Concepts and Planning

Microsoft Exchange Server

Version 5.5

Microsoft Corporation

Document No. X03-40136

Printed in Ireland: 03

Contents

Before You Begin

Before you set up Microsoft® Exchange Server, it's important to plan your system. Planning is essential for large organizations, but even small organizations should consider their system and user needs before installing Microsoft Exchange Server. System administrators are encouraged to use this book to plan their Microsoft Exchange Server rollout.

This book describes the concepts for planning a Microsoft Exchange Server system and includes an overview of the product features.

Microsoft Exchange Server *Concepts and Planning* is accessible from the **Help** menu in the Administrator program. It is also available separately as a printed document from Microsoft.

Microsoft Exchange Server Documentation

Microsoft Exchange Server provides comprehensive print and online product documentation. You can install the online books described in this section from the Microsoft Exchange Server compact disc during Setup. You can also order printed versions of many of the books by using the coupon provided in the back of *Microsoft Exchange Server Getting Started.* The following documentation is available for Microsoft Exchange Server.

Microsoft Exchange Server Getting Started Presents the basic information needed to get a Microsoft Exchange Server system running in a typical organization. It provides a brief overview of the product and instructions for installing the server component of Microsoft Exchange Server. The guide also describes how to perform basic Microsoft Exchange Server tasks, such as creating mailboxes and using public folders, and provides product support information.

This book is provided with Microsoft Exchange Server as a printed document. It is also accessible from the **Help** menu in the Administrator program.

Microsoft Exchange Server Operations Provides step-by-step instructions for administering Microsoft Exchange Server, including how to set up and configure Microsoft Exchange Server sites, servers, mailboxes, and connectors. It also provides comprehensive information about using the Microsoft Exchange Server Administrator program.

This book is accessible from the **Help** menu in the Administrator program. It is also available separately as a printed book from Microsoft.

Microsoft Exchange Server Maintenance and Troubleshooting
Provides comprehensive information about monitoring and troubleshooting Microsoft Exchange Server. It includes instructions for using Microsoft Exchange Server tools and Windows NT® tools, as well as those from other sources that you can use to resolve problems with Microsoft Exchange Server.

This book is accessible from the **Help** menu in the Administrator program. It is also available separately as a printed book from Microsoft.

Microsoft Exchange Server Migration Describes concepts for migrating from foreign systems to Microsoft Exchange Server. It also provides instructions for using migration tools to move users from systems such as Microsoft Mail for PC Networks and Microsoft Mail for AppleTalk Networks (also known as Quarterdeck Mail) to Microsoft Exchange Server.

This book is accessible from the **Help** menu in the Administrator program.

What's New: Microsoft Exchange Chat Service Describes the new features available with Microsoft Exchange Chat Service. These new features include new administrative commands, extensions to the Internet Relay Chat (IRC) protocol, security enhancements, and improved server performance and scalability.

This book is accessible from the **Help** menu in the Administrator program.

Microsoft Exchange Chat Service Operations Provides instructions for installing, configuring, and administering Microsoft Exchange Chat Service. It explains how Chat Service works and offers guidelines for automating server operation and improving performance. This guide also describes the administrative tools available in Chat Service and includes a comprehensive command reference for the **chatcmd** utility.

This book is accessible from the **Help** menu in the Administrator program.

Online Help Provides online information for the Microsoft Exchange Server Administrator program. You can access Help from the **Help** menu or by pressing F1.

Online Documentation Set Provides Microsoft Exchange Server books online as a Hypertext Markup Language (HTML) file. They are automatically set up during Microsoft Exchange Server Setup and can be accessed from the **Help** menu in the Microsoft Exchange Server Administrator program. You can also access these books from the **Start** menu by choosing **Programs**, **Microsoft Exchange**, and **Books Online**.

Technical Support Information For technical support information, see *Microsoft Exchange Server Getting Started.*

About This Guide

This book is organized into two parts, and includes an appendix and a glossary.

Part 1 "Concepts" Introduces the benefits and components of Microsoft Exchange Server. Explains how Microsoft Exchange Server maintains and shares information. Includes an overview of security features and support for Internet protocols and describes how to connect Microsoft Exchange Server sites to other sites and to foreign systems.

Part 2 "Planning" Explains the steps involved in planning your sites, servers, and connections. Introduces important information that you should consider before rolling out or deploying your Microsoft Exchange Server system.

Appendix Describes factors that affect system performance and how to optimize performance by using the Microsoft Exchange Server Performance Optimizer.

Glossary Provides brief definitions of terms introduced in this guide.

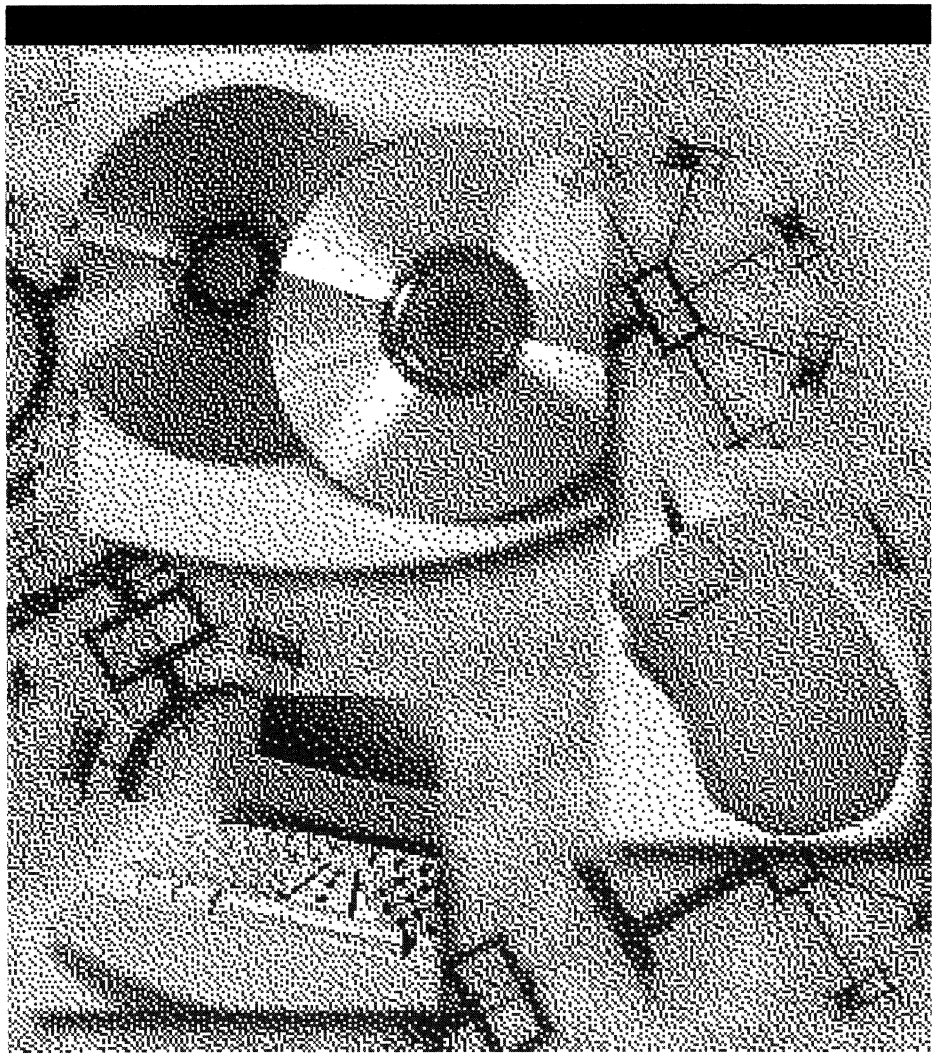
Document Conventions

To help you locate and interpret information easily, *Microsoft Exchange Server Concepts and Planning* uses the following conventions:

Convention	Description
ALL CAPITALS	Acronyms and names of certain commands.
bold	Menus and menu commands, command buttons, property page and dialog box titles and options, command-line commands, options, and portions of syntax that must be typed exactly as shown.
Initial Capitals	Names of applications, programs, files, servers, and named windows, and directory names and paths.
italic	Information you provide, terms that are being introduced, and book titles.
`monospace`	Examples, sample command lines, program code, and program output.
SMALL CAPITALS	Names of keys on the keyboard.

PART 1

Concepts



CHAPTER 1

Introduction to Microsoft Exchange Server

Microsoft Exchange Server is a powerful corporate messaging system that you can use to support your organization with electronic mail. People in your organization will be able to exchange information with anyone, anywhere, anytime, even with people using different messaging systems.

Microsoft Exchange Server is based on a scalable architecture; it can grow as your organization grows. You can make connections to other systems such as the Internet. Most important, you can centrally manage your organization, including sites, servers, and mail recipients, with an easy-to-use graphical interface. Microsoft Exchange Server runs on Windows NT Server.

After you plan and set up your system, users in your organization can do the following:

- Send information to and receive information from users in other sites, organizations, and systems.
- Store and organize all types of information.
- Share information by using public folders to participate in discussions, post information in a bulletin board, track customer accounts from a shared database, or access product information from a reference library.
- Schedule appointments and group meetings, and track tasks.

As an administrator, you can protect your users' privacy by using the advanced security features of Microsoft Exchange Server.

Benefits of Microsoft Exchange Server

Microsoft Exchange Server provides network administrators with the following benefits:

- Centralized administration
- Connectivity
- Internet protocol support
- Adaptability
- Security
- Monitoring, troubleshooting, and performance optimization capabilities

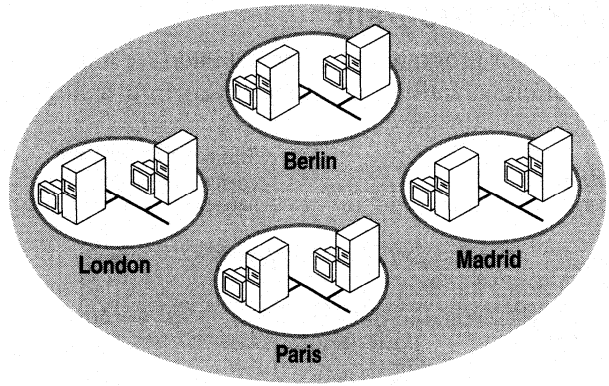
Centralized Administration

With Microsoft Exchange Server, you can administer all servers in your company from a central location, whether your company is small or spread out across a large region. The Microsoft Exchange Server Administrator program can run on a Microsoft Windows NT Server computer or a Microsoft Windows NT Workstation computer.

Organizations, Sites, and Locations

The largest administrative unit in Microsoft Exchange Server is the *organization,* which encompasses all servers that provide the messaging infrastructure for your company. Generally, a company has just one organization.

All servers in an organization are grouped together into sites. A *site* is a group of servers that share the same directory information and can communicate over high-bandwidth, permanent, and synchronous connections. All directory changes in a site are updated and replicated automatically. If you have the appropriate permissions, you can fully administer the site where you are logged on and view all other sites in the organization.

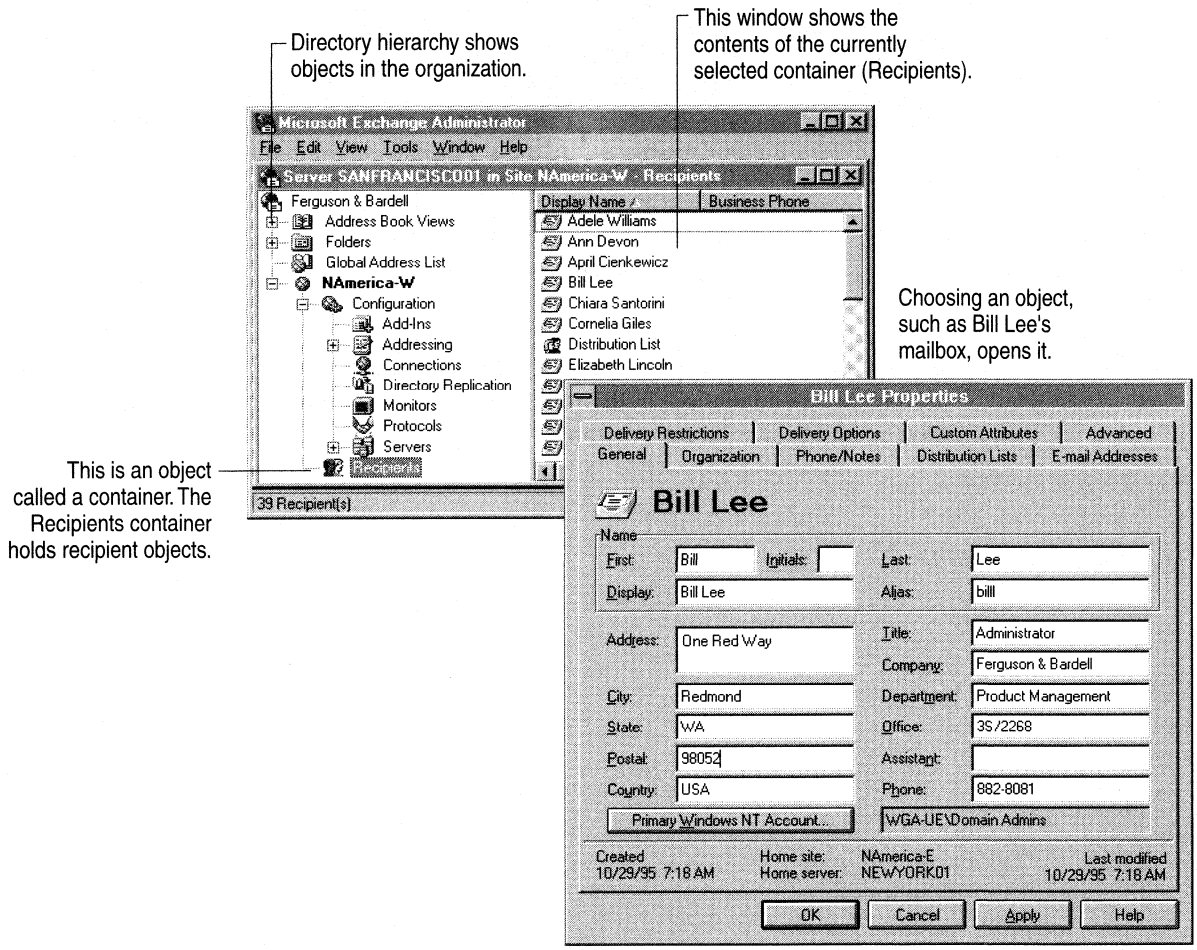


Sites in an organization

Within a site, you can group servers into *locations.* A location is a group of servers connected across a high-bandwidth network. Although you do not need to assign servers a location, both public folder access and mail routing will take advantage of location information if it is provided.

Administrator Program

The Administrator program is a graphical interface that you use to configure and maintain your organization's sites and servers from a single location.



Connectivity

Microsoft Exchange Server includes several options for connecting sites and connecting to foreign systems.

Component	Description
Site Connector	Provides the simplest mechanism for connecting two Microsoft Exchange Server sites in an organization.
X.400 Connector	Can be configured to connect sites within an organization, or to route messages to foreign X.400 systems. The X.400 Connector conforms to the 1984 and 1988 International Telegraph and Telephone Consultative Committee (CCITT) X.400 standards.
Dynamic RAS Connector	Can be used between Microsoft Exchange Server sites that don't have a permanent connection.
Microsoft Mail Connector	Provides connectivity to Microsoft Mail for PC Networks and Microsoft Mail for AppleTalk Networks (also known as Quarterdeck Mail).
	Provides connectivity to MS® Mail (PC) gateways, including AT&T Mail, Fax, IBM Professional Office System (PROFS) and OfficeVision, MCI MAIL, MHS, and SNADS. (Note: These components must be purchased separately.)
Internet Mail Service	Provides connectivity to the Internet so that users can exchange messages with other people on the Internet. Can also be configured to connect sites within Microsoft Exchange Server.
Microsoft Exchange Connector for Lotus cc:Mail	Provides message transfer and directory synchronization between Microsoft Exchange Server and Lotus cc:Mail systems.

In addition to connecting to sites and to foreign systems, you can use the Microsoft Schedule+ Free/Busy Connector, which exchanges Microsoft Schedule+ free and busy information with MS Mail (PC) so that users can view other people's free and busy times.

Internet Protocol Support

Microsoft Exchange Server supports several Internet protocols. An Internet protocol is a set of standards designed to enable different types of computers to communicate with one another and to exchange information through the Internet.

Component	Description
Network News Transfer Protocol (NNTP)	Enables clients to read and post information to USENET newsgroups.
Post Office Protocol version 3 (POP3)	Enables users with POP3 clients to retrieve mail from their Microsoft Exchange Server Inbox.
Internet Message Access Protocol, Version 4rev1 (IMAP4rev1)	Enables IMAP clients to access messages stored within a user's private and public folders on a Microsoft Exchange Server computer.
Lightweight Directory Access Protocol (LDAP)	Enables LDAP clients to access directory information from the Microsoft Exchange Server directory.
Hypertext Transfer Protocol (HTTP)	A method that World Wide Web servers use to send Hypertext Markup Language (HTML) pages over the Internet for display by a Web browser.

Adaptability

Microsoft Exchange Server can be adapted to suit both large and small organizations, with or without existing messaging systems. It can be used in many countries and is available in many languages.

Microsoft Exchange Server provides tools for converting e-mail and user account information from other systems, including DEC ALL-IN-1, PROFS or OfficeVision, MS Mail (PC), MS Mail (Appletalk), Lotus cc:Mail, and others, as follows:

Source extractors copy directory, message, and scheduling data from other systems. In addition, templates are provided for writing custom source extractors.

Migration Wizard imports data created with source extractors.

For more information on source extractors and the Migration Wizard, see *Microsoft Exchange Server Migration.*

Import and export commands (in the Administrator program) used in place of or with source extractors and the Migration Wizard.

Security

Microsoft Exchange Server uses the security features of Windows NT Server, including user authentication, access control (permissions), and auditing to prevent unauthorized use of the system. Microsoft Exchange Server also provides advanced security features, which protect information during transmission.

Monitoring, Troubleshooting, and Performance Optimization Features

You can use tools included with Microsoft Exchange Server and Windows NT Server to check the state of servers, their connections, and their performance, including Server Monitor, Link Monitor, and Windows NT Performance Monitor.

Other tools included with Microsoft Exchange Server and Windows NT Server troubleshoot and track problems with servers:

- Windows NT Event Viewer
- Windows NT Control Panel
- Windows NT Server Manager

The Performance Optimizer included with Microsoft Exchange Server analyzes the server's hard disk and memory configurations to determine the best location for components. You should use the Performance Optimizer:

- After running Setup.
- After changing the server's hardware configuration.
- After making changes to the server's role in the site, such as adding or removing a connector.
- To help move files to other disks for special configurations.
- To experiment with parameter settings for a particular installation.

Components

The server components perform actions that the client components request, such as looking up names, sending messages, and storing information in private and public folders.

Each server has core and optional components. All server components are implemented as Windows NT Server services. The core components are installed during Setup and must be running at all times. In addition, they must all reside on the same Windows NT Server computer. The core components provide the main messaging services: message transfer, delivery, and storage, and directory services.

Following are the core server components and their functions:

Directory maintains information about an organization's recipients, distribution lists, servers, and messaging infrastructure. Other components use the directory to map addresses and route messages. The directory is automatically replicated to all servers in the organization.

Information store provides server-based storage, holds users' mailboxes and public folders, and enforces security. The information store also replicates public folders, enforces storage limits, and delivers messages to users on the same server. It maintains information in two databases: the public and private information stores. The public information store maintains information stored in public folders. The private information store maintains all messages in users' mailboxes.

Internet Mail Service provides connectivity to the Internet and other systems that use Simple Mail Transfer Protocol (SMTP) The Internet Mail Service can be used to establish a dial-up connection to an Internet service provider (ISP) or a remote site at specified intervals, or to connect sites within a Microsoft Exchange Server organization.

Message transfer agent (MTA) submits, routes, and delivers messages to other Microsoft Exchange Server MTAs, information stores, connectors, and third-party gateways.

System attendant A maintenance service that must be running for other Microsoft Exchange Server services to run. It performs the following tasks:

- Assists in running the monitoring tools by gathering information about the services running on each server in a site.
- Checks messaging connections.
- Checks directory-replication information and corrects inconsistencies.
- Logs information about messages for message tracking.
- Builds routing tables in a site.
- Generates e-mail addresses for new recipients.
- Helps enable and disable digital signatures and encryption for mailboxes.

Optional Components

The optional components provide connectivity and directory exchange with other systems, as well as advanced security. Following are the optional server components and their functions:

Advanced Security manages security information used for digitally signing and encrypting messages sent between users.

Connectors transfer messages between sites, organizations, and foreign systems. In addition to the Site Connector, Microsoft Exchange Server includes these connectors: X.400, Internet Mail Service, Dynamic RAS, Microsoft Mail, and Connector for cc:Mail. In addition, the Microsoft Schedule+ Free/Busy Connector enables users to exchange free and busy information.

Microsoft Outlook™ Web Access enables users to access their mailboxes and public folders through a Web-based e-mail client that operates in a Web browser window.

CHAPTER 2

Storing and Maintaining Information

Microsoft Exchange Server maintains information in a variety of ways, on both servers and clients. This chapter describes the server's information store and the directory—key components used to share and manage information. You'll also learn about replicating information, an important feature of Microsoft Exchange Server.

Note It is strongly recommended that you back up Microsoft Exchange Server files on a regular basis, in the event that you need to restore a server following a hardware or software failure. For more information about backing up and restoring servers, see *Microsoft Exchange Server Maintenance and Troubleshooting.*

Information Store

The information store makes it possible for users to send mail and use public folders. The information store performs the following tasks:

- Stores public folders in the public information store.
- Stores users' messages in the private information store.
- Provides rules and views.
- Maintains storage and age limits.
- Delivers messages addressed to users on the same home server as the sender.
- Forwards messages addressed to recipients on other servers and systems to the message transfer agent (MTA) to deliver.

Microsoft Exchange Server uses a fault-tolerant, transaction-based architecture for its information store.

If a power outage or other abnormal system shutdown occurs, Microsoft Exchange Server uses *transaction log files* to reconstruct the data. Transaction log files minimize response times for user requests and provide fault tolerance in the event that data needs to be restored.

If a message is sent to multiple mailboxes located on the same server, each person's mailbox contains a reference to a single shared copy of the message in the private information store, minimizing storage needs. This is called *single-instance storage*.

Mailboxes

Before you install your clients, you must create mailboxes that are associated with their Windows NT user accounts. A mailbox is a recipient object in the directory and is the delivery location for messages for a designated owner. A user mailbox contains information such as messages, documents, and spreadsheets and is located on the user's home server. Although a mailbox typically is used by only one person, it can be used by several people. A user can be simultaneously logged on to the same mailbox from different computers.

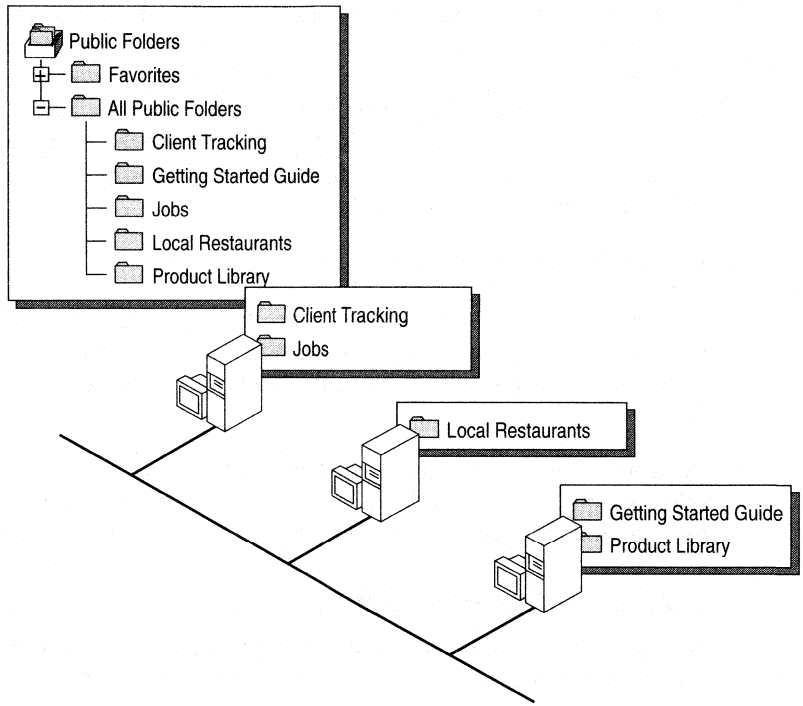
Messages are delivered to the user's Inbox. Users can create folders in their mailbox and then use the Inbox Assistant to automatically move messages and other information to these folders.

Mailboxes can be configured to support multiple Internet protocols such as the Internet Message Access Protocol, Version 4rev1 (IMAP4rev1), Post Office Protocol version 3 (POP3), and Hypertext Transfer Protocol (HTTP).

Public Folders

A *public folder* holds information that can be shared by a group of users. Public folders can be configured for different types of applications, such as bulletin boards, discussion forums, and customer tracking systems. For example, a manager can create a public folder to hold background information about a project. A Help group can create a public folder to store commonly asked questions.

The list of public folders available to a user is displayed as a hierarchy, which can be viewed from Microsoft Outlook or from the Microsoft Exchange Server Administrator program. Although the hierarchy is available on all users' public folder servers, the data contained in public folders is stored in a distributed fashion on various servers throughout the organization. Users are not required to know the name or location of the server where the data is stored. The following illustration shows the public folder hierarchy:



Controlling Access to Public Folders

Depending on the permission they are granted, both administrators and users can control access to public folders. Each folder has an access control list, which is a list of mailboxes that can access the folder. A set of permissions is associated with each user on the access control list. The permissions define the type of access that a user has been given. Permissions include, for example, whether the user can read, write, or delete items in a folder. Users can define a custom role by selecting a group of permissions that provide a certain level of access and determine whether the folder is visible.

You can control access to public folders at any branch within the hierarchy. Access permissions to public folders are copied from the next higher-level folders at the time they are created. By setting permissions at the appropriate level in the hierarchy, you can control how public folders are used.

Sets of permissions are organized as roles. For example, roles defined for public folders include owners (who have complete access to the folder) and reviewers who can only read the items.

Microsoft Exchange Server also enables you to grant anonymous access so that users can access public folders without having a mailbox or being a custom recipient in that organization. An *anonymous user* can log on to a Microsoft Exchange Server computer but is restricted to viewing and accessing the content of public folders that have been granted anonymous permissions. You can specify which folders and address lists to publish to anonymous users by using the Administrator program or Outlook.

Maintaining Public Folders

You have a range of options for controlling how information in public folders is maintained. You can set age limits on public folders to specify how long the contents should be stored before they are deleted. You can also set folder size limits.

In addition, you can control which servers are configured to store public folder information. You can dedicate certain servers to hold only private folder information and dedicate other servers to hold only public folder information.

Public Folder Replication

A public folder can be configured to have replicas on multiple public folder servers. Each public folder server in an organization can have zero or one replica of each public folder. Each replica of a public folder is equivalent; that is, there is no master replica. The process of keeping these replicas up-to-date and synchronized with each other is called *public folder replication*. Replicas contain all the folder's contents, permissions, and design elements (such as forms behavior and views). They are useful for distributing user load on servers, distributing public folders geographically or across sites, and even for backing up public folder data.

You can create replicas of public folders from any site in your organization. During replication, changes made to items in the replica are sent to all other replicas of the public folder throughout the organization. Changes made to the folder properties or the public folder hierarchy are replicated to all public folder servers (even servers without replicas of the content of folders).

Public folder replicas are not identical at all times. Servers within an organization communicate with each other to accomplish replication on a scheduled basis. As users add, edit, or delete items in a replica, other replicas contain different information until the next scheduled replication takes place.

Changes are replicated through messages. When a change occurs to a public folder replica, the information store sends the changes to all the information stores that contain replicas of this data. When scheduling replication, you should balance the frequency of replication with the message traffic it may create. You can schedule replication messages to be sent during off-hours to minimize message traffic, and you can limit the size of replication messages so that large messages don't cause delays.

Viewing Public Folder Contents

Users can view the contents of all public folders that have replicas on servers in their site, provided they have permissions. They can view the contents of public folders in another site, but only if you have configured *public folder affinity* in that site. Public folder affinity allows users to access information in other sites without replicating the public folders to their own site. If a public folder replica is available in more than one site, the public folder affinity cost is used to determine the order for connecting to the other sites. The lowest cost connection is used first.

When a user tries to view the contents of a public folder, you can control:

Access You can control whether the user can view the contents of a public folder or a replica. For example, if you want users in site A to view a public folder in site B, add site B to the public folder affinity list for site A.

Cost If there are multiple sites with a replica of the same folder, you can consider cost and then order the connection attempts in the least expensive way.

When a user tries to open a public folder, the following process determines which replica of a public folder is accessed:

- If a public folder replica is on the user's home server, the user is connected to that replica.
- If the user's home server belongs to a *location* within a Microsoft Exchange Server site, the system will search for a replica on any server belonging to that location. If one is found, that server will be used. If multiple replicas are available, a copy will be selected in such a way that the load is balanced.
- If a replica cannot be found within the location or if the user's home server does not belong to any location within the site, the system will search for a public folder replica on servers belonging to a special wild-card location ("*"). If a server bearing the location value of "*" contains a replica, that replica will be used. If multiple replicas are available, a copy will be selected in such a way that the load is balanced.
- Microsoft Exchange Server will then search any server in the site, regardless of its location, for a replica of the public folder. If multiple replicas are available, a copy will be selected in such a way that the load is balanced.

- If no replica exists on any server within the user's site, and public folder affinity is configured, the user is connected to a replica in another site based on the affinity. If there are several sites with replicas, the site chosen is based on the affinity for that site and the cost associated with that site connection.

Directory

The directory describes your organization's infrastructure and recipients. Each component in the system is represented as an *object*. For example, each user's mailbox is represented as a directory object. Each object has a set of properties. When you configure components of your organization, you assign values to these properties by using the Administrator program.

Most objects in the directory represent individual items in the organization, such as a particular server or recipient. In addition, there are objects called *containers* that hold collections of individual objects or other containers. The collection of objects that make up an organization is presented as a hierarchy.

The Address Book displays recipient names (mailboxes, distribution lists, custom recipients, and public folders) in the directory, and can contain one or more address lists. Using the Address Book, users can address messages and look up locations or phone numbers. It is organized into various lists, which contain mailboxes, custom recipients, distribution lists, and public folders. Users can access information in the same way they would use a telephone directory. The Address Book can contain one or more of the following address lists:

Global address list Contains all recipient objects in the organization and is available to every user.

Custom address lists Contains address lists that you, the administrator, define. For example, if you have a Recipients container (Public Folders) that contain all public folders in your organization, your users can send mail to those public folders by using either the public folder address list or the global address list.

Offline address books Contain the recipient objects found in any Recipients container in the directory. You configure this address book so that remote users can access addresses when they are not connected to the network. By default, offline address books use the Recipients container for the local site.

Directory Components

The directory has two main components—a database and a service.

Directory database The directory database stores all the directory objects.

Directory service The directory service is a Microsoft Windows NT Server process that manages information in the directory database and handles directory requests from users, services, and applications. The directory service:

- Provides the Microsoft Exchange Server Address Book.
- Enforces the rules governing the structure and contents of the directory.
- Sends directory replication notifications to directories on other servers and processes directory replication notifications from other servers.

Directory Usage

Not only is the directory important to users and administrators, it is also crucial to Microsoft Exchange Server processes and third-party programs.

Users Access directory information through the Address Book. Users can also access directory information through LDAP.

Administrators Use the Administrator program to create, modify, or delete directory objects and to import or export directory objects.

Microsoft Exchange Server processes Access the directory to obtain information needed for certain tasks. For example, the system attendant uses connector configuration information to build the routing table.

Third-party programs Access the directory in a variety of ways, such as by manipulating the directory objects and by synchronizing the Microsoft Exchange Server directory with other directories.

Controlling Access to the Directory

You can control access to directory objects. Each object has an *access control list,* which is a list of Windows NT user accounts and groups associated with the object. This list is used to determine whether a user or process has been granted access to an object.

A set of permissions is associated with each account on the access control list. Permissions define the type of access that an account has been granted. These include, for example, whether the account has been given the right to modify the object.

These sets of permissions are presented in the Administrator program as roles. For example, typical users are granted the role of User on their mailboxes. Microsoft Exchange Server also enables you to grant anonymous access so that users can access directory objects without having a mailbox or being a custom recipient in that organization. An anonymous user can log on to a Microsoft Exchange Server computer but is restricted to viewing and accessing directory objects that have been granted anonymous permissions. You can specify which directory objects and address lists to publish to anonymous users by using the Administrator program or Outlook.

When you configure permissions on a directory object, you select a Windows NT user account and specify the type of access it has. For example, if you grant Maria Black's user account Admin permissions on the site object, Maria Black can administer all the recipients in the site.

If you find that none of the predefined roles are appropriate, you can specify a custom set of permissions.

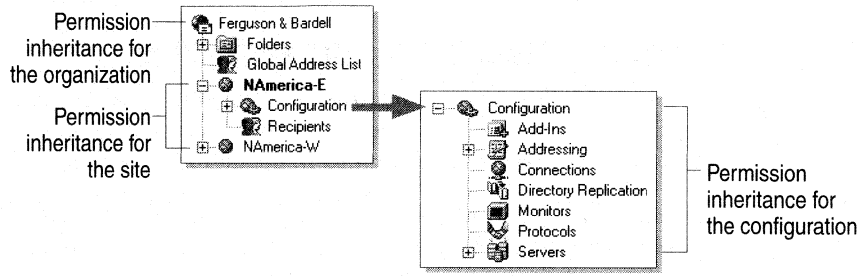
Permissions and Inheritance

It isn't necessary to set permissions individually for every object in the directory. In general, objects inherit permissions from those defined for their containers. This means that permissions can be set once across different levels of the organization and can be inherited by many other objects. Permissions are inherited as follows:

The organization object Windows NT user accounts with permissions on the organization object can change the display name of the organization. Permissions on this object are not inherited by any other object.

Site objects Windows NT user accounts with permissions on the site object can modify the site object and all the recipients in a site. The Recipients container and all its objects inherit permissions from the site object. An administrator who adds users to the system could be granted Admin permissions on the site.

Configuration objects Windows NT user accounts with permissions on the configuration object can configure routing, replication connection, and other processes. The following illustration shows the permission inheritance on the configuration objects:



Directory Replication

Directory replication ensures that directory information is current among servers. Directory information is automatically updated on all servers in the same site, and can be configured to be updated automatically with servers in other sites.

Each Microsoft Exchange Server computer has a local directory. At any given time, the local directories on two servers might contain different information. For example, if you create a new mailbox on server A, the addition won't show up on server B until the directory on server B gets updated through directory replication.

There are two directory replication processes: intrasite (within a site) and intersite (between sites). Intrasite directory replication does not need to be configured; it starts automatically. Intersite directory replication must be configured.

Directory Replication Within a Site

Intrasite replication is a way to distribute a directory among servers within a site. Each directory notifies the others of its changes. Directory replication within a site has the following characteristics:

- Every server has a copy of the directory that can be written to. This enables the directory changes to be made on any server.
- Every server has a direct connection with every other server in the site. This means that directory replication can start from any server in the site.
- Directory replication automatically starts within five minutes after a change to a directory object is made.
- Directory change notifications and requests for updates are done through remote procedure calls (RPCs).

During directory replication within a site:

- A directory change is made and other servers are notified of the change, one directory at a time.
- Each directory requests an update and is then updated.

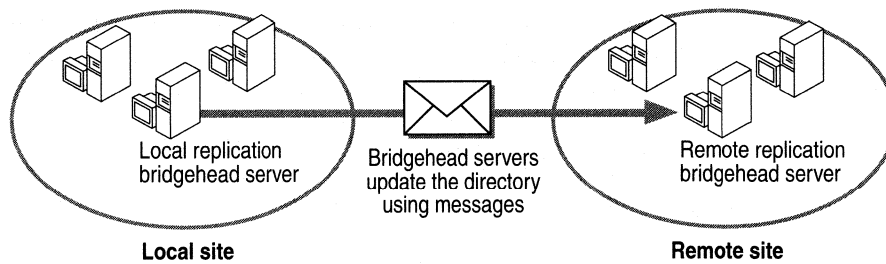
Directory Replication Between Sites

To establish directory replication between sites, you configure a *directory replication connector* between them. You must establish mail connectivity between two sites before you can replicate their directories.

One server is required at each end point. The servers at each end point of a directory replication connector are called *directory replication bridgehead servers,* which request directory updates from each other. You can only configure one directory replication connector between two sites.

Directory replication between sites has the following characteristics:

Point-to-point The replication bridgehead servers are the only two points of contact for replicating directory information between two sites. The following illustration shows directory replication between sites:



Scheduled Intersite directory replication runs on a schedule that you set up. This schedule determines when a local site requests directory updates from the remote site.

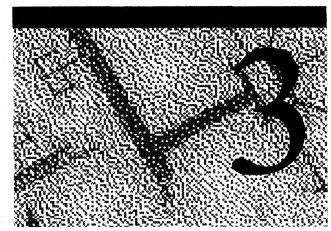
Messaging-based Communication between bridgehead servers is done through messages. Requests for updates, and the updates themselves, are sent as messages through MTAs and connectors.

During directory replication between sites:

1. A message is sent from the local site to request directory updates from the remote site.
2. The requested updates are sent from the remote site using messages.
3. The directory at the local site is updated.
4. All other directories at the local site are updated through intrasite replication.

CHAPTER 3

Security



Microsoft Exchange Server provides a variety of ways to keep your system secure. This chapter describes the different aspects of security and how they work.

There are four aspects of security within Microsoft Exchange Server, as follows:

Windows NT Server security Identifies and validates users when they log on.

Access control (permissions) Grants users the permission to access resources.

Auditing Detects and logs security-related events.

Microsoft Exchange Server advanced security Enables users to encrypt messages and provides verification of the originator by associating a digital signature with the message.

Windows NT Server Security

Microsoft Exchange Server uses aspects of the Windows NT Server security model, which includes the following elements:

- User account—Contains information about a user, such as the user's name and password, the groups that the user belongs to, and the rights and permissions granted to that user.
- Domain—A group of Windows NT Server computers that share user accounts and a security policy. A domain can contain one or more Windows NT Server computers and Microsoft Exchange Server computers, as well as other types of servers and clients. The domain is the basic unit of security.
- Trust relationship—The connection between two domains that makes it possible for a user account in one domain to access resources, such as servers and printers, in another domain.

These elements of Windows NT Server security are used to validate users who access Microsoft Exchange Server.

For more information about Windows NT Server security, see your Windows NT Server documentation.

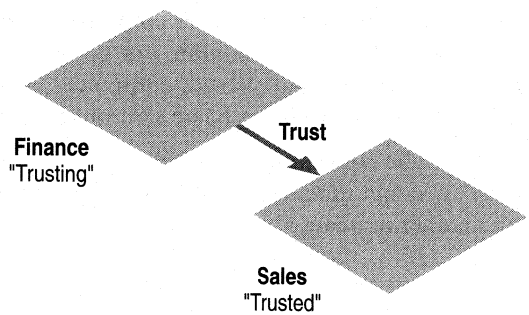
User Authentication

Before users or processes can access Microsoft Exchange Server, they must log on to Windows NT Server by supplying a unique user name and password. The system must validate or *authenticate* this logon information. When a user logs on, Windows NT Server identifies a *security context*. The security context determines the user's access to system services.

Note You can configure Microsoft Exchange Server to support anonymous access for some Internet protocols, such as the Network News Transfer Protocol (NNTP), Internet Message Access Protocol, Version 4rev1 (IMAP4rev1), and Lightweight Directory Access Protocol (LDAP), so that nonvalidated users can access information stored in Microsoft Exchange Server. Users connecting to Microsoft Exchange Server anonymously don't need a Windows NT user account to access information. For example, if you want certain public folders to be accessible to IMAP4 users outside of your organization, you can enable anonymous connections.

A user needs to log on only once to gain access to Microsoft Exchange Server. This is in contrast to other security models that require separate passwords for different resources, such as printers, file servers, or e-mail.

Each Microsoft Exchange Server computer in a site is also a member of a Windows NT domain. To enable users to access the entire network, you can establish trust relationships between domains. Domains with trust relationships share account information and validate rights and permissions. In a trust relationship, one domain (the *trusting domain*) trusts the other (the *trusted domain*). Users from the trusted domain can be given rights and permissions to objects in the trusting domain as if they were members of the trusting domain.



When a user logs on to a domain where a trust relationship is set up, the account is verified by *pass-through authentication*. Pass-through authentication makes it possible for users to log on to domains in which they have no account. In other words, a user can have an account on only one domain yet still access the entire network including all its trusted domains.

User Accounts

All Microsoft Exchange Server mailboxes are associated with one or more Windows NT user accounts. For a user to log on to a Microsoft Exchange Server computer, the domain where the server is located must have a trust relationship with the domain that has the user account. For example, a user can view the contents of a public folder on a Microsoft Exchange Server computer in another domain if that domain contains the user account or has a trust relationship with another domain that contains the account.

Windows NT user accounts are stored and maintained on the primary domain controller of a domain. You can create two types of user accounts: global and local. Most accounts are global user accounts.

Groups

You can organize user accounts into *groups,* which makes granting permissions easier. You only have to perform one action to give permissions to a whole group of users. For example, if a group of administrative assistants needs to access the same mailbox, you can define a group called Admin Assistants and create a mailbox called Assistants. You can then give the Admin Assistants group permission to use the Assistants mailbox so that every time users in the group logged on to Windows NT Server, they could access their mailbox.

