70-237 Pro: Designing Messaging Solutions With Microsoft Exchange Server 2007
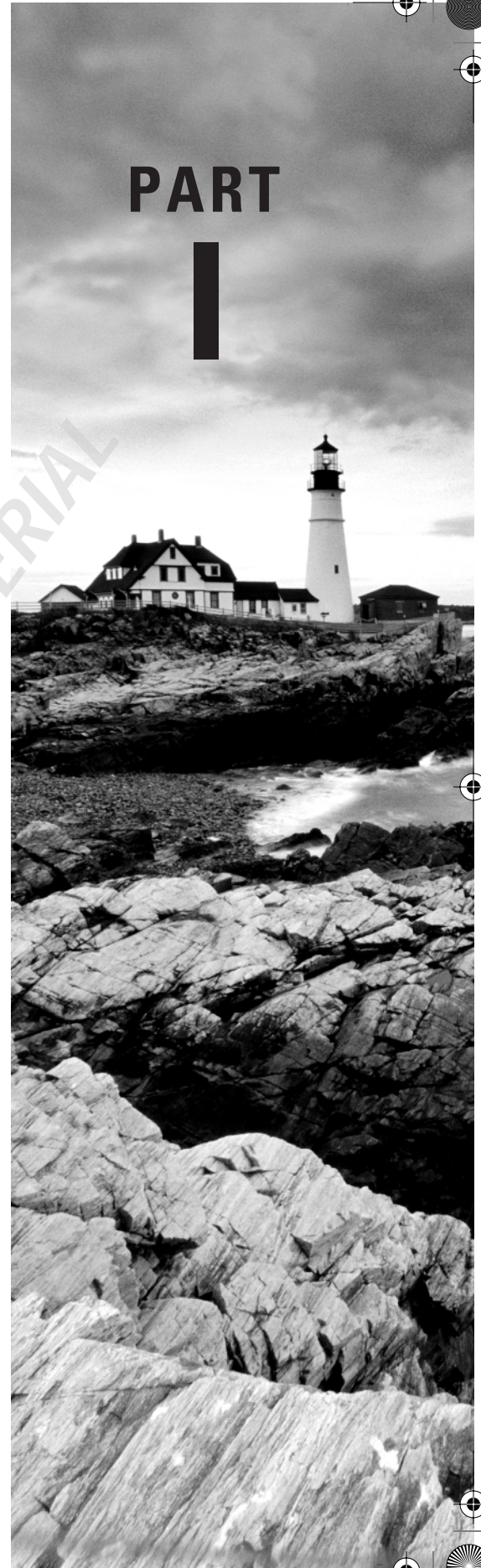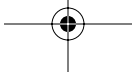
PART

I

Chapter

1

Designing and Planning Messaging Services

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Evaluate and recommend Active Directory configuration**
- ✓ **Evaluate and plan server deployment based on best practices, budget, and other business factors**
- ✓ **Evaluate network topology and provide technical recommendations**
- ✓ **Design and plan for new Exchange features**
- ✓ **Design organization configuration to meet routing requirements**

Designing and planning Messaging Services is one of the most important tasks of a messaging IT pro and needs careful considerations in many areas. This chapter introduces you to important Exchange design topics: Active Directory (AD) requirements, server placement, and message-routing considerations.

The main subjects of this chapter are as follows:

- Defining Active Directory prerequisites

- Designing an administrative model

- Planning Exchange Server 2007 placement

- Understanding Exchange Server 2007 roles

- Reviewing the current and planned network topology and providing technical recommendations

- Understanding new Exchange features

- Understanding internal and external message routing

Evaluating and Recommending Active Directory Configuration

As an Exchange Server 2007 message professional, your responsibilities normally will not include a single domain with a single Exchange Server installation. The Active Directories and Exchange organizations you plan, manage, or support will be highly complex as well as dispersed around the world. To cover this exam requirement, this section will teach you some specific commands and considerations that are special to medium-to-large organizations. Here you will learn about all the requirements of Active Directory for Exchange Server 2007.

Defining Active Directory Prerequisites

The following section will teach you about Exchange Server 2007 and how it uses Active Directory to store configuration data. It starts with the high-level basics of Active Directory and Exchange data and continues with explanations of software version requirements as well as Active Directory preparation for Exchange.

Exchange Uses Active Directory to Store Information

The Active Directory database is divided into logical partitions, namely the schema partition, the configuration partition, and a domain partition for every domain. Here's how Exchange Server 2007 uses each of these partitions.

The Schema Partition

Before Exchange Server 2007 can store information in Active Directory, this partition needs to be modified so Exchange-related objects (e.g., connector or mailbox information) and attributes (e.g., Exchange Mailbox server or a user object) can be stored there. The schema partition stores the general layout of all Active Directory objects and its attributes. It includes two types of information:

Schema classes: The objects that can be created

Schema attributes: The properties that can be used for each object

> **NOTE**
>
> Each and every domain controller and global catalog server in the Active Directory contains a complete replica of the schema partition. Thus it is important to plan the Exchange Server 2007 schema extension accordingly— it will initiate a full replication on all domain controllers and global catalog servers in your forest.

> **WARNING**
>
> It is true that the Exchange Server 2007 schema extension also includes the Exchange 2003 schema extension. However, if you are ever planning on install-ing an Exchange 2003 server, you must install it as the first server and install Exchange Server 2007 afterwards. Once you have installed an Exchange Server 2007 server, you will not be able to install Exchange 2003 anymore.

The Configuration Partition

As the name implies, the configuration partition stores information about the forest-wide con-figuration. For example, the configuration of AD sites and site links is stored here. Therefore, it is available on every domain controller and global catalog server throughout the forest.

Exchange Server 2007 stores information like global settings, address lists, connections, and so on to the configuration partition. You can take a look at what information Exchange Server 2007 stored in the configuration partition by following Exercise 1.1.

EXERCISE 1.1

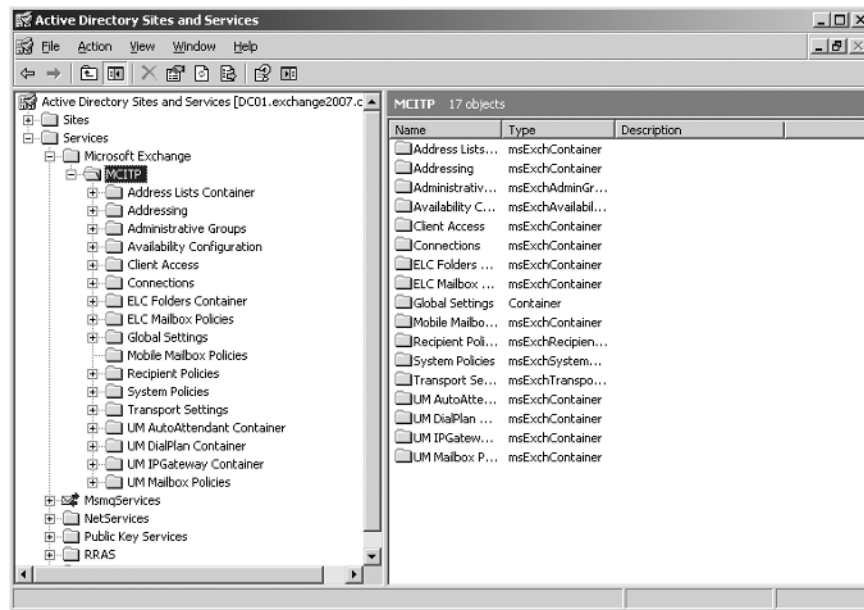#### Looking at the Exchange Configuration

To look at the Exchange configuration, follow these steps:

1. Click Start ➢ All Programs ➢ Administrative Tools ➢ Active Directory Sites and Services.

EXERCISE 1.1 *(continued)*

2. Click on View ➢ Show Services Node.

3. Expand Services to find Microsoft Exchange container, as shown below.

Important: Please be aware that any modification in this container directly impacts the Exchange Server 2007 configuration and thus might crash your system!

The Domain Partition

The domain partition holds domain-related information in containers as well as organizational units (OUs). It includes information about users, groups, and computers in that domain. Exchange Server 2007 creates for every domain-prepared domain (which means that the Exchange Setup / PrepareDomain has been run for the domain) an OU called "Microsoft Exchange Security Groups" where it will store Exchange related management groups.

The domain partition is stored on every domain controller of that specific domain. Every global catalog server has a subset of information from every domain partition in the forest, as well as the complete partition from its own domain. For example, a global catalog server in a different domain will contain information of the individual user, such as the user's display name or its SMTP addresses, but not its password.

Active Directory Requirements

For Exchange Server 2007 there are several requirements that Active Directory and domains must meet. Consider the following when evaluating your current Active Directory design:

- The server on which the Schema Master role runs must have at least Windows Server 2003 SP1 installed.

- You need to run Windows Server 2003 SP1 or later on global catalog servers in every Active Directory site where you plan to install Exchange Server 2007. I recommend that you upgrade all your domain controllers to prevent any problems.

- All domains that will include Exchange Server 2007 servers or recipients must have an Active Directory domain functional level Windows 2000 Server Native or higher; Windows Server 2003 functional level is recommended.

> **WARNING** Windows Server 2008 (formerly code-named Longhorn) is supported only with Exchange Server 2007 Service Pack 1 or later. You cannot install Exchange Server 2007 in any AD site that contains Windows Server 2008 domain controllers, nor can you install it on a Windows 2008 member server!

Preparing Your Active Directory and Domains

This section walks through the steps required to prepare your Active Directory and domains to run Exchange Server 2007.

Preparing the Schema Only

If you need to extend the schema of your Active Directory *separately* from the Exchange Server 2007 installation, you can run the following from a command prompt from the Exchange Server 2007 setup directory: `Setup /PrepareSchema`. Especially in larger organizations where Active Directory and Exchange administration are separated, you will need to plan well ahead to do this.

You must be a member of the Schema Admins group and the Enterprise Admins group and run the `/PrepareSchema` command on the server that is in the same Active Directory domain ad site as the Schema Master role. I strongly recommend doing this directly on your Schema Master server.

However, this command is not needed, as it is part of the Preparing Active Directory switch `/PrepareAD`.

