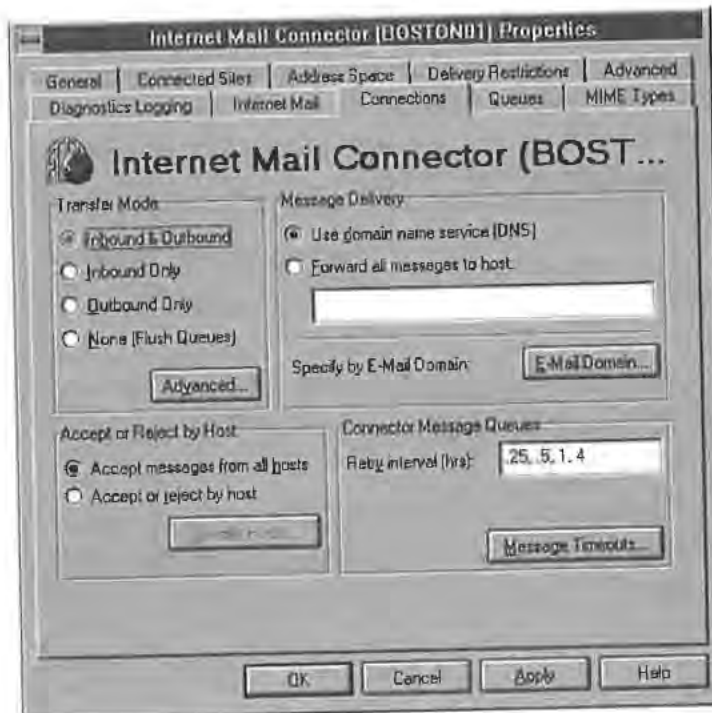


FIG. 3.13
Internet Connector
Connections Properties.



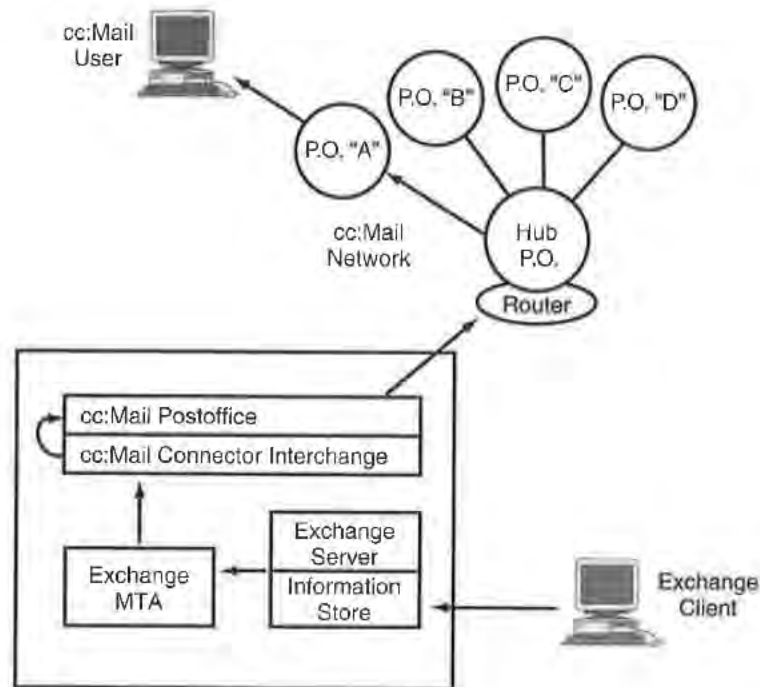
cc:Mail users are to be directly imported into the Microsoft Exchange Global Address Book and will appear just like any other Custom Recipient Exchange user.

Just as with the Microsoft Mail Connector, a cc:Mail post office is created on the Exchange server, resulting in Exchange server users appearing in the cc:Mail directory like all other cc:Mail users. This gives transparency to the cc:Mail user. As far as he or she is concerned, all users in the Global Address Book are local.

Exchange enables the administrator to set the paths to the standard Import and Export utilities that come with cc:Mail. These utilities are used to import and export directory and message data from the Exchange server to all other cc:Mail post offices in the cc:Mail network. Examples of the uses of this connector are shown in Figure 3.14.

On the cc:Mail side, Exchange looks just like any other post office; by using Automatic Directory Exchange (ADE), all cc:Mail post offices, including the Exchange cc:Mail post office, can be kept up to date as users are added on both sides. The following Figure 3.15 illustrates some of the components involved.

Microsoft realized that cc:Mail is a large player in the LAN-based messaging market. By making the cc:Mail Connector available, it has leveraged this popularity. In some organizations, many dollars have been spent on training personnel to install and maintain cc:Mail, as well as hardware resources. Using Exchange means that your organization will not have to throw away existing mail systems to roll out a new one.

FIG. 3.14Architecture of the
cc:Mail Connector.

Understanding Gateways

Gateways provide a way for Exchange to integrate disparate information services into Microsoft's Universal Inbox, using the single Exchange Viewer to organize all types of information. These include voice mail, fax, paging, as well as email from other vendors' systems.

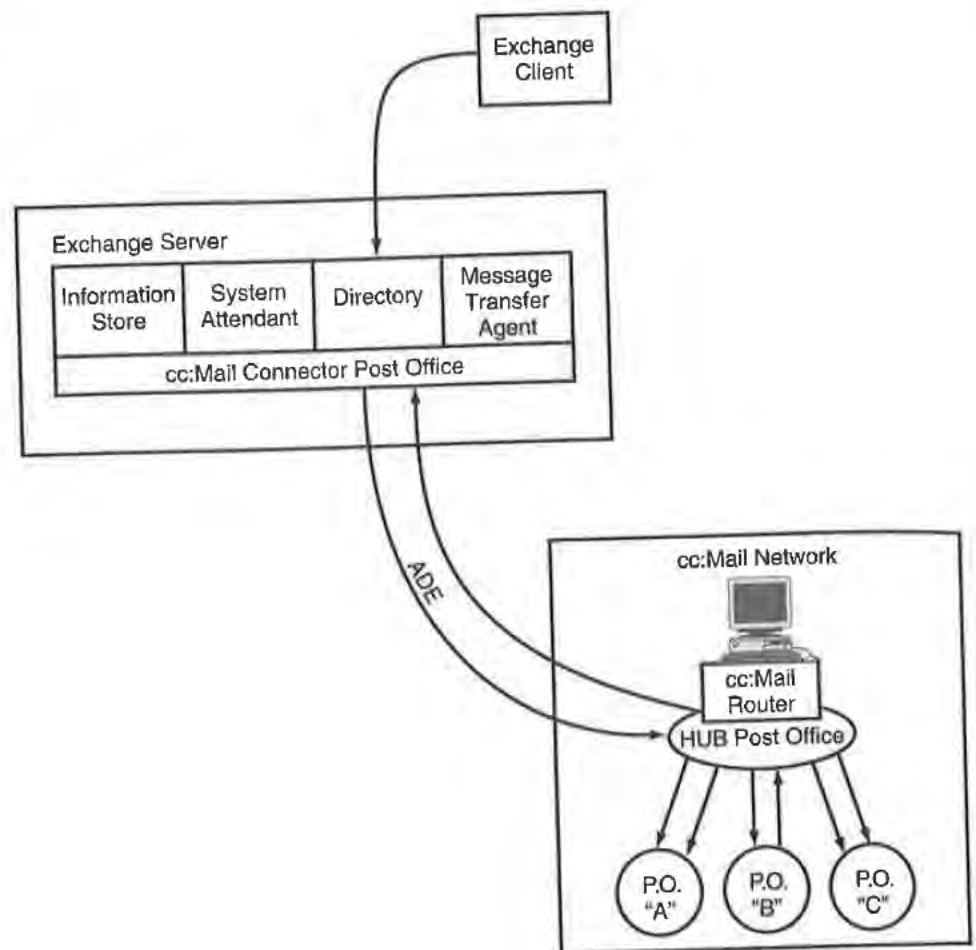
Despite the variety of information services that snap into Exchange, the end user sees no difference. To them, the addressee is the addressee. A user can address a message and send it, and the addressee might get a page, fax, voice mail, or Internet message. The addressee may be using cc:Mail, PROFS, SNADS, or Microsoft Mail, and the user sending the message would never know because all they need to know is the addressee's name in the Global Address Book.

Using Microsoft Mail Gateways

In addition to native Exchange gateways, Exchange can use standard Microsoft Mail 3.x gateways by using the Microsoft Mail Connector described earlier in this chapter. Each gateway uses the Microsoft Mail Connector to exchange data with foreign mail systems. This may be useful for sites with large Microsoft Mail installations that are slowly migrating to Exchange, but want to provide the core messaging functions first and add connectors and gateways later. In addition, some organizations are hesitant to sway from things that work. For example, if the Microsoft Mail gateway to PROFS has been working fine, some may be hesitant to roll out an Exchange PROFS connector or gateway because they haven't had the opportunity to test it and get their staff familiar with it. Figure 3.16 shows how Microsoft Mail gateways fit into the Exchange topology.

FIG. 3.15

ADE Synchronization
between the cc:Mail and
Exchange.



In the preceding case, the PROFS gateway for Microsoft Mail simply talks to the Microsoft Mail Connector post office. When configuring the PROFS gateway for Microsoft Mail, you simply point it at the Microsoft Mail Connector post office and the exchange of information becomes transparent.

With Exchange, Microsoft took those concerns into consideration and provided the flexibility to use legacy systems in the migration to a robust Exchange environment.

Connector for Lotus Notes

This is a new connector to Exchange 5.5. The Exchange Connector for Lotus Notes allows for the delivery of messages between Exchange and Lotus Notes to be transparent.

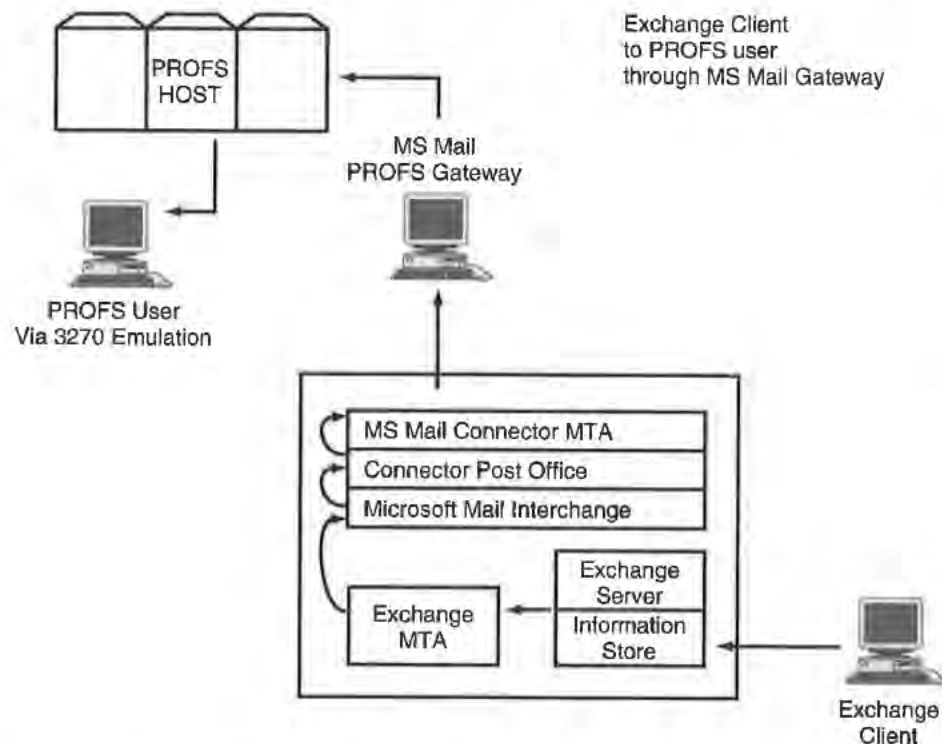
The Connector for Lotus Notes provides:

- The capacity for sharing rich text messages between Exchange and Lotus Notes users with very little loss of fidelity
- Support for Object Linking and Embedding (OLE)

- Support for Lotus Notes Document Links
- Support for the passing of file objects between the two systems with the attributes and the launch capability preserved
- Directory Synchronization between the two systems
- The ability to monitor and log the connector activity
- The Note Configuration Utility, this utility will automatically set permissions, create the database files required by the connector, and update several Lotus Notes settings

FIG. 3.16

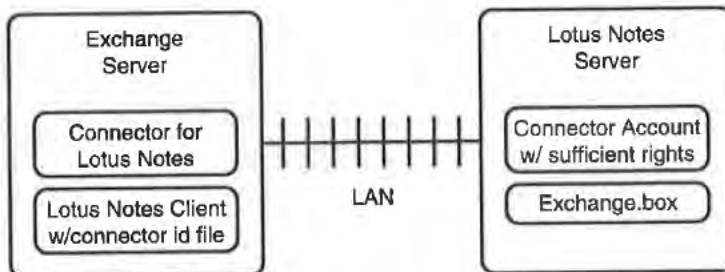
Message flow of Exchange to PROFS using PROFS Gateway for Microsoft Mail.



The Exchange Connector for Lotus Notes is used for message transfer and directory synchronization between Exchange and Lotus Notes. Multiple instances of the connector can be used, dependent upon your organizations messaging needs. Each Exchange server in your environment can run only one instance of the connector that directly services one connection to a Lotus Notes/Domino server. Also, a connection can only be configured to service one Lotus Notes/Domino server.

The Connector for Lotus Notes and the Lotus Notes Client are installed on the Exchange Server. On the Lotus Notes Server, a user needs to be created. This will create the connector ID file, which is used by the connector. These users need to be granted appropriate permissions to the Lotus Notes Public Address Book and Exchange.box. An example of this connector is shown in Figure 3.17.

