Planning the Domino System

Powered by Notes

The First Groupware and E-mail Server for the Net
COPYRIGHT

Under the copyright laws, neither the documentation nor the software may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form, in whole or in part without the prior written consent of Lotus Development Corporation, except in the manner described in the software agreement.

© Copyright 1995 - 1997 Lotus Development Corporation
55 Cambridge Parkway
Cambridge, MA 02142

All rights reserved. First edition printed 1997. Printed in the United States.

Domino, Domino.Action, Domino.Broadcast, Domino.Connect, Domino.Merchant, Lotus Notes Desktop, Notes, NotesBench, NotesPump, NotesSQL, Notes Desktop, Notes Mail, Weblicator, and Work The Web are trademarks and Lotus, Lotus Notes, Lotus Organizer, LotusScript, Notes Mail, NotesView, SmartSuite, and Word Pro are registered trademarks of Lotus Development Corporation. cc:Mail is a trademark of cc:Mail, a wholly-owned subsidiary of Lotus Development Corporation. IMS is a trademark and AIX, AS/400, CICS, DB2, IBM, OfficeVision, and OS/2 are registered trademarks of International Business Machines Corporation. SAP and R/3 are registered trademarks of SAP AG. Soft-Switch is a registered trademark of Soft-Switch, Inc., a wholly-owned subsidiary of Lotus Development Corporation.

Other product and company names mentioned herein may be the trademarks or registered trademarks of their respective owners.
## Contents

**Chapter 1  Planning the Domino System ........ 1**
- Using Lotus Domino .................. 1
- Domino as a business solution ........ 2
- Using *Planning the Domino System* ........ 3
- About using Lotus Web sites to locate additional information ........ 4

**Chapter 2  Planning a Domino Deployment ........ 7**
- Sharing information and reengineering processes with Domino ........ 7
- Assessing the needs of your organization ........ 7
- Assessing business needs ........ 8
- Assessing technical issues ........ 8
- Success depends on people ........ 9
- Planning for Domino at an organizational level ........ 10
- Where to include Domino ........ 10
- Upgrade to Domino ........ 10
- Establish a time frame ........ 11
- Create a rollout team ........ 11
- Make Domino deployment a success ........ 11
- Integrating Domino into your information systems infrastructure ........ 12
- Planning for future growth ........ 13
- Using Domino Server.Planner for capacity planning ........ 14
- About using NotesBench statistics with Domino Server.Planner ........ 15
- Planning for Domino on the Internet ........ 16
- Planning a Domino intranet ........ 17
- Planning for Domino clients ........ 17
- Planning for rolling out Domino in a workgroup ........ 18
- Upgrading to the new software ........ 18
- Using Domino in daily activities ........ 19
- Deploying the software ........ 19
- Planning a pilot project for Domino ........ 19
- Supporting the Domino deployment ........ 20
- Planning for Domino administration ........ 21
- Planning for security ........ 23
- Naming conventions and requirements ........ 24
- Guidelines for naming a Domino server ........ 25

**Chapter 3  Using Domino as a Business Solution ........ 27**
- Creating an intranet based on Domino ........ 27
- Accessing enterprise and legacy data from Domino ........ 28
- Creating an electronic store on the Internet with Domino ........ 29
- Managing documents in an organization ........ 30
- Integrating Domino and Notes with other applications ........ 31
- Ensuring access to Domino ........ 31
### Chapter 4 Deploying Applications

- Deploying applications on Domino .......... 33
- Using templates .................................. 33
- Programming support ............................. 33
- Deploying database applications to the Internet ...... 35
- Designing databases for better performance .......... 36
- Distributing applications on Domino .............. 37
- When to create a replica .......................... 37

### Chapter 5 Deploying Domino to the Internet

- About using Domino on the Internet ................ 39
- Using Domino to create an interactive Web site ...... 40
- Using Domino.Action to create a Web site .......... 41
- Setting up a Domino infrastructure for the Internet ... 42
- About Internet messaging ............................ 43
- About the Lotus Domino SMTP/MIME MTA .......... 45
- An MTA, not just a gateway .......................... 45
- Built on standards .................................. 45
- Configuring directory access with LDAP ............... 46
- Configuring Domino newsgroups ....................... 47

### Chapter 6 Deploying a Domino Intranet

- Types of Domino intranets .......................... 49
- Getting a return on your intranet investment .......... 51
- Intranet security .................................... 52
- About intranet applications .......................... 53
- About mail on your intranet .......................... 54
- Pushing information to your users ..................... 54
- Scaling your Domino intranet ......................... 55

### Chapter 7 Deploying a Domino Extranet

- About deploying a Domino extranet .................. 57
- About administering individual extranet security ...... 58
- Using an extranet to access Notes mail over the Internet .... 59

