IP addresses and domains.

Requiring Secure Inbound Connections

If you want to require secure inbound connections to increase security, you can enable SSL for your virtual server, thus providing a marked increase in communications security over the default unsecured connections. To configure SSL security for your virtual server, you need to install a server certificate first and then configure the settings you desire.

To configure SSL security for a virtual server, perform the following steps:

1. Open the Exchange System Manager.
2. Locate the Protocols folder for the physical server that houses the virtual server of concern and expand it.
3. Right-click the virtual server of concern, and select Properties from the context menu.
4. Switch to the Access tab, and click the Certificate button to start the Web Server Certificate Wizard.
5. Click Next to dismiss the first page of the Web Server Certificate Wizard.
6. Complete the steps required to request and submit a server certificate using the Web Server Certificate Wizard.
7. After the certificate has been installed, return to the Access tab, and click the Communication button to open the Security dialog box shown in Figure 6.19.

Figure 6.19 After a server certificate has been installed, you can enable SSL-secured communications to the virtual server.

8. Select the Require Secure Channel check box to require SSL-secured communications to this virtual server. In addition, if you want to require only 128-bit connections, select the Require 128-bit Encryption check box. Note that clients that do not support 128-bit encryption cannot make connections to the virtual server with this check box enabled. Click OK to close the Security dialog box.
9. Click OK to close the virtual server Properties dialog box.

Requiring Authenticated Inbound Connections

You can also require that users successfully authenticate themselves to the Exchange server before being able to make an inbound connection to the virtual server. Even if you do not plan on configuring the authentication options, you might want to consider that the default virtual server configuration allows for anonymous access, allowing anyone to potentially access your server.

To configure authentication for a virtual server, perform the following steps:

1. Open the Exchange System Manager.
2. Locate the Protocols folder for the physical server that houses the virtual server of concern and expand it.
3. Right-click the virtual server of concern, and select Properties from the context menu.
4. Switch to the Access tab, and click the Authentication button to open the Authentication dialog box shown in Figure 6.20. Note that the authentication methods available will vary by the type of virtual server you are configuring.

Figure 6.20 You have several authentication methods from which to choose.

5. Unless you are configuring a publicly accessible newsgroup server, it is advisable to configure the server to not allow anonymous connections.
6. If you are not using SSL security, you need to remove the Basic authentication method from your virtual server as well. Basic authentication sends user credentials over the network in an unencrypted format. If SSL is in use, Basic authentication can be used with relative safety.
7. If given the option to use Integrated Windows authentication (IWA), as in the case of an SMTP virtual server, you should always opt to use it. IWA uses standard Windows security to validate users and passes cached logon information to the Exchange server to perform authentication if this information is available. This information is already encrypted without the need for SSL, but SSL can be implemented to further secure the virtual server.
8. Click OK to close the Security dialog box.
9. Click OK to close the virtual server Properties dialog box.

Restricting Multiple Concurrent Connections and Enforcing Connection Time Limits

You can also very easily configure your virtual servers to limit the number of concurrent connections allowed as well as to limit the amount of time a connection remains in place. Both of these items provide somewhat increased

security; however, the primary purpose is to increase the availability of the virtual server by limiting the resources users can consume.

To configure connection limits for a virtual server, perform the following steps:

1. Open the Exchange System Manager.
2. Locate the Protocols folder for the physical server that houses the virtual server of concern and expand it.
3. Right-click the virtual server of concern, and select Properties from the context menu.
4. On the General tab, shown in Figure 6.21, you can configure the maximum number of concurrent connections and the timeout limit for sessions. Note that, by default, there is no maximum limit imposed on the maximum number of concurrent connections allowed.

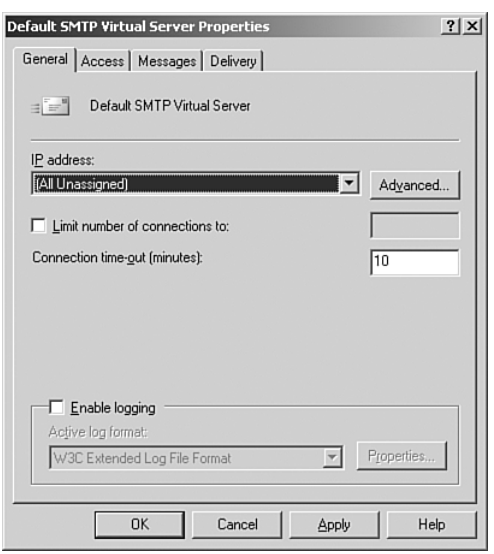

Figure 6.21 You should configure the connection number and connection timeout limits to increase virtual server availability.