FIG. 3.17
Exchange Connector for
Lotus Notes Architec-
ture.



Integrating with Microsoft Windows NT Server

In this chapter

Core Functionality of Windows NT 88

Understanding the Windows NT Domain Architecture 91

Understanding Exchange and Windows NT atin System Integration

Exchange Windows NT Dependencies 98

Exchange Server is part of the BackOffice suite of server products that runs on top of the Windows NT operating system. Windows NT is a powerful 32-bit multithreaded, multitasking operating system. The Exchange Server can leverage this functionality by utilizing as many threads or application processes as needed to provide a robust messaging infrastructure.

You should now have an understanding of the core components and framework for the Exchange server and client. This chapter helps you understand the way Exchange integrates with the operating system. We will also discuss how Exchange can leverage the Windows NT platform to provide a robust and fault-tolerant messaging solution.

Core Functionality of Windows NT

Windows NT is a 32-bit operating system. It provides multitasking and multithreading capabilities. This means that the operating system can simultaneously process multiple requests or instances of an application.

Windows NT is more than just an operating system. It is a framework to develop fault-tolerant client server applications. To enhance the operating system, Windows NT provides a full set of Application Programming Interfaces (APIs) and Software Development Kits (SDKs). The operating system is more than a file and print server; it is an application server. Through the use of the APIs and SDKs, many applications can harness the power of the operating system.

The operating system runs on a variety of platforms, including Intel and the Alpha platform. Although Exchange 5.0 also supported Power PC and MIPS platform, Microsoft offers only limited support. This portable operating system has several key benefits. The following sections cover the benefits in detail.

Supporting Multiple Protocols

Windows NT provides native support for the following protocols: TCP/IP, IPX, NetBEUI, AppleTalk, DLC, SNA, X.25, and X.400(TP/x). This enables the operating system to support a wide array of clients. Windows NT can communicate with UNIX, Banyan Vines, DEC Pathworks, NetWare, Apple Macintosh, and of course all of the Microsoft networking clients, including MS-DOS, Windows For Workgroups, Windows 95, and Windows NT Workstation.

This feature enables Windows NT to interoperate in a heterogeneous environment. You will not be "bound" by implementing the Windows NT operating system into one of these environments. Windows NT can offer additional functionality in these situations. The alternative is providing native support that would be very costly or impossible.

For example, Windows NT can be easily added to a Novell NetWare environment to provide Remote Networking or Dial-in access. The Windows NT operating system ships with a complete remote access server component integrated with the OS. With NetWare you would have to purchase an additional product known as NetWare Connect to obtain this capability.

With Exchange, NetWare clients can easily access an Exchange server running on Windows NT with native IPX client software installed. Clients communicate with industry standards

known as Remote Procedure Calls (RPC) by using the Exchange server. Windows NT supports every major communication protocol. Therefore, a client can connect to Exchange by using RPCs over TCP/IP or IPX in a NetWare environment.

In addition, Microsoft has released a standard for Remote Procedure Calls (RPCs) over AppleTalk, the Macintosh's native communications protocol. In order for a Macintosh workstation to connect to a Windows NT Exchange server, it can make RPCs over TCP/IP or AppleTalk. This functionality shows Microsoft's firm commitment to a Macintosh operating system and recognizes that the Macintosh operating system has an important share in the marketplace (see Figure 4.1).

FIG. 4.1
NT supports most industry-standard network protocols, as seen in this OSI model.

Support

APPLICATION	Server Message Block (SMB)		
SESSION	NetBIOS	Named Pipes	SMTP
TRANSPORT	NetBEUI	SPX	TCP
NETWORK		IPX	IP
DATA LINK	LAN Drivers		
	NDIS	ODI	Media Access Control
PHYSICAL	Network Card		

Using C2 Level Security

Security is a key element of any messaging system. Users want to know that their message will get to its destination without someone intercepting it. Exchange expands upon the Class C2 Level of Security, which is at the heart of the Windows NT operating system. The Department of Defense defines this level of security.

Class C2 requires a secure logon, discretionary access control, and full auditing capabilities. The secure logon requires that users identify themselves with a unique logon identifier (user ID) and password. This logon must be validated before accessing any system resources.

The discretionary access control enables the owner of a resource, whether it is a file, sub-directory, or printer, to determine who can access the resource. This also defines the level of control the user has over the resource. The owner grants rights to a user or group of users.

Auditing is the capability to log the security information of each operating system transaction to a file based on user ID. This feature provides the capability to detect and record important security-related events or instances in which security is challenged.

C2 security has several other components to its matrix of functionality. The Exchange server leverages its core features, however. Not all aspects of C2 security are required for use with Exchange. You also do not have to use every feature of C2 security when working on or creating a network application operating system. The company using the C2 security system can determine the level of security required.

Using Integrated Administrator Tools

Windows NT provides several tools to assist in managing the network as well as the operating system. Windows NT includes the Server Manager, the Event Viewer, and the User Manager to manage processes, define security privileges, provide auditing and security logging, and to create new users and groups, respectively.

The Server Manager enables the administrator to view all the servers from a single domain, multiple trusted domains across the enterprise, or individual servers and workstations inside a domain. The available functions enable you to control the share or access points to the file systems of a server, and to stop and start application processes. Using these functions, you can also close user sessions and manage specialized access via AppleTalk, NetWare Gateways, and the File Transfer Protocol (FTP).

The Event Viewer, also known as the Event Log, is the centralized repository for system, application, and security information for a server or workstation. From a remote console, an administrator can pull up the event viewer to see the entries of a network server. All BackOffice-certified applications must write the events to the event viewer. Events can be informational (blue), cautionary (yellow), and serious (red) in nature. You will be able to tell whether your tape backup has finished properly and at what time of day it completed. From the system, you will see whether there have been any problems related to the operating system and the hardware. From the security log, you can view all the information predetermined for auditing.

The event will store information related to the Exchange server and all its gateways, connectors, and external processes. It will also store security information. Exchange itself has a security log, which extends the basic functionality provided by the event log.

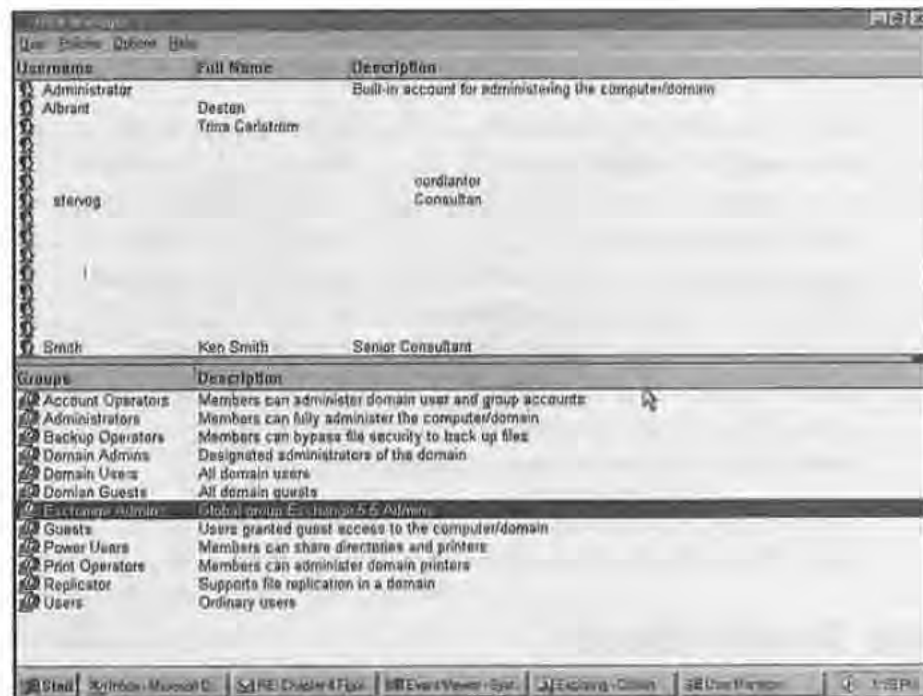
The User Manager is a tool used by the security administrators or domain administrators to create the single domain logon user ID. This ID includes all the user's application profiles, the group memberships profile, and time and workstation restrictions. The User Manager helps you define trust relationships among domains, define auditing functionality, and define general domain user account functions.

From the User Menu, you can select to create a new user, a local group, or a global group. The user ID is the individual ID used in conjunction with the password to be authenticated by the domain to access network resources. Local groups are those residing within the single domain in which they were created. If the domain is referred to as "Dallas," all local groups created in this domain will be able to access resources only within the domain. Global groups, however, can be used to provide access to trusted domains. A local group can contain local user IDs, as well as global groups from both the local and trusted domains.

Exchange adds the functionality of creating a mailbox for users at the same time as the creation of their domain user account (see Figure 4.2). This gives the mail, security, and domain administrators control over the same set of user accounts. In large organizations, this is the responsibility of a Network Security Group. This one group would be responsible for creating the user IDs, as well as the appropriate mailboxes.

FIG. 4.2

Windows NT User Manager enables you to create domain user IDs, including the Exchange mailbox.



Users	Full Name	Description
Administrator		Built-in account for administering the computer/domain
Albrant	Deaton	
	Tina Carlstrom	
stervog		Coordinator Consultant
Smith	Ken Smith	Senior Consultant

Groups	Description
Account Operators	Members can administer domain user and group accounts
Administrators	Members can fully administer the computer/domain
Backup Operators	Members can bypass file security to back up files
Domain Admins	Designated administrators of the domain
Domain Users	All domain users
Domain Guests	All domain guests
Exchange Admins	Global group Exchange 5.5 Admins
Guests	Users granted guest access to the computer/domain
Power Users	Members can share directories and printers
Print Operators	Members can administer domain printers
Replicator	Supports file replication in a domain
Users	Ordinary users

The functionality provided by these three tools is built into the Windows NT operating system. These tools can be run on remote machines, 16-bit workstations, and from the Internet.

Understanding the Windows NT Domain Architecture

At the heart of the Windows NT network operating system is the fundamental architecture of the domain model. A domain is a logical grouping of servers and workstations. One server in a

domain must be the Primary Domain Controller (PDC) and subsequently have Backup Domain Controllers (BDCs). Windows NT provides the capability to build servers as "name servers," which belong to the domain. These servers, however, are not responsible for replicating user account and security information throughout the domain. The PDC and BDCs remain synchronized by updating each other's user and security databases at regular intervals 24 hours a day, seven days a week.

The domain architecture consists initially of a single PDC of a single domain. From there, Windows NT architecture can grow in any number of combinations that can include multiple BDCs in a single domain or a number of trusted domains with BDCs and member servers.

Trust Relationships Among Multiple Domains

Trust relationships can be created between multiple domains. Trusts enable users from one domain to be granted secure access to resources in a second domain. This maintains the concept of the single network logon. Users will see no change from a single domain to multiple domains.

Two types of trusts exist: one-way and two-way. One-way trusts are set up to enable users from the second, or "trusted" domain, to access resources of the first or "trusting" domain. The second domain, however, has the freedom to create its user accounts and manage its own domain independently of the first domain. This can be illustrated by using a distributed administration model in which certain divisions have their own network administration; however, there is a central domain providing corporate-wide resources. The divisional domains can completely administer their own domains without affecting the central domain. The central domain has the capability to enable the divisional domain to access the central resources. This is useful because full administrator privileges can be given out at the divisional level without administrative rights over the entire WAN.

Two-way trusts grant access and administrative functionality among all domains that are in them. This is also known as the Complete Trust domain model (see Figure 4.3).

Single Domain Model

A domain is a logical grouping of servers that shares the same user accounts database and provides a single logon for all users to all the servers in the domain. As a comparison, on Novell version 3.x networks, each server maintains its own user account database or "bindery." In this way, user accounts must be individually created on each server.

The concept of a domain is primarily used for centralized administration. All the servers in a domain are updated with a single action. Regardless of when the user ID is created or modified, all the servers maintain the single logon for the group of servers in the domain.

A single domain consists only of a PDC. For small organizations, additional BDCs can be added to validate user access rights. A BDC is recommended if this system is in a production environment. This second Windows NT server will provide some fault tolerance. In the single domain, there are no trust relationships. Small organizations primarily use the single domain. These

Establishing trust relationships between domains enables one domain to access the resources of another.

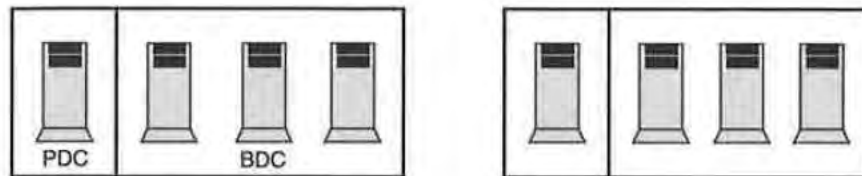
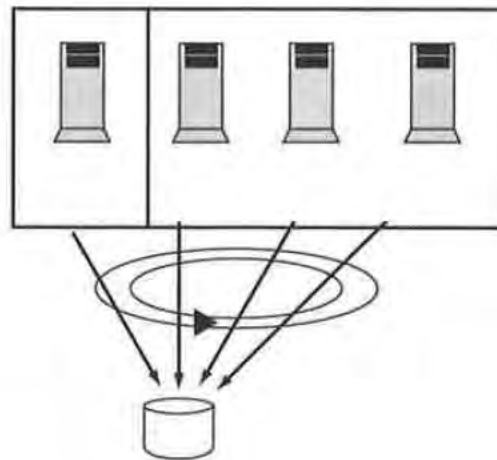


FIG. 4.4

The Single domain model represents the simplest form of a Microsoft Windows NT network.