### Chapter 8 Deploying Domino Servers

- About setting up Domino servers ..................... 61
- About partitioned servers ............................ 62
- About server topology and replication ................. 62
- Examples: About server topology and replication .... 64
- About hub-spoke topology ............................ 66
- Designating servers for tasks ......................... 66
- About passthru servers ................................ 68
- About Domino and file servers ....................... 68
- Deploying Domino in multi-protocol environments ...... 69
- About integrating Domino with Microsoft Windows NT ... 69
- Planning for replication .............................. 70
- About using replication in an organization .......... 71
- About database replicas and database copies .......... 71
- About replicating servers ............................ 72
- Planning replication scheduling ....................... 73
- About improving replication performance .............. 75
- About using replicas on Notes workstations .......... 76
## Chapter 9 Deploying Clients 83

### About deploying clients 83

- Deploying Notes clients and creating
  - Notes users 84
  - Common Setup Profile 85
  - Register multiple users 85
  - Automated installation 85
- About distributing Notes IDs 86
- About communication 86

## Chapter 10 Deploying Mail 87

### About deploying mail 87

- About deploying Domino as a mail server 88
- Planning mail routing in a
  - Domino system 88
- About mail routing and the Internet 90
  - How mail travels between Notes and the Internet 90
  - How mail travels from the Internet to Notes 91
- About the components of the
  - SMTP MTA 92
  - Add-in Controller 92
  - Outbound Message Conversion 92
  - Outbound Session Controller 92
  - Outbound Session Handler(s) 93
- About configuring the
  - SMTP/MIME MTA 95
  - Preparing to configure the MTA 95
  - Using the Ping utility to test connectivity 96
- About connecting
  - SMTP/MIME MTAs 96
- About connecting one
  - SMTP/MIME MTA directly to the Internet 97
- About accessing the Internet
  - through a firewall or other mail relay 100
  - Example: Accessing the Internet through a firewall or other mail relay system 100
- About using one MTA for Internet messages and one MTA for Intranet messages 105
- About mail routing and domains 110
- About mail routing and multiple
  - Public Address books 111
Separate Public Address books  .................................. 111
Directory assistance ............................................. 111
Cascading Public Address books  ....................... 112
Summary of methods for managing multi-domain Public Address books  .................. 113
Mail routing within a Domino named network  .................. 113
Mail routing between Domino named networks ................. 114
About server connections for mail routing ............. 114
About mail routing and priority levels .................. 115
About mail files ............................................. 115
About accessing mail from Internet clients .............. 116
About shared mail ........................................ 116
About accessing mail from MAPI clients ............... 116
Setting up the Calendar and scheduling across your organization .................. 117

Chapter 11 Ensuring Security in a Domino System  ........ 119
About security in a Domino System ....................... 119
About Internet security .................................... 120
Firewalls ........................................... 120
Proxy servers ......................................... 121
Encryption ......................................... 121
Internet activity tracking ................................. 122
Notes client .......................................... 122
About network security ................................ 122
Guarding against unauthorized access ................... 122
Guard against viruses .................................. 123
Guard the physical system .............................. 124
About hierarchical naming ............................. 124
Verifying identities .................................... 124
Organize the company ................................ 125
About Domino server security ....................... 127
About Web browser client security .................. 128
About Notes client security ........................ 128
About database security ............................. 130
Access levels ....................................... 130
Permissions ........................................ 130
Roles ............................................. 131
Internet .......................................... 131
About database encryption ......................... 131
About controlling access to database design elements .... 132
About mail security .................................. 133

Chapter 12 Administering Domino ....................... 135
About administering Domino servers ............ 135
Optimizing server performance .................... 136
Dividing administration responsibilities ................. 137
Administration guidelines for better server performance .................. 137
Monitoring and maintaining servers ................ 138
Checking for dead mail ................................ 139
About the Database Fixup utility ..................... 139
About the Log database ............................. 140
Monitoring server events and statistics ................ 140

Appendix A Improving Domino Server Performance ........ 143
About editing the NOTES.INI file to improve performance .......... 143
About improving NLM server performance ................ 144
Improving STARTUP.NCF .......................... 144
Improving AUTOEXEC.NCF ............. 145
About improving OS/2 Warp server performance ........ 146
Choosing a file system ............... 146
Disk swapping ...................... 147
Disk caching ...................... 147
Configuring memory ................ 148
Configuring your disk .............. 148
About improving Windows NT and Windows 95 performance .......... 148
About improving UNIX server performance ................ 149

Index .......................... Index-1
Chapter 1  
Planning the Domino System

The Lotus® Domino™ server and Lotus Notes® client are powerful tools for communication, collaboration, and sharing information. To get the most benefit from Domino and Notes™, carefully plan how to set up your Domino system and how to deploy it. Deployment is the process of configuring your network infrastructure, installing the Domino servers and clients, setting up applications and mail, and reengineering your business processes to take advantage of the capabilities of Domino. Planning the Domino System is an overview that aims to help you succeed with your Domino deployment.

Using Lotus Domino

The Lotus Domino server answers the need for a complete Internet and intranet server. With Domino, you gain standards-based Internet messaging, groupware, interactive Web sites, and the ability to automate business processes. By combining Domino with Lotus Notes, you leverage the functionality of the most feature-rich client available, one that combines integrated Web browsing, calendar and scheduling features, e-mail, applications, and integration with other software like office suites. Domino and Notes function as the single entry point to all of your organization’s information.