5. Click OK to close the virtual server Properties dialog box.

Configuring SMTP Relay Settings

The final virtual server configuration item we examine is that of configuring SMTP relay settings. In recent years, we have all heard the horror stories of

email servers (of all types) being abused by spammers who have located an open SMTP relay configuration. This type of situation is easily avoidable, and providing an open SMTP relay is just plain irresponsible. In addition, having an open SMTP relay is one of the quickest ways to find your organization listed on a Relay Black List (RBL), which many organizations and service providers use to filter out potential spam messages. The bottom line is that you owe it to your organization and the Internet community as a whole to ensure that your Exchange servers do not become spamming tools.

It is important to understand that you do not need to allow relaying to all Internet hosts to enable inbound email to reach your organization. The process of relaying occurs when a user sends mail from one organization through another organization. The net result is that the email appears to have originated from the organization used as a relay instead of where it truly came from, thus masking the identity of the party actually sending the emails. Open SMTP relays are a spammer's best friend on the Internet.

To configure the SMTP relay settings, perform the following steps:

1. Open the Exchange System Manager.
2. Locate the Protocols folder for the physical server that houses the virtual server of concern and expand it.
3. Right-click the virtual server of concern, and select Properties from the context menu.
4. Switch to the Access tab, and click the Relay button to open the Relay Restrictions dialog box shown in Figure 6.22.

Figure 6.22 You need to carefully configure relaying on Exchange servers exposed to the public.

5. Configure the relay restrictions as you need. As an example, if the server in question was functioning as a front-end server, you might configure it to only allow relaying from your internal Exchange servers.
6. Click OK to close the Relay Restrictions dialog box.
7. Click OK to close the virtual server Properties dialog box.

Introduction to Front-end/Back-end Arrangements

By default, Exchange Server 2003 installs OWA and Outlook Mobile Access (OMA) in the Exchange organization. Although OWA and OMA can be used quite effectively internally within an organization to enable non-Windows-based clients to access Exchange mailboxes, their primary purpose is to allow users to access their Exchange mailboxes when away from the network. A typical example of a user using OWA might be a manager who is on vacation, but still needs to monitor his email daily to ensure that any items requiring his attention are taken care of promptly.

Given that the primary intended purpose of OWA (and OMA) is to provide Exchange mailbox access to users located outside of your protected internal network, some additional considerations must be given to creating and implementing a secure and highly available solution. Enter the concept of front-end/back-end Exchange servers. If you've ever worked with Network Load Balancing (NLB) or clustering, you are probably familiar with this concept. If not, a short introduction (with an emphasis on the Exchange specifics of the topic) is in order.

To learn more about NLB and clustering, be certain to read *MCSE 70-293 Training Guide: Planning and Maintaining a Windows Server 2003 Network Infrastructure* by Will Schmied and Rob Shimonski, Que Publishing, 2003.

Figure 6.23 depicts a sample front-end/back-end Exchange implementation designed to support only OWA using SSL-secured connections.

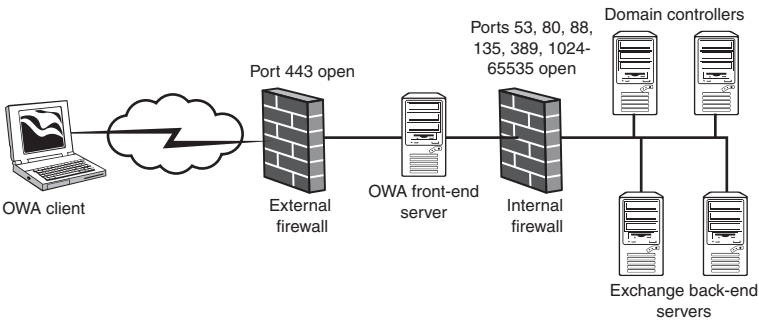

Figure 6.23 A front-end/back-end Exchange server configuration should be used to provide increased security and reliability.