Preparing Your Active Directory

To prepare your Active Directory for Exchange Server 2007, you must run the following command: `Setup /PrepareAD`. Please consider the following when running this command:

- You need to run it on a server in the root domain.

- You must be a member of the Enterprise Admins group, and if the schema also needs to be extended you also need to be part of the Schema Admins group.

- If you have Exchange Server 2003 servers, you must have Exchange Full Administrator permissions.

Exchange Server 2007 setup does the following tasks preparing your Active Directory environment:

1. Extend the schema if it was not done already.

2. Configure global Exchange objects in the configuration partition. These include Exchange Administrative Group (FYDIBOHF23SPDLT), Exchange Routing Group (DWBGZMFD01QNBJR), and so on.

3. Create an OU in the root domain called Microsoft Exchange Security Groups, which includes the following universal security groups (USGs):

   ▪ Exchange Organization Administrators

   ▪ Exchange Recipient Administrators

   ▪ Exchange View-Only Administrators

   ▪ Exchange Servers

   ▪ ExchangeLegacyInterop

4. Prepares the root domain as mentioned in next section.

> If your Active Directory site topology is complex, you have to check before you continue to make sure that replication to all domain controllers in your forest took place. Tools like the Active Directory Replication Monitor (`replmon.exe`) that is part of the Windows 2003 Resource Kit Tools can assist you with monitoring the progress.

Preparing Domains

If you are in larger environment where your Active Directory consists of multiple domains, you also need to prepare every domain for Exchange Server 2007. Your domain preparation will do the following things to the domain:

▪ Set permissions on the Domain container for the Exchange Servers, Exchange Organization Administrators, Authenticated Users, and Exchange Mailbox Administrators.

▪ Create an OU called Microsoft Exchange System Objects and set permissions on this container for the Exchange Servers, Exchange Organization Administrators, and Authenticated Users.

▪ Create a global group called Exchange Install Domain Servers and add it to the Exchange Servers USG in the root domain.

There are two possible ways to prepare domains: you can prepare them all together or you can run the command domain by domain. Preparing all domains together might seem like the easiest way to prepare all domains, but sometimes you might not be able to do this. Consider the following situations:

▪ You have a regional Active Directory domain design; no central administration is available.

▪ Permissions for the Enterprise Admin group were removed from some domains.

- Not all domains can be contacted; Exchange Server 2007 setup needs to contact at least one domain controller from every domain to make the changes.
- Firewalls prevent some locations from communicating to each other directly.

For each command, you must consider the requirements in Table 1.1.

T A B L E   1 . 1   Exchange Server 2007 Setup—Domain Preparation Considerations

Setup Command	Consideration
`Setup /PrepareAllDomains`	Requires Enterprise Admin permission, Domain Admin permission in all domains, and network access to every domain.
`Setup /PrepareDomain:<FQDN of domain>`	Requires Domain Admin permission in the domain that you want to prepare. If it is a domain that did not exist when you ran `/PrepareAD`, you also need to be a member of the Exchange Organization Administrators group.

> You must prepare every Active Directory that will host Exchange Server 2007 servers or Exchange-specific objects like mailboxes, distribution lists, contacts, or public folders. You do not need to prepare the root domain, as this was done during the "Preparing Your Active Directory" section.

Isolating Exchange Server 2007 from your Active Directory

To completely separate your Exchange Server 2007 installation from your Active Directory implementation, you have the option to create an Exchange resource forest. A *resource forest* is a completely different Active Directory environment created for the sole purpose of serving Exchange Server 2007. For example, I've seen this strategy in hosting (or outsourcing) environments where the company managed the user accounts but they outsourced their mailboxes to a hosting company. To configure this, the following is required:

- The minimum forest functional level of both forests must be Windows Server 2003
- A forest-to-forest trust needs to be established

Designing an Administrative Model

It is important to consider a thoroughly planned administrative model for your organization when you integrate Exchange Server 2007 into your Active Directory. Generally there are three ways to organize your administrative roles:

- A single administrative team manages both Windows Server and Exchange Server.
- Permissions are split between Windows and Exchange administrators.
- The Exchange administrator role is isolated by using an Exchange resource forest.

Using the first or last option, you don't need much extra configuration in Exchange Server 2007. However, splitting permissions is a more complex story. After offering some background in the following sections, I will explore this topic in detail under the heading "The Split-Permissions Model."

Exchange 2003 was based on an administrative role model of two layers: organization– and administrative group–based. This model has proven to be insufficiently flexible, especially for medium-to-large organizations. Thus, Exchange Server 2007 uses a more granular administrative roles model similar to the built-in Windows Server security groups.

Administrative Roles

Exchange Server 2007 uses the following predefined roles to manage permissions:

- Exchange Organization Administrators
- Exchange Recipient Administrators
- Exchange View-Only Administrators
- Exchange Server Administrators

All roles expect Exchange Server Administrators provide you with permissions to any domain that was prepared for Exchange (i.e., `Setup /PrepareDomain`). You cannot change the scope of them.

To assign a role to a group or account, you can either use the Exchange Management Console (EMC) and configure it in the Organization Configuration pane, or use the `Add-ExchangeAdministrator` command in the Exchange Management Shell (EMS). Figure 1.1 shows the Exchange Management Console where you can view and modify all administrative roles.

FIGURE 1.1   Exchange administrative roles in the Exchange Management Console
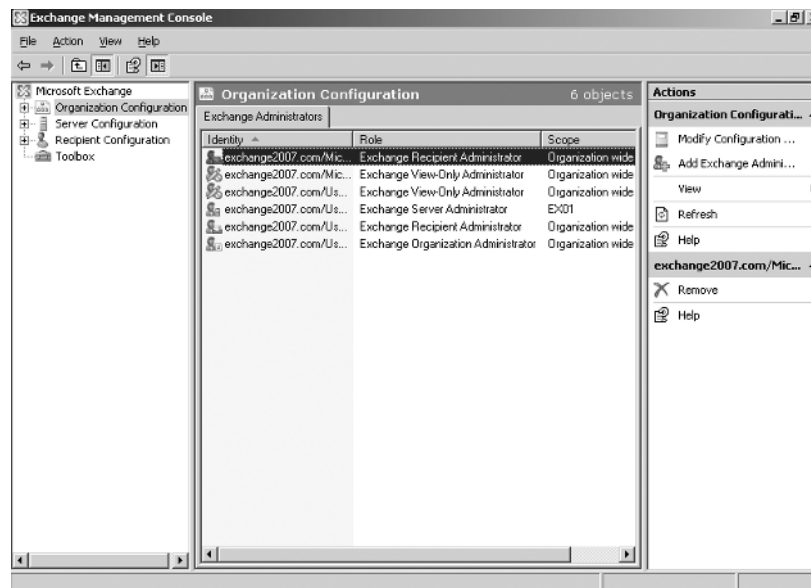
> **NOTE**
>
> During the initial Exchange setup in the root domain (i.e., `Setup /PrepareAD`) all groups (except Exchange Server Administrators) are created as a security group in the Microsoft Exchange Security Groups container. You can see those using Active Directory Users and Computers.

Exchange Organization Administrators

The Exchange Organization Administrators role is the most powerful role in Exchange Server 2007. As in Exchange Server 2003, you get full access to all Exchange-related servers and objects in your organization. You need this role for any configuration that impacts all your Exchange servers, like connectors or global settings.

The following list provides an overview of what permissions you receive when you are part of this role:

- Owner permission to the Exchange organization in the configuration partition of Active Directory
- Read access to all domains that were prepared for Exchange
- Write access to all Exchange-specific attributes in all domains that were prepared for Exchange
- Membership in local Administrators group of all Exchange servers in your organization

> **WARNING**
>
> Because this role automatically gets write permissions on the Exchange-specific attributes in all domains that where prepared for Exchange, Exchange Organization Administrators can assign or remove a mailbox from any user account in the forest—no need to be a full Domain Admin or an Account Admin!

Exchange Recipient Administrators

The Exchange Recipient Administrators manage mailboxes, contacts, groups, dynamic distribution lists, and public folder objects. They can add or remove SMTP addresses, enable or disable specific groups for mail, or create a contact. This role also lets you manage Unified Messaging and Client Access settings on mailboxes. Basically, you can think of the Exchange Recipient Administrators as the Exchange user management team.

You receive the following permissions when you're part of this role:

- Read access to all domains that have been prepared for Exchange
- Write access to all Exchange-specific attributes in all domains that have been prepared for Exchange
- Membership in the Exchange View-Only Administrators group—thus the ability to view the complete Exchange configuration

Exchange View-Only Administrators

As an Exchange View-Only Administrator you will receive read-only access to the Exchange organization and to all Windows domains that contain Exchange recipients. You can assign this role to people that want to look at the Exchange configuration (for example, to see connector settings) but that don't perform changes.

You receive the following permissions when you're part of this role:

- Read permission to the Exchange organization tree in the configuration partition of Active Directory
- Read access to all domains that have been prepared for Exchange

Exchange Server Administrators

The Exchange Server Administrators role was designed to delegate access for one or more servers to either a security group or a user. Exchange Server Administrators can administer one or more particular Exchange server(s), but they cannot change anything of global impact to the Exchange organization. For example, they can manage storage groups or databases on their server(s), but they cannot move mailboxes to a server they don't have permission on.

> **NOTE** This is the only administrative role whose scope can be set on one or more Exchange servers. All other roles are organization-wide!

You receive the following permissions when you're part of this role:

- Owner permissions on server object(s) within the configuration partition
- Local Administrator on the Exchange server(s)
- Membership to Exchange View-Only Administrators thus you can view the complete Exchange configuration

> **TIP** You can delegate this role to users and global or universal security groups, but not to domain local groups.

The Split-Permissions Model

Some organizations, especially the more complex and geographically widely dispersed, may face the problem of the standard Exchange administrative roles not fitting in their security system. For example, suppose an administrator of a location in Germany needs to manage his mailboxes. Being part of the Exchange Recipient Administrators group grants him full permissions on all user objects in all domains, whereas he manages only a single OU in one domain of a complex forest. In this case, a more granular split-permissions model needs to be implemented to address this incongruity.

Split permissions are especially useful when you are thinking of separating the following tasks from each other:

- User-related

- Contact-related

- Group or dynamic distribution list–related

- Recipient management for some or all the aforementioned tasks

As details of the split-permissions model go far beyond the scope of this book and the scope of the exam, I will present just the basic concept so you understand what needs to be done.

