Microsoft® Exchange 2000 Server

Microsoft Exchange 2000 Server Design and Implementation for Woodgrove Bank

White Paper

Published: October 2001

Table of Contents

Microsoft Exchange 2000 Server Design and Implementation for Woodgrove Bank

White Paper

Published: October 2001

Introduction

The purpose of this document is to outline Microsoft® Exchange 2000 Server terms and concepts, show specific design details for the Woodgrove Bank Exchange environment, and describe best practices with regard to Exchange 2000 design principals.

This document outlines the following areas:

- Exchange terms and concepts that the reader must understand before continuing to other sections.
- The existing environment and coexistence information for Woodgrove Bank.
- Specific details about the Exchange 2000 design for Woodgrove Bank.

This document is not intended to be a complete design or implementation guide; it is intended to be a general guide based on best practices gathered through project experience. For this reason, this document does not provide a rigorous discussion of all the issues that factor into a Microsoft Windows® 2000 or an Exchange 2000 design and implementation. It is intended to familiarize the reader with only the basic architectural components of Windows 2000 and Exchange 2000 and the particulars of the design implemented at the fictitious Woodgrove Bank.

For more information about any of the subjects covered in this white paper, see the numerous white papers available at http://www.microsoft.com/exchange, and Microsoft Windows 2000 and Exchange 2000 online documentation.

Intended Audience

This document targets a broad audience. All the members of your information technology team, technology managers, and business decision makers are encouraged to read this document.

Project Vision

Woodgrove Bank has a vision to provide its user community with the best tools in a reliable, manageable, and secure environment. This provides Woodgrove Bank with a competitive advantage both internally and externally. Implementing Windows 2000 and Exchange 2000 fits into this vision by providing Woodgrove Bank

with the most powerful tools available today in an environment that can be centrally managed and controlled. By completing this project, Woodgrove Bank will have a world-class operating environment that addresses many of its current needs and allows future scalability as Woodgrove Bank progresses.

Project Overview

Woodgrove Bank is targeting the following four primary objectives for the overall Windows® 2000 and Exchange 2000 project.

Increase Manageability of the Server and Workstation Environment

Woodgrove Bank deals with efficiently managing their current environment. The existing Microsoft Windows NT® Server version 4.0 environment is divided into three different Windows NT 4.0 domains. Woodgrove Bank is not able to control the amount of administrative access that administrators have because of the level of granularity Windows NT provides for granting or denying administrative access. By upgrading to Windows 2000, Woodgrove Bank will also implement Microsoft Active Directory™ directory service. Active Directory will provide Woodgrove Bank with the granularity to provide its administrators with the necessary level of permissions. Windows 2000 will also provide many other management advantages over the existing environment such as Windows Management Instrumentation (WMI), Microsoft Management Console (MMC), Group Policies, Terminal Services, and disk quotas.

The existing Microsoft Exchange Server version 5.5 environment is deployed over 50 physical sites. While this was necessary for the existing network, the proposed network will allow Woodgrove Bank to centralize many, if not all, of its current servers running Exchange 5.5 to a few servers running Exchange 2000. This reduction of servers, combined with Exchange 2000 integration with Active Directory, will provide Woodgrove Bank with a messaging environment that is significantly easier to manage.

The current workstation operating system, Windows 95,does not provide Woodgrove Bank with the centralized level of control it requires to manage the workstation environment. Workstation computers upgraded to Windows 2000 Professional coupled with Windows 2000 Server Active Directory will give Woodgrove Bank the ability to centrally control the workstation environment through Group Policies, manage user data with Microsoft IntelliMirror®, and take advantage of the latest workstation deployment tools.

Increase the Security of the Woodgrove Bank Environment

Woodgrove Bank wants to take better control of the existing infrastructure by providing a higher level of security in all areas. The management features of Windows 2000 (Group Policies and Active Directory) combined with the default security enhancements to the Windows 2000 operating system (Kerberos authentication and the NTFS file system) and optional enhancements (Internet Protocol security [IPSec], Encrypting File System [EFS], and public key infrastructure [PKI]) will give Woodgrove Bank the flexibility to make their environment as secure as their business requirements dictate.

Increase the Reliability of the Environment

By putting Windows 2000 Professional on the workstations, Woodgrove Bank can expect a significantly more reliable operating system due to the inherent reliability improvements incorporated within Windows 2000. On its servers, Woodgrove Bank can take advantage of the high availability features of Windows 2000 and Exchange 2000, such as clustering, Network Load Balancing, and Distributed file system.

Provide User Community with Updated Technology

Running Windows 2000 Professional on the workstations will provide Woodgrove Bank users with the latest hardware compatibilities, such as universal serial bus (USB) and Advanced Configuration and Power Interface (ACPI) power management. Windows 2000 will also provide users with new features and capabilities, including support for multiple languages and improved laptop functionality such as the ability to hibernate and synchronize files and folders for offline use.

Running Windows 2000 will make many difficult tasks simpler, for example, locating and adding printers. Users at Woodgrove Bank will be able to search Active Directory for the closest printer that meets their requirements.

With Exchange 2000, users can take advantage of an updated Microsoft Outlook® Web Access client, full-text indexing, and optional features such as Instant Messaging and Microsoft Exchange 2000 Conferencing Server.

Technology Overview

The following section defines several terms and concepts used throughout this paper. It is important to understand these terms and concepts in order to understand the design principals and configuration details used in the Woodgrove Bank Exchange 2000 design.

Terms and Concepts

- **Active Directory** Active Directory is the directory service included with Windows 2000 Server. It stores information about objects on a network and makes this information available to users and network administrators. Active Directory gives network users access to permitted resources anywhere on the network using a single logon process. It provides network administrators with an intuitive, hierarchical view of the network and a single point of administration for all network objects.
- **Domain** In Windows 2000 and Active Directory, a domain is a collection of computers defined by the administrator of a Windows 2000 Server network that share a common directory database. A domain has a unique name and provides access to the centralized user accounts and group accounts maintained by the domain administrator. Each domain has its own security policies and security relationships with other domains and represents a single security boundary of a Windows 2000 computer network. Active Directory is made up of one or more domains, each of which can span more than one physical location. For the

Domain Name System (DNS), a domain is any tree or subtree within the DNS namespace.

> **Note** Although the names for DNS domains often correspond to Active Directory domains, DNS domains should not be confused with Windows 2000 and Active Directory networking domains.

- **Trees** Multiple domains joined hierarchically in a contiguous namespace form a tree.
- **Trust relationship** A trust relationship is a logical relationship established between domains that allows pass-through authentication in which a trusting domain honors the logon authentications of a trusted domain. User accounts and global groups defined in a trusted domain can be granted rights and permissions in a trusting domain—even though the user accounts or groups do not exist in the trusting domain's directory.

  In Windows NT Server version 4.0, domain A can access domain B, domain B can access domain A, domain C can access domain B, domain B can access domain C. However, domain A can not access domain C and domain C can not access domain A because transitive trusts did not exist in Windows NT 4.0. In Windows 2000, not only can domain A access domain B, domain B access domain A, domain C access domain B, domain B access domain C, but domain A can access domain C and domain C can access domain A (Figure 1).

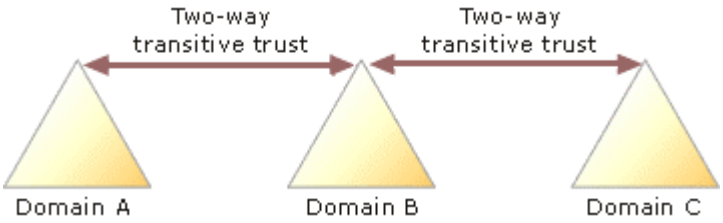

Figure 1 Example of Trust relationships

- **Forest** A forest is a collection of one or more Windows 2000 Active Directory trees, organized as peers and connected by two-way transitive trust relationships between the root domains of each tree. All trees in a forest share a common schema, configuration, and global catalog. When a forest contains multiple trees, the trees do not form a contiguous namespace.
- **Global catalog** A global catalog is a domain controller that contains a partial replica of every domain directory partition in the forest as well as a full replica of its own domain directory partition and the schema and configuration directory partitions. The global catalog holds a replica of every object in Active Directory, but each object includes a limited number of its attributes. The attributes in the global catalog are those most frequently used in search operations (such as a user's first and last names) and those attributes that are required to locate a full replica of the object. The global catalog enables users and applications to find objects in Active Directory given one or more attributes of the target object, without knowing what domain holds the object. The Active Directory replication system builds the global catalog automatically. The attributes replicated into the global catalog include a base set defined by Microsoft. Administrators can specify additional properties to meet the needs of their installation.
- **Exchange integration** Exchange 2000 leverages and is dependant on Active Directory. Active Directory provides a unified infrastructure for users, messaging,

and network resource administration. Directory information such as mailboxes, contacts (mail users outside the organization), and distribution groups are stored in Active Directory. This unified infrastructure enables administration of Exchange 2000 users to be done from the same tools as those used to manage Active Directory, thus saving on administrative costs.

To use Active Directory, Exchange extends the Active Directory schema and provides additional options for Exchange tasks, such as moving mailboxes, creating e-mail addresses and mailboxes, and mail-enabling user groups. Therefore, replication of user configuration information is done through the existing Active Directory infrastructure rather than as an additional load imposed by Exchange, as was the case with Exchange 5.5.

An Active Directory forest may contain only one Exchange 2000 organization. This level of interaction ensures that synchronization of directories is entirely based on Active Directory. Exchange 2000 stores its configuration information within the configuration container of Active Directory. This information replicates throughout the forest and is the primary reason why only one Exchange 2000 organization can exist in a Windows 2000 forest.

Any change made to a server running Exchange 2000 using Exchange System Manager is written to the configuration container in Active Directory. If a domain controller is unavailable or replication is complete, the server running Exchange 2000 will not have the updated information.

Exchange 2000 requires that a global catalog server be available in the same domain as the server running Exchange. Furthermore, Exchange 2000 automatically selects the most appropriate global catalogs for its use based on the Windows 2000 site. For this reason, at least one global catalog server must be in the same site as the servers running Exchange 2000.

- **Mixed mode and native mode** Exchange 2000 can operate in two modes: mixed and native. In mixed mode, Exchange 2000 can coexist in the same Exchange site as a server running Exchange 5.5. In native mode, coexistence is not possible.