Notice on the external firewall that only port 443 is open—HTTP over SSL. Inbound OWA client requests are passed to the front-end Exchange servers. These servers then communicate with the back-end Exchange servers, performing authentication of the user and making the user's mailbox available to them via OWA. Notice that several ports are open on the internal firewall. These ports are

- *53*—Port 53 is used by the front-end server to resolve hostnames on the protected internal network through Domain Name System (DNS) queries.
- *80*—Port 80 is used for the OWA traffic.
- *88*—Port 88 is used for Kerberos authentication between the front-end server and the domain controllers located on the protected internal network.
- *135*—Port 135 is used for Remote Procedure Call (RPC) to the global catalog servers and for service discovery.
- *389*—Port 389 is used for Lightweight Directory Access Protocol (LDAP) communications to domain controllers on the protected internal network through DNS queries.
- *1024–65535*—Ports 1024–65535 are used for RPC to the global catalog servers and for service discovery. In addition, port 3268 is used for LDAP communications to global catalog servers.

If you do not allow RPC ports to be open on the firewall separating the front-end and back-end Exchange servers, no client authentication can be performed on the front-end server; thus, these virtual servers need to allow anonymous access. Obviously, this is not a recommended configuration.

To further increase network security, you can implement IPSec secured communications between the front-end and back-end Exchange servers.

Configuring, Managing, and Troubleshooting Front-end/Back-end Servers

If you currently do or are planning to support users using OWA, you need to set up a secure front-end/back-end Exchange server arrangement. To achieve this goal, some of the tasks that you need to perform include, but are not limited to, the following:

- Configuring an Exchange server as a front-end server
- Configuring firewalls
- Implementing IPSec between front-end and back-end servers
- Disabling unnecessary services on front-end servers
- Troubleshooting front-end and back-end servers

We briefly examine each of these topics in the following sections.

Configuring an Exchange Server as a Front-end Server

After you've installed Exchange Server 2003 on your front-end server, you can easily configure it to act as a front-end server by changing one configuration item and then restarting it. Open the server Properties dialog box by right-clicking on the server and selecting Properties from the context menu. Select the This Is a Front-end Server check box, as shown in Figure 6.24, and click OK to close the server Properties dialog box. A warning message box appears, informing you that you need to restart the server to complete the process. In addition, the warning message box encourages you to install a server certificate to increase server security. After the server has restarted, you should install a server certificate for the HTTP virtual server and enable SSL security as previously discussed in the "Requiring Secure Inbound Connections" section of this chapter.

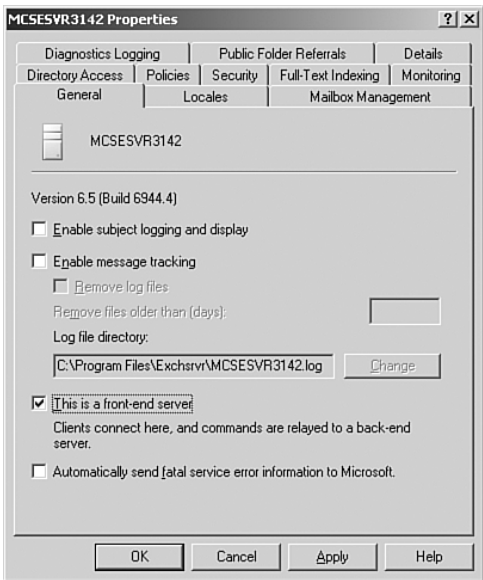

Figure 6.24 You need only select one configuration option to configure the server as a front-end server.

It is not recommended that you move the front-end server physically into the screened subnet between the internal and external firewall until you have completed all required firewall configuration.

You do not need to perform any special configuration on the servers that will be the back-end servers. You must, however, ensure that they can communicate with the front-end servers over TCP port 80 for HTTP.