Basically the split-permissions concept of Exchange Server 2007 is based on the following two tasks:

- You assign the user or group the Exchange View-Only Administrators role.

- You assign the user or group specific Exchange-related permissions on the Active Directory objects (e.g., for all user objects of a specific organizational unit).

I call this concept "just the permissions needed," so permission is granted only on specific attributes. Using the Exchange Management Shell, you can use the `Add-ADPermission` command to delegate just the right permissions.

> The split-permissions model goes into more depth than just delegating full control over an organizational unit. It's about managing only the Exchange-related attributes. Thus, an administrator with split permissions can create a mailbox for a user, but is not able to reset the password for that user. That is the key difference!
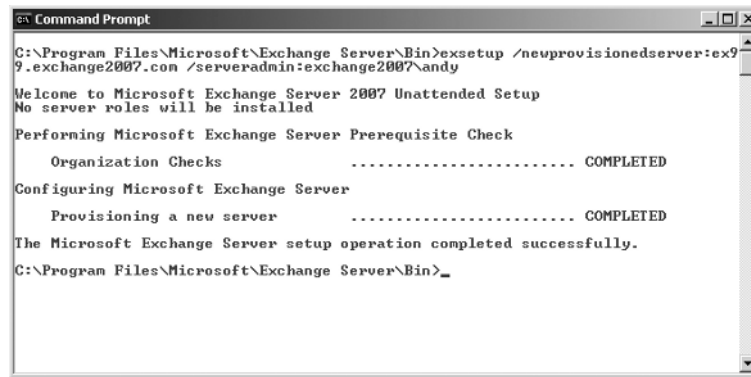
Server Provisioning

Besides the administrative roles, Exchange Server 2007 also supports *server provisioning*, or delegation of the ability to install servers. Exchange administrators now have the flexibility of a setup command to create the necessary server object within the configuration partition and to delegate the permissions required to install the rest of the server to a user account.

To provision a server you first must create a computer account for the new Exchange server (if it does not yet exist). Then log on to an existing Exchange server in your organization using an account that is a member of the Exchange Organization Administrators group. In your Exchange binary folder you must use the following command:

```
Exsetup /NewProvisionedServer:<FQDN of server name> /
ServerAdmin:<domain\account>
```

Figure 1.2 shows an example of the server provisioning giving the user account ANDY the permission to install the Exchange server EX99. Once the provision is finished, you can see the provisioned server object in the EMC in Server Configuration. It appears with the server role Provisioned.

F I G U R E   1 . 2   Server provisioning

> **NOTE**   You cannot delegate the first Exchange Server 2007 server installation; this server must be installed by an account that is a member of the Exchange Organization Administrators group.

You can remove a server that has been provisioned or where the provision failed using the following command:

```
Exsetup /RemoveProvisionedServer:<FQDN of server name>
```

Real World Scenario

The Practical Case for Server Provisioning

For smaller Exchange installations, server provisioning might seem like something you'll never need. This is true if you're talking about single-site Exchange installations that are run by a single Exchange administrator. But once you have a multisite Exchange installation where every site wants to manage their Exchange servers on their own, you might have trouble.

In a combined Exchange organization, there must be a single instance that controls the global topics such as connectors or settings. If everybody manages these settings, and if your fellow admin configures something wrong, then your users may not be able to send/receive emails for some time. So, what can you (as the "global" Exchange administrator) do to solve this?

You can install Exchange Server for your fellow administrators or give them Exchange Organization Administrators permission so they can do it on their own. The best solution is to use server provisioning—you can pre-assign the administrators with the correct permissions so they can install their own Exchange server and do not interfere with any global settings as they just have Exchange Server Administrators permission on their server.
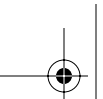
Evaluating and Planning Server Deployment Based on Best Practices, Budget, and Other Business Factors

This section will look at what is required to make up a good server deployment plan. Business factors and budget are discussed here, as are best practices. The discussion should provide you with a good understanding of when to place a server at a specific location and when not to.

Planning Exchange Server 2007 Placement

In this section you will learn how to plan the placement of Exchange Server 2007. Deciding where to put a Mailbox server is one of the most critical planning aspects of the Exchange design. Thus it's important to analyze what's available today before stepping down into the different areas that you need to consider in your design.

Analyze What You Have Today!

Understanding what is currently implemented in terms of messaging and Active Directory is an important starting point. You should investigate any area of importance that might have influence in creating your Exchange design.

Active Directory Site Topology

As a first step in planning where to deploy servers, you always should have a solid understanding of your Active Directory site topology. This is especially important in medium-to-large organizations, where the site topology can get geographically or politically dispersed and complicated.

A good practice is to collect all information and to document it so you can review it with your Active Directory team. Consider collecting the following items for your documentation:

- Sites and their subnet associations
- Subnets that have overlapping site associations or do not belong to any site
- IP site links and member sites
- IP site link costs
- Domain controllers in each site (including which domain controllers are global catalog servers)

Assessing this material will give you a solid understanding of you network and where you could place Exchange servers.
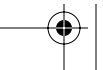
Gathering Business Requirements

Besides collecting the technological requirements, remember to include what business requirements you have for the Exchange Server 2007 design. You should consider the following in your plans:

IT strategy: Administrative model, migration strategy, etc.

Budget: How much is available for hardware, how much for software, etc.?

Licensing and maintenance requirements: What licenses are available, what are "end-of-life" products, details about maintenance contracts, etc.?

Acceptable downtime for messaging: Current Service Level Agreement on messaging, the current disaster recovery strategy, etc.

Security policies: Special considerations regarding the companies security policies, such as message encryption, SPAM filtering, or virus protection.

Regulatory requirements: Does your company's market segment have any special requirements for archiving or tracking (SOX, etc.)?

Client access needs: What kind of access do the clients expect (mobile, voice, fax, etc.)?

Messaging information: How is messaging currently used, how many messages are received/sent internally or from the Internet, and what external connections exist?

Consider Domain Controller and Global Catalog Servers

In planning your Exchange Server 2007 placement, always consider domain controller or global catalog servers. These factors are especially important as Exchange Server 2007 does not start without communicating to a global catalog server. Thus it is vital that you consider the following in your planning:

- At least one domain controller of the same domain as the Exchange server must be available in the AD site where you plan to install Exchange Server 2007.

- At least one global catalog must be available in the same AD site where you plan to install Exchange Server 2007.

- For redundancy reasons, it's always good to have at least two global catalog servers available in an AD site where Exchange Server 2007 will be installed.

- If you use 64-bit domain controllers, it increases the directory service performance significantly, even though 32-bit domain controllers are still supported.

> Especially in large organizations with more than 20,000 objects in your Active Directory, you should consider upgrading to 64-bit domain controllers.

- As in previous Exchange versions, the recommended 4:1 ratio of Exchange cores to global catalog cores applies for Exchange Server 2007. For example, if you have two

Exchange servers with four cores per servers, you should have at least two cores dedicated for global catalogs.

- If you're planning to host Exchange servers for multiple domains at a single AD site, then you must include domain controllers from each domain for which you host resources.

Exchange Server 2007 System Requirements

You must also understand the system requirements for Exchange Server 2007; that way you can plan your server hardware accordingly. Table 1.2 lists these requirements.

T A B L E   1 . 2   System Requirements for Exchange Server 2007

Component	Minimum Requirement
Processor	x64 architecture–based computer with Intel processor (that supports Intel Extended Memory 64 Technology—EM64T) or AMD processor that supports AMD64. Intel Itanium family IA64 cores are not supported.
Operating system	Microsoft Windows Server 2003 x64 or Windows Server 2003 R2 x64, Standard or Enterprise Edition.
Memory	2 GB of RAM per server.
Available hard-disk space	1.2 GB where you install Exchange Server 2007 200 MB on system drive.
File format	Disk partitions must be in NTFS file format, not the file allocation table (FAT) file system.

Using Exchange Server 2007 on Member Servers or Domain Controllers

You must also consider on what Windows 2003 server role you want to install Exchange Server 2007: member servers or domain controllers. Even though Microsoft supports the installation of Exchange Server 2007 on domain controllers, I strongly advise against it. This is because you need to be a local administrator to manage an Exchange Server 2007 server, and local administrators will automatically receive Admin permissions on all of your domain controllers.

There might be circumstances, such as branch-office situations, in which you do not have a choice, as hardware is spare or budget is limited. I've seen situations where a single piece of hardware held everything: domain controller, Exchange server, file and print services. However, avoid that if possible.

WARNING   As a protective feature, Dcpromo, which is the command to promote a Windows 2000 or 2003 member server to a domain controller, cannot be run anymore once you have installed Exchange Server 2007 on a Windows 2003 member server. After Exchange Server 2007 is installed, changing the role from a member server to a domain controller or vice versa is not a Microsoft-supported scenario.

Exchange Server 2007 Roles

In order to manage Exchange Server 2007 in a more natural way, server roles were implemented. These roles enable administrators to easily choose which features should be installed on an Exchange server. They provide the following advantages over the model used in previous Exchange versions:

- They reduce attack surface, as only required roles are installed.
- They allow you to install the servers for their intended role only.
- They provide more possibilities for scalability and reliability.
- They lower complexity to reduce system outages.

In Exchange Server 2007 you can choose from five server roles, namely Mailbox server, Hub Transport server, Client Access server (CAS), Unified Messaging server, and Edge Transport server. The following table provides you with an overview as well as the main planning aspects for each role. More details about the Exchange Server 2007 roles are covered in later chapters of this book.

TABLE 1.3   Exchange Server 2007 Roles Overview

| Server Role	Description	Planning Aspect
Mailbox server	Hosts your mailboxes as well as public folder databases.	You must plan Exchange servers at the AD sites where most of the users are located or depending on your IT Strategy in key regional datacenters. Detailed planning for this role is covered in Chapters 2 and 9 of this book.