By using the power of Domino to Work The Web™, you can create an interactive Web site that displays different content to different people. Internet applications on Domino produce dynamic content managed by the Domino object store. Other Web applications are static and based on file systems, whereas Domino is truly interactive. Domino security lets you limit access while distributing responsibility for content creation, site design, and user management within your organization. Set up your site through a Graphical User Interface (GUI) from either a Notes client or a Web browser without having to learn HTML, CGI, Perl, or Java. If you want to use these tools, Domino supports them fully.

Domino leads the market in supporting open standards. For messaging, Domino supports Post Office Protocol 3 (POP3), Internet Message Access Protocol (IMAP), Lightweight Directory Access Protocol (LDAP), Simple Mail Transfer Protocol (SMTP), and Multipurpose Internet Mail Extensions (MIME). For Web use, Domino supports HyperText Transfer Protocol
(HTTP), HyperText Markup Language (HTML), and Network News Transfer Protocol (NNTP). Domino Internet security includes support for the Secure Sockets Layer (SSL) protocol and X.509 certificates. You can use your existing Internet infrastructure with Domino and be assured that your system works with other systems based on open protocols. The Domino server for the Web is available on a number of platforms, including IBM® OS/2®, Microsoft Windows NT, Novell NetWare, and several types of UNIX operating systems.

The Domino server is available in two configurations: the Lotus Domino 4.6 Mail server, a complete messaging server, and the Lotus Domino Web server, which combines the messaging functionality of the Domino Mail server with the power of Internet and intranet application development. Upgrading from the Domino Mail server to the Domino Web server is straightforward.

Domino makes developing applications that automate business processes easy. For an organization with heterogeneous platforms and operating systems, use the seamless cross-platform design of application databases created with the Lotus Notes Designer for Domino client. With the Notes Designer for Domino client, you can create applications from a GUI with no knowledge of programming or scripting languages. Templates make setting up and configuring applications “out of the box” fast and easy. Applications on Domino can route information automatically, alert users that an item is overdue or needs attention, exchange information with enterprise software like relational databases and transaction processing systems, and “push” information to user desktops.

Domino supports a wide variety of clients: the Notes client, the most feature-rich client available; POP3 and IMAP clients such as Lotus Mail and Qualcomm Eudora; NNTP clients such as Internet news readers; Internet browsers such as Microsoft Internet Explorer and Netscape Navigator; and LDAP clients.

---

**Domino as a business solution**

Managing information is one of the foremost challenges organizations face. Data resides in multiple formats in many locations. Making information available in an organized, timely way is critical. Domino solves many of the difficulties and breaks down many of the barriers you face in managing information. Tap the power of the Internet as an information resource and as a means of advertising and commerce with Domino web sites and electronic store fronts. A Domino intranet brings advanced messaging, scheduling,
databases, and knowledge-archiving capabilities to your organization. To achieve greater efficiency and closer ties with other organizations, such as suppliers and distributors, create a Domino extranet to allow them controlled access to information in your organization. Domino integrates with other knowledge systems, including:

- Enterprise information systems such as SAP® R/3®, transaction processing systems such as Tuxedo and Tandem, and relational databases such as Oracle and Sybase with Domino.Connect™
- Document management and control systems through Domino.Doc
- Office productivity suites such as Lotus SmartSuite® and Microsoft Office
- Intranet push technology such as PointCast with Domino.Broadcast™
- Online commerce systems such as CyberCash with Domino.Merchant™
- Network computers

Domino provides a single security and administration point for your data and gives users a consistent interface; users see information from a system like SAP R/3 presented the same way they see data from the Internet or from a database. Applications hosted on Domino leverage this access to information with sophisticated workflow automation capabilities.


---

**Using Planning the Domino System**

This guide discusses the concepts, terms, requirements, features, and tradeoffs of a Domino system. Use this guide to develop a comprehensive plan for rolling out and deploying Domino in your organization. *Planning the Domino System* contains references to other parts of the Domino and Notes documentation set that go into greater detail about procedures and technical information.

Read the guide in order; if you do not plan to use certain features of Domino, such as the extranet features, you can skip those sections.
About using Lotus Web sites to locate additional information

Lotus provides several Web sites designed to help you locate the latest information on Domino, Notes, and other Lotus products:

- http://www.lotus.com is the main Lotus home page, which contains general information on Lotus products and services, including press releases, downloadable software, support, and purchasing information. You can use the Lotus home page to gain access to the sites and pages below or access them directly using the URLs provided.
- http://www2.lotus.com/services/notesua.nsf contains Domino, Notes, and related product documentation, browsable documentation databases, ordering information, tips on using the documentation, links to provide feedback, and the latest information on the product.
- http://www2.lotus.com/notes.nsf contains Notes product information and software. Use this Web site to download Notes products and review product specifications, demos, and press releases.
- http://domino.lotus.com contains the latest information on Domino, including software discussions, tips on creating Web applications, documentation, and bug reporting.
- http://www2.lotus.com/partners.nsf contains Notes application development and Business Partner information, including development tips and techniques, innovative applications, developer discussions, and updates on the latest product releases. You can also use this Web site to find out information and request an application for the Lotus Business Partner program.
- http://www2.lotus.com/developers/tools.nsf contains the latest tools and information for developing Notes applications and integrating them with back-end systems, such as DBMS and transaction systems. Use this Web site to download the latest version of the Notes APIs, participate in software discussions, and review white paper and redbook information.
- http://www.net.lotus.com contains the latest information and software for Internet applications using Domino technology, such as Domino.Action™.
• http://support.lotus.com contains support information on Lotus products, including common questions and solutions, user discussions, downloadable files, and Lotus support phone numbers. You can also use this Web site to search the KnowledgeBase for technical information on Lotus products.