  While in mixed mode, administrative groups map directly to sites in an Exchange 5.5 organization. Thus, Exchange 5.5 sites that replicate through Active Directory Connector (ADC) to Active Directory appear as administrative groups in Exchange 2000, and administrative groups appear in Exchange 5.5 as Exchange sites.

  Additionally, there is direct correlation between administrative and routing groups and Exchange 5.5 sites.

  When the first server running Exchange 2000 is installed, the default first routing group and administrative group are created. Each subsequent server installed must have an administrative group and routing group specified for it to join. Every server in the Exchange 2000 organization must belong to an administrative group and a routing group.

- **Exchange distributed architecture** Exchange 2000 operates under a distributed and extensible architecture, which enables services and mailboxes to be partitioned across multiple servers. As usage grows, adding additional servers

running Exchange 2000 to the organization to accommodate extra users is a simple task. In addition, Exchange 2000 can run on a cluster server, which enables two to four servers to provide performance and resilience.

Exchange 2000 Enterprise Server places no limitations on the amount of data that can be stored in a single message store. Exchange 2000 also uses single-instance storage to provide an efficient storage mechanism for mailbox data. For example, a 10-megabyte (MB) message delivered to multiple recipients located on the same mailbox store takes up only 10 MB of space, because only one instance of the message is deposited in the message store. Recipients of the message access the same message seamlessly.

In previous versions of Exchange, the time taken to perform backup and recovery of messaging stores significantly influenced the number of users that a single server running Exchange could support. Exchange 2000 addressed this issue by adding the capability for multiple messaging stores on each server and allowing message stores to be backed up simultaneously.

- **Front-end and back-end servers** An Exchange 2000 front-end server is a computer that redirects and proxies HTTP, Post Office Protocol version 3 (POP3), and Internet Message Access Protocol (IMAP) traffic to a server running Exchange 2000 that has an Exchange store (back-end server). Clients connect to the front-end server, which looks up the user's mailbox in Active Directory and then proxies the traffic to the corresponding back-end server. MAPI-based clients do not connect to front-end servers; they connect directly to their home back-end server.

  Using a front-end and back-end deployment has the following advantages:

  - **Single namespace** The primary advantage of a front-end and back-end server architecture is the ability to expose a single, consistent namespace. You can define a single namespace for users to access their mailboxes (for example, http://mail for Outlook Web Access). Without a front-end server, each user must know the name of the server that stores their mailbox. This complicates administration and compromises flexibility, because every time your organization grows or changes and you move some or all mailboxes to another server, you must inform the users. With a single namespace, users can use the same URL or POP3 and IMAP4 client configuration, even if servers are added or removed or if mailboxes are moved from one server to another server. In addition, creating a single namespace ensures that Outlook Web Access, POP3, or IMAP4 access remains scalable as your organization grows.

  - **Ability to offload processing** You can configure Exchange 2000 to support Secure Sockets Layer (SSL) traffic between the client and the server to protect the traffic from third-party interception. However, encrypting and decrypting message traffic uses processor resources. Therefore, when SSL encryption is in use, the front-end and back-end server architecture provides an additional advantage because the front-end servers can handle all encryption and decryption processing. This improves performance by removing processing tasks from back-end servers, while still allowing data to be encrypted between the client and the servers running Exchange 2000.

  - **Firewalls** You can position the front-end server as the single point of access on or behind an Internet firewall, which is configured to allow only

traffic to the front-end from the Internet. Because the front-end server has no user information on it, it provides an additional layer of security for the corporation. In addition, because you can configure the front-end server to authenticate requests before proxying them, the back-end servers are protected from denial-of-service attacks.

- **Increased IMAP4 access to public folders** IMAP4 allows a server to refer a client to another server. Exchange 2000 supports this functionality in cases where a public folder store on a particular server does not contain the content requested. However, this requires a client that supports IMAP referrals. Most existing clients do not support IMAP referrals. When a nonreferral-enabled IMAP4 client (see RFC 2221 and RFC 2193) connects through a front-end server, the client has access to the entire public folder hierarchy. When a front-end server proxies a command to a back-end server, it automatically handles any referral response that is passed back when attempting to access a folder that is not available on the back-end server. This makes the referral transparent to the client.

- **Outlook Web Access** Outlook Web Access in Exchange 2000 does not use MAPI to communicate with the Exchange store and no longer uses Active Server Pages (ASPs) for client access. Client access continues to use HTTP; however, Outlook Web Access is now built into the Exchange store and uses Internet Information Services (IIS) to receive requests and pass them to the Exchange store.

  IIS, which is integrated with Windows 2000, handles incoming HTTP requests from Web browsers and sends HTTP responses from Exchange 2000 or Outlook Web Access. IIS receives a client request, looks at the namespace, and passes the appropriate information for the context of the URL back to the Web browser. If the server houses the Exchange 2000 mailbox store, Outlook Web Access uses a high-speed channel to access the mailbox store. If the server is a front-end server, Outlook Web Access uses HTTP to direct the request to a back-end server.

  SSL provides the best level of security because the entire communications session is encrypted. SSL is not an authentication mechanism itself. Rather, SSL provides a secure channel for any authentication mechanism. Although it is possible to use any authentication mechanism with SSL, the most common implementation is Basic with SSL.

- **Administrative groups and routing groups** Exchange 2000 uses administrative and routing groups to independently manage administration and message transfer operations, respectively.

  At a high level, administrative groups give you the ability to group servers running Exchange 2000 together for the purposes of administrative control. Administrators can delegate different levels of permissions throughout the administrative group. Administrative groups are used to separate management of system policies, routing groups, public folder hierarchies, servers, virtual server resources, chat communities, and other administrative elements.

  These permissions vary between administrative groups. Using just one administrative group for all servers enforces centralized administration. Multiple administrative groups allow for different policy settings to be applied to different servers or offices if required.

Administrative groups are essentially used to define the management topology of the organization and help to simplify system management.

Routing groups provide a mechanism for managing message traffic within an organization. Messages sent between servers in the same routing group are sent using Simple Message Transfer Protocol (SMTP).

Messages sent between servers in different routing groups travel across the network based on the defined routing group topology over a defined protocol (such as SMTP or X.400). Routing groups enable efficient use of network (LAN and WAN) resources.

Note Routing groups are independent from Active Directory sites and do not follow the same rules.

- **Connectors** Communication between servers in different routing groups is established with connectors. If you define bridgehead servers, all message traffic that leaves a routing group leaves through one of the bridgehead servers. Similarly, all message traffic coming into that routing group enters through a bridgehead server.

- **Routing group connector** SMTP is the native transport for the routing group connector and obtains its routing and next hop information from a link state table. A routing group connector is unidirectional; therefore, you must create two routing group connectors to properly link two routing groups.

  When you use a routing group connector to connect a server running Exchange 2000 with a server running Exchange 5.5, the server running Exchange 2000 automatically uses remote procedure call (RPC) communication, because it cannot detect whether the server running Exchange 5.5 has Internet Mail Service.

- **SMTP connector** The SMTP connector uses SMTP to transfer messages between routing groups. You can use the SMTP connector to fine-tune your routing configuration to a greater extent than you can with a routing group connector. Options for SMTP connectors include issuing authentication before sending mail, specifying Transport Layer Security (TLS) encryption, and issuing a command to remove mail from the queue on the remote server.

- **X.400 connector** X.400 connectors are used to establish an X.400 messaging route between two Exchange routing groups. When you use an X.400 connector to connect two routing groups, the bridgehead server in each routing group is configured to provide the connection. Multiple X.400 connectors are configured to use a different transport type.

- **Link state tables** In Exchange 2000, each server maintains a link state table to determine the best route for a message. The link state table replaces the Gateway Address Resolution Table (GWART) in Exchange 5.5. Because each server has complete information about the routing status from the source to the destination, it generates a loop-free route for the message. Additionally, if no route is available (because of a link failure), the message remains on the source server in a queue until the link is available.

  To maintain the link state tables across the entire messaging system, Exchange assigns one routing group master for each routing group. If the master fails, you can manually set a different server as the master.

Servers receive updated link state information in two ways:

- Within a routing group, the master updates the other servers over TCP port 691. When the master receives an update from another server, it immediately sends that update to each server in its routing group.
- Within and between routing groups, each server compares link state information with other servers when transferring messages with SMTP. Exchange 2000 extends SMTP to include an additional SMTP verb to compare and update link state information. Similarly, Exchange 2000 extends the X.400 protocol so that X.400 connectors used as routing group connectors can update this information; thus, as messages flow, the link states are automatically updated. Even if no messages travel over a connector between two routing groups, a periodic poll updates the link state.

- **Storage groups, mailbox stores, and public folder stores** A storage group is a collection of mailbox and public folder stores (databases) on a server running Exchange 2000 that share the same Extensible Storage Engine (ESE) instance and transaction log. Individual databases within a storage group can be mounted and dismounted. Each server running Exchange can support up to 20 databases (four storage groups, each storage group holds up to five databases) for holding user mailboxes or shared public folders.

  Administrators can back up and restore multiple mailbox and public folder stores independently and concurrently. Servers can hold many user mailboxes while still providing viable backup and recovery procedures. Depending on the size of the organization, all users within a single office could be housed in their own database, and, as a result, multiple offices could have their data stored on one server running Exchange.

  The following list outlines some of the factors related to storage group design:

  - **Backup and restore** Mailbox and public folder stores can be backed up and restored independently of each other whether they are part of a cluster or not. This ability to independantly back up and restore databases is likely to have the greatest impact on the number of storage groups and databases you decide to use because of the potentially large amount of data that will need to be backed up and restored. For example, a server holding 2,000 mailboxes, each with a limit of 100 megabytes (MB), requires a mailbox store of up to 200 gigabytes (GB). It is then necessary to have backup and restore procedures and hardware in place that can perform the backup within the time available (normally 3 to 4 hours at night, allowing for nightly online maintenance) and restore within the service level agreement (normally 1 to 2 hours).
  - **Hardware** The choice of disk subsystem and backup tape devices will affect the size of your mailbox and public folder stores, and therefore the number of users stored on each server. A slow disk subsystem is likely to be a bottleneck for Exchange because use of the mailbox and public folder stores is disk process intensive. It is a practical requirement that for each storage group, the transaction logs and the databases be on separate spindles.
  - **Single instance storage** Single instance storage means that a 10-MB message sent to 100 users on the same server results in only 10 MB of storage in the mailbox or public folder store. Single instance storage applies

only to each database; therefore, the fewer mailbox and public folder stores that you implement, the more efficient data storage will be.