Configuring Firewalls

As we saw previously in the "Introduction to Front-end/Back-end Arrangements" section of this chapter, you need to ensure that selected ports are made available on both the external and internal firewalls to ensure that your front-end/back-end OWA solution functions properly. In addition to the ports we discussed previously, you need to open additional ports to support other Exchange services. (We only examined those ports used specifically for the sample front-end/back-end OWA implementation.)

As we discussed previously in the "Introduction to Virtual Servers" section of this chapter, several other ports must be made available for other Exchange services to function properly. As a review, Table 6.4 presents the common ports that you need to enable on your internal and external firewalls for Exchange.

Table 6.4 Common Exchange Ports

Port	Function	External Firewall	Internal Firewall
110	POP3	Open *	Open *
995	POP3 over SSL	Open *	Open *
143	IMAP4	Open *	Open *
993	IMAP4 over SSL	Open *	Open *
25	SMTP	Open *	Open *
119	NNTP	Open *	Open *
563	NNTP over SSL	Open *	Open *
80	HTTP	Open *	Open *
443	HTTP over SSL	Open *	Open *
389	LDAP to domain controller	Closed	Open
3268	LDAP to global catalog	Closed	Open
88	Kerberos authentication	Closed	Open
53	DNS	Open	Open
135	RPC port mapping	Closed	Open
1024–65535	RPC service ports (can be manually assigned to a specific port using a Registry modification)	Closed	Open

Items marked with an asterisk (*) in Table 6.4 need only be open if the service is being used. In addition, you need only open the non-SSL port if SSL is not being used to secure that connection type. It is always recommended to use SSL security for inbound connections at the external firewall.

In regard to DNS, it is recommended that you place a DNS server with a secondary zone in the screened subnet for name resolution and configure one DNS server in your protected internal network as the only DNS server allowed to forward queries from the internal network outside to the Internet.

Implementing IPSec Between Front-end and Back-end Servers

One of the single greatest things you can do to increase security of the communications between your front-end and back-end Exchange servers is to

secure the communications between them using IPSec. This security, however, comes at the price of increased system utilization, as you might expect.

A common mistake that is made when configuring IPSec for use in this situation is to attempt to use the Secure Server (Require Security) policy. By applying this policy to a computer, you are telling that computer that it is not allowed to create or accept any communications with other computers that are not also using IPSec and have matching encryption and authentication settings configured. The net result of this mistake in configuration is that your front-end and back-end servers will be able to communicate with each other, but not with any other hosts, including Internet clients (for the front-end servers) and domain controllers (for the back-end servers). Of course, you can also create a custom IPSec policy for your servers if you want. In any case, the Secure Server (Request Security) IPSec policy can be used (with minor modifications) to provide a secure communications tunnel between the front-end and back-end Exchange servers through the internal firewall. You should also give consideration to implementing IPSec security between your front-end servers and your domain controllers and global catalog servers as well—after all, the communications between these servers are juicy pieces of information that attackers might like to get hold of as well.

But what exactly is an IPSec policy? An IPSec policy is a set of rules that defines how and when communication is secured between two endpoints. This is done through the configuration of various rules. Each rule contains a collection of actions and filters that begin when they encounter endpoints that match.

Policies allow you to quickly and easily configure IPSec based on the settings required within your organization. Windows Server 2003 comes with the following three preconfigured IPSec policies that might or might not meet your needs:

- *Client (Respond Only)*—This policy requires IPSec-provided security only when another computer requests it. This policy allows the computer to attempt unsecured communications first and switch to IPSec-secured communications if requested. This policy contains the default response rule, which creates dynamic IPSec filters for inbound and outbound traffic based on the requested protocol and port traffic for the communication that is being secured. This policy, which can be used on workstations and servers alike, provides the minimum amount of IPSec security.
- *Server (Request Security)*—This policy requests security from the other computer and allows unsecured communication with non-IPSec-aware computers. The computer accepts inbound unsecured traffic, but always attempts to secure further communications by requesting IPSec security

from the sending computer. If the other computer is not IPSec-enabled, the entire communication is allowed to be unsecured. This policy, which can be used on workstations and servers alike, provides a medium level of IPSec security.