• http://www.lotus.com/notesmta contains information on Lotus Notes Messaging Services, which allow Domino administrators to set up mail routing from different mail systems. These Messaging Services include message transfer agents (MTAs), such as the SMTP/MIME, cc:Mail, and X.400 MTAs.

• http://www.lotus.com/systems contains information on systems management and software distribution utilities you can use to manage Domino and Notes.

• http://www.lotus.com/contacts contains telephone numbers, e-mail addresses, and mail addresses to use when you need to contact Lotus.

• http://www.support.lotus.com/css/feedback.htm lets you provide feedback and suggestions for Lotus products. Lotus uses these suggestions to help plan and improve Lotus products.

To access information on the Web, you must use a Web browser, such as the Web Navigator. If you need information on connecting your Notes workstation to the Web, see your server administrator.
Chapter 2
Planning a Domino Deployment

Lotus Domino offers unprecedented power, access, and ease of use. With it, you can access data stored in legacy systems, build a Web site, create applications that process orders and monitor inventory, and share knowledge with team members, customers, and partners worldwide. Begin by examining your organizational needs, resources, and requirements. Building a picture of what you want to accomplish helps to ensure smooth implementation.

Sharing information and reengineering processes with Domino

Most organizations have two needs for an information technology like Domino: to share information in a controlled manner and to streamline and automate business processes.

Sharing information involves creating knowledge repositories, communicating, and collaborating. With Domino, users quickly find information and can easily share it with others. New information is placed in central databases and discussion forums. Teams and workgroups collaborate on projects and ideas, revising and updating plans in an organized, timely fashion.

Refining business processes involves using Domino to remove inefficiencies from business activities by automating them. Groups identify an activity critical to their work, assess the process by which they accomplish that activity, and use applications on Domino to move that process online and to remove unnecessary steps.

Assessing the needs of your organization

*Planning the Domino System* will help you understand how to apply a Domino solution to your business needs. Consider the following issues to avoid false starts, duplicated efforts, and inefficiencies, and help you maximize the return on your investment in Domino.
Assessing business needs

To assess your business needs, consider the following questions:

- What information does my organization need to share?
  Consider the flow of information both within and across workgroups and functional areas. Also examine the flow of information vertically within the company and with customers and suppliers.
- What information do I want to restrict access to?
- How do I want to make information available?
- What information exists that is useful but difficult to access?
  Consider data stored in paper records, in legacy systems, and knowledge that employees have that is not captured in another form.
- What processes are critical to the success of my organization?
- Which of these processes are “rate-limiting steps,” or activities that are the slowest point in a chain?
- Who participates in these processes at each step?
  It will be important to include these people in process reengineering and in the move to automating the process.
- What activities in my organization should be outsourced — performed by contractors, customers, or suppliers? Conversely, what activities undertaken by customers or suppliers should my organization assume responsibility for?

Assessing technical issues

Technical issues also affect your use of Domino and your ability to share information and reengineer business processes. Consider the following questions:

- What platforms does my organization use for its servers, clients, and mainframes? How standardized are these platforms across the organization?
- What platforms do my customers, suppliers, and partners use? How do we handle interoperability and intercommunication issues such as messaging and file sharing?
- What software does my organization use to meet its needs, such as word processing, messaging, spreadsheets, databases, and file archiving? How standardized are these programs across the organization?
- What software programs do my customers, suppliers, and partners use? How do we handle interoperability, file exchange, and communication?
• How does my organization communicate? Is information flow voice-based (telephony and voice mail), paper-based (memos, letters, faxes), or computer-based (e-mail, discussion forums, document sharing)? If we use a combination of these methods, what is the rationale for each method?

• How should my organization communicate?

• For computer-based communication, what is the backbone of this system (for example, LAN, WAN, Internet)? How easily do different groups connect electronically? What connections exist to the systems of customers, partners, and suppliers? How efficient and reliable are these connections? How does my organization handle remote and mobile communications?

• How does my organization guarantee 24x7 reliability for mission-critical software applications and hardware?

• How does my organization ensure secure communication? How do we ensure the security of a Web site and of activities that occur on it (for example, information exchange via forms, electronic commerce)?

• How does my organization use the Internet? If it has a Web site, how do we maintain that site and ensure that information is up to date? How do we communicate via Internet messaging?