- **Number of users** Multiple storage groups and mailbox and public folder stores provide a mechanism for distributing user data across multiple physical disks. This ability to distribute can improve performance and scalability of Exchange systems and also enable different policies to be applied to users. For example, standard users may have a default maximum mailbox size of 100 MB and recovery of failed mail is required within 3 hours, but managers require more than 100 MB and recovery within 30 minutes. In this situation it would be appropriate to have two mailbox stores: standard users on one mailbox store and managers on another.
- **Number of servers in each cluster (if configured)** Each node of an Exchange 2000 cluster will support at least one storage group. You can configure a maximum of four storage groups with five databases per storage group. A cluster server can accommodate a number of Exchange virtual servers, each having allocated hard disks. If a node fails, an Exchange virtual server will fail over to one of the other nodes.
- **User limits** To assist in managing storage on servers running Exchange 2000, configure mailbox limits on all user mailboxes.

- **Clustered servers** An organization may choose to implement Exchange 2000 in a clustered environment. If so, the servers running Exchange 2000 must run Windows 2000 Advanced Server or Windows 2000 Datacenter Server.

  Clustering provides redundancy by grouping together independent servers to provide messaging services. Servers running Exchange 2000 in a cluster operate as multiple Exchange virtual servers with each individual Exchange virtual server supporting and managing one or more mailbox and public folder stores.

  If a hardware failure occurs (memory, CPU, or power supply) on one of the nodes, the other nodes in the cluster will take over the operational load of the failed server.

  Mailbox and public folder stores reside on disks that are shared between nodes and connected through a SCSI or fiber-bus. The maximum number of storage groups and that should run on a clustered node is four, and the maximum number of mailbox and public folder stores within a storage group is five.

- **Public folders** Public folders provide a shared repository for information in Exchange. Typically public folders are used to store collaborative information and provide an area for discussion forums. Public folders can contain mail items, contact databases, and shared calendars and can be customized to provide custom message forms and routable messages.

- **Universal distribution groups** Universal distribution groups are similar to Exchange 5.5 distribution lists. Because Windows 2000 groups can be mail-enabled, a universal mail-enabled group can be used just like an Exchange 5.5 distribution list. ADC by default converts Exchange 5.5 distribution lists into universal distribtuition groups.

- **Universal security groups** Unlike universal distribution groups, you can use universal security groups to grant permissions in any domain in the forest. Universal security groups, like universal distribution groups, are particularly

useful for Exchange 2000 because they can contain members from any domain. To set permissions on public folders in Exchange 2000, you must use a group type that allows you to view and modify group membership on local or global domains. The Exchange store automatically converts universal distribution groups into universal security groups as needed.

- **Collaboration** Exchange 2000 provides individual and shared messaging, calendaring, contact management, and collaboration through shared public folders as mentioned above.

  In addition, Exchange 2000 offers Instant Messaging and presence information, chat, and conferencing services (installed separately as Microsoft Exchange 2000 Conferencing Server) for real-time collaboration.

- **Policies** Policies are used in an Exchange 2000 organization to ensure consistent configuration across all servers, mailbox stores, and public folder stores. You can use policies to configure items such as message tracking, mailbox limits, and deleted item retention. Policies reduce administrative burden because a single change can be propagated to all servers running Exchange 2000 rather than administrators having to configure each server.

- **Full-text indexing** Full-text indexing allows users to quickly locate messages and documents stored within mailbox and public folder stores that have certain words in the message body, message subject, or within an attached document. Users can search other message properties and attributes by using standard search techniques.

  The use of full-text indexing translates into less time searching for information and higher user productivity. However, full-text indexing puts some extra load on the CPU and 25 to 30 percent additional disk space is required.

- **Extensibility** Extensibility refers to the ability to expand the Active Directory schema with additional object classes and attributes. Exchange 2000 is extensible to developers through well documented Internet standard interfaces.

Best Practices

The following are recommended best practices.

- Group users who send messages to each other often in the same mailbox store to improve storage and operation efficiency. It is strongly recommended that you follow this strategy in any organization.
- Avoid loading each server to the maximum number of 20 mailbox and public folder stores.
- Use an Exchange-aware commercial backup application for point-of-failure recovery; otherwise, offline backups, which restore only data to the previous backup, will be required.
- Procure the appropriate technology to ensure that backups of mailbox and public folder stores can be performed within an acceptable time period. Backup operations should not impact business operations.
- Allow enough time for Exchange to perform the tasks associated with online maintenance (an internal, automated Exchange Server process that includes

online defragmentation). By default, online maintenance tasks are scheduled to occur between 1 A.M. and 7 A.M.

- For large storage space requirements, separate server operations onto separate disks (for example, different disks for transaction logs and mailbox stores).

Current Environment and Coexistence Strategy

The following sections describe the existing Exchange 5.5 environment information and the proposed ADC configuration.

Current Messaging Architecture

A thorough understanding of the current environment is critical to a successful design. The following section is a brief overview of Woodgrove Bank's current messaging environment. The information in this section was gathered by interviewing support staff at Woodgrove Bank with little physical research performed and will be leveraged during the Exchange 2000 design process.

Site Structure

The current messaging architecture is composed of roughly 60 Exchange 5.5 sites, which all share the same Exchange organization name (Figure 2). Site names usually match city names or regions where the servers running Exchange 5.5 reside. Most sites have only one server running Exchange, with the exception of Chicago, London, WoodgroveBankOnline, Americas, and Europe.

There are two hub sites (Americas and Europe) within the environment that are directly connected in a peer configuration. Each hub site is then configured in a hub-and-spoke topology with other sites in their respective geography. All sites use Site Connectors and Directory Replication Connectors to connect to their corresponding hub site.

The Americas site connects to all cites and regions within North America, South America, and Asia. Likewise, the Europe site connects to cities in that area of the world. The only exception to this rule is the Africa site, which connects to the Americas site.

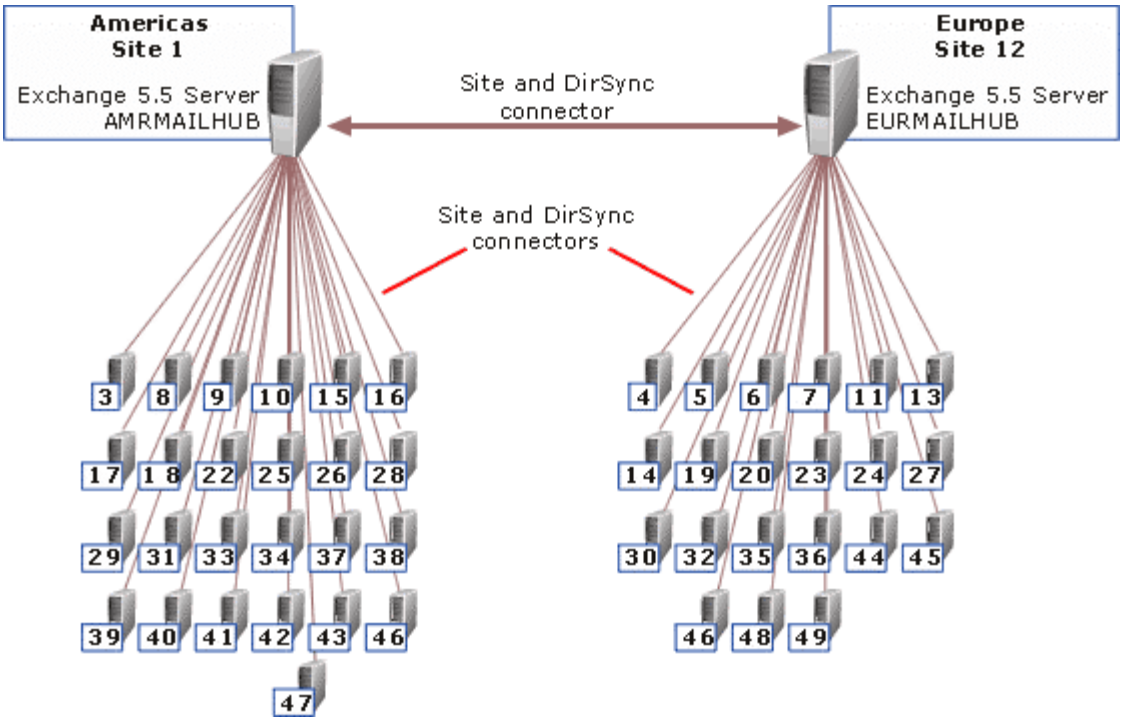

Figure 2 Woodgrove Bank Exchange 5.5 site configuration

Exchange Servers

All servers running Exchange in the environment run Exchange 5.5 Service Pack 3 (SP3) with hot fixes. Table 1 outlines Exchange site names and their associated servers.

Table 1 Exchange 5.5 site names and associated servers

Site Number	Site Name	Server
1	Americas	AMRMAILHUB
2	Amsterdam	AMSNTAPP
3	Atlanta	ATLNTAPP
4	Barcelona	BARNTAPP
5	Bogota	BOGNTAPP
6	Brussels	BRUNTAPP
7	Budapest	BUDNTAPP
8	Buenos Aires	BUENTAPP
9	Chicago	CFOEXCHANGE
		CHINTAPP
10	Dallas	DALNTAPP
11	Düsseldorf	DUSNTAPP
12	Europe	EURMAILHUB
13	Frankfurt	FRANTAPP
14	Geneva	GENNTAPP
15	Hong Kong	HONNTAPP
16	Houston	HOUNTAPP

Site Number	Site Name	Server
17	Johannesburg	JOHNTAPP
18	Los Angeles	LAXNTAPP
19	Leeds	LEENTAPP
20	London	LONMAIL
		LONMAIL-A
21	Madrid	MADNTAPP
22	Manchester	MANNTAPP
23	San Mateo	MATNTAPP
24	Melbourne	MELNTAPP
25	Mexico City	MEXNTAPP
26	Miami	MIANTAPP
27	Milan	MILNTAPP
28	Minneapolis	MINNTAPP
29	Montreal	MONNTAPP
30	Munich	MUNNTAPP
31	New York	NYKNTAPP
32	Paris	PARNTAPP
33	Philadelphia	PHINTAPP
34	Pleasanton	PLSNTAPP
35	Prague	PRANTAPP
36	Rome	ROMNTAPP
37	Santiago	SANNTAPP
38	Sao Paolo	SAONTAPP
39	Santa Fe	SFENTAPP
40	San Francisco	SFRNTAPP
41	Singapore	SNGNTAPP
42	WoodgroveBankOnline	WBONTAPP
		WBNTEXC
43	Stamford	STANTAPP
44	Stuttgart	STUNTAPP
45	Sydney	SYDNTAPP
46	Tokyo	TOKNTAPP
47	Toronto	TORNTAPP
48	Vienna	VIENNTAPP
49	Zurich	ZURNTAPP

Connectors and Gateways

Several types of connectors are used within Woodgrove Bank's Exchange environment. However, the configuration and distribution of these connectors and gateways is quite simple. All connectors and gateways are configured on one of two servers (AMRMAILHUB and EURMAILHUB).