T A B L E   1 . 3   Exchange Server 2007 Roles Overview *(continued)*

Server Role	Description	Planning Aspect
Hub Transport server	Manages all internal message routing within the Exchange organization as well as hosts transport rules that can be applied to messages.	Required in every AD site where a mailbox server is installed. In this AD site a global catalog must be available. A rule of thumb regarding sizing: one Hub Transport processor per three Mailbox server cores. For redundancy reasons you should have at least two Hub Transport servers in larger or critical AD sites.
Client Access server (CAS)	This role hosts the Availability service and Autodiscover needed for Outlook 2007, Exchange Active-Sync, client protocols such as POP3, IMAP4, Outlook Web Access, Outlook Anywhere, and Web services.	Is required in every AD site where a Mailbox server is installed. Recommendation is one CAS processor per four Mailbox cores.
Unified Messaging server	Connects Exchange with your telephone system or private branch exchange (PBX) to have voice access to your mailbox or receive faxes.	Supports approximately 60 concurrent calls per server. Planning aspect should include the number of users as well as how they use Unified Messaging. A single Unified Messaging server can host approximately 3,000 heavy users.
Edge Transport server	Acts as a smart host and SMTP relay in your perimeter network and handles all Internet-facing mail flow. Provides antispam and antivirus functionality. Provides address rewriting and process rules to protect the internal network.	Depending on the size of your organization, you should plan at least two servers to provide redundancy in case of problems. It can handle 100 messages per second, including antivirus software scanning.

Exchange Server 2007 server roles can coexist on a single Exchange machine with a few rules to consider:

▪   The Mailbox role, Hub Transport role, Client Access role, and Unified Messaging role can coexist on a single server if the Mailbox server is not clustered.

▪   On clustered Mailbox servers, only the Mailbox role can be installed.

▪   Edge Transport cannot be shared with any other server role.

Figure 1.3 provides an overview of all the Exchange Server 2007 roles, their functionality, and their connections.

FIGURE 1.3 Exchange Server 2007 roles
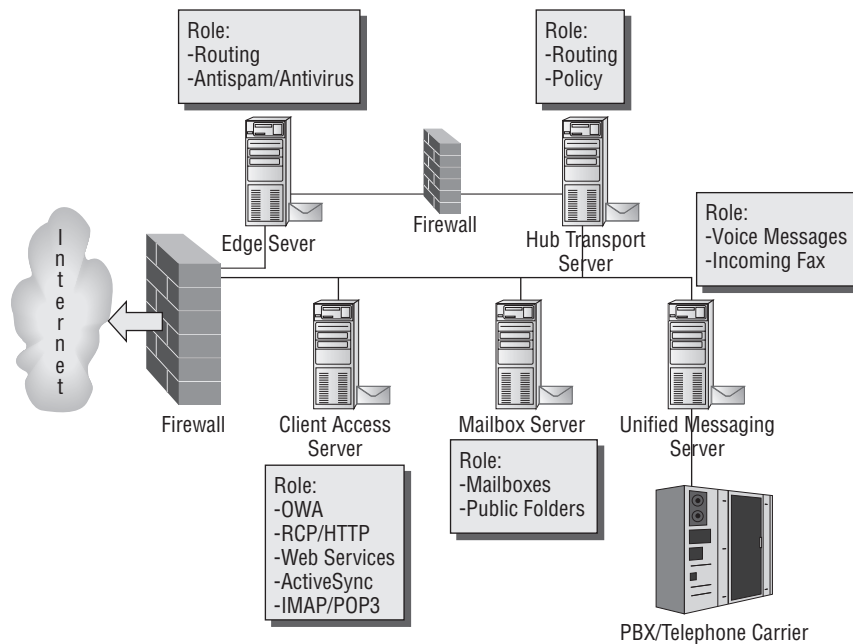
> In a smaller organization you will probably end up having a server that hosts multiple roles, mainly the Mailbox, Client Access, and Hub Transport roles. The larger the organization, the more dedicated those server roles will get.

Exchange Server 2007 Editions and Licenses

The next important area to consider when planning your Exchange server deployment is which editions of Exchange Server 2007 you will use and what type of licenses you will buy for your users. This topic is especially important, as it can save you money if you plan thoroughly.

Exchange Server 2007 Editions

As in previous Exchange versions, there are two server editions available: Standard and Enterprise. Whereas the Standard Edition is targeted for small-to-medium companies, it also can be used for specific server roles as well as in small branch offices. The Enterprise Edition supports failover cluster and more storage groups and databases, and thus is targeted to large companies. Table 1.4 provides an overview of each edition's offerings.

T A B L E   1 . 4   Exchange Server 2007 Edition Offerings

Feature	Standard Edition	Enterprise Edition
Storage group support	5 storage groups	50 storage groups
Database support	5 databases	50 databases
Database limit	16TB storage limit	16TB storage limit
Single-copy clusters	Not supported	Supported
Local continuous replication	Supported	Supported
Cluster continuous replication	Not supported	Supported

> As a general guideline, you should consider Exchange Server 2007 Enterprise Edition for large Mailbox servers that host 1,000-plus users or that need high availability due to their importance. All other servers, like Hub Transport or Client Access servers, should have Exchange Server 2007 Standard Edition to preserve your budget.

Exchange Server 2007 Client Access Licenses

Exchange Server 2007 comes with two client access license (CAL) editions that are also called Standard and Enterprise. The difference from the server editions is that the CAL is an additive license, so you always need to buy a Standard Edition CAL and then add an Enterprise Edition CAL to gain advanced functionality, such as managed folders.

Both CAL editions can run against either server edition; thus a Standard CAL can run against an Enterprise Edition server and vice versa. Table 1.5 shows an overview of what each CAL edition offers.

T A B L E   1 . 5   Exchange Server 2007 Client Access Licenses

Features	Standard CAL	Enterprise CAL
Email, shared calendaring, contacts, tasks	X	
Outlook Web Access	X	
Exchange ActiveSync	X	

T A B L E   1 . 5   Exchange Server 2007 Client Access Licenses *(continued)*

Features	Standard CAL	Enterprise CAL
Unified Messaging		X
Per-user/per-distribution list journaling		X
Managed email folders		X
Forefront security		X

Making Up a Server-Placement Plan

After considering all these points, you are ready to pull it all together. Build a table that consists of the following columns to plan you server placement:

- Server role (Mailbox, CAS, etc.)
- Number of users to be hosted on this server (special for Mailbox servers)
- AD site location
- Number of global catalog servers in AD site
- Domain
- Windows 2003 server role (e.g., member server)
- Exchange Server 2007 server edition (Standard or Enterprise)

Once again, consider the following general rules regarding Exchange server roles when creating your server-placement plan:

- Hub Transport servers must communicate with global catalog servers. Thus there must be at least one in its AD site.
- Mailbox servers must be located in the same AD site where Hub Transport servers are available. All sending of email is done using the Hub Transport server.
- As the Client Access server provides the connectivity point to the Mailbox servers, a Client Access server must be deployed to the same AD site where Mailbox servers are located. Every user uses the Client Access server to connect directly to the Mailbox server to retrieve messages, but sending messages is done through the Hub Transport server.
- Unified Messaging servers must be located in the same AD site with a Hub Transport server, as they submit messages through this server. The Unified Messaging server should also be located in a hub site or near the IP/Voice over Internet Protocol (VoIP) gateway or IP private branch exchange (IP/PBX).

This list will provide you with an overview and start your planning considerations but you should also consider areas that are covered in the next sections.

Evaluating Network Topology and Providing Technical Recommendations

Evaluating the network topology on which Exchange Server 2007 will communicate is important so that you will not be surprised by problems that have been forgotten in planning. Especially in the network area, changes need time to be implemented, so considering this well will save time later when implementing Exchange Server 2007.

Reviewing Current and Planned Network Topology

The first step is to collect all information about your network, the perimeter network, and its external collections as thoroughly as possible from a variety of sources. They include the following:

- Physical network topology (verify that TCP/IP is used everywhere, and that IPv4 or IPv6 and IP subnets are used according to location)
- Physical network connections or links internally (LAN and WAN links, router, etc.)
- Any external physical network connection (e.g., Internet, partner companies, etc.)
- Interconnection of physical network connections (i.e., hub-and-spoke, ring or star, point-to-point)
- Physical network speed (separate between guaranteed bandwidth and available bandwidth for every network link)
- Any network protection that might interfere (e.g., firewalls that protect physical links or network link encryption devices that reduce the link speed)
- Firewall port availability to external and internal systems
- Server name resolution used in locations or between locations (i.e., DNS/WINS name resolution)
- Defined namespaces in DNS
- Perimeter network servers (any servers that are located in a perimeter network, especially any server that provides SMTP-relay functionality)

Make sure you write down any changes that might occur in the near future so you can include them in the planning from the start.

> In large organizations, gathering this information might be quite a time-consuming effort, as you have to sit together with many different network teams to get a thorough understanding of the details of the network! If you want to evaluate a global network including many sites, make sure you talk to at least one network team on every continent and ask them for their opinions. This will provide you with much insight into their current network problems and potential that you can use when planning the messaging design.

Avoiding Pitfalls by Providing Technical Recommendations

The following list provides ways to avoid potential pitfalls on the network topology side. Any problems must be rectified before Exchange Server 2007 can be installed at the location.

- Make sure that the physical network speed of locations that will host Exchange Server 2007 have at least 64 Kb per second of bandwidth available.

- Exchange Server 2007 supports TCP/IP v4 (IPv4) addresses only, not IPv6 addresses. If you already implemented IPv6 addresses anywhere in your company, make sure that the company also supports IPv4 addresses; otherwise the clients will not be able to communicate with Exchange Server 2007.

- IP subnets should map to the locations of the company and should be non-overlapping between locations. However, sometimes single locations have multiple IP subnets, which is fine. If IP subnets are spanned between multiple physical locations, make sure the WAN link between them matches LAN link speed—i.e., 10 megabits per second (Mbps) or more.

- Make sure your Active Directory sites match IP subnets for each location.

- Domain Name System (DNS) must be used for network name resolution.

- DNS is configured correctly in your Active Directory forest, using a single, unified namespace.

- Active Directory uses service (SRV) resource records in DNS to register a list of domain controllers for client use. If you do not use Windows Server 2003 DNS Service for Active Directory, make sure that your DNS server software supports this!

- DNS must be able to resolve Internet DNS URLs to successfully deliver messages to the Internet. The DNS configuration must allow this.