Success depends on people

Ultimately, success depends on your employees. You must plan for the questions, needs, and capabilities of the users on your system. Consider the following questions:

• What is the level of knowledge in my organization regarding computer hardware and software? What is the comfort level of the average user with these tools?

• What is the level of knowledge and comfort with computer tools in the organizations of my customers, partners, and suppliers?

• How will I train users on the new software? How will I ensure that their questions are answered in the training phase and as they use the system?

• How will new users learn the system? How can I design the system to be more intuitive?

• How will I migrate users from existing tools to the new software solution? How will I answer their questions, overcome their skepticism, and invest them in using the new system?

• How can I convince my customers, partners, and suppliers to move to and use the new system?

Chapter 2: Planning a Domino Deployment 9
Planning for Domino at an organizational level

Once you decide to use Domino in your organization, you must plan carefully how to implement your Domino system. Domino is used primarily in three contexts: Internet, intranet, and extranet. Planning the Domino System has sections on each of these contexts. In any context, though, you must follow similar steps in planning.

Where to include Domino

Domino acts as a messaging backbone, a Web server, an applications server, and a knowledge repository, to name only a few of its capabilities. The more you include Domino in the key parts and processes of your business, the better your results.

Upgrade to Domino

Consider how to upgrade to Domino from your existing systems. How will you convert your directory information and e-mail files to Domino? If you use an Internet mail system, the conversion should be seamless, as Domino supports Internet standards such as MIME, POP3, IMAP, LDAP, HTTP, and HTML. If you use a LAN-based or mainframe system, plan the conversion process more carefully. Your organization will have to use both Domino and your existing system during a transitional coexistence period. Lotus offers a number of upgrade paths to Domino and has tools such as the Microsoft Mail conversion kit to assist you in this process. For details and more information, visit the Lotus web site at http://www.lotus.com/migration.

Domino can replace other systems and processes. You can automate business workflow in ways that obviate other systems, including paper-based routing. With the integrated Notes Web Navigator, you can move from other browsers to Domino. By using additional Domino solutions, such as Domino.Doc, you can replace systems like document management software. The advantage to this is having a single software, object store, and user interface to access and manage your organization’s information. Domino can act as the nexus for your company — the single resource for finding information, whether that information resides on the Web, in a relational database, or in an e-mail message.

You can also move information that exists in other forms — paper, magnetic tapes, voice mail, other databases — into databases hosted on Domino. Domino lets you store images, sounds, file attachments, HTML, Web pages, and many other types of information in these databases. Domino includes templates for databases that act as libraries for other types of information, such as Lotus SmartSuite documents and Microsoft Office documents.
Create a process for converting information stored in other formats into databases and for notifying users where the new information is located. Maintain these pointers to the new location of the information after the conversion process is finished; people who use the information sporadically will need guidance in the future. Consider establishing a database that tracks where information has moved; users can check this database if they cannot find data.

Help your users make the transition to Domino. Have them use databases, e-mail, calendar and scheduling, and other Domino features.

**Establish a time frame**

Establish a time frame for deploying Domino. Consider the time needed to plan the system; install, set up, and configure the software; train users; migrate from existing solutions to Domino; and resolve issues that appear during the rollout period. Set a date after which the older systems are no longer available. Decide whether to roll out Domino to your entire organization at once or gradually. The first option is faster and has a shorter coexistence with present systems and greater awareness from employees. The second option allows for a more gradual learning curve and may be less disruptive to employees and their work.

**Create a rollout team**

Create a Domino rollout team responsible for planning and implementing your deployment. Consider the skills and members needed on this team: hardware and software expertise, system administration, network analysts, representatives from each group where the software will be deployed, and management champions of the deployment, among others. This team should work with the organization to design a rollout plan, incorporate feedback from a pilot project or from the rollout into the plan, implement Domino, and support it. In addition, the group should promote Domino inside the organization, educate users about its capabilities and advantages, and identify and remove roadblocks that could interfere with deployment.

**Make Domino deployment a success**

Consider how to ensure the success of your rollout. Establish responsibility and accountability for the Domino deployment. Allocate sufficient resources — budget, people, IS personnel, and management support — to make the project a priority and increase its ability to succeed. Perform a cost-benefit analysis for Domino to guide you in how, where, and when to deploy and as justification for the project. Examine how Domino impacts or redesigns your business processes and reengineer them to take advantage of the capabilities Domino provides. Look at communication at all levels of the organization and between groups to see how Domino can break down barriers to sharing information. Review the security of your organization’s systems and consider how Domino impacts your security architecture.
Integrating Domino into your information systems infrastructure

Domino runs on a number of protocols and operating systems, improving your ability to integrate it into your existing system. Examine your capabilities in the following areas and determine whether you need to expand them to get the most from Domino:

- **Servers**
  Look at server disk space, RAM, CPU power and speed, and the number of connections your server operating system can handle. Consider server locations, access and access times, and workload.

- **Workstations**
  Look at whether your workstations can handle the Domino client. Consider workstation disk space, RAM, and CPU power and speed.