Each of these servers has an Internet Mail Connector configured to connect to the Internet through an SMTP host located on IP address 192.168.0.10 (Figure 3). Each Internet Mail Connector is configured to route mail outbound through the SMTP host, which also scans for viruses. If a virus is found, the message is halted and not

delivered to the destination. Only the AMRMAILHUB server is configured to receive mail from the Internet, which is relayed through port 25 on the SMTP host. The SMTP host also scans for viruses inbound. If a virus is found, the message is deleted. All mail is then delivered to the destination recipient through RPC to the destination server.

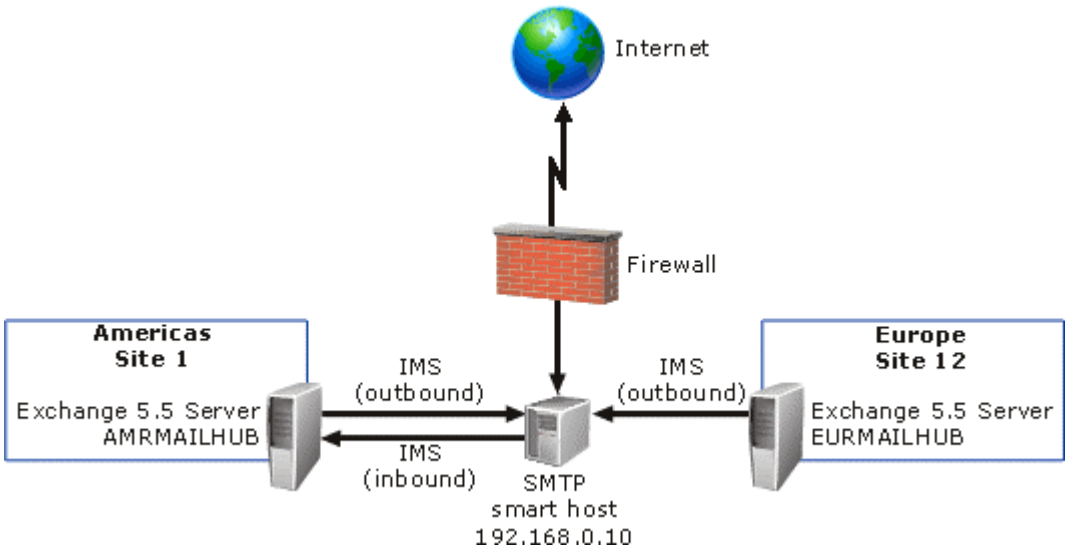

Figure 3 Existing configuration of Internet Mail Connectors

Public Folders

Public folders are not used heavily at Woodgrove Bank with the exception of the Marketing folder. According to the Woodgrove Bank staff most or all public folders should reside on AMRMAILHUB with some replicas on servers in the Europe site. Overall there are six top-level folders and very few sub folders. In addition, the default permissions on all public folders are set to "read." Some users have special permissions that allow them to add or modify content. Overall, the public folder structure is simple and will be easy to integrate with Exchange 2000.

Additional Servers

An Outlook Web Access server is configured to support a limited amount of users. The existing Outlook Web Access server is not capable of supporting any Exchange 2000 users and should remain functional until the migration is complete.

Active Directory Connector

It is recommended that you use ADC, which is included on the Exchange 2000 compact disc, to synchronize all users from the existing Exchange 5.5 organization to Active Directory. ADC also synchronizes users from Active Directory back to the Exchange 5.5 environment. Connection agreements act as the control mechanism for replicating directory and configuration information between an Exchange 5.5 environment and Active Directory.

Three types of connection agreements should be used within Woodgrove Bank's environment to replicate users between Exchange 5.5 and Active Directory.

Configuration Connection Agreements

A configuration connection agreement replicates Exchange-specific configuration information between the Exchange 5.5 directory and Active Directory. Configuration connection agreements allow Exchange 2000 to coexist with previous versions of Exchange. You can view configuration connection agreements in Microsoft Management Console (MMC) for the ADC server that hosts the configuration connection agreement or by viewing the bridgehead servers at each end of the connection agreement. Configuration connection agreements are automatically created by Setup when you install a server running Exchange 2000 in an existing Exchange 5.5 organization. Woodgrove Bank will have two configuration connection agreements.

Recipient Connection Agreements

Recipient connection agreements replicate Exchange 5.5 recipient objects to Active Directory. They also replicate information from Active Directory back to the Exchange 5.5 environment. ADC displays recipient connection agreements showing the names of the connection agreements. Recipient connection agreements can be defined as a one-way or a two-way connection and can be directed to any variation of containers in both the Exchange 5.5 environment and Active Directory.

The following are recipient objects synchronized by ADC:

- **Mailboxes** Use a recipient connection agreement to bring Exchange 5.5 mailbox information into Active Directory by creating a mail-enabled, disabled user. If you have already used Active Directory Migration Tool to create an enabled user account, ADC modifies that existing account to make it mail-enabled.
- **Custom recipients** Use a recipient connection agreement to bring over all of the custom recipients from Exchange 5.5 to Active Directory as mail-enabled contacts.
- **Distribution lists** Use a recipient connection agreement to replicate distribution lists from Exchange 5.5 to Active Directory as distribution or security groups (the Windows 2000 version of a distribution list).

  Note The Windows 2000 domain must be in native mode for distribution lists to come across as universal security groups.

Public Folder Connection Agreements

Public folder connection agreements are responsible for replicating public folder proxy objects between the Exchange 5.5 directory and Active Directory. These objects are necessary for sending e-mail directly to the folder. Each public folder connection agreement is two-way and replicates between the site-naming context in Exchange 5.5 and the Exchange system objects container in the Active Directory domain. ADC displays public folder connection agreements showing the names of the connection agreements.

Public folder connection agreements function in the following ways:

- Public folder connection agreements always use two-way replication.

- Public folders are the only objects you can replicate in a public folder connection agreement. To replicate other objects, you must create a different type of connection agreement.
- For public folder connection agreements, ADC automatically selects the Windows organizational unit, the Exchange container, and the default destination containers for Windows and Exchange. You cannot change these containers.
- Public folder connection agreements are always primary connection agreements from Exchange and this cannot be changed. This is beneficial because a primary connection agreement can create new objects, whereas all other types of connection agreements only replicate information to existing objects.
- Public folder connection agreements cannot be connection agreements between organizations. Establishing a public folder connection between organizations requires the use of an additional tool, which is not required in this environment.

Connection Agreement Implementation

The following section outlines recommendations for placement of user accounts in both Active Directory and the Exchange 5.5 environment. The names outlined in this section are only recommendations.

This section uses graphical representations of the recommended configuration (Figure 4), as well as, screen shots, tables, diagrams, and a brief description of each critical container.

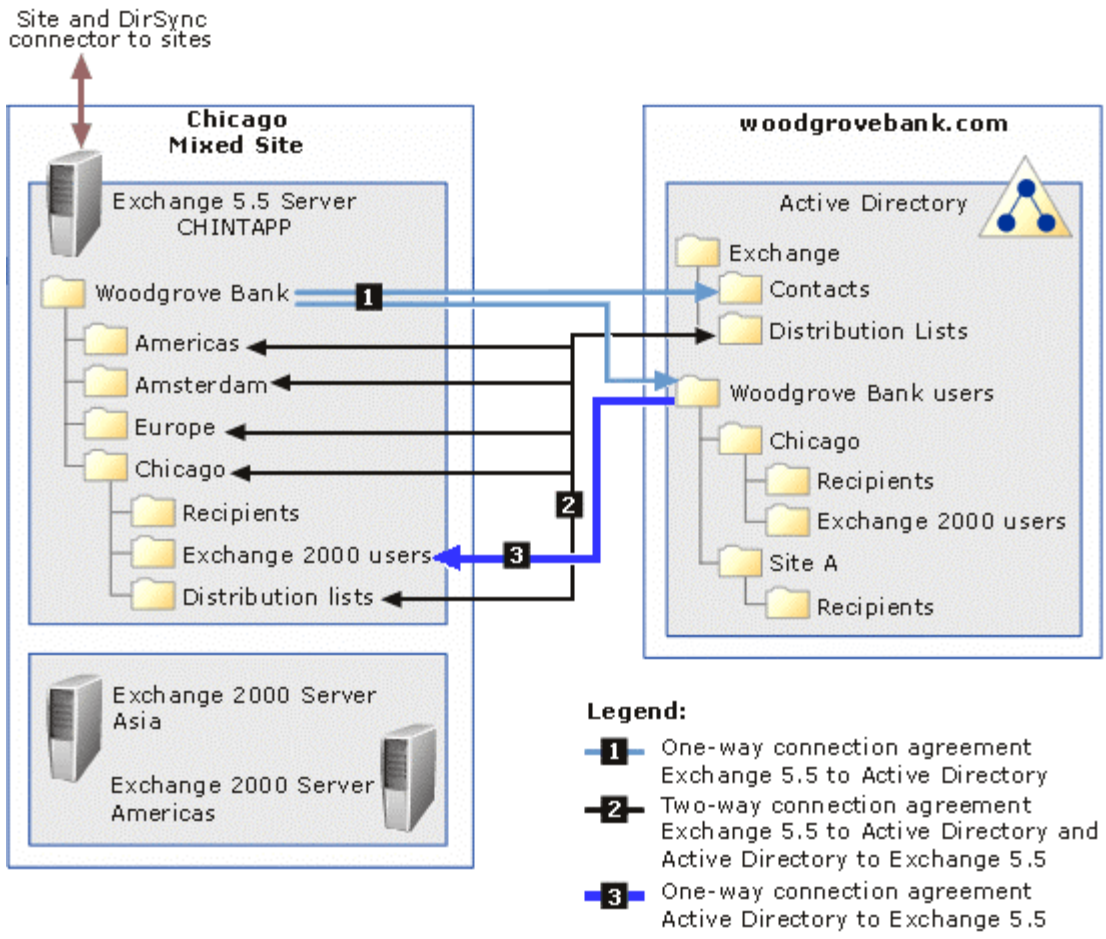

Figure 4 Recommended connection agreement configuration

Configuration Connection Agreements

Configuration connection agreements are located on the server running ADC and are created automatically when ADC is installed. ADC creates the configuration connection agreement, which facilitates Exchange 2000 and Exchange 5.5 communication. A configuration connection agreement does not require any special configuration and should not be modified. Two configuration connection agreements (ConfigCA _Chicago_<*Server Name*> and ConfigCA_London_<*Server Name*>) are created after Exchange 2000 is installed in the Chicago and London Exchange 5.5 sites.