- The company must have its own domain and domain name. Exchange Server 2007 requires an appropriate mail exchanger (MX) resource record in DNS to receive messages from the Internet.

- You cannot use a disjoint DNS namespace! A *disjoint namespace* is the scenario in which the primary DNS suffix of a computer does not match the suffix of the domain name where that computer resides.

Designing and Planning for New Exchange Features

Several new features in Exchange Server 2007 need special consideration in your design. For automation of administrative tasks you can use the Exchange Management Shell, or you can implement voice access to your mailboxes using the Unified Messaging server role. It is also worth considering in your design that the Edge Transport server role can replace existing third-party smart hosts. They are covered in this section.

The Exchange Management Shell

The Exchange Management Shell (Figure 1.4) is a new task-based command-line shell and scripting language that will tremendously ease the way you do administration. Using the EMS you can perform every task that can be done in the Exchange Management Console, and additional tasks that cannot be done there.

F I G U R E 1 . 4   The Exchange Management Shell
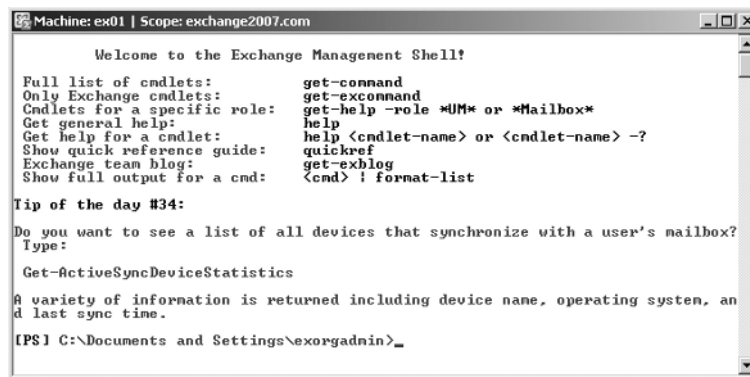
The planning aspect of this new feature is mainly that all Exchange administrators should get training to understand the basics of how to use the EMS and how to create batch processes that ease their daily business lives. By default, the Exchange Management Shell can be used by anybody that has Exchange-related permissions. Thus, Exchange Server Administrators or Exchange Recipient Administrators can use it to modify configuration or object attributes.

Unified Messaging

Unified Messaging is one of the key new features in Exchange Server 2007. Using it you will be able to access your mailbox not only with Microsoft Outlook, but also using a standard telephone line. Unified Messaging provides the following features to the user:

Call answering: Acts like an answering machine.

Fax receiving: You can receive a fax, but not send a fax!

Voice access to your mailbox: Listen to, forward, and reply to email messages and voice mail, listen to calendar entries and accept or reject them, dial contacts, or set voicemail "out of office" messages.

User configuration: Gives you voice access to your Unified Messaging system. You can define a personal greeting or describe how to search in the organization's directory.

The Unified Messaging IP Gateway

The Unified Messaging (UM) IP Gateway connects your telephone system to your Exchange environment. It is used with a legacy PBX to convert the circuit-switched protocols found on a telephony network to IP-based packet-switched protocols. To support Exchange Server

2007 Unified Messaging, one or both of the following can be used to connect the telephony network infrastructure to your data network infrastructure:

- IP/PBX (a single device)
- PBX (legacy) and an IP/VoIP gateway (two separate devices)

Of course, depending on the size of your organization, you might include additional UM IP Gateways depending on the requirements of your telephony network. You should talk to your telephony people in your organization to plan how to best implement this feature for your organization.

A Unified Messaging Deployment Plan

To implement Unified Messaging in your organization, you must follow these common steps:

1. Deploy the Unified Messaging server role: Depending on the size of your organization and number of users you want to connect using Unified Messaging, you should add the role to an Exchange server or set up a dedicated Unified Messaging server in your environment.

2. Receive telephone lines or organize channels: Start talking to your telephone people to receive phone lines that you can organize.

3. Deploy IP/VoIP gateways: Once you receive the information, you can start to deploy IP/VoIP gateways and add the channels or numbers.

4. Make sure you have the correct Client Access License (CAL) for your users! They need an Enterprise CAL for using Unified Messaging.

Edge Transport

Another new feature in Exchange Server 2007 is the implementation of a smart host and SMTP relay version of Exchange Server that is not part of your company's domain and will be placed in the perimeter network or directly on the Internet. A smart host is a designated server through which an email server routes all outgoing messages. Placing previous Exchange Server implementations outside your company's firewall was always dangerous: the Active Directory and Exchange Server needed full access to your company's network, so any security threads could have spread into your company easily.

As a solution, most of the Exchange Server implementations that I know about use dedicated smart-relay software, mainly based on Linux operating system. The Edge Transport server now fills this gap. It uses the Active Directory Application Mode (ADAM) to store configuration and recipient information locally. Thus only information that is needed on the server is stored there. It handles all Internet-facing mail flow as well as provides protection against spam and viruses.

Antivirus and Antispam

The Edge Transport server includes some sophisticated agents that help you to prevent messages that include spam or viruses from entering the organization. They provide different

layers of protection, including attachment, connection, content, recipient, and sender filtering, as well as a sender ID agent.

Messaging Policy and Compliance

To satisfy any legal, regulatory, or internal requirements to filter, process, or store messages going inside and outside the organization, the Edge Transport role is equipped with the following agents:

Address Rewrite agent: This agent lets you modify SMTP addresses on messages that go inside or outside of the Exchange organization. This is especially useful in scenarios where the internal email address should not be disclosed or should be standardized after a company merger.

Edge Rules agent: Using rules, you are able to control the flow of messages that are sent or received from the Internet. The rules are based on specific words or text patterns in the message subject, body, header, or From field, the spam confidence level (SCL), or attachment type. Actions include quarantining a message, dropping or rejecting messages, appending additional recipients, or logging an event.

Planning for the Edge Transport Server

To plan the implementation of the Edge Transport server, consider the following issues:

- Edge Transport servers are stand-alone servers. Never plan to integrate them into your Active Directory, as they still will use ADAM and not utilize AD.

- An Edge Transport server can be subscribed to an Active Directory site. This will integrate the Edge Transport into the Exchange organization, starting synchronization of all Exchange organizational configurations (e.g., accepted domains). If you do not integrate the Edge server into your Exchange organization it will act as a stand-alone server and you also will not be able to use the antispam features, recipient lookup, or safe list aggregation features.

- Plan where you want to place Edge Transport servers in your perimeter network. For load-balancing consider installing multiple machines for every Internet connection.

- You can coexist with available smart host servers, but to receive the full benefit you should concentrate on a single implementation only.

Designing Organization Configuration to Meet Routing Requirements

This section will show you how Exchange Server 2007 routing works and what design-related aspects you should include in your Exchange Server 2007 implementation plan. After a discussion of internal message routing, we will look at external message routing.

Real World Scenario

Using Edge Transport Servers to Ease Administration

A great benefit of using Edge Transport servers for smart-host functionality is when you use Edge subscription in your Exchange organization. A subscription basically connects the stand-alone Edge Transport server to your configuration information; thus you will be able to configure your Edge Transport servers using Exchange Management Console or Exchange Management Shell.

I have seen companies that had quite a few smart-host servers out there sitting at the Internet connection points. Whenever there was an SMTP address change or a new address to add, we needed to configure it at every smart host that routed messages. Guess what happened? Occasionally some servers were missed, and so sometimes the message resulted in a non-delivery receipt (NDR) and sometimes not. Figuring out where the problem resides was then an extremely difficult task.

Now, with the Edge Transport role, we plan to homogenize our entire smart-host server farm using Exchange Server 2007. That way we can reduce not only the number of servers installed, but also the administrative effort.

Internal Message Routing

In Exchange 2000 and Exchange 2003 you defined message routing inside an Exchange organization by using routing groups and routing group connectors. Exchange Server 2007 introduces major changes to internal message routing:

- The message-routing topology and routing decisions are based on the Active Directory site topology (AD sites and IP site links).
- Routing is configured automatically, so you do not need to configure any routing group connectors.

Table 1.6 provides an overview of internal message routing in Exchange Server 2007 as it correlates to Exchange 2000/2003.

TABLE 1.6   Internal Message Routing in Exchange Server 2007 Compared to Exchange 2000/2003

Exchange Server 2007	Exchange Server 2000/2003
Hub Transport server	Dedicated bridgehead server
Active Directory site	Routing group

T A B L E   1 . 6   Internal Message Routing in Exchange Server 2007 Compared to Exchange 2000/2003 *(continued)*

Exchange Server 2007	Exchange Server 2000/2003
IP site link	Routing group connector
Cost of IP site link	Cost of routing group connector

Routing between Exchange Server 2007 and Exchange 2000/2003 is explained in Chapter 4, "Designing and Planning Coexistence and Migrations." Here I will focus entirely on the Exchange Server 2007 routing technology.

Before we dig deeper into Exchange Server 2007 internal message routing, two concepts that should be explained—namely the Exchange Server 2007 routing table and the least-cost routing path.

The Exchange Server 2007 Routing Table

Every Exchange Server 2007 Hub Transport server calculates the routing topology based on the Active Directory configuration that includes AD sites, AD site links, Exchange servers and their relation to AD sites, SMTP connectors, third-party connectors, and mailbox and public folder stores; as well as legacy Exchange 2000/2003 routing groups and connectors. This will make up what is called the *routing table*.

> **NOTE**   The routing table is calculated every time the Hub Transport server is started or when configuration changes (e.g., Active Directory change notifications) occur.

Least-Cost Routing Path

When multiple routing paths exist for a message, the routing path is calculated based on an algorithm to select a single path over which the message will be routed. The following logic is used:

- Calculate the cost to the target AD site by adding all IP site link costs or connector costs between the source and the target site. If there are multiple paths, only the path with the lowest aggregated cost will be used.
- If there are multiple paths with the same lowest aggregated costs, the routing path with the least hops is selected.
- If there are still multiple paths available, the site name with the lowest alphanumeric name is selected. Starting with the site name to the target AD site, the algorithm will go backward along the path until it finds a site name that doesn't match.

> **WARNING**   Remember: there might be other factors like message size limits or connector scope that can influence the least-cost routing path!