M

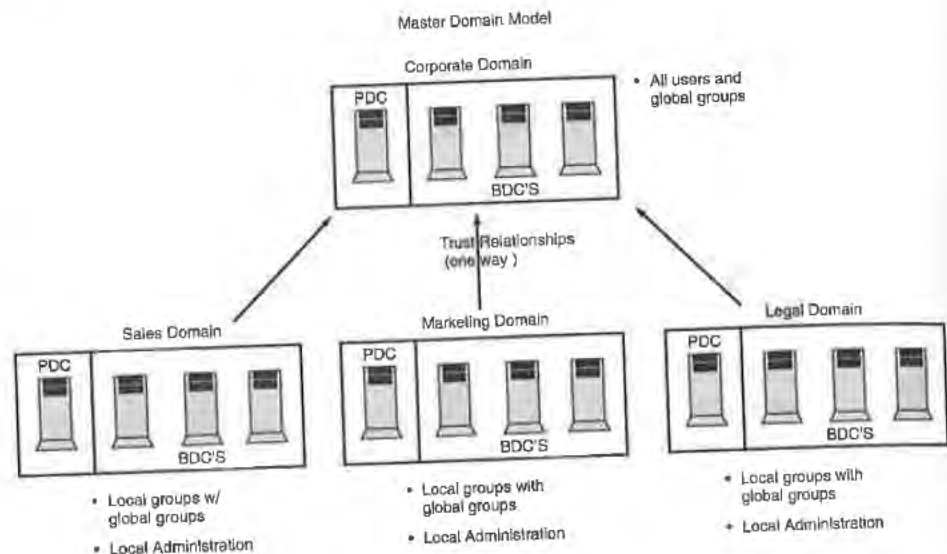
M

In a large organization, for example, the MIS Division manages from a central point. Therefore, the same should hold with the domain architecture. From one location, all users and security are maintained. The master domain referred to as "Corporate" houses all users and global groups. The resource domains, "Sales," "Marketing," and "Legal," only maintain local groups. When a resource is needed from the Sales domain, a local group is created in Sales, and its members include a global domain group from Corporate.

One disadvantage to this model is that performance might decrease as the number of users and groups grows. For this reason, larger domains need to consider the Multiple Master domain model (see Figure 4.5).

FIG. 4.5

The Master domain model puts global groups and users in the master domain. This model also places resources in separate domains.



Multiple Master Domain Model

The Multiple Master domain extends the Single Master domain into a broader scope. This domain model is typically seen in very large organizations. If your organization has two major corporate headquarters and many divisions, you might choose to implement the Multiple Master domain model.

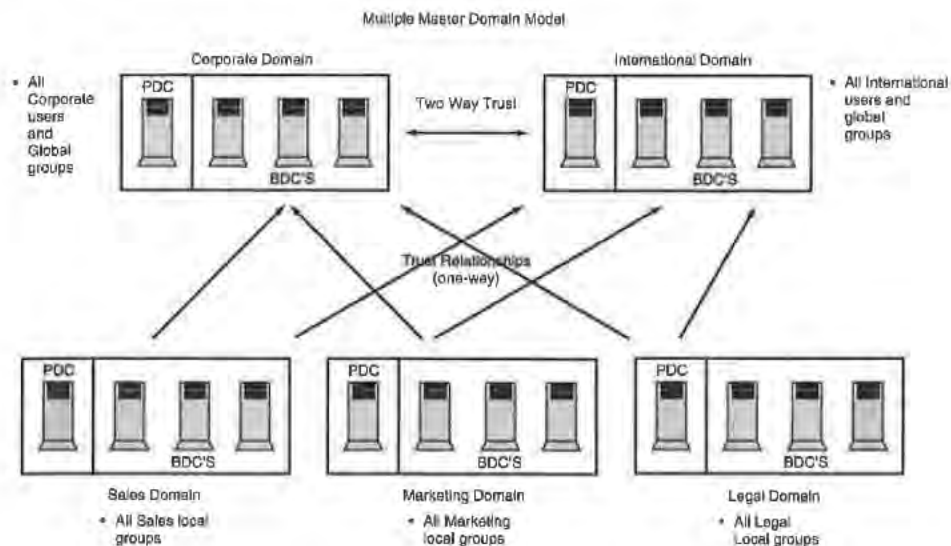
Building on the previous example, the Multiple Master domain model has two tiers of domains (see Figure 4.6). The first tier interconnects the master domains. "Corporate" and "International" are the two domains. These two domains each house their respective users and global groups. These domains are then configured with a two-way trust. These domains trust each other; therefore, only one copy of each user ID is needed.

The second tier of domains includes all the resource domains. These domains each maintain a one-way trust to the two Master domains. This model can be scaled to networks with any number of users. You can easily have upwards of 10,000 users supported with this model. The resource domains can then be grouped logically based on function and geographic location. The

resource domains also provide for local administration at the divisional level. The disadvantage to this model is that there are more trust relationships to manage. Also, not all user accounts are located in one domain.

FIG. 4.6

The Multiple Master domain model provides the scaling capability needed in a large organization when the master domain model is not sufficient.



Complete Trust Domain Model

The final option available for a Windows NT domain model is the Complete Trust domain. This model is best used in companies in which management of users and groups is distributed among different departments. Rather than being centralized, this model extends the administration down to the divisional level. Every domain trusts every other domain on the network. One immediate disadvantage to this model is that an administrator of one domain has full rights over every other domain in the model. This can lead to security problems. If you are going to use this model, an auditing process could help manage who has made administrative changes on the various domains.

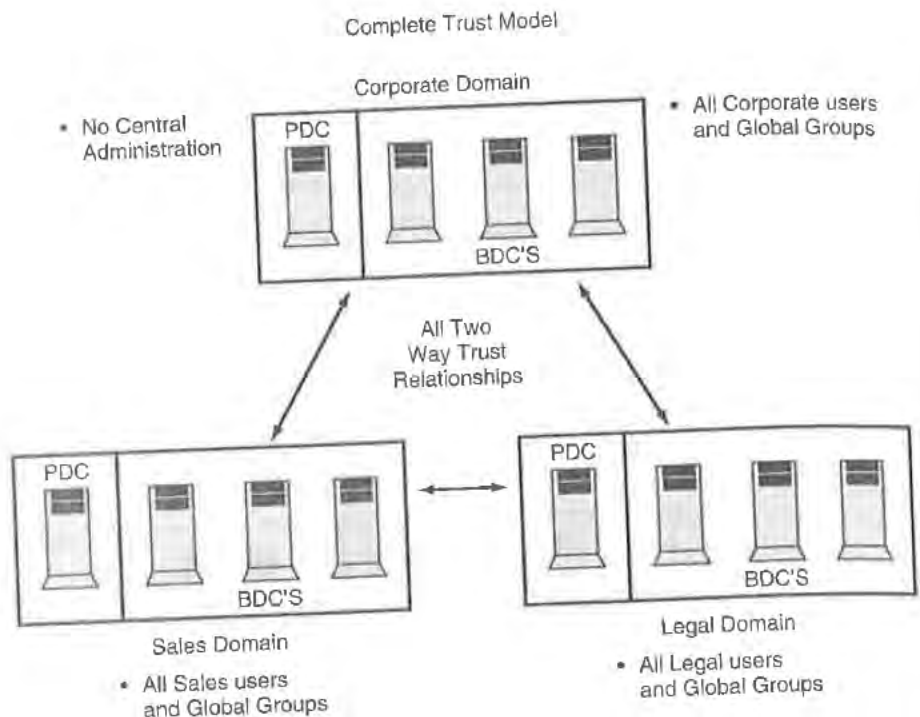
In this model, the resources and the user accounts are grouped into divisions (see Figure 4.7). Again, the only situation in which a Complete Trust is appropriate is when there is a lack of centralized management. This model is not practical for corporations with a large central department. The reason is that the model lacks the security needed for a large enterprise network.

Several options exist for a Windows NT domain model. In Chapter 5, "Designing Exchange Topology," you are given the criteria for selecting which domain architecture to use when planning to deploy Exchange in your environment.

Microsoft also provides a tool through its BBS and Internet site to assist with planning a domain architecture. This tool is referred to as the Domain Planner. It is a Visual Basic application that steps you through the options when choosing your domain and trust relationships.

FIG. 4.7

The Complete Trust domain model is intended for decentralized management and carries many security risks for an enterprise network.



Understanding Exchange and Windows NT Operating System Integration

This section explains how Exchange leverages the Windows NT operating system. Exchange has been created to exploit all the features of Windows NT Server, including all the tools. These tools include the single logon, permissions that can be user defined, the User Manager for Domains, the Event Viewer, and the Performance Monitor.

Comparing Windows NT and Exchange Terminology

Exchange runs on top of the Windows NT OS. However, it has hooks into the OS to provide a robust, high performance messaging system. Not all of the Windows NT terminology applies or directly converts to Exchange terminology. The reason is that the messaging platform has its own architecture.

Exchange uses the concepts of Organizations and Sites, whereas Windows NT uses domains. Organizations are at the top of the Exchange hierarchy. Typically, you find only one Organization name in the entire enterprise. Sites, on the other hand, can be geographic locations, divisions, or functional areas. Sites can also map one-to-one with domains.

Sites can span across multiple domains, provided that the domains are trusted. This is necessary because a server within a site must authenticate each user.

Both the Windows NT domain model and the Exchange architecture use the term "server." Within Windows NT, a server can be a PDC, a BDC, or a domain member server. Within

Exchange, servers exist within a site. It is not necessary for the Exchange server to be either the PDC or a BDC of a domain. For performance reasons, it would be best for the Exchange server to simply be a member server. This way, the Exchange servers share the resources of a domain without having to continually replicate security information or validate user access to the network.

Utilizing Integrated Features

Following is a list of Exchange's features that help the Exchange server to closely integrate with the Windows NT Server:

■ Exchange runs as a Windows NT service.

Exchange is a 32-bit application written to integrate with the Windows NT Server. Therefore, all the core components and optional connectors of Exchange run as services of the Windows NT OS. This means that they will run in the background and do not require a user to manually execute their application components. A service is an application that the operating system is aware of, and manages its execution. In addition, the service will log the activity of the process to the Application Event Viewer. From the performance monitor, you can verify the impact the process has on the operating system. From the Server Manager, you can stop and start the processes.

The 32-bit architecture of the executable enables Exchange to utilize the multithreaded, multitasking capabilities of the OS. Exchange runs in the background on the server. If a sudden burst of messages is passed to the Exchange server that needs to be forwarded, the executable can spawn more threads to effectively deal with the increased load.

This integration is only one way in which Exchange leverages the Windows NT operating system (see Figure 4.8).

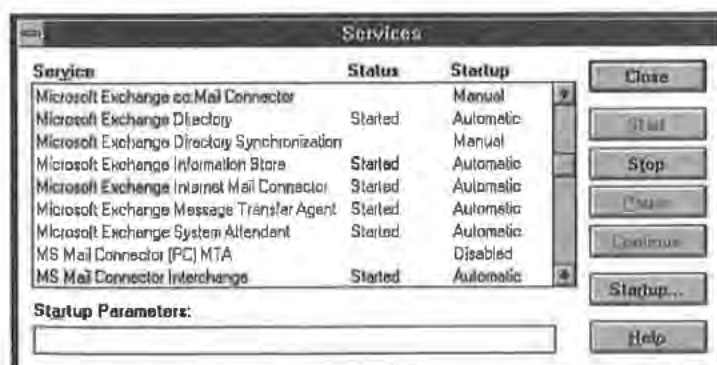
■ Additions to the User Manager for Domains.

Exchange adds functionality to the User Manager for Domains already discussed in this chapter. Exchange places an additional menu item with which you can administer user mailboxes from within the same consistent interface. Additionally, while you are creating users and assigning them group membership for Windows NT file access, a dialog box pops up to add the users' mailbox to Exchange. The user can be added to any Exchange server across the enterprise as long as the administrator has permission to do so.

Part
I
Ch
4

FIG.

The Windows NT Service Manager enables you to start, stop, and services, control properties.



■ Additions to the Performance Monitor.

Exchange extends the functionality of the Performance Monitor bundled within Windows NT. This extensive monitoring tool enables you to observe processor and disk space utilization, memory allocation, page faults, and over a thousand more counters.

Exchange adds some specific counters to the performance monitor, which enable the administrator to view statistics of critical elements of the Exchange processes. These include the number of open tables on the message store, cache hits, I/O performance on reads and writes, RPC packets per second, number of bytes sent and received, and more.

Exchange Windows NT Dependencies

Exchange relies on the Windows NT operating system for certain functionality. The major function is that you must create a user account in the operating system for Exchange to run its services. Exchange also can import and export names from the Windows NT domain user database. This facilitates a quick migration to Exchange from your existing Windows NT Network architecture.

Exchange relies on the connectivity that Windows NT provides. Exchange enables all types of clients to connect to its servers. Novell NetWare clients, Macintosh, UNIX, and all the Windows clients can connect to Exchange using their native protocols. This is made possible through Windows NT's use of RPCs and multiple protocol support.

For remote access solutions, Exchange again relies on the Windows NT OS. Windows NT has an integrated remote access server as part of the operating system. The Windows NT server running Exchange can be configured for a user to dial directly into the server and access Exchange, as well as any other network resources. For performance reasons, it might be more appropriate to set up the remote access server on a dedicated server.

For WAN connections, Windows NT supports X.25 and ISDN without any additional software. An Exchange server can be configured to use an X.25 or ISDN connection to bridge the message route. If WAN links are already in place, these dial-up solutions provide a second level of fault tolerance, and an additional message route in an emergency.