Recipient Connection Agreements

Intra-organizational connection agreements need to be configured to replicate objects between the Exchange 5.5 directory and Active Directory. To replicate mailbox users, custom recipient, and distribution list information into Active Directory, three types of recipient connection agreements should be defined:

- **Mailboxes** It is recommended that you use dual one-way connection agreements to replicate mailboxes and users between Exchange 5.5 and Active Directory. This type of connection agreement should be used to bring Exchange 5.5 mailbox information into Active Directory by creating a mail-enabled, disabled user. Likewise, this connection agreement will bring mail-

enabled Active Directory user accounts into Exchange 5.5 as mailboxes. Active Directory user accounts are represented by mailboxes in Exchange 5.5. However, no Active Directory user data is located in the Exchange 5.5 directory. The following organizational units and recipient containers should be used in mailbox replication at Woodgrove Bank:

- **The Woodgrove Bank Users organizational unit** The purpose of this organizational unit is to hold all Exchange 5.5 mailbox information in Active Directory by creating Mail-Enabled Disabled-Users. Actually, ADC creates a complex organizational unit hierarchy under the Woodgrove Bank Users organizational unit that is based on the existing Exchange site names and containers. This complex structure is where the Mail-Enabled Disabled-Users will be located. The top-level Woodgrove Bank Users organizational unit is where native Active Directory users will be located and where Active Directory users should be placed after they migrate from Exchange 5.5 (Figure 5 and Table 2).

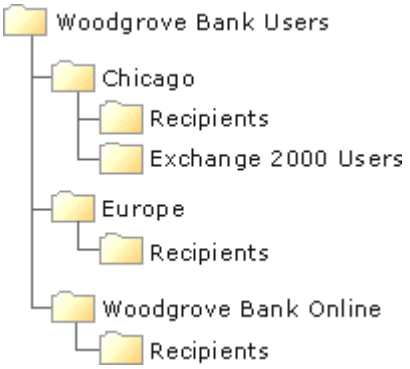

Figure 5 Structure of the Woodgrove Bank Users organizational unit

Table 2 Woodgrove Bank Users organizational unit connection agreement

Connection Agreement Name	Connection Type	Exchange 5.5 Container	Windows 2000 Organization Unit
Exchange 5.5 to Active Directory (Mailboxes)	One-way connection agreement from Exchange	o=Woodgrove Bank	ou=Woodgrove Bank Users,dc=Woodgrove Bank,dc=com

- **The Exchange 2000 users recipient container** This container should be located in the Chicago site in Exchange 5.5. The Exchange 2000 users container should be used to isolate and represent all Active Directory users in the Exchange 5.5 environment. The Exchange 2000 users container will replicate throughout the Exchange 5.5 environment based on standard site replication topology.

Table 3 Exchange 2000 users recipient container connection agreement

Connection Agreement Name	Connection Type	Windows 2000 Organization Unit	Exchange 5.5 Container
Exchange 5.5 to Active Directory (Mailboxes)	One-way connection agreement from Windows	ou=Woodgrove Bank Users,dc=Woodgrove Bank,dc=com	cn=Exchange 2000 Users,ou=chicago, o=Woodgrove Bank

- **Custom recipients** It is recommended that you use a one-way connection agreement to replicate custom recipients between Exchange 5.5 and Active Directory. This connection agreement will be used to replicate Exchange custom recipients into Active Directory by creating contacts in Active Directory. Likewise,

Active Directory contacts will appear as custom recipients in the Exchange 5.5 environment.

- **The Exchange organizational unit** This organizational unit will contain two subordinate organizational units—contacts and distribution lists. For custom recipient replication, only the contacts organizational unit will be populated and modified (Figure 6).

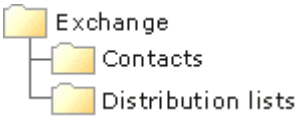

Figure 6 Structure of the Exchange organizational unit

- **The contacts recipient container** This container should be located in the Chicago site in Exchange 5.5. The contacts container should be used to isolate and represent all contacts in the Exchange 5.5 environment. The contacts container will replicate throughout the Exchange 5.5 environment based on standard site replication topology.

Table 4 Contacts container connection agreement

Connection Agreement Name	Connection Type	Exchange 5.5 Container	Windows 2000 Organization Unit
Exchange 5.5 to Active Directory (custom recipients)	One-way connection agreement from Exchange	o=Woodgrove Bank	ou=Contacts,ou=Exchange,dc=Woodgrove Bank,dc=com

- **Distribution lists** The purpose of these connection agreements is to manage membership changes automatically in each system. No special administrative effort will be needed to synchronize changes between the two systems after these connection agreements are configured.

  It is recommended that you use multiple two-way connection agreements to replicate distribution lists (from Exchange 5.5 to universal security groups) in Active Directory.

  A two-way connection agreement should be created for each site. Every container in that site should be selected as part of the connection agreement (from Exchange 5.5). The default destination should be the distribution lists organizational unit in Active Directory

  The two-way connection agreements will also synchronize universal distribution groups back into Exchange 5.5 as distribution lists. In this design, the connection agreement properties for the Chicago site two-way connection agreement are configured to replicate to the distribution list container in the Chicago Exchange 5.5 site. All other connection agreements should point to the recipients container in the associated site. In other words, only the connection agreement configured for the Chicago site should point to the distribution lists container in Exchange 5.5 (Figure 7).

  Note This design is time consuming to configure and requires a solid understanding of Active Directory Connector.

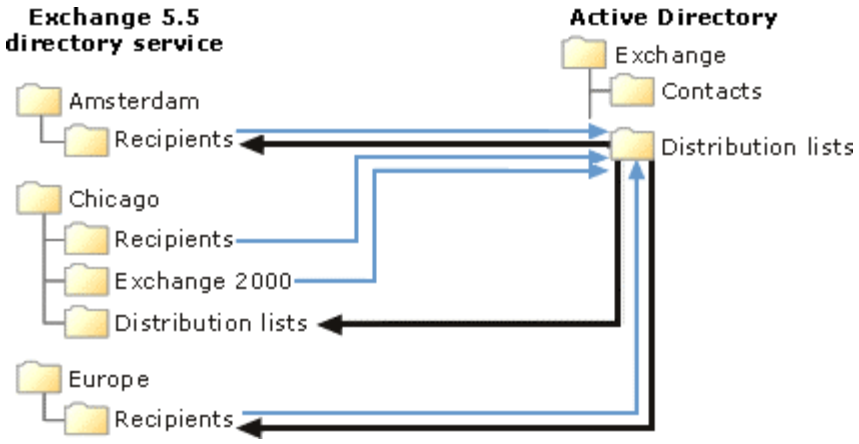

Figure 7 Distribution list to universal distribution group connection agreement

- **The Exchange organizational unit** This organizational unit will contain two subordinate organizational units—contacts and distribution lists. For distribution list replication, only the distribution list organizational unit will be populated and modified.
- **The distribution lists recipients container** This container should be located in the Chicago site in Exchange 5.5. Use the distribution lists container to isolate and represent all universal distirbution groups in the Exchange 5.5 environment. The distribution lists container will replicate throughout the Exchange 5.5 environment based on standard site replication topology.

Table 5 Distribution Lists container connection agreement (Exchange 5.5 to and from Active Directory)

Connection Agreement Name	Connection Type	Exchange 5.5 Container	Windows 2000 Organization Unit
Exchange 5.5 to and from Active Directory (distribution lists and universal distribution groups)	Two-way connection agreement from Exchange	ou=container; ou=site, o=Woodgrove Bank	ou=Distribution Lists, ou=Exchange, dc=Woodgrove Bank,dc=com

Note When creating the connection agreement between distribution lists and universal distribution groups, select at least every container with Exchange 5.5 distribution lists, or for simplicity, select every container. This prevents extraneous organizational units from appearing in Active Directory.

Table 6 Distribution Lists container connection agreement (Exchange 5.5 to or from Active Directory)

Connection Agreement Name	Connection Type	Exchange 5.5 Container	Windows 2000 Organization Unit
Exchange 5.5 to or from Active Directory (distribution lists or universal distribution groups)	Two-way connection agreement from Windows	ou=Distribution Lists, ou=Exchange, dc=Woodgrove Bank,dc=com	ou=Distribution Lists, ou=Chicago, o=Woodgrove Bank

Note Only one connection agreement can point to the container mentioned above. All other connection agreements will need to point to a random container in their home site.

Public Folder Connection Agreements

A single two-way public folder connection agreement should be created for replicating public folders proxy objects between the Exchange 5.5 directory and Active Directory. Because the server running Exchange 2000 is in the same site, no special configuration is needed. The only step is to create the connection agreement with a name, set a schedule, and accept all other defaults.

Proposed Exchange 2000 Design

The following section outlines the proposed Exchange 2000 design for Woodgrove Bank. It contains details about the Exchange 2000 configuration, example hardware, and topology design.

Exchange 2000 Design Goals

Exchange 2000 is being designed as the messaging and collaboration environment for Woodgrove Bank. The proposed system will replace the existing Exchange 5.5 environment throughout the organization. Microsoft Outlook® 2002 will be the messaging client along with supplemental e-mail access through Outlook Web Access.

Currently, Woodgrove Bank has approximately 50 servers running Exchange 5.5 in its environment. This number of servers will be unnecessary after the existing Exchange 5.5 environment is replaced. Because it is running 50 servers, it is likely that Woodgrove Bank has a high total cost of ownership (TCO).

The new design attempts to minimize TCO; therefore, this design recommends a centralized Exchange 2000 environment using a minimal amount of servers. This approach will significantly reduce TCO and will provide users with a high level of availability and functionality. Also, a significant return on investment (ROI) may be realized within a short time.