Windows NT provides built-in *global* and *local* groups, and the ability to customize them. Adding a user to a predefined group provides the user with all the access rights of that group. Changing the access rights of the group automatically changes the rights of all group members. You should use built-in groups whenever possible. For more information about Windows NT groups, see your Windows NT Server documentation.

Service Accounts

Microsoft Exchange Server includes a variety of services, such as the information store and the message transfer agent (MTA). Before you install Microsoft Exchange Server on the first server in a site, you need to create a Windows NT user account that Microsoft Exchange Server will use to start and run these services. This is called a *service account.* Microsoft Exchange Server computers use the service account to validate other servers in the site and give them access to Microsoft Exchange Server services. For example, for an MTA on one Microsoft Exchange Server computer to interact with another MTA, Windows NT Server must verify the security context of the requesting MTA.

A Microsoft Exchange Server computer doesn't need to be in the same domain as the service account, provided that the domain has a trust relationship with the domain containing the service account. However, all Microsoft Exchange Server computers in the same site must use the same service account to communicate with each other.

Permissions

You use permissions to control access to resources. A *permission* provides specific authorization to perform an action. Different levels of permissions exist for different objects.

You can also use built-in groups of permissions, called *roles*. For example, the Admin role gives a user a number of permissions, including Add child, Modify user attributes, and Delete.

Mailbox Permissions You grant permission to log on to a mailbox by using the Microsoft Exchange Server Administrator program. You can set one or more Windows NT user accounts to have user permission on a mailbox. When a user attempts to log on to a mailbox, Microsoft Exchange Server determines whether that user has permission to access that mailbox.

Public Folder Permissions Permission to access a public folder can be granted by the owner of a public folder, through Microsoft Outlook. Permissions to use public folders can be given to mailboxes, distribution lists, and public folders. For example, you can create an Employees distribution list and a Managers distribution list and, for each list, define different permissions on the Company Policies public folder. The Employees distribution list might have read-only permission, whereas the Managers list might have both reading and writing permissions.

Directory Permissions Permissions to use the directory are granted to Windows NT user accounts. Users logged on to the Windows NT domain can view the directory in the Administrator program, but they need permission to modify it. An example of a directory permission is Add child, which enables users who have this permission on the Recipients container to create mailboxes.

Auditing

Auditing refers to the system's ability to detect breaches in security. Because Microsoft Exchange Server is a Windows NT Server application, it uses the auditing capabilities of the operating system. Windows NT Server can track significant events related to the operating system itself, such as logon activities and changes to system files. Administrators do not need to have permission to administer Windows NT Server.

In addition, you can configure Microsoft Exchange Server to audit changes to Microsoft Exchange Server services and directory objects. All events are recorded in the Windows NT Event Log, which identifies the action and the Windows NT user account that performed the action. For example, if a user tries to modify a mailbox, and auditing has been configured, Microsoft Exchange Server records the event in the Event Log, along with information about who performed the action.

Microsoft Exchange Server Advanced Security

Microsoft Exchange Server advanced security provides the following benefits:

End-to-end authentication Ensures that a signer's identity is authentic.

Confidentiality Encrypts a message so that only intended recipients can read the message.

Data integrity Ensures that the contents of a message haven't changed since the message was signed.

Advanced security includes digital signatures and data encryption. By using digital signatures, a person can "sign" a message so that the recipient can be sure that the message came from the indicated source and wasn't changed during transit. Digitally signed messages undergo two processes: *signing* and *verifying*. A message is signed when it is sent, and the signature is verified when the message is received.

By using data encryption, a user can scramble data to ensure that only the intended recipient of a message can read it. Encrypted messages undergo two processes: *encryption* and *decryption*. A message is encrypted when sent and decrypted when received.

Note Microsoft Exchange Server supports the Data Encryption Standard (DES), and the CAST and Secure/Multipurpose Internet Mail Extensions (S/MIME) encryption algorithms. DES encryption is available only with Microsoft Exchange Server software used in the United States and Canada.

Key Management Server

To use the advanced security features of Microsoft Exchange Server, you must configure at least one computer in your organization as the server that stores and manages the security database. This server is called the *Key Management (KM) server.* You can configure up to one KM server per site.

The KM server provides the following services:

- Creates public and private encryption keys.
- Maintains backups of private encryption keys and public signing keys.
- Generates temporary keys.
- Maintains the original copy of the revocation list.
- Issues certificates for Certification Authorities (CAs) in other organizations.

Note The KM server uses Microsoft Certificate Server to certify public signing and encryption keys. For information about Microsoft Certificate Server, see your Microsoft Internet Information Server version 4.0 documentation.

Private encryption keys and public signing keys for security-enabled users and the revocation list are stored in the key management database. The KM server database itself is encrypted, so that the highest level of security is maintained.

After you configure the KM server, you must enable advanced security for your users. You give users temporary keys so that they can complete the advanced security process. A temporary key is used only once, and it secures the connection between the KM server and the client. You should distribute temporary keys to users in person for maximum security. You can enable advanced security for users individually or in bulk.

Advanced Security Keys

Microsoft Exchange Server uses public/private key technology to provide advanced security. Keys are used to digitally sign and encrypt data. Each mailbox is given two key pairs: one for encrypting and decrypting, the other for signing and verifying. Each key pair consists of a *public key* (publicly known) and a *private key* (known only to the key's user). The KM server generates encryption keys, and Outlook generates signing keys.

The public encryption key is used to encrypt a message; the public signing key is used to verify the source. When a user encrypts a message, each recipient's public encryption key completes the process. When a user receives a signed message, the public signing key verifies the person who signed the message.

Private keys are stored in an encrypted security file (.epf) on each user's local disk. When a user receives an encrypted message, the private encryption key decrypts the message. When a user signs a message, the private signing key is used.

A *bulk encryption key* is also encrypted and sent with the message. The encrypted bulk encryption key is referred to as a *lock box*. The lock box ensures that the bulk encryption key is secure while the message is encrypted. If a message is sent to multiple recipients, the message contains a different lock box for each recipient. After the message and lock box are received, the lock box is decrypted and the contents of the lock box (the bulk encryption key) decrypts the message.

Certificates

Public keys must be certified by a CA. In Microsoft Exchange Server, the CA is Microsoft Certificate Server. A *certificate* binds the user's public key to the mailbox.

Each certificate includes:

- A unique serial number.
- The directory name of the CA.
- The user's directory name.
- The directory name of the KM server requesting the certificate from the CA.
- The expiration date of the user's public key.

Every user has two certificates:

Encryption certificate Contains the user's public encryption key and is an attribute of the user's mailbox in the directory.

Signing certificate Contains the user's public signing key and is stored in the user's security file.

Revocation

Revocation warns users when they verify signed messages that contain a revoked certificate. Revoking a user's advanced security is not the same as deleting a user, and should be done only if the security of the user has been compromised. For example, you should consider revoking advanced security if it appears that someone is signing messages on behalf of a user or someone has gained access to the user's security file and password. You can enable security again by assigning the user another temporary key.

A revocation list contains the serial number and expiration date of each revoked user's certificate. The KM server stores the revocation list in the key management database and then writes it to the directory. The revocation list in the directory is then cached on the client and updated daily.

You should limit the use of revocation. As the revocation list grows larger, the client's performance and advanced security operations degrade. This is because each time the client verifies a message's signature, it must access it in the revocation list. If the list is long, this operation may take longer.

Additional Security Features

The KM server provides the following additional features that you can use to increase security:

Certificate Trust List Enables organizations to establish trust with other organizations so that users can verify the digital signature of messages sent by users in other trusted organizations.

Multiple password policy Enables administrators to configure the KM server to require multiple passwords to perform certain tasks.

Certificate Trust List

With a certificate trust list, an organization can ensure that the CA that issues a certificate can be trusted, even if the CA is in another organization. This is the most secure way to verify the source of messages sent from another organization. It is also transparent to users—they don't need to perform any additional steps to send a digitally signed message to a user in a trusted organization.

Because certification establishes trust between CAs, security keys sent between users in certified organizations are automatically trusted. For example, even if a digitally signed message is sent with the sender's key (by using a key exchange form), the recipient is not certain who actually sent the message because the signature was issued by an unknown CA. However, if the message is signed by a CA in a trusted organization, the recipient can verify that the signer's identity is authentic, because the organizations' CAs trust each other.

Multiple Password Policy

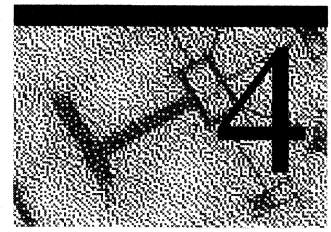
The multiple password policy prevents administrators from making changes to the KM server without the authorization of one or more other administrators. For example, you can set your KM server so that the cooperation of three administrators is necessary to recover or revoke a user's key.

You can require multiple passwords to perform the following tasks:

- Add or delete administrators who can manage the KM server.
- Recover or revoke a user's security keys.
- Import or untrust another CA's certificate.

CHAPTER 4

Connecting to Other Sites and Systems



Microsoft Exchange Server uses connectors and services to connect Microsoft Exchange Server sites with each other or with foreign systems. Addresses and address spaces are an important part of this connection process.

The following components can be used to connect Microsoft Exchange Server sites:

- Site Connector
- Dynamic RAS Connector
- Internet Mail Service
- X.400 Connector

The following components are used to connect Microsoft Exchange Server sites to foreign systems:

- Internet Mail Service
- Microsoft Mail Connector for PC Networks
- Microsoft Mail Connector for AppleTalk Networks
- X.400 Connector
- Microsoft Exchange Connector for Lotus cc:Mail

In addition to connecting sites and foreign systems, you can also access scheduling information. The Microsoft Schedule+ Free/Busy Connector enables Microsoft Exchange Server to share Schedule+ free and busy information with Microsoft Mail for PC Networks (MS Mail [PC]).

Addresses

Microsoft Exchange Server uses a variety of addresses. Each Microsoft Exchange Server has a site address, and each mailbox has a recipient address. Custom addresses can be created for recipients on other mail systems. Address spaces are used by connectors to define the types of messages they transmit.

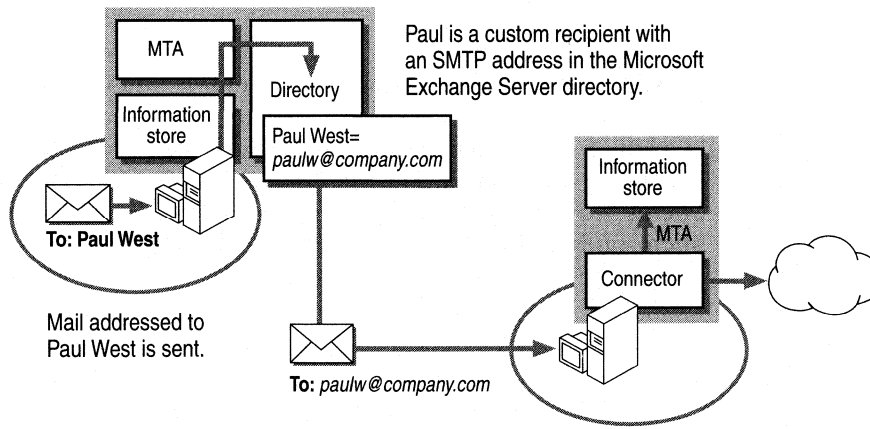
Site and Recipient Addresses

Microsoft Exchange Server creates site addresses by using the organization name and site name provided during Setup. Recipient addresses are created by using site addresses. Both site and recipient addresses are stored in the directory. It is important to ensure you have valid site addresses before adding mailboxes or connectors.

Site and recipient addresses are created for the following address types: MS (MS Mail [PC]), SMTP (Internet), and X400 (X.400). If third-party gateways are installed, other addresses can also be generated.

Microsoft Exchange Server creates a *distinguished name* for every object in the directory, such as a mailbox or distribution list. The distinguished name is used to route messages within a Microsoft Exchange Server organization. If the distinguished name cannot be resolved, the Microsoft Exchange Server uses the X.400 address of the object. It is important to retain the X.400 address for every object in the directory, even if you are not connecting to another X.400 system.

When a message is routed to a custom recipient, the distinguished names of the recipient and originator are replaced with an address of the same type as the recipient. This ensures that the message can be delivered to the foreign system, and that a reply can be routed back to the originator with the correct address type. An illustration of the address conversion follows.



If the recipient is not defined in the Microsoft Exchange Server directory, the address must be in the form required by the foreign system. In this case, only the originator's address is converted to the native format of the foreign system.

For information about viewing and modifying site and recipient addresses, see *Microsoft Exchange Server Operations.*

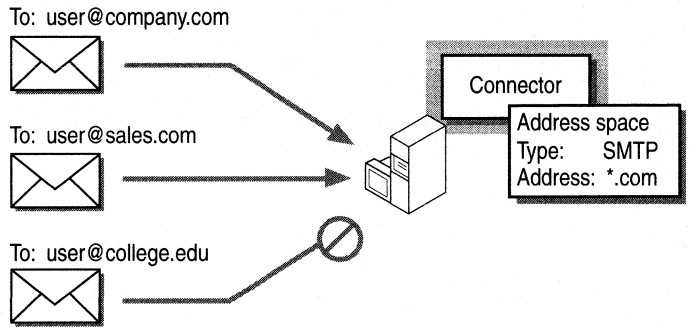
Address Spaces

Microsoft Exchange Server connectors are gateways used to create paths for messages sent outside a site. The following connectors are available with the Microsoft Exchange Server:

Connector	Connects to
Site Connector	Another Microsoft Exchange Server site.
Dynamic RAS Connector	Another Microsoft Exchange Server site.
X.400 Connector	Another Microsoft Exchange Server site or an X.400 system.
Microsoft Mail Connector	Servers running MS Mail.
Internet Mail Service	Another Microsoft Exchange Server or another system using Simple Mail Transfer Protocol (SMTP).
Microsoft Exchange Connector for Lotus cc:Mail	Servers running Lotus cc:Mail.

The *address space* represents the path a connector uses to send messages outside the site, and it identifies the recipient address types and addresses. You can use address spaces to control whether messages from an organization, site, or location can travel through the connector. A connector must have at least one address space.

As shown in the following illustration, Ferguson and Bardell uses the Internet Mail Service to establish a link its West coast Internet service provider (ISP). The Internet Mail Service address space is type SMTP, and the address is *.com. The message transfer agent (MTA) uses this Internet Mail Service to process only SMTP messages addressed to recipients with the .com domain identifier.



For more information about address spaces, see *Microsoft Exchange Server Operations.*

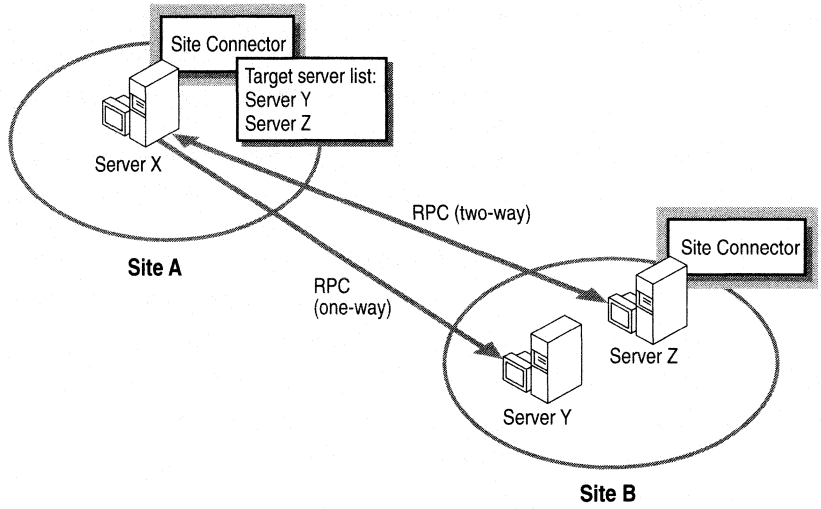
Site Connector

Site Connectors are easy to configure and provide the most efficient way to connect two sites. A Site Connector is a direct connection of a server in a local site with a server in a remote site. Site Connectors are used when you have local area network (LAN) or wide area network (WAN) connectivity between all the servers in the sites.

Site Connectors have a *target servers* list, which contains the names of the servers available in the remote site. When a server in the local site sends a message to a remote site, it establishes a connection to a server on the target servers list. If the first selected server isn't available, the next server is contacted until a connection is made or the list is exhausted. This provides natural fault tolerance.

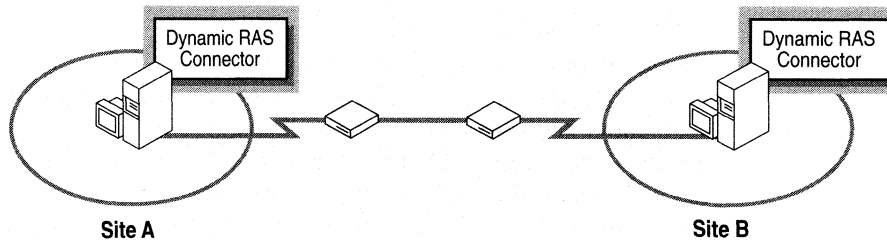
You can assign each server a *cost* to help determine load balancing. For example, suppose you have two servers in the target servers list, one with a cost of 10 and one with a cost of 20. Because the latter server costs twice as much as the other server, it will be used less often.

A Site Connector can have a *bridgehead server*—a server in the local site chosen to establish the connection to the remote site. Using a bridgehead server helps you control which servers send and receive messages between sites.



Dynamic RAS Connector

You can use the Dynamic RAS Connector between Microsoft Exchange Server sites that don't have a permanent connection.



The Dynamic RAS Connector provides an inexpensive way to add remote offices to your messaging system, especially if message traffic is low and the message exchange can be scheduled. This connector is also useful as a backup connection for sites with primary connectors that are unavailable.

Internet Mail Service

You can use the Internet Mail Service to exchange information with other messaging systems that use SMTP, as defined in RFC 821. The message format for Internet Mail is defined in RFC 822 and RFC 1521.

The Internet Mail Service adheres to the following RFCs:

RFC	Description
821	SMTP, which is used to relay Internet mail
822	Defines an Internet message format for carrying a single plain-text body.
1521, 1522	Multipurpose Internet Mail Extensions (MIME). Extends RFC 822 to carry multiple body part, nontextual message bodies and textual information in multiple character sets in the same message.
1123	Internet Hosts Requirements
1566	Simple Network Management Protocol (SNMP)
1869	SMTP Service Extensions (ESMTP)
1870	Size Extension
1891	Delivery Status Notification (DSN)
1985	ETRN

The Internet Mail Service is a Windows NT Server service. You can configure the Internet Mail Service to send mail, receive mail, or do both.

How the Internet Mail Service Works

The following sections describe how the Internet Mail Service works:

Inbound Mail

An SMTP host makes a connection to port 25 on the Internet Mail Service and sends either one or many messages in the same connection. The same sending host and other hosts can create simultaneous connections and transfer many messages in parallel. After the Internet Mail Service accepts a message, it places it in the Exchsrvr\Imcdata\In subdirectory, and then attempts to deliver the message to the Microsoft Exchange Server computer for final delivery by the MTA or information store to the recipients.

The Internet Mail Service verifies the recipients in the Microsoft Exchange Server directory. If the recipients aren't in the Microsoft Exchange Server directory, a non-delivery report (NDR) is returned to the sender. All valid recipients will receive the message.

The Internet Mail Service converts the message to Microsoft Exchange Server format, and the message is placed in the IN folder in the information store of the Internet Mail Service server. The information store delivers the message to the recipients if their mailboxes are on the same server as the Internet Mail Service; the MTA delivers the message if the recipients' mailboxes are on a different server.

An incorrectly formatted Internet message is placed in raw form into an attachment called Message.txt and sent to the recipients. The recipients can use a different viewer to view the message, or save it to disk.

Note The **Accept & Reject Hosts** settings in the **Connections** property page and the **Message Size** settings in the **General** property page can affect inbound mail transfer. You can modify these settings on the Internet Mail Service object by using the Microsoft Exchange Server Administrator program.

Outbound Mail

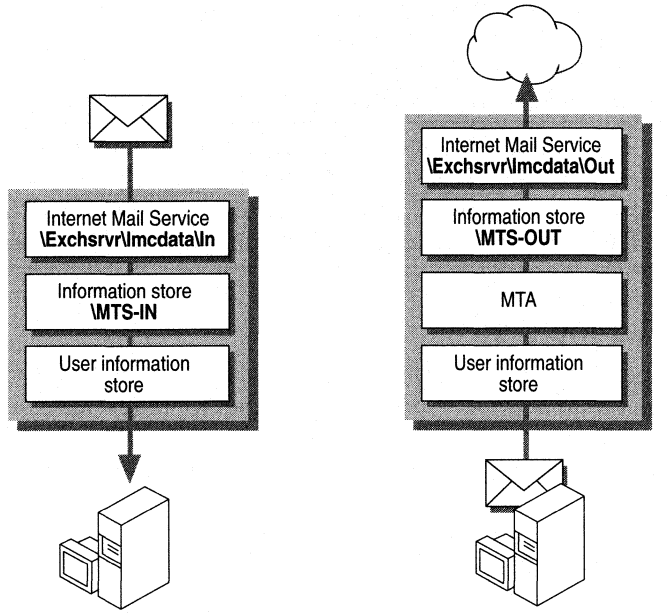
Outbound messages are placed in the OUT folder in the information store of the Internet Mail Service's server. The Internet Mail Service converts the messages into the appropriate Internet mail format based on the e-mail addresses of the recipients. One or many messages can be created, depending on the format choices.

The messages are created in the \Exchsrvr\Imcdata\Out subdirectory. The Internet Mail Service locates the possible destinations for the recipients, opens one or many connections to port 25 on other SMTP hosts, and delivers the message.

The sender receives an NDR if the Internet Mail Service can't convert the message to Internet Mail format or locate an SMTP host to deliver the message to.

Note The following settings can affect outbound mail transfer: the **Message Size** setting in the **General** property page, the **Message Content Information** settings in the **Internet Mail** property page, and the **Message Delivery, Transfer Mode,** and **Connector Message Queues** settings in the **Connections** property page. You can modify these settings on the Internet Mail Service object by using the Microsoft Exchange Server Administrator program.

The following illustration shows how inbound and outbound messages are processed:



Inbound message **Outbound message**

Message tracking provides a record of the inbound and outbound message handling. By default, message tracking is disabled.

Addressing and Routing

SMTP addresses have the following format:

recipient@domain

where *recipient* is the name of a person or other message recipient, and *domain* is the fully qualified domain name (FQDN) of the system that hosts the recipient. This domain name is associated with an Internet protocol (IP) address and is used to route messages between systems.

Most domain names have a hierarchical structure and are divided into subdomains separated by periods, as in this sample address:

franwilson@sanfrancisco.fab.com

In this address, *franwilson* is a local recipient in the *sanfrancisco.fab.com* domain, and *sanfrancisco.fab.com* is a subdomain of *fab.com,* which is a subdomain of *com,* the top-level domain.

The domain name indicates only the administrative organization of the domain; it does not represent a physical connection and gives no indication of the topology of an organization. For example, the domains *sanfrancisco.fab.com* and *newyork.fab.com* are not necessarily connected through a network connection.

Note After installation, always verify your site addressing to ensure that the SMTP address is correct for your organization.

IP Addresses

Each domain is usually identified by a unique IP address that describes the host's physical location. With Microsoft Exchange Server, the IP address used by the Internet Mail Service identifies the server on which the connector is installed.

IP addresses are assigned by the network administrator, or by an Internet service provider who can ensure that each address is unique. For systems that are not connected to the Internet or other networks that use SMTP, IP addresses need only be unique within the local system.

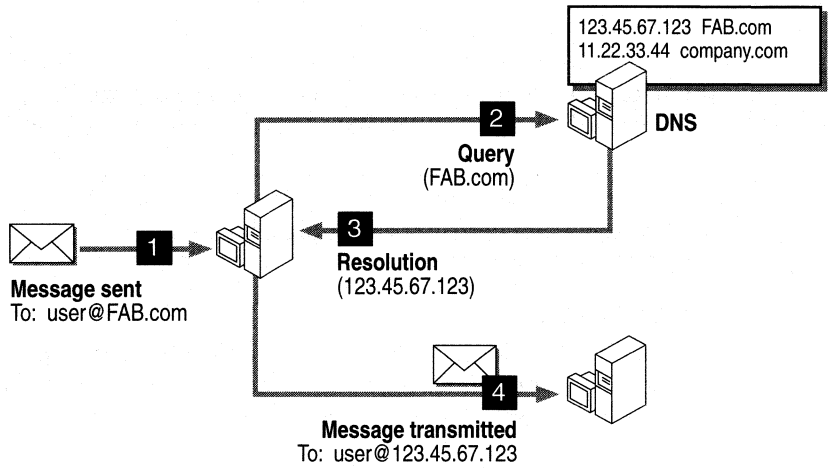
Note The use of Dynamic Host Configuration Protocol (DHCP) is not recommended with the Internet Mail Service unless the lease is permanent.

Using the Internet Mail Service with DNS

A domain name, such as *fab.com,* must have a corresponding IP address, such as 123.45.67.123. The *Domain Name System (DNS)* is commonly used to resolve domain names to the IP addresses that will be receiving mail. DNS is a hierarchical, distributed database that contains information about hosts, name tables, and Internet work addresses. It is found in any Transport Control Protocol/Internet Protocol (TCP/IP) network.

The Internet Mail Service determines where each message should be routed by querying the DNS name server or a local host table. If the sender and the recipient are associated with the same SMTP host (the Internet Mail Service), the message is delivered to the recipient locally.

The following illustration shows how DNS queries are resolved:



Note Names in some DNS name servers, such as those inside a corporation, may not be visible outside the organization.

Each domain receiving Internet mail may have its own DNS name server. Usually primary and backup DNS name servers are used. Your organization may already have a DNS name server, or you may be using an Internet service provider for this service.

If you plan to deliver mail by resolving Internet domain names, you must list in your TCP/IP configuration one or more DNS name servers that are members of the Internet hierarchy. The IP addresses of these servers must be specified in the DNS configuration of TCP/IP in Windows NT Server.

One of the most common implementations of DNS is Berkeley Internet Name Domain (BIND), which runs on UNIX. The following examples in this section use BIND.

If you want a domain name to be accessible from the Internet, a mail exchanger (MX) record must exist to specify how to route mail to that domain.

MX records An MX record is used to point to one or more computers that will process mail for an organization or site. Your domain name may be registered with an MX record. When using Microsoft Exchange Server, if the SMTP site address is different from the host and domain name configured in TCP/IP, you must create an MX record. MX records can help ensure fault tolerance because mail goes to the next MX candidate. They are also used when your mail host name is not the same as the top-level domain.

In the following example of an MX record, the domain name is *fab.com*, and all messages addressed to *user@fab.com* are processed by a host server called Sales.

```
fab.com IN MX 10 sales.fab.com
```

Multiple hosts can be listed, which is helpful when you are using backup computers.

Address (A) records An A record provides the actual IP address of the host computer. The host name and domain name are configured in the DNS configuration of TCP/IP in Windows NT Server. There is usually only one A record per host.

For example, if your domain name is fab.com, your mail host name is Sales, and the host IP address is 123.45.67.123, the A record in DNS would be:

```
sales.fab.com          IN A 123.45.67.123
123.45.67.IN_Addr      IN PTR sales.fab.com
```

Note For faster name resolution, it is common to have an MX defined, even if the A record is the same.

CNAME records A CNAME, or alias, record is optional. It indicates that one computer (IP address) has multiple names. (In this case, it is usually more common to use MX records.) For example, if mail is addressed to business.fab.com, but is processed by sales.fab.com, business is an alias of sales, and the CNAME record would be:

```
business.fab.com IN CNAME sales.fab.com
```

Note In addition to the A record, when adding another Microsoft Exchange Server computer to the DNS, you must add an IN-ADDR (reverse lookup) record. Other host computers can locate the computer's IP address to determine the name of the system.

Using the Internet Mail Service Without DNS

You can use the Internet Mail Service without installing DNS. To do so, update the Windows NT Server Hosts file with the IP address and domain name of all hosts to which the Internet Mail Service should transfer messages.

You also need to add the domain name and IP address of the Internet Mail Service server to the Hosts file or DNS of all SMTP servers that forward mail to the Internet Mail Service.

A sample Hosts file can be found in the Windows NT Server system directory under Drivers\Etc. The following is an example of a Hosts file:

```
123.45.67.123        sales.fab.com
11.22.33.44          company.com      sales.company.com
```

Internet Mail Formats

The Internet Mail Service formats outbound messages according to RFC 822. This RFC assumes that the message body consists of 7-bit ASCII characters and that the lines in the message body do not exceed 1,000 characters.

However, many people now send messages that contain rich text, such as bold and italic formatting, documents and spreadsheet attachments, images, audio, and video. Because most of these types of data are in binary format, specific mechanisms for conveying this data in messages are required.

The Internet Mail Service supports the following mechanisms for sending binary data in Internet mail.

Multipurpose Internet Mail Extensions (MIME)

MIME is the standard for exchanging multimedia messages on the Internet. MIME describes the contents of a particular type of data so that the receiving system can display the data accordingly. For example, suppose that a message includes an attachment created in Microsoft Word. When the message is sent, the Internet Mail Service can tag the data as being of type application/msword so that the recipient can view the contents of the attachment by using Microsoft Word.

MIME specifies seven major content types. Each content type can have many subtypes to further specify the content of data.

Primary Type	Description
Text	Content that is primarily textual and probably can be read in raw form
Application	Content that doesn't fit into any of the other categories
Multipart	Message made up of multiple parts, such as both text and an application
Image	Pictures
Audio	Sounds
Video	Moving images
Message	Common when dealing with embedded messages or delivery reports such as NDRs or Read Receipts

File attachments from an Apple Macintosh® computer will be mapped to MIME-standard body parts so that MIME-compliant clients and gateways can decode these attachments. Additionally, the Internet Mail Service maps any incoming body parts to Windows or Macintosh file types.

Uuencode and Uudecode

Uuencode and uudecode are tools that prepare binary files for transport between UNIX systems. Uuencode is used extensively to encode non–7-bit data in messages. When the message is received at the destination, the encoded data must be decoded by uudecode. The Internet Mail Service automatically encodes data in outbound messages and decodes parts in incoming messages.

Microsoft Exchange Server Rich Text Formatting

Although Internet mail provides extremely rich formatting capabilities for communicating data, certain types of information are not communicated well, such as positional information for attachments and OLE objects as attachments. These limitations can be overcome when communicating with other Messaging Application Programming Interface (MAPI)-based systems by sending Microsoft Exchange Server rich text formatting information in Internet mail. The receiving system, if MAPI-capable, can reconstruct the message as if it were sent between two Microsoft Exchange Server recipients on the same server, preserving all the positional information and data.

Either MIME or uuencode can be used when sending Microsoft Exchange Server rich text formatting in Internet mail.

Choosing a Formatting Method

When configuring the Internet Mail Service, you can choose whether attachments should be encoded through MIME or uuencode by default, and whether Microsoft Exchange Server rich text formatting should be used. These settings can also be specified on a per e-mail domain basis. When composing a message, users can override the option to encode attachments through MIME or uuencode. To override this option, Send Options for Internet is used.

Note Users can also indicate whether Microsoft Exchange Server rich text formatting should be sent on a per-recipient basis. The administrator can also indicate whether a custom recipient should be sent Microsoft Exchange Server rich text formatting. The default or per e-mail domain setting for rich text formatting should be set to **User** for this to work.

Dial-up Options

You can use the Internet Mail Service with the Windows NT Remote Access Service (RAS) to connect to another site or Internet service provider. You specify how frequently the connection is established and how long the connection to the site or provider remains open.

Your Internet service provider may require a command that identifies you and notifies you that you are ready to receive messages. When the connection is established, you can specify a command, such as a ping command, to run on the local computer.

Microsoft Exchange Server supports the use of an SMTP extension called ETRN. After the client host submits the ETRN command to the server host, a new connection is established from the server host to the client host. This validates the identity of the client host.

For more information about using ETRN, see Chapter 9, "Planning Connections to Other Sites and Systems." Additional information is also available in *Microsoft Exchange Server Operations* and RFC 1985, "SMTP Service Extension for Remote Message Queue Starting."

Routing Internet Mail

The Internet Mail Service can intercept and selectively reroute inbound messages from SMTP hosts, Post Office Protocol version 3 (POP3) clients, and Internet Message Access Protocol, Version 4rev1 (IMAP4rev1) clients. These messages are selectively rerouted to other SMTP hosts before they are processed by the Internet Mail Service. You can use the **Routing** property page to enable the Internet Mail Service to act as a smart host that can route messages between the Internet and other SMTP hosts without the need to define custom recipients. If mail from POP3 clients is to be routed to recipients outside the Microsoft Exchange Server organization, you must configure the Internet Mail Service to reroute mail.

If your organization uses multiple SMTP hosts, you can use the **Routing** property page to designate the Internet Mail Service as the single point of contact to the Internet. Other SMTP hosts can be configured to forward all messages to the Internet Mail Service, where the **Routing** property page has been configured to route messages appropriately.

The **Routing** property page contains a list of domain names and associated SMTP hosts. For each recipient of every inbound message the Internet Mail Service receives, the **Routing** property page compares the domain name on the address to the list of domain names in the **Routing** property page. If a match is found, the message for that particular recipient is rerouted to the associated host.

The match is compared to the rightmost part of the domain name in the recipient address. Only full subdomains are compared. For example, if the domain name in the table is sea.com, it matches an address of x.sea.com as well as sea.com, but not chelsea.com. The list is searched from the most specific match to the least specific match. For example, user@x.sea.com would match x.sea.com, sea.com, or .com. However, if x.sea.com is in the list, it is used because it is the most specific match. This occurs regardless of its placement in the list.

In cases where the associated SMTP host is set for **<inbound>**, domain names in the list represent names that should be handled by the Internet Mail Service. If the recipient address matches one of these domain names, the Internet Mail Service processes the recipient normally and attempts to deliver the message to the Microsoft Exchange Server. If no match is found, the Internet Mail Service reroutes the message outbound to the domain name in the recipient's address. For this reason, it is important to ensure that any domain names that must be routed to the Microsoft Exchange Server are listed in the **Routing** property page. In particular, any domain names used in SMTP addresses for Microsoft Exchange users must be defined in the **Routing** property page. Otherwise, reports and replies will not be deliverable and could cause routing loops.

For more information on using the **Routing** property page, see *Microsoft Exchange Server Operations.*

Message Tracking

Messages sent to and from Microsoft Exchange Server can be tracked to determine the cause of mail-related problems. You can:

- Track messages to locate slow or stopped connections.
- Find unaccounted mail.
- Track an unauthorized message and remove it from the system.

When message tracking is enabled, each component handling mail records its activities in a log maintained by the system attendant on each server. The log becomes a trace of the processing of each message as each component receives, processes, and delivers it to the next component. The tracking logs are stored in Exchsrvr\Tracking.log.

How a Message Is Tracked

When a message is passed from a client to the Internet, multiple events are logged into the tracking log. Each log records one day's activities on the server. The tracking log can be displayed by using the Microsoft Exchange Server Message Tracking Center.

The following table describes the Internet Mail Service activity in the tracking logs:

Field Name	Description
SMTP transfer out	The message is received by the Internet Mail Service from the Microsoft Exchange Server information store.
SMTP inbound received	The message is received by the Internet Mail Service from the Internet.
SMTP transfer in	The message is received by the Microsoft Exchange Server information store from the Internet Mail Service.
SMTP message rerouted	The message was received by the Internet Mail Service and rerouted to another domain. For information on rerouting, see "Routing Properties" earlier in this chapter.

For more information about message tracking, see *Microsoft Exchange Server Operations.*

ESMTP

The Internet Mail Service supports SMTP Service Extensions (ESMTP). ESMTP is an extension to SMTP that defines a means whereby an SMTP server can inform an SMTP client of the extensions it supports. ESMTP does not require modification of existing SMTP client or server configuration.

For more information on ESMTP, see RFC 1869, "SMTP Service Extensions."

How ESMTP Works

An SMTP client supporting ESMTP starts an SMTP session by issuing the **EHLO** command instead of the **HELO** command. A successful response issues a list of SMTP extensions that the server supports. If the server does not support ESMTP, an error response is generated.

The following is an example of a successful response to the **EHLO** command from the server abc.def.ghi.com as requested by the client rst.uvw.xyz.com. The server supports the SMTP Delivery Status Notification (DSN) and Size of the Message (SIZE) commands.

```
Server: 250 XVR
Server: <wait for connection on TCP port 25>
Client: <open connection to server>
Server: 220 abc.def.ghi.com SMTP service ready
Client: EHLO rst.uvw.xyz.com
Server: 250- abc.def.ghi.com says hello
Server: 250-DSN
Server: 250-SIZE
Server: 250-Xauth
Server: 250-Xexch50
```

For more information on ESMTP, see RFC 1869, "SMTP Service Extensions" and RFC 1870, "SMTP Service Extension for Message Size Declaration."

X.400 Connector

You can use the X.400 Connector to establish an X.400 messaging route between two Microsoft Exchange Server sites or between a Microsoft Exchange Server site and a foreign X.400 system. An X.400 messaging route defines the path that an X.400 message follows to reach its destination. It enables the MTAs in both sites or systems to communicate. A foreign X.400 system is a messaging system other than Microsoft Exchange Server that complies with the 1984 or 1988 X.400 standards.

Understanding X.400

The X.400 Recommendations define the standards of an electronic messaging system and enables users to exchange messages regardless of the system.

The X.400 Recommendations were developed by an organization known as the Comité Consultatif International Télégraphique et Téléphonic (CCITT). The CCITT publishes recommendations every four years. Each publication is identified by a color:

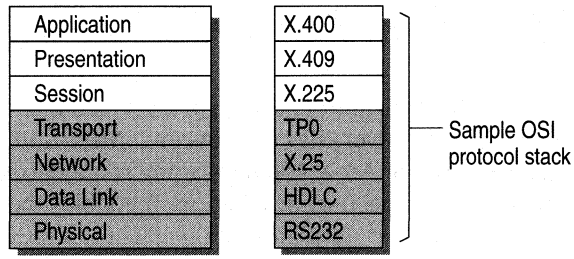
- 1984 - Red Book
- 1988 - Blue Book
- 1992 - White Book

The Electronic Messaging Association (EMA), which includes private e-mail software development companies, develops specifications for e-mail software development. The EMA publishes standards that further define the X.400 Recommendations.

The X.400 Recommendations are based on the Open Systems Interconnection (OSI) reference model defined by the International Organization for Standardization (ISO). The X.400 Recommendations specify the structure of a message handling system, message structure and components, and the method used to transfer messages. Microsoft Exchange Server complies with the 1984 and 1988 X.400 Recommendations.

The OSI reference model provides a layered architecture that standardizes the method computers use to exchange information through a communications network. The OSI model separates computer-to-computer communications into seven layers: application, presentation, session, transport, network, data link, and physical. The top three layers usually relate to the operating system and applications that run on it. The other layers determine the way networks interconnect.

The following diagram illustrates the seven OSI layers and examples of the protocols and standards that are used in each layer:



Using the OSI model, an administrator can choose the physical network, the protocols and transports transmitted over the network, and the software and hardware used on each end of the connection. As long as each layer receives and transmits information correctly to the layers above and below, it doesn't matter what combination of hardware and software is used in each layer.

X.400 runs on the application layer of the OSI model. This enables application processes to access network services. X.400 represents services that support user applications, such as software for file transfers, database access, and e-mail.

X.400 Message Handling System

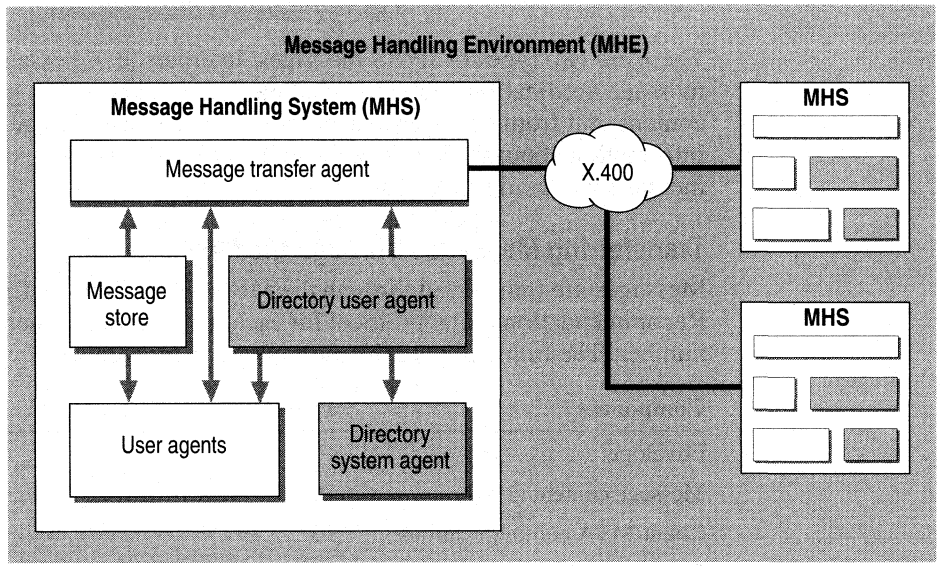
An X.400 message handling system (MHS) is a collection of components that work together to transfer messages. The X.400 Recommendations specify that an MHS should have the following components.

Component	Description
User agent (UA)	Prepares, submits, and receives messages for a user. Displays messages and provides other functions, such as text editing and security.
MTA	Forwards and relays messages within the network.
Message transfer system (MTS)	Two or more MTAs.
Message store (MS)	Stores messages transferred between MTAs and user agents (1988 Recommendations only). Known as the information store in Microsoft Exchange Server.
Access unit (AU)	Gateway to other messaging systems.

The set of message handling system components and users is called a message handling environment (MHE). An MHE can include several messaging systems connected through gateways or public data networks, or just one message handling system where messages are contained within the system.