System Service Account

The system service account enables Exchange servers to authenticate one another when transferring messages, updating the global address list, or performing directory synchronization. This account must be created with certain specifications.

It is important to carefully plan the implementation of this account. You must have a domain model that supports these user accounts. Whether you have a trusted or untrusted domain, you must ensure that the Exchange services can be authenticated between servers. If this does not occur, mail will not be forwarded from one system to another.

Security Models

Exchange relies on the C2 level security of the operating system. Any user who attempts to access the system must first be authenticated by the domain. Exchange extends the single logon ID. Therefore, the domain logon also validates users for accessing the Exchange mailbox. As mentioned previously, in the file-sharing mail systems, users had full access to the file system that comprised the post office. Exchange now manages the access to the post office based on the central domain user database.

Exchange itself provides three levels of security. The user accounts are leveraged from the Windows NT user database. From within the Exchange Administrator Program, a user account can be specified as a complete administrator, a local administrator, or a read-only administrator.

There are many issues related to using Exchange on the Windows NT operating system. Windows NT provides connectivity to almost any other operating system used in the enterprise. Windows NT should not be a point of concern when deploying Exchange. The Windows NT OS interoperates more easily with your existing network operating systems and mail environments than some proprietary systems that communicate with themselves (this is the case with PROFS or OfficeVision). Exchange leverages the Windows NT OS to provide a strong messaging backbone. ●

Part

I

Ch

4

Mailbox Names

A mailbox name should be easy to identify and similar in form to your organization's internal phone lists. Because Exchange's address book lists mailbox names, you may want to create mailbox names that sort properly when they display. Review Table 5.8 for a breakdown of mailbox names.

Table 5.8 Guidelines and Restrictions for Mailbox Names

Field	Guideline	Restrictions
First Name	User's first name	Up to 16 characters; can be changed.
Last Name	User's last name	Up to 40 characters; can be changed.
Alias Name	To route messages to non-Exchange systems, an alias name is used. Identify the external mail systems within your organization, such as PROFS, MHS, MCI Mail, AT&T Mail, and determine their unique requirements, such as PROFS can accept up to eight characters for an email address. For best results, the alias name should bear a recognizable resemblance to the original name—Kent Joshi becomes KJOSHI.	Up to 64 characters; can be changed
Display Name	Base this name on how you want to display it in the Address book and Administrator window. Be sure to consistently use the same format for all names, such as Last Name, First Name.	Up to 256 characters; can be changed.
Directory Name	Exchange uses this name to route mail messages. This is an internal name and is not displayed to users or administrators. Exchange sets this to the first alias name specified, but you can use another.	Up to 64 characters; must be unique; can't be changed.

Email Addresses

When Exchange communicates with other (or foreign) mail systems, such as the Internet, Exchange must have a valid address format the other mail system understands. A foreign messaging system user whose address exists both on a foreign mail network as well as in the Exchange directory is referred to as a custom recipient. Exchange recipients (including mailboxes, custom recipients, distribution lists, and public folders) that have addresses on foreign mail systems are known as foreign email addresses.

Exchange automatically generates an email address for the following mail systems: X.500, X.400, Microsoft Mail (PC), and the Internet (SMTP). Exchange does this to provide the widest possible compatibility with other messaging systems. Keep in mind that other addresses may be generated if you have installed a PROFS or another third-party gateway.

X.500 Addresses

X.500 was designed to provide an international standard for enterprise-wide directory service access. The 1988 X.500 directory service guidelines form the basis of Exchange's directory service. Exchange stores in the directory all X.500 object classes in an X.500 schema.

The directory objects are organized in a hierarchical structure known as the Directory Information Tree (DIT), and they are identified by a unique item called a distinguished name (see example later in this chapter).

Table 5.9 shows how the X.500 object name maps to an Exchange object.

Table 5.9 Mapping X.500 Names to Exchange Objects

X.500 Name	Attribute	Exchange Server Object
Country	c=	Country
Organization	o=	Organization
Organizational Unit	ou=	Site Name
Common Name Container	cn=	Exchange Server Recipient
Common Name	cn=	Exchange Server Recipient or directory name

For example, the distinguished name for Kent Joshi, who has a mailbox in Los Angeles within the Software Spectrum organization, is o=SWS/ou=LosAngeles/cn=recipients/cn=KJOSHI. When you remove the naming labels, you receive the form that Exchange uses: SWS/LosAngeles/recipients/KJOSHI.

Because X.500 doesn't support all object classes and attributes, Exchange also includes support for titles, organization charting information (who reports to whom in an organization), additional phone numbers, arbitrary attributes created by the administrator, and alternate recipients.

X.400 Addresses X.400 is a widely recognized and accepted international standard by the messaging industry. Exchange's compliance with the X.400 standard is important for organizations that want to use email with heterogeneous mail systems, as well as those who want to communicate with external companies via public carriers.

X.400 addresses can contain all the uppercase and lowercase letters, all numbers (0–9), a space, left and right parentheses, the plus and equal signs, the comma and the period, the hyphen and the forward slash or solidus (/), and the colon and question mark. In addition, X.400 addresses can contain the following attributes, which are listed in hierarchical order in Table 5.10.

Table 5.10 X.400 Attributes

Description	Attribute
Country	c=
Administrative Management Domain (ADMD)	a=
Private Management Domain (PRMD) (Exchange organization)	p=
Organization (Exchange server site)	o=
Organizational units	ou1=;ou2=; ou3=; and ou4=;
Common name	cn=
Generation qualifier	q=
Initials	i=
Surname (last name)	s=
Given name (first name)	g=

For example, the following is a valid X.400 address for Kent Joshi, who has a mailbox in Los Angeles within the Software Spectrum organization:

```
g=Kent;s=Joshi;o=Los-Angeles;p=SWS;a=mci;c=us;
```

This address also represents the minimum information you need to receive email from someone else.

Microsoft Mail Addresses If you connect to Microsoft Mail for PC Networks or Microsoft Mail for AppleTalk Networks systems, character restrictions are as follows:

Microsoft Mail network name	10
Post office name	8
Mailbox name	8

A valid Microsoft Mail address for Kent Joshi, who has a mailbox in Los Angeles within the Software Spectrum organization, is SWS/LSANGLES/KJOSHI. For more information on connecting to Microsoft Mail, please see Chapter 7, "Planning Connections to Microsoft Mail Systems." For information on migration from Microsoft Mail to Exchange, please see Chapter 8, "Migrating from Microsoft Mail Systems."

SMTP Addresses Exchange's SMTP connector is a dependable way to exchange mail transparently with SMTP users as well as with Mail users on other LANs over an SMTP backbone. SMTP also enables Mail users to easily access mail networks such as UUCP, BITNET, and Internet.

When communicating with the Internet or other SMTP systems, look at their particular character or addressing limitations. In general, SMTP addresses can include all uppercase and lowercase letters (A-Z), all numbers (0-9), and the hyphen (-). However, spaces are not permitted.

A valid SMTP address for Kent Joshi, who has a mailbox in Los Angeles within the Software Spectrum organization, is KJOSHI@LOS-ANGELES.SWS.COM.

External System Addresses If your organization has other mail systems (PROFS, SNADS, and so on), you want to examine any conditions they place on usable characters and addressing. This way you can properly configure the Alias Name field (see the section "Mailbox Names" earlier in this chapter) for your particular mail system.

Step 7 Linking Your Sites

Now that you have your sites laid out and the proper email address to share information, the next question is: How do I link my sites? This step explains the methods you can use to link your sites and discusses the pros and cons of different connectors and how this affects the Exchange Server.

Site Connector

The site connector is the most efficient way to connect two sites if they are on the same logical LAN. It also offers the greatest performance because it uses RPC for communication.

Listed in the Table 5.11 are the pros and cons when using the site connector.

Table 5.11 Pros and Cons of Using the Site Connector

Pros	Cons
Provides automatic load tolerance.	Requires a permanent, highbalancing and fault bandwidth connection of at least 56Kbps or higher (class B or C link).
Easiest site connection option to configure and manage because a site network transport isn't involved.	Transmits more frequently than other connection options. If you are charged for network traffic, such as frame relay or packets, you may want to examine another site connection option.
Messages don't need to be translated between sites.	Cannot control message size.
Configures both sides of the connection at the same time.	Cannot schedule connections.
Messages take fewer hops to reach their destinations.	Can overwhelm network links when multiple Exchange servers use the same link.

RAS Connector

The RAS connector is useful where no permanent LAN or WAN connection exists, but you can link up to another site remotely. This is usually the case with small branch offices where permanent links are expensive or not available.

You can also use the RAS Connector to provide a redundant connection for sites using one of the other site connection options. For example, you can configure the RAS connector to handle message routing in cases where the primary connector link becomes unavailable.

Table 5.12 reveals the pros and cons when using the RAS connector.

Table 5.12 Pros and Cons of Using the RAS Connector

Pros	Cons
You can schedule connections	Transfer is limited by speed of modem.
Can link sites over an asynchronous, periodic connection.	Link saturation is more likely because all site message traffic is flowing through one dial-up link.

X.400 Connector

The X.400 connector is useful where you are connecting to other sites via slow network links or on private or public packet networks. In addition, the X.400 connector provides compatibility with 1984, 1988, and future MTAs. This means you can communicate via X.400 with companies that are at different stages of implementing X.400 technology.

Exchange Server supports X.400 over the following OSI transports: TP0/X.25, TP4/(CLNP), and TP0/RFC 1006 to TCP/IP. After configuring to a transport, Exchange routes the message with standard X.400 messaging protocols.

Table 5.13 reveals the pros and cons when using the X.400 connector.

Table 5.13 Pros and Cons of Using the X.400 Connector

Pros	Cons
Connects to foreign, non-Exchange	Must configure network transports, systems that support X.400 standard.
You can schedule connections.	Bottlenecks may appear because all mail traffic flows through one central server.
Can determine messaging infrastructure topology.	Must verify that the existing routing through Exchange's network (bridges, routers) can support the required protocols.
You can control message size.	

Internet Mail Service

Although the Internet Mail Service can link two sites, the main purpose is to connect to the Internet using the SMTP (Simple Mail Transfer Protocol). You can also link most UNIX systems and any mail systems supporting plain text-RFC 822, MIME (Multipurpose Internet Mail Extensions)-RFC 1521, Microsoft Mail server format, or Uuencode/Uudecode standards.

Table 5.14 lists the benefits and drawbacks when using the Internet Mail Service.

Table 5.14 Pros and Cons of Using the Internet Mail Service

Pros	Cons
Can forward all mail to a single host.	Must configure a network transport (TCP/IP).
Can configure service to accept or reject host connections.	You cannot schedule connections.
Can configure service to receive inbound or outbound messages or both.	

Microsoft Mail Connector

The Microsoft Mail Connector provides seamless connectivity to Microsoft Mail for PC Networks, Microsoft Mail for AppleTalk Networks, and Microsoft Mail for PC Networks gateways (PROFS, SNADS, Netware, MHS, and FAX). It uses a "shadow" post office that is structured like a Microsoft Mail 3.x post office.

The Microsoft Mail Connector runs over the following transports: TCP/IP, IPX/SPX, NetBEUI, X.25, Asynchronous, and Remote Access Service (RAS).

Table 5.15 lists the benefits and drawbacks when using the Microsoft Mail Connector.

Table 5.15 Pros and Cons of Using the Microsoft Mail Connector

Pros	Cons
Can connect directly to another Microsoft Mail post office, which enables you to replace it without additional software.	In most cases, you must configure a network transport.
Enables you to migrate your Microsoft Mail network in phases instead of all at once.	Must verify that the existing network infrastructure (bridges, routers) can support the required protocols.

Lotus cc:Mail Connector

The Exchange Connector for Lotus cc:Mail enables you to tightly integrate Exchange into existing cc:Mail environments. After you install the server, Exchange Server and cc:Mail terms can exchange messages and synchronize directories. The cc:Mail Connector supports both DB6 and DB8 cc:Mail post offices. Like the Microsoft Mail connector, you can take a phased approach to migration that causes minimal disruption in an organization.

Table 5.16 lists the benefits and drawbacks when using the Lotus cc:Mail connector.

Table 5.16 Pros and Cons of Using the Lotus cc:Mail Connector

Pros	Cons
Can connect directly to another cc:Mail post office, which enables you to replace it without additional software.	In most cases, you must configure a network transport.
Enables you to migrate from network in non-disruptive phases instead of all at once.	Must verify that the existing cc:Mail network infrastructure (bridges, routers) can support the required protocols.

Lotus Notes Connector

The Exchange Connector for Lotus Notes enables you to tightly integrate Exchange into existing Lotus Notes mail environments. After you install the server, Exchange Server and Notes systems can exchange messages and synchronize directories. Like the Microsoft Mail connector, you can take a phased approach to migration that causes minimal disruption among your user population.

Table 5.17 lists the benefits and drawbacks when using the Lotus Notes connector.

Table 5.17 Pros and Cons of Using the Lotus Notes Connector

Pros	Cons
Can connect directly to another Notes server, which enables you to replace it without additional software.	In most cases, you must configure a network transport.
Enables you to migrate from Notes system in non-disruptive phases instead of all at once.	Must verify that the existing network infrastructure (bridges, routers) can support the required protocols.
Can schedule connections	

Step 8 Planning Your Public Folder Infrastructure

This step provides a high-level introduction to Exchange Public Folders, an approach to the selection of tools for building information sharing solutions, and finally, an approach that organizations of any size can take to develop a public folder infrastructure for collaborative solutions.

Every organization has documentation on procedures and processes, forms for services, bulletins, business processes, and other information that needs to be available to the organization employees or specific workgroups. To aid in the collaborative use, distribution, and sharing of this information, a number of different solutions have been developed and widely implemented. These solutions primarily fall into two categories: the Intranet and Groupware.