Woodgrove Bank has elected to adopt the centralized Exchange 2000 messaging architecture with servers located in both hub locations (Chicago and London). Administration will be delegated to local administrators. However, centralized control over the Exchange environment will be established for administrators in Chicago.

Clients will access messaging resources across the new Virtual Private Network (VPN)–based WAN to their corresponding hub location.

The following list outlines the benefits of a centralized messaging architecture with servers in hub locations compared to a fully centralized or an expansive decentralized messaging architecture:

- **Reduced TCO** Considering the drastic reduction in the number of servers currently used to run Exchange 5.5, ongoing maintenance, repair costs, and administration will be reduced dramatically.
- **Client access time** Client access time should be satisfactory over the new high-speed VPN. Outlook 2002 has also been enhanced to improve performance.
- **Security** All servers running Exchange will be located at secured data centers instead of being located in each of the remote offices, which typically do not have good physical security.
- **Simplicity** A complex routing topology is not required to support the messaging infrastructure.
- **Faster message delivery** Fewer Exchange servers and simpler routing leads to faster message delivery times.
- **Roaming user support** Locating servers centrally allows users to easily move about offices and access their mail without noticeable performance loss.

Woodgrove Bank did not outline plans for developing on the Exchange 2000 development platform; therefore, the system was designed to optimize base functionality like messaging, calendaring, directory services, public folders access, and Instant Messaging.

Exchange 2000 Design Overview

Woodgrove Bank requested that the new Exchange 2000 environment be designed to support approximately 2,600 users, roughly double the current amount of users. Based on these requirements, the Exchange environment should consist of seven servers. A total of three mailbox servers (Americas, Europe, and Asia) are recommended. Both the Americas and Europe servers will be designed to support 1,000 users. The Asia server will have the capability of supporting 600 users.

ADC, SMTP Connector, and Outlook Web Access require two servers. The Outlook Web Access component (Exchange 2000 front-end server) should be installed on its own server isolated in a perimeter network on the firewall. The other server should run ADC and SMTP Connector.

It is recommended that Woodgrove Bank use two additional servers as recovery servers in the event that a production server running Exchange 2000 fails. These recovery servers can also be used as part of a single mailbox recovery strategy. The recovery servers should have enough storage capacity to hold all of the storage groups (the number of *.edb files) for the largest production mailbox server. Configuring a recovery server in each of the hub locations is recommended.

ADC will serve as the connector between the Exchange 5.5 and Exchange 2000 environment. The same server will also function as the SMTP virtual server for Woodgrove Bank, which will be responsible for inbound and outbound Internet mail.

Messaging will rely on global catalog servers for Active Directory and address book information. Clients will connect to the global catalog server closest to their location.

Instant Messaging and Microsoft Exchange 2000 Conferencing Server will be tested during the pilot phase. However, an extensive design for these services has not been completed.

All servers running Exchange 2000 should run on Windows 2000 Server with Service Pack 2.

Exchange 2000 Enterprise Server with Service Pack 1 (SP1) is recommended for all servers running Exchange 2000. The fixes described in the following knowledge base article are also recommended for all servers running Exchange 2000.

Q291222, "XGEN: Rollup of Selected Exchange 2000 Server Post-Release Fixes"

> **Note** It is highly recommended that you update all servers to the most recent service packs when they become available.

Exchange 2000 Design Components

The following section outlines individual components of the Exchange 2000 design. The information below provides recommendations for the specified component but does not cover conceptual information. For conceptual information, please refer to the "Terms and Concepts" section earlier in this document.

Integration with Active Directory

Four forests will comprise the Active Directory environment. These separate forests will all serve a different function used primarily for testing. Exchange 2000 will also be added to these separate forests.

Only one of the forests (composed of the woodgrovebank.com domain) will hold the production Exchange 2000 services. This forest will also be the production forest and can be referred to as the woodgrovebank.com forest root.

All Exchange 2000 servers will be installed in the woodgrovebank.com domain, which is the only production domain for this enterprise. The Active Directory domain will consist of about 50 sites. Each site will have a local global catalog server.

It should be understood that Exchange 2000 integrates tightly with Active Directory. Exchange 2000 does not have its own directory; it relies on Active Directory. All other information regarding Active Directory integration is not specific to Woodgrove Bank. For additional information about integration with Active Directory, refer to the "Terms and Concepts" section earlier in this document.

Administration and Routing Groups

Initially, all Exchange 5.5 sites are represented in Exchange 2000 by an administrative group and a corresponding routing group. This configuration cannot be changed while in mixed mode. Any changes to administrative groups must be made after the migration to Exchange 2000 is complete and switched to native mode.

After the migration is complete, switch the Exchange 2000 environment to native mode. It is recommended that you create a new administrative group and assign permissions to the appropriate users and groups. Then, move all routing groups (Chicago and London) along with their associated servers running Exchange 2000 (Americas, Europe, and Asia) and move those routing groups under the new administrative group.

After the routing groups are moved, create a new routing group and move all servers running Exchange 2000 (located in the other routing groups) into the single routing group.

The name of the administrative and routing group should be a simple name such as Exchange.

It is recommended that Woodgrove Bank have only one administrative and routing group for simplicity of administration. Some performance gains could be realized by using two routing groups and a routing group connector. However, the overall gains would be minimal because of the high link speeds between the locations. Figure 8 provides a more detailed description of the process.

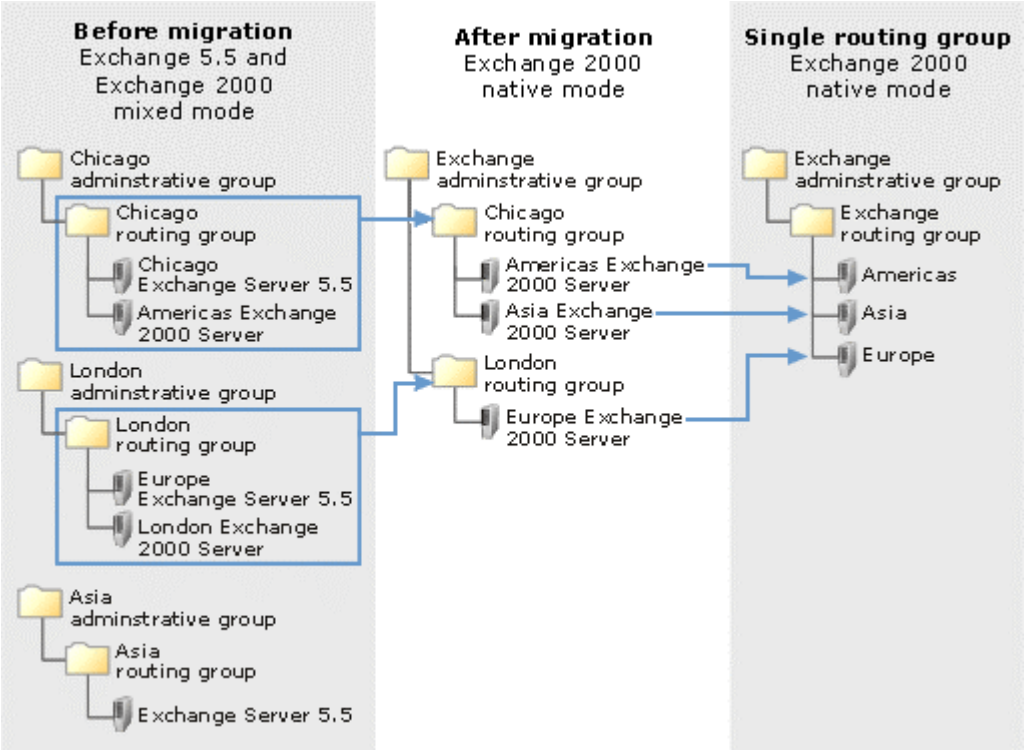

Figure 8 Exchange 2000 administrative and routing groups

Mailbox Servers

A total of three mailbox servers (Americas, Europe, and Asia) are recommended. Both the Americas and Europe servers will be designed to support 1,000 concurrent users. The Asia server will have the capability to support 600 concurrent users. These servers are designed to support roughly 2,600 total users or approximately double the current user population of Woodgrove Bank.

The Americas and Asia servers will be located in the Chicago data center. The Europe mailbox server will be located in the London data center.

The Americas and Asia servers running Exchange 2000 should be installed into the existing Chicago Exchange 5.5 site. Likewise, the server running Exchange 2000 server should be installed into the London Exchange 5.5 site.

The design recommends using moderate specifications for the mailbox servers. Based on the existing user base, potential growth, and current business requirements; these servers will be adequate to support the environment for 3 years.

Woodgrove Bank's business requirements dictate a 200-MB user limit for each mailbox. While Exchange is capable of supporting several hundred gigabytes of data, a more conservative limit is recommended initially. In the event of a total catastrophic failure, a 200-MB limit based on 1,000 users could take 24 hours or more to recover an entire server. A majority of Service Level Agreements (SLAs) would define a 24-hour recovery time as unacceptable. Therefore, the server configurations will be specified to accommodate the 200-MB user limit.

The mailbox servers at full capacity will be capable of supporting 200 MB per user with extra space for public folders. Currently, public folders are not heavily used and can be replicated to each of the mailbox servers for optimum client access performance. However, if public folder requirements change and more space is needed, using a separate server for public folders is recommended.