An X.400 MHS usually works with directory services, including the directory user agent and directory system agent. Directory services are not part of the X.400 Recommendations, but the 1988 X.400 Recommendations allow the use of directory services. The directory is a database of all objects in the message handling system, such as mailboxes and distribution lists.

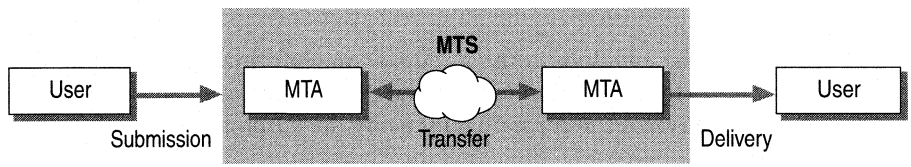
The following diagram illustrates how the components of the MHS work together to transfer messages:



The user agents and message transfer agents in the MHS form the message transfer system (MTS) and the interpersonal messaging service (IPMS).

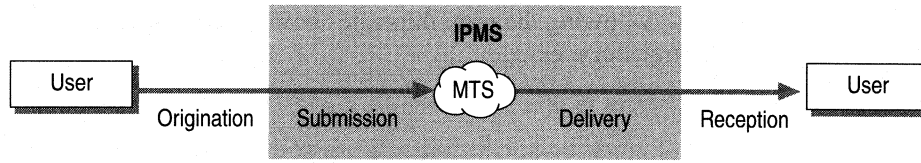
The MTS is a collection of one or more MTAs that submit, transfer, and deliver messages through the MHS. The MTS is the infrastructure of message handling.

In the following example, a user agent submits a message to the MTA within the MTS for delivery to one or more MTS users. The MTS accepts the message and provides any necessary store and forward features, such as distributing the message to more than one recipient. The MTA then routes and delivers the message.



The IPMS enables messages to be exchanged from person to person. When a message is sent from one user to another, the IPMS invokes the services of the underlying MTS to submit and deliver the message to its destination.

The following illustration shows how the MTS functions within the IPMS:



There are two types of IPMS messages: interpersonal messages and interpersonal message notifications. Interpersonal messages contain text, graphics, or other content sent from one user to another. Interpersonal message notifications contain information about the status of the delivery of the message, or whether the message was read or not read.

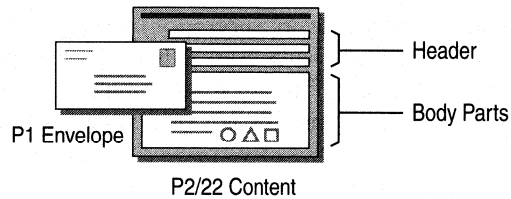
Transferring Messages Through the MHS

Messages are transferred through the MHS by protocols defined in the X.400 Recommendations. The protocol for each message component is assigned a number. The following are the most common protocols:

Component	Protocol
Envelope	P1
Message content (1984)	P2
Client-MTA communications	P3
Client-message store	P7
Message content (1988)	P22

Message Components

An X.400 message has two components: an envelope and its content.



The envelope contains addressing information, including the address of the originator and recipient, the delivery priority, and message trace information. The envelope is formatted by using the P1 protocol.

Most X.400 messages are made up of one or more *body parts,* together with *header* information. The body parts make up the text of the message. The header contains address, routing, and trace information, and determines how the message is transported.

The X.400 body contains the actual message, which can include text, graphics, sound, or other kinds of data. The X.400 Recommendations specify standards for different types of content in body parts. Body parts are referred to by body part numbers.

The following table shows the X.400 body part types and numbers that can be used with Microsoft Exchange Server:

Body Part Type	Body Part Number	Description
IA5 text	BP 0	International alphabet number 5. Includes U.S. English, German, Norwegian, and Swedish.
Teletex 61	BP 5	U.S. English teletex.
Forwarded interpersonal message	BP 9	Embedded and forwarded messages.
ISO 6937 text	BP 13	Eastern Europe and German characters.
Bilaterally defined (binary)	BP 14	Simple transfer of binary attachments.
Binary file transfer (file transfer body part [FTBP])	BP 15 FTBP	Transfer of attachments using FTBP, which includes file name, size, and properties. Available for MTA conformance modes only.
ISO 8859-1	Encapsulated within BP 15	Latin 1 code page. Available for MTA conformance modes only.

The header fields contain information such as the message originator, recipients, and expiration time, which is useful for tracing messages and troubleshooting. Microsoft Exchange Server uses the following header fields:

Field	Description
originator	Originator/recipient (O/R) address of originator.
authorizing-users	O/R addresses of **send on behalf of.**
primary-recipients	Recipients specified on the **To** line.
copy-recipients	Recipients specified on **Cc** line.
blind-copy-recipients	Recipients specified on **Bcc** line.
expiry-time	Message is deleted if it is not read by the specified time.
deferred-delivery-time	Message is sent at the specified time.
subject	Up to 128 characters (truncated from up to 255 characters). Sent using Teletex T.61.
importance	Low, medium, or high.
sensitivity	Low, medium, or high.

Microsoft Exchange Server Content Options

To ensure that messages are transferred correctly, it is important to understand how Microsoft Exchange Server implements X.400 content options. The options you use depend upon the X.400 system you connect to.

To specify content options in the X.400 Connector, you use the **Advanced** property page in the Microsoft Exchange Server Administrator program. When you configure for 1984 MTA conformance, text content is sent using the P2 protocol, and attachments are sent using BP 14. When you configure for 1988 MTA conformance, text content is sent using the P22 protocol, and you can configure the server to send attachments using either BP 14 or BP 15 (FTBP).

In addition to the P2 and P22 content types, Microsoft Exchange Server provides a third message content type called message database encoding format (MDBEF). MDBEF is the format used by the Microsoft Exchange Server information store. Using MDBEF with an X.400 Connector between two Microsoft Exchange Server sites provides faster throughput because messages do not have to be converted to P2/22 and then back to MDBEF. To send messages using MDBEF content, select the **Allow Microsoft Exchange contents** check box under **X.400 link options** in the X.400 **Advanced** property page. The Microsoft Exchange Server computers must be replicated to transmit messages in MDBEF format.

Messages that contain MAPI properties, such as rich text formatting and OLE attachments, are encapsulated using the transport-neutral encapsulation format (TNEF) and sent as an X.400 attachment. If the receiving system can process the TNEF attachment, the message is displayed with the rich text formatting or icon representation. If the receiving system cannot process TNEF or MAPI attachments, the message text and attachments may not be readable.

The Microsoft Exchange Server MTA is capable of relaying messages from a 1988 X.400 link to a 1984 X.400 link and vice versa. However, when the Microsoft Exchange Server MTA relays a 1988 body part that is not supported by a 1984 X.400 system, the message content appears blank on the receiving system. For example, ISO 8859-1 is a 1988 body part that is not supported on a 1984 link. The Microsoft Exchange Server relay MTA is connected to a system on the 1988 link that supports ISO 8859-1 and to a system on the 1984 link that supports IA5. The Microsoft Exchange Server relay MTA cannot convert ISO 8859-1 to a supported 1984 body part such as IA5. You can use the **Convert incoming messages to MS Exchange contents** option in the relay MTA **General** property page to convert the content to MDBEF. The content can then be converted to the P2 format of the receiving system connected by the 1984 link.

X.400 Addressing

A management domain is a set of messaging systems managed by an organization that contains at least one MTA. The management domain is divided into two parts: an administrative management domain (ADMD) and a private management domain (PRMD).

An ADMD is managed by a public service provider and is the highest level management domain that transmits third-party message traffic. The service is usually provided by a telephone carrier such as Sprint, AT&T, or British Telecom.

A PRMD is a network owned by a private company. PRMDs can communicate with ADMDs and other PRMDs but are not permitted to relay messages between PRMDs.

The ADMD and PRMD structure is similar to that of the telephone system. An ADMD can be compared with a telephone carrier that provides your phone service. The service is leased from the ADMD in the form of a PRMD. This is similar to the way in which a telephone line is assigned. The PRMD has a unique network address that can have multiple users.

Originator/Recipient (O/R) Addresses

Users of an MTS are identified by an O/R name. The O/R name is included on the P1 envelope and is used by the MTS to route and deliver messages.

Microsoft Exchange Server automatically creates X.400 addresses for every mailbox based on the site and organization name you specify during Setup. It is important to understand the elements of O/R addresses to modify the site address, create custom-recipient addresses, and specify the addresses of other X.400 systems in the X.400 Connector configuration.

The O/R address consists of required and optional fields containing attributes and values. The attributes necessary for a valid address vary depending on the recipient system. Not all attributes are required for delivery in an X.400 system. After the correct attributes are identified, the attribute and its value are combined in an address format with an equal sign (=) separating the two. A delimiter is added between fields for parsing. X.400 fields can be separated by a semicolon (;) or a slash (/). Different systems can require different delimiters.

You can use either the abbreviation or the label to identify an attribute. The following table shows valid abbreviations and labels, as well as the maximum length allowed for the value. The domain-defined attribute (DDA) field is case sensitive; the other attributes are not.

Attribute Type	Abbreviation	Label	Maximum Characters
Given name	Given name	G	16
Initials	Initials	I	5
Surname	Surname	S	40
Generation qualifier	Generation	Q	3
Common name	Common name	CN	32
X.121 address	X.121	X.121	15
User agent numeric ID	N-ID	N-ID	32
Terminal type	T-TY	T-TY	3
Terminal identifier	T-ID	T-ID	24
Organization	Organization	O	64
Organizational unit 1	Org.Unit.1	OU1	32
Organizational unit 2	Org.Unit.2	OU2	32
Organizational unit 3	Org.Unit.3	OU3	32
Organizational unit 4	Org.Unit.4	OU4	32
Private management domain name	PRMD	P	16
Administrative management domain name	ADMD	A	16
Country	Country	C	2
Domain-defined attribute	DDA	DDA	8,128

DDA uses the format *DDA:type=value*; for example, DDA:SMTP=MariaBlack@fab.com. There may be up to four DDAs in a single X.400 address. DDAs are order dependent. When parsing from left to right, the first DDA is encoded first, the second DDA is encoded second, and so on.

With the exception of *DDA,* the format for the fields is *Label=Value;* for example, g=Joe.

The following are examples of valid X.400 addresses using labels and different delimiters:

C=US;A=MCI;P=MSFT;S=EMAIL

C=US;ADMD=MCI;PRMD=FAB;S=EMAIL

C=US/ADMD=MCI/PRMD=FAB/S=EMAIL

C=US;A=TELEMAIL;P=MMC;O=SALES;OU1=INSIDE;S=LAST;G=FIRST

C=US;ADMD=TELEMAIL;PRMD=MMC;O=SALES;OU1=INSIDE;S=LAST;G=FIRST

C=US/A=TELEMAIL/P=MMC/O=SALES/OU1=INSIDE/S=LAST/G=FIRST

C=US/ADMD=TELEMAIL/PRMD=MMC/O=SALES/OU1=INSIDE/S=LAST/G=FIRST

X.400 Addresses in Microsoft Exchange Server

An X.400 address is created by providing the value for all required attributes and any optional attributes until a unique address is formed. The following table illustrates the required and optional attributes that can be used to create a mnemonic X.400 address with Microsoft Exchange Server. All attribute values can contain numeric or alphanumeric characters.

Attribute	Comments
Personal name	Includes Given Name, Initials, Surname, and Generation. If the Personal Name attributes are used, the Surname is required.
Common name	Optional.
Organization	Optional.
Organizational units	Optional.
PRMD	Optional.
ADMD	Required. A single blank character can be used in the ADMD field to indicate that no ADMD is specified.
Country	Required.
DDAs	Optional.

Note At least one of the Personal Name, Common Name, Organization, Organizational Units, or PRMD attributes must be used in addition to ADMD and Country. If a DDA is used, you still must specify one of the other optional fields.

Microsoft Exchange Server can use X.121 addresses in the X.400 environment. X.121 is a standard universal addressing scheme for public data networks. The following table illustrates the required and optional attributes that can be used to create an X.121 address with Microsoft Exchange Server. All attribute values can contain numeric or alphanumeric characters.

Attribute	Comments
X.121 address	Required.
PRMD	Required only for 1988 X.400 compatibility.
ADMD	Required. A single blank character can be used in the ADMD field to indicate that no ADMD is specified.
Country	Required.
DDAs	Optional.

For more information about X.400 address attributes, see *Microsoft Exchange Server Operations.*

Global Domain Identifier

Microsoft Exchange Server uses the X.400 global domain identifier in a relay environment. The global domain identifier consists of the country, ADMD, and PRMD name of the remote MTA. It is used for inserting trace elements and can be used for troubleshooting an unsuccessful relay attempt. It is also used to prevent message looping in wide-area messaging environments.

If you are using a public X.400 network as a backbone between two Microsoft Exchange Servers, messages may not be routed correctly if the global domain identifier used for Microsoft Exchange Server is the same as the global domain identifier of a connected foreign system.

Microsoft Mail Connector for PC Networks

You can exchange messages between Microsoft Exchange Server and one or more MS Mail (PC) systems by using the Microsoft Mail Connector over LAN, asynchronous, or X.25 connections.

The Microsoft Mail Connector (PC) contains the following components that work together to transfer messages:

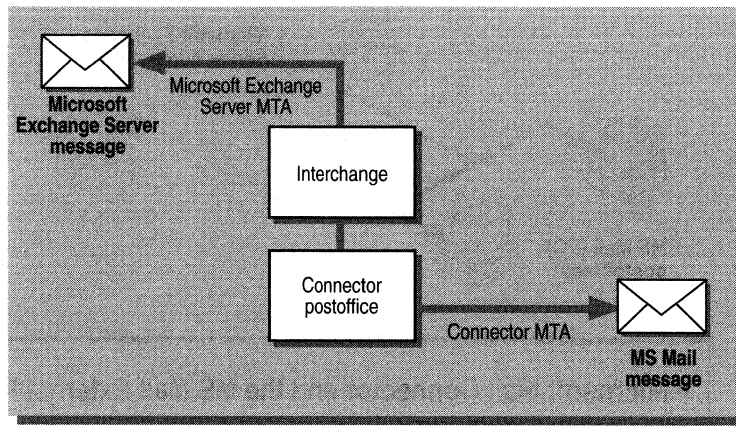
Microsoft Mail Connector interchange A Windows NT Server service that routes and transfers messages between Microsoft Exchange Server and the Microsoft Mail Connector postoffice.

Microsoft Mail Connector postoffice A temporary information store for messages in transit. This postoffice is sometimes referred to as a *gateway postoffice* or *shadow postoffice* because it is dedicated to message transfer and has no local mailboxes.

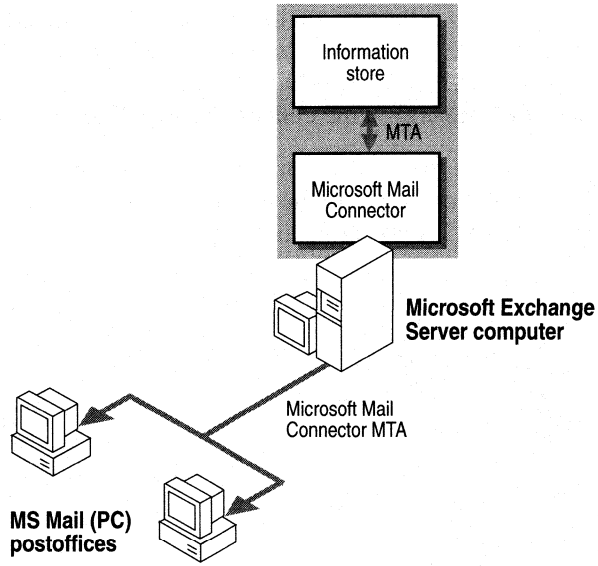
Microsoft Mail Connector (PC) MTA A Windows NT Server service that connects to and transfers mail between the Microsoft Mail Connector postoffice and one or more MS Mail (PC) postoffices.

When a message is submitted to the Microsoft Exchange Server MTA for an MS Mail recipient, it is transferred to the connector interchange. The connector interchange converts it to MS Mail format, converts attachments as needed, and then places the message in the connector postoffice.

Messages destined for an MS Mail postoffice available over a LAN connection are picked up and delivered to the destination postoffice by a Microsoft Mail Connector (PC) MTA, as shown in the following illustration.



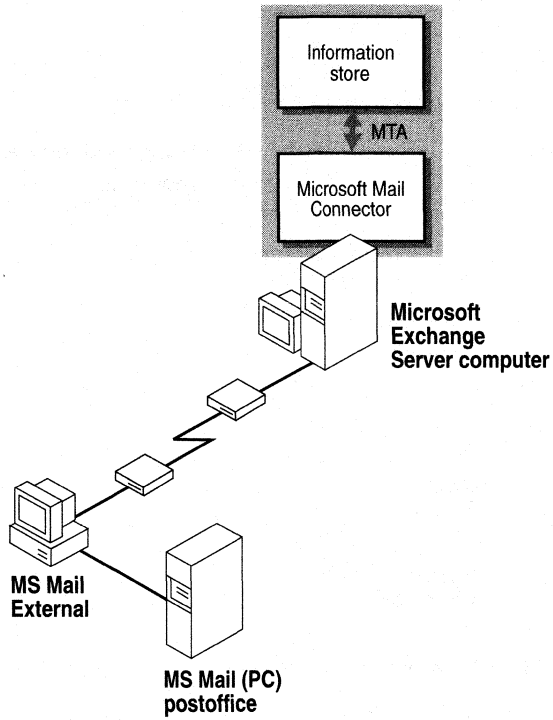
For example, when connecting to an MS Mail postoffice on the same LAN, you can configure the Microsoft Mail Connector to receive messages from the Microsoft Exchange Server MTA, convert the message to MS Mail format, and deliver it to the destination postoffice by using the Microsoft Mail Connector MTA.



Microsoft Mail Connector and the MS Mail External Program

The Microsoft Mail Connector combines the functions of a gateway postoffice and External MTA program. The Microsoft Mail Connector MTA component of the Microsoft Mail Connector can perform most functions of the MS Mail External MTA and Multitasking MTA programs, including message delivery and distribution to recipients on MS Mail postoffices on the same LAN. In certain cases (when migrating from MS Mail (PC), for example), you may want an existing MS Mail External or Multitasking MTA to continue performing some of the functions provided by the Microsoft Mail Connector. Although the MS Mail External and Multitasking MTA programs do not provide the advanced features of the Microsoft Mail Connector, you can integrate the Microsoft Mail Connector into any MS Mail system by using existing External and Multitasking MTA programs. If you have remote clients within your MS Mail system, you must maintain an instance of the External program. All mail transmission between a remote client and an MS Mail postoffice is processed by the External MTA program and cannot be replaced by the Microsoft Mail Connector.

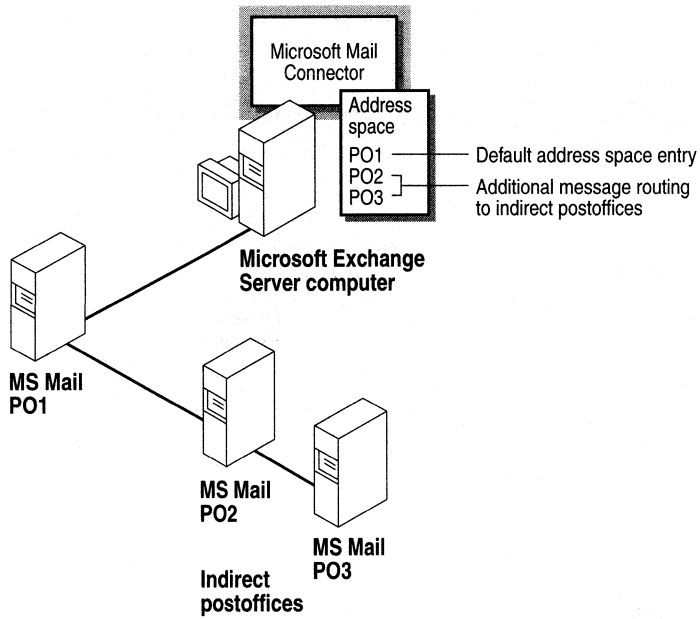
When connecting to an MS Mail postoffice over asynchronous or X.25 service, you must set up an instance of the MS Mail External (or Multitasking MTA) at the remote postoffice, because message delivery and distribution to an MS Mail postoffice can be performed only over a LAN connection.



LAN Connection to Existing Postoffices

The simplest type of connection between Microsoft Exchange Server and MS Mail (PC) can be set up when both systems reside on the same LAN. You can set up most of the message transfer and routing information from the Administrator program.

The following illustration shows how the Microsoft Mail Connector address space can be configured to include indirect postoffice routing to indirect MS Mail postoffices:



Creating this type of connection involves:

- Configuring the Microsoft Mail Connector interchange.
- Defining a connection to the directly connected MS Mail postoffice.
- Setting up a single connector MTA instance for LAN service.
- Configuring message routing to Microsoft Exchange Server on each MS Mail postoffice.
- Adding the network and postoffice names of each indirect MS Mail postoffice to the address space of the direct connection.

When you have configured this connection, messages for any postoffice listed in the address space are sent to the directly connected postoffice and then transmitted to the destination postoffice.

You must define each external MS Mail postoffice that you want to communicate with. For some messaging systems, you may have to work harder to ensure that the network and postoffice routing information is correct for each postoffice. The Microsoft Mail Connector, however, can automatically extract indirect routing information from an MS Mail postoffice, so that you don't have to manually configure routing information for an MS Mail postoffice connected indirectly (regardless of LAN, asynchronous, or X.25 connection) through a directly connected MS Mail postoffice.

Automatic uploading of routing information from an MS Mail postoffice requires a LAN connection. If you are connecting to an MS Mail postoffice through an asynchronous or X.25 connection, all indirect routing information must be entered manually through the Microsoft Mail Connector property pages.

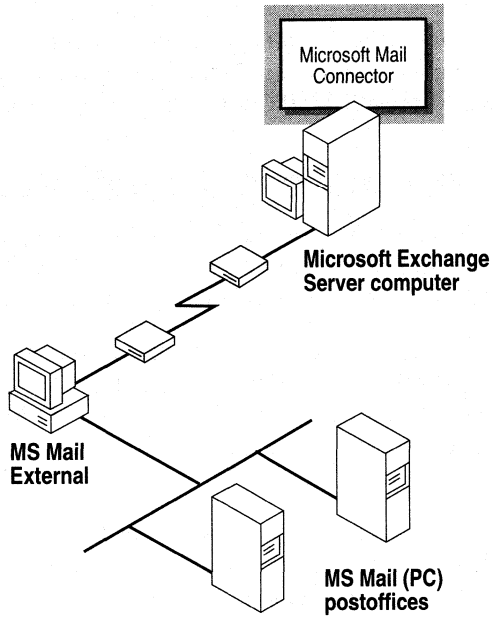
Asynchronous and X.25 Connections for Remote Postoffices

Messages destined for an MS Mail postoffice available over an asynchronous or X.25 connection are retrieved by a connector MTA and delivered to the External or Multitasking MTA program that services the destination postoffice.

If the message is not retrieved by any instance of the connector MTA, it remains in the connector postoffice until it is retrieved by a LAN-connected instance of the MS Mail External or Multitasking MTA program or an MS Mail gateway installed on the connector postoffice. Otherwise, the message expires and returns to the sender.

The type of connection between indirect postoffices has no effect on message routing. However, if you want to set up a direct asynchronous or X.25 connection between the Microsoft Mail Connector and an MS Mail postoffice, you must set up an instance of the MS Mail External or Multitasking MTA program on the same LAN as the MS Mail postoffice. This program must be configured to connect over asynchronous or X.25 connections and typically requires a dedicated computer.

The following illustration shows how the External program is used when connecting a remote MS Mail postoffice to a Microsoft Exchange Server computer across an asynchronous connection:



The External or Multitasking MTA program provides the message transfer and modem management functions necessary to communicate over a remote connection. To create this type of connection, you must:

- Configure the Microsoft Mail Connector interchange.
- Define a connection to the MS Mail postoffice.
- Set up a single connector MTA instance for asynchronous service.
- Set up the External or Multitasking MTA program on MS Mail.
- Configure message routing to Microsoft Exchange Server from MS Mail.

In many cases, you can set up this type of connection to integrate Microsoft Exchange Server with an existing MS Mail system without making significant changes to the configuration.

Using Multiple Microsoft Mail Connector (PC) MTAs

Microsoft Mail Connector (PC) MTA instances perform differently depending on the type of connection they service. For example, if you set up a connector MTA instance to service only LAN-connected postoffices, you can select which MS Mail postoffices you want serviced and configure various message handling options for both the MTA and each postoffice. If you set up a connector MTA instance to service asynchronously connected postoffices, it automatically services every asynchronous postoffice you connect to from that Microsoft Mail Connector.

More about Microsoft Mail Connector (PC) MTAs

When you configure the Microsoft Mail Connector, you create instances of the connector MTA. Each instance is named and registered as a Windows NT Server service on the Microsoft Exchange Server computer on which it was created. Each instance can be started or stopped independently of any other service.

Each instance of the connector MTA services one primary type of connection, such as a LAN, asynchronous, or X.25 connection. You should set up as many connector MTA instances as you need to provide connectivity to your MS Mail postoffices. Although every instance of the connector MTAs can service LAN-connected postoffices if necessary, you should group postoffices by the type of connection and then create a separate instance of the connector MTA to service each group. This optimizes performance when you have multiple LAN, asynchronous, and X.25 connections. For example, if there are only a few MS Mail postoffices on the same LAN compared with the number of postoffices with asynchronous connections, you can set up a single connector MTA for asynchronous and LAN connections and then add the LAN-connected postoffices to the list of postoffices serviced by that connector MTA. However, if you have several LAN connections, it is more efficient to set up two instances of the connector MTA: one to service LAN connections, and one to service asynchronous connections.

Using Multiple Microsoft Mail Connectors

If there are many MS Mail postoffices within your organization, or multiple MS Mail postoffices spread over a large area, you can set up multiple Microsoft Mail Connectors to connect all MS Mail and Microsoft Exchange Server users.

Note Every server in a site uses the same MS Mail e-mail address. From the MS Mail perspective, each Microsoft Exchange Server site appears as one large MS Mail postoffice, regardless of the number of servers or recipients in that site. If multiple connections are required, you should set up a Microsoft Mail Connector in each site.

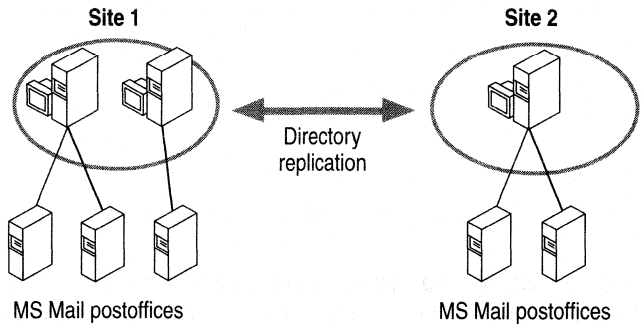
When planning multiple outgoing routes from one or more Microsoft Mail Connectors to MS Mail, you should:

- Install a Microsoft Mail Connector on any or all Microsoft Exchange Server computers in your site.
- Use identical address information in the **Address Space** property pages of two or more Microsoft Mail Connectors to route messages.

After a route through a Microsoft Mail Connector is selected, the message is transferred to the connector postoffice and placed in an outgoing connector MTA queue. If the connector MTA stops running or can't deliver the message, the message remains in the queue until the connection is reestablished or until the message expires.

Using Microsoft Exchange Server as a Backbone to MS Mail (PC)

You can connect two or more MS Mail postoffices by using Microsoft Exchange Server with the Microsoft Mail Connector, as shown in the following illustration:



This type of connection can be used to connect individual postoffices or to connect two or more MS Mail sites into one messaging system. To create this type of connection, you need to:

- Set up message transfer from each site to an MS Mail postoffice, as shown in the illustration.
- Verify that messages are correctly routed through the Microsoft Mail Connector between each Microsoft Exchange Server site and each local MS Mail postoffice.
- Set up directory replication between the connected Microsoft Exchange Server sites, to exchange information about the connected MS Mail postoffices.

If two MS Mail postoffices are connected with Microsoft Exchange Server, each postoffice views the other as being connected indirectly through one or more other postoffices (each site appears as a single MS Mail postoffice). If you add information about additional indirectly connected MS Mail postoffices, this information is shared among all sites to which directory information is replicated.

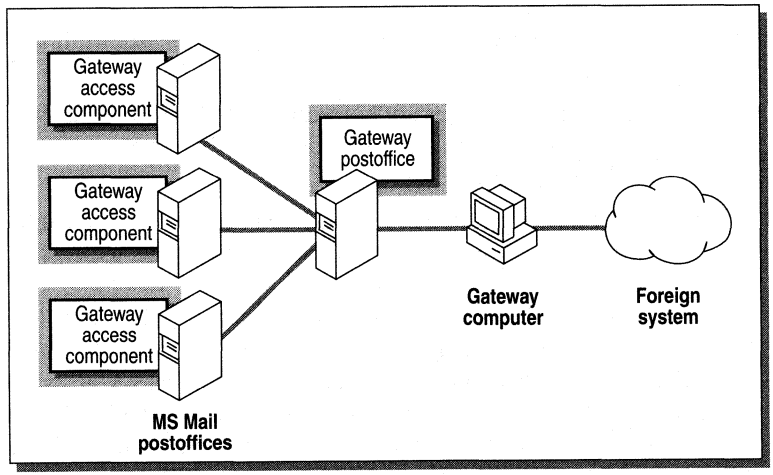
If you set up directory synchronization between Microsoft Exchange Server and connected MS Mail postoffices, all information that you add to Microsoft Exchange Server is distributed to those postoffices. For more information about synchronizing directories between Microsoft Exchange Server and MS Mail systems, see the "Directory Synchronization" section later in this chapter.

Microsoft Mail Connectors and MS Mail (PC) Gateways

To provide messaging service between Microsoft Exchange Server and other systems, you can use the following gateways with Microsoft Exchange Server:

- AT&T Easylink Services
- Fax
- IBM PROFS and OfficeVision
- MHS
- SNADS
- MCI MAIL Gateway (M-Bridge for Microsoft Mail for PC Networks)

Typically, an MS Mail gateway configured to service MS Mail postoffices requires that the gateway program run on a dedicated computer. Also, gateway access software must be installed on all postoffices that send mail through the gateway. One postoffice, directly connected to the gateway, is selected as the gateway postoffice, as shown in the following illustration:



Microsoft Exchange Server clients and MS Mail (PC) clients can share gateway access in two ways:

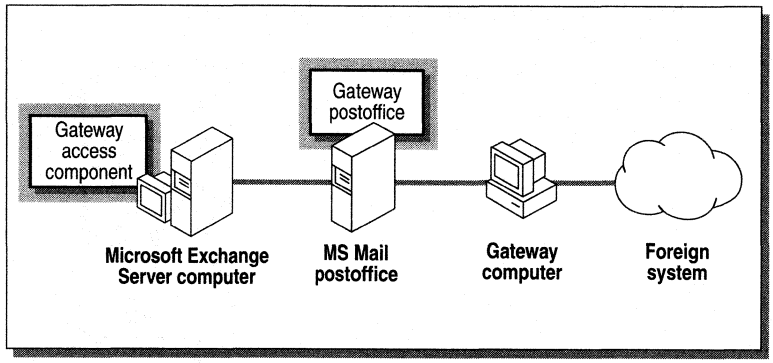
- Use existing MS Mail (PC) gateways between Microsoft Exchange clients and foreign systems.
- Use the Internet Mail Service or the X.400 Connector (or both) as gateways between MS Mail (PC) postoffices and foreign systems.

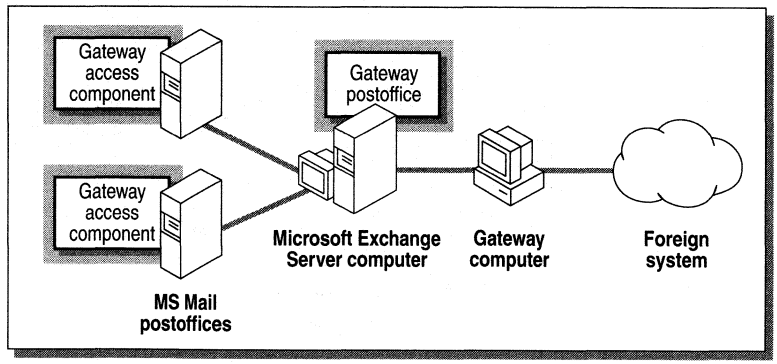
Using Existing MS Mail (PC) Gateways

For an existing MS Mail (PC) system using MS Mail (PC) Gateways, there are two ways for Microsoft Exchange clients to send mail to the foreign system:

- Install the MS Mail version 3.*x* Gateway Access Component on the Microsoft Exchange Connector postoffice.
- Install the MS Mail v3.*x* Gateway on the Microsoft Exchange Connector postoffice.

In either case, the MS Mail v3.*x* gateway process moves mail between the gateway postoffice and the foreign system. The following illustration shows both configurations:

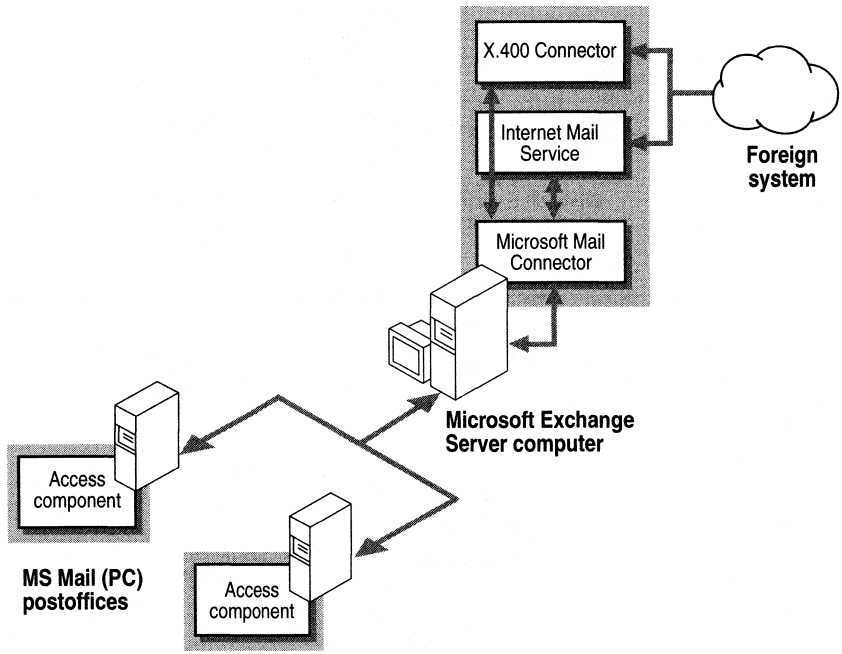




Using Microsoft Exchange Server Connectors as Gateways

Both the Internet Mail Service and the X.400 Connector can serve as gateways between an MS Mail (PC) system and a foreign system. For example, you can install the Microsoft Exchange X.400 Connector or Internet Mail Service (or both) on a Microsoft Exchange Server computer. For every MS Mail (PC) postoffice that you want to access the foreign system, you must install a gateway access component. The MS Mail (PC) postoffices must be connected to the Microsoft Exchange Server computer by the Microsoft Mail Connector. Typically, a mail message is passed from the MS Mail (PC) postoffice to the MS Mail Connector, which is passed to either the X.400 Connector or Internet Mail Service. The message is then transferred from either the X.400 Connector or Internet Mail Service to the foreign system. A message from the foreign system to an MS Mail recipient takes the reverse route.

The following diagram illustrates these routes:



Microsoft Mail Connector (AppleTalk)

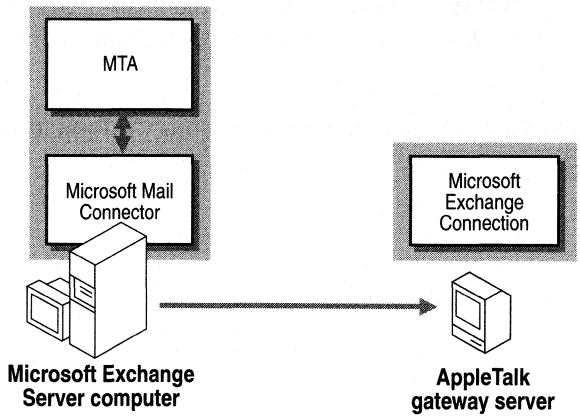
Microsoft Mail for AppleTalk Networks (also known as Quarterdeck Mail) uses server-based gateway software to exchange messages with other systems. MS Mail (AppleTalk) uses a client/server system to store and transfer information. You can connect Microsoft Exchange Server and an MS Mail (AppleTalk) gateway server by using the following software:

Microsoft Mail Connector A Microsoft Exchange Server component used to convert messages to MS Mail format and connect to MS Mail servers and postoffices. The Microsoft Mail Connector uses postoffices similar to MS Mail (PC) postoffices (also called gateway postoffices or shadow postoffices). The connector is dedicated to message transfer and has no local mailboxes.

Microsoft Exchange Connection A gateway program for MS Mail (AppleTalk). An MS Mail (AppleTalk) server running this gateway software acts as a hub for messages to and from a Microsoft Exchange Server computer.

To set up communication between Microsoft Exchange Server and MS Mail (AppleTalk), you must install and configure the Microsoft Mail Connector on a Macintosh-accessible volume. Then start the required services, including Services for Macintosh, and install and configure the Microsoft Exchange Connection on the MS Mail (AppleTalk) gateway server.

The following diagram illustrates how the system appears after installation:



Messages from Microsoft Exchange Server are converted to MS Mail format by the Microsoft Mail Connector and are then transferred to and from the MS Mail (AppleTalk) gateway server by the Microsoft Exchange Connection program. Messages from MS Mail (AppleTalk) are handled in the opposite order.

When you install Microsoft Exchange Connection on the MS Mail (AppleTalk) gateway server, you connect to the Microsoft Mail Connector postoffice. The Connection Installer program (for the Macintosh computer) creates a directory structure in the connector postoffice to use as the transfer point between the two systems. This directory structure, referred to as the *connection store,* is where Microsoft Exchange Server and MS Mail (AppleTalk) messages and other information are exchanged.

A directory synchronization requestor program for MS Mail (AppleTalk) is installed with the Microsoft Exchange Connection. You can use the requestor to automatically exchange address directory updates between MS Mail (AppleTalk) and Microsoft Exchange Server. To do so, assign the requestor the network manager's account ID and password when you install and configure the Microsoft Exchange Connection. This enables the requestor to log on as network manager to perform directory synchronization tasks when necessary. Address lists are exchanged in the form of special system messages. The requestor sends MS Mail (AppleTalk) address list changes to the Microsoft Exchange Server directory synchronization server, retrieves server address list changes, and integrates them into the MS Mail (AppleTalk) address list.

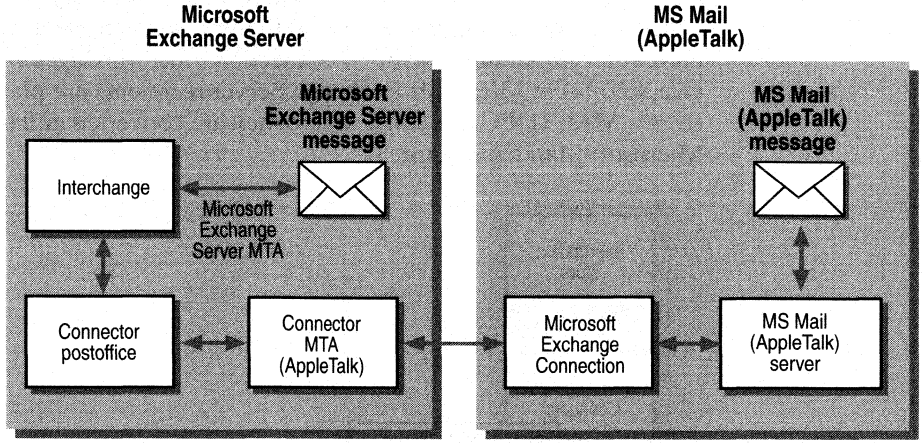
Microsoft Mail Connector

The Microsoft Mail Connector contains the following components that work together to transfer messages to and from MS Mail (AppleTalk):

Microsoft Mail Connector interchange A Windows NT Server service that routes messages between Microsoft Exchange Server and the Microsoft Mail Connector postoffice.

Microsoft Mail Connector postoffice A temporary information store for messages in transit.

Microsoft Mail Connector (AppleTalk) MTA A Windows NT Server service that works with the Microsoft Exchange Connection gateway to transfer messages between the Microsoft Mail Connector postoffice and MS Mail (AppleTalk).

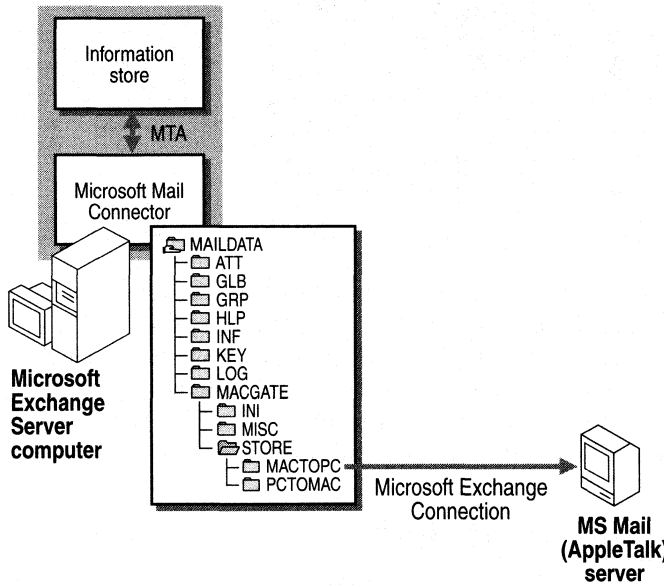


When a message is submitted to the Microsoft Exchange Server MTA for an MS Mail (AppleTalk) recipient, it is passed on by the connector interchange. The connector interchange converts messages and attachments to text and places the message in the connector postoffice. The Microsoft Mail Connector (AppleTalk) MTA converts messages to Macintosh-compatible file format and places each message in a folder for retrieval by the Microsoft Exchange Connection.