The Intranet has quickly become a popular mechanism through which to make information easily available to users through relatively low bandwidth connections. The browser has become a ubiquitous component of the corporate and home computer. As this technology matures and addresses some of the security issues with which it is still struggling, the browser will solidify its position as a mechanism for business transactions.

Groupware enables employees to communicate, collaborate, and share information through memos and files so that they all work more effectively. Exchange provides a messaging environment along with structured tools that enable group collaboration in different ways. The main tool Exchange provides for this is Public Folders.

Introduction to Public Folders

Public folders are repositories for information that different users can share and different types of clients can access. Public folders can contain many different types of information, from simple messages to complex multimedia clips. Public folders can also contain custom forms for contributing and reviewing information and rules, and views for finding and organizing information. Public folders provide an environment for all kinds of custom applications, such as bulletin boards, discussion forums, customer tracking systems, and workflow applications. Public folders reside in the public information store (MDBDATA\PUB.EDB) on an Exchange Server computer. You can replicate (copy) individual public folders, if you desire, to one or more additional Exchange Server computers. When a change is made in a public folder, the change copies on a scheduled basis to every replica of the folder that exists throughout the Exchange Server organization. This replication is based on a multi-master architecture. This implies that a change on any instance of the public folder immediately replicates throughout the hierarchy.

Public folders are an important part of Exchange. They provide flexibility by using a variety of forms, views, access rights, and structures. You can also use public folders to replace or complement distribution lists, reducing storage requirements and network traffic. More importantly, instead of just reducing network traffic and hard disk requirements, public folders can hold important background information on projects, customers or other business-related activities. Some of the ways in which public folders can be leveraged to improve business processes include the following:

- People joining a virtual project team or a process in-progress can read items from the recent past and catch up on events.
- You can create a custom form and install it in a folder for employees to record information of any activities, telephone calls, or information related to customers. When a customer calls into a call center, the customer representatives can quickly review up-to-date customer-related information and provide more responsive and improved customer service.
- A help desk can maintain a folder of commonly asked questions and answers.
- You can put month-end reports into public folders for executives to track progress on projects and people.

Note that you can create, design, and view public folders only with an Exchange client. Use the Exchange Administrator program to configure public folder replication and a variety of other administrative options. In summary, folders are as follows:

- Organization-wide public information repositories
- Contain many different types of information
- Contain standard forms, custom forms, rules, and views
- Can be replicated throughout the Exchange organization as well as to users local hard drive

- Serve as the foundation for enterprise and/or departmental-wide groupware and workflow collaborative solutions

Selecting Tools for Information Sharing Solutions

As an organization plans for the implementation of managed information sharing solutions, you must realize that an effective and successful collaborative system contains elements from several different environments and technologies in order to adequately both the business and end-user needs.

In recent years, another popular solution to disseminate information has emerged from what was the core set of Internet technologies. The intranet (Intra-organizational network) leverages the same software as existing Internet access applications. The software—coupled with the broad availability and distribution of the browser interface—led to its popularity.

When comparing the intranet to Exchange public folders, organizations must recognize that each solution has its strengths and weaknesses. Exchange is effective at enabling users to communicate and capture their discussions into public folders. Exchange also provides a secure repository where users can submit, update or delete documents they have provided for internal consumption. Additionally, Exchange provides power users the tools with which to develop and deploy electronic forms for general use. These grassroots efforts can form the foundation for more complex workflow forms-based applications. The strengths of the World Wide Web include its ability to integrate multimedia components such as audio, video, or images, into a web page. Additionally, you can enhance the web pages by adding additional information from virtually any source through the use of hyperlinks. Unfortunately, using an intranet may present some significant challenges including security, limited document management solutions, and a limited set of standard third-party tools for integration and other administrative tasks.

When deciding which information sharing technology is best for a particular application, you must consider the following two key factors:

- The nature of the data driving the application
- The nature of the user interface (GUI) in which the data is presented

Traditional client/server applications are effective in scenarios where both the data and the user interface are well-structured. The client/server applications tend to struggle when either the data or the GUI are unstructured. In the cases where the data is unstructured, Exchange provides a good solution. In contrast, the web's unstructured interface is a good fit when the data needs is structured, such as when you publish relatively static information.

In summary, you must analyze and define the user requirements in regards to the source and nature of the information that the application uses and the nature of the GUI that best meets the user needs. After you define these two items, you can select the right technical solution or develop a hybrid solution to meet your users' needs in the most effective and efficient manner. Finally, it is recommended that you develop your organization's intranet and Exchange public folder infrastructures in conjunction—with the objective that they compliment each other.

Microsoft Exchange Connector for cc:Mail enables administrators to seamlessly integrate Exchange Server and cc:Mail systems, allowing them to exchange messages and synchronize directory entries from both DB6 and DB8 environments. Customers have the flexibility to use a phased approach to migration that minimizes disruptions within an organization.

The migration process of moving users from one messaging system to another can include mailboxes and attachments, addresses, and scheduling information from your existing system. This chapter covers planning methods for interoperability and migrating users to Exchange Server. Exchange's robust migration features support multiple scenarios for interconnecting to cc:Mail. Tools like Migration Wizard greatly simplify migration and ensure a smooth transition to Exchange.

Understanding the Architecture

The minimal software version required for the Exchange cc:Mail connector with cc:Mail is Lotus cc:Mail DB6, Post Office Database version 6.0, cc:Mail Import version 5.15, and Export version 5.14. Support for cc:Mail DB8 requires Lotus cc:Mail Post Office Database version 8 and cc:Mail Import/Export version 6.0.

Connecting Exchange to Lotus cc:Mail

The Exchange Connector for Lotus cc:Mail enables administrators to integrate Exchange into cc:Mail environments. Once installed, Exchange Server and cc:Mail systems can exchange messages and synchronize directories with both DB6 and DB8 cc:Mail post offices. When you introduce Exchange Server into a cc:Mail environment, cc:Mail users will benefit from Exchange Server's strong connectivity to the Internet and other systems. Also, customers can take a phased approach to migration that will minimize disruption with an organization.

The cc:Mail connector has a lot to offer in addition to fast performance: It also can transfer messages, attachments, embedded messages, OLE attachments, and file links. The connector does not support all of the linking features in the Exchange client. An Exchange Server system enables users to embed objects into the message body, link objects to the message body, insert links to files, insert shortcuts to Exchange folders, and insert shortcuts to Internet sites.

The cc:Mail connector really enhances connectivity because you can connect cc:Mail systems to Exchange Servers and immediately take advantage of Exchange's Internet Mail Service, which provides significant performance benefits over Lotus' SMTP gateway along with MIME compatibility. You can also use any other Exchange Connector (such as Microsoft Mail) through the cc:Mail connector.

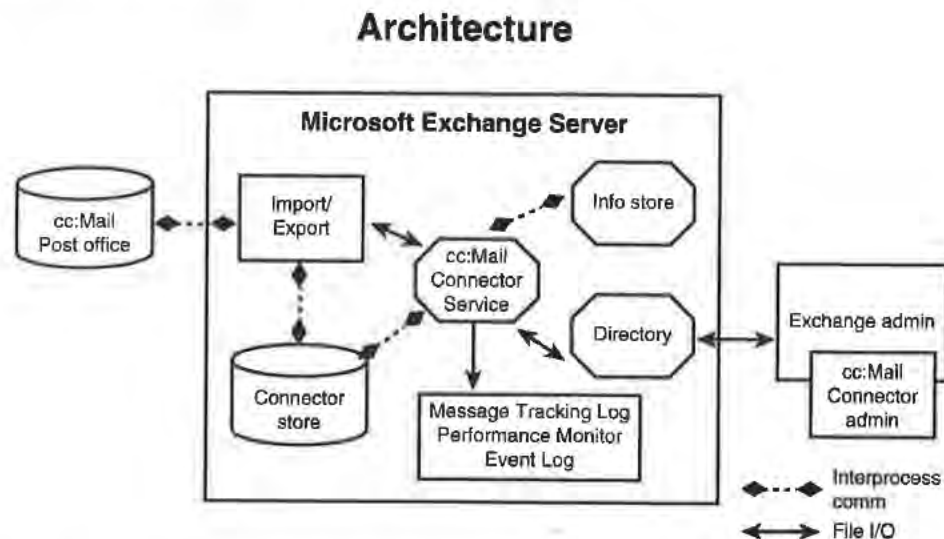
Understanding How the Connector Works

Microsoft Exchange Server uses two components to communicate with cc:Mail systems: the cc:Mail connector and the cc:Mail Import and Export programs. The connector for cc:Mail is a Windows NT Service that executes Import and Export to transfer messages between Exchange Server and cc:Mail. It also synchronizes some or all of the Exchange Global Address List (GAL) with the cc:Mail directory.

When a message is submitted to the Exchange Server message transfer agent (MTA), the MTA consults the directory service (DS) to determine where the message should be moved. In the case of cc:Mail addresses, the messages are moved to the cc:Mail connector. The connector for cc:Mail service receives the messages, converts them to ASCII file format, converts attachments as needed, and places the messages in the connector store. If the Import program can't deliver the message, a non-delivery report (NDR) is sent back to the sender. See Figure 9.1 for an overview of the components of the cc:Mail connector.

FIG. 9.1

Architectural layout of the cc:Mail connector.



Directory synchronization in cc:Mail is a scheduled or on-demand process that performs a full synchronization of the cc:Mail directory on the connected post office with the Exchange directory. This process, like message transfer, uses the Import and Export programs provided by cc:Mail and controlled by the connector service.

From cc:Mail to Exchange, the service spawns the export process against the connected post office, which places the resulting address information file into the connector store. This file is then retrieved by the cc:Mail connector service and processed into an import container specified during the setup of the connector. The import container can be any Exchange recipient's container, including the Global Address List.

From Exchange to cc:Mail, the service spawns the import process. In order for this to succeed, there must be data to import. The cc:Mail connector service retrieves Exchange recipient information from the directory service and places that information in a file in the connector store. These addresses are then imported into the cc:Mail post office.

Figure 9.2 shows a screen shot of the connector for cc:Mail and the information required to connect to a post office. The configuration and setup for message transfer requires only a post office name, UNC path, and password. Unlike in the cc:Mail MTA, extensive drilling down in multiple screens isn't necessary to establish routing. Directory synchronization requires only basic configuration steps in which you choose what you want to export and what you want to import.

FIG. 9.2

Information required for the connection to a cc:Mail post office.



Using Multiple Connectors to cc:Mail

Directory synchronization is flexible and easy to configure, and it allows you to synchronize cc:Mail mailing lists and bulletin boards, as well as all types of Exchange recipients. You may elect to synchronize specific entries or types of entries between the two systems.

The Exchange cc:Mail connector fully integrates with Windows NT. Performance Monitor counters exhibit transfer rates, queue sizes, nondelivery occurrences, and directory synchronization events. Events are logged to Windows NT Event Log in several different categories. Read receipt and nondeliverable reports are generated for both systems to use link monitors in testing connectivity between your downstream post offices.

If you have many cc:Mail post offices within your organization or multiple cc:Mail post offices spread over a large area, you can set up multiple connectors to link all cc:Mail and Exchange Servers. From the cc:Mail perspective, each Exchange Server site appears to be one large cc:Mail post office, regardless of the number of servers or recipients in that site.

When planning multiple outgoing routes to one or more connectors to cc:Mail, consider doing these things:

- Install a connector on any or all Exchange Server computers in your site, depending on your messaging traffic.
- Use identical address information in the Address Space properties sheets of two or more cc:Mail connectors to route messages.
- Install at least one Exchange Server 5.0 in every site that indirectly communicates with cc:Mail. Exchange 5.0 is required for cc:Mail address generation of Exchange Server recipients.

Lotus cc:Mail address generation enables cc:Mail users to send mail to Exchange users. (The Exchange Server users must have an address of the type CCMAIL.) Exchange Server automatically generates a cc:Mail address (*Username at siteproxy*) for each recipient, a public folder, a distribution list, and a custom recipient based on the site addressing. This enables cc:Mail users to send mail to any Exchange user. The administrator configures the cc:Mail e-mail address format in the Site Addressing properties sheet for the site.

Using the Migration Wizard

Once your Exchange Server and Lotus cc:Mail systems are connected, it is easy to enable them to coexist or to migrate from cc:Mail to Exchange. The cc:Mail component of the Migration Wizard enables you to upgrade custom recipients to mailboxes and retain former cc:Mail addresses so that old mail on both systems will be redirected to the new Exchange mailbox. The Migration Wizard also copies cc:Mail files to the recipient's Exchange mailbox and copies BBSs (bulletin boards) to Exchange public folders.

The Migration Wizard can create new Windows NT accounts, and you can choose from three methods how you want the Windows NT accounts for migrated users created (accounts can be created and given a random password). With the first method, you create Windows NT accounts for each mailbox and generate random passwords. The account name and passwords are written to the file ACCOUNT.PASSWORD in the working directory of the Migration wizard. The second method is to create accounts and use the Windows NT account alias as the password. The final option is to not create Windows NT accounts that match the alias of a mailbox but instead to create the mailbox without an associated Windows NT account. This means that no one will be able to access these mailboxes until a Windows NT account is associated with them.

Figure 9.3 shows the options the wizard offers for creating Windows NT accounts during migration.

Creating Addresses in Your Host System

If you don't have a directory synchronization requestor for your host system, then you need to handle the following:

- Export the mailbox and foreign system addresses from Microsoft Exchange Server with directory export.
- Change the format of the file.
- Import the addresses into your host system.
- Extract Custom Recipients from PROFS.