Hub Transport Server Routing Rules

As explained before, Hub Transport server is the only Exchange Server 2007 server role to route messages within an Exchange organization. Of course, the Edge server role can also route messages, but only to and from the Internet.

> **WARNING**   Another difference between Exchange Server 2007 and previous Exchange versions is that any message must now be sent through a Hub Transport server, even if the recipient is on the same Mailbox server as the sender.

Internal message routing in Exchange Server 2007 uses SMTP as its primary message-transport protocol and is based on the following two basic rules:

If the message target recipient is within the same AD site the Hub Transport server delivers the message directly to the Mailbox server where the recipient mailbox resides.

If the message is targeted to a recipient located in a different AD site the Hub Transport server sends it directly to a Hub Transport server in the target AD site. This means that the message does not relay to each AD site along the least-cost routing path as previous versions of Exchange did! It will choose the target Hub Transport server using round-robin load-balancing mechanisms. Only if the preferred Hub Transport server becomes unavailable will it choose another Hub Transport server.

As most large-scale network environments are complex, some situations require special configurations. What happens when the target AD site is offline due to network problems? Or what about firewall settings where network traffic is forced to flow through specific AD sites? These issues are covered in the following paragraphs.

Queue at Point of Failure

Exchange Server 2007 uses the least-cost routing path information when no Hub Transport server in the destination AD site responds due to network issues or server outages. In this situation the least-cost routing path will be used in reverse order: from the destination AD site to the source AD site. All AD sites will be contacted along this path, and if a Hub Transport server is available, the message will be queued there in a retry state. Thus the message will be delivered to a Hub Transport server that seems to be the closest one to the target Hub Transport server from the IP site link cost perspective. This is called *queue at point of failure*.

For example, say you have Site 1, Site 2, and Site 3 that have a cost of 5 and are connected Site 1 to Site 2, and Site 2 to Site 3. Hub Transport servers exist in all three sites. Let's assume that we have a message being sent from Site 1 to Site 3. Under normal behavior the Hub Transport server in Site 1 would send it directly to the server in Site 3. However, if the server in Site 3 is offline, the message cannot be sent directly. Queue at point of failure would be when the Hub Transport server delivers the message to the server in Site 2 for queuing, as it knows that this site is closer to the target site (Site 3) than its own server is.

Hub Sites

One way to interfere with the least-cost routing path is by defining hub sites through which all message flow must be relayed. You can think of this situation as a former hub-and-spoke design with a messaging backbone.

You might have hub sites if a firewall prevents direct communication between certain AD sites or if a company policy exists where all message traffic must be routed through a special AD site.

> **WARNING**   A hub site is considered only when it lies on the least-cost routing path calculated by the Hub Transport server. Before you implement hub sites, it is important that you review your Active Directory topology to make sure that the least-cost routing path always includes the AD sites you want to define as hub sites.

You can configure hub sites using the Exchange Management Shell and the `Set-AdSite` command. You have to do this site by site, so keep track of what changes you made!

The following command shows an example where I set the hub site to the AD site Site2. You have to be Exchange Organization Administrator to configure this.

```
Set-AdSite -Identity "Site2" -HubSiteEnabled $true
```

Modifying IP Site Link Costs

The Active Directory site topology might not be optimum for Exchange message routing in specific cases. For that reason there is a way to modify the least-cost routing path by modifying the cost of IP site links. Doing so will add an Exchange-specific cost to the IP site link but will not modify the current setting in Active Directory costs. Of course, if you set an Exchange cost, this overrides the Active Directory cost for message-routing purposes.

> **WARNING**   After considering your Active Directory site topology and placing your servers in the right sites, you should carefully consider if you need to implement Exchange-related IP site link costs, as they are quite hard to manage.

The following Exchange command-shell command assigns an Exchange-specific cost of 20 to the IP site link called Link3-4:

```
Set-ADSiteLink -Identity "Link3-4" -ExchangeCost 20
```

Delayed Fan-Out

In a message that is addressed to multiple recipients, the routing technology I explained before would mean that a copy is created for every recipient. However, Exchange Server 2007 uses a technique called *delayed fan-out* to preserve bandwidth when routing messages with many recipients.

After each recipient has been resolved by the Hub Transport server, Exchange Server 2007 compares the routing path for each recipient. The splitting of messages into multiple copies does not occur until a Hub Transport server is reached, which splits up the routing path. Microsoft calls such a Hub Transport server a *fork* in the routing path.

For example, we have a message addressed to one recipient in every AD site, Site 1, Site 2, Site 3, and Site 4. From an Active Directory standpoint, they are all connected sequentially, Site 1 to Site 4. The first message will get transferred to Site 2 as a single message where the Hub

Transport will deliver a local copy to the recipient in Site 2 and deliver one message, including recipients in Site 3 and Site 4, to the Hub Transport server in Site 3. As you can see, especially for messages with large numbers of recipients, this feature saves a lot of bandwidth.

External Message Routing

Now you've got a grip on internal message routing, so let's turn to routing of the external variety. In this section I will provide an overview of what features exist for message routing to external systems, like the Internet or foreign systems.

In Exchange Server 2007, external connectors are classified in the following three ways:

- Send connectors
- Receive connectors
- Foreign connectors

These types of connectors can be configured on Hub Transport and Edge Transport servers. Connectors can be configured using the Exchange Management Console, but many more details are available when using the Exchange Management Shell.

Send and Receive connectors always use SMTP as their message protocol, where Foreign connectors might use other message protocols, such as X.400, to transmit messages.

> **NOTE** You do not need to configure an Internet connection if you have an Edge Transport server, as it will be installed automatically when you subscribe the Edge Transport server to the Exchange organization.

Send Connectors

Using Send connectors you can configure an outbound SMTP connection. Send connectors allow you to do the following:

- Set one or more source servers that the connector uses to deliver messages.
- Configure a dedicated address space for the connector.
- Decide where to route the messages to (by using a smart host or just using DNS MX resolution).

Here's how Send connectors factor into planning: If you don't use Edge Transport servers as Internet smart-relay hosts, then you should include Send connectors wherever you have a network connection point, such as a direct partner connection, an internal re-route, or an Internet connection.

Receive Connectors

To receive external messages, you need a Receive connector. This connector acts as an inbound connection point that you can configure to accept connections based on IP address ranges and port numbers.

Real World Scenario

Using Direct Connectors to Business Partners

In my company we work very closely with a couple of other companies; we also have a direct network link connecting us all together. This link is used to exchange confidential data as well as access to certain systems.

As these links normally are utilized only during specific times of the day, it's a big benefit to configure Send and Receive connectors using these links. They have their own SMTP address space, and messages use only the direct connection.

Not only does my company save the traffic that would be generated by all the messages first being sent to the Internet and then being received by the target again, but we also improve security as messages are not routed over the Internet.

> **NOTE** You can configure a Receive connector on a per-server scope only. Thus, if you want to have many servers receive messages, you need to configure every server.

Receive connectors have configuration limits that you can set, such as number of active connection, maximum message size, or maximum recipients per message. You also can set the type of authentication required to send a message. What does this have to do with planning? Well, you should configure Receive connectors at every Hub Transport server that serves an external inbound connection. Also, you should have dedicated Receive connectors for your applications that want to send messages so that you understand how many applications send messages to your system.

Foreign Connectors

A Foreign connector does not use the SMTP protocol for communication. Third-party Short Message Service (SMS) gateways or fax gateways are examples.

To be able to communicate with these third-party systems, the connector uses a Drop directory on the Hub Transport server to send messages to the foreign gateway servers. Foreign gateway servers can send messages to Exchange Server 2007 by using the Replay directory.

Every foreign connector has an address space assigned to it that includes the following elements:

Connector Scope: What Hub Transport servers can use the connector

AddressSpaceType: For example, fax or SMTP

AddressSpace: An valid address space for the AddressSpaceType

AddressSpaceCost: Routing costs

Table 1.7 shows a list of connectors that are no longer available in Exchange Server 2007, and it describes how to maintain their functionality in Exchange Server 2007.

T A B L E   1 . 7   Discontinued Connectors and What to Do in Exchange Server 2007

Connected System	What to Do
Lotus Notes/Domino 5.x or earlier	Retain a computer with Exchange Server 2000/2003 in your Exchange organization.
Lotus Notes Domino 6.x or later	Implement SMTP as your mail-routing protocol and use Microsoft Transporter Suite for Lotus Domino for directory sync.
Novell Groupwise	Retain a computer with Exchange Server 2000/2003 in your Exchange organization.
X.400 connectivity	Retain a computer with Exchange Server 2000/2003 in your Exchange organization.

Planning for Foreign connectors is a key task when doing an Exchange Server 2007 design. You should consider the following in your plan:

▪   Consolidate Foreign connectors to save budget.

▪   Plan for fault tolerance when implementing Foreign connectors; make sure the Drop directory is available.

▪   Make sure the third-party connector is fully supporting Exchange Server 2007 before you move it over to the Exchange server, especially if you are in an environment where Exchange 2000/2003 still exists.

> **NOTE**   Remember: if you need Exchange 2003 servers in your environment, you need to install them before installing Exchange Server 2007!

Viewing the Routing Table

Unfortunately the WinRoute tool that was used to view the routing table in Exchange Server 2000/2003 does not work with Exchange Server 2007. Microsoft did not provide any replacement with the release version of Exchange Server 2007, but will provide a new version in Exchange Server 2007 Service Pack 1.

> **TIP**   The Routing Log Viewer for Exchange Server 2007 can read the routing topology from your Hub Transport and Edge Transport server roles and will provide a view into the routing table logs. The Routing Log Viewer tool will be part of the Mail flow tools within the Toolbox in Exchange Server 2007 Service Pack 1.

Summary

Planning a message service for a medium-to-large organization is quite a time-intensive and difficult task. You have to consider many factors, and you have to be especially aware of products that might interfere with the message service. Exchange Server 2007, with its tight integration with Active Directory, requires an Exchange messaging IT pro to have an excellent understanding of all Active Directory–related technologies, such as the impact of IP sites and IP site links.

To start off your planning, you should thoroughly investigate what is available within the company itself.

- From a technical perspective, you need to understand the company's network topology, its Active Directory implementation, how messaging is done today, and what other products might interfere with the messaging system.