- *Secure Server (Require Security)*—This policy is implemented on computers that require highly secure communications, such as servers transmitting sensitive data. The filters in this policy require all outbound communication to be secured, allowing only the initial inbound communication request to be unsecured. This policy has a rule to require security for all IP traffic, a rule to permit ICMP traffic, and the default response rule to respond to requests for security from other computers. This policy, typically used only on servers, provides the highest level of IPSec security on a network. This policy can also be used on workstation computers if you want. Non-IPSec-enabled computers cannot establish any communications with computers using this policy.

Before you start working with IPSec, you should understand a few key features of its implementation in Windows Server 2003:

- IPSec in Windows Server 2003 is policy-based. It cannot be configured without an IPSec policy being in place, allowing an administrator to more easily apply settings to groups of objects, such as computers or users.
- IPSec on Windows Server 2003 can use Kerberos v5, a digital certificate, or a shared secret (string) for user authentication.
- IPSec mutually authenticates computers prior to any data being exchanged.
- IPSec establishes a security association (SA) between the two host computers involved in the data transfer. An SA is the collection of a policy and keys, which defines the rules for security settings.
- IPSec encrypts data using Data Encryption Standard (DES) or Triple DES (3DES).
- IPSec uses the MD5 or SHA1 algorithm for data hashing.
- IPSec is invisible to users. IPSec operates at the Network level of the Open Systems Interconnect (OSI) model; therefore, users and applications do not directly interact with the protocol. After an IPSec tunnel has been created, users can connect to applications and services as if they were on the local network and not on the other side of a public network.

To learn more about IPSec, including how to implement and configure it to use custom policies, be certain to read *MCSE 70-293 Training Guide: Planning and Maintaining a Windows Server 2003 Network Infrastructure* by Will Schmied and Rob Shimonski, Que Publishing, 2003.

Looking back at our sample front-end/back-end configuration after we've applied IPSec, you can see how traffic flows in Figure 6.25. Remember that all traffic travels over the same physical network; the different paths simply represent different protocols—or secured and unsecured traffic.

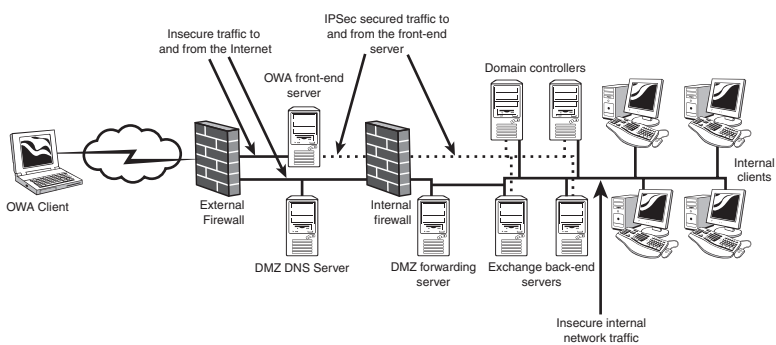

Figure 6.25 You need to implement IPSec between your front-end servers and your back-end servers, domain controllers, and global catalog servers to increase security.

Disabling Unnecessary Services on Front-end Servers

It only stands to reason that if you're configuring a server for the sole purpose of providing a front-end for OWA, you don't need to have all of the installed Exchange services running. The practice of disabling unnecessary services is known as *reducing your attack vector* and is done in many other situations besides configuring servers for OWA.

You might want to consider configuring increased security on your front-end servers by using a security template that imposes a stricter configuration on the server. The *Windows Server 2003 Security Guide*, located at **www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.asp**, contains some very good information in Chapter 11 about hardening bastion hosts (those computers in the DMZ), along with some preconfigured security templates.

To increase the security of your front-end servers, you need to disable the following services: Microsoft Exchange Management, Microsoft Exchange MTA Stacks, and Microsoft Exchange Routing Engine. However, you cannot simply disable these services—you need to start several services first, then disable these services, and, finally, restart some services that are still needed.