Microsoft Exchange Connection

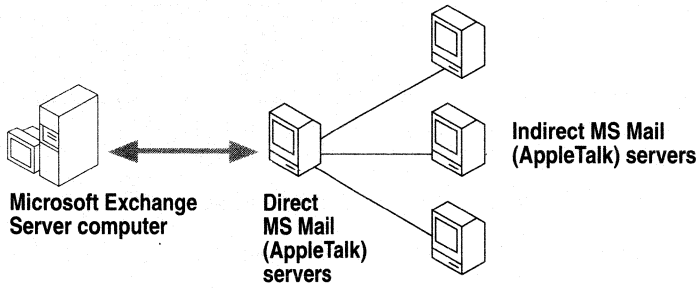
You use the Microsoft Exchange Connection Setup program to install and configure the Microsoft Exchange Connection gateway. You can configure and modify the gateway configuration, connect times, accounts, and recipients by logging on as network manager and running MS Mail.

Messages from Microsoft Exchange Server to MS Mail (AppleTalk) are converted to text by the connector interchange and then placed in the Microsoft Mail Connector postoffice's connection store PCTOMAC directory by the Connector (AppleTalk) MTA. They are retrieved from this directory by the Microsoft Exchange Connection and delivered to the correct recipient (or forwarded to the correct server) at the scheduled connection time. Messages from MS Mail (AppleTalk) to Microsoft Exchange Server recipients are placed in the connection store's MACTOPC directory, where they are converted and transferred by the Microsoft Mail Connector.



Connecting MS Mail (AppleTalk) and Microsoft Exchange Server Sites

You can connect an MS Mail (AppleTalk) site with a Microsoft Exchange Server site by using the Microsoft Mail Connector and Microsoft Exchange Connection, as shown in the following illustration:



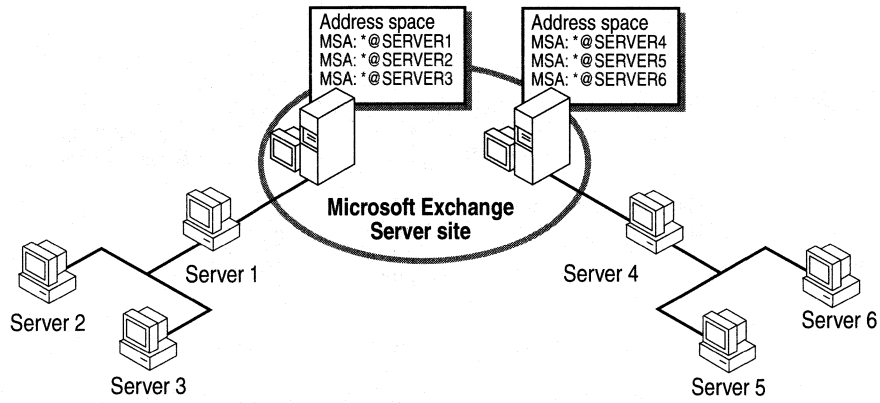
To create this type of connection, you need to:

- Set up the Microsoft Mail Connector on a Windows NT file system (NTFS) volume on the Microsoft Exchange Server computer and then make the connector postoffice Macintosh-accessible.
- Set up the Microsoft Exchange Connection on the MS Mail (AppleTalk) gateway server.
- Configure the Microsoft Mail Connector and Microsoft Exchange Connection to route messages between systems.
- Set up the gateway access component on each indirect MS Mail (AppleTalk) server that you want to communicate with Microsoft Exchange Server.
- Add the e-mail address of each indirect MS Mail (AppleTalk) server to the Microsoft Mail Connector address space, to enable messages for indirect servers to be sent from the Microsoft Exchange Server site.

After a connection is made between the two systems, you can use directory synchronization to ensure that new message routing information is shared between MS Mail (AppleTalk) servers and Microsoft Exchange Server computers.

Using Microsoft Exchange Server as a Backbone to MS Mail (AppleTalk)

You can connect two or more existing MS Mail (AppleTalk) systems that use Microsoft Exchange Server with the Microsoft Mail Connector. Routing to individual MS Mail (AppleTalk) servers can be configured in the connector address space. The following illustration shows how wildcard characters (*) are used in the address space to configure routing to multiple MS Mail (AppleTalk) systems.



Directory Synchronization

If you use other messaging systems in addition to Microsoft Exchange Server, you must maintain at least two sets of directories. Microsoft Exchange Server provides directory synchronization, which maintains address information between your organization and any system that uses the MS Mail directory synchronization protocol.

Directory Synchronization Protocol

The MS Mail (PC) directory synchronization protocol automatically synchronizes directories on all postoffices in an MS Mail (PC) system. The postoffices can be on the same LAN, connected asynchronously, or connected by a gateway. The MS Mail (PC) directory synchronization protocol is fault tolerant, which ensures directory integrity even if the network fails. Any changes or updates to addresses on one postoffice are automatically sent to other postoffices in the organization, which reduces address list maintenance and enables more efficient and frequent updates.

The MS Mail directory synchronization protocol uses two components:

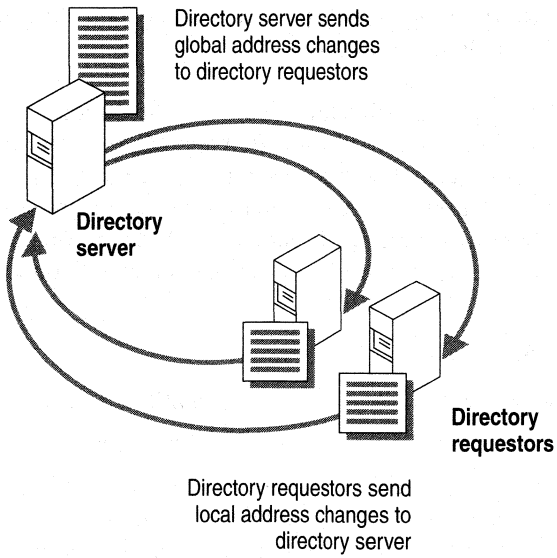
Directory server postoffice Acts as a central repository for directory changes.

Directory requestor postoffice Submits directory changes to the directory server postoffice.

Each postoffice in the MS Mail (PC) system is either a directory server postoffice or a directory requestor postoffice. One postoffice in the organization must be designated as the directory server. The directory server collects the address updates for the group of requestor postoffices. These requestors can be located on any network in the organization that can communicate with the directory server. The process that distributes all this information is called the *directory synchronization agent,* which can be hosted on computers running MS-DOS®, OS/2, or Windows NT Server.

You need to set up a schedule for directory updates. At the scheduled time, the directory synchronization agent sends these updates to the directory server postoffice, which then sends each requestor postoffice any new global address list updates in the form of a message file. The MS Mail Dispatch program processes the updates into the requestor postoffices' address lists.

Each requestor postoffice sends a message to the server postoffice on a regular basis (typically once a day) to request updates. When the requestor postoffice updates its address list, it sends a verification message to the server postoffice, which ensures that the server does not send the same update to that requestor postoffice again.



The Microsoft Mail Connector and the MS Mail Dispatch Program

An instance of the MS Mail Dispatch program must remain on a LAN with MS Mail directory requestors. The Dispatch program launches programs necessary to carry out directory synchronization requests on the network.

Implementing Directory Synchronization

Microsoft Exchange Server uses an enhanced implementation of the MS Mail directory synchronization protocol. It allows the same fault tolerance, but the following features make it easier to administer:

- More scheduling options, which improves time zone management and scheduling of directory updates.
- Better response times.
- Better error reporting and logging.
- Load balancing so that you can configure multiple Microsoft Exchange Server computers for directory synchronization and balance the directory synchronization load among them.

There is another important difference between the directory synchronization protocol implementation in MS Mail (PC) and Microsoft Exchange Server. With MS Mail (PC), changes are based on sequence numbers relative to each directory server/requestor relationship. Although these numbers are still maintained by Microsoft Exchange Server, the directory synchronization component uses the Microsoft Exchange Server directory to track address list updates.

Requestors and Servers

Directory synchronization involves sending notifications about address changes in the local system to the remote system, and vice versa.

To set up directory synchronization between Microsoft Exchange Server and an MS Mail (PC) system, MS Mail (AppleTalk) system, or a system that supports the MS Mail (PC) synchronization protocol, you must configure a directory synchronization component on each side. Either component can be configured as a server or a requestor.

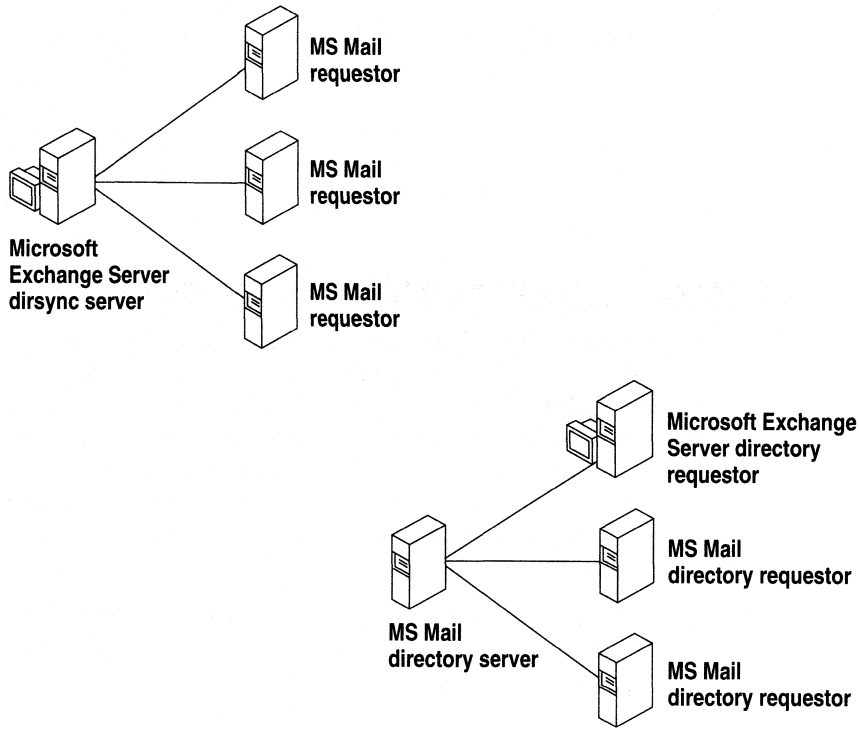
The directory synchronization agent can be configured for either of two roles:

Dirsync requestor Periodically queries the Microsoft Exchange Server directory for changes to recipient information. When Microsoft Exchange Server recipients are added, deleted, or modified, the directory synchronization component sends (according to schedule) an update message to the MS Mail directory server postoffice. It also requests MS Mail address updates from the MS Mail directory server postoffice.

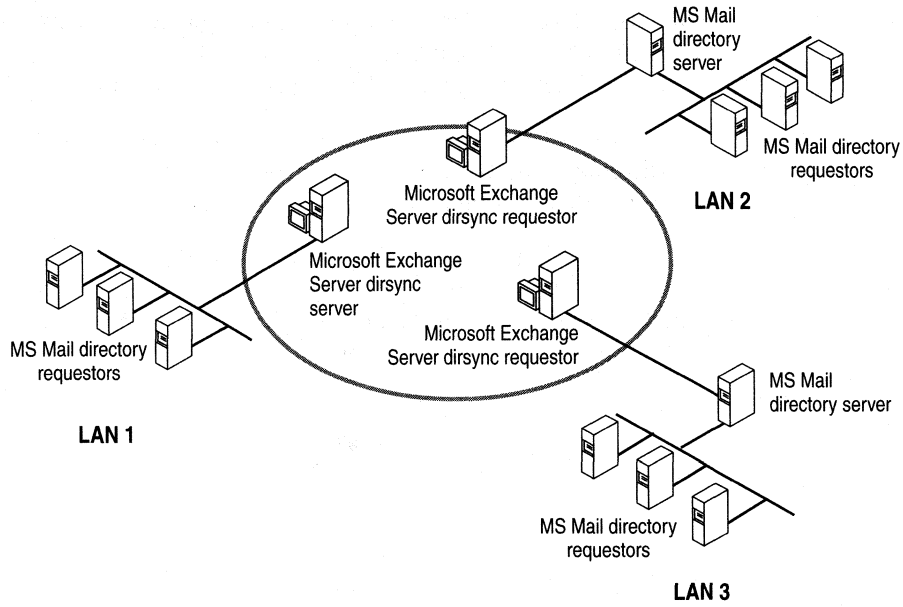
Dirsync server Processes incoming update messages from one or more MS Mail directory requestors and incorporates the updates in the directory as custom recipient objects. It also sends updates on Microsoft Exchange Server recipients in response to update requests from an MS Mail directory requestor postoffice.

A Microsoft Exchange Server computer can be configured as either a directory synchronization server or requestor, but not both. Therefore it can't participate in more than one directory synchronization process at the same time.

In the following figure, the illustration on the left shows a single Microsoft Exchange Server computer configured as a dirsync server to multiple MS Mail requestors. The illustration on the right shows the Microsoft Exchange Server computer as a dirsync requestor.



Multiple dirsync requestors in a Microsoft Exchange Server organization cannot use the same Microsoft Mail directory server postoffice. Conversely, a single Microsoft Exchange Server computer cannot act as requestor to multiple MS Mail directory servers. The following illustration demonstrates the relationship between multiple MS Mail directory servers and multiple Microsoft Exchange Server dirsync requestors. Notice there is only one dirsync server for this Microsoft Exchange Server site.

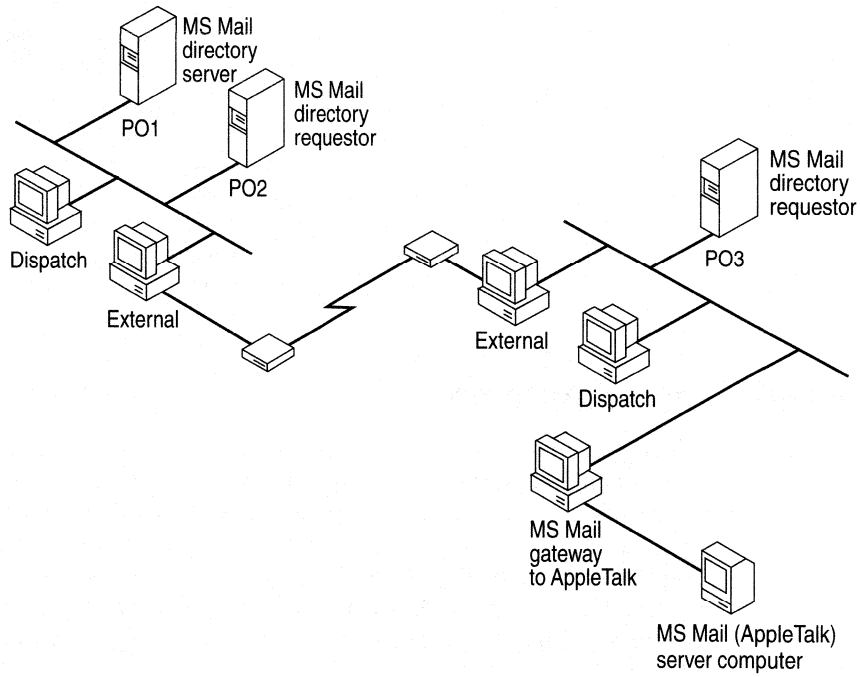


Remote Directory Synchronization Requestors

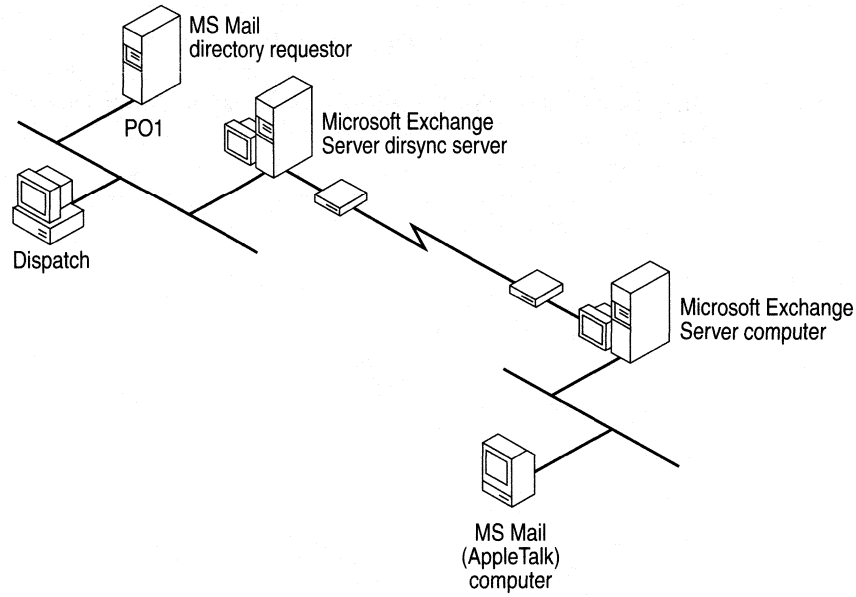
For a Microsoft Exchange Server to act as a dirsync server for an existing MS Mail directory synchronization system, you must configure it to replace the existing MS Mail directory server. To do so, you must define a remote dirsync requestor instance for each Microsoft Mail directory requestor postoffice. This is similar to the way in which a list of requestors is created and maintained for an MS Mail server. These requestor postoffices can be MS Mail (PC), MS Mail (AppleTalk), or any foreign system that supports the MS Mail (PC) directory synchronization protocol.

The Microsoft Mail Connector should be installed and configured on a Microsoft Exchange Server prior to setting up directory synchronization between MS Mail (PC) and MS Mail (AppleTalk) systems.

The following illustration is an example of an existing MS Mail directory synchronization system that includes both MS Mail (PC) and MS Mail (AppleTalk) postoffices on two LANs connected asynchronously. On one LAN there is an instance of the MS Mail gateway to AppleTalk Networks. Both LANs have instances of the MS Mail External and Dispatch programs. If Microsoft Exchange Server is installed on each LAN, instances of the MS Mail External and MS Mail gateway to AppleTalk Networks can be replaced by Microsoft Mail Connector MTA services.



If both Microsoft Exchange Server computers replace existing MS Mail postoffices, one can act as dirsync server for the remaining MS Mail postoffices. As mentioned earlier, an instance of the MS Mail Dispatch program must remain on a LAN with MS Mail directory requestors. The following illustration is an example of such a configuration:



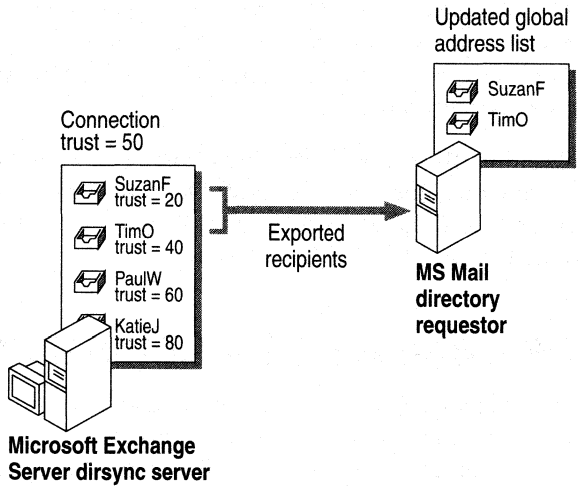
Import and Export Containers

When you configure directory synchronization, you must identify import and export containers. *Import containers* are used to store the imported MS Mail addresses. *Export containers* are the Microsoft Exchange Server recipients that you want to be exported to MS Mail. You select the recipients for the export containers from the directory. By default, a dirsync requestor does not export any recipient objects from Microsoft Exchange Server to MS Mail. However, you can configure a dirsync requestor to export recipient objects from Microsoft Exchange Server.

You can use containers to simplify dirsync management. For example, for each remote dirsync requestor, you can place recipient names imported to the dirsync server into separate import containers. These same containers can also act as directory synchronization export containers to other remote dirsync requestors. Having separate containers enables you to manage which recipient names are exported during the directory synchronization process to other remote dirsync requestors.

Trust Levels

You can control which specific Microsoft Exchange Server objects are exported to MS Mail (PC) during directory synchronization by setting a *trust level* for each recipient object and export container. Only recipients with a trust level equal to or lower than the trust level specified for a connection are exported to MS Mail. Trust levels are set arbitrarily by the administrator to represent a threshold of acceptance or rejection for a recipient object being either imported or exported. The following illustration shows that only recipients with a trust of 50 or less are exported to the MS Mail directory requestor to be incorporated into its global address list:



MS Mail doesn't have trust levels, but you can set trust levels in import containers. If you modify trust levels for a recipient object after it has been imported, the modifications are overwritten during any subsequent directory synchronization import cycle that includes the recipient object.

Microsoft Schedule+ Free/Busy Connector

The following describes the process of sharing free and busy information between Microsoft Exchange Server and MS Mail (PC) systems.

When the Schedule+ Free/Busy Connector is started, it determines whether an administrator's mailbox (ADMINSCH) has been created for the Microsoft Exchange Server computer. If a mailbox has not been specified, the connector stops. If a mailbox has been specified, the Schedule+ Free/Busy Connector searches the global address list for custom recipients designated as ADMINSCH for the MS Mail (PC) system. The Schedule+ Free/Busy Connector then searches for a distribution list of accounts to whom it will send scheduling updates from Microsoft Exchange users. If the list is empty, the connector stops.

The Schedule+ Free/Busy Connector checks the Inbox of the ADMINSCH account on the Microsoft Exchange Server for free and busy information sent from the MS Mail (PC) system to Microsoft Exchange Server. If it finds an entry in the ADMINSCH account, the Schedule+ Free/Busy Connector searches the Schedule+ Free/Busy system folder for a corresponding entry. The Schedule+ Free/Busy Connector moves free and busy updates for MS Mail (PC) users from the Inbox to the system folder.

The Schedule+ Free/Busy Connector checks the Schedule+ Free/Busy system folder to determine whether any Microsoft Outlook users have updated their schedules. It sends any changes in the system public folder to the ADMINSCH accounts defined in the MS Mail (PC) system.

Microsoft Exchange Connector for Lotus cc:Mail

The Microsoft Exchange Connector for Lotus cc:Mail is used for message transfer and directory synchronization between Microsoft Exchange Server and Lotus cc:Mail systems. You can connect a cc:Mail network to a Microsoft Exchange Server organization using one connector or multiple connectors, depending upon your messaging requirements. Each Microsoft Exchange Server computer in your organization can run one instance of the connector that directly services one connection to a cc:Mail post office. You cannot service one cc:Mail post office from more than one connector.

You configure the Connector for Lotus cc:Mail by using the Microsoft Exchange Server Administrator program. You can administer it from any Microsoft Windows NT Workstation computer or Microsoft Windows NT Server computer that is part of your network.

How the Connector for cc:Mail Works

Microsoft Exchange Server uses the connector and the cc:Mail Import and Export programs (Import.exe and Export.exe) to communicate with cc:Mail systems.

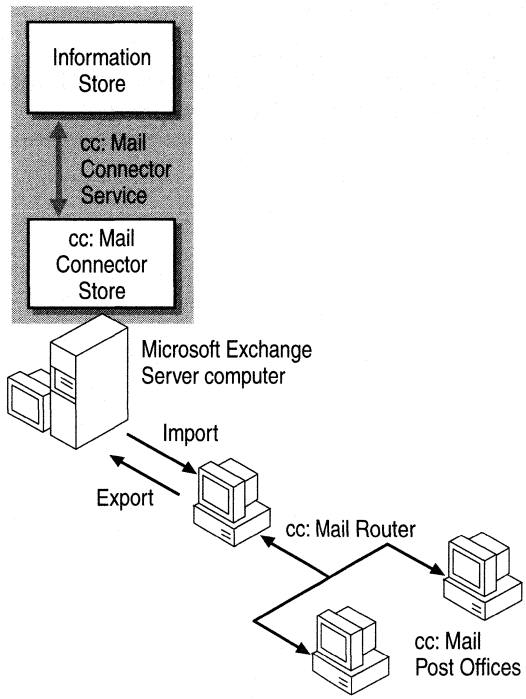
Connector for cc:Mail Service A Windows NT Server service that transfers messages between Microsoft Exchange Server and cc:Mail. It also synchronizes some or all of the Microsoft Exchange Server global address list with the cc:Mail directory.

Connector for cc:Mail Store A set of file directories located on the Microsoft Exchange Server for messages in transit.

Lotus cc:Mail Import/Export Imports Microsoft Exchange Server messages and directory entries to cc:Mail post offices, and exports cc:Mail messages and directory entries to Microsoft Exchange Server.

When a message is submitted to the Microsoft Exchange Server MTA for a cc:Mail recipient, it is transferred to the Microsoft Exchange Server information store. The Connector for cc:Mail service retrieves the message, converts it to ASCII file format, converts attachments as needed, and then places the message in the connector store. If the Import program can't deliver the message, an NDR is sent back to the sender.

The connector service calls the cc:Mail Import program to submit messages for delivery to the destination post office, as shown in the following illustration:



The process of sending a cc:Mail message to a Microsoft Exchange Server recipient is similar. The cc:Mail Export program is called by the Connector for cc:Mail service to export messages to the connector store. The service retrieves the message from the connector store and then passes it on to the Microsoft Exchange Server information store.

Lotus cc:Mail Import and Export Programs

The cc:Mail Import and Export programs are the interfaces between the connector and a cc:Mail post office on the same LAN. Message format translation is necessary when sending to and from either system. The cc:Mail Export program writes cc:Mail messages in a fixed format to a file in the connector store. The Connector for cc:Mail service converts the messages and message attachments and then uses the cc:Mail Import program to import the messages to the cc:Mail post office.

Access to a licensed copy of Lotus cc:Mail Import and Export programs is required for every Microsoft Exchange Server computer with a connector. Edit your server's system path environment variable to include the location of the Import and Export files, or place them in a directory included in your system path. You should store licensed copies of the Import and Export programs on the server where the connector is installed.

Note The connector supports the Lotus cc:Mail Import/Export for MS-DOS only. Lotus cc:Mail Import/Export for OS/2 is not supported.

CHAPTER 5

Internet Protocol Support

The Internet is a collection of networks and gateways that use Transport Control Protocol/Internet Protocol (TCP/IP) to handle data transfer and message conversion from the sending network to the receiving network. An Internet protocol is a set of standards designed to enable different types of computers to communicate with one another and to exchange information through the Internet.

In addition to providing Simple Mail Transfer Protocol (SMTP) support, Microsoft Exchange Server supports the following:

- Internet News Service/Network News Transfer Protocol (NNTP)
- Post Office Protocol version 3 (POP3)
- Internet Message Access Protocol, Version 4rev1 (IMAP4rev1)
- Lightweight Directory Access Protocol (LDAP)
- Hypertext Transfer Protocol (HTTP)

You can set properties for Internet protocols at the site level or at the server level by using the Microsoft Exchange Server Administrator program. For more information on configuring properties for NNTP, POP3, IMAP4, LDAP, and HTTP, see *Microsoft Exchange Server Operations.*

Internet News Service/NNTP

The Internet News Service enables Microsoft Outlook users to participate in USENET newsgroup discussions. It also enables users running third-party applications that support NNTP (such as Microsoft Internet News or Free Agent) to access *newsgroup public folders*. NNTP is an application protocol that is used in TCP/IP networks. It defines a client/server command set for access to newsgroups. Newsgroup public folders are public folders that are accessible as USENET newsgroups.

Users can read and post items, such as messages and documents, to USENET *newsgroups.* For example, scientists can exchange research information by posting messages to a newsgroup public folder for their area of interest. Other scientists around the world can then read and respond to the items in the newsgroup. Items in newsgroups are replicated to USENET host computers in *nevsfeeds.* The Internet News Service uses NNTP commands to define the communication between hosts.

Before installing the Internet News Service and setting up a newsfeed, you should become familiar with USENET newsgroups and how to use and plan your newsfeed.

Understanding USENET Newsgroups

USENET is a network of host computers that exchange messages, which are organized by topic into groups, called newsgroups. Within USENET, there are more than 18,000 different global and regional newsgroups that are publicly shared. Organizations can subscribe to USENET to obtain access to newsgroup information.

USENET newsgroups are organized according to subject, and a newsgroup is available for nearly every conceivable topic. The most popular newsgroup categories, called *hierarchies,* are alt and the "big-eight" (comp, humanities, misc, news, rec, sci, soc, and talk). Several hundred other hierarchies exist for regional and special interest discussion forums.

The following table describes the alt and big-eight newsgroup hierarchies:

Hierarchy	Description
alt	Alternative or controversial topics.
comp	Computer topics, such as computer science and information about software and hardware.
humanities	Humanities topics, such as philosophy.
misc	Miscellaneous topics that aren't classified under other categories.
news	Information about USENET.
rec	Topics relating to recreational activities, hobbies, and the arts.
sci	Topics relating to the sciences and scientific research.
soc	Newsgroups for socializing and addressing social issues.
talk	Discussions about politics, religion, and other issues.

Each hierarchy contains numerous newsgroups, or subcategories, for related topics. For example, the alt.coffee newsgroup includes topics related to coffee, the rec.travel newsgroup includes topics about travel, and so on.

The following newsgroups provide useful information about USENET and newsgroups for new users:

Newsgroup	Description
news.announce.newusers	Lists frequently asked questions (FAQs) about USENET.
news.newusers.questions	Provides a forum for new users to ask for help.
news.announce.newgroups	Includes announcements about new USENET newsgroups.
news.admin.*	Provides help topics related to news administration and information about network abuse, such as flooding networks with mail (also known as *spamming*).

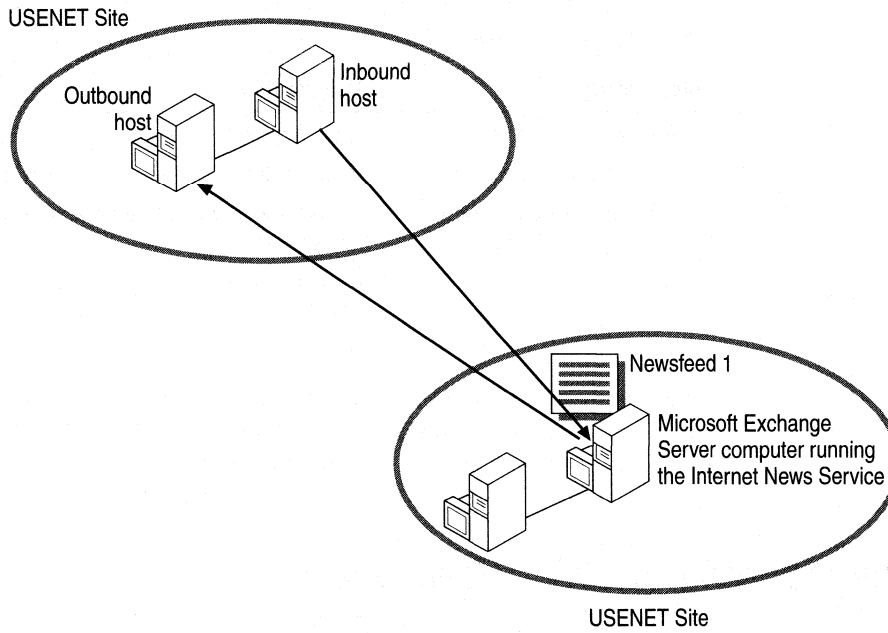
You can configure the Internet News Service to accept some or all available newsgroups by subscribing to those listed in the active file that your Internet newsfeed provider supplies. An active file contains the newsgroups that you can obtain from your newsfeed provider in a newsfeed.

Understanding USENET Newsfeeds

The flow of items from one USENET site to another is called a newsfeed. A newsfeed replicates items in newsgroups between host computers. One or more servers, or hosts, running NNTP make up a USENET site. Note that a USENET site is different from a Microsoft Exchange Server site.

Each USENET site receiving a newsfeed can be configured to accept and generate an NNTP connection and newsfeed. The host computer that receives your newsfeed is configured as the *outbound host*. The host computers that provide your newsfeed are configured as the *inbound hosts*. A host computer can be configured as both the inbound and outbound host.

The following illustration shows how the Internet News Service exchanges items in newsgroups with other USENET sites:



Planning for the Internet News Service

Before you configure the Internet News Service and set up newsgroup public folders, you should make initial preparations. For example, you should determine how much disk space you will need for the newsgroups you want to make available in your organization. You should also contact an Internet newsfeed provider and exchange information, such as the address of your Microsoft Exchange Server computer and your newsfeed provider's USENET host computer.

Planning Guidelines

Before you configure your newsfeed, plan your system requirements by considering the following:

Network throughput A USENET newsfeed can send hundreds of megabytes or gigabytes of data across your network. Therefore, make sure that your Internet connection has the bandwidth to support a newsfeed without disrupting other network traffic, such as e-mail.

Storage space The Microsoft Exchange Server computer running the Internet News Service must have enough disk space to support your newsfeed. To determine this, you should consider the size of the newsfeed and whether age limits will be set on newsgroup public folders. The daily volume of a full USENET newsfeed is more than 1.7 gigabytes, or 200,000 messages.

Load balancing The Microsoft Exchange Server computer running the Internet News Service should be able to support the number of users you expect to be accessing the newsgroup public folders. You should also consider whether you can distribute the load on the server by replicating the newsgroup public folders to other servers. Another consideration is that NNTP clients, unlike Outlook users, do not have transparent access to public folders on multiple servers. The client must be configured to connect directly to a server that has a replica of the newsgroup public folder the user wants to access.

Public folder replication The directory and public information store replicate public folder changes on a scheduled basis. Whenever a new public folder is created on a server, the resulting change in the public folder hierarchy is replicated to all other servers in the organization. If your network topology includes remote Microsoft Exchange Server sites that are connected over low-bandwidth connections, when you set up a newsfeed, make sure that the connections do not become saturated with replication messages. If the newsfeed includes a large number of newsgroups, it may be necessary to phase in the new folders over several days to prevent a flood of replication messages that could saturate your network.

POP3 Client Support

The Post Office Protocol version 3 (POP3) enables users with POP3 clients to retrieve mail from their Microsoft Exchange Server Inbox. Any third-party e-mail client that supports POP3 can connect to a Microsoft Exchange Server computer to access messages. To send outbound messages from Microsoft Exchange Server, POP3 e-mail clients can use the Internet Mail Service or any other SMTP server. Microsoft Exchange Server POP3 support is compliant with RFCs 1939 and 1734.

POP3 Routing

When POP3 is used to retrieve messages from a user's Microsoft Exchange Server Inbox, the client submits requests to the server. POP3 e-mail clients can retrieve messages only from their Microsoft Exchange Server Inbox. They do not have access to private or public folders or to encrypted messages. When a POP3 client sends a message, the Internet Mail Service routes messages to the Microsoft Exchange Server computer or to other SMTP hosts, depending on the recipient's address.

IMAP4 Client Support

IMAP4 enables clients to access and manipulate unencrypted messages stored within the users' private and public folders on a Microsoft Exchange Server computer. All third-party e-mail clients that support IMAP4 (RFC 2060) can be used to connect to a Microsoft Exchange Server computer and access messages. To send outbound messages from Microsoft Exchange Server, IMAP4 e-mail clients can use the Internet Mail Service or any other SMTP server.

IMAP4 works in a similar way as POP3. When IMAP4 is used to access messages, the client submits requests to the Microsoft Exchange Server computer. When an IMAP4 client sends a message, the Internet Mail Service routes messages to the Microsoft Exchange Server computer to other SMTP hosts, depending on the recipient's address.

LDAP Support

Lightweight Directory Access Protocol (LDAP) enables users and processes to access directory information from the Microsoft Exchange Server directory. As an administrator, you can grant or restrict users' access to Microsoft Exchange Server by setting permissions. Clients with permission to use LDAP can browse, read, modify, and search directory listings in the Microsoft Exchange Server directory. For example, users can search for specific information, such as phone numbers and office locations, from any application that supports LDAP. Many LDAP clients can access a single Microsoft Exchange Server computer and perform queries for directory information, such as user names and locations.

HTTP Support

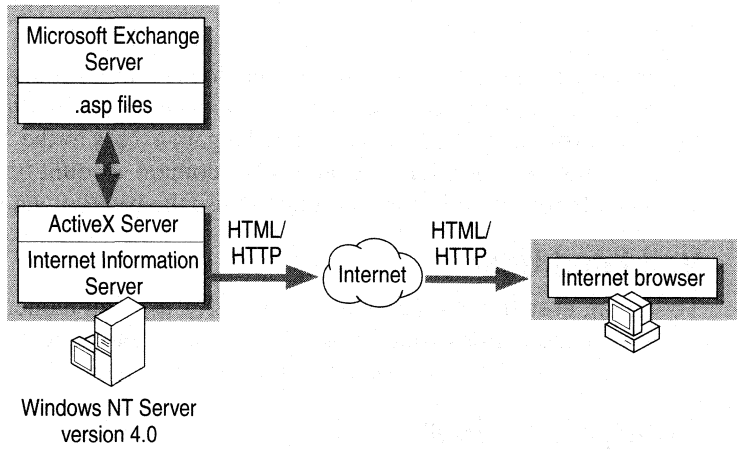
Hypertext Transfer Protocol (HTTP) is the set of conventions that World Wide Web servers use to send Hypertext Markup Language (HTML) pages over the Internet for display by a Web browser. Microsoft Exchange Server provides Microsoft Outlook Web Access, a Web-based e-mail client application that interacts with the Active Server function built into Microsoft Internet Information Server (IIS).

With Outlook Web Access, users can access data on a Microsoft Exchange Server computer by using an Internet browser from a UNIX, Macintosh, or Microsoft Windows-based computer. Outlook Web Access provides Web-based public access to Microsoft Exchange Server public folders and global address lists. Validated users can log on to their personal accounts to read and send private mail. Using Web-based public folder access, an organization can build private and public discussion forums on the Internet and on its intranet. Users can publish information on the Internet without converting documents to HTML format.

Microsoft Outlook Web Access Installation

Microsoft Exchange Server Setup installs Outlook Web Access script files (.Asp files) on the Microsoft Exchange Server computer. The .asp files provide the functionality and user interface for the Outlook Web Access client.

Outlook Web Access is integrated with Microsoft Windows NT Server version 4.0 and is configured through the Microsoft Exchange Server Administrator program. The following illustration shows a possible configuration of Microsoft Exchange Server and Outlook Web Access:



As an alternative, you can run Internet Information Server on a separate computer that maps to a shared path from your Microsoft Exchange Server computer.

Outlook Web Access Operation

To access the logon page for their Microsoft Exchange Server computer, users start their Web browser and connect to the Internet, specifying the Uniform Resource Locator (URL) of their Active Server (IIS system). The Web browser then displays an introductory Web page that prompts users to log on by using their mailbox name. Users must type their Microsoft Exchange Server mailbox alias and press the ENTER key. The **Enter Network Password** dialog box then appears, prompting users for their user name and password. Users must type their complete Windows NT user account logon credentials and password. For example, users must enter their domain name and Windows NT user account alias in the **User name** box in the format: *domain\Windows NT user account alias,* followed by their Windows NT user account password in the **Password** box.

After typing the complete logon information, users can access their private mailbox and public folder data. Microsoft Exchange Server Message Application Program Interface (MAPI) data, Active Server scripts, and remote procedure call (RPC) data are translated to HTML on the Active Server and transmitted to the browser using the HTTP protocol.

Authentication

Users can access a Microsoft Exchange Server computer through the Internet by logging on with a secure connection as a validated user or as an *anonymous user.* Outlook Web Access uses Windows NT authentication to grant users Web-based access to their mailboxes.

When a user accesses the logon page and logs on to a Microsoft Exchange Server computer, an authenticated session is established between the browser and the Internet Information Server computer. To gain access to the Microsoft Exchange Server computer, the user's Windows NT domain account password must be validated before permission is granted to use the program and its data.