- It is also crucial to know about the business factors of the company: What is the future IT strategy? Who are the key stakeholders of the IT system and what are their expectations? Are large data centers in their focus, or do they like to build more sites with messaging servers? You should also consider the company's acceptable amount of server downtime, their existing Service Level Agreements, and any security or regulation requirements.

If you can consider all these topics together and if you understand what Exchange Server 2007 can offer, then you have a good way to create a solid plan for a messaging service. And that is exactly what is required to be an excellent Exchange messaging IT professional.

Exam Essentials

Understand how Exchange Server 2007 relies on Active Directory   Exchange Server 2007 depends heavily on Active Directory and has certain requirements in terms of Service Packs applied to domain controller or global catalog servers. You need to understand the requirements of Exchange Server 2007 on the Active Directory, and what functional mode your domains and forest must run in. Also, it is important to know which domains need to be prepared for Exchange and how the preparation is done.

Know about the Exchange Server 2007 administrative roles and permissions   To design a good Exchange Server 2007 permissions model, you need to have a good understanding of which administrative roles you have available for delegating certain tasks, and of how they apply to your system. You should understand when to use the split-permissions model and when you need to use server provisioning.

Understand the different Exchange Server 2007 roles and their planning aspects   Exchange Server 2007 comes with new server roles that all have specific functions and need separate planning. To build a good plan for implementing these roles, you need to understand all requirements as well as their specific features. Additionally, it is important to understand budgetary decisions (e.g., what Exchange Server edition you will use) and other business factors that might impact where you plan to install an Exchange server.

Have a solid understanding of your network topology   The network topology is the basis of a good messaging environment and thus it is very important to know exactly what is going on in your organization's network, as well as where its external connections are. Based on this evaluation, you must understand what requirements Exchange Server 2007 has on the network topology to prevent problems. Understanding each technical recommendation in this chapter will help you there.

Get to know the new features of Exchange Server 2007   As Exchange Server 2007 introduces a couple of new features that might improve your user's working experience, you need to have a good understanding of what the benefits of these new features are and of how to plan them into your overall messaging design. In particular, the Unified Messaging and Edge Transport server roles offer quite a bit of potential.

Understand how Exchange Server 2007 improves message routing   As the routing topic is key to every messaging system, you must have a thorough understanding of what is improved by Exchange Server 2007. What aspects of internal and external message routing are different from previous versions of Exchange? Be sure you understand exactly when you need to define a hub site and when to define Exchange-specific costs. You should also be able to describe the term *delayed fan-out*.

Review Questions

1. What Active Directory requirements do you have if you want to install Exchange Server 2007 into your forest? (Select all that apply.)

    A. Windows Server 2003 Service Pack 1 or later must be installed on the server that hosts the Schema Master role.

    B. All domains where you want to install Exchange Server 2007 must run in Windows 2003 domain functional mode.

    C. Domains where you install Exchange Server 2007 must run in Windows 2000 native domain functional mode.

    D. Install at least Windows Server 2003 Service Pack 1 on all global catalogs that are located in AD sites where you plan to install Exchange Server 2007.

2. Which groups in the following list will be created in the Microsoft Exchange Security Groups container during Exchange Server 2007 setup? (Select all that apply.)

    A. Exchange Recipient Administrators

    B. Exchange View-Only Administrators

    C. Exchange Servers

    D. ExchangeLegacyInterop

    E. Exchange Organization Administrators

3. What actions in the following list does the setup command `/PrepareAD` perform? (Select all that apply.)

    A. Prepares all domains (`/PrepareDomain`)

    B. Extends the schema if it was not extended yet

    C. Configures global Exchange objects in the configuration partition

    D. Prepares the root domain (`/PrepareDomain`)

4. Which of the following statements regarding Exchange Server 2007 domain preparation (`Setup /PrepareDomain`) is correct? (Choose one.)

    A. All domains must be domain-prepared; otherwise Exchange Server 2007 will not work correctly.

    B. All domains that will include Exchange Server 2007 servers, as well as the root domain, need to be domain-prepared.

    C. The root domain (even if no Exchange Server 2007 is installed in it) and all domains that will include either Exchange Server 2007 servers or Exchange-related objects like mail-boxes must be domain-prepared.

    D. All domains that will include Exchange Servers 2007, as well as the root domain (even if no Exchange Server 2007 is installed in it) and domains that include global catalog servers that are part of an Exchange Server 2007 AD site must be domain-prepared.

5. What permission do you need to prepare a child domain for Exchange Server 2007 (i.e., run `Setup /PrepareDomain`)? (Select all that apply.)

   A. Exchange Organization Administrators permission on the Exchange organization.

   B. Administrator permission on the Exchange Server.

   C. Domain Admin permission in that domain (if the domain existed when `/PrepareAD` ran).

   D. If the domain that did not exist when you ran `/PrepareAD`, you need to be member of the Exchange Organization Administrators group as well as Domain Admin.

6. In order to manage all Exchange-related objects in the Active Directory, what Exchange role do you need to perform this task? You do not have any extra Active Directory permissions like Domain Admin assigned to your account! (Select all that apply.)

   A. Exchange Organization Administrators

   B. Exchange Recipient Administrators

   C. Exchange View-Only Administrators

   D. Exchange Server Administrators

7. The user Joel has Exchange Server Administrator permissions on Server A and Server B. What statement is true regarding his permissions? (Choose one.)

   A. Joel is able to move mailboxes between Server A and Server B.

   B. Joel can change the Exchange organization configuration (e.g., adding a new address list) and also any Exchange Server configuration (e.g., dismount a database) on Server A and Server B.

   C. Joel can add and remove mailboxes to Server A and Server B as well as move mailboxes between those servers.

   D. Joel can change any Exchange Server configuration (e.g., dismount a database) on Server A and Server B.

8. The Exchange Server Administrator role can be delegated to the following Active Directory objects. (Select all that apply.)

   A. User object

   B. Universal security group object

   C. Global group object

   D. Local group object

9. In my Exchange organization, I want to delegate the right to install an Exchange Server 2007 server for a user called Andy. As I don't want to give full permissions using the Exchange Organization Administrators group, what can I do instead? (Choose one.)

   A. I can create a server object for Andy's new server and try to delegate using the Exchange Server Administrator role.

   B. I can add Andy to the Exchange Recipient Administrators group and give him local Administrator permission on his new Exchange Server 2007 server. That will be sufficient to install Exchange Server 2007.

   C. I can create a computer object in Active Directory for the Exchange Server 2007 server and use the `/ProvisionServer` command with Exchange setup.

   D. I can create a computer object in Active Directory for the Exchange Server 2007 server and use the `/NewProvisionedServer` command with Exchange setup.

10. Which of the following statements regarding domain controller and global catalog requirements for Exchange Server 2007 is correct? (Select all that apply.)

   A. At least one global catalog must be available in the same AD site where you plan to install Exchange Server 2007.

   B. At least one domain controller of the same domain as the Exchange server must be available in the AD site where you plan to install Exchange Server 2007.

   C. All domain controllers must be upgraded to 64-bit.

   D. All global controllers in the AD site where you plan to install Exchange 2003 must be upgraded to Windows Server 2003 Service Pack 1 or later.

11. You are about to create a server plan for a smaller location (fewer than 250 mailboxes) where, based on business factors, the decision was made to install an Exchange mailbox server. A domain controller that is a global catalog is available in the AD site. The budget is not the biggest one; based on best practices, what should you do? (Choose one.)

   A. To preserve budget you should install the Exchange Mailbox role on the domain controller.

   B. You should buy one new server that will host the Exchange Mailbox role, the Client Access role, and the Hub Transport role for that location. Nothing more needs to be done.

   C. You should buy three new servers, one for each role: Mailbox, Client Access, and Hub Transport.

   D. You should buy one new server where the Exchange Mailbox role is being installed on. Nothing more needs to be done.

12. Andy is working on an Exchange Server placement plan for a larger site (3000-plus mailboxes). The business factors dictate that the Mailbox server must be highly available. Additionally, the company heard about a new Exchange Server 2007 feature to call into their mailboxes and the IT decision-maker wants to use it. Which of the following routes should Andy take? (Choose one.)

   A. He should install a clustered Mailbox server that includes the Hub Transport, the Client Access, and the Unified Messaging roles on a single clustered machine. This will provide sufficient availability for the messaging system.

   B. He should install a clustered Mailbox server and two other servers: one for Client Access and Unified Messaging roles and one for the Hub Transport server.

   C. He should install a clustered Mailbox server and install three other servers: two of those hosting the Client Access and Hub Transport server roles, and one for the Unified Messaging role.

   D. He should install a normal Mailbox server that includes all four server roles required: Mailbox, Hub Transport, Client Access, and Unified Messaging server.

13. Which of the following are network requirements of Exchange Server 2007? (Select all that apply.)

   A. TCP/IP v4 (IPv4).

   B. TCP/IP v6 (IPv6).

   C. Domain Name Service (DNS).

   D. AD sites must be connected by a permanent WAN or LAN link.

14. Which of the following are features included in Exchange Server 2007 Unified Messaging? (Select all that apply.)

    A. Call answering

    B. Fax sending

    C. Voice access to mailbox

    D. Delayed fan-out

15. Your messaging system currently includes five Internet connections where per connection you have two smart hosts each running on the Linux operating system. You are planning to replace them using Exchange Server 2007. You want to manage them centrally in your Exchange organization.

    A. You need to install the Edge Transport server role on 10 servers that are stand-alone and use the Edge subscription to the closest Exchange Hub Transport hosting AD site.

    B. You need to install the Edge Transport server role on 10 servers that will join the Active Directory and use the Edge subscription to the closest Exchange Hub Transport hosting AD site.

    C. You need to install the Hub Transport server role on 10 servers that will join the Active Directory and just configure connectors between each server and the closest Exchange Hub Transport servers.

    D. You need to install the Hub Transport server role on 10 servers as stand-alone and con-figure connectors between each server and the closest Exchange Hub Transport servers.