Mail sent in Microsoft Exchange Server computers and incoming mail from Microsoft Exchange Server gateways can be routed to the PROFS addresses. You can use this rather than using directory synchronization, but you have to repeat the process on a regular basis to update the Microsoft Exchange Server directory with changes in the existing system directory.

Creating the REMADDR File To create custom recipients, extract a file of IBM PROFS addresses. Move the file to the Microsoft Exchange Server computer. Import the IBM PROFS address file into Microsoft Exchange Server with the Migration Wizard to create custom recipients. To do this, complete the following steps:

NOTE The custom recipient information is created with PROFS target addresses. If mail sent from Microsoft Exchange Server mailboxes is routed through X.400 or SMTP to reach the PROFS host, you must modify the custom recipient data before importing it to have the proper address type and address.

1. On the computer where you installed the source extractor, log on as the MIGRATOR VM ID.
2. Type **MIGWIZRD** and press Enter to start the source extractor. The screen displays the following code:

```
Source Extractor for IBM (R) PROFS (R) and OfficeVision (TM)
Microsoft Exchange Server Migration Wizard
```

The following parameters are specified in MIGPARMS DATA file.

You can change these parameters using this menu, or by using XEDIT.

```
OV/VM (PROFS) Nickname File: File name:           File type:
Accounts File:              File name:           File type:
PROFS Calendar MIGRATOR vmid (PROFS system only)
Notify VM id                : HOWARDS
File Transfer VM id         : MIGXFER
Thread timeout (min)        : 30
Spool Console required      (TRUE/FALSE) : FALSE
Number of migration threads : 05
Replace previously migrated accounts (TRUE/FALSE) : TRUE
```

<< BACK	NEXT >>	FINISH	CANCEL	HELP
F10/F22	F11/F23	F12/F24	F3/F15	F1/F13

3. (Optional) In the OV/VM (PROFS) Nickname File field, type the name and file type of the nickname file. If this field is not filled in, the source extractor uses OFSUAD FILE, if access to this file is available.
4. (Optional) In the Accounts File field, type the name and file type of the accounts file with a list of VM IDs for which you want to create custom recipients. If you plan to create custom recipients for all VM IDs, skip this step.
Anywhere from one to all VM IDs can be specified in an account file. The account file has one VM ID on each line.
5. In the Notify VM ID field, type the VM ID to which alert messages are sent. This VM ID doesn't need to have administrator privileges.
6. In the File Transfer VM ID field, type the VM ID to which all the extractor data should be written.

7. Press the F11 key to continue. The screen displays the following:

```
Source Extractor for IBM (R) PROFS (R) and OfficeVision (TM)
Microsoft Exchange Server Migration Wizard
```

What information would you like to migrate?

Type Y to select option, or N to reject it.

```
Y Remote addresses creation information (REMADDR FILE)
N Mailbox creation information (MAILBOX FILE)
N Email messages (Notelogs and In-basket)
  From: 1994/10/28 to 1995/10/28
N Schedule information (Calendars and Reminders)
  From: 1995/10/28 to 1996/10/28
N Documents from OFSINDEX FILE
  From: 1994/10/28 to 1995/10/28
N Personal Address Book (Nicknames and Distribution lists)
```

<< BACK	NEXT >>	FINISH	CANCEL	HELP
F10/F22	F11/F23	F12/F24	F3/F15	F1/F13

8. Set the Remote Addresses Creation Information to Y. Set all other options to N.
9. To continue, press the F11 key. The screen displays the remote address file.
10. Edit the remote address file as needed to remove VM IDs for which you don't want Microsoft Exchange Server custom recipients, or to change the display names. The source extractor uses XEDIT as the editor, and all XEDIT commands and subcommands are available.

11. Press F12 to complete the process.

This procedure creates REMADDR FILE on the MIGRATOR 191 minidisk and sends REMADDR PRI and REMADDR PKL to the reader of the file transfer VM ID. The REMADDR PRI and REMADDR PKL files are in ASCII format.

Moving the REMADDR Address to the Microsoft Exchange Server To move the REMADDR address to the Microsoft Exchange Server, take these steps:

1. Log on as the MIGXFER VM ID.
2. Type **MIGXFER** and press Enter to start the transfer tool.
3. The transfer tool modifies the file named REMADDR FILE to the migration file format and transfers it from the reader to the minidisk. The MIGXFER EXEC also creates MIGXFER BAT, MIGRATOR PKL, and MIGPURGE EXEC on the minidisk.
4. Download the MIGXFER BAT file to the personal computer.
5. From the personal computer, type the following to transfer the REMADDR FILE and packing list file to the personal computer as REMADDR.PRI and MIGRATOR.PKL:
`MIGXFER <path to your terminal emulation software>`
6. On the host, type **MIGPURGE** to remove the files from the reader.
7. (Optional) Edit the REMADDR PRI file to remove addresses, modify display names, change the target address type, or add additional directory import fields and data. For example, if you want all the custom recipients to have telephone number data, you can add the field Telephone-Office1 to the end of the first line in the directory section, and then add telephone numbers to the end of each line of data.

The migration files now can be imported into Microsoft Exchange Server with the Migration Wizard. See the section, "Importing Migration Files," later in the chapter for the next step.

Creating Mailboxes

The procedure for creating mailboxes is exactly the same as for creating custom recipients except that, in step 8 of the extracting process, set Mailbox Creation Information to Y. A MAILBOX file is created in place of the REMADDR file.

Migrating Data The process of migrating data creates secondary files, and autologs onto the VM IDs that are being migrated. The VM IDs to migrate cannot be in use during the extracting process.

Extracting E-Mail Data To extract e-mail data, take the following steps:

1. Log on as the MIGRATOR VM ID.
2. Type **MIGWIZRD** and press Enter to start the source extractor. The screen displays the following information:

Source Extractor for IBM (R) PROFS (R) and OfficeVision (TM)
Microsoft Exchange Server Migration Wizard

The following parameters are specified in MIGPARMS DATA file.

You can change these parameters using this menu, or by using XEDIT.

```
OV/VM (PROFS) Nickname File: File name:      File type:
Accounts File:                File name:      File type:
PROFS Calendar MIGRATOR vmid (PROFS system only) :
Notify VM id                  : HOWARDS
File Transfer VM id           : MIGXFER
Thread timeout (min)          : 30
Spool Console required        (TRUE/FALSE) : FALSE
Number of migration threads   : 05
Replace previously migrated accounts (TRUE/FALSE) : TRUE
```

```
<< BACK      NEXT >>      FINISH      CANCEL      HELP
F10/F22      F11/F23      F12/F24      F3/F15      F1/F13
```

3. (Optional) In the OV/VM (PROFS) Nickname File field, type the name and file type of the nickname file. If this field is not filled in, the extractor uses OFSUAD FILE.

TIP

If you are migrating only a few accounts, create an accounts or nickname file with these accounts in it and set the appropriate field to point at the file.

4. (Optional) In the Accounts File field, type the name and file type of the accounts file with a list of VM IDs for which you want to create custom recipients.
5. (Optional) If you are migrating calendars from a PROFS system, enter the corresponding VM ID in the PROFS Calendar MIGRATOR VM ID field. Ignore this step if you are migrating calendars from OfficeVision.
6. In the Notify VM ID field, type the VM ID to which error messages are sent. This VM ID doesn't need to have administrator privileges.
7. In the File Transfer VM ID field, type the VM ID to which all the extractor data should be written.
8. In the Thread Timeout field, type the maximum number of minutes it should take to migrate each VM ID. When this time runs out, the MIGWIZRD EXEC reuses the thread.
9. In the Spool Console Required field, set the value to TRUE to send console updates to the MIGRATOR VM ID to monitor progress.
Alternatively, set the value to FALSE so that the console updates are not sent.
10. In the Number of Migration Threads, set the number of VM IDs that will be migrated simultaneously. If you set this number too high, it can affect performance and resources on the host computer.
11. In the Replace Previously Migrated Accounts field, set the value to TRUE if you want to migrate data for VM IDs that previously were migrated.

Alternatively, set the value to FALSE if you do not want to migrate previously migrated VM IDs.

12. Press the F11 key to continue. The screen displays the following information:

Source Extractor for IBM (R) PROFS (R) and OfficeVision (TM)
Microsoft Exchange Server Migration Wizard

What information would you like to migrate?

Type Y to select option, or N to reject it.

N Remote addresses creation information (REMADDR FILE)
N Mailbox creation information (MAILBOX FILE)
Y Email messages (Notelogs and In-basket)
From: 1994/10/28 to 1995/10/28
Y Schedule information (Calendars and Reminders)
From: 1995/10/28 to 1996/10/28
Y Documents from OFSINDEX FILE
From: 1994/10/28 to 1995/10/28
Y Personal Address Book (Nicknames and Distribution lists)

<< BACK	NEXT >>	FINISH	CANCEL	HELP
F10/F22	F11/F23	F12/F24	F3/F15	F1/F13

13. Set the options to Y or N, based on the information you need to migrate. Also, update the date range for each type of information that is being migrated.

CAUTION

The date range doesn't update dynamically. To avoid not migrating recent items, set the To dates to a future date, in case you forget to update them.

14. Press F11 to continue. The screen displays the accounts file.
15. Edit the accounts file as needed to remove VM IDs that you do not want to migrate. The status field can have the following three possible values:
- Init**—Not migrated yet but will be migrated.
 - Timeout**—Attempted to migrate VM ID, but reached the timeout limit before migration was finished. Will be migrated.
 - Done**—Exported data from this VM ID in the past. Will be migrated only if Replace Previous Migrated Accounts field is set to TRUE.
16. (Optional) If you didn't create a small nickname file or accounts file with your list of VM IDs to be migrated, pare down the full list of users to only the ones you want to migrate.

17. Press F12 to start extracting data. The screen displays the following information:

```
Source Extractor for IBM (R) PROFS (R) and OfficeVision (TM)
Migrating mailbox information...
Migrating users...
Max_threads=05. Replace=1
N_input=63
AUTO SUFINE EXEC MIGRATE MIGRATOR READ
AUTO STGRAY EXEC MIGRATE MIGRATOR READ
```

RUNNING MSVM7

18. When the MIGWIZRD EXEC is finished, type **SHUT** to end the program.

This process creates several items in the reader of the file transfer VM ID, depending on the options selected in the second screen, which are described in the following table:

Item Name	Description
MAILBOX FILE	Information to create mailboxes
<VM ID> PKL	Packing list for the migration files of the VM ID
<VM ID> PRI	Primary intermediate file for the migration files of the VM ID
<VM ID> SEC	Secondary intermediate file for the migration files of the VM ID

These files are stored in ASCII format and should not be edited. For each VM ID there can be multiple primary intermediate files.

Migrating Files to Microsoft Exchange Server To move the migration files to Microsoft Exchange Server, follow these steps:

1. Log on as the MIGXFER VM ID.
2. Type **MIGXFER** and press Enter to start the transfer tool. The screen displays the following information:

```
Source Extractor for IBM (R) PROFS (R) and OfficeVision (TM)
```

```
There are 180 K bytes available on A disk.
```

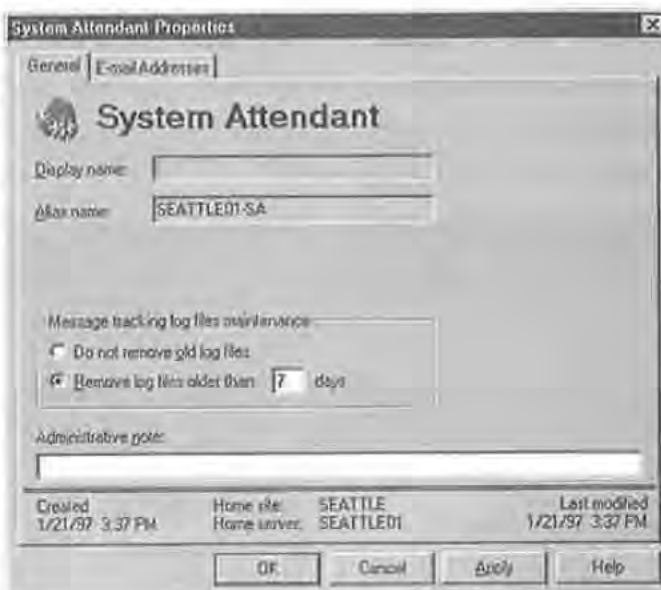
```
Total size of selected files is 1892 K.
```

```
Select a subset of files that can be transferred by editing this file.
```

```
User ID          File Size
00000 * * * Top of File * * *
00001 REMADDR          6080
00002 MAILBOX          4960
00003 EAST03           1328
00004 EAST02          36628
00005 EAST01          10064
00006 CENT01          98776
00007 CENT02         309728
00008 CENT03         282512
```

FIG. 13.27

The System Attendant General property page.

**CAUTION**

Opting to keep old log files on a server with a high volume of message traffic could easily take up many megabytes of storage space. If you do select Do not remove old log files, make sure to keep track of log file sizes!

6. Enter any additional information (such as reasons for keeping all old log files) in the Administrative note box provided.
7. Click Apply to set these properties and continue with other properties. If you are done with all settings, click OK to return to the Administrator program.