To disable unnecessary services on your front-end server, perform the following steps:

1. Open the Services console.
2. Stop the following services:
   - ➤ Microsoft Exchange Information Store
   - ➤ Microsoft Exchange Management
   - ➤ Microsoft MTA Stacks
   - ➤ Microsoft Routing Engine
   - ➤ Microsoft Exchange System Attendant
   - ➤ World Wide Web Publishing Service
3. Configure the following services with a Startup Type of Disabled:
   - ➤ Microsoft Exchange Management
   - ➤ Microsoft MTA Stacks
   - ➤ Microsoft Routing Engine
4. Start the following services again to restore functionality to the front-end server:
   - ➤ Microsoft Exchange Information Store
   - ➤ Microsoft Exchange System Attendant
   - ➤ World Wide Web Publishing Service

Troubleshooting Front-end and Back-end Servers

When troubleshooting front-end/back-end servers, you are looking at four basic items:

- *Are the required services in operation?*—By checking the event logs and the Services console, you can quickly determine the status of required services and perhaps gain some insight into why they might not be working correctly.
- *Are the required ports open on the applicable firewall?*—A firewall misconfiguration manifests itself quite easily by the inability to pass traffic through the firewall on desired ports.
- *Does basic network connectivity exist across the firewall between the front-end and back-end servers?*—Troubleshooting basic network connectivity across the firewall between the front-end and back-end servers can be done very easily by using the ping command.
- *If IPSec is being used, is it working properly?*—IPSec troubleshooting is more involved than any of the other troubleshooting items we've looked at and, thus, we examine it in more detail following this list.

If you have problems with IPSec, you should first verify that any routers or firewalls you might be passing through are configured to support IPSec traffic. You need to allow the following traffic:

- Protocol ID 50 and 51 or Encapsulating Security Payload (ESP) and Authentication Header (AH) traffic
- UDP port 500 for IPSec negotiation traffic

Following are some other basic troubleshooting tips for IPSec:

- *You are not able to establish any communications with a computer*—In this case, you should first verify that basic network connectivity exists between the computers in question. Ensure also that all required network services, such as Dynamic Host Configuration Protocol (DHCP) and DNS, are operating properly for both computers. This might also be the result of a computer that has been removed from the domain, which causes IPSec communications to fail.
- *Communications are occurring, but not as expected*—Ensure that you have the correct (and compatible) IPSec policies assigned on both computers.
- *No hard associations are being formed*—If soft associations are currently in place, a hard association is not formed. You need to completely stop all communications between the computers for about 5–10 minutes to allow the soft associations to time out. The easiest way to do this is to disable the network connection. After you have allowed the soft association to time out, you can check to see that a hard association has been

formed. If a hard association still has not been formed, you need to examine your IPSec policy to verify that unsecured communications are not allowed.

- *IPSec communications are failing after configuring a digital certificate for authentication*—You must make certain that the required digital certificate is installed on the computers attempting to communicate using that IPSec policy. This can also be the result of specifying an incorrect certificate authority (CA).
- *Some computers can create IPSec connections and some cannot*—This situation is most likely caused by not having the same IPSec policy applied to all your computers. If you are intentionally using different policies, ensure that they share at least one common authentication and security method.

Exam Prep Questions

Question 1

You are preparing to create a new IPSec policy that will be used to secure traffic between your front-end and back-end Exchange Server 2003 computers. What available user authentication methods does IPSec in Windows Server 2003 offer? (Choose all that apply.)

- ❑ A. NTLM v2
- ❑ B. Kerberos v5
- ❑ C. EFS
- ❑ D. Digital certificate
- ❑ E. Shared secret
- ❑ F. WEP

Answers B, D, and E are correct. The Windows Server 2003 IPSec implementation can use Kerberos v5, digital certificates, or shared secrets to perform user authentication. Answer A is incorrect; NTLM v2 is used for network authentication with Windows 2000 Server and Windows Server 2003. Answer C is incorrect; the Encrypting File System (EFS) is used to encrypt files and folders to add extra security to them. Answer F is incorrect; Wired Equivalent Privacy (WEP) is used as both an encryption and authentication methods on wireless LANs.

Question 2

This morning, one of your users has called you complaining that she cannot access a newly created public folder by using Outlook. When she uses Outlook Express, however, she can access the public folder successfully. Why do you suspect the user is having this problem?

- ❍ A. The user is attempting to access the default public folder tree.
- ❍ B. The user's computer does not have the required version of Outlook installed.
- ❍ C. The user does not have the correct client permissions configured on the public folder.
- ❍ D. The user is attempting to access a general-purpose folder tree.