Table 7 Mailbox server hardware recommendations

Type of Server	Hardware Specifications
Mailbox server sized for approximately 1,000 mailboxes	• Dual 866 MHz Pentium III Xeon processor with a 256K L2 cache and • 1 GB of RAM • 4 X dual-channel RAID controller • 64-MB O/B RAID Controller Cache set • Dual redundant 10/100 TX NICs • Dual hot-swappable power supplies • Two 18-GB 10,000-RPM hot-plug disk drives—RAID 1 (system files) • Two 36-GB 10,000-RPM hot-plug disk drives—RAID 1 (log files for default and storage group 1) • Two 36-GB 10,000-RPM hot-plug disk drives—RAID 1 (log files for storage group 2) • Three 36-GB 10,000-RPM hot-plug disk drives—RAID 5 (indexing and queue logs files) • Two 36-GB 10,000-RPM hot-plug disk drives—RAID 1 (default first storage group) • Five 36-GB 10,000-RPM hot-plug disk drives—RAID 5 (stores for storage group 1) • Five 36-GB 10,000-RPM hot-plug disk drives—RAID 5 (stores for storage group 2)

Type of Server	Hardware Specifications
Mailbox server sized for approximately 600 mailboxes	• Dual 800-MHz Pentium III Xeon processor with a 256K L2 Cache • 640 MB of RAM • 4 X dual-channel RAID controller • 64-MB O/B RAID Controller Cache set • Dual redundant 10/100 TX NICs • Dual hot-swappable power supplies • Two 18-GB 10,000-RPM hot-plug disk drives—RAID 1 (system files) • Two 36-GB 10,000-RPM hot-plug disk drives—RAID 1 (log files for default and storage group 1) • Two 36-GB 10,000-RPM hot-plug disk drives—RAID 1 (log files for storage group 2) • Three 36-GB 10,000-RPM hot-plug disk drives—RAID 5 (indexing and queue logs files) • Two 36-GB 10,000-RPM hot-plug disk drives—RAID 1 (default first storage group) • Four 36-GB 10,000-RPM hot-plug disk drives—RAID 5 (stores for storage group 1) • Four 36-GB 10,000-RPM hot-plug disk drives—RAID 5 (stores for storage group 2)
Recovery server sized for approximately 1,000 mailboxes	• Dual 866 MHz Pentium III Xeon processor with a 256K L2 Cache • 1 GB of RAM • 4 X dual-channel RAID controller • 64-MB O/B RAID Controller Cache • Dual redundant 10/100 TX NICs • Dual hot-swappable power supplies • Two 18-GB 10,000-RPM hot-plug disk drives—RAID 1 (system files) • Two 36-GB 10,000-RPM hot-plug disk drives—RAID 1 (log files for default and storage group 1) • Two 36-GB 10,000-RPM hot-plug disk drives—RAID 1 (log files for storage group 2) • Three 36-GB 10,000-RPM hot-plug disk drives—RAID 5 (indexing and queue logs files) • Two 36-GB 10,000-RPM hot-plug disk drives—RAID 1 (default first storage group) • Five 36-GB 10,000-RPM hot-plug disk drives—RAID 5 (stores for storage group 1) • (5) 36-GB 10,000-RPM hot-plug disk drives—RAID 5 (stores for storage group 2)

Using these specifications, it is possible to achieve a recovery time of less than 1.5 hours in the event of a single message store failure on any of the mailbox servers. The failure of a single storage group could require up to 7.5 hours to recover on the Americas and Europe server and up to 4.5 hours on the Asia server. A catastrophic server failure could take as much as 24 hours to recover because of the time needed to rebuild the operating system and server hardware.

If a faster recovery time is needed, you can use the recovery servers to replace the production system. In this case, the recovery server would be brought online and installed with Exchange 2000. Users would then be able to access their new mailboxes and begin to send messages and perform group collaboration. The

EXMERGE process can then be run in the background to merge the user's old messages into their new mailboxes.

The recovery servers for each hub location should be capable of supporting their production counterpart in the event of a catastrophic failure. Recovery servers should also have enough disk space to recover all of the mailbox and public folder stores on a server running Exchange.

Storage Groups

This section covers storage group configuration per server. At a high level, each mailbox server should have two mailbox stores plus the default first storage group, which will accommodate the public folder storage group. The Americas and Europe server should have five mailbox stores per storage group and a public folder and message store in the default first storage group.

The Asia server should have three mailbox stores per storage group and one public folder store in the default first storage group. All other servers will default to the default first storage group with one mailbox and public folder store.

Each mailbox store should contain between 50 and 100 users depending on the size of the user population. For example, if Woodgrove Bank has 1,300 users then 50 mailboxes should be located on each mailbox store. If the population is 2,600 users, then each mailbox store should have 100 users.

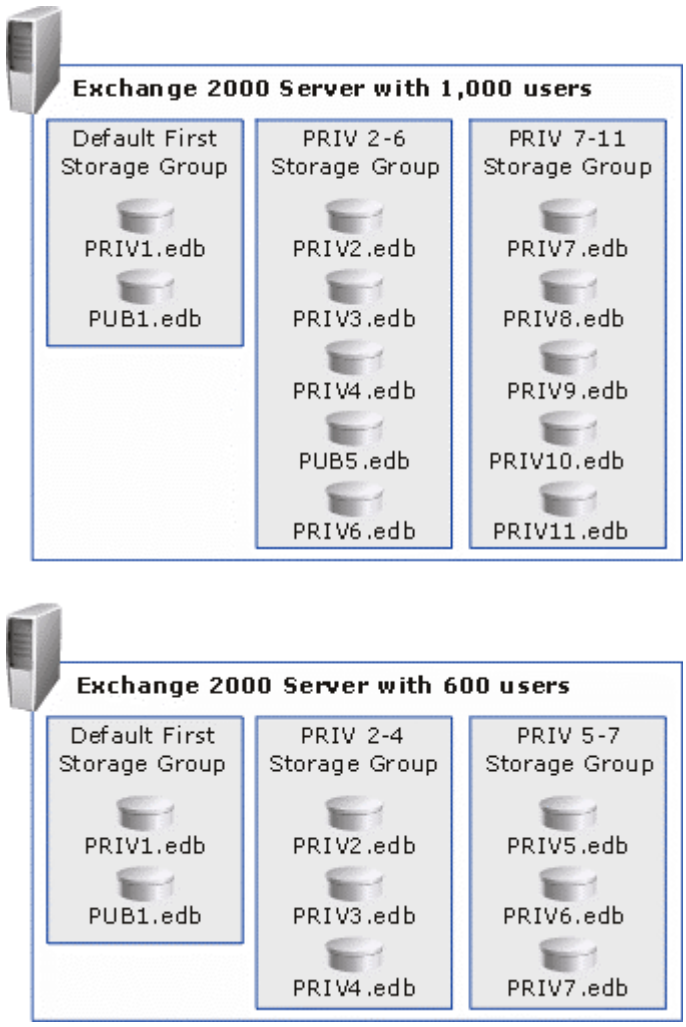

Figure 9 Exchange 2000 storage group configuration

Installable File System

The Installable File System (IFS) is a storage technology that functions as a filing system. It makes mailboxes and public folders available as traditional folders and files through standard 32-bit Windows processes such as Microsoft Internet Explorer or the command prompt. IFS makes it possible for you to map Exchange folders as shared network drives. IFS is used primarily for customized applications that use the Exchange mailbox store. Clients can use IFS by sharing drive M on the server running Exchange 2000.

However, the use of IFS is not recommended for Woodgrove Bank. There is no need or added benefit because customized applications are not used within Woodgrove Bank's Exchange 2000 system.

Routing Topology and Connectors

The routing topology at Woodgrove Bank will be very simple. During the migration and while in mixed mode, Exchange will use standard RPC calls between servers in the same site regardless of whether the servers run Exchange 5.5 or Exchange 2000. Communication between sites will take place over the existing site

connectors. Simply stated, the routing topology will not change from what is currently implemented.

Once in native mode, all Exchange 2000 servers (Americas, Europe, and Asia) should be placed in the same routing group as defined in the "Administrative and Routing Groups" section of this paper. Servers in the same routing group will communicate with each other directly over SMTP. Communication between servers running Exchange 2000 in the same routing group will occur as often as needed.

Public Folders

Each Exchange 2000 mailbox server should have a public folder store located in its default first storage group. For specific information about the server configuration, see the "Storage Groups" section earlier in this paper. The top-level public folder hierarchy will be created under the Chicago administrative and routing groups. This public folder tree will be the default tree for all MAPI clients. All servers in the mixed mode Exchange environment will associate with this public folder tree.

Existing public folders in the Exchange 5.5 environment should also be replicated to each of the new servers running Exchange 2000 (Americas, Europe, and Asia).

After the migration to Exchange 2000 is complete, public folders should be relocated on a chosen mailbox server. Clients will gain access to the local copy of the public folder store, which will improve performance. Public folder replication should be configured at set intervals and performed as often as needed. The replication schedule should be based on the users need to have updated information across all instances of the public folder store.

It is assumed that all clients will connect to public folders through MAPI. Therefore, only one public folder hierarchy can exist within the Woodgrove Bank Exchange organization.

Based on the low usage of public folders at Woodgrove Bank, it is recommended that administrators set public folder replication for every two hours between the hours of 8 A.M. and 6 P.M. and once again at 12 A.M.

After the Exchange 2000 environment is switched to native mode, move the public folder tree under the new administrative group defined in the "Administrative and Routing Group" section of this document.

Woodgrove Bank also wants to receive Internet newsgroup feeds. A thorough design of newsgroups feeds is out of scope for this project. However, based on best practices, it is recommended that administrators use a separate public folder server for newsgroups when implemented. Organizations tend to underestimate the storage capacity and management needed for newsgroup feeds.

The default Internet newsgroups public folder should be redirected to store information on the dedicated public folder server. By default, this folder will be linked to the first storage group in the Chicago routing group. This folder is automatically created under the first administrative group. The default Network News Transfer protocol (NNTP) virtual server (located in an administrative group) will be linked to the Internet newsgroups public folder by default, so no special configuration is needed. Then, the NNTP feed can be linked to the NNTP virtual server.

Outlook Web Access (Front-End Server)

One Outlook Web Access front-end server is recommended, which should be placed in the perimeter network (Figure 10). The Outlook Web Access server should be secured on the Internet in two ways. First, the Outlook Web Access server should be located behind the firewall or in the perimeter network where only a few ports will be opened. The most critical ports for Outlook Web Access are HTTP (port 80) and HTTPS/SSL (port 443). Secure Sockets Layer (SSL) is used to encrypt all data sent over the secure channel on the Internet and is highly recommend.

A server running Exchange 2000 is designated as a front-end server by selecting **This is a front-end server** under the server's property page. The server will then automatically redirect all HTTP requests to the appropriate back-end server.

An external DNS mapping must be defined to direct external Internet clients to the Outlook Web Access front-end server. A DNS name such as owa.woodgrovebank.com is recommended. Users gain access to the Outlook Web Access client by typing the DNS name into the Internet Explorer address window with */Exchange* appended.

For example, a user would type in https://owa.woodgrovebank.com/exchange. After the user gains access to the page, they are prompted for their Active Directory user account, domain, and password. After successful authentication, the user is allowed into their mailbox. Outlook Web Access has a similar look and feel to Outlook® 2000 and Outlook 2002; therefore, no special training should be required for normal usage.