Validated User

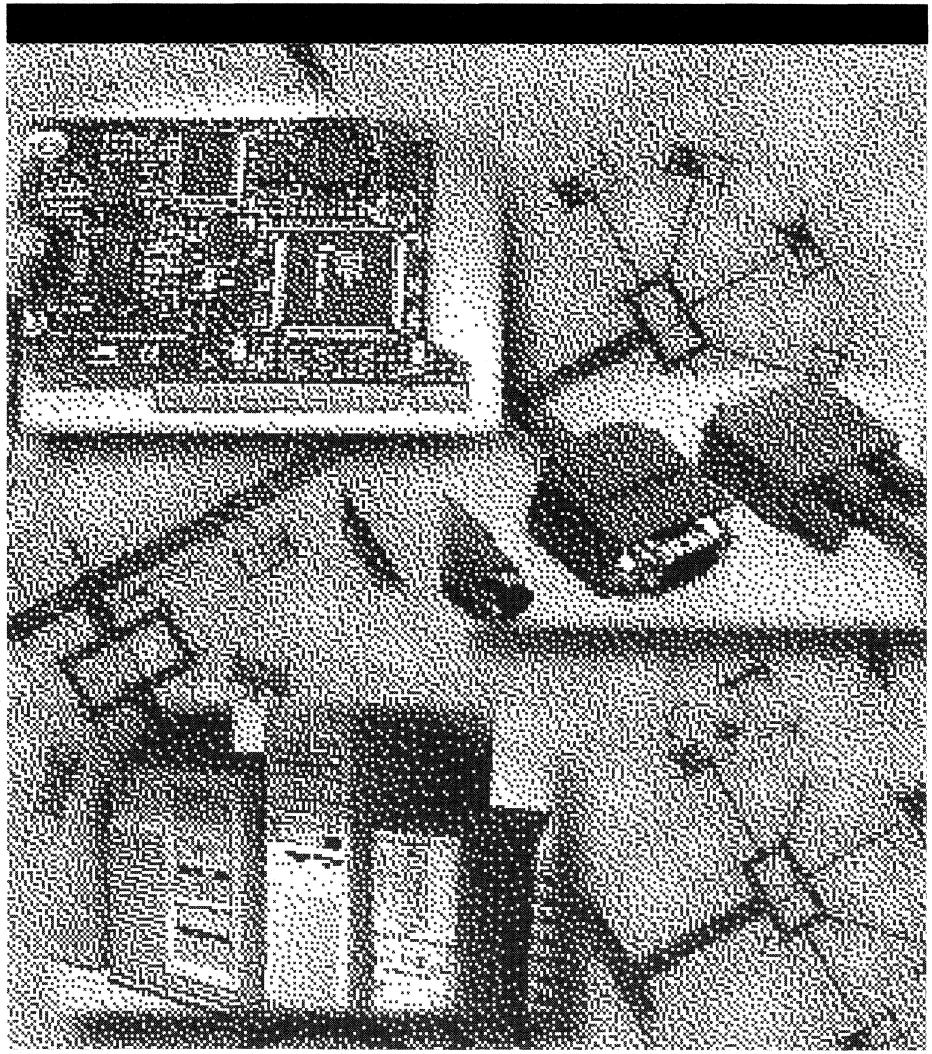
To log on, users must type their Windows NT account name, password, and mailbox name. After validation is successfully completed, users have the same permissions as when they log on to a computer connected directly to the network.

Anonymous User

An anonymous user is a nonvalidated Web user who is not recognized by Microsoft Exchange Server. A user can log on to a Microsoft Exchange Server computer anonymously but is restricted to viewing and accessing only published public folders and address lists. You can specify which folders and address lists to publish by using the Microsoft Exchange Server Administrator program.

PART 2

Planning



CHAPTER 6

Assessing Your Needs and Resources

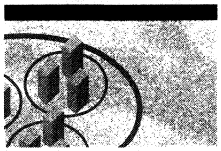
Careful planning of your organization's messaging needs is very important. If your organization is small or you have only a few servers, planning your Microsoft Exchange Server rollout is relatively simple.

The most effective way to plan your system is to use a "top down" approach, starting with the organization. To begin planning, design a prototype topology. Then validate and optimize that design until it meets your requirements.

To validate your design, consider projected server load and client response times. To optimize the design, consider several topology options and identify their costs and benefits. Each option can include a brief overview of the topology plan, network maps showing the data path, and routing diagrams. Finally, analyze, review, and test each option. Revise your plans as necessary to maximize performance, reliability, and service to users.

After the design meets your organization's requirements, determine how to set up Microsoft Exchange Server. Your plan should outline the procedures for installing the new system in your organization. Finally, roll out your plan in phases until all users are on the new system.

Planning Considerations



1 User Needs

Determine what applications and services your users require.

2 Geographic Profile

Identify your company's physical locations by city and country.

3 Network Topology

Determine the network size, bandwidth, traffic patterns, and protocols.

4 Windows NT Server Domain Models

Choose the most appropriate Windows NT Server domain model for your organization.

5 Sites and Site Boundaries

Determine the appropriate number of sites and how sites are mapped to domains based on factors such as network bandwidth, network traffic, cost, performance, and the Windows NT Server domain model.

6 Naming Conventions

Establish naming conventions for elements in your organization, such as sites, servers, and mailboxes.

7 Site Connections

Decide how you will connect your sites and what types of site connections you will configure.

8 Connections to Other Systems

Identify the type of connectivity to other systems that users need.

9 Migration

Determine how you will migrate mailboxes and mail from your existing mail system to Microsoft Exchange Server.

10 Administrative Policy

Establish the administrative policies for your organization, such as permissions and administrative duties.

User Needs

To assess user needs, identify the types of applications and services your users require, such as e-mail, scheduling, folders, and connections to other systems. Use this data to group users according to software, hardware, and training needs; server disk space needs; type of public folders required; predicted message volume; and other factors. You can then map user needs to the features available in Microsoft Exchange Server.

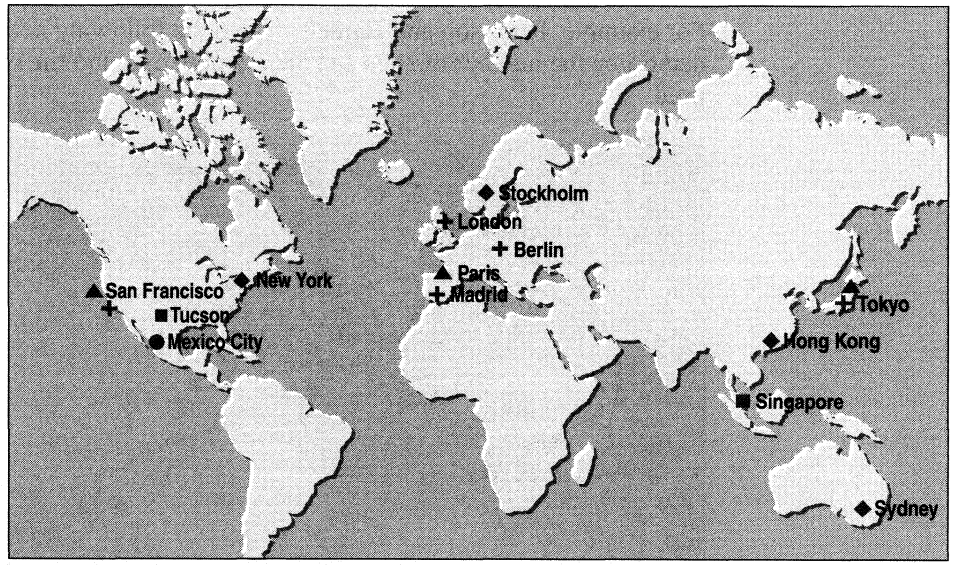
For example, Ferguson and Bardell grouped users by function, identified the most important needs for each group, and then mapped these needs to features available in Microsoft Exchange Server.

Function	Needs	Feature
Field personnel	Remote access to e-mail.	Remote connectivity
	Newswire application for news and weather forecasts.	Public folders and sample applications
Research and development	E-mail connectivity to the Internet.	Internet Mail Service
Sales	Connectivity to other locations through X.400.	X.400 Connector
Administrative and management support	Verification of information source.	Digital signatures
	Confidentiality of data.	Encryption
Manufacturing	At least two public folders, one for product specifications and one for safety information.	Public folders
All	Same tools and functionality on different operating systems.	Common interface across several platforms

Geographic Profile

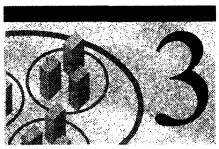
The geographic profile shows all the locations where your company has facilities. It may represent a small region or a large geographical area. Use a map or diagram to identify the number and types of users at each location. A visual representation helps you identify available network connections and network traffic.

For example, Ferguson and Bardell created the following map to identify its various facilities and the percentage of users within each respective facility throughout the world: oil exploration rigs, finance centers, manufacturing facilities, sales subsidiaries, and administrative offices.



●	Oil fields	(10%)
■	Manufacturing	(15%)
▲	Finance	(15%)
◆	Sales	(24%)
+	Administration	(36%)

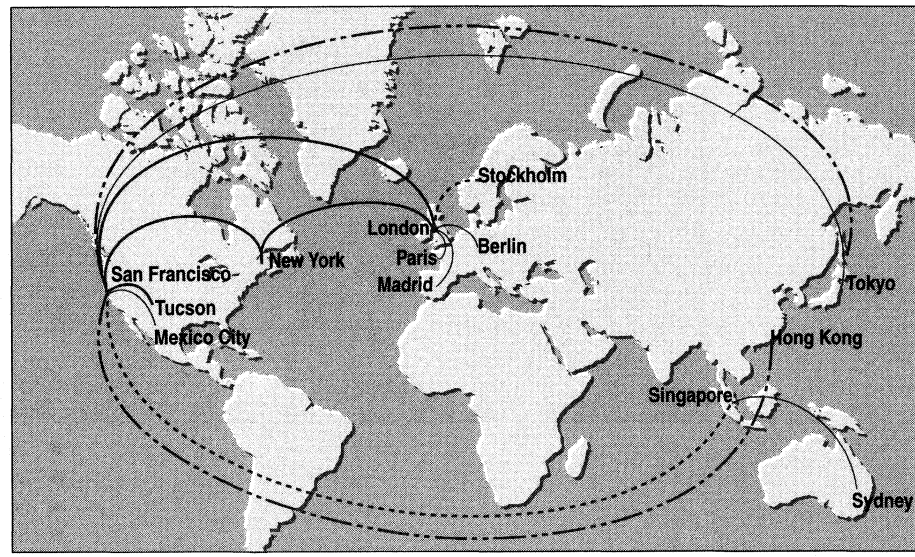
Network Topology



Site boundaries, site connections, message routing, directory replication, and system administration depend on topology. When planning your network topology, assess the following network issues:

- Size
- Bandwidth
- Type
- Traffic patterns
- Protocols

For example, Ferguson and Bardell created the following network diagram to determine the number of sites and their boundaries, and the types of connections used.



Network Size

In planning your organization, you need to determine the size of the network needed, because network size affects other decisions you have to make. For example, if you have a small network with a few sites, you may not need to consider how to replicate data over a wide area network (WAN) connection. However, for a large network you may need to consider:

- Setting up multiple sites.
- How to move data (such as directories and public folders replicated between sites) over WAN connections.
- How to configure Microsoft Exchange Server so that users can access information locally.

Network Bandwidth

For each type of network, performance is determined by many factors, including *network bandwidth* (how much data can be transmitted across the network). The amount of bandwidth available depends on the data transfer rate across the network and the physical characteristics of the communications line. When deciding on server locations, you need to consider bandwidth. For example, servers in the same site require faster and higher bandwidth connections than servers in different sites.

You should consider both *total available bandwidth* (the bandwidth provided by a network connection) and *net available bandwidth* (the bandwidth available after consumption by other applications).

Consider total available bandwidth so that you can:

- Choose the best type of connection between sites.
- Set directory and public folder replication schedules.
- Set costs appropriately.
- Configure public folder affinity values, which are used to determine which site Microsoft Outlook uses to connect to remote public folder replicas.

Microsoft Exchange Server performance is greatly affected by net available bandwidth, because performance decreases as traffic increases and applications compete for bandwidth. For example, if a database application is running with Microsoft Exchange Server, you should consider how much of the total available bandwidth the application consumes when it transfers data. You must also consider the bandwidth that a client consumes when sending messages and attachments.

The client/server architecture of Microsoft Exchange Server efficiently uses bandwidth by minimizing unnecessary overhead. Nevertheless, you should think about ways to minimize network traffic. For example, if you configure public folder replication to occur after business hours, bandwidth consumption will be lower during peak hours.

When designing your organization, consider the network bandwidth costs. The way that you transmit data also affects bandwidth costs. You should make sure that network connections between servers have enough bandwidth to handle bursts in traffic as well as typical traffic.

When choosing the appropriate bandwidth range, consider the number of servers, the message volume, and the traffic volume generated by public folder replication. The higher the traffic volume, the more bandwidth needed. Generally, you should design sites so that connections between servers are in the medium-to-high or very high-bandwidth range. You may be able to use the low-to-medium bandwidth range if you have low message volume or little public folder use. For example, if two servers are connected by a 64 kilobyte (KB) connection and you expect a high volume of messages, you should consider placing the servers in different sites. On the other hand, if they are connected by a 128KB connection, you can place them in the same site.

Network Types

Depending on your company's needs, your organization can span networks of different sizes and types. For example, a single local area network (LAN) that connects a few computers for sharing files and printers might use Ethernet, but a WAN that connects computers in a worldwide organization might use a backbone over T1 lines.

You need to consider reliability when choosing which type of network to use. For example, satellite connections have very high bandwidth but may not be reliable; an Ethernet network with a lower bandwidth may be more reliable.

Network Traffic Patterns

If you can predict network traffic patterns, you can determine whether the total available bandwidth can sustain bursts of traffic during heavy network use. If network traffic exceeds the available bandwidth, client/server response times become unpredictable. To prevent this, measure bandwidth use to determine whether a network connection is close to full capacity, then measure total packets per second to determine whether close bridges and routers are close to full capacity. You can measure these parameters by using dedicated network-monitoring products.

Network Protocols

Protocols are sets of rules that enable computers to connect with each other and exchange information. To design your network topology, you need to know what network protocols you have.

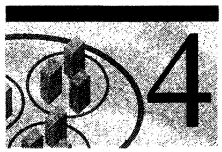
Outlook can run on a variety of networks, including Novell NetWare, versions 3.1*x* and 4.*x*, and Banyan VINES, version 5.54 or later. To integrate clients on other networks, you must choose one or more of the protocols supported by Windows NT Server.

Windows NT Server supports the following built-in protocols used by Microsoft Exchange Server:

- Transport Control Protocol/Internet Protocol (TCP/IP)
- Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX [NWLink])
- NetBIOS Extended User Interface (NetBEUI)

For more information, see the Microsoft Windows NT Server documentation.

Windows NT Server Domain Models



A *domain model* is a group of one or more domains arranged for user and resource management.

There are three Windows NT Server domain models:

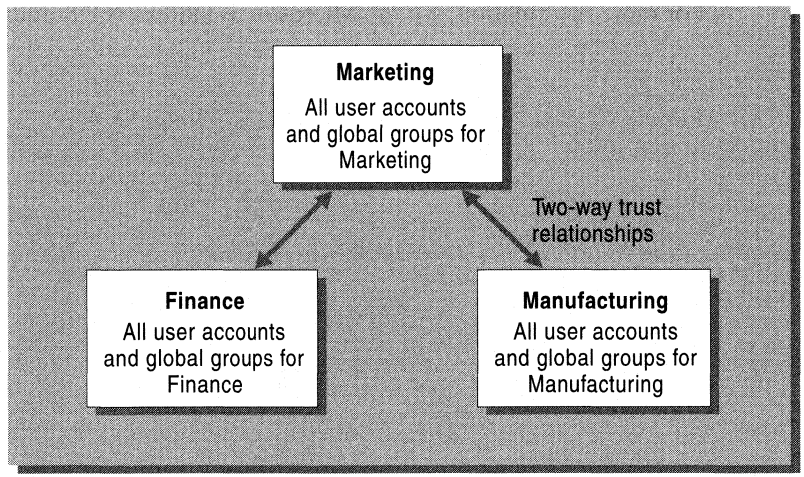
- Single
- Single master
- Multiple master

It is important to choose a domain model carefully or to study the existing one. If a domain already exists, find out how it is structured, how trust relationships are set up, why that model was chosen, and where the domain controllers are located. You need to incorporate this information into your organization plan.

The model you choose depends on your administrative resources and the network size. A single domain can handle up to 40,000 user accounts, and multiple master domains can handle more than 100,000 users.

Trust Relationships

Combined with trust relationships, domain models are extensible and flexible. You can use one-way or two-way trust relationships to distribute, rather than centralize, the management of users and domains among departments. For example, you can design your domains so that every domain in the network trusts every other domain, as the following figure illustrates. This way, each department can manage its own domain and define its own users and global accounts, yet these users and global accounts can still be used on all domains.



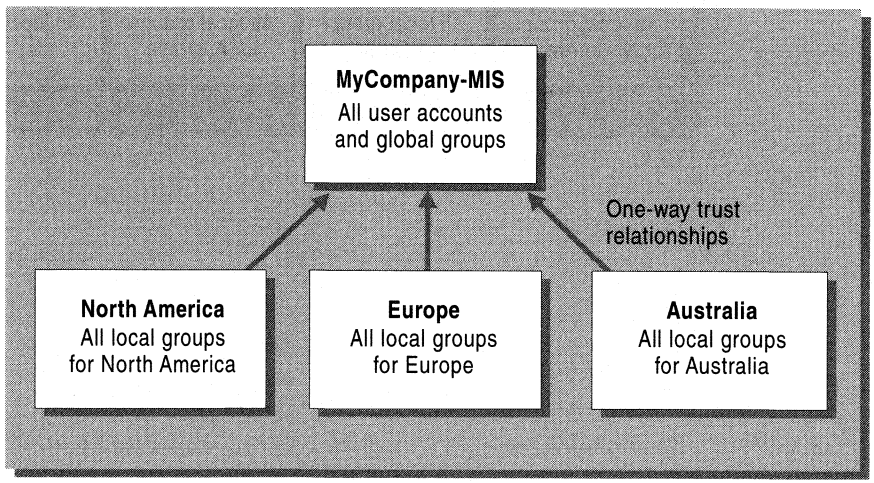
Single Domain

The single domain model is the simplest. Because there is only one domain, no trust relationships are necessary. All Windows NT user accounts are created in this domain. The single domain model is a good choice if your organization requires centralized management that is easy to administer.

Single Master Domain

The single master domain model provides centralized administration and the benefits of multiple domains. Each organizational group can manage its own resources, but user accounts and global groups are defined in the *master* (or *first-tier)* domain.

All users log on to their accounts in the master domain, but resources, such as printers and file servers, are located in the other domains, which are called *resource* (or *second-tier)* domains. Each resource domain establishes a one-way trust relationship with the master domain, and users with accounts in the master domain can use resources in all the other domains. You can manage the entire multidomain network, as well as its users and resources, by managing only the master domain.

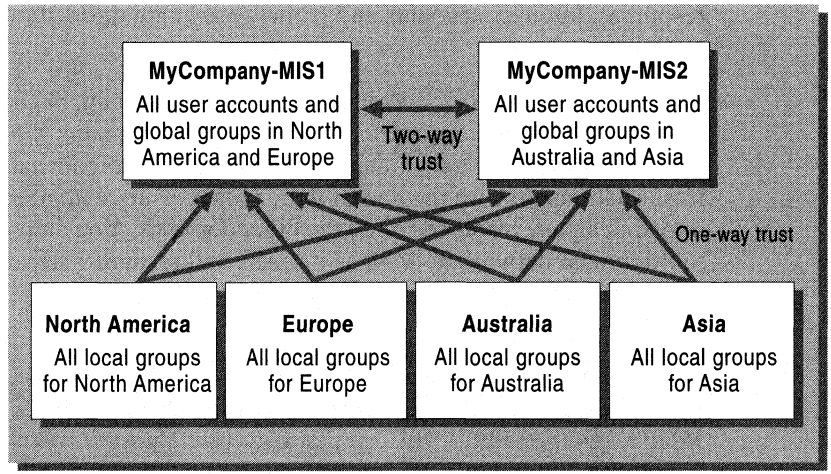


The advantage of the single master domain model is its flexibility. For example, if your network requires four domains, you can consolidate the administration of user accounts in one domain instead of creating a separate user account database for each domain.

Multiple Master Domain

The multiple master domain model provides centralized administration for large companies organized by groups, departments, or locations. Because this model can be expanded easily, it is useful for organizations that anticipate substantial growth.

With the multiple master domain model, two or more single master domains are connected by a two-way trust relationship. The master domains serve as account domains, with every user account created and maintained on one of the master domains. The resource domains don't store or manage user accounts, but do provide resources such as shared file servers and printers. Each resource domain trusts all master domains in a one-way trust relationship. A resource domain can trust other resource domains but is not required to do so.



Choosing a Domain Model

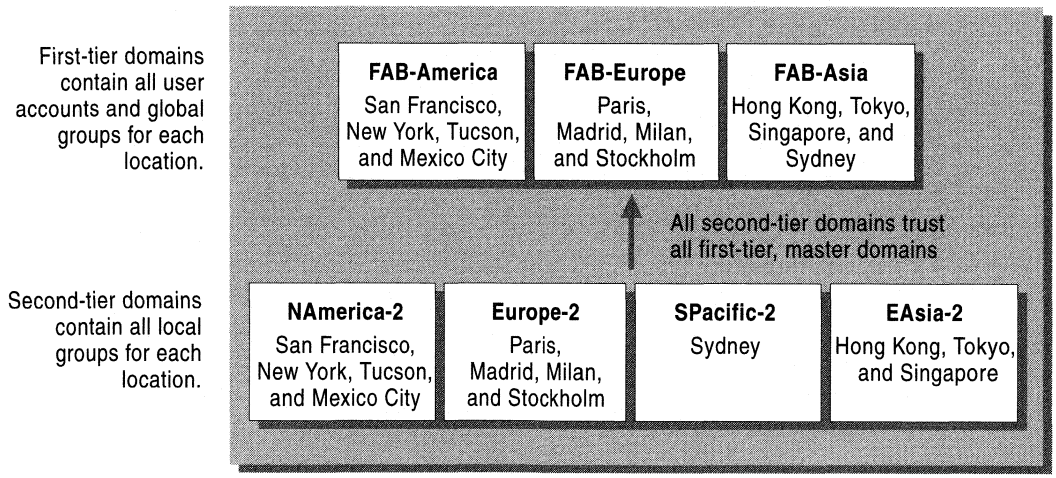
Use the following table to determine which domain model best suits the needs of your organization.

Domain attribute	Single domain	Single master domain	Multiple master domain
Less than 40,000 users/domain	X	X	—
More than 40,000 users/domain	—	—	X
Centralized account management	X	X	X*
Centralized resource management	X	—	—
Decentralized account management	—	—	X*
Decentralized resource management	—	X	X

* You can have either centralized or decentralized account management under the multiple master domain model.

For example, Ferguson and Bardell implemented a multiple master domain model with the following characteristics:

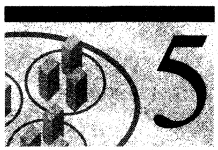
- Each main region is its own second-tier domain with its own administrator, who creates and manages local groups, files, and printers.
- Each of the three master domains trusts each other, and each second-tier domain trusts all the master domains. Second-tier domains do not trust each other.



Ferguson and Bardell decided to use the multiple master domain model because:

- It can expand as the company grows.
- It enables centralized management of user accounts (through the master domains) and distributed management of network resources (through the second-tier domains).
- Users can connect to resources in all trusted domains as the result of pass-through authentication.
- It minimizes the number of authentication sessions per domain, which reduces network traffic and enables good performance in the master domains.
- Departments can manage their own resources.

Sites and Site Boundaries



There are several factors to consider when determining where to draw site boundaries. In general, you should make sites as large as possible. The network connections between servers should have enough bandwidth to support the expected load.

All servers in a site must meet the following conditions:

Connectivity A site can only span a network connection that supports synchronous remote procedure calls (RPCs), and this connection between servers must be permanent.

Adequate bandwidth There must be enough bandwidth between servers to handle the volume of data transmitted within the site. As mentioned earlier, you need to consider message volume, and directory and public folder replication. If you expect the message traffic between servers to be low and your public folder use to be light, you may not need much bandwidth.

Same security context for all servers All servers in a site must be able to authenticate Microsoft Exchange Server users and services. Windows NT user accounts and service accounts must be in the same domains as the servers or in trusted domains. All Microsoft Exchange Server services within a site must use the same service account.

Note You must carefully plan the number of sites and their boundaries. If you change site boundaries after sites have been set up, you may have to reinstall and reconfigure all affected servers.

You should also consider the following factors when determining the number of sites and site boundaries:

Administration Keep the number of sites low and, as mentioned earlier, make the sites as large as possible. Ideally, sites should have no more than 50 servers. If you want to administer a group of servers collectively, place servers in the same site.

Cost To control cost, place servers that have expensive connections in separate sites. Also consider the type and number of servers per site. In some cases, it may be more cost effective to have several inexpensive servers than to have a few, expensive servers. You should weigh performance versus cost.

Performance To maximize performance, draw site boundaries so that servers using connections with similar bandwidths are placed in the same site. For example, if the connection between servers in San Francisco and New York is fast but the connection between San Francisco and Mexico City is slow, place the Mexico City server in a separate site. Other factors also affect performance, including the number of servers per site.

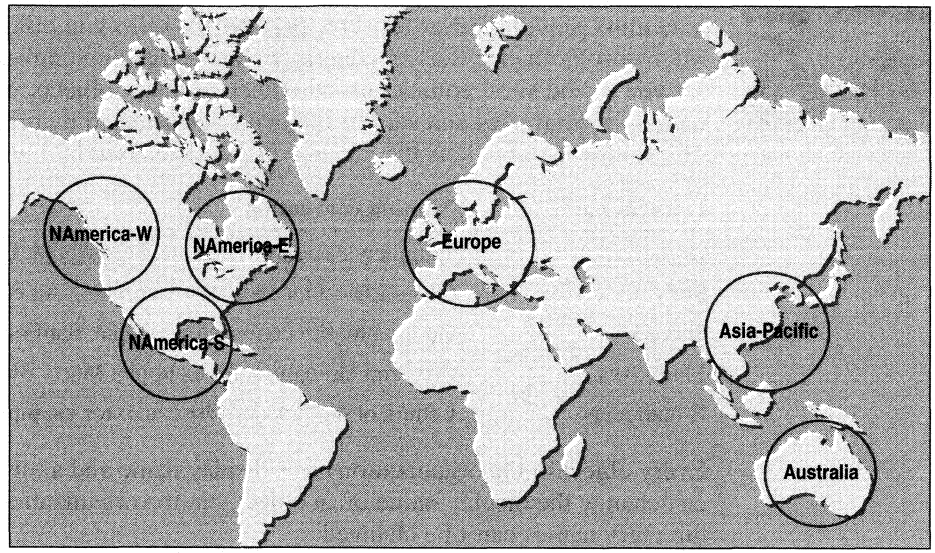
Directory replication Directory replication occurs more often within a site than between sites because the network bandwidth between sites is usually lower than it is within a site. If automatic and frequent replication between servers is needed, place the servers in the same site. If you want to control when replication occurs, place servers in different sites.

Organization issues Grouping users that work together on the same servers and in the same site improves performance, reduces network traffic, and provides the most efficient use of resources.

In the earlier example, Ferguson and Bardell's primary concern in determining site boundaries was available bandwidth. They set a threshold at 64KB or greater for placing servers in the same site. Based on this, they put San Francisco and Tucson in the same site because they are connected through a permanent, high-bandwidth connection, they are geographically close, and they can be administered together.

San Francisco and New York also have a permanent, high-bandwidth connection between them. However, this connection is shared by a database application that tracks all domestic sales and requires a lot of bandwidth during peak business hours. The administrators calculated that the available bandwidth on this connection is less than 64KB; therefore, New York was placed in a separate site.

Ferguson and Bardell created the following sites:



Mapping Sites and Windows NT Domains

You can map sites to Windows NT domains in different ways. You can have every site map to one domain or to several domains. You don't need to map all domains to your sites, provided that the Microsoft Exchange Server users and services can be authenticated by the domains containing the Microsoft Exchange Server computers. Remember that all Microsoft Exchange Server computers in a site must use the same service account.

Naming Conventions

You must provide names for directory objects when you install and configure Microsoft Exchange Server. Carefully planned naming conventions make it easy for you to add sites, connectors, and other directory objects. You should choose names for your sites and servers that won't be affected by organizational changes. The following table lists the naming conventions used by Ferguson and Bardell:

Element name	Naming convention
Organization	Company name; for example, Ferguson & Bardell.
Sites	Geographical location; for example, NAmerica-W.
Servers	Geographical location; for example, SanFrancisco01.
Mailboxes	First and last names; for example, Maria Black.
E-mail alias	Letters of the first and last name; for example, *mariabl.*

Every object in the organization has a display name and a directory name. You can change the display name of an object, but the organization, site, and server directory names can't be changed.

By default, the directory name is used to generate e-mail addresses. The Setup program maps the directory name elements, such as organization and site name, to the e-mail addresses, according to the naming conventions for any given system. For example, the Internet address for a user called Maria Black is *mariabl@NAmerica-W.FAB.com.*

Directory Names

All directory objects are uniquely identified by a *distinguished name* (DN), which includes the full name, organization name, and site name. For example, the distinguished name for Maria Black's mailbox (MariaBl) is:

```
o=FAB/ou=NAmerica-W/cn=recipients/cn=MariaBl
```

where: **o** (organization) indicates the organization name, **ou** (organizational unit) indicates the site name, **cn** (common name) indicates the Recipients container, and **cn** (common name) indicates the e-mail alias.

Organization Name

Choose a unique organization name. The organization name will be part of the directory names of all directory objects, such as mailboxes, public folders, and distribution lists. It is used to generate e-mail addresses and can contain up to 64 characters. You can't change the directory name after creating it.

Site Names

Choose unique site names. Sites can be named by geographic or physical location, or by function. Site names are used to generate foreign e-mail addresses and directory names. Site names can contain up to 64 characters.

Server Names

By default, the Windows NT Server computer name is used for the Microsoft Exchange Server name. For this reason, it is important to plan what names you want to use for your Microsoft Exchange Server computers *before* you install Microsoft Windows NT Server. Server names can contain up to 15 characters and must be unique.

Note To change the server's name after installation, you must remove the server from the site, rename the server, and then reinstall Microsoft Exchange Server.

The following characters *can't* be used in server names:

Character	Symbol
•	Bullet
¤	Currency sign
¦	Broken vertical bar
§	Section sign
¶	Paragraph sign
#	Number sign
$	Dollar sign
;	Semicolon
^	Accent circumflex, carat
,	Comma
“	Curly quotation mark
{ }	Brackets
~	Tilde

Mailbox Names

Choose mailbox names that are easy to identify. You may also want to consider coordinating mailbox naming conventions with the naming scheme used for Windows NT user accounts or for previous e-mail systems. If you are concerned about the sort order of display names for mailboxes in the Address Book, choose naming conventions accordingly. If you have several users with the same name, establish naming conventions that distinguish the users. For example, if two users in your organization have the same name, specify the users' department names in their display names to minimize confusion.

When you configure a mailbox, you must specify names for different fields.

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	Because some foreign e-mail systems restrict their e-mail addresses to less than 64 characters, use a short name to identify the user. The alias name should be easily recognizable and have some relationship to the user's name. For example, Maria Black's alias name might be *mariabl.* The Microsoft Exchange Server Administrator program generates the directory name by using the first alias name specified for the mailbox.	Up to 64 characters; can be changed.
Display Name	Use the mailbox name as you want it displayed in the Administrator window and in the Address Book. For example, you can use First Name, Last Name (Bill Lee), Last Name, First Name, Initial (Lee, Bill D.), or First Initial, Last Name (BLee). Be consistent so that all mailboxes are displayed in the same way.	Up to 256 characters; can be changed.
Directory Name	By default, this name is generated by using the first alias name specified, but you can determine your own scheme for directory names.	Up to 64 characters; must be unique; cannot be changed.

You can create mailboxes for company resources, such as conference rooms. If you do this, keep in mind that the naming scheme you use determines how these resources are displayed and sorted in the Address Book. For example, the naming scheme for conference room mailboxes may be: conference room, building, (size of room). This will be displayed in the Address Book as: Tahoe conference room, 2A, (20).

E-mail Addresses

E-mail addresses are used for routing messages. To communicate with other e-mail systems, Microsoft Exchange Server users must have an address that other systems can understand. Similarly, users in other systems must be represented by e-mail addresses in Microsoft Exchange Server. A user whose address is on another e-mail system but exists in the Microsoft Exchange Server directory is called a *custom recipient.* An *e-mail address* is the address by which Microsoft Exchange Server recipients (mailboxes, distribution lists, public folders, and custom recipients) are known to other mail systems.

Microsoft Exchange Server automatically generates X.400, Microsoft Mail for PC Networks, and Internet Simple Mail Transfer Protocol (SMTP) addresses for each recipient based on the directory name of the site and the organization. For example, the following are e-mail addresses for the user Maria Black, whose mailbox is in the NAmerica-W site in the FAB organization.

Address type	E-mail address
X.400 address	`g=Maria; s=Black; o=NAmerica-W; p=FAB; a=mci; c=us`
MS Mail (PC)	`FAB/NAMERICA/MARIABL`
Internet (SMTP)	*`mariabl@NAmerica-W.FAB.com`*

If third-party gateways are installed, other addresses may also be generated. Gateways typically use the Alias Name field and other fields (such as the organization and site directory names) to generate e-mail addresses. Different gateways have different limits and restrictions for generating addresses.

X.400 Addresses

Microsoft Exchange Server supports X.400 addressing to enable direct communication with other X.400 messaging systems. The X.400 address identifies a Microsoft Exchange Server recipient in the global X.400 address space.

The following are the hierarchically-ordered attributes of an X.400 address:

Attribute	Description
c	Country (required)
a	Administrative management domain, or ADMD (required)
p	Private management domain, or PRMD (required)
o	Organization
ou1, ou2, ou3, and ou4	Organizational units
cn	Common name
q	Generation qualifier
i	Initials
s	Surname (required)
g	Given Name

For example, a valid X.400 address for Maria Black is:

```
c=us;a=mci;p=FAB;o=NAmerica-W;s=black;g=maria
```

The following characters are valid in an X.400 address.

Character	Designation
A, B, ..., Z	Uppercase letters
a, b, ..., z	Lowercase letters
0, 1, ..., 9	Digits
(space)	Space
'	Apostrophe
(	Left parenthesis
)	Right parenthesis
+	Plus sign
,	Comma
-	Hyphen
.	Period
/	Forward slash
:	Colon
=	Equal sign
?	Question mark

Microsoft Mail

If you connect to MS Mail (PC) or Microsoft Mail for AppleTalk Networks (also known as Quarterdeck Mail) systems, you can use a maximum of 10 characters for the Microsoft Mail network name, postoffice name, and mailbox name.

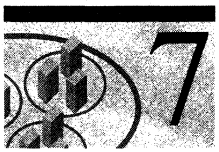
SMTP

If you connect to the Internet or other SMTP systems, consider any character restrictions that SMTP imposes on its addressing scheme. In general, you can use lowercase and uppercase letters (a-z and A-Z; no distinction is made between lowercase and uppercase), numbers (0–9), and hyphens (-). Spaces are not allowed in SMTP addresses. Note that the default address is *user@site.org.com.*

Other E-mail Addresses

If you connect to foreign systems using third-party gateways, such as IBM Professional Office System (PROFS) and SNADS, consider the character restrictions. For example, PROFS and SNADS addresses usually contain only the uppercase letters (A-Z), numbers (0–9), and the following special characters: $, #, and @. When configuring recipients, restrict the characters that you use in the Alias Name field to the number allowed.

Site Connections



After you choose sites and the site boundaries, you can connect them by using the Site Connector, an X.400 Connector, the Internet Mail Service, or a Dynamic RAS Connector.

Site Connector The simplest way to connect two sites is by using the Site Connector. Following are the advantages and disadvantages of using the Site Connector:

Advantages	Disadvantages
Minimizes message routing steps.	Connections cannot be scheduled.
Provides automatic load balancing and fault tolerance.	Can saturate network connections when multiple servers attempt to connect at the same time.
The connections in the local and remote site are configured at the same time.	

X.400 Connector Use the X.400 Connector if you want to take advantage of your existing X.400 backbone. To connect two sites by using an X.400 Connector, configure a Microsoft Exchange Server computer at each site to support the X.400 Connector. When the X.400 Connector is configured, you can decide whether to convert messages from their internal format to the X.400 P2 format.

Following are the advantages and disadvantages of using the X.400 Connector:

Advantages	Disadvantages
You can schedule connections.	Bottlenecks may occur because all message traffic must go through one bridgehead server on each site unless you configure multiple bridgehead servers in the site.
You can control message size.	
Enables messages destined for Microsoft Exchange Server recipients to pass in a native (highly efficient) format.	Because specific network protocols are used with the X.400 Connector, you must verify that existing bridges and routers can support these protocols.
Supports Transfer Control Protocol/Internet Protocol (TCP/IP), Transport Class 4 (TP4), and X.25 protocols.	

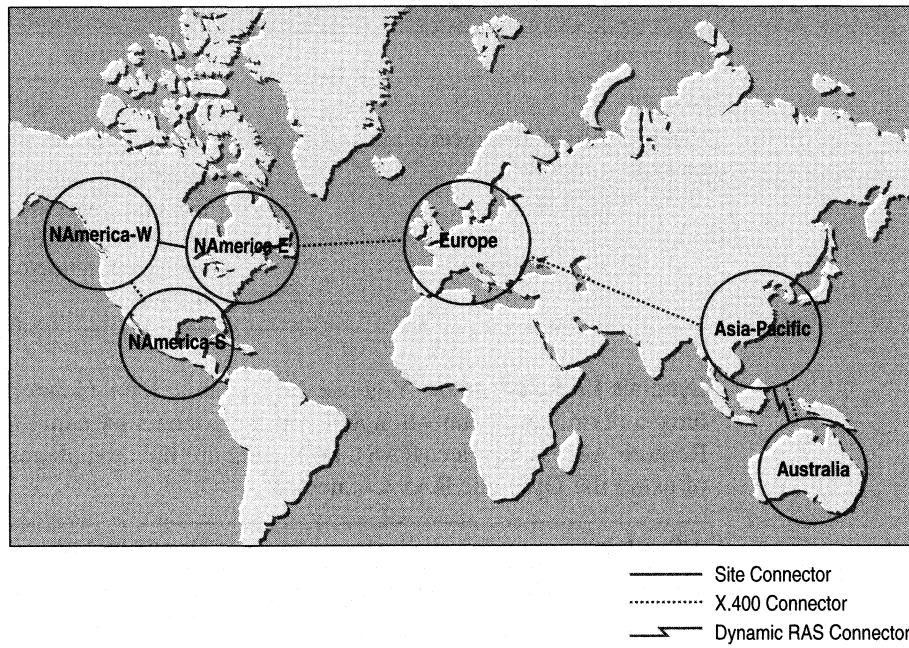
Internet Mail Service You can use the Internet Mail Service to connect sites by using an existing SMTP network as a backbone. Following are the advantages and disadvantages of using the Internet Mail Service as a site connector:

Advantages	Disadvantages
Message sizes can be set.	Connections cannot be scheduled.
Can be configured to receive messages, send messages, or both.	Message format conversion is required.
	Bottlenecks may occur because all message traffic must go through one bridgehead server at each site unless you configure multiple bridgehead servers in the site.

Dynamic RAS Connector You use the Dynamic RAS Connector when you don't have a permanent connection and you can connect by using the Windows NT Remote Access Service (RAS). Following are the advantages and disadvantages of using the Dynamic RAS Connector:

Advantages	Disadvantages
You can control when connections are made.	Data transfer is dependent on the speed of the modem.
Works over asynchronous, nonpermanent connections.	Bottlenecks may occur because all message traffic must go through one bridgehead server on each site unless you configure multiple bridgehead servers in the site. Public folder hierarchy replication can consume significant network bandwidth.
Supports asynchronous and integrated service digital network (ISDN) connectivity.	

For example, Ferguson and Bardell used the following Site Connector, X.400 Connectors, and Dynamic RAS Connector to connect sites in the organization.



Connections to Other Systems

To connect to other systems, you must choose the appropriate connectors.

Microsoft Mail Connector Use this connector to take advantage of existing Microsoft Mail 3.*x* gateways, such as PROFS, SNADS, NetWare MHS, and FAX.

Internet Mail Service Use this connector to connect to the Internet or to an SMTP backbone.

X.400 Connector Use this connector to take advantage of your existing X.400 backbone. This connector supports the following protocols:

- TP0/X.25
- TP4
- TCP/IP

Microsoft Exchange Connector for Lotus cc:Mail Use this connector to transfer messages and synchronize directories between Microsoft Exchange Server and Lotus cc:Mail systems.

Migration

Migration is the process of moving mailboxes and mail from your existing e-mail system to Microsoft Exchange Server. For a smooth migration process:

- Decide migration methods.
- Plan timing and organization issues.
- Plan connections and maintenance.

Before you migrate to Microsoft Exchange Server, you need to make some strategic decisions. You should be able to answer the following questions:

- Which users should be migrated first?
- Should migration be done in phases or all at once?
- What coexistence issues need to be addressed while both systems are in operation?
- What is the best way to maintain directories, foreign system addresses, mail, and messaging applications during and after migration?
- How will offsite users be handled?
- How will connectivity to foreign systems be established?

Migration planning is critical to prevent downtime, data loss, and disruption of information flow. A proper strategy can reduce your administrative duties before, during, and after the migration.

For more information about migration, see *Microsoft Exchange Server Migration.*

Administrative Policy

Your organization plan is a working document. How it is implemented and changed can be influenced by the policies that you establish. When developing and implementing an administrative policy, you need to:

- Establish permissions within the site.
- Delegate administrative duties.
- Document work.
- Prepare for disasters.
- Schedule regular backups.

It is important to establish administrative policies for emergencies, such as a server being corrupted, removed, or destroyed. With emergency plans, you can lessen the severity of disruptions. For more information on disaster recovery planning, see the *Microsoft Exchange Server Resource Guide, Supplement.*

You should define roles and tasks for the people administering Microsoft Exchange Server. You can give one administrator permissions for the entire organization, another administrator permission for individual sites, and another administrator permission for individual servers. You can also give an administrator permission to view, but not change, the hierarchy of the organization, its elements, and its configuration.

To make it easier for the group to administer Microsoft Exchange Server, you can create an Admin public folder to keep administrators informed about system issues.

To reduce administrative duties, you can also create a Windows NT Server global group that includes the Windows NT user accounts for all Microsoft Exchange Server administrators in a site. Membership in this group gives a user all the permissions granted to the group. You can add or remove members. You can also add or remove the permissions assigned to the entire group, rather than to each user account.

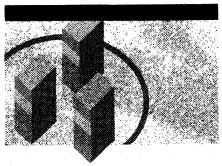
If you are using multiple domains within a site, create this group in the domain where you centralize your administrative functions for the other domains. In a single master or multiple master domain model, create this group and all the user accounts for Microsoft Exchange Server administrators in the master domain.