Answer D is correct. General-purpose folder trees can only be accessed by HTTP or NNTP. Outlook Express supports NNTP, but Outlook does not.

Answer A is incorrect; the default public folder tree can be accessed using MAPI, HTTP, or NNTP. Answer B is incorrect; because Outlook does not support NNTP, the version of Outlook installed is not an issue. Answer C is incorrect; because the user can access the public folder she needs, the status of her client permissions is most likely not a problem.

Question 3

You are preparing to implement a front-end/back-end server solution that will provide OWA to your remote users. Company policy requires that all connections from the Internet to company resources must be secured. To meet this requirement, you have installed a server certificate on the server and enabled the Require Secure Channel check box. What port must you ensure is open on the Internet-facing firewall to support your configuration?

- ❍ A. 443
- ❍ B. 389
- ❍ C. 88
- ❍ D. 119

Answer A is correct. Port 443 is required to support HTTP over SSL. Answer B is incorrect; port 389 is used for LDAP queries to a domain controller and should not typically ever be opened on an external firewall. Answer C is incorrect; port 88 is used for Kerberos authentication and should never be opened on an external firewall. Answer D is incorrect; port 119 is used for NNTP and needs to be open on an external firewall if NNTP access is required to or from the Internet. However, NNTP is not related to configuring HTTP over SSL.

Question 4

You have recently created a new public folder in the default public folder tree of your Exchange organization. You need each member of the Accounting group to be able to create and read items in the public folder as well as be able to modify and delete items they have created. What role do you need to assign to each member of the Accounting group?

- ❍ A. Publishing Editor
- ❍ B. Publishing Author
- ❍ C. Author
- ❍ D. Reviewer

Answer C is correct. The Author role grants the user permission to create and read items in the public folder. The user can also modify and delete items they have created within the public folder. Answer A is incorrect; the Publishing Editor role grants the user permission to create, read, modify, and delete all items within the public folder. The user can also create new child folders within the public folder. Answer B is incorrect; the Publishing Author role grants the user permission to create and read items in the public folder. The user can also modify and delete items they have created as well as create new child folders within the public folder. Answer C is incorrect; the Reviewer role grants the user permission only to read items in the public folder.

Question 5

You have recently created a new public folder in the default public folder tree of your Exchange organization. You need the Marketing group to be able to only read items in the public folder. What role do you need to assign to the Marketing group?

- ❍ A. Author
- ❍ B. Reviewer
- ❍ C. Contributor
- ❍ D. Editor

Answer B is correct. The Reviewer role grants the user permission only to read items in the public folder. Answer A is incorrect; the Author role grants the user permission to create and read items in the public folder. The user can also modify and delete items they have created within the public folder. Answer C is incorrect; the Contributor role grants the user permission to create new items in the public folder but cannot view the contents of the folder. Answer D is incorrect; the Editor role grants the user permission to create, read, modify, and delete all items in the public folder.

Question 6

You are the network administrator of a large, distributed Exchange Server 2003 organization that spans four routing groups. Routing group connectors are in place between all routing groups with the following costs:

- ➤ Routing Group 1–Routing Group 2: 1
- ➤ Routing Group 2–Routing Group 3: 3
- ➤ Routing Group 3–Routing Group 4: 2

- Routing Group 1–Routing Group 3: 1
- Routing Group 1–Routing Group 4: 3
- Routing Group 2–Routing Group 4: 2

A client who has her mailbox located in a mailbox store in Routing Group 1 needs to connect to a public folder replica that is located in a public folder store in Routing Group 3. Which path will the client's request take to access the public folder replica?

- ❍ A. Routing Group 1 to Routing Group 3
- ❍ B. Routing Group 1 to Routing Group 2 to Routing Group 3
- ❍ C. Routing Group 1 to Routing Group 4 to Routing Group 3
- ❍ D. Routing Group 1 to Routing Group 4 to Routing Group 2 to Routing Group 3

Answer A is correct. Routing group connectors, like WAN links, have costs associated with them. The value of the cost is administrator configured and can be used to indicate the preferred route between two routing groups due to link speed, link utilization, or link cost issues. Routing group connector cost values range from a low value (better) of 1 to a high value (worse) of 100. The lowest total routing group cost between two routing groups is the preferred path between those two routing groups, thus answers B, C, and D are incorrect.