- **Operating systems**
  Look at your operating system(s) and whether you need to upgrade to newer versions. If you have multiple operating systems in one organization, you need Support analysts who are knowledgeable about Domino and its clients on each platform.

- **Protocols**
  Look at the network protocols in use in your organization and whether they are the most efficient option. If you have multiple protocols, you need multiple Domino named networks.

- **Network**
  Look at how much traffic your network can route at any one time and where slowdowns occur. Consider whether you need faster routers or more connections. Examine your security infrastructure, including firewalls, access points, challenge/response points, and modem access.

- **Connections**
  Look at how users connect to your network and systems and how you will support these connection types with Domino. Are these connections adequate? Should you upgrade? For example, your organization might want to move from a fractional T1 Internet connection to a full T1 to take advantage of the Internet features of Domino. Look at your network. Do you have adequate bandwidth and speed? What fault-tolerant capabilities are in place? Have you set up alternative routing paths if part of the network goes down?
• Fault tolerance
  Look at which areas and applications are mission-critical. Do you have 24x7 access to these resources? How do you guarantee access? Domino Advanced Services can be used to provide failover and fault-tolerance support for Domino servers.

• Remote and mobile use
  Look at which users need to access Domino when not connected to your network. Do you have adequate modems and remote servers available? Are your modems fast enough to handle replication via phone lines? How will remote and mobile users obtain support?

• Internet access
  Look at how you access the Internet. What type of connection do you need? What kind of security will you set up? Where should the connection point to the Internet be located?

Create a map of your organization’s information systems infrastructure. Include server locations, network connections, routers, firewalls, proxies, protocols, external access points, Internet access points, and data stores. This site map helps you plan where to locate Domino servers and decide on a Domino server topology. Use the map to consider how to route mail, set up replication between servers, and create remote connections for users.

As you examine your present infrastructure, think about your future needs. Will the infrastructure still work? How will you expand your capacity? By factoring growth and change into your deployment plan, you ensure a smooth transition in the future.

For more information on integrating Domino into your network, see Configuring the Domino Network.

Planning for future growth

The scalability, or capacity for expansion, of your system depends on how well you plan for growth. For example, if you initially deploy your system with just a few servers and decide on a peer-to-peer topology for server communication, you might need to rethink your topology as you add servers. Additionally, you might need to upgrade your network and computing infrastructure as you add servers and users. If you find yourself in this situation, consider deploying a Domino server cluster as a way to achieve scalability with the added advantages of server and database availability.

For information about Domino server clusters, see Chapter 9 in Getting Started with Domino.
When you plan for server capacity, use the following table as a guide for how many active sessions a server supports with a given protocol. Because a Domino server reuses sessions it finds are inactive, the number of users connected to a server at any given time can exceed the numbers in the table; these are the recommendations for active sessions.

Server capacity depends on how many processors it has, their speed, and how much RAM the server has. For information about optimal server configurations, consult your hardware vendor and the NotesBench statistics for the server.

<table>
<thead>
<tr>
<th>OS/Protocol</th>
<th>TCP/IP</th>
<th>IPX/SPX</th>
<th>NetBIOS</th>
<th>VINES</th>
<th>AppleTalk</th>
<th>X_PC</th>
<th>X.25</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS/2</td>
<td>Server capacity</td>
<td>Server capacity</td>
<td>100</td>
<td>50. Greater than 50 with Banyan VINES patch 5.54(20)</td>
<td>50</td>
<td>64 ports</td>
<td>64</td>
</tr>
<tr>
<td>Windows 95</td>
<td>Server capacity</td>
<td>Server capacity</td>
<td>not applicable</td>
<td>not applicable</td>
<td>not applicable</td>
<td>64 ports</td>
<td>not applicable</td>
</tr>
<tr>
<td>Windows NT (Intel, Digital Alpha)</td>
<td>Server capacity</td>
<td>Server capacity</td>
<td>252</td>
<td>Server capacity, not applicable on Digital Alpha</td>
<td>255</td>
<td>64 ports</td>
<td>64</td>
</tr>
<tr>
<td>AIX®</td>
<td>Server capacity</td>
<td>Server capacity</td>
<td>not applicable</td>
<td>not applicable</td>
<td>not applicable</td>
<td>64 ports</td>
<td>not applicable</td>
</tr>
<tr>
<td>Solaris (SPARC)</td>
<td>Server capacity</td>
<td>Server capacity</td>
<td>not applicable</td>
<td>not applicable</td>
<td>not applicable</td>
<td>64 ports</td>
<td>not applicable</td>
</tr>
<tr>
<td>Solaris Intel Edition</td>
<td>Server capacity</td>
<td>Server capacity</td>
<td>not applicable</td>
<td>not applicable</td>
<td>not applicable</td>
<td>64 ports</td>
<td>not applicable</td>
</tr>
<tr>
<td>HP-UX</td>
<td>Server capacity</td>
<td>Server capacity</td>
<td>not applicable</td>
<td>not applicable</td>
<td>not applicable</td>
<td>64 ports</td>
<td>not applicable</td>
</tr>
<tr>
<td>NLM</td>
<td>Server capacity</td>
<td>Server capacity</td>
<td>not applicable</td>
<td>not applicable</td>
<td>120</td>
<td>64 ports</td>
<td>not applicable</td>
</tr>
</tbody>
</table>

**Using Domino Server.Planner for capacity planning**

One of the most challenging areas for planning is determining the number, speed, and size of servers on which to run Domino. This decision depends on the needs of your organization, its existing information systems infrastructure, and the hardware capabilities of manufacturers. Evaluating these parameters was difficult in the past. Lotus has developed a tool that greatly enhances your ability to plan and eases the process of evaluating
hardware options. You can add the latest specifications from hardware manufacturers to your testing by downloading specs from the Internet. The specifications are signed Notes databases based on audited vendor tests of their hardware.