CHAPTER 7

Planning Your Sites

When you plan your organization, you define the number and location of sites and the connections between them. This chapter helps you plan your sites by outlining factors in determining the number and type of servers required for each site. You should also consider what services your users need. After you gather information about your sites, you can use it with performance data to match users, public folders, and special services with the appropriate hardware.

Planning Considerations



1 Network Layout Within a Site

To reduce traffic across bridges and routers, locate servers on the same local area network (LAN) segments as the users.

2 Integrating Network Operating Systems

If users in your site have a network operating system other than Windows NT Server, you may need to install additional software to integrate the clients with Microsoft Exchange Server.

3 Defining the Users in Your Site

To optimize performance, group users and determine usage patterns.

4 Connecting to Other Sites

When planning connections to other sites, consider redundancy, bandwidth, and network traffic.

5 Message Routing Strategy

When planning connections to other sites and systems, consider your message routing strategy.

6 Client Languages

Consider what languages your users will need.

7 Remote Access

Decide what type of remote access services your site will support.

8 Directory Replication

Consider your strategy for directory replication if your organization spans multiple sites.

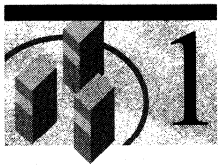
9 Public Folders

Determine how you will provide public folder access.

10 Backing Up and Restoring Servers

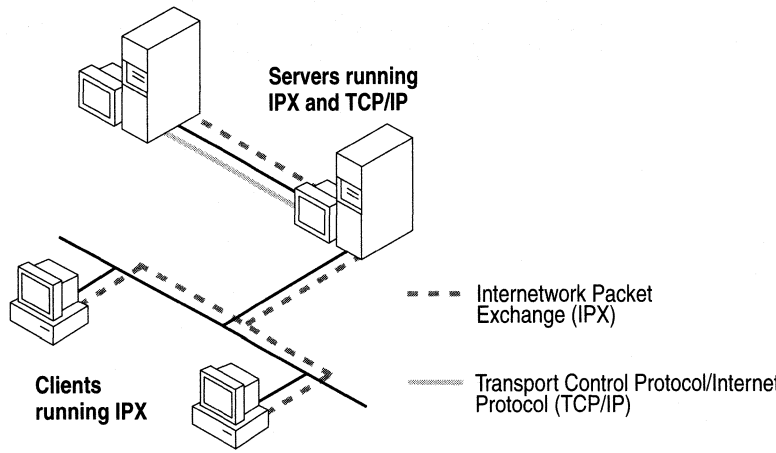
Plan your organization's strategy for backing up and restoring servers, including how frequently backups will occur and the type of backup mode that meets your organization's needs.

Network Layout Within a Site

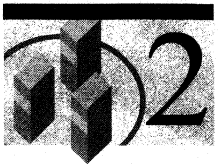


Start your site layout with a drawing of your logical network. Each network segment corresponds to a physical location. For example, one segment can serve a building or a floor in a building. After you determine your network's logical layout, draw diagrams that show the physical location of each network segment.

Within your site, one or more protocols can be routed between every segment of your network. All servers must have at least one protocol in common. Servers can communicate with each other by using protocols that are different from those used for client communication, as shown in the following illustration:



Integrating Network Operating Systems



Both the existing messaging system and the network operating system in a site may impact your site planning. If your organization already has a messaging system, you need to plan how to migrate users from that system to Microsoft Exchange Server.

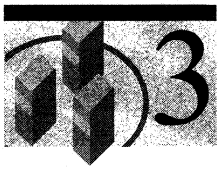
For information about migration, see *Microsoft Exchange Server Migration.* If your site has a network other than Windows NT Server, decide how to integrate clients from the other network into your site. You may need to install additional software on your servers to enable the clients to communicate with the servers.

If a client computer is running Novell NetWare software, it can connect to a Microsoft Windows NT Server computer running Microsoft Exchange Server. Because communication between servers and clients is protocol independent, clients can choose from a variety of configurations to integrate Microsoft Exchange Server with NetWare.

To log on to Microsoft Exchange Server computers, users on NetWare networks must have Windows NT user accounts so they can be authenticated in the Windows NT domain. Microsoft Exchange Server provides source extractors that automate the process of migrating user accounts from NetWare to Windows NT Server.

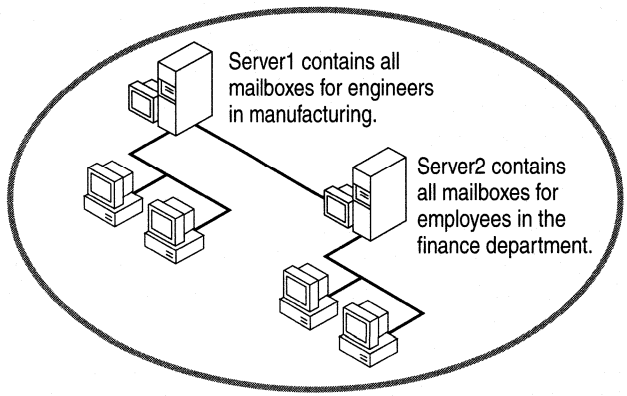
Note If a Banyan VINES client is running the VINES Internet protocol (IP), it can connect to a Microsoft Windows NT Server computer running Microsoft Exchange Server. Microsoft Outlook supports Banyan VINES networking on clients running Windows® for Workgroups, Windows NT Server, and Windows NT Workstation.

Defining the Users in Your Site



To define the people who will be connecting to Microsoft Exchange Server by using e-mail clients, you need to add the users to your layout by grouping them and then examining each group's information needs.

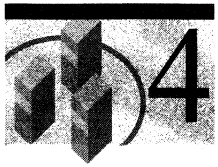
Because people communicate primarily with others in their own workgroup, it may be most efficient to group users together on one server. Microsoft Exchange Server performance is optimized when messages are sent between users on the same server. Hard disk space is also conserved because a message sent to a group of people on the same server is stored as a single copy.



To set up the groups, review your organization chart or survey each LAN segment. Add the groups to your layout with the name of the group and an estimate of the group's size. If a group is too large for one server, break it into smaller groups. Describe your groups in ways that help you design the site.

The amount of messages exchanged among users varies greatly. By predicting the volume of messages, you can better plan your hardware needs.

Connecting to Other Sites



You can configure sites to exchange directory information, public folders, and messages. This section explains how to locate the connections in your site and how this affects your server planning.

When you plan your site, remember that you can limit the volume of information exchanged between sites. You may want to do so if the available connection speed between sites is too slow for the data volume.

If you have more than one site in your organization, you must configure at least one connector to connect with other sites. You also need to determine which servers should host those connections. When planning connections between sites, you should consider the following factors:

Redundant connections Redundant connections prevent a single failure from interfering with mail delivery. For example, if a site has more than one server, you may want to configure more than one connector from different servers in this site to another site. If a server is down, the backup connector on the other server can handle the traffic. You may also want to configure multiple routes for the message, in case the network is down.

Bandwidth between sites You can configure one or more messaging bridgehead servers to connect to other sites. If the available bandwidth between sites is high, you should configure multiple servers in the site to connect with other sites. If bandwidth is low, you can configure a single messaging bridgehead server to control network traffic between the sites.

Message traffic Traffic between sites can consist of directory and public folder replication messages, mail sent from one site directly to another, and pass-through traffic. *Pass-through* traffic, which originates in another site and is destined for a third site, increases the load on the servers that it passes through.

Tailoring Traffic Between Sites

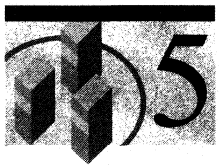
To limit traffic between sites, you should consider the following options:

Limit the size of messages The number and size of messages that users send between sites can vary greatly. You can't limit the number of messages, but you can limit message size to prevent users from sending large messages.

Reduce pass-through traffic There are several ways to reduce pass-through traffic. One way is to have traffic flow through a dedicated messaging bridgehead server with no users. Another is to have traffic flow into the site to one server and flow out of the site from another server, with neither server having any users. Or, have traffic flow into and out of the site on all servers, to distribute the load on all servers.

Consider using public folder affinity When servers in one site are accessible to clients in another site, you can specify public folder affinity between sites, instead of replicating public folders. *A public folder affinity* is a number that is used to determine the order in which connections are attempted. Using public folder affinity reduces network traffic caused by replication, reduces or eliminates replication latency, and reduces required storage space. However, it can cause more network traffic than configuring a replica if users in a remote site frequently access the data.

Message Routing Strategy



Routing between sites or to another e-mail system requires planning and configuration. Here are several strategies for routing messages to other sites:

- To reduce the effect of pass-through mail on multiple servers or servers with mailboxes, concentrate all inbound and outbound mail on a few servers.
- Configure one connector across one connection that has high available bandwidth and high reliability, and that can be carefully monitored.
- Configure multiple connectors across different connections with the cost weighted to the cheapest, fastest, or most reliable connection.

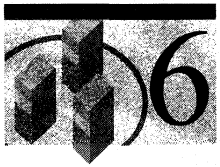
When planning the routing of messages to another system, you should consider such factors as the amount of messages, the effect of pass-through message traffic on servers, and routing costs. You also need to consider how to set up connectors to other systems. Will there be one connector for the entire organization or one or more per site? You need to evaluate the structure of your organization and the advantages and disadvantages of each configuration.

If there is only one connector to the other system, messages must pass through other sites to reach the site with the connector. This pass-through traffic may increase intersite traffic. For this reason, it may be more cost-effective to route messages from one site. For example, if you use a fax gateway, long-distance charges may be lower from one site than another.

You can also route messages through multiple connectors to minimize pass-through traffic. Gateways in multiple sites may also be more economical. In the case of the fax gateway, if you want the sites to pay their own long-distance fax charges, you should install a connector or gateway in every site.

For more information on routing, see "Planning Connections to Other Sites and Systems."

Client Languages

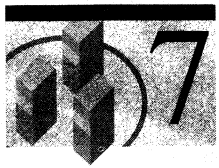


Microsoft Outlook is available in many languages. Any Microsoft Exchange Server computer can be used with any localized client computers. When you survey your users, consider their language needs. Different languages require different code pages. The Microsoft Exchange Server Setup program automatically installs all code pages for all the available languages on your server.

Foreign language templates display fields (such as user properties in the Address Book) in the user's language. For example, when a user selects the sender's address on a message, the sender's properties are displayed in a template.

You should install the appropriate language templates for your users. By default, Microsoft Exchange Server installs the display templates for your server's language. Additional languages are included on your Outlook compact disc. A template installed on only one server is available to all servers in the site and is automatically replicated to all other servers in the site.

Remote Access



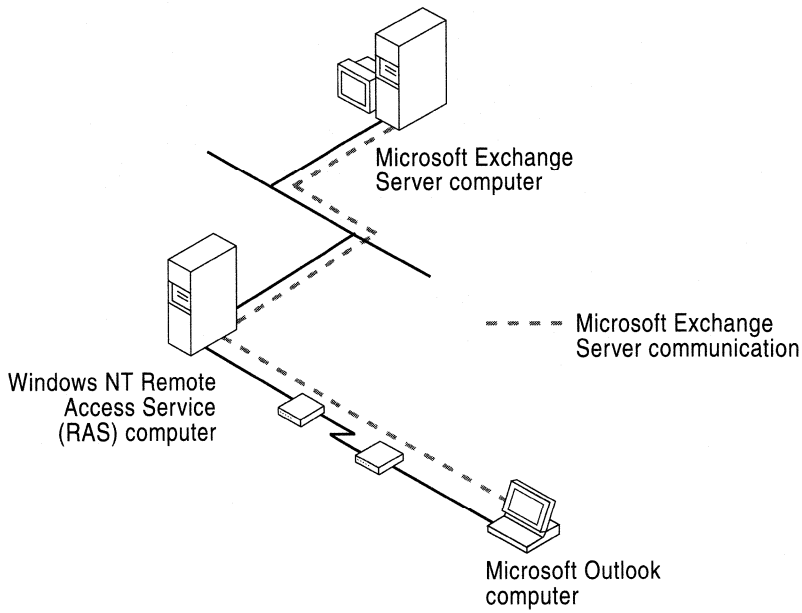
Remote access refers to network access over telephone lines. Some messaging systems have separate client programs for remote computing, but Microsoft Exchange Server has remote networking available to all clients. If users have the appropriate network support and remote communications software installed, they can make remote network connections to personal and public folders on Microsoft Exchange Server computers.

Remote users and mobile users with portable or laptop computers can work offline or online:

Work offline They can use Outlook offline and later connect to a Microsoft Exchange Server computer and send mail composed offline, download new mail, and download the offline address book.

Work online They can use a modem to connect to a Microsoft Exchange Server computer.

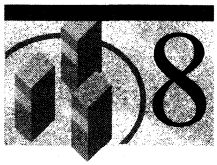
To connect to a Microsoft Exchange Server computer, remote users must use a dedicated remote server or connect directly to a Microsoft Exchange Server computer that provides the remote access software.



Microsoft Exchange Server can run on Microsoft Windows NT Server computers with any of the following remote access software installed:

Remote access software	Description
Microsoft Windows NT RAS server	Supports connections from RAS and ShivaRemote clients.
Shiva LanRover	Supports connections from ShivaRemote and RAS clients.
Other	Any remote access server software that is compatible with RAS or the network software that is currently used by your mobile users.

Directory Replication



Within a site, you don't need to plan directory replication because all directories are automatically synchronized. However, you do need to plan and configure directory replication between sites, beginning with these steps:

1. Determine your directory replication topology.
2. Identify the replication bridgehead servers.
3. Determine a schedule for directory replication.

The directory replication topology affects the time it takes to fully replicate directories. Because it is difficult to change your directory replication topology after it's in place, careful planning is important. Your topology must include all sites in your organization. It will grow with your organization as new sites are added. Your topology should also minimize the number of sites through which messages are replicated.

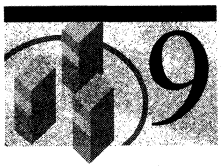
In addition, your replication topology should map to your messaging topology so that directory replication messages travel on the least costly connections.

You should also decide how many bridgehead servers to configure for each site. If you have many sites, consider balancing the load among servers by choosing a different bridgehead server for each remote site. You can add bridgehead servers as new sites are added. When you configure directory replication, remember that replication generates message traffic.

You also need to determine when directory information should be exchanged with other sites. The directory replication schedule is based on how often your organization needs an updated directory. If replication occurs too frequently, bridgehead servers won't be able to receive and process replication messages before they request new updates. This results in redundant requests.

If two sites are connected through a slow connection, schedule directory replication between these two sites so that the slow connection is used only occasionally. This minimizes the use of that connection and improves performance.

Public Folders



If users will access public folders, will they connect to public folder replicas in their site, or will they connect to public folders in remote sites by using public folder affinity?

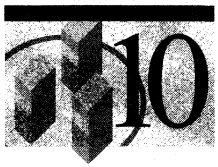
Determine when public folder replications will occur between sites. When you configure the public folder replication schedule, remember that message traffic will also be generated.

If your users frequently connect to public folders in another site, you should replicate the public folders to the local site to minimize traffic across the site connection. If your users do not connect to public folders frequently in another site, configure public folder affinity between the sites to minimize replication traffic across the connection. If there are multiple sites with a replica of the same folder, determine the order of connection attempts, based on a public folder affinity cost parameter.

You should also consider how you group servers into locations. A location is a group of servers connected across a network. By grouping servers into locations, you enable users to access public folder replicas more quickly because each server automatically searches for public folder replicas within its location.

Also consider who has permission to create top-level public folders and how public folders should be organized. For example, you could organize public folders by topic, language, or department.

Backing Up and Restoring Servers



It is very important to create backups of your Microsoft Exchange Server files. Creating backups enables you to restore your server in the event of a hardware failure or software corruption. When you plan your backup strategy, consider the following:

Location of tape drives If your tape drive is on a server, consider the impact the additional load will have on the other services the server provides. Depending on how many tape drives you have, you may decide to provide tape backup on most servers to avoid backing up data across the network.

Capacity and speed of your hardware The capacity and speed of your hardware are important because these factors determine how quickly you can perform a complete restore in the event of a disaster. The time required to back up and restore a server is determined by a number of factors, including the tape drive speed, the speed of the network, CPU speed, available memory, and the amount of load on the server. You can back up and restore data more quickly by using a tape drive located on a server rather than on the network.

Circular logging Circular logging overwrites transaction log files after the data they contain has been committed to the database. By enabling circular logging, you reduce disk storage space requirements. However, you will only be able to restore information to the last full backup—not to the last transaction. Also, if you plan to use circular logging, note that you cannot perform incremental or differential backups.

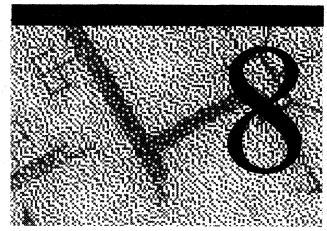
Backup schedule You may decide to perform a full backup once a week and an incremental or differential backup during the week. You should back up the information store as often as possible, depending on the server load. You should also back up the directory of each server at least once. Back up the directory for at least one server daily, but rotate which server you are backing up. The advantage of having a more current directory backup is that fewer changes will need to be replicated when the restore is completed.

Storing backup tapes at another location To avoid losing all your backup tapes in the event of a disaster (such as a fire), store tape backups of the most important data in your organization at another location.

Validating your backups Verify that your backups are being performed correctly by restoring the information store on an alternate server and sending messages from a mailbox on the server.

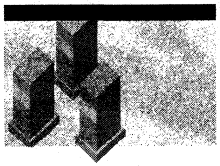
CHAPTER 8

Planning Your Servers



After you plan your organization and sites, you need to plan the number and type of servers, and the number of users that each server will support. The number of servers in a site depends on the number of users to be supported, and the number of public folders and connectors you need. However, for efficient administration, no site should have more than 50 servers. You can use the scaling information, your site layout, and the recommendations in this chapter to plan your hardware and software requirements.

Planning Considerations



1 Server Roles

Consider special services, such as connectors and public folders, that affect server loads and hardware. Also plan which servers will be Windows NT domain controllers.

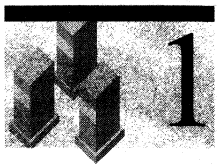
2 Server Hardware

Consider performance when planning server hardware.

3 Designing Servers

Consider user needs and the load placed on servers when you start designing your server layout.

Server Roles



All Microsoft Exchange Server computers in a site can perform the same functions, including directory services, message transfer, and message storage. Some servers can contain additional software and perform specialized services. Before planning server hardware, users needs, and network placement, determine which services you need in your site and how they affect your plans.

In addition to hosting mailboxes, servers can:

- Provide messaging connectivity to other sites, foreign systems, or the Internet.
- Provide directory replication between sites.
- Provide directory synchronization with foreign systems.
- Act as a Key Management server for the organization.
- Store public folders.

You can also provide these additional Windows NT Server services:

- Domain controllers
- Remote Access Service (RAS) servers

If all your servers have a standardized configuration and a consistent user load, distribute these services evenly among all servers in the site.

Connectivity Server

If you want to communicate with other sites or foreign systems, you must install and configure the appropriate connector. Any server can run the connectors. A single server can run multiple connectors of different types. Connectors increase the load on a server. To reduce the load, you can install the connector on a server that has no mailboxes.

Key Management Server

If you plan to use the advanced security features of Microsoft Exchange Server, configure only one server in your organization to store and manage the advanced security database. This server is known as the Key Management (KM) server.

When configuring the KM server, consider the following:

- The KM server should be in the domain where you plan to centralize administration.
- The KM server must be physically secure and backed up regularly.
- The KM server must use the Windows NT Server file system (NTFS) format.

For maximum security, configure your KM server as a dedicated server in a separate site. The load on the KM server is negligible because the server is primarily used for generating keys, which is done infrequently.

Public Folder Server

By default, every server in your site can maintain public folders. You can, however, dedicate a server in the site to maintain all public folders. You can use the Administrator program to delete either the public or the private information store if you want to dedicate the server to a particular role. A site can have one or more public folder servers.

One or more servers can use the same public folder server. Dedicating a server to public folders provides the following advantages:

- Reduction in memory, CPU, and disk requirements on the mailbox server.
- Simpler planning and administration of servers.
- Improved performance in mail delivery.
- Easier back up of public folders.

When choosing a public folder server, consider disk type, disk space, and future expandability. The public information store should be on a fast, striped drive for best performance. Also consider increasing the RAM and CPU power of this server, especially if the public folders are large, searched and sorted, and replicated to other servers.

Domain Controllers

Windows NT Server computers can serve as domain controllers that authenticate logon requests within each domain. There are two types of domain controllers:

Primary domain controllers (PDCs) A domain has only one PDC, which maintains the security database of all user account information in the domain. All changes to the security database must be made on the copy stored on the PDC.

Backup domain controllers (BDCs) A domain can have any number of BDCs. Although not required, one or more BDCs provide load balancing and fault tolerance. A BDC also stores copies of the domain's security database and can be used to authenticate user names and passwords when the PDC is not available. Because the PDC automatically replicates all changes to a BDC, the BDC is always up-to-date, so that the domain continues to function if the PDC fails.

Although a Windows NT Server computer with Microsoft Exchange Server installed does not have to be a domain controller, you should decide whether to host Microsoft Exchange Server on domain controllers. Base your decision on the type and number of servers available in the site.

You can designate one Microsoft Exchange Server computer as a domain controller if it has enough capacity to perform Microsoft Exchange Server tasks and authenticate logon requests.

In large domains, the most significant issue for domain controllers is the amount of memory. Domain controllers supporting more than 15,000 users should have enough memory to perform administrative tasks. Estimate the necessary amount of memory according to the size of the *Security Accounts Manager* (SAM) *database,* which holds security information, including user account names and passwords. The domain controller needs approximately three times the system memory of the SAM database.

If the Microsoft Exchange Server computers are the only Windows NT Server computers in your network, designate one of them as the PDC. The others can be designated as BDCs or servers without domain control responsibilities. Alternatively, you can dedicate Windows NT Server computers as domain controllers.

Place your domain controllers in a domain with reliable network connectivity. If a domain has servers at different physical locations connected by a wide area network (WAN) connection, each location should have at least one BDC.

In a large domain, the domain controller can be very busy validating Windows NT user accounts as users log on. You can install a Windows NT Server computer to act as a domain controller to transfer this workload from the Microsoft Exchange Server computer.

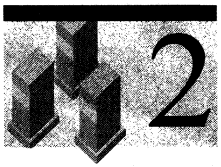
You should configure at least one server as a BDC, but you should have several BDCs in a domain. In a site with slow or unreliable connections, have at least one BDC in every segment of the WAN. If the connection to the main part of the network is down, the BDC can continue to validate all the local users.

RAS Server

If your users need remote access connectivity, they can connect to Microsoft Exchange Server by using a dedicated RAS server, or they can connect directly to a Windows NT Server computer, which provides both Microsoft Exchange Server and RAS connectivity.

To run Microsoft Exchange Server on a RAS server, you may need to add resources to compensate for the increased load. Generally, you should increase the processor speed and the amount of memory for every simultaneous connection you expect.

Server Hardware



Your hardware decisions will have a significant effect on the performance of your Microsoft Exchange Server system. Carefully consider the following hardware issues:

- Disk quantity, capacity, and speed
- Memory
- Type and number of processors
- Type and number of network adapter cards
- Outside communications hardware, such as modems or X.25 adapters
- Number of users or services on the server
- Expandability
- Type and number of tape drives for backup

With the user information gathered during site and organization planning, determine the maximum number of simultaneous users on your server. If the server provides other services, such as connections to MS Mail (PC) or the Internet, such services may require more server resources or may support fewer users per server.

For more information about performance, see Appendix A, "Optimizing Performance," or the *Microsoft Exchange Server Resource Guide, Supplement.*

Planning for Growth

When choosing hardware for servers, consider future needs and choose servers that can be easily expanded. As the number of users and connectors in a site grows, you can reconfigure the existing hardware rather than add more servers. There are several ways to make the most of existing server hardware for Microsoft Exchange Server:

- Increase the amount of system memory for each server.
- Upgrade the processors on existing servers or use multiprocessors in existing servers.
- Increase the number, speed, and size of the disks or disk arrays.
- Add more disk drives to the volume set.
- Replace disk drives and volume sets with striped drive arrays.
- Limit the number of non-Microsoft Exchange Server software processes on the server by moving them to other computers.

By planning ahead, you can choose hardware that can be easily upgraded. If you identify a bottleneck after installation, you can upgrade rather than purchase a new server or change the site layout.

Distributing or Concentrating Servers

Hardware that can be used with Microsoft Exchange Server ranges from single processor 486 computers to the most powerful configuration that Windows NT Server supports. Therefore, you can have an organization of 10,000 users, with 100 users on 100 servers, or with 500 users on 20 servers. This decision depends on your organization's needs and budget.

The following table lists the advantages and disadvantages of using more computers that are less powerful:

Advantages	Disadvantages
Fewer users are affected when a server fails.	There is more hardware to maintain.
Each server can be customized to meet user needs.	Customized hardware increases support costs.
It's less expensive to increase capacity.	Minor increases in users or load require more hardware.
More hardware choices are available.	Bottlenecks increase with fewer users per server.
Each server can be physically close to the users, reducing network traffic for client/server interactions.	

The following table lists the advantages and disadvantages of using fewer computers that are more powerful:

Advantages	Disadvantages
The system is designed for upgrades.	Network adapters must be able to handle more traffic to each server.
There is less network traffic. With more users per server, there is more local delivery.	Larger information stores take longer to back up and restore.
There are less storage requirements.	More users are affected when a server fails.
Fewer replication changes are required.	

Planning Processor (CPU) Needs

Microsoft Exchange Server needs enough processing power to handle requests from clients and other servers in the site and to handle optional services such as third-party gateways, connections to other sites, RAS servers, and file servers for client installations. If your I/O subsystem is fast and is not a bottleneck, and if you have enough memory to handle Microsoft Exchange Server services and other services, a fast processor improves performance.

Multiple processors can significantly increase a server's performance. However, some overhead is associated with using multiple processors. Although Microsoft Exchange Server is designed for maximum scalability across processors, performance will improve by adding a second or third processor. The more processors added, the smaller the incremental performance increases. Not all servers need multiple processors, and not all hardware can support multiple processors, so plan your choices accordingly.

Planning Memory Needs

Microsoft Exchange Server runs on a wide range of hardware configurations and makes the best use of physical memory. For optimal performance, your servers should have enough physical memory to avoid heavy use of the system page file. Because accessing the page file is much slower than accessing physical memory, increasing the amount of memory can greatly improve performance. However, other hardware resources, such as the CPU or I/O subsystem, may become bottlenecks as you increase physical memory.

The size of the Microsoft Exchange Server memory cache is adjusted automatically when you run the Performance Optimizer. By default, Microsoft Exchange Server uses all of the physical memory available. If you run other programs on your servers, you can restrict the amount of memory used by Microsoft Exchange Server.

Planning I/O Subsystem Needs

When planning your server's I/O subsystem, consider doing the following:

- Partition your disks.
- Allocate enough disk storage space for future growth of the information store and transaction log files.
- Choose high-speed caching controllers to increase the speed of disk-intensive processes.

Adding more disk drives will help increase performance, especially if disk I/O is random in nature, as it is with the public and private information stores. All drives have mechanical limitations on performance, so adding more drives distributes the workload more efficiently.

After deciding on a storage solution, run the Performance Optimizer to evaluate the I/O subsystem and to recommend locations for relevant Microsoft Exchange Server files. If new disks are being added to a server, use the Performance Optimizer to experiment with I/O setup.

Partitioning Disks

To expand disk space, before installing Microsoft Exchange Server you can configure your disk for easy volume-set expansion. You should configure multiple physical disks into one virtual disk or striped set to host your Microsoft Exchange Server databases. Disk striping creates a virtual disk over two or more disks, which provides high capacity and high performance.

Hosting the page file on the same striped set as the databases improves I/O performance; this is important for servers low in memory.

If your computer has multiple disk drives, you may also want to consider other disk administration options (such as disk striping with parity and disk mirroring) to increase fault tolerance.

For more information, see your Windows NT Server documentation.

Disk Usage for Transaction Log Files

One of the most important performance considerations is whether to put the information store transaction log file on its own physical disk. Using a dedicated physical disk for files increases fault tolerance and system performance. The Performance Optimizer can be used to configure the directory transaction log files so that they reside on their own disk drive. Use the Windows NT file system (NTFS) format if the server will be backed up infrequently or if the size of the log files may grow to more than 2 gigabytes (GB).

Modifications to the directory database are usually infrequent, so putting the directory transaction logs on a separate drive isn't necessary. However, you can put the logs on servers used for large directory imports (running the directory synchronization component) or servers used primarily for large directory modifications.

If the Microsoft Exchange Server computer has only a few drives and a small amount of memory, and it can't support many users, you can put transaction log files and databases on the same striped set. However, the increased sensitivity to insufficient memory causes performance to decrease as the load on the server increases. When in doubt, dedicate a disk to the log files—disks are cheaper than memory.

Disk Usage for the Information Store

In addition to planning disk space and usage for transaction log files, you should consider disk capacity for the information store. A server can have only one private and one public information store. The size of the information store grows as mailboxes, public folders, connectors, remote users, log files, and messages grow in numbers.

To improve performance, control the use of disk space by placing limits on the:

- Size of mailboxes
- Size of messages
- Age of information in public folders
- Size of public folders

Later, you can adjust your available disk space by using the following strategies:

- Add another server to the site and move a group of mailboxes to the new server.
- Move public folders to other servers in the site and don't replicate them within the site.
- Increase the frequency of connections to other sites and systems, to keep outbound queues small.
- Monitor the amount of disk space used by individual mailboxes, and have users delete outdated mail messages or configure the information store to automatically delete old messages.
- Replace the existing disk with a larger-capacity disk or add more disks.

Choosing Caching Disk Controllers

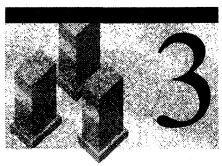
Choose a server that has a caching disk controller with a high-speed bus interface, such as the Peripheral Component Interconnect (PCI) PC Card. These controllers provide optimal performance for Microsoft Exchange Server. Most of these controllers support hardware disk striping, which offers greater performance and less CPU use than Windows NT Server software striping.

Planning Network Adapters

Microsoft Exchange Server makes the best use of network resources. High-speed network adapters and network drivers optimize Microsoft Exchange Server performance. High-speed network adapters can achieve high throughput rates with low CPU use.

Because many clients will be simultaneously using the server, you should install one or more high-performance network adapters, based on a high-speed bus such as PCI or Extended Industry Standard Architecture (EISA). Installing multiple adapters in a multiprocessor server means that a single server can handle more clients, with each adapter servicing a separate network segment or protocol.

Designing Servers



When designing your servers, consider load—specifically the number of users each server will host and the users' e-mail usage patterns. Also consider the effect of additional loads on the server and whether you plan to use many low-end servers or a few high-end servers.

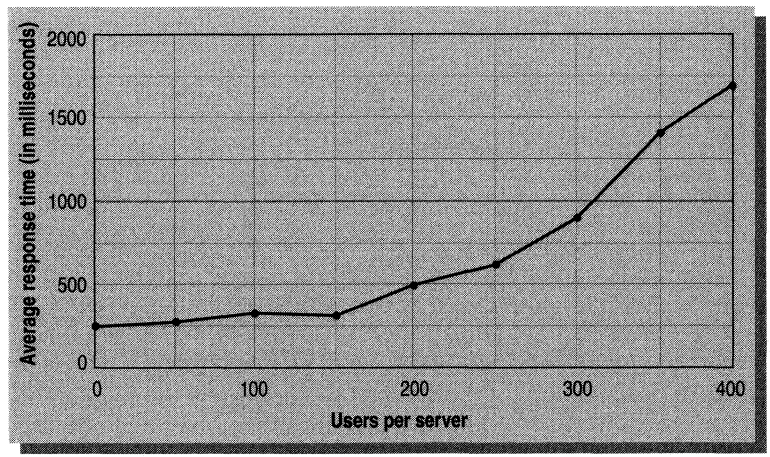
If you expect significant load, use more powerful servers. The following table shows possible configurations:

Server type	Processors	RAM	Disk configurations	Users
Low-end	1 Intel Pentium	32 MB	2 – 2 GB	100 – 300+
Middle	1 Intel Pentium	64 MB	5 – 2 GB	250 – 600+
High-end	3 Intel Pentiums	256 MB	8 – 2 GB	500 – 1,000+

Note Systems with reduced instruction set computer (RISC) processors may require more memory than Intel systems.

The number of users per server type may vary, depending on your definition of acceptable performance. For example, a low-end server might be able to support 320 users with average client response times of one second, as shown in the following graph:

Light users on a low-end server



Planning Site Layout

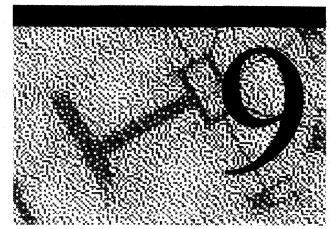
The site layout provides many views of user groups and their needs. When planning your sites, consider the following suggestions for designing your servers so that you make the tradeoffs that best suit the needs of your organization.

- Locate users and their home server on the same network segment. High network bandwidth between user and server is more important than high network bandwidth between servers.
- Group mailboxes that send messages to each other on the same server to take advantage of local delivery and single-instance storage.
- On a WAN, keep users on the same local area network (LAN) segment as their server to reduce the network traffic across bridges and routers.
- On a WAN, distribute client installation points, network shares, and the Microsoft Exchange Server Administrator program.
- Distribute mailboxes and important public folders so that failure doesn't stop business.
- Concentrate mission-critical mailboxes, public folders, and connectors on servers with fault-tolerant or upgradable hardware.

For more information, see Chapter 7, "Planning Your Sites."

CHAPTER 9

Planning Connections to Other Sites and Systems



After you plan your Microsoft Exchange Server organization, sites, and servers, you can plan connections to other sites and systems. This chapter provides an overview of the steps for setting up these connections. For information about configuring connectors, see *Microsoft Exchange Server Operations.*

Following are important considerations:

Messaging processes Microsoft Exchange Server routing and addressing processes will influence your connection plans, especially if you will be routing messages over multiple or restricted connections.

Types of connections Local area network (LAN) or wide area network (WAN) connections typically provide the highest throughput, but other connection types may be used.

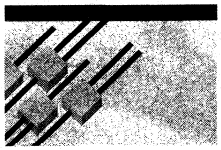
Network protocols and addressing A common network protocol must be configured on each system that communicates over a LAN or WAN connection, and systems must be able to communicate with each other over the network.

Message transfer protocols Message transfer protocols used between your sites or used by other messaging systems may determine your choice of connectors.

Message transfer options Each message transfer protocol provides a variety of message transfer options for configuration on each connected system.

By using Microsoft Exchange Server, you can establish communications between sites and with numerous foreign systems. The following sections describe how to choose and configure the Site Connector, Microsoft Mail Connector for PC Networks, Microsoft Mail Connector for AppleTalk Networks, X.400 Connector, Internet Mail Service, and the Microsoft Exchange Connector for Lotus cc:Mail. This chapter also describes the various types of routing costs.

Planning Considerations



1 Routing

Consider how message routing affects server efficiency. Modify routing by assigning costs to each connection, or by setting a schedule for desired connection times.

2 Site Connector

Deliver a message to any server in a remote site by using the Site Connector.

3 X.400 Connector

Connect Microsoft Exchange Server sites across slower network connections and private or public packet networks. Also, connect to foreign systems by using X.400 services.

4 Internet Mail Service

Use the Internet Mail Service to exchange information with foreign systems that use the Simple Mail Transfer Protocol (SMTP).

5 Microsoft Mail Connector for PC Networks

Connect Microsoft Exchange Server and one or more MS Mail (PC) systems by using the Microsoft Mail Connector.

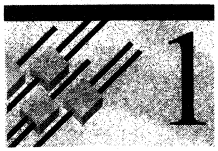
6 Microsoft Mail Connector for AppleTalk Networks

Connect Microsoft Exchange Server and one or more Microsoft Mail for AppleTalk Networks (also known as Quarterdeck Mail) systems by using the Microsoft Mail Connector.

7 Microsoft Exchange Connector for Lotus cc:Mail

Connect Microsoft Exchange Server and one or more Lotus cc:Mail systems by using the Connector for cc:Mail.

Routing



Understanding how routing works can help you configure the Microsoft Exchange Server for efficient message transfer. Messages are submitted to a Microsoft Exchange Server computer by a user, another Microsoft Exchange Server computer, or a foreign mail system through a connector or gateway.

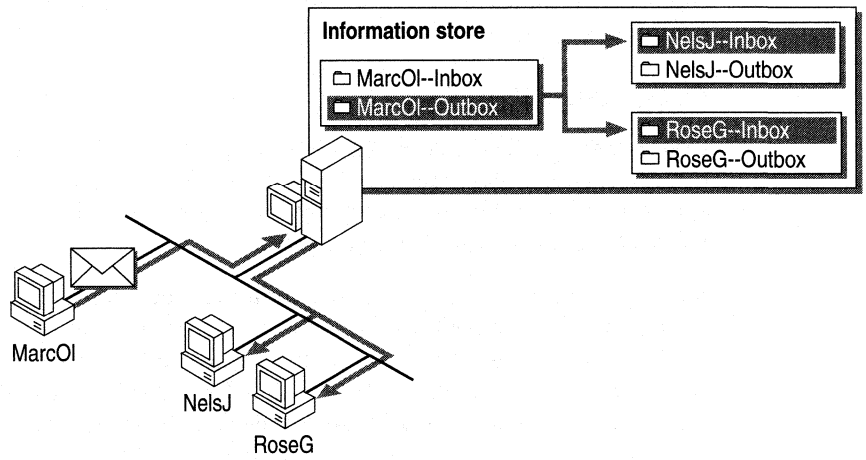
Messages can be routed to the following:

- A recipient on the same server.
- A recipient on a different server in the same site.
- A recipient in a different site or foreign system.

Routing to the Same Server

When the recipient is on the same server as the originator, the Microsoft Exchange Server information store delivers the message directly to the recipient's mailbox. The recipient's distinguished name (DN) is used to route the message.

As shown in the following illustration, a message from MarcOI is delivered to NelsJ and RoseG by the information store on the same server.



Routing to a Different Server in the Same Site

When the recipient is not on the same server as the originator, the message transfer agent (MTA) uses the recipient's DN to determine the location of the server and routes the message to the other Microsoft Exchange Server MTA. The MTA delivers the message to the information store.

Routing to a Different Site or Foreign System

Messages sent to recipients in other sites or systems are delivered through connectors. To determine which connectors to use, how many connectors to use, and how to configure them for efficient delivery, you need to understand how routing works. The Microsoft Exchange Server MTA can route messages to:

- Another Microsoft Exchange Server MTA in a different site (through the Site Connector or Dynamic RAS Connector).
- A remote X.400 MTA (through the X.400 Connector).
- Connectors or gateways that connect to foreign systems, such as the Microsoft Mail Connector or the Internet Mail Service.

Two processes are used to determine which connector a message is sent through: *routing* determines all the connectors that can deliver the message; *selection* determines the most efficient connector to use.

Connector Routing

Connectors and the Internet Mail Service are used to create paths for messages to be sent outside a site. These paths are represented by *address spaces.* An address space is a set of address components used by a connector or service to identify messages that it is responsible for processing.

Messages to other systems are routed through the appropriate address for the system, such as an SMTP address for a message traveling through the Internet. Each connector has at least one address space and can have one or more connected sites associated with it. You define address space and connected sites information by using the **Address Space** and **Connected Sites** property pages in the Microsoft Exchange Server Administrator program. These associations create the Gateway Routing Table (GWART). The GWART is replicated throughout the organization, so each server is aware of all possible routes.

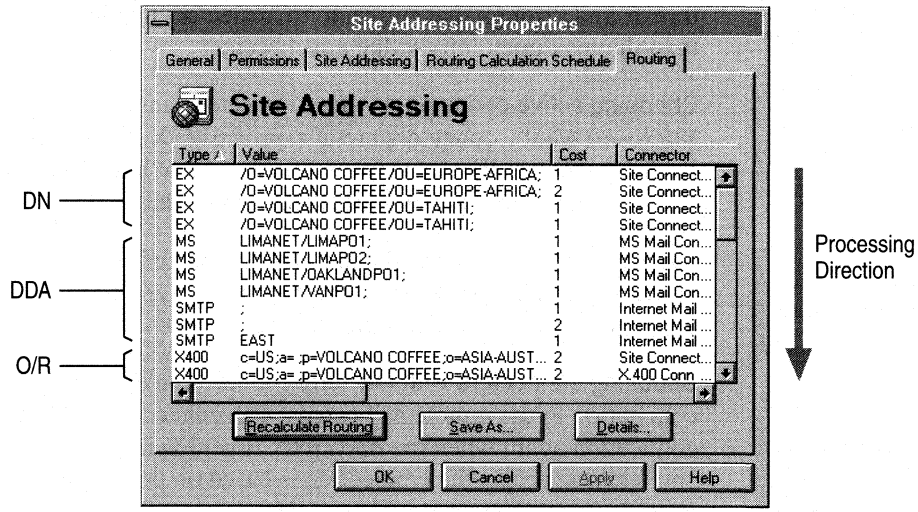
When a message is sent, the MTA compares the recipient's address type with data in the GWART to determine the connectors that can deliver the message. There are three groups of address types:

Distinguished Name (DN) This address type is only searched when a DN for the recipient is found in the directory. This Microsoft Exchange Server address type is EX.

Domain Defined Attribute (DDA) The DDA is the format for a custom recipient address. The address types MS and SMTP are created automatically. However, other DDA addresses can be used with custom or third-party gateways.

Originator/Recipient (O/R) Address This is the X.400 address. The address type is X400.