Question 7

You are the network administrator of a large, distributed Exchange Server 2003 organization that spans four routing groups. Each routing group contains a replica of the default public folder tree. If an administrator located in Routing Group 1 and an administrator located in Routing Group 2 both edit the properties on the same public folder, how does Exchange determine which changes to keep?

- ❍ A. The administrator who has the highest level of Exchange permissions is considered authoritative and will have his changes kept.
- ❍ B. The changes that are made most recently will be kept.
- ❍ C. The changes that are made on the original public folder tree will be kept.
- ❍ D. The administrator who has the highest level of Windows Active Directory permissions is considered authoritative and will have his changes kept.

Answer B is correct. During public folder content conflict detection, the changes that are made to multiple replicas of the same public folder will be kept based on the most recent saved version of the folder. Answers A and D are incorrect; the total level of Exchange or Windows Active Directory permissions has no relevance on conflict detection. Answer C is incorrect; all

public folder replicas are considered a multimaster; thus, a change to any one replica is just as good as a change to any other replica (including the original public folder tree).

Question 8

You are the administrator responsible for seven public folder stores within your organization. Recently, some users have been complaining that it takes an excessively long time to perform searches against the public folder trees. What can you do to reduce the amount of time it takes when users perform searches against your public folders?

- ❍ A. Create additional replicas.
- ❍ B. Configure public folder referral across your routing group connectors.
- ❍ C. Create and configure a full-text index on your public folder stores.
- ❍ D. Create and configure a full-text index on your public folders.

Answer C is correct. To improve client search speed, you should create and configure full-text indexes on the public folder stores that contain the public folder trees of concern. Answer A is incorrect; creating additional replicas increases overall client access speed to public folders, but greatly increases search speed. Answer B is incorrect; configuring public folder referral across your routing group connectors allows clients to locate public folders not in the same routing group as their mailbox, but do not improve the speed at which searches are performed against public folders. Answer D is incorrect; full-text indexing is configured on a public folder store as a whole, not on a public folder.

Question 9

You are the administrator responsible for seven public folder stores within your organization. Recently, some users have been complaining that it takes an excessively long time to perform searches against the public folder trees. To alleviate this problem, you have configured full-text indexing on your public folder stores. Which of the following attachment types will users be able to search within when searching in public folders? (Choose all that apply.)

- ❑ A. .txt
- ❑ B. .vbs
- ❑ C. .exe
- ❑ D. .htm
- ❑ E. .doc
- ❑ F. .vsd
- ❑ G. .zip

Answers A, D, and E are correct. When configured on a public folder store, full-text indexing also indexes some attachments types that are stored in the public folder. The following attachment types can be indexed: .eml, .txt, .htm, .html, .asp, .doc, .xls, and .ppt. Answers B, C, F, and G are incorrect; .vbs (VBScript) files, .exe (executable applications) files, .vsd (Visio Drawing) files, and .zip (WinZip Archives) files are not capable of being full-text indexed.

Question 10

You are preparing to implement a front-end/back-end server solution that will provide OWA to your remote users. Company policy requires that all connections from the Internet to company resources must be secured. To meet this requirement, you have decided that you will use HTTP over SSL for all inbound connections to the front-end OWA server. What do you need to do first to enable SSL support on the HTTP virtual server?

- ❍ A. Place a check mark in the Require Secure Channel check box.
- ❍ B. Install a digital certificate from your organization's certificate authority.
- ❍ C. Configure an IPSec tunnel between the front-end server and the Internet-facing firewall.
- ❍ D. Open port 443 on the firewall separating the front-end server from the protected internal network.

Answer B is correct. Before you can enable SSL (by selecting the Require Secure Channel check box), you must first install a digital certificate from one of your organization's certificate authorities. Answer A is incorrect; you will select the Require Secure Channel check box only after installing a digital certificate. Answer C is incorrect; creating an IPSec tunnel between the front-end server and the Internet-facing firewall would not provide any help for this problem and is, in most cases, not required. Answer D is incorrect; port 443 must be open on the Internet-facing firewall to support HTTP over SSL, not on the firewall protecting the internal network.