Setting E-Mail Addresses for the System Attendant

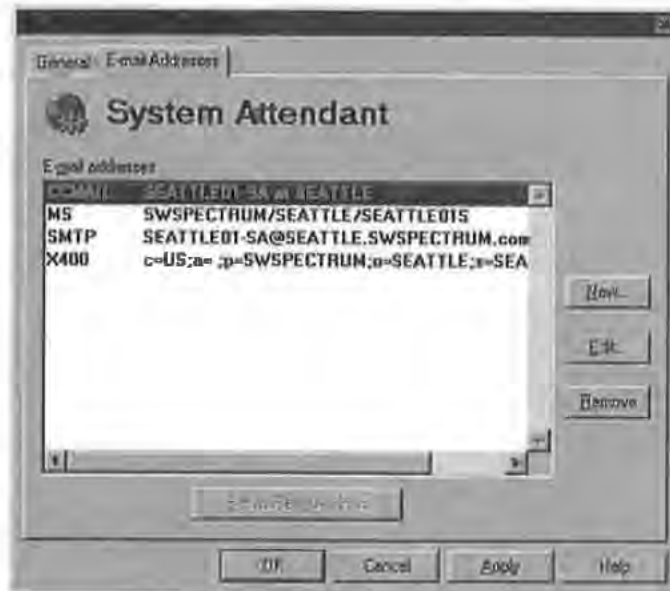
E-mail addresses are used by the various Exchange gateways and connectors to identify specific directory objects to other messaging systems. The System Attendant, though not capable of receiving messages, is a directory object just the same and has a set of e-mail addresses associated with it. There are four default addresses created each for cc:Mail, Microsoft Mail Post Office, SMTP, and X.400.

Complete the following steps to add, modify, or remove e-mail addresses from the System Attendant:

1. Click the E-mail Addresses of the System Attendant Properties page (see Figure 13.28). The four default addresses (cc:Mail, Microsoft Mail Post Office, SMTP, and X.400) are displayed.

FIG. 13.28

The E-mail addresses page displays the four default addresses for this System Attendant.



2. Click **N**ew to add a specific e-mail address for this system attendant. Select an existing address and click **E**dit to modify it, or click **R**emove to delete it.
3. Click **A**pply to set these properties and continue with other properties. If you are done with all settings, click **O**K to return to the Administrator program.

All other functions of the System Attendant (such as checking directory replication inconsistencies and gathering information about other running Exchange services) are carried out without additional configuration by the administrator.

Configuring Address Book Views

The Address Book Views pages enable you to restrict what entries users are able to see in the Global Address List (GAL). This feature also allows users to create and see address book views sorted by various mailbox characteristics. You can create new Address Book Views in Exchange 5.5 by selecting **F**ile, **N**ew Other, **A**ddress **B**ook View from the toolbar in the Exchange Administrator program.

The pages that will be covered are as follows:

- The General page
- The Group By page
- The Permissions page
- The Advanced property page

The General Page

Use the General page to specify a Display name and Directory name for your Address Book View.

Go through the following steps to change the Display name and/or the Directory name of your address book view:

1. Select the General tab of your new Address Book View property pages. You will then see a screen similar to Figure 13.29.

FIG. 13.29

Setting the Display Name and the Directory Name from the General page.



2. Enter a Display name for this object as you want it to be displayed in the Exchange Administrator program.
3. Enter a Directory name for this object. Once you apply your changes, you will be unable to change this directory name.
4. Enter an administrative note that pertains to this object if desired.
5. Click Apply to set these properties and continue with other properties. If you are finished setting options, click OK to return to the Administrator program.

The Group By Page

This page defines how the recipient objects in the Address Book view are grouped (see Figure 13.30).

To group recipient objects with specific attributes that appear in the Group items by box on the Group By page, complete the following steps:

1. Click on the Group By page of the Address Book View property pages.
2. Use the drop-down menu for Group items by to select an attribute you want to use to group items.
3. Use the pull-down menu for Then by to select additional attributes you want to group items.

- FIG. 13.30

The screenshot shows the 'Technology Dept. Properties' dialog box with the 'Security' tab selected. The 'Group or users to' list contains 'Users'. The 'Permissions' section shows 'Deny' selected for 'Full Control'. The 'Permissions' list is empty. The 'Permissions' section also includes 'Full Control' and 'Full Control' with 'Allow' and 'Deny' buttons. The 'Permissions' section also includes 'Full Control' and 'Full Control' with 'Allow' and 'Deny' buttons. The 'Permissions' section also includes 'Full Control' and 'Full Control' with 'Allow' and 'Deny' buttons.

The Permissions property page allows you to specify the rights users will have to view the Address Book (see Figure 13.31).

1. Click on the Permissions page of the Address Book View property pages.
2. The Windows NT accounts with inherited permissions is a read-only list box that displays all Windows NT accounts with inherited rights for this object.
3. Click the **Add** button to add Windows NT accounts and groups to the list of accounts and groups with permissions for this object.
4. The **Remove** button removes the currently selected Windows NT account or group from the list of accounts and groups with permissions for this object.
5. Use the Roles drop-down menu to assign a role to the currently selected Windows NT account or group. Roles are sets of rights that define how much or what type of access a user or group has to an object. You can define custom roles or use the default roles that come with Microsoft Exchange. For example, you can assign an account or group to the search role from this tab. The search role will restrict users or groups from viewing any other Address Book view other than the one in which they have this search role.
6. Click **Apply** to set these properties and continue with other properties. If you are finished setting options, click **OK** to return to the Administrator program.

Message Transfer Configuration

In this chapter

- Understanding the Transfer Agent Components **302**
- Performing MTA Site Configuration **303**
- Configuring Local MTA Properties **308**

The Microsoft Exchange Message Transfer Agent (MTA) is the key component that provides addressing, routing, and message delivery. Proper configuration of MTA settings is important to an efficient Exchange organization. As described in Chapter 3, "Exchange's Integrated Server Components," a message that originates in an Exchange mailbox reaches its destination in only two ways. The first is when a message is addressed to a user on the same Exchange server and is delivered by the information store. The second is when a message is addressed to a user on a different server or foreign system, and the MTA handles the message transfer.

Understanding the Transfer Agent Components

The Microsoft Exchange Message Transfer Agent is a Windows NT service running on each Exchange server in your organization. For connection to Microsoft Mail systems, an additional service called the Microsoft Mail Connector (PC) MTA negotiates message transfer with Microsoft Mail networks.

Configuration of the Exchange MTA is handled through two sets of properties sheets:

- *MTA Site Configuration*. Defines overall settings for message transmission within the entire Exchange site.
- *Message Transfer Agent (for a specific Exchange server)*. Defines server-specific MTA settings, such as message size limits and logging levels.

Some of the essential parameters involved in performing MTA site configurations are listed here:

Message Tracking. To keep records of Message Transfer Agent activity within a Microsoft Exchange site and enable message tracking. A daily log file is generated and stored in the EXCHSRVR\TRACKING.LOG directory. Message tracking log files are in a text format. The full file name, to use an example, might be EXCHSRVR\TRACKING\970122.LOG. The individual log files are named using this format: YYYYMMDD.log. For example, a log file for MTA activity on Jan 22, 1997 would have the name 970122.log.

Message Queues. Each server has a list of messages that are waiting to be delivered by its MTA. The queues are distinguished as being either Private or Public information store messages. Messages are held in the queue until the MTA can successfully transfer the messages by establishing a connection with the remote MTA or until the messages exceed their lifetimes (as set in the messaging defaults).

Messaging Defaults. Settings for how (and how long) to transfer a message before certain timeouts occurs are called messaging defaults. These values are set in the MTA Site Configuration properties and are used by all MTAs in the site unless a specific connection uses MTA override parameters.

MTA Overrides. Certain connectors (specifically, the dynamic RAS connector and the X.400 connector) provide for object-specific MTA settings. Use the Override property to change the default Microsoft Exchange Server MTA attributes when using a specific X.400 or dynamic RAS connector. Remember their existence when you define messaging defaults in the MTA Site Configuration properties sheet. The Override property is for developing flexibility in MTA configuration.

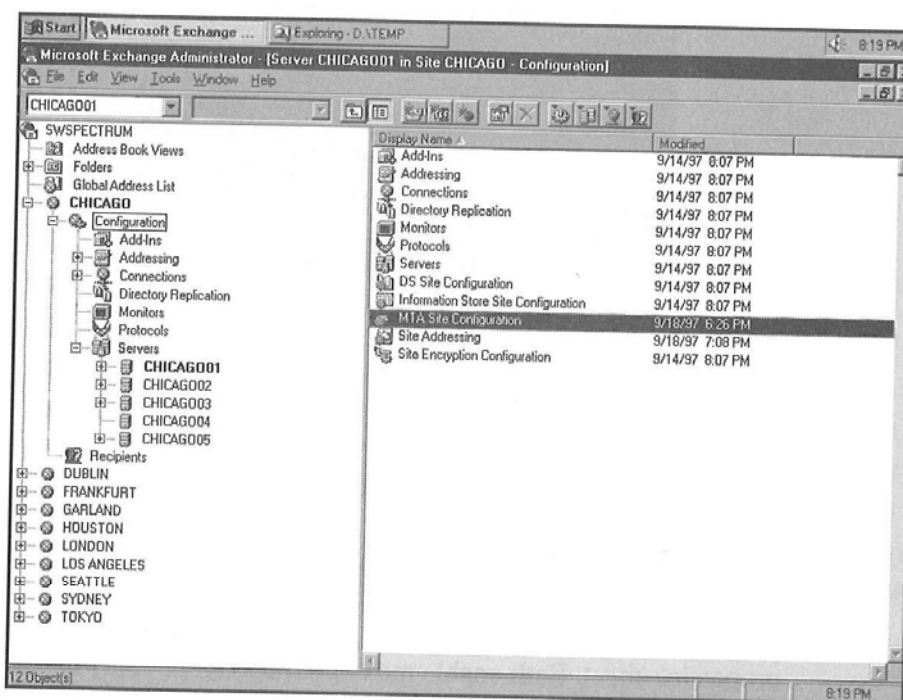
Performing MTA Site Configuration

To open the MTA Site Configuration properties sheet, follow these steps:

1. Navigate to your desired site with the Exchange Administrator program, and then expand the site container.
2. Highlight the Configuration container of the selected site (see Figure 14.1). All the site configuration objects appear in the right pane of the Administrator program's window.

FIG. 14.1

The MTA Site Configuration is located in the Configuration container.



3. Select the MTA Site Configuration object from the list.
 4. Open the MTA Site Configuration Object properties sheet by double-clicking the object.
- At this point, you have three property pages to configure:

- *General.* Sets the MTA site configuration display name and the dead-letter recipient, and enables message tracking.

- *Permissions*. Sets security rights to the MTA Site Configuration object.
- *Messaging Defaults*. Defines connection and transmission parameters for the MTAs in your site.

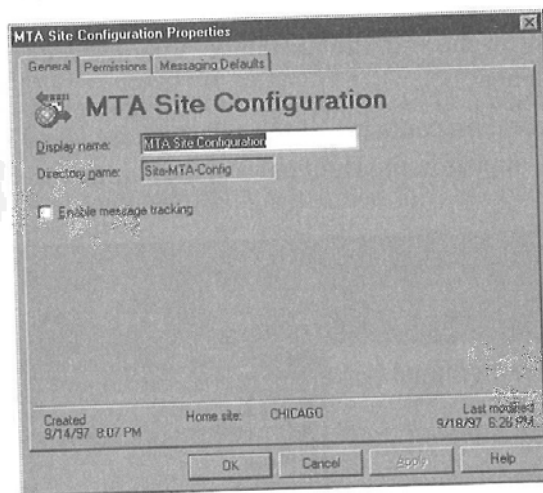
The General Tab

To configure the General features, such as the display name of the MTA Site Configuration Object, follow these steps:

1. Click the General tab of the MTA Site Configuration properties sheet (see Figure 14.2).

FIG. 14.2

The General page of the MTA Site Configuration properties sheet.



2. Type a new name in the Display Name box, if you want. The default name is MTA Site Configuration.

NOTE By default, the directory name is Site-MTA-Config, and it cannot be changed. This is the unique object name that the site MTA has assigned. ■

3. Click the Enable Message Tracking check box to instruct the System Attendant to keep a daily log of all messages processed by the MTA. This check box corresponds to the "Enable Message Tracking" check box in the Information Store Site Configuration properties sheet. Both enable message tracking, but only for their respective services.
4. Click Apply to set these properties and continue viewing and changing other properties.
5. When you finish changing settings, click OK to return to the Administrator program.

The Permissions Tab

This page of the properties sheet allows you to define certain Windows NT user accounts that have rights to modify this directory object. See Chapter 12, "Using the Administrator Program," for a detailed description on working with the standard Permissions properties sheet.

The Messaging Defaults Tab

To set the messaging default values for the MTA Site Configuration object, follow these steps:

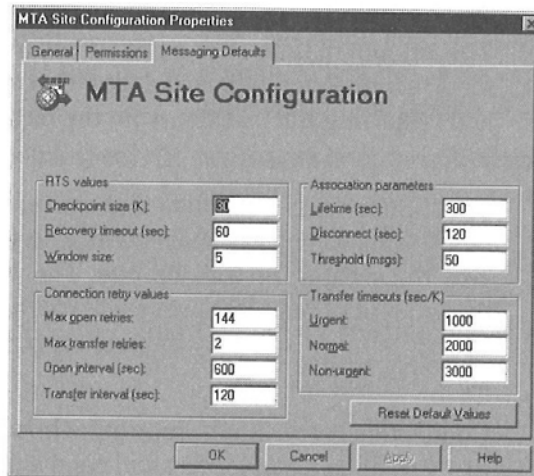
1. Click the Messaging Defaults tab of the MTA Site Configuration properties sheet (see Figure 14.3).

TIP

To return to the default Message Transfer Agent settings, click the Reset Default Values button.

FIG. 14.3

Messaging defaults control each connection made by the MTA.



2. Enter specific MTA configuration variables, as described in Table 14.1.

To the right of each item listed in the table is a box that contains a default numeric value. Replace any value with a number that will be used in establishing a connection through any MTA in the current site.

3. Click Apply to set these properties.
4. When you finish changing settings, click OK to return to the Administrator program.