Each line of the GWART indicates an available path that the MTA can use to route messages. The MTA scans the GWART to find an address space that matches the recipient's address and chooses connectors with address spaces similar to the recipient's address. You can view the contents of the GWART, including the address type each connector routes, in the **Routing** property page of the Site Addressing object as shown in the following illustration.

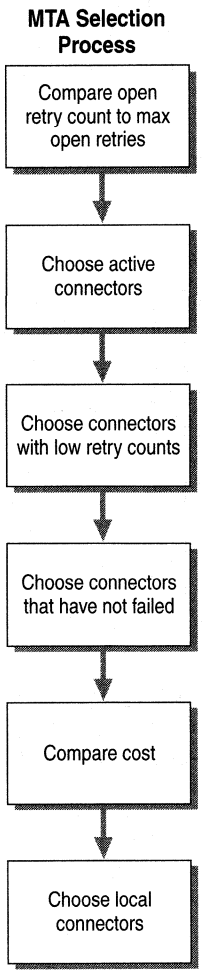


If more than one connector can send the message, a connector selection process determines the most efficient connector to use. If no connectors can service the address space, the message is returned to the originator with a non-delivery report (NDR).

Connector Selection

A selection process is used to identify the connector that can most efficiently deliver the message. Each time a connector or group of connectors meets the connector selection criteria, it is passed to the next step. Each of these steps applies to MTA-to-MTA connections, which include the X.400 Connector, the Dynamic RAS Connector, and the Site Connector. Connectors and gateways for foreign systems are chosen based only on the address spaces they process and the address space cost. Although Microsoft Exchange Server is designed to make routing decisions automatically, you can influence which connectors are chosen by adjusting specific connector settings used in the process.

The flow chart at left shows the steps the MTA uses to select a connector:



Comparing open retry count to max open retries The *open retry count* is the number of times the MTA has attempted to transfer a message through a specific connector. *Max open retries* is a setting on each connector (except foreign system connectors) that specifies the number of times a message can attempt to be transferred through that connector. Connectors that have an open retry count less than the max open retry value are chosen.

Choosing active connectors Site Connectors, Internet Mail Services, and Microsoft Mail Connectors are always active. X.400 Connectors and Dynamic RAS Connectors have activation schedules that have four settings: active now, active in the future, never active, and remote initiated.

All active connectors are chosen first; a group of connectors that will become active is chosen next. If no connectors are active and none will become active, connectors that are initiated remotely are chosen.

Choosing connectors with low retry counts The open retry count starts when the connection to the remote MTA fails. The connector attempts to establish the connection again when the open retry timer expires. The number of times the connector attempts the connection is based on the configuration of the max open retries setting. The open retry counters are compared with each other, and connectors with the lowest number of open retries are chosen.

Choosing connectors that have not failed Each MTA maintains an open retry timer for each connector that is on the same server. Connectors on other servers skip this step. The open retry timer begins as soon as a connection fails. Any connector that is not in a retry state is chosen. The open interval value determines how long the connector waits before attempting the connection again. This prevents the MTA from routing a message to a connector that failed the last time it tried to establish a connection.

For example, if you are using a Site Connector and Dynamic RAS Connector and the LAN is down, a message is routed to the Site Connector because it has a lower cost. The connection fails because the LAN is down so the message is routed to the Dynamic RAS Connector. The next message to arrive before the open retry timer expires on the Site Connector is routed directly to the Dynamic RAS Connector.

Comparing costs You specify costs when the address space is determined for each connector. Connectors with the lowest cost are chosen first. For more information, see "Routing Costs," later in this chapter.

Choosing local connectors A local connector can send the message directly to the remote site, as in a messaging bridgehead server. Remote connectors require the MTA to pass the message to a messaging bridgehead server before the message can be passed to the remote site. Using local connectors reduces the need for the additional processing power and increased bandwidth required to transmit the message.

Load Balancing

If more than one connector is chosen to deliver a message, load balancing is implemented. In load balancing, one of the connectors is chosen randomly, rather than by queue size, message size, or other variables.

In the case of the Site Connector, if more than one Site Connector is selected, the MTA chooses a connector based on cost. Target MTAs with a cost of 0 are tried first, and target MTAs with a cost of 100 are tried last. Random selection is used only after all target MTAs with a cost of 0 have been tried. All target MTAs are tried before the message is rerouted. You can influence which Site Connectors are used more frequently by adjusting the cost value assigned to each connector. A *connection cost* is not a dollar amount; instead, it represents the desirability of one route compared to other routes.

Rerouting and Retries

If the message is not sent to the connector, the MTA attempts to reroute the message. When a message is rerouted, the MTA performs routing and selection again to find the most efficient connector.

When a message is sent to a connector or gateway for a foreign system, such as the Microsoft Mail Connector or the Internet Mail Service, the MTA considers the message delivered when it reaches the connector. Rerouting does not occur, even if the foreign system connector cannot deliver the message.

A message routed to a connector with an activation schedule of *never active* or *remote initiated* is not rerouted unless the activation schedule is changed while the message is waiting to be delivered.

The max transfer retries and transfer interval settings in the **Override** property page for the Site Connector, Dynamic RAS Connector, and X.400 Connector determine how many times and at what intervals the MTA sends a message through the connector. A retry count is stored on each message for each connector that has been tried.

When a message is routed to a connector that fails to connect to the other MTA, the retry count is incremented and the message is immediately rerouted. If the message cannot be delivered after all connectors have been tried, the message is returned with an NDR.

Routing Costs

When a message is sent, the Microsoft Exchange Server MTA determines the number of available routes and compares the routing cost of each connection.

You can influence the routing process by assigning costs to each connection, or by setting a schedule for desired connection times.

Microsoft Exchange Server considers the total cost of a path from end to end, and always chooses the lowest cost route available at the time. Cost values can be assigned from 1 to 100, as described in the following table:

Value	Usage
1	Used 100% of the time.
2 - 99	Lowest values are used first.
100	Used only if no other paths are available.

The administrator evaluates these values to identify primary and backup paths for message transfer. Often these values are assigned based on the dollar cost of a specific network connection.

There are two types of routing costs in Microsoft Exchange Server: address space costs and connected site costs.

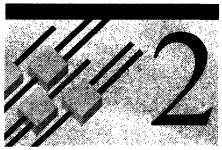
Address Space Costs

Address space costs are used to optimize message routing between sites or with foreign systems. If more than one address space is available, the address space with the lowest cost will be used. For example, a leased-line connection may be assigned a cost of 1, a frame-relay connection a cost of 5, and a satellite connection a cost of 50. You use the **Address Space** property page in the Administrator program to configure address space costs for connectors.

Connected Site Costs

Connected site costs are configured only for connectors that connect Microsoft Exchange Server sites. The connected site costs may be based on the physical costs of sending messages between two sites. For example, a site connected by a Site Connector, on the same physical LAN and using remote procedure calls (RPCs), may be assigned a lower connected site cost than a site connected by an X.400 Connector using X.25. You configure connected site costs by using the **Routing Address** property page, which is accessed by using the **Connected Sites** property page.

Site Connector



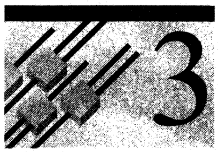
The easiest way to connect two Microsoft Exchange Server sites is to use the Site Connector. The Site Connector enables any server in a site to deliver a message to a server in another site.

A Site Connector maintains a list of *target servers* in the remote site. Any MTA in the local site can choose a target server from this list and send the message to that server. For the message to reach its final destination, the target server may have to forward the message to another server within the same site.

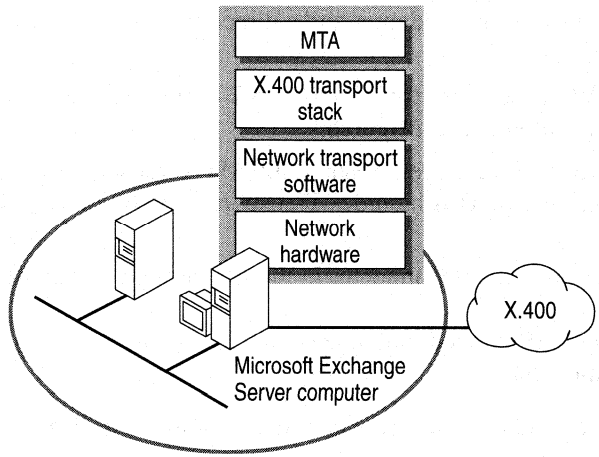
You can designate specific servers to manage communication between sites. To accomplish this, you configure the Site Connector to use *messaging bridgehead* servers. A messaging bridgehead server receives a message from other servers in its own site and then transfers that message to a messaging bridgehead server in a remote site.

To use a Site Connector, you must have LAN connectivity with a protocol capable of using RPCs. To configure a Site Connector between two servers, you must have administrative permissions on both of the servers.

X.400 Connector



The X.400 Connector connects Microsoft Exchange Server sites across slower network connections and private or public packet networks. It also connects to foreign systems through X.400 services. To install an X.400 Connector, identify one Microsoft Exchange Server computer in each site to provide the connection. These servers are called *messaging bridgeheads*. An X.400 transport stack is configured on a specific server, and defines the local system. The X.400 Connector is added to the site, and defines the remote system.



Microsoft Exchange Server site

You need to set up only one X.400 Connector to another system to connect it with your entire organization. Or you can use multiple X.400 Connectors to connect your organization to other X.400 systems.

Before using an X.400 Connector, consider the following issues:

- Bandwidth requirements
- Network transport requirements
- MTA options
- Message content options
- Connections to foreign X.400 systems

Bandwidth Requirements

Each X.400 Connector increases the number of tasks that the Microsoft MTA performs and increases the load on the server running the transport software and maintaining the connection. This load varies, depending on message traffic.

Network Transport Requirements

After you select the type of transport stack you need, install and configure the network software and hardware required to support the connection. For example, to connect to another X.400 system over Transport Control Protocol/Internet Protocol (TCP/IP), install and configure TCP/IP network software for Windows NT Server before configuring an X.400 transport stack and an X.400 Connector.

To use an X.25 connection, at least one Microsoft Exchange Server computer in your site must have:

- An Eicon X.25 port adapter and a direct or dial-up connection to the other system.
- Eicon WAN services for Windows NT Server software (version 3/Release 3 or later) installed and configured.
- A Microsoft Exchange Server X.400 MTA transport stack for X.25 installed and configured. This includes Transport Class 0 (TP0) software for use with X.25.
- At least one X.400 Connector in the site defined to use the transport stack.

To use a TCP/IP connection, at least one Microsoft Exchange Server computer in your site must have:

- A network adapter and connection that supports TCP/IP.
- Windows NT Server TCP/IP network services.
- A Microsoft Exchange Server X.400 MTA transport stack for TCP/IP. This includes Request for Comments (RFC) 1006 software that supports X.400 connections over a TCP/IP network.
- At least one X.400 Connector in the site defined to use the transport stack.

To use a Transport Class 4 (TP4) connection, at least one Microsoft Exchange Server computer in your site must have:

- A network adapter and connection that support TP4.
- Windows NT Server TP4 network services.
- A Microsoft Exchange Server X.400 transport stack for TP4. This includes Connectionless Network Protocol (CLNP) software for use with TP4.
- At least one X.400 Connector defined in the site to use the transport stack.

X.25 services are supplied with Eicon WAN Services for Windows NT Server. TCP/IP software is provided with Windows NT Server, and TP4 is provided with Microsoft Exchange Server. Microsoft Exchange Server X.400 transport stacks are provided with the X.400 Connector software.

MTA Options

You need to configure how the Microsoft Exchange Server MTA transfers information to and from the MTA in a foreign system with these options:

- Route messages. This option controls message transmission through the connected X.400 system, based on the recipient address.
- Restrict user access to the connection. This option prevents certain users from sending messages.
- Control when the MTA connects and transfers messages. You can choose between scheduled, continuous, remote-initiated, and suspended connections.
- Control how the MTA transfers messages to other MTAs after a connection is established. You can choose between two-way or one-way transfer, and whether the sending or receiving MTA initiates connections.
- Override MTA options, such as time limits for urgent message transmission.

In a typical setup, configure the two connected MTAs identically.

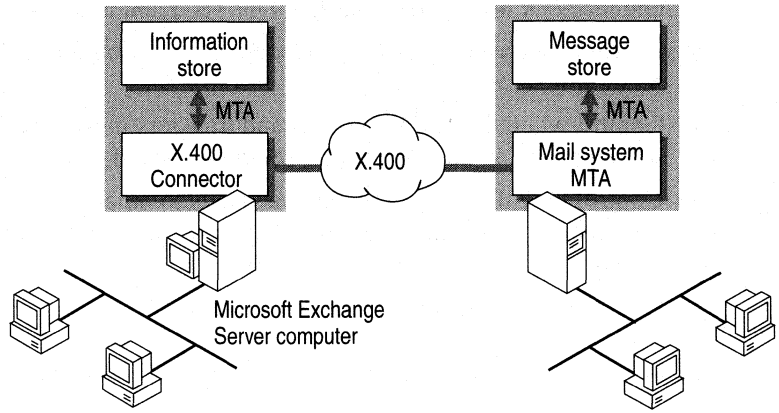
Message Content Options

Message content options are determined by the type of system you are connecting to. If you want to use an X.400 system as a backbone to communicate with another Microsoft Exchange Server site or organization, you may be able to use Microsoft message database encoding format (MDBEF) format. The MDBEF format is the internal message format used by the information store. With MDBEF, no conversion is required, and the message content can be transmitted in compressed form, which reduces the overall load.

Some systems may not recognize the MDBEF format. If this is the case, choose a standard X.400 message format.

Connections to Foreign X.400 Systems

To connect to foreign systems compliant with the 1984 or 1988 X.400 Recommendations, use the X.400 Connector. The following illustration shows the routing system.



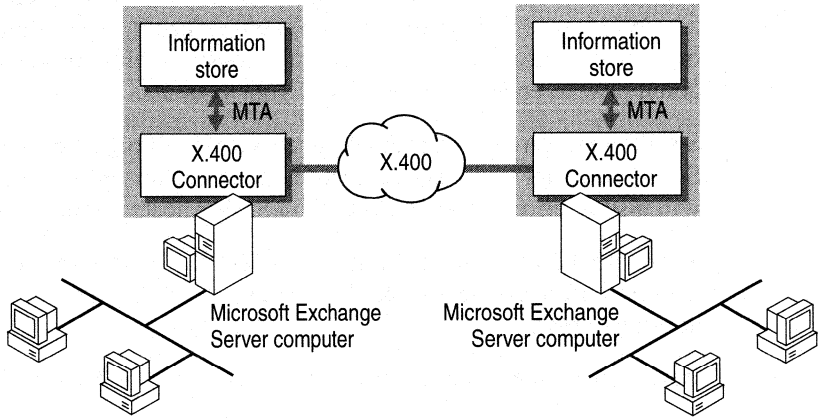
To create this type of connection:

1. Install and configure the necessary Windows NT Server network software and hardware on a Microsoft Exchange Server computer in your site or organization.
2. Set up a Microsoft Exchange Server X.400 MTA transport stack that corresponds to the installed network software and hardware.
3. Define a new X.400 Connector that specifies how to connect and communicate with the MTA of the other X.400 system.
4. Configure the necessary network software and hardware on the other X.400 system.
5. Configure the other X.400 system's MTA to match the configuration of the Microsoft Exchange Server MTA.

When this process is complete, Microsoft Exchange Server can connect and transfer messages to and from the other X.400 system. If additional routing information is configured, messages can also be sent and received from indirectly connected systems.

Backboning over Public X.400

You can connect to another Microsoft Exchange Server site or organization using a public X.400 carrier or another X.400 system through an X.400 Connector. This process is shown in the following illustration.



To create this type of connection:

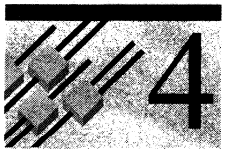
1. Set up message transfer from each Microsoft Exchange Server site to points of connection (MTAs) for the public X.400 carrier (as shown in the illustration), and then verify that messages are correctly routed between each site and its point of connection.

   The points of connection to the public X.400 carrier consist of MTAs, and are either directly or (more likely) indirectly connected to each other as well as to other MTAs.

2. Set up routing between the two public X.400 carrier points of connection so that messages from either point are routed to the correct Microsoft Exchange Server site.
3. Add the X.400 e-mail address of each Microsoft Exchange Server site to the other X.400 Connector address space so that messages for the other site are correctly routed to the public X.400 carrier.

When this process is completed, each Microsoft Exchange Server site can exchange information with the other site over the public X.400 carrier.

Internet Mail Service



You can use the Internet Mail Service to exchange information with foreign systems that use SMTP.

The Internet Mail Service is a component of Microsoft Exchange Server that runs as a Windows NT Server service. When connecting to the Internet, many organizations have security concerns. Consult with your network administrators about how to ensure the security of your systems.

SMTP hosts on the Internet will need access to Port 25 on the Internet Mail Service servers in your organization. Your organization's Internet Mail Services will also require access to Port 25 on SMTP hosts on the Internet.

There are many Domain Name System (DNS) setup issues that you may need to address before connecting to the Internet. Consult with your network administrators.

Before using the Internet Mail Service, consider the following issues:

- Types of configurations
- Installation requirements
- Number of connectors
- Limitations on access given to certain SMTP systems
- Message content options

Types of Configurations

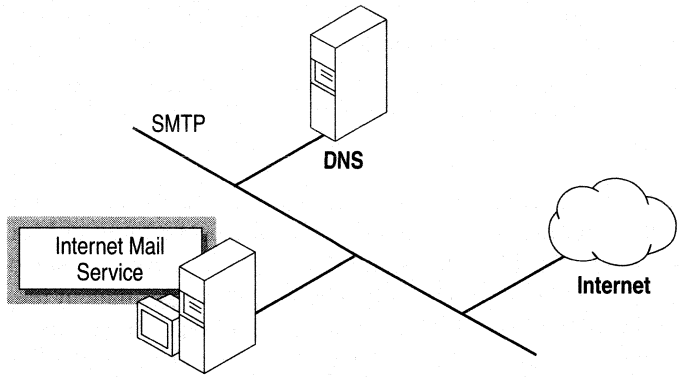
This section describes four types of configurations:

- Connecting directly to the Internet.
- Forwarding mail to a host for final delivery to the Internet.
- Using a dial-up connection with ETRN.
- Setting up Microsoft Exchange Server as an ETRN server.
- Connecting Microsoft Exchange Server sites with the Internet Mail Service.

Connecting Directly to the Internet

With this configuration, you send and receive mail directly to and from other SMTP hosts on the Internet. The Internet Mail Service has two network adapters: one adapter manages the internal network traffic, the other adapter processes mail to and from the Internet. (When TCP/IP is bound to each adapter, the server is referred to as *dual-homed.*)

A server that participates in the Internet DNS must assist with host-name-to-IP-address resolution for destinations on the Internet. Other mechanisms can also be used for host-name-to-IP-address resolution, such as the Windows NT Server local Hosts file or the Windows Internet Naming System (WINS).



To create this type of connection, use the following steps. These procedures are described in further detail in *Microsoft Exchange Server Operations.*

Step	Procedure in Operations
1. Install Windows NT TCP/IP, and configure the host and domain name. If DNS will be used, type the IP address of the DNS server.	Installing and Configuring TCP/IP
2. If using DNS, add the host name, domain name, and IP address to the DNS serving the Internet Mail Service computer.	Adding the Internet Mail Service Computer to DNS
If not using DNS, use the local Hosts file to specify the host name and IP address of the hosts to which the Internet Mail Service will forward mail. Add these hosts to the **Connections** property page of the Internet Mail Service.	Updating the Hosts File When Not Using DNS
3. Add the host name and domain name of the Internet Mail Service computer to DNS or to the Hosts file of SMTP hosts that will forward mail to the Internet Mail Service.	

Step	Procedure in Operations
4. Verify the site address.	Site Addressing
5. Assign the administrator's mailbox and define the address space.	Configuring Internet Mail Service property pages
6. Use Windows NT Control Panel Services to start the Internet Mail Service.	Starting the Internet Mail Service
7. Test the connection to ensure that the Internet Mail Service is configured properly.	Testing the Connection

Before you start the Internet Mail Service, install and configure Windows TCP/IP on the Windows NT Server computer where the Internet Mail Service resides. Configure TCP/IP with a static IP address. Dynamic Host Configuration Protocol (DHCP) can be used, but only when there is a permanent lease on the DHCP IP address. In the TCP/IP DNS configuration, type the server name as the host name, specify a domain name, and provide the IP address of the DNS servers that will be used.

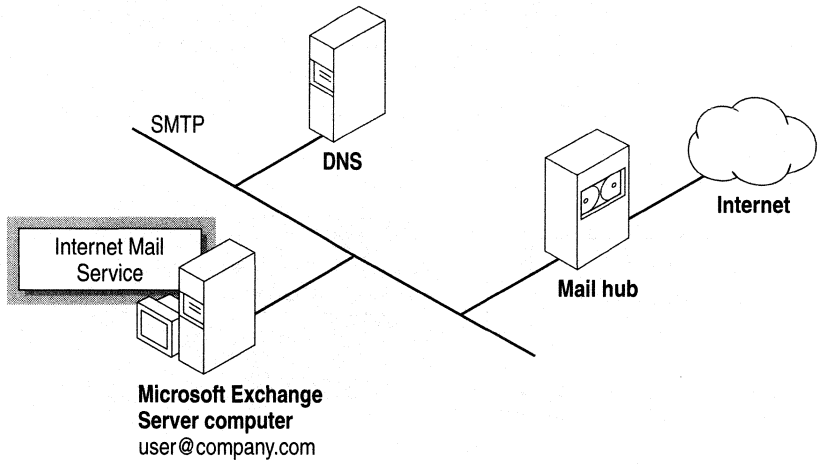
In DNS, you must specify an address record (A record) for the Internet Mail Service. If the name of the host for the Internet Mail Service is the same as the e-mail domain, no mail exchanger (MX) record is needed. Otherwise, add an entry to map the e-mail domain to the Internet Mail Service host name. If you are not using DNS, update the local Hosts file to specify the host name and IP address of the hosts to which the Internet Mail Service will forward mail. Then add the host name and domain name of the Internet Mail Service computer to the DNS or to the Hosts file of SMTP hosts that will forward mail to the Internet Mail Service. The Microsoft Exchange Server site address must match the entry in the DNS.

Use the Internet Mail Service **Address Space** property page to define the address spaces for which the Internet Mail Service is responsible. If the Internet Mail Service will process all SMTP traffic, specify SMTP for the address space with no e-mail domain specified.

To complete the Internet Mail Service setup, specify an administrator's mailbox on the **Internet Mail** property page. The mailbox specified will receive delivery status messages. Use other options for delivery, content, and security settings as needed.

Forwarding Mail to a Host

You may decide to use the Internet Mail Service with an existing mail hub connected directly to the Internet, for all Internet mail traffic. Microsoft Exchange Server will forward all Internet mail to this computer for final delivery to the Internet, as shown in the following illustration.

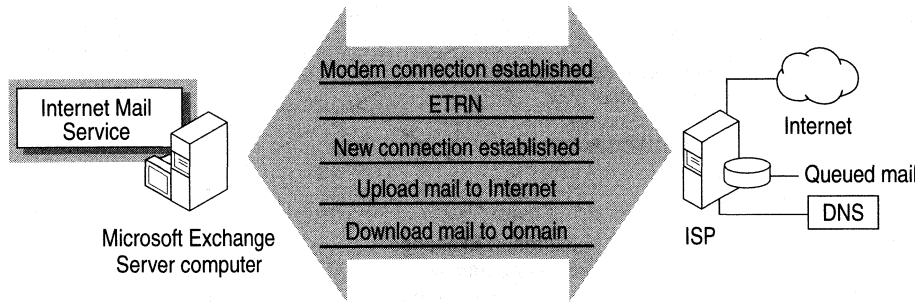


To create this type of connection, follow the steps in the previous section, "Types of Configurations," with one additional procedure. Use the Internet Mail Service **Connections** property page to specify the name of the smart host to which the Internet Mail Service will forward messages.

Note There may be other SMTP hosts within your organization. You need to determine whether your existing mail hub transfers Internet mail between these hosts directly, or through the Internet Mail Service.

Using a Dial-up Connection with ETRN

Dial-up connections can be used when you do not want to have a permanent connection but would like to connect to an Internet service provider (ISP) or remote site at specified intervals. When planning a dial-up connection, you need to determine the command you will use to retrieve mail from your ISP. Contact the provider to find out which commands are supported. The ETRN command is recommended because it is the easiest to configure. You can use the Internet Mail Service with ETRN and Remote Access Service (RAS) to connect to another site or to an Internet provider, as shown in the following illustration.



To create a dial-up connection with ETRN, follow the steps in "Types of Configurations" earlier in this chapter, with one additional procedure. Use the Internet Mail Service **Dial-up Connections** property page to specify connections, logon information, and a schedule. Note that support for ETRN is enabled by default.

For more general information about ETRN, see Chapter 4, "Connecting to Other Sites and Systems." For specific configuration procedures, see *Microsoft Exchange Server Operations.*

Setting Up Microsoft Exchange Server as an ETRN Server

Microsoft Exchange Server can be used as a host SMTP server, and will respond to ETRN commands from remote hosts. This functionality is useful for ISPs that are using Microsoft Exchange Server. Under RFC 1985, messages will be dequeued for all subdomains of a domain if it is preceded by an @ symbol. For example, if a host specifies the command ETRN@company.com, messages queued for all subdomains of company.com (such as sales.company.com and dept1.company.com) will be dequeued, in addition to messages queued for the top-level domain, company.com.

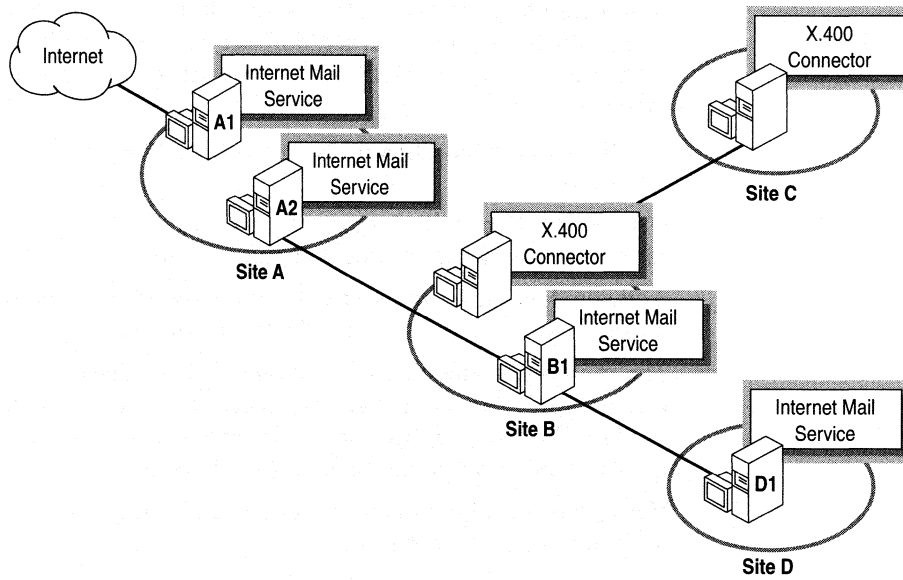
Client hosts with intermittent connections to a Microsoft Exchange Server computer must be assigned static IP addresses so that DNS resolutions will map to the correct host at the time of dequeueing.

To prevent unnecessary retries while the client host is not connected, consider setting the **retry interval** option so that it is higher than **message timeouts**. In addition, you may want to set the **Notify sender for queued mail** option for a longer period of time.

For more information about configuring these options, see *Microsoft Exchange Server Operations*.

Connecting Microsoft Exchange Server Sites over the Internet

The Internet Mail Service can also be used to connect Microsoft Exchange Server sites within the same organization, as shown in the following illustration. In addition, this illustration shows how one site can service external Internet mail traffic through a separate Internet Mail Service.



Note All Internet Mail Services between computers connect over the Internet.

To create this type of connection, use the following steps:

1. Install Windows NT Server TCP/IP on each computer running the Internet Mail Service. Configure the host and domain name in the TCP/IP configuration of each computer running the Internet Mail Service. Enable DNS if it will be used.

2. If you are using DNS, add an A record to specify the host name, domain name, and IP address of IMS A1 to the DNS serving the Internet Mail Service A1 computer.

   If you are not using DNS, use the local Hosts file to specify the host name and IP address of the hosts to which the Internet Mail Service A1 computer will forward mail.

3. Add the host name and domain name of the Internet Mail Service A1 computer to DNS or to the Hosts file of SMTP hosts that will forward mail to the Internet Mail Service.

4. To route inbound mail to other sites when using DNS, add an MX record for each site to associate the A record with the host name of the other sites. For example, in the illustration, an MX record is required to associate site A with site B and site D. Because of the MX record, mail destined for sites B and D will be sent to the site through site A.

   If you are not using DNS, make sure that the host and domain names of each computer running the Internet Mail Service are listed in the Hosts file, and that each site is entered in DNS or the Hosts file of all hosts that will be forwarding mail to the sites.

5. Use the **Connected Sites** property page in site A to add a new connected site for site B.

6. Use the **Routing Address** property page in site A to add the routing address for the Internet Mail Service computer on site B.

7. Add site A to the **Connected Sites** property page for the Internet Mail Service on site B, and use the routing address for site A.

8. The **maximum message size** option should be disabled if you are using the Internet Mail Service as a site connector. This ensures that system messages used for directory replication and information store updates are not prevented from passing through the Internet Mail Service.

9. Verify the site address and assign the administrator's mailbox for each Internet Mail Service in the organization.

10. Use Windows NT Server Control Panel Services to start the Internet Mail Service.

11. Test the connection to ensure that the Internet Mail Service is configured properly.

For best performance when connecting sites, configure the Internet Mail Service to use Multipurpose Internet Mail Extensions (MIME) encoding. When sending rich text formatting, the Internet Mail Service processes attachments differently when performing MIME encoding than it does with uuencode. Attachments are transmitted using rich text formatting instead of being broken out separately as they are in uuencoded messages. This results in much better performance when processing messages, due to the internal design of the Internet Mail Service. Therefore, to maximize site replication performance, use MIME encoding with rich text formatting when connecting sites through the Internet Mail Service.

For more information, see *Microsoft Exchange Server Operations.*

Installation Requirements

You must install TCP/IP network services on the Microsoft Exchange Server computer that will run the Internet Mail Service. If you expect a high level of message traffic, consider using a higher speed network connection.

For more information about setting up TCP/IP network software, see the Windows NT Server documentation.

Number of Connectors

Each Internet Mail Service can accept multiple incoming connections and initiate multiple outbound connections. If you expect heavy message traffic, consider using multiple Internet Mail Services in your site and organization. In addition, you can configure specific Internet Mail Services to:

- Only accept messages.
- Only send messages.
- Receive and send messages.
- Forward all mail to relay hosts for final delivery.
- Send mail to final destinations, using DNS.

If your site has a single Internet Mail Service, you will most likely configure it as both a server and a client, so it can send messages to and receive messages from connected SMTP hosts. If your site has more than one Internet Mail Service, you can configure one or more Internet Mail Services to handle only incoming messages and other Internet Mail Services to handle only outgoing messages.

More About SMTP Addresses and Using Multiple Connectors

You should also consider SMTP addresses when planning how many Internet Mail Services to set up, and where they should be placed. The default SMTP domain name used for Microsoft Exchange Server is based on the organization and site name. For example, Ferguson and Bardell's *FAB* organization name and *NAmerica-W* site name are used to generate the following default domain name:

namerica-w.fab.com

This domain name is appended to the user name to generate an SMTP e-mail address for messages sent through the Internet Mail Service in this site. For example, a user named *Fran Wilson* sending an SMTP message from this site has the following SMTP address:

franwilson@namerica-w.fab.com

You may want to install more than one Internet Mail Service in your organization to reflect the correct site locations, or you may want to use the same SMTP e-mail domain on all sites to avoid exposing your internal messaging topology.

For information about changing the site address, see *Microsoft Exchange Server Operations.*

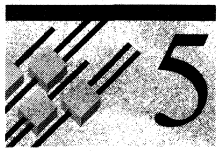
Controlling Access

You can control which SMTP hosts can send mail to the Internet Mail Service. This is a safeguard against unreasonable use of the Internet Mail Service. For example, if message transfer is impaired by excessive mail from a particular host, you can configure the Internet Mail Service to reject connection requests from that SMTP system.

Specifying Message Content Options

For outbound messages, you can choose whether attachments will be encoded by MIME or uuencode. You can also choose a character set and specify numerous interoperability settings. These settings can be specified separately for each e-mail domain.

Microsoft Mail Connector (PC)



You can connect Microsoft Exchange Server and one or more MS Mail (PC) systems by using the Microsoft Mail Connector (PC) over LAN, asynchronous, or X.25 connections. The Microsoft Mail Connector is a component of Microsoft Exchange Server that runs as a Windows NT Server service. Before using Microsoft Mail Connector (PC), consider the following issues:

- Types of configurations
- Directory synchronization
- Installation requirements

Types of Configurations

You can install one, a few, or many Microsoft Mail Connectors in a site. You may need only one to service an entire site, or you may want to install one on every server in your site. The number of connectors you install should be determined by your message volume. For example, you may want to centralize traffic between a Microsoft Exchange Server site and an MS Mail (PC) system on the same LAN. This would require a Microsoft Mail Connector in every site. This configuration uses Microsoft Exchange Server as a backbone for MS Mail (PC) postoffices in your organization.

If you connect the Microsoft Mail Connector to an MS Mail postoffice set up as a hub for message transfer, you can route mail to every MS Mail postoffice directly connected to that hub. With a LAN connection, you can upload routing information for these postoffices from the hub to the connector. The hub provides an indirect connection between the connector and all these postoffices.

Note You must apply the **MailerDisable** command on any existing External MTAs or Multitasking MTAs responsible for delivering mail to the Microsoft Exchange Shadow postoffice, including any other mail transfer executables such as File Format Application Programming Interface (FFAPI) gateways. For more information, see the *Microsoft Mail 3.2 Administrator's Guide.*

Directory Synchronization

Microsoft Exchange Server uses *directory synchronization* to share address information with foreign systems. Directory synchronization is the process of exchanging address information between your organization and any system that uses the MS Mail directory synchronization protocol. You can configure directory synchronization to:

- Synchronize Microsoft Exchange Server and MS Mail (PC) address information.
- Replace directory server postoffices in an existing MS Mail (PC) system.
- Exchange MS Mail template information. The templates record information about recipients, such as locations and phone numbers. You can map MS Mail templates and Microsoft Exchange Server recipient attributes to each other.

When planning directory synchronization between Microsoft Exchange Server and a mail system that uses the MS Mail (PC) directory synchronization protocol, consider the following:

- Because the directory synchronization process uses e-mail messages to update address information, Microsoft Exchange Server and MS Mail (PC) must be directly connected through the MS Mail Connector or a third-party gateway, or backboned through another connector. You must also make sure that routing is configured with redundant connections so that messages can still be routed if one connection fails.
- The Dispatch program transfers address list updates between MS Mail (PC) postoffices. If Dispatch is not running, MS Mail (PC) postoffices cannot compose update messages in the appropriate format.
- You can configure only one directory synchronization (dirsync) server for each site. Only one dirsync server can be configured for each MS Mail directory requestor postoffice.
- Schedule directory synchronization to minimize traffic on the network. To do so, schedule directory synchronization when traffic is at a minimum. Also make sure that there is enough available bandwidth to support directory synchronization traffic.
- When setting trust levels for directory synchronization, determine what directory information you want to exchange. Configure trust levels so that only this information is exchanged between the two systems.

- Microsoft Exchange Server enables two users to have the same display name provided that their directory name is different. MS Mail does not support this for users who are on the same postoffice.
- If you have multiple MS Mail directory server postoffices, you can replace them with a single Microsoft Exchange Server computer configured as the dirsync server for the MS Mail directory requestor postoffices that belonged to the MS Mail directory server postoffices. You can also replace existing MS Mail directory server postoffices with multiple Microsoft Exchange Server computers in different sites, if the sites are configured to replicate directory information.

Installation Requirements

Before using the Microsoft Mail Connector:

1. Verify that an asynchronous or X.25 connection between Microsoft Exchange Server and the appropriate MS Mail postoffice is properly configured.
2. Install and start all required Microsoft Exchange Server components.
3. Install the Microsoft Mail Connector by running Microsoft Exchange Server Setup and selecting the **Microsoft Mail Connector** option.

Microsoft Mail Connector (AppleTalk)

The Microsoft Mail Connector is a component of Microsoft Exchange Server that runs as a Windows NT Server service. With the Microsoft Mail Connector, users can exchange messages over a LAN from Microsoft Exchange Server to an MS Mail (AppleTalk) system. When you connect the MS Mail Connector (AppleTalk) with Microsoft Exchange Server, the connector recognizes the MS Mail (AppleTalk) address format (*mailbox@server*). For example, a Microsoft Outlook user can send a message to recipient John Chen on the San Francisco Marketing server by using this e-mail address: *John Chen@San Francisco Marketing*.

Before using Microsoft Mail Connector (AppleTalk), consider the following:

- Types of configurations
- Gateway limitations
- Installation requirements

Types of Configurations

Before you connect a Microsoft Exchange Server site to an MS Mail (AppleTalk) system, determine how many Microsoft Mail Connectors you need. In general, your decision should be determined by your network topology. For example, if you have multiple MS Mail (AppleTalk) servers geographically dispersed across multiple LANs, you may require one Microsoft Mail Connector on each LAN.

Also consider how many MS Mail (AppleTalk) servers will indirectly connect to a Microsoft Mail Connector through access components. The performance of the Microsoft Mail Connector and the Microsoft Exchange Connection depends on message traffic. For example, multiple MS Mail (AppleTalk) servers on the same LAN, with a single instance of the Microsoft Mail Connector servicing one MS Mail (AppleTalk) server and remaining MS Mail (AppleTalk) servers through access components may not be advisable. For a higher volume of message traffic, connecting a site to multiple MS Mail (AppleTalk) servers on the same LAN requires more than one Microsoft Mail Connector.

Gateway Limitations

In general, do not put more than 27,000 recipients in a recipient export container for an MS Mail (AppleTalk) requestor. Although the limit is 32,000, the gateway processes are slowed if more than 27,000 recipients are used. To circumvent this limitation, you can extract the access component from an MS Mail (AppleTalk) server and install it on another MS Mail (AppleTalk) server.

Installation Requirements

When the Microsoft Exchange Connection is installed on an MS Mail (AppleTalk) server, it is designated as the gateway server. This gateway server acts as a messaging hub for other MS Mail (AppleTalk) servers, called *gateway access servers*. This process is similar to the way in which Microsoft Mail Connection software is used to connect MS Mail (PC) and MS Mail (AppleTalk) systems.

Microsoft Mail Connector Requirements

For each Microsoft Exchange Server computer, there can be only one instance of the Microsoft Mail Connector. To use the Microsoft Mail Connector with MS Mail (AppleTalk), your Windows NT Server configuration must include:

- Windows NT Server Services for Macintosh, installed on your Microsoft Exchange Server computer.
- A Windows NT Server file system (NTFS) partition, required to support Windows NT Server Services for Macintosh. Microsoft Exchange Server must be installed on the NTFS partition.
- Sufficient hard disk space to store incoming and outgoing messages, until they are transferred to the MS Mail (AppleTalk) server.

You can configure a Microsoft Mail Connector on any Microsoft Exchange Server computer. However, you cannot configure multiple connections from a single site to a single MS Mail (AppleTalk) server.

Microsoft Exchange Connection Requirements

The Microsoft Exchange Connection is a gateway for the MS Mail (AppleTalk) server. This gateway works with the Microsoft Mail Connector (AppleTalk) MTA to transfer messages between the Microsoft Mail Connector postoffice and MS Mail (AppleTalk). MS Mail (AppleTalk) server requirements include:

- A Macintosh computer with an extra 2 MB of RAM, in addition to the basic RAM requirements for an MS Mail (AppleTalk) server.
- Sufficient hard disk space to store incoming and outgoing messages, until they are transferred to the Microsoft Mail Connector postoffice.
- MS Mail (AppleTalk), version 3.1*c* or later.
- System 7.1 or later.

Connecting Microsoft Exchange Server with Quarterdeck Mail Server

To connect Microsoft Exchange Server to Quarterdeck Mail Server computers in multiple sites, you should use multiple connections rather than backboning. If you keep Microsoft Exchange Server messages on a Microsoft Exchange Server computer and Quarterdeck Mail messages on a Quarterdeck Mail Server computer, you avoid problems with message conversion and the delays inherent in transferring messages between two native formats. It also makes it possible to have more than 32,000 Microsoft Exchange Server addresses on the Quarterdeck Mail Server system.

Note No additional configuration is required to make a single connection between Microsoft Exchange Server and a single Quarterdeck Mail Server computer.

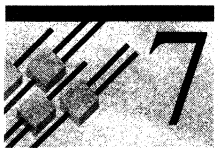
To configure multiple connections to Quarterdeck Mail Server computers, you must add an addressing dynamic-link library (DLL) to Microsoft Exchange Server that automatically generates Quarterdeck Mail proxy addresses for Microsoft Exchange Server users. The Quarterdeck Mail proxy enables Microsoft Exchange Server to convert addresses to the correct Microsoft Exchange Server format so that the replies will work. To automatically create the MSA address type, install Macproxy.dll before adding any users to Microsoft Exchange Server.

In addition, all Quarterdeck Mail Server sites must exchange address lists with each other. If the sites are not fully replicated, Quarterdeck Mail Server cannot resolve the name that the gateway submits, and Microsoft Exchange Server will send a non-delivery report (NDR).

In small, isolated sites, backboning over Microsoft Exchange Server may be the only way to deliver messages. Macproxy.dll may be required in this configuration if more than one Quarterdeck Mail Server computer has a connection to Microsoft Exchange Server.