Domino Server.Planner considers operating system parameters; Domino version; RAM; the number, size and speed of CPUs; disk I/O; the number and speed of communication ports; the number and speed of network adapters; and cost. The application tests a variety of Domino tasks and workload levels against different server configurations. You can set the minimum acceptable performance levels for connection time, variability, and query tolerance. The application considers performance based on replication and mail routing.

Server.Planner offers evaluations based on average response time and the percentage of queries that fall into various response time intervals. Using Lotus Components, you can graph results and share them with others via e-mail. Server.Planner runs on any Notes 4.5 or later client. You can use Server.Planner with the NotesBench™ reports provided by hardware vendors to determine what hardware to purchase to optimize your Domino system.

With Server.Planner and an estimate of your organization’s needs, you can preview how various server configurations will work. By calculating the response times and reliability you need from each server and your total need for server capacity, you can estimate the number, type, and configuration of servers you need to have.

To download server planner, visit the Lotus Notes.Net site at http://www.notes.net/down.nsf/welcome.nsf and select to download Server.Planner.

About using NotesBench statistics with Domino Server.Planner

Developed by Lotus, NotesBench is a benchmarking tool for vendors to demonstrate how many users and transactions a particular hardware configuration can support. NotesBench measures both single CPU and SMP (Symmetric MultiProcessing) servers for the number of documents replicated per unit time, number of messages processed per unit time, and number of total active concurrent users supported while using messaging and groupware functions. NotesBench models the processing loads of an enterprise organization environment. NotesBench and Domino Server.Planner results let you compare the offerings of various vendors and plan your hardware acquisitions. For more information on NotesBench, see the Lotus web site at http://www.lotus.com/ntsdoc96/1f6.htm.
Planning for Domino on the Internet

Domino establishes an Internet presence for your organization and ties the Internet to your business. With Domino, you can set up interactive Web sites; send and receive Internet mail; provide access to directory information via LDAP; and give controlled access to pieces of your intranet. Consider the following issues in planning to deploy Domino to the Internet:

- Internet connection
  Look at how your organization connects to the Internet. If you access the Internet via phone lines, you may need a higher-bandwidth connection. How will the Domino server that hosts your Web site connect to the Internet? How will you guarantee access? What resources does your Internet Service Provider (ISP) offer?

- Security
  Look at how you control access from the Internet to your Web site, your servers, and your intranet. Is your security adequate? See Chapter 11.

- Web site content
  Look at the content you want to place on your Web site. Who will create it? Who will maintain it and keep it up to date? What content should not be placed on your site? Will you make any intranet information available?

- Web site roles
  Look at the division of responsibilities for your Web site. Who controls security, content creation, content approval, site additions and deletions, and site architecture, among other issues? Domino lets you distribute responsibilities via access levels, roles, and permissions in each Web database.

- Web site structure
  Look at how your Web site will be laid out. What is the pattern of links and pages? How many levels will the site comprise? What sections will the site be divided into? How will users reach them?

- Web site appearance
  Look at how your Web site should appear to users. Consider standardizing the site’s appearance to give it a distinctive “look.” Create a set of guidelines to guide page creation.
• Web site navigation
  Look at how users will reach pages and how your site will guide them to the content they are looking for. How will the site provide context for a user who reaches a page from a Web search engine? How will you guide users back to their starting point? Can you provide a constant visual hierarchy or map?

• Web site search
  Look at how you will let users search the contents of your Web site for terms, phrases, and items.

• Internet mail access
  Look at how you will set up Internet mail access. Domino includes the Lotus Domino SMTP/MIME MTA (Message Transfer Agent) to route Internet mail and make it available to Notes clients.

For more information, see Chapter 5.

Planning a Domino intranet

A Domino intranet networks computers in your organization so your employees can share information and resources. Based on the Domino server, the intranet can be accessed via browsers, news readers, mail programs, and the Notes client. Protect your intranet from unauthorized access with a firewall, proxy server, and other security.

For more information, see Chapter 6.

Planning for Domino clients

Domino supports a wide variety of clients, from Web browsers to news readers to Internet mail programs to the Notes client. To decide which client or client mix to purchase, consider your needs and the costs of the clients. Single-purpose clients, like news readers or Internet mail clients, are simple, cheap, and easy to learn. However, they are suitable for a limited number of tasks and must be combined with other clients to expand their capabilities. For example, browsers can interact with Domino databases and read mail, but to send mail they require adding an Internet mail (POP3 or IMAP) program. To work when not connected to the Internet, browsers need a program like Lotus Weblicator™.