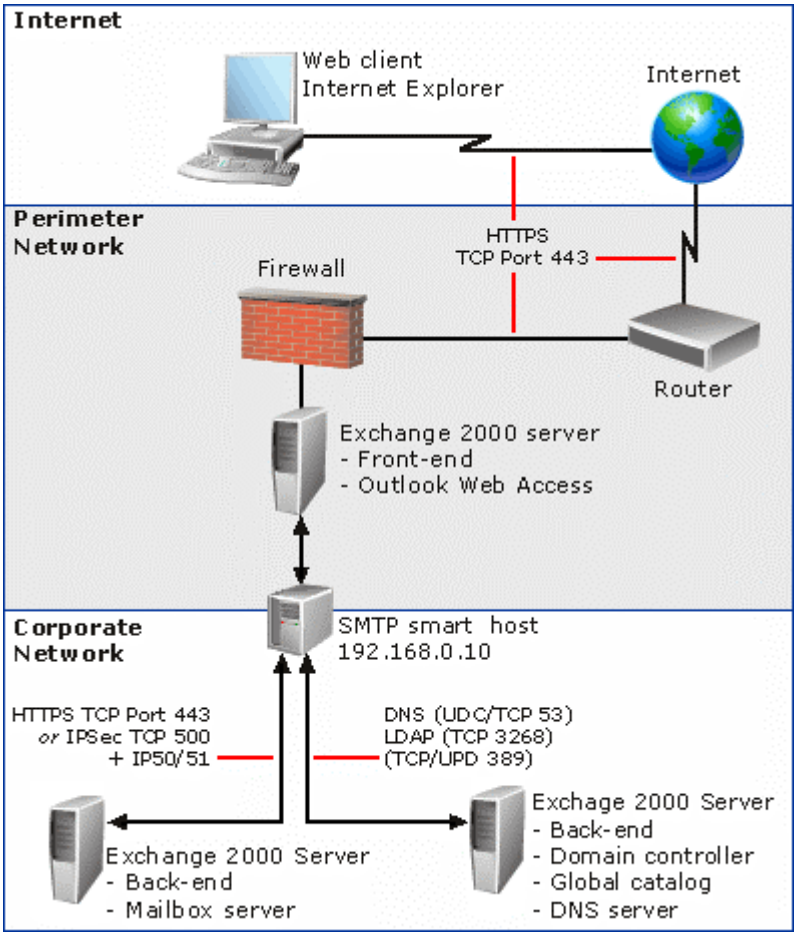

Figure 10 Exchange 2000 Outlook Web Access configuration

SMTP Virtual Servers

A default SMTP virtual server will be created on each server running Exchange 2000 when installed (Figure 11). Each default SMTP virtual server is capable of sending and receiving through the Internet without any special configuration (assuming DNS is configured properly). Recipient policies determine which domains are accepted for routing. By default, only the woodgrovebank.com domain will be allowed to route mail through the system. In other words, no mail relaying (RFC 821) should be allowed at Woodgrove Bank.

It is highly recommended that administrators use a dedicated server running Exchange 2000 for the SMTP Connector. Then, link each of the SMTP virtual servers to the SMTP Connector server and configure the connector to route to the appropriate smart host (192.168.0.10).

> **Note** A SMTP Connector is needed to route mail to the SMTP smart host. Default SMTP mail delivery to any domain is supported through the default SMTP virtual server.

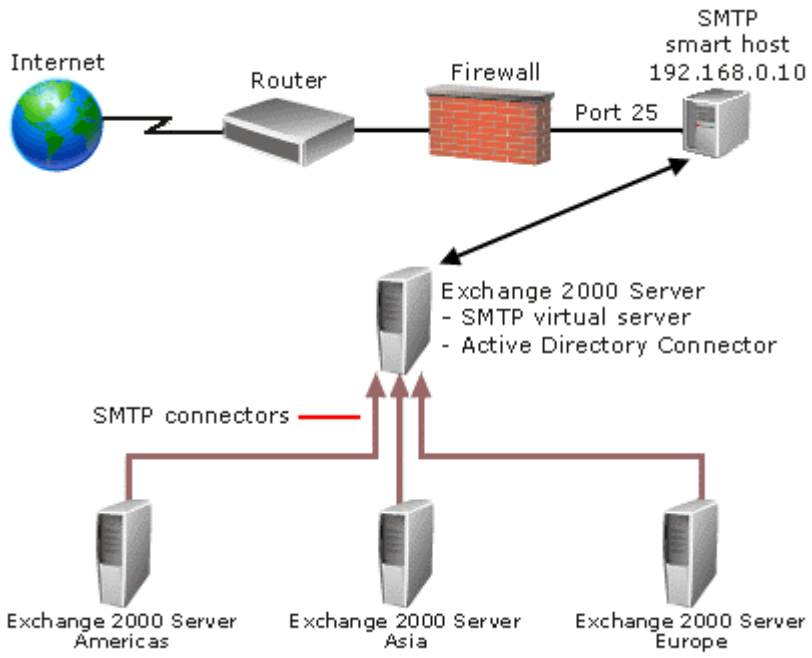

Figure 11 Exchange 2000 SMTP configuration

Instant Messaging Service

The Instant Messaging component of Exchange should be installed because it is a useful tool for reducing the amount of extraneous mail sent over the system. Instant Messaging is a real-time communication utility, which can be used to pass messages between two or more users without having to compose a formal message. In most cases, Instant Messaging is a better utility to use for informal communication with users in your immediate workgroup.

The Instant Messaging component should be installed on the SMTP gateway server. By installing the Instant Messaging component on the SMTP gateway server, if a mailbox server is unavailable, users can still use Instant Messaging to communicate. When installing the Instant Messaging virtual server, Woodgrove Bank should use the domain name im.woodgrovebank.com and then add a DNS RVP service record to redirect requests to woodgrovebank.com to the im.woodgrovebank.com server. By employing this method, users will be able to add other users to their Instant Messaging contact lists using the users SMTP e-mail address.

Client communication takes place over the RVP protocol. It is recommended that administrators use the MSN® Messenger Service for Exchange. For specific details about the Instant Messaging service, see the *Microsoft Exchange 2000 Resource Kit*.

Policies

The use of policies defined at the administrative group level is recommended. Multiple policies may be needed in order to accommodate different time zones and physical location dependencies. The following table outlines some of the settings it is recommended that Woodgrove Bank implement.

Table 8 Policy recommendations

Policy	Item and Setting
Storage Limits	Warning = 75/175 MB Prohibit Send = 100/200 MB Prohibit Receive = Not used **Note** The 75 and 100 limits are initial settings defined by Woodgrove Bank.
Deleted Items	Keep deleted items = 15 days Keep deleted mailboxes = 60 days **Note** Do not permanently delete mailboxes until the store has been backed up.
Indexing	Update Interval = 12 A.M. to 4 A.M. Monday through Friday Rebuild Interval = 12 A.M. every Saturday
Maintenance	Defrag = Sunday through Saturday 2 A.M. to 6 A.M. **Note** Assumes backups are performed from 8 P.M. to 12 A.M. Sunday through Saturday

Security

Security is and can be very complicated. A full security plan is not in scope for this project. Many default security features are part of the Exchange 2000 system and can be used. It is recommended that a full security audit is performed and recommendations are made at the time of implementation. Woodgrove Bank should define their exact security requirements and then configure the Exchange 2000 environment accordingly.

Virus Protection

It is recommended that customers deploy an anti-virus solution based on the Exchange Virus Scanning API. The Virus Scanning API was released with Exchange 5.5 SP3 and is included with Exchange 2000. The new API enhances the current core feature set by providing the abilities to optimize and configure the scanning process at multiple levels as well as providing Exchange administrators with built-in functionality to monitor the performance of the new API.

An external SMTP anti-virus smart host is used for scanning inbound mail from the Internet over port 25. Woodgrove Bank will continue to run a third-party anti-virus product to protect their Exchange environment.

Disaster Recovery

This section outlines disaster recovery policies recommended for Woodgrove Bank.

- **Backups** It is recommended that Woodgrove Bank implement a nightly, full-backup strategy for all servers running Exchange 2000. It is also recommended that Woodgrove Bank test the backup and recovery process periodically. Backups should be performed daily between 8 P.M. and 12 A.M. Because of the amount of storage space required, the use of multiple backup devices will be needed to achieve an acceptable backup time. Using only one device, it would take 8 hours or more to backup a single server running Exchange.

  Other strategies, such as differential and incremental backups, can complicate and extend recovery times. Therefore, these strategies are not recommended and should be avoided.

  SLAs produced for Woodgrove Bank should detail acceptable recovery times in the event of partial or total system failure. SLAs, specifically the restoration of

data, will largely depend on the speed at which data can be recovered from the backup device and the amount of transaction logs that need to be replayed before the Information Store service is started.

If realistic SLAs are to be met, it is recommended that administrators perform full testing of the backup solution to the maximum sizes of stores based on the time taken to backup and recover.

- **Deleted item recovery** Deleted item retention allows individual users to recover previously deleted items from within Outlook. Deleted item retention also applies to mailboxes when an administrator deletes the mailbox. Using a generous limit with this feature (defined through system policies) greatly reduces the chances of having to recover data. The recommended settings are outlined in the "Policies" section earlier in this document.
- **Outlook Offline Storage Files** Client computers will also be configured with an offline storage file (an .ost file), which is used by end users to view their mail when not connected to the network. An .ost file is stored on the user's local hard drive and is updated every time the user chooses. Because .ost files are stored on the local drive, an .ost file provides an extra level of recovery for each user.

Content Indexing

Built in full-text content indexing and search of both e-mail and attached documents translates into less time searching for information and higher productivity. However, there will be some extra load on the CPU and the administrator should allow 25 to 30 percent additional disk space. The recommended settings for indexing are outlined in the "Policies" section earlier in this document.

Offline Address Books

To support mobile users, the offline address list allows a user to copy the contents of a server-based address book into a set of offline address book files (files with an .oab extension) stored on the local client's hard disk.

Based on the amount of users at Woodgrove Bank, it is recommended that administrators use the global address list (GAL) as the source for offline address book generation. Offline address books are configured through System Manager. An offline address book is associated with a mailbox store on a server running Exchange 2000 and can be unique among administrative groups. It is recommended that administrators generate an offline address book on each of the Exchange 2000 mailbox servers (Americas, Europe, and Asia).

For more information: http://www.microsoft.com/exchange/

Did this paper help you? Please give us your feedback. On a scale of 1 (poor) to 5 (excellent), how would you rate this paper?

mailto:exchdocs@microsoft.com?subject=Feedback: Case Study: Woodgrove Bank Microsoft Exchange 2000 Enterprise Server Design and Implementation

◆ ◆ ◆ ◆