For information about installing Macproxy.dll, see *Microsoft Exchange Server Operations*.

Microsoft Exchange Connector for Lotus cc:Mail



The Microsoft Exchange Connector for Lotus cc:Mail is used for message transfer and directory synchronization between Microsoft Exchange Server and Lotus cc:Mail systems. You can connect a cc:Mail network to a Microsoft Exchange Server organization using one connector or multiple connectors, depending upon your messaging requirements. Each Microsoft Exchange Server computer in your organization can run one instance of the connector that directly services one connection to a cc:Mail post office. You cannot service one cc:Mail post office from more than one connector.

Installation Requirements

The following software must be installed and running on the cc:Mail post office directly connected to the Connector for Lotus cc:Mail:

- Lotus cc:Mail Post Office Database version 6 and cc:Mail Import version 5.15 and Export version 5.14.
- Lotus cc:Mail Post Office Database version 8 and cc:Mail Import/Export version 6.0.

cc:Mail Address Generation

For cc:Mail users to address Microsoft Exchange users, the Microsoft Exchange Server users must have an address of type CCMAIL. Microsoft Exchange Server automatically generates a cc:Mail address for each recipient based on the site address.

When the connector is initially installed in a site, the cc:Mail e-mail address generator creates an address of type CCMAIL (*username* at *siteproxy*) for every recipient, public folder, distribution list, and custom recipient in the site. You configure the cc:Mail e-mail address format in the **Site Addressing** property page for the site.

Formatting of cc:Mail e-mail addresses is flexible. For example, the recipient Grover Smith in the site Ferguson will by default have the address *Smith, Grover at Ferguson* but can also have any of the following cc:Mail e-mail addresses:

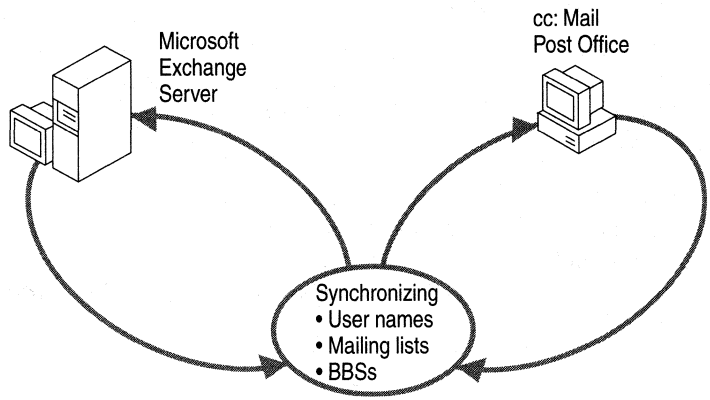
- Grovers at Ferguson
- Grover Smith at Ferguson
- Grover.Smith at Ferguson

Microsoft Exchange Server version 5.0 or later Setup installs the cc:Mail e-mail address generator for the site where the server resides. You must install one instance of Microsoft Exchange Server 5.0 or later in every site that communicates with cc:Mail.

Directory Synchronization for Lotus cc:Mail

If you use other messaging systems in addition to Microsoft Exchange Server, you must maintain at least two directories. The connector provides directory synchronization to maintain address information for both systems.

Any changes or updates to addresses in either system are synchronized at predetermined times that are set on the connector.



You can set up a schedule for directory updates or launch a directory synchronization cycle manually. After directory synchronization occurs, the address lists from both systems are adjusted to reflect any changes since the last directory synchronization cycle.

Import and Export Containers

When you configure directory synchronization, you must identify an *import container* and one or more *export containers.* The import container is used to store the imported cc:Mail addresses. Export containers hold the Microsoft Exchange Server recipients that you want to export to cc:Mail.

Trust Levels

You can control which specific Microsoft Exchange Server objects are exported to cc:Mail during directory synchronization by setting a *trust level* for each recipient object and export container. Only recipients with a trust level equal to or lower than the trust level specified in the **Export Containers** property page are exported to cc:Mail. Set the trust level for a recipient in the **Advanced** property page for the client object's properties.

One-off Addressing

One-off addresses are addresses used for messages to mailboxes that are not in your global address list or in your personal address book. They are called one-off because they are often used to send one piece of mail off to an address and are not used again. You can send a one-off message in either direction: from a Microsoft Outlook to a cc:Mail client, or from a cc:Mail client to a Microsoft Outlook.

A message sent from a Microsoft Outlook to a cc:Mail address will be delivered one of two ways. If the recipient is *responsible,* the connector will deliver the message to the custom recipient. A responsible cc:Mail recipient is represented as a custom recipient object in the global address list. Therefore, the connector is responsible for delivering the message to the custom recipient. A *nonresponsible* recipient address is not represented as a custom recipient and must be sent as a one-off address.

A one-off message sent from a Microsoft Outlook user to a cc:Mail user is addressed in the **To** box for a new message in Microsoft Outlook. It is not necessary for the cc:Mail user address to be present in a personal address book or the Microsoft Exchange Server global address list. For example, you can send a message to Grover Smith at post office Ferguson by typing the following in the **To** box.

[ccmail:smith,grover at ferguson]

A message sent from a cc:Mail client to a Microsoft Outlook user can be sent as a one-off if the Microsoft Exchange Server site is present in the cc:Mail address book. The intended recipient does not have to be listed in the cc:Mail address book. To send a one-off message from a cc:Mail client, select the site (represented as a post office), and type the user name. If you are using a comma in a user address (for example, "Smith, Grover,") you must prefix the one-off address with a comma (for example, ",Smith, Grover at Ferguson").

Using Multiple Connections to cc:Mail

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 Microsoft Exchange Server users.

From the cc:Mail perspective, each Microsoft Exchange Server site appears as one large cc:Mail post office, regardless of the number of servers or recipients in that site.

When planning multiple outgoing routes from one or more Connectors to cc:Mail, consider:

- Installing a connector on any or all Microsoft Exchange Server computers in your site, depending upon your messaging traffic.
- Using identical address information in the **Address Space** property pages of two or more Connectors to cc:Mail to route messages.
- Installing Microsoft Exchange Server 5.0 or later on at least one computer in every site that will indirectly communicate with cc:Mail. Microsoft Exchange Server 5.0 or later is required to generate cc:Mail addresses for Microsoft Exchange Server recipients.

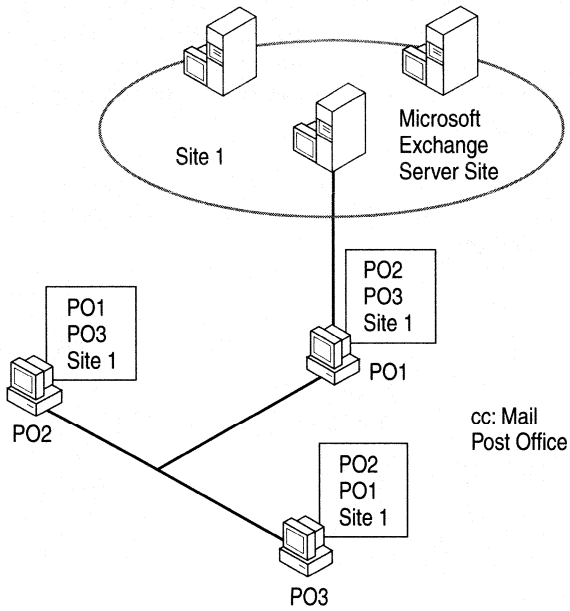
Connecting Microsoft Exchange Server and cc:Mail

There are multiple ways to connect Microsoft Exchange Server to cc:Mail. You can connect one or more Microsoft Exchange Server sites to one or more cc:Mail post offices.

Single Microsoft Exchange Server Site to Multiple cc:Mail Post Offices

The post offices in a cc:Mail system view a Microsoft Exchange Server site as a single cc:Mail post office. Microsoft Exchange Server computers in a site distribute directory information to one another using directory replication. Every cc:Mail post office must have an entry for a remote post office with the site address name. Directory synchronization creates remote post office entries for Microsoft Exchange Server sites in the cc:Mail directory. It is recommended that you run regular directory synchronization cycles. If you are not using directory synchronization, you must manually include Microsoft Exchange Server site names using the cc:Mail Administrator program. A cc:Mail user addresses all recipients in the site by *username* at *sitename*.

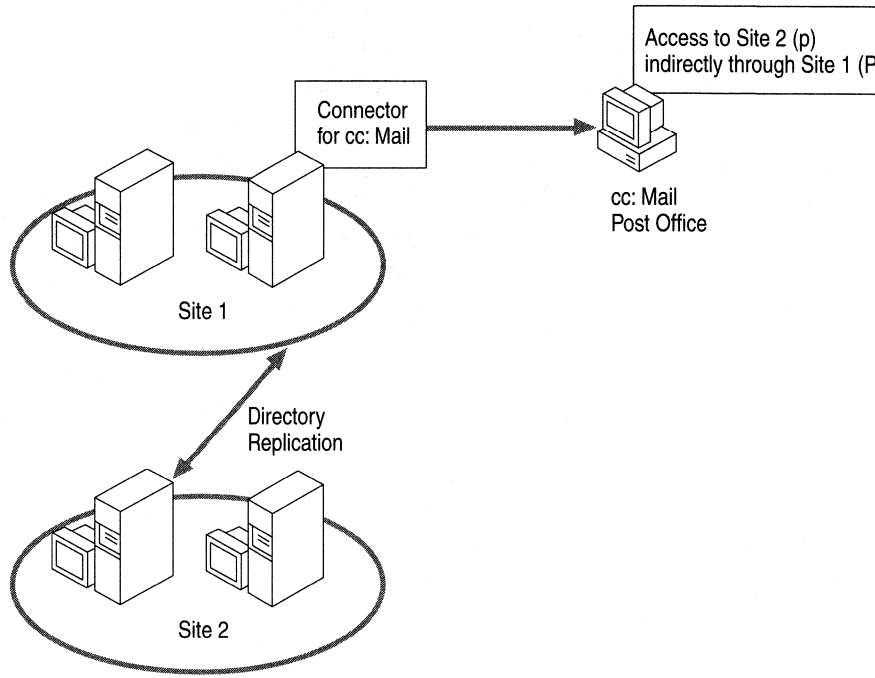
The following illustration shows how cc:Mail addressing can be configured to allow cc:Mail post offices direct and indirect access to a Microsoft Exchange Server site.



Multiple Microsoft Exchange Server Sites to a Single cc:Mail Post Office

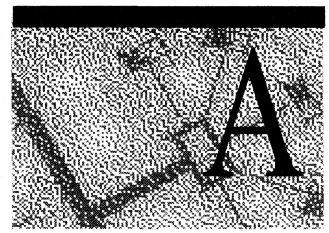
A single cc:Mail post office can access multiple Microsoft Exchange Server sites by configuring a cc:Mail post office address for each site. If you are not using directory synchronization, use the cc:Mail Administrator program to manually enter the Microsoft Exchange Server site names as if they were a cc:Mail post office. For example, suppose a cc:Mail post office accesses multiple Microsoft Exchange Server sites. Each site appears as a single cc:Mail post office to users on the cc:Mail system.

The following illustration shows how cc:Mail addressing can be configured to allow a single cc:Mail post office direct and indirect access to multiple Microsoft Exchange Server sites.



APPENDIX A

Optimizing Performance



How many users can be supported on a Microsoft Exchange Server computer? This is the most frequently asked question about performance—and the most difficult one to answer.

The number of users that a server can support isn't the same for every organization. Organizations use e-mail in different ways and have different hardware. The number of users per server also depends on what an organization considers to be acceptable response times and what tradeoffs can be made between server load and client response times.

This chapter provides background information about performance to help you implement Microsoft Exchange Server and describes the issues to consider when you're deciding how many users your server can support. It also describes how server hardware affects performance and how Microsoft Exchange Server optimizes performance. For more information about planning your servers, see Chapter 8, "Planning Your Servers." For more information about optimizing performance, see the *Microsoft Exchange Server Resource Guide, Supplement.*

Different Needs for Different Organizations

How many users per server? That depends on what type of hardware you have and how the users in your company will use Microsoft Exchange Server.

Users vary widely in how they use their messaging, scheduling, and workgroup computing resources. An organization's culture and location also affect how people use the messaging system. Users may send and receive hundreds of messages per week, or only one or two. Some users interact with the server 12 hours at a time; others connect only once a week for a few minutes. They may read hundreds of messages in dozens of public folders every day, or none at all. A small percentage of users in an organization may generate a high percentage of the total load on a server. For more information, see "Evaluating Usage" later in this chapter.

The server hardware may also vary widely. A company with large, centrally-located or well-connected sites may use a few expensive, high-end, multiprocessor servers with large amounts of RAM and dozens of disk drives to set up as many users per server as possible. Another company may use hundreds of inexpensive, lower-end servers to connect their many small, geographically diverse locations.

Many organizations have different-sized sites with different kinds of connectivity and therefore have different requirements for servers and the users they support. Most organizations want the most cost-effective hardware, but they need to consider other issues, such as maintenance and administration costs and floor space.

Factors That Affect Number of Users Per Server

There isn't an explicit limit to the number of users you can configure for a server; however, there may be practical limits. This can limit the number of users on large servers, depending on:

- The amount of server storage that each user needs.
- The values of user quota limitations, if used.
- The degree to which single-instance storage of messages and attachments increases the logical storage capacity of the server.
- The extent to which personal folder files (.pst files) are used.
- The number of rules, views, and other customized configurations defined by users on the server.

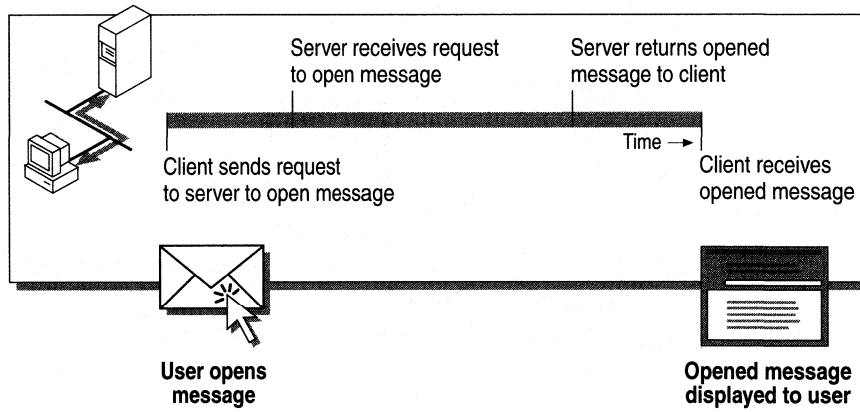
There may also be practical limitations dictated by the time it takes to back up a large server.

How a Server Responds to Different Loads

The main factor in determining the number of users that a server can support is the load each user places on the server. You can think of *load* in terms of user actions and background actions.

User Actions

A *user action* is an action, such as opening a mailbox, that the user performs on the client. The server performs actions in response to such a user action. From the user's point of view, these actions are synchronous. For example, opening an unread message in a mailbox on the server entails processing time for the server to receive and interpret the request and to evaluate any access restrictions. This happens in the time it takes for the remote procedure call (RPC) issued by the client application to return control to the client. The time the user perceives the operation to take is this time plus any additional processing time needed by the client application to draw the message window and perform other tasks.

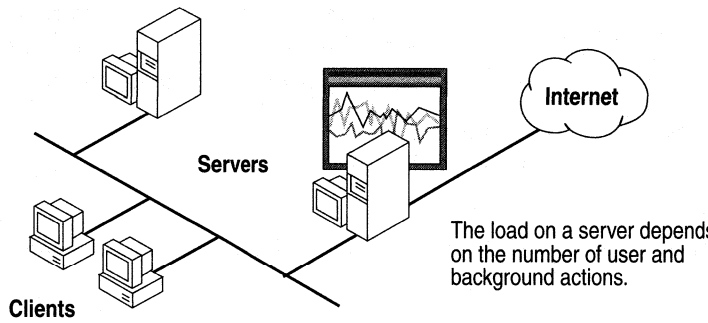


When users interact with the server directly, their actions place an immediate incremental load on the server. User actions are the most significant load factor on servers that directly support users (as opposed to backbone or connector servers). For any given server, the load created by user actions is proportional to the number of users actively interacting with the server and the actions they perform.

Background Actions

In addition to performing synchronous user actions, a server performs asynchronous, *background actions*: accepting, transferring, and delivering messages, making routing decisions, expanding distribution lists, replicating changes to public folders and directory service information, executing rules, and monitoring storage quotas. A server can perform these tasks asynchronously on behalf of users, whether they are connected or not. This work is referred to as *asynchronous* because the time it takes for these actions to be completed doesn't influence the users' perception of the system's speed, provided that the actions are completed within a reasonable amount of time.

In general, as with user actions, the load caused by background actions is proportional to the number of users on the server and the actions they perform. However, other factors, such as whether the server has connectors to other sites or systems, can have a significant impact. For dedicated connector or backbone servers, which don't directly support users, user actions place almost no load on the server. The load on the server is almost entirely the result of background actions.



Evaluating Usage

You can predict how actions will affect server load by considering aggregates over time. For example, you can evaluate all the user's actions (such as sending or reading messages and other activities) and all the background actions of the server on his or her behalf during a certain time period (such as an eight-hour workday). This can help you classify the user's activity level in comparison to others. Estimate how many actions a user performs over time, the load those actions place on the server, and then make rough performance predictions based on an "average" user.

To determine how many users a server can support, then, you need to determine the patterns of the users in your organization. For example, you can classify the users in your organization according to low, medium, and heavy usage, based on daily averages.

Type of usage	User Pattern
Low	Sends 3 messages.
	Reads new mail 5 times and old mail 12 times.
	Makes 1 change to his or her schedule.
Medium	Sends 6 messages.
	Reads new mail 15 times and old mail 12 times.
	Makes 5 changes to his or her schedule.
Heavy	Sends 8 messages.
	Reads new mail 20 times and old mail 12 times.
	Makes 10 changes to his or her schedule.

You can also use the Microsoft Exchange Server Load Simulator (Loadsim.exe) tool to help you determine the level of performance that's acceptable for your organization's users. Load Simulator can help you determine how many users your Microsoft Exchange Server computer can support. It is designed to provide a realistic load on a Microsoft Exchange Server computer by simulating the behavior or users on one or more Microsoft Outlook computers. For more information on running the Load Simulator tool, see the *Microsoft Exchange Server Resource Guide*.

How Load Affects Response Time

A server consists of hardware, including one or more CPUs with a particular architecture and processing speed, some amount of physical memory (RAM), one or more disk drives of certain speeds and sizes, and their controllers. This hardware, specifically the CPUs, RAM, and I/O subsystem, are the critical server hardware resources.

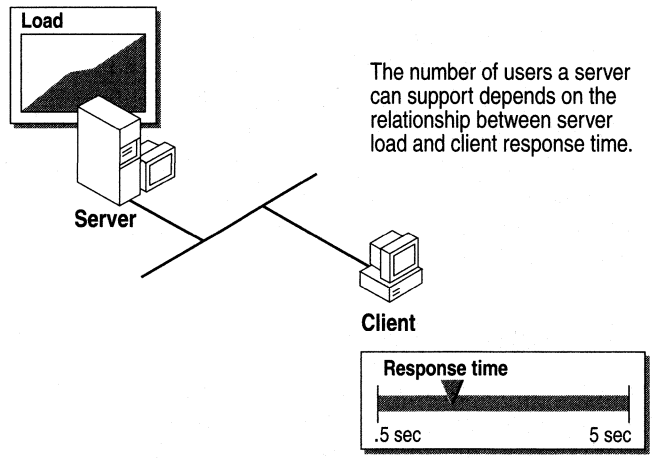
When a server responds to a user action or performs background actions, it uses each of these three resources to some degree. For example, responding to an open message request from a client may require several milliseconds of CPU processing time, one or more disk accesses, and enough memory to perform the operation.

When actions don't overlap in time, all the server hardware is dedicated to each action and the server is essentially idle between each action. Each action is completed as quickly as possible and doesn't need to wait for hardware resources to become available. In this case, the server is essentially *unloaded.*

When more users connect to the server or when many background actions are occurring, actions begin to overlap, and there is competition for the server hardware resources. Bottlenecks occur because the server must wait for hardware to become available so that it can complete its tasks. When this happens, a server is *under load.*

When a server is under load, actions may take longer to complete than if the server were unloaded. For user actions, this can result in increased response time for clients. If the server is under an excessive load, users may perceive the server as slow or unresponsive. This relationship between server load and client response time defines the number of users that a server can support.

Imagine a server with users who all perform the same actions, but their actions are evenly distributed over time. With only one user connected to the server, each user-initiated action is completed before the next one starts. The response times that a user experiences will be near the theoretical minimums possible for the client's hardware, server, and network.



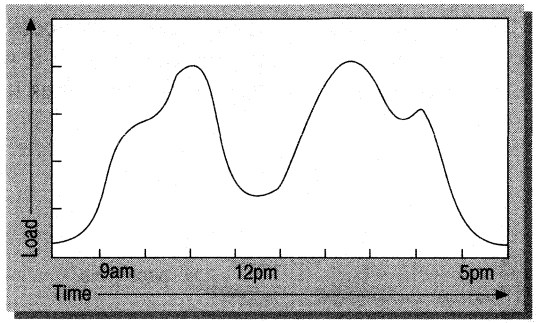
At some point, as the average load on a server increases the response times move from acceptable to unacceptable. This crossover point defines the number of theoretical "average" users that the server can support.

Uneven Loading

Actions that cause load are not evenly distributed over time. For example, a burst of activity in the early morning, when users arrive at work and catch up on mail, may place the greatest load on a server. On the other hand, there may be lulls in activity during lunch hours, evenings, and weekends. Also, load varies over time because of individual differences in usage level and schedule.

You should consider uneven loading when you plan your organization. You can reserve server capacity for bursts of activity by setting up fewer than the maximum number of average users on a server.

The following graph illustrates the e-mail usage patterns of a typical organization:



Resources That Affect Performance

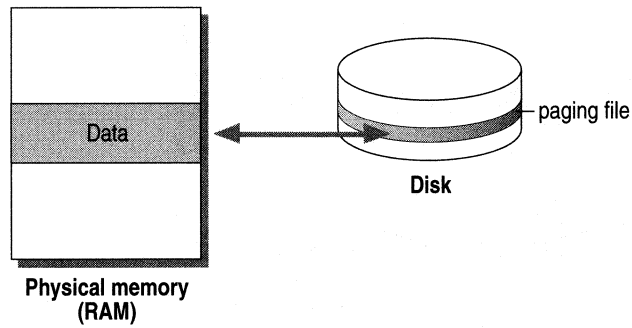
Performance is affected by the CPU, memory, the I/O subsystem, and the network hardware. If a server is under load and has poor response times, you need to examine these resources in your organization.

CPU

The type and number of CPUs dictate the performance potential of Microsoft Exchange Server. For example, computers based on the Pentium processor offer better performance than computers based on the 486 chip. Also, a 133 MHz Pentium performs better than a 100 MHz Pentium with a similar configuration. In general, computers with multiple CPUs offer better performance potential than computers with just one CPU; however, more processor power does not always result in increased performance. Upgrading a CPU or adding additional CPUs provides few benefits when other hardware resources, such as the I/O subsystem, are the sources of bottlenecks.

Memory

Windows NT Server uses virtual memory to swap data between physical and virtual memory as memory needs change. For example, if Microsoft Exchange Server needs more memory than is available, Window NT Server swaps data between the server's physical memory (RAM) and a temporary paging file on the server's disk. Typically, data that the server frequently accesses is stored in physical memory and is moved to the paging file when it is no longer needed. When the data is needed again, the operating system pages it back into physical memory.

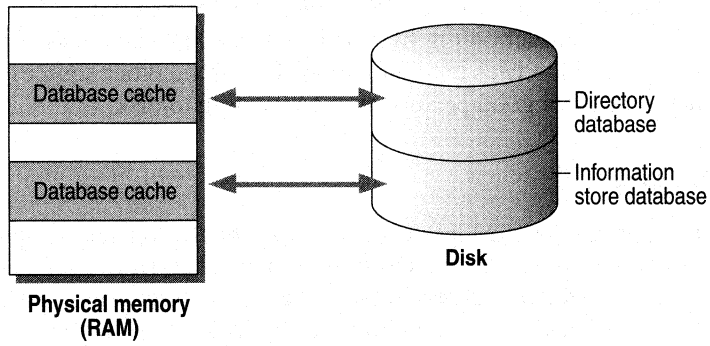


If the most frequently accessed pages can't all fit into physical memory, excessive paging can occur. *Paging* can be considered as contention for memory. Some contention is tolerable, but as it increases, the system spends too much effort passing pages between physical memory and the paging file. Excessive paging is called *thrashing,* which is a common cause of unacceptable performance.

Typically, as memory contention increases enough to cause thrashing, response times increase exponentially. One indication of thrashing is that the CPU is under-used, but the I/O subsystem is working excessively. You should try to prevent thrashing, especially during mission-critical activities, by adding more memory—not more disk space—to the server.

Data is moved between database caches in physical memory and databases stored on the server's disk. Data currently needed for a process is stored in a database cache; it is moved to the database on the server's disk when the data is no longer needed. This process is similar to paging. For example, when a client requests that a message be opened, the information store moves the appropriate data from its database on disk to its database cache. As with thrashing, adding more RAM improves performance, in this case because more of the database can be cached in memory.

You can adjust the size of the database caches. If they are too large, even a server with a lot of physical memory may thrash severely. On the other hand, setting the cache sizes too small for the load on the server may cause excessive I/O operations to the database, because not enough information is cached in physical memory for the amount of load on the server. You can use the Microsoft Exchange Server Performance Optimizer to adjust cache sizes if needed. For more information, see the "Using the Performance Optimizer" section later in this chapter.



I/O Subsystem

The I/O subsystem, including the type and number of disk controllers, the type of drives installed, and the choices required for disk fault tolerance and redundant array of inexpensive disks (RAID) configurations, affects overall system performance.

If a server has enough RAM to prevent thrashing, most I/O operations are used to provide server processes (such as the directory and the information store) with the data they need to complete tasks. If a server is low on memory, most I/O operations will be used up by paging.

Microsoft Exchange Server issues I/Os to the disk subsystem on the server to read data from disk into memory or to write data to permanent storage. For example, when a user opens his or her Inbox, the set of properties in the default folder view must be accessed for each of the first 20 or so messages in the user's inbox folder and returned to the user. If this information is not already cached in memory on the server from a recent previous access, it must be read from the server's information store database on disk before the action is completed.

Microsoft Exchange Server reads and writes to disk synchronously or asynchronously. Although all read I/Os and asynchronous write I/Os can be considered random, many synchronous writes to disk are sequential. For example, writing to the information store or directory databases is random, whereas writing changes to transaction log files on disk are sequential actions. Sequential disk access is much faster than random access because the I/O to the drive is completely sequential; the disk head typically does not need to physically move from one disk location to another to access logically contiguous pieces of data.

To take advantage of the sequential nature of transaction log files, put the database transaction log files on a dedicated physical disk drive. Hosting the transaction log files on their own disk, with no other sources of disk I/O on the drive, ensures good performance for writing to disk.

Network Hardware

For optimal network performance, you should consider adapter types and the type of network medium, such as twisted pair cable, fiber optic cable, and coaxial cable. The adapter characteristics that most affect performance are the bus type, bus width, and throughput rates. To optimize performance:

- Install one or more high-performance network adapters in the server.
- Use a minimum of necessary protocols.
- Segment the local area network (LAN), if appropriate.

An important performance issue is the quality of the network. For example, putting a server on a fiber distributed data interface (FDDI) ring with a capacity of 100 Mb/s provides better connectivity and performance than a server attached to a token ring network. An overloaded Ethernet segment, where many collisions occur, can also reduce performance. You should also consider wide area network (WAN) connectivity and quality, especially when trying to determine site boundaries or whether clients should access their server across the WAN.

Related Factors

Performance can be affected by other applications running on the server. Typically, a dedicated server running Microsoft Exchange Server and no other applications, or a server with few other applications running, has greater performance potential than a server servicing additional applications. For example, simultaneously providing services that aren't resource-intensive because they don't require the server to respond to client requests (such as the server acting as a domain controller, Windows Internet Naming Service [WINS] server, or Dynamic Host Configuration Protocol [DHCP] server), won't decrease performance. However, simultaneously running resource-intensive applications, such as Microsoft Systems Management (SMS) Server, SQL Server™, or SNA Server, may have a large effect on performance.

Using the Performance Optimizer

You can use the Performance Optimizer, a tool provided with Microsoft Exchange Server, to obtain the maximum performance from your system. The Setup program prompts you to choose whether to run Performance Optimizer following Setup. You should also rerun the Performance Optimizer:

- After changing the server hardware configuration.
- After changing the server's role in the site, such as adding or removing a connector.
- To help move files to other physical disks.
- To experiment with different parameter settings.

The Performance Optimizer analyzes the server's disk and memory configurations to determine the best location for the information store, directory, message transfer agent (MTA), and transaction log files. It also determines how much memory should be used for the information store and the directory, based on the total memory available on the server.

The Performance Optimizer performs the following optimization tasks:

1. Analyzes the hard disk configuration and determines which drives provide the fastest sequential access time and random access time. Reserves the drive with the fastest sequential access time for the transaction log file.

   Note The Performance Optimizer inspects logical drives, not physical disks. If a physical disk is divided into multiple partitions, it analyzes each partition and indicates that files should be moved to different partitions on the physical disk. Although there are no performance gains in this configuration, the Performance Optimizer makes this recommendation because it cannot detect whether the drives are physical or logical.

2. Chooses the fastest random access drive on which to place the files for the selected server type. For example, if the server is a public folder-only server, it places the public information store on the fastest random-access drive.
3. Detects the amount of physical memory in the server and calculates the size of the caches for the directory and the information store, based on the information you provide about how the server will be used.

   The default values for the directory and information store caches are appropriate for most installations. Although larger caches may provide better performance in some circumstances, performance depends on the amount of physical memory available.

Glossary

A

Address Book Displays recipient names (mailboxes, distribution lists, custom recipients, and public folders) in the directory. The Address Book can contain one or more address lists. See also global address list.

address list A collection of recipients (mailboxes, distribution lists, custom recipients, and public folders) in the Address Book, organized by their Recipients containers. *See also* global address list.

address space Address information that identifies a message and its route.

Administrator program A graphical user interface that enables administrators to manage and configure Microsoft Exchange Server objects, such as organizations, sites, and servers.

advanced security Provides administrators and users with the ability to protect and verify messages.

alias Typically a shortened version of the mailbox owner's name, used to address messages.

anonymous public folder A public folder that anonymous users can access.

anonymous user A nonvalidated user who is not recognized by Microsoft Exchange Server, and who can only access published folders and address lists.

authentication Validation of a user's Windows NT Server logon information. *See also* trust relationship.

B

backbone The network connection between local area network (LAN) segments.

bridgehead server A Microsoft Exchange Server computer that acts as the endpoint of a connection between two sites and is responsible for routing messages through that connection.

browser Software that interprets Hypertext Markup Language (HTML) files posted on the World Wide Web, formats them into Web pages, and displays them to the user.

C

certificate Information used for digital signatures and encryption that binds the user's public key to the mailbox.

client/server architecture The structural basis of Microsoft Exchange Server. The client sends requests to a server, and the server carries out the instructions.

connector A Microsoft Exchange Server component that routes messages between Microsoft Exchange Server sites and other messaging systems. For example, the Internet Mail Service enables Microsoft Outlook users to exchange messages with other users on the Internet.

container In the Microsoft Exchange Server Administrator program, an object that contains other objects. For example, the Recipients container is composed of recipient objects.

control message A command used by USENET host computers to create and remove newsgroups or cancel messages that have already been posted.

cross certification Enables organizations to establish trust with other organizations so that users can verify the digital signature of messages sent by users in other cross-certified organizations.

custom recipient A recipient in a foreign system whose address is in the Address Book.

D

delegate A person with permission to manage mail for another user, send mail for another user, or do both.

delivery receipt (DR) A notice confirming that a message was delivered to its intended recipient.

digital signature An advanced security feature that enables users to verify the source of messages and to verify that the contents have not been modified during transit.

directory Stores all information about an organization's resources and users, such as sites, recipients, and servers. Other components use the directory to address and route messages.

directory export The process of exporting user account information from the directory.

directory import The process of importing user account information into the directory.

directory hierarchy In the Administrator program, the hierarchical structure of objects in the directory.

directory object A record such as a server, mailbox, or distribution list in the directory. Every object has properties that can be defined.

directory replication The process of updating the directories of all servers within and between sites.

directory replication bridgehead server A Microsoft Exchange Server computer that acts as the endpoint of a directory replication connection between its site and a remote site, and requests directory updates from the remote site.

directory synchronization The process of synchronizing a Microsoft Exchange Server directory with directories from Microsoft Mail for PC networks and Microsoft Mail for AppleTalk Networks (also known as Quarterdeck Mail).

direct postoffice A postoffice connected through a local area network (LAN), an asychronous connection, or an X.25 connection.

distribution list A group of recipients addressed as a single recipient. Administrators can create distribution lists that are available in the Address Book. Users can create distribution lists and add them to their personal address books.

domain A group of servers running Windows NT Server. A domain can also include other types of servers and clients.

domain controller The Windows NT Server computer that maintains the security database for a domain and authenticates domain logons. Windows NT domains can have one primary domain controller (PDC) and one or more backup domain controllers (BDCs).

domain name system (DNS) A collection of distributed databases (domain name servers) that maintain the correlation between domain name addresses and numerical Internet protocol (IP) addresses.

Dynamic RAS Connector A Microsoft Exchange Server component that routes messages between sites on the same local area network (LAN) using the Windows NT Remote Access Service (RAS).

E

e-mail addresses The addresses by which recipients (mailboxes, distribution lists, custom recipients, and public folders) are known to foreign systems.

encryption An advanced security feature that provides confidentiality by allowing users to conceal data. Data is encrypted as it resides on disk and travels over a network.

F

fault tolerance The ability of a system to respond to an event such as a power failure so that information is not lost and operations continue without interruption.

firewall A combination of hardware and software that provides a security system, usually to prevent unauthorized access from the Internet to an internal network or intranet.

foreign system A messaging system other than Microsoft Exchange Server.

form A structure for posting and viewing information. An example is a Send form, such as a purchase requisition.

G

gateway Delivers messages from Microsoft Exchange Server to foreign systems.

global address list Contains mailboxes, custom recipients, distribution lists, and public folders in an organization.

H

home server The Microsoft Exchange Server computer that contains a user's mailbox.

Hypertext Markup Language (HTML) A system of marking up, or tagging, a document so that it can be published on the World Wide Web. Documents prepared in HTML contain reference graphics and formatting tags. You use a Web browser (such as Microsoft Internet Explorer) to view these documents.

Hypertext Transfer Protocol (HTTP) The set of conventions that World Wide Web servers use to send Hypertext Markup Language (HTML) pages over the Internet for display by a Web browser. This protocol enables a user to use a client program to enter a Uniform Resource Locator (URL) or to click a hyperlink to retrieve text, graphics, sound, and other digital information from a Web server.

I

inbound host The host computer that provides a newsfeed.

Internet Message Access Protocol, Version 4rev1 (IMAP4rev1) Enables clients to access and manipulate messages stored within their private and public folders on a Microsoft Exchange Server computer.

information service A tool that enables Microsoft Exchange Server and foreign systems to exchange mail.

information store A Microsoft Exchange Server core component that stores users' mailboxes and folders. *See also* public information store, private information store.

Internet The collection of networks and gateways that use Transport Control Protocol/Internet Protocol (TCP/IP) to handle data transfer and message conversion from the sending network to the receiving network.

Internet e-mail address Consists of a user name and a domain name, with the two separated by an at (@) sign, such as username@company.com.

Internet Mail Service A Microsoft Exchange Server component that enables users to exchange messages with Internet users. It can also be used to connect sites over any Simple Mail Transfer Protocol (SMTP) backbone.

Internet News Service Enables Microsoft Outlook users and users of third-party Network News Transfer Protocol (NNTP) applications to participate in USENET newsgroup discussions.

intranet A network within an organization that uses Internet technologies such as the Hypertext Transfer Protocol (HTTP) or File Transfer Protocol (FTP). Access to an intranet is available only to certain people, such as users within an organization.

K

key Digitally signs and encrypts data for security-enabled users.

Key Management server (KM server) A Microsoft Exchange Server computer installed with advanced security information.

L

Lightweight Directory Access Protocol (LDAP) Enables LDAP clients to access directory information from a Microsoft Exchange Server directory.

local delivery message A message sent between recipients that share the same home server.

M

mailbox The delivery location for incoming messages.

message transfer agent (MTA) A Microsoft Exchange Server core component that routes messages to other Microsoft Exchange Server MTAs, information stores, connectors, and third-party gateways.

Messaging Application Programming Interface (MAPI) A standard interface that Microsoft Exchange Server and Microsoft Outlook components use to communicate with one another.

messaging profile A group of settings that provide Microsoft Exchange Server with information about a client's configuration.

Microsoft Mail Connector A Microsoft Exchange Server component that provides connectivity to Microsoft Mail for PC Networks gateways and Microsoft Mail for AppleTalk Networks (also known as Quarterdeck Mail) gateways.

Microsoft Outlook Web Access Interact with the ActiveX™ Server function built into Microsoft Internet Information Server. These components create Hypertext Markup Language (HTML) for a Web-based e-mail client on a Microsoft Exchange Server computer.

Microsoft Schedule+ Free/Busy Connector Enables users to share free and busy information with one another.

multiple password policy Enables administrators to configure the Key Management (KM) server to require multiple passwords to perform certain tasks.

Multipurpose Internet Mail Extensions (MIME) A standard that enables binary data to be published and read on the Internet. The header of a file with binary data contains the MIME type of the data; this informs client programs (such as Web browsers and mail packages) that they connect process the data as straight text.

N

Network News Transfer Protocol (NNTP) An application protocol used in TCP/IP networks. Enables clients to read and post information to USENET newsgroups.

newsfeed The flow of items from one USENET site to another.

newsgroup An Internet discussion group that focuses on a particular category of interest.

non-delivery report (NDR) A notice that a message was not delivered to the recipient.

non-read notification (NRN) A notice that a message was deleted before it was read.

O

object A record, such as a site, server, connector, mailbox, or distribution list in the Microsoft Exchange Server directory.

offline address books Contain the recipient objects found in any Recipients container in the directory.

organization A collection of Microsoft Exchange Server computers grouped into sites.

outbound host The host computer that receives a newsfeed.

P

permission Authorization to access an object or perform an action.

Post Office Protocol version 3 (POP3) Enables users with POP3 clients to retrieve mail from their Microsoft Exchange Server Inbox.

private information store The part of the information store that maintains information in users' mailboxes.

profile *See* messaging profile, user profile.

protocol The part of an Internet address before the colon (such as http, ftp, and news) that specifies the access scheme for the address. Examples of protocols within an Internet address are: http://www.someones.homepage/default.html and news:alt.hypertext

public folder A folder stored in the public information store; includes information such as messages, spreadsheets, graphics, and voice mail.

public folder affinity Enables users in one site to open public folders on servers in other sites.

public folder replication The process of updating identical copies of a public folder on multiple Microsoft Exchange Server computers.

public information store The part of the information store that maintains information in public folders.

R

read receipt (RR) A notice that a message was read by its intended recipient.

recipient In the directory, an object that can receive messages and information. Recipients are mailboxes, distribution lists, custom recipients, and public folders.

remote procedure call (RPC) Standard protocol for client/server communication; a routine that transfers functions and data between client and server processes.

replication *See* directory replication, public folder replication.

revocation Warns users when they receive signed messages from users whose advanced security has been revoked.

role A group of permissions.

routing The process of transferring and delivering messages.

routing table Contains information that the MTA needs to route messages.

S

security context An aspect of Windows NT Server that controls the type of access a user, process, or service has to system services.

service account A Windows NT user account that is used to run Microsoft Exchange Server services.

signing An advanced security feature that verifies the sender's identity and verifies that the message hasn't been modified during transit.

Simple Mail Transfer Protocol (SMTP)
A protocol used by the Internet Mail Service to transfer messages between a Microsoft Exchange Server site and an SMTP messaging system, such as the Internet.

site One or more Microsoft Exchange Server computers (usually in the same geographical location) that share the same directory information.

Site Connector A Microsoft Exchange Server component that enables users in sites on the same local area network (LAN) to exchange messages.

system attendant A core maintenance service included with Microsoft Exchange Server.

T

target server A Microsoft Exchange Server computer that acts as the end point of a connection between two sites.

temporary key A random character string given to users to enable advanced security.

transaction log file A file that provides fault tolerance in the event that data needs to be restored to the information store or directory databases.

trust relationship The relationship between two domains that enables a user in one domain to access resources in another domain.

U

Uniform Resource Locator (URL)
An address of an object, document, or page or other destination. A URL expresses the protocol (such as Hypertext Transfer Protocol [HTTP]) to be accessed and where the destination is located. A URL may also specify an Internet e-mail address.

USENET The collection of host computers and networks that exchange news articles organized by subject.

USENET site One or more host computers that run the Network News Transfer Protocol (NNTP). A USENET site is different than a Microsoft Exchange Server site.

user account Contains information such as the user name, password, group membership, and permissions.

user profile A group of settings that provides the operating system with information about a client's configuration.

W

World Wide Web The World Wide Web is a system for exploring the Internet by using hyperlinks. When you use a Web browser, the Web appears as a collection of text, pictures, sounds, and digital movies.

X

X.400 Connector A Microsoft Exchange Server component integrated with the MTA that can be configured to connect sites within Microsoft Exchange Server, or to route messages to foreign X.400 systems.

X.400 Recommendations Defines the standard interfaces of an electronic messaging system. These recommendations specify the structure of a message handling system, message structure and components, and the method used to transfer messages.

X.400 transport stack Networking software required to support X.400 server-to-server message transport.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X