16. Which of the following is included in the Exchange Server 2007 routing table? (Select all that apply.)

    A. Active Directory sites

    B. Active Directory site links

    C. Exchange servers and their relation to AD sites

    D. Exchange Client Access servers

    E. Exchange mailbox and public folder stores

17. Joel sends a 5 MB message to 100 recipients located in five AD sites; the local one is Site 1 and there are four distant sites called Site 2, Site 3, and Site 4. These AD sites are all hosting Exchange Server 2007 Hub Transport servers and include IP site links that are configured in the following way: Site 1 – Site 2, Site 2 – Site 3, Site 2 – Site 4, Site 2 – Site 5. Which of the following statements about what will happen with the message is true? (Choose one.)

    A. The Hub Transport server in Site 1 will connect to all other sites and send one message for each recipient.

    B. The Hub Transport server in Site 1 will calculate the routing path for every recipient and connect to all four sites to send one message per site that include the recipients for their respective site. The Hub Transport will deliver the message to all local recipients directly to their mailbox store.

    C. The Hub Transport server in Site 1 will calculate the routing path for every recipient and deliver the mail to all local recipients. For all recipients that are not in the same site, it will create a single message to be sent to the Hub Transport server in Site 2. This server will again

calculate the routing path for every recipient and deliver the mail to all distant sites (one message for each site) as well as to the local recipients.

D. The Hub Transport server in Site 1 will deliver the message to all local recipients and send one message to Site 2. There the Hub Transport server will also deliver the message to all local recipients and send one message to Site 3. This will continue until we've reached all recipients.

18. We're in an Active Directory environment that includes four AD sites: Site 1, Site 2, Site 3, and Site 4. They are all linked sequentially, Site 1 – Site 2, Site 2 – Site 3, and Site 3 – Site 4. All AD sites include Hub Transport servers. A message will be sent from Site 1 to Site 4 but all Hub Transport servers are not available using a direct connect. What will happen? (Choose one.)

A. The message will stay on the Hub Transport server in Site 1 until a Hub Transport server in Site 4 is reachable.

B. The message will be transferred from Site 1 to Site 2 and stay there until a Hub Transport server in Site 4 is reachable.

C. The message will be transferred from Site 1 to Site 3 and stay there until a Hub Transport server in Site 4 is reachable.

D. The message will be transferred to another Hub Transport server in Site 1 to try a different connection to Site 4.

19. What external connectors are available on a Hub Transport server? (Select all that apply.)

A. Send connector

B. SMTP connector

C. Foreign connector

D. Lotus Notes Domino connector

E. Receive connector

F. X.400 connector

20. Sigi is an administrator at a global company with 10,000 users that have mailboxes. The company's IT strategy is to consolidate as much as possible but be careful that all users are still able to use the full functionality of their Outlook 2007 client. Their Active Directory consists of 5 domains that include a root domain that is empty. They currently have firewalls between 2 of their 10 AD sites installed. Active Directory and messaging administration is separated. What is important to consider when planning a message system in this environment? (Select all that apply.)

A. The network topology has to be evaluated if data center consolidation is possible.

B. The AD site design must be reviewed.

C. All domains that include Exchange-related objects or Exchange servers have to be prepared; as does the empty root domain.

D. An extra forest for Exchange Server 2007 must be implemented to ease the process of separated administration.

E. As they have firewalls between AD sites, the Exchange routing feature of setting hub sites must be used.

Answers to Review Questions

1. A, C, D. Exchange Server 2007 requires only the Windows 2000 native domain functional mode, even though it is a good practice to use the Windows Server 2003 domain functional mode. From the software side it is required to install Windows Server 2003 Service Pack 1 or later on domain controllers and global catalog servers that communicate with Exchange Server 2007.

2. A, B, C, D, E. Exchange Server 2007 setup creates an organizational unit in root domain called Microsoft Exchange Security Groups, including the following universal security groups (USGs): Exchange Organization Administrators, Exchange Recipient Administrators, Exchange View-Only Administrators, Exchange Servers, ExchangeLegacyInterop.

3. B, C, D. The Prepare Active Directory command `Setup /PrepareAD` extends the schema if it was not already extended, configures global Exchange objects in the configuration partition (e.g., Exchange Administrative Group—FYDIBOHF23SPDLT), creates an organizational unit in the root domain called Microsoft Exchange Security Groups with five groups, and prepares the root domain. The command to prepare all domains is `Setup /PrepareAllDomains`.

4. C. The root domain has to be prepared every time, no matter if Exchange-related objects or servers will be installed to it. Other domains that need to be prepared are those that will include Exchange Server 2007 or Exchange-related objects like mailboxes, groups, or contacts. Domains that include global catalog servers that are contacted by Exchange Server 2007 do not need to be prepared.

5. C, D. To run `/PrepareDomain` in a child domain you must be a Domain Admin if the domain existed during `/PrepareAD`; otherwise you need to be a Domain Admin as well as a member of the Exchange Organization Administrators group. As you can run this command from any server, you do not need to be an Administrator on the Exchange Server.

6. A, B. Only as an Exchange Organization Administrator or an Exchange Recipient Administrator can you manage Exchange-related objects throughout the Active Directory in any domain. The Exchange View-Only Administrator and the Exchange Server Administrator need extra permission on the domain, organizational unit, or object level before being able to manage them in Exchange.

7. D. Joel can only perform any server-related task. He cannot modify any global configuration, such as adding an address List, nor is he able to add or move any mailboxes to his Exchange servers, as he needs extra permissions on these mailboxes to do that.

8. A, B, C. You can delegate the Exchange Server Administrator role to any object that is globally Active Directory–available. Because a domain local group is available only in the domain where it exists, it cannot be used for delegation.

9. D. If you chose A, Andy would be an Exchange Server Administrator for an existing server but would not be able to install a new Exchange server to the organization. Answer B would provide him the permission to manage any recipient object (e.g., assign a mailbox to a user) as well as local Administrator permissions on the new server; he still would not have sufficient permissions to install an Exchange server. Option C does not exist as an Exchange setup syntax; thus will also fail.

10. A, B, D. In the site where you plan to install Exchange Server 2007 you must have a global catalog as well as a domain controller from the same domain where Exchange Server 2007 is installed. Also, all global catalog servers located in the same AD site as Exchange Server 2007 servers need to be upgraded to Windows Server 2003 Service Pack 1 or later. In order to increase performance, you can upgrade your domain controller to 64-bit machines, but this is not a requirement.

11. B. In a smaller location the best practice is to put all three roles (Hub Transport, Client Access, and Mailbox) required for a site on a single machine. This will preserve the budget but provide full functionality. Installing Exchange Server 2007 on a domain controller is generally not recommended, and buying three machines would not be good for the budget. The last option, using a single server and installing only the Exchange Mailbox role on it does not work because a Mailbox server always requires a Hub Transport and a Client Access role to be installed in the same AD site.

12. C. The first option is not correct as you cannot add other roles to a mailbox server that is clustered. The second option is valid, but provides high availability only for the mailbox store. If either the Client Access server or the Hub Transport server goes down, the complete location will not be able to send messages. Thus it is not a preferred option. The third option considers all aspects: the clustered Mailbox server as well as the Hub Transport and Client Access server roles installed on both machines, thus providing failover. Unified Messaging is part of the Client Access server, so that requirement is also satisfied. The last option does not provide sufficient availability for a large site.

13. A, C, D. Exchange Server 2007 requires TCP/IP v4 and does not support TCP/IP v6 yet. The DNS must be installed as the primary name-resolution method. All AD sites that host Exchange Servers must have a permanent WAN or LAN link between them—dial-up is not supported anymore in an Exchange Server 2007 organization.

14. A, C. Only call answering and voice access to mailbox are features of Unified Messaging. Sending faxes is not supported, but receiving faxes is. Delayed fan-out is not a feature of Unified Messaging, but rather a feature of Exchange Server 2007 routing.

15. A. In order to replace the existing smart relay servers, you should install the same number of stand-alone Edge Transport servers (important as they are located in an insecure network), and in order to receive organizational configuration from the Exchange organization, the servers must establish an Edge subscription each. Using the Hub Transport server for these tasks is not correct as this server role is not as secure for Internet-facing traffic as the Edge Transport server is. Joining an Edge server to a domain is also not secure!

16. A, B, C, E. The Exchange routing table consists of AD sites, AD site links, Exchange servers and their relation to AD sites, SMTP connectors, third-party connectors, mailbox and public folder stores, as well as legacy Exchange 2000/2003 routing groups and connectors. Client Access servers do not route any messages, and thus are not part of the routing table.

17. C. This question is about a routing feature called delayed fan-out. Basically, a message with multiple recipients is kept as one message until the routing path divides. In our situation this means that the message is kept as a single message until Site 2. There it will be divided, as Site 3 and 4 are directly connected to Site 2. The great benefit is bandwidth savings, especially considering that the message was 5 MB in size. Option A would be the most bandwidth-consuming one, so it is wrong. Option B would send a single message for each site, not considering the routing path; therefore it is also wrong. Option D considers sending a message from Site 1 to Site 2 and then to Site 3 and then to Site 4, which is not the way delayed fan-out is implemented in Exchange Server 2007.

18. C. This question is about an Exchange Server 2007 routing feature called queue at point of failure. If the Hub Transport server cannot make a direct connection to the target AD site, it will calculate the least-cost routing path for the message and go backwards. Thus the Hub Transport server will first try to connect to the target AD site named Site 4, then try Site 3, and if no Hub Transport is reachable there it would give Site 2 a try. As every Hub Transport server is capable of communicating with other AD sites, there would are no intra-AD site transfer of messages in Exchange Server 2007.

19. A, C, E. Exchange Server 2007 includes only three types of external connectors: a Send connector and a Receive connector that both support SMTP message transfer, and a Foreign connector that uses a Drop directory to send and receive messages from any foreign system, like a fax system. Old connectors like Lotus Notes Domino or X.400 connector are not available in Exchange Server 2007.

20. A, B, C, E. This is quite a complex scenario that includes an awful lot of information. The key here is to ask if the topics make sense during planning. This is true for option A, as it is always key to evaluate the network topology—especially the bandwidth—before considering a data center approach. Option B is obvious: you have to review the AD site design. Option C should test your skills regarding domain preparation in a multidomain environment, and is also true. Option D is wrong. You can also have a split-permissions model within a single forest; thus you do not need to plan for an extra forest implementation. Option E is important and valid, as it will optimize any routing that occurs in the Exchange organization. If you have firewalls between AD sites, you must configure a hub site so Exchange routing knows about it.