Table 14.1 MTA Site Configuration Parameter Values

Variable	Description
RTS Values	Reliable Transfer Service (RTS) values determine how often you want to verify information as it is being transferred, how long you want to wait after an error to restart the transfer, and how often you want a verification that another system has received your transfer.
Checkpoint Size (K)	Sets the amount of data to be transferred before a checkpoint is inserted. If an error occurs and the message must be retransferred, the process restarts from the most recent checkpoint. If you specify zero, no checkpoint is set. The default is 30. Checkpointing slightly reduces transmission speed. You should decrease the checkpoint size when the link is less reliable.
Recovery Timeout (Sec)	The amount of time after an error occurs that the MTA waits for a reconnection before deleting checkpointed information and restarting the transfer from the beginning. The default is 60.
Window Size	The number of checkpoints that can go unacknowledged before data transfer is suspended. The greater the window size, the greater the transfer rate. The window size determines the amount of resources set aside for the receiving station. Specify window size only if the checkpoint size is greater than zero. The default is 5.
Connection Retry Values	Connection retry values determine how many times you want to try to open a connection and send a message and how long you want to wait to reopen a connection or resend a message after an error.
Max Open Retries	The maximum number of times the system tries to open a connection before it sends a non-delivery report (NDR). The default is 144.
Max Transfer Retries	The maximum number of times the system tries to transfer a message across an open connection. The default is 2.
Open Interval (Sec)	The delay (in seconds) between attempts to open a communication channel. By default, the delay is 600 seconds.
Transfer Interval (Sec)	The delay (in seconds) between attempts to retransmit a failed message packet. By default, this delay is 120 seconds.

Variable	Description
Association Parameters	Associations are paths that are opened to other systems. Each association is contained within a connection and is used to transfer messages to a system. You may have multiple associations in each connection. You can determine how long to keep an association, how long to wait for a response before disconnecting, and the number of messages you will let wait before you open another association.
Lifetime (Sec)	The maximum time that an idle connection between MTAs remains open. By default, an idle link is held open for 300 seconds after the last communication.
Disconnect (Sec)	The maximum time allowed for establishing or terminating a connection before the session is ended independently. By default, this time is 120 seconds.
Threshold (Msgs)	The maximum number of queued messages to a remote system. When this is exceeded, the MTA opens another association. The default is 50.
Transfer Timeouts (Sec/K)	Messages of different priorities require different levels of attention. For example, an urgent message is processed more quickly than a non-urgent message. If a transfer fails, you must determine how long to wait before sending a non-delivery report (NDR). The transfer timeout is the amount of time to wait before sending that NDR. You can assign a different amount of time for each message priority.
Urgent	The delay (in seconds per kilobyte of total message size) between retries of urgent messages. By default, this delay is 1,000 seconds. This is a timeout value before messages are sent.
Normal	The delay (in seconds per kilobyte of total message size) between retries of normal messages. By default, this delay is 2,000 seconds. The trend here is that the less important the message, the longer you wait for a transmission.
Non-Urgent	The delay (in seconds per kilobyte of total message size) between retries of non-urgent messages. By default, this delay is 3,000 seconds.

NOTE If you combine the default 144 Max Open Retries with the default 600-second Open Interval, Exchange waits 24 hours before returning a message as undeliverable. ■

The following section discusses configuring Message Transfer Agent properties for each Microsoft Exchange Server.

Configuring Local MTA Properties

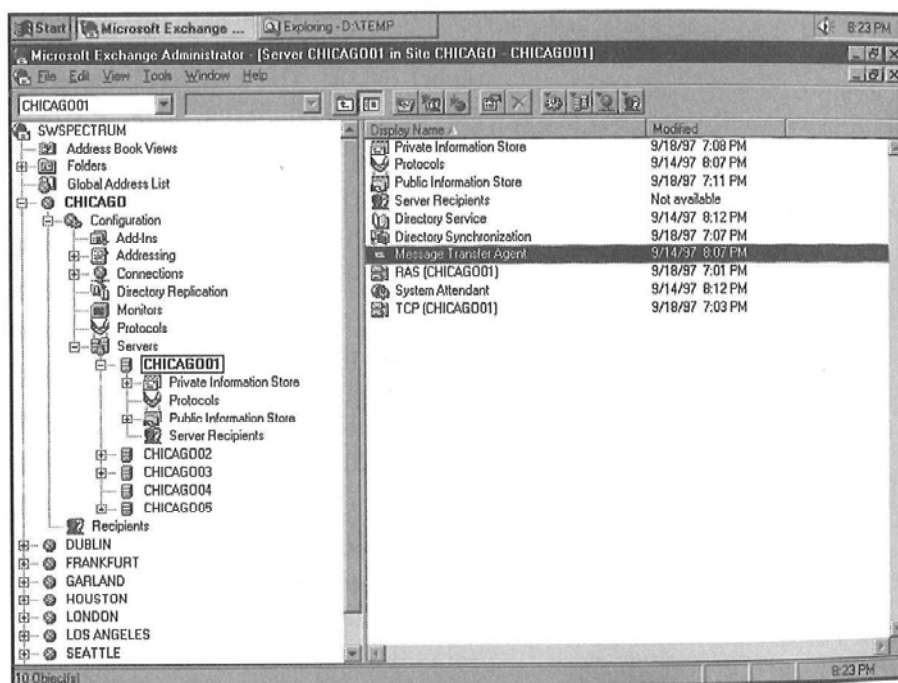
Each Microsoft Exchange Server has a Message Transfer Agent. The MTA properties sheet is designed to configure and manage this service.

First, you must select the MTA from the server within your site. Follow these steps to do so:

1. Navigate to your desired site with the Exchange Administrator program, and then expand the site container.
2. Highlight the Configuration container of the selected site. All the site configuration objects appear in the right pane of the Administrator program's window.
3. Open the Servers container by double-clicking it. A list of Exchange servers in your site appears.
4. Click the name of the server that houses the MTA you want to configure (see Figure 14.4). A list of server objects appears in the right pane of the Microsoft Exchange Administrator program window.

FIG. 14.4

The Message Transfer Agent directory object is located inside the server container.



5. Click the Message Transfer Agent object, and then open its properties sheet.

The following three pages become available for you to configure:

- **General.** Sets local MTA name, password, and general message transmission preferences for this server.
- **Queues.** Lists messages awaiting transmission by the local MTA.
- **Diagnostics Logging.** Sets the level of events that are entered in the Windows NT Event Log.

These pages are covered in the sections that follow.

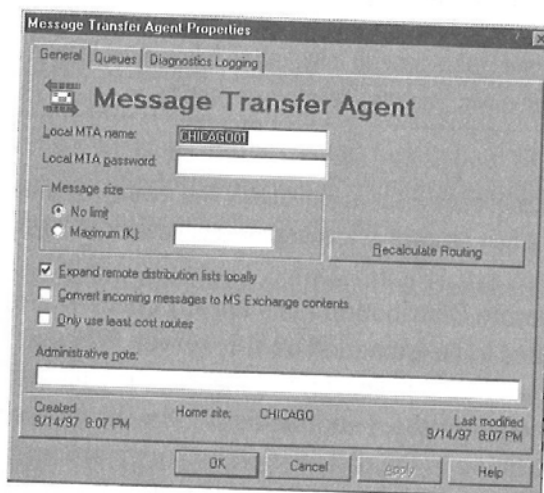
The General Tab

To set values for the local MTA name and password and other general message transfer preferences for this server, follow these steps:

1. Click the General tab of the Message Transfer Agent properties sheet (see Figure 14.5).

FIG. 14.5

The General page of the Message Transfer Agent properties sheet.



2. Type a name in the Local MTA Name box. This name will be used by remote MTAs (either on remote Exchange servers or foreign messaging systems) to identify this MTA. By default, this name is the name of the Exchange server on which the MTA is installed.
3. Type a password in the Local MTA Password box, if necessary. If you enter a password in this box, any remote MTA (either on remote Exchange servers or foreign messaging systems) must be configured to provide this password for authentication. By default, this box is blank, and no authentication is required of the remote MTA.

NOTE If you decide to change the Local MTA Name or to add or change the Local MTA Password, be sure to take into consideration any previously established MTA connections. All remote sites (and foreign systems, such as X.400) must be adjusted to reflect the new information. Authentication is never required between two MTAs in the same site. ■

4. In the Message Size section, click the option button that indicates how you want to restrict the passage of messages through this message transfer agent.

Click the No Limit option button to allow this MTA to deliver messages of any size.

If you want to set a size limit, click the Maximum (K) option button, and then, in the text box, type an upper limit (in kilobytes) for messages that travel through this MTA. Any message that exceeds this size limit will be returned as undeliverable.

TIP

Use these settings as a filter to manage the messaging load for all traffic to and from this server. The upper-limit settings have precedence over message-size settings in individual connectors and recipient objects.

5. Click the Recalculate Routing button to rebuild the routing tables for this MTA. (See Chapter 2, "Understanding Exchange's Organization and Sites," for more information on routing tables.) New routing information for this MTA will propagate to all Exchange servers within the site automatically.

TIP

Rebuilding routing tables sometimes takes several minutes, so it is a good idea to go through each MTA properties sheet, make all changes, and then recalculate routing.

NOTE

Routing tables are rebuilt once a day automatically. The routing table will rebuild when it detects a change in a new gateway or a change in a connector configuration. ■

6. Click the Expand Remote Distribution Lists Locally check box to force distribution lists created on remote sites to be expanded on this server. When a message is sent to a distribution list by a user on this server, the message is split into its component recipients locally. If this box is not checked, the distribution list is expanded in the remote site, following the configuration in the distribution list's own properties sheet. By default, this box is checked, and distribution lists are expanded locally.

NOTE

Consider both the physical location of the majority of the distribution list's recipients and the messaging load on the local server. If you choose the default settings, make certain that the local server can handle the extra messaging traffic: Expanding large distribution lists can be a considerable load on an already overburdened Exchange server. Also, if you know that the majority of the distribution list's recipients reside on Exchange servers in the remote site, consider allowing the list to be expanded there. ■

7. Click the Convert Incoming Messages to MS Exchange Contents check box to convert all messages to Exchange's MAPI-compliant format automatically. By default, this option is not selected, and messages are kept in the format in which they arrive at the MTA (such as standard X.400 format).

8. Click the Only Use Least Cost Routes check box if you don't want this MTA to reroute messages destined for an unavailable server through another possible route. This option configures an individual message transfer agent (MTA) to send messages using only least-cost routes. Only the least-cost route for each message will be attempted. This allows you to prevent messages from being routed to connectors in other sites when a connector in the local site is unavailable. If a message cannot be routed through the least-cost route, Microsoft Exchange Server generates a non-delivery report (NDR).
9. If you want, make an entry in the Administrative Note text box.
10. Click Apply to set these properties and continue with other properties.
11. When you finish changing settings, click OK to return to the Administrator program.

This page controls the functioning of local server MTA. Using this page you can limit the message size sent, how messages are routed when multiple routes are available, and where distribution lists are expanded.

The Queues Tab

The Queues tab of the Message Transfer Agent properties sheet lists messages that are awaiting delivery by the MTA. The two primary windows are Queue Name (which shows the queue that you are currently viewing) and Message List (which displays the messages in that queue). From the Message List window, you can view details about a specific message in the queue, change a message's delivery priority, or delete it.

The Message List window has three columns that contain information about a particular message:

- *Originator*: The original sender of the message.
- *Submit Time*: The time of the next transfer attempt for this message.
- *Size*: The size of the message, in kilobytes.

To configure the Queues property page, follow these steps:

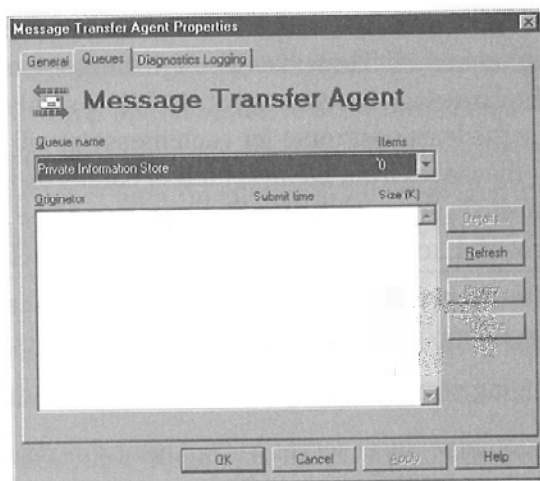
1. Click the Queues tab from the Message Transfer Agent properties sheet (see Figure 14.6).
2. From the Queue Name drop-down list, select the message queue you want to display. The list shows queues for the private and public information stores, as well as for any installed gateways.

NOTE The Internet Mail Connector and Microsoft Mail connector have separate queues that you can access through their properties sheets. ■

3. Select a message, and then click Details to view additional information about it. The additional message information includes the message originator, submit time, message size, and priority. This button is dimmed if no messages are in the queue.

FIG. 14.6

Messages waiting to be delivered are held in the queue.



4. Click the Refresh button to update the Message List window with the latest list of messages in the MTA queue.
5. Click Priority to display the message's priority, and then change the priority of the message if you want. Priority can be low, medium, or high. Messages are sent in order of priority. A message's priority is set when a message is created.
6. To remove a message from the MTA queue, select a message and click Delete.
7. Click Apply to set these properties and continue with other properties.
8. When you finish changing settings, click OK to return to the Administrator program.

Using this page, you can monitor the messaging queues on this server. You can monitor the dynamic RAS connector, X.400 connector, Internet Mail Service, and public and private information stores.

The Diagnostics Logging Tab

This properties sheet works in conjunction with the Windows NT Event Log to record various "events" that occur within the message transfer agent.

FIG. 14.7

The Diagnostics Logging page for the site MTA.