The Notes client integrates e-mail, database interaction, Web access, calendar and scheduling features, personal information management, and offline capabilities in one package. Users perform all of their tasks from one place.
With the new capabilities of Notes, users can integrate other software like office suites into their Notes tasks. Notes Active Document support allows users to create documents like spreadsheets or presentations and then share them with others using Notes workflow and security capabilities.

For more information, see Chapter 9.

Planning for rolling out Domino in a workgroup

Plan a training program that includes demonstrations, hands-on practice, documentation, and resources for questions and problems. Many companies use both a formal and informal training program.

- The formal program uses professional trainers, consultants, or employees who are expert in using Domino. It is short-term and is often presented as a seminar or class. The program combines instructor presentations with laboratory exercises and reading assignments to give users a basic grounding in the software.

- The informal program makes resources available to users as they interact with the software and encounter questions and problems. These resources often include a central help desk able to answer questions on software and hardware issues as well as local experts in each group who are knowledgeable about the system.

Consider using computer-based training (CBT) or Web-based training for users. Set up a database for user questions; other users and support analysts can answer the questions. This reduces calls to the help desk and provides a knowledge resource for users. In addition, you may want to have occasional presentations on aspects of the software.

Upgrading to the new software

Plan how to upgrade users, data, and functions from existing systems to the new software. For example, if your organization has an application to process human resources data from employees, you must consider how information is presently processed, decide how to encourage employees to use the new system, and plan how to move data from the old human resources system into the application.

If human resource functions are presently handled by phone, you make employees aware of the new Domino system via announcements, memos, e-mail, and a message on the phone system, and then encourage them to use the new software application. Gradually transition employees to the new system by offering incentives for using the application and by phasing out access to the old system.

18 Planning the Domino System
Depending on how older data is stored, you may want to migrate it to the application or enable the application to access the older data. The Domino solution for enterprise data, Domino.Connect, accesses information stored in relational databases, enterprise information systems, and transaction processing applications.

**Using Domino in daily activities**

Plan to get users to integrate Domino into their daily activities. Using mail, discussion databases, knowledge databases, and specialized applications such as the human resources example described above helps users become familiar with the Domino system and enthusiastic about using it. By moving from other applications, such as different messaging, scheduling, and database programs, to Domino, you present users with a consistent, easy to use interface for all of their tasks. This increases productivity and decreases the learning involved for new employees.

Consider standardizing how Domino is presented to users. You can do this for browser access by creating a Web page that contains links to all the databases and resources the team needs. With the Notes client, use a portfolio or multiple portfolios to group applications and databases a team needs. Users can work in one place — the portfolio — and have access to all the necessary information.

Make sure users have consistent access to Domino by providing enough network bandwidth and server power. If the workgroup is one that needs highly reliable access, put its databases and mail files on clustered servers using Domino Advanced Services.

**Deploying the software**

Plan to deploy the software by setting up Domino servers and clients. Have users begin communicating via e-mail, collaborating in databases, and using the Internet with Domino. Encourage them to share their experiences and feedback about Domino and about the rollout procedure so that you can adapt your deployment plan to avoid problems and leverage strengths.

**Planning a pilot project for Domino**

In larger companies and especially in enterprise organizations, consider a pilot project for deploying Domino. A pilot project is a limited-scale deployment to one group or business unit that serves as a model for the rest of the organization. Use a pilot project to test your assumptions, plans, and expectations regarding Domino, your migration to Domino, and your deployment. Choose a group for the pilot project that is comfortable with software and with change and learning. Make sure the group is invested in the project by discussing its benefits for them and encouraging them to share.
their concerns. Invest in additional resources to support their transition to Domino and to capture their experiences and feedback for use in planning your organizational deployment.

Think of a pilot project as a beta release of your deployment plan — it allows you to test your plan under actual business conditions and to work out any issues before moving to a company-wide rollout.

Pilot projects may not be necessary for smaller companies, who have fewer issues regarding scalability, and for companies who need to deploy Domino quickly. Even without a pilot project, capture feedback and experiences to evaluate and modify your deployment strategy as you move through it.

---

**Supporting the Domino deployment**

Domino is a powerful application and users will have questions about using the software. Plan several levels of support for end users, application designers, and administrators. In addition, consider users who may need additional support, such as remote and mobile users. Establish two resources for initial questions: “local experts,” or users within a group who have advanced knowledge of Domino, and a central help desk. Each group should have one or more users who have advanced knowledge of and experience with Domino who can answer common questions and troubleshoot simple problems. They should be comfortable with software and hardware, willing to learn and act as a resource for others, and skilled at answering questions and helping users overcome nervousness and frustration. Local experts are an excellent informal resource for questions and can reduce the workload for your help desk. Consider providing additional training for local experts, including training them in advance of your deployment.

The central help desk handles all software and hardware problems. Users contact the help desk at one phone number, giving them a single resource for all questions, which reduces confusion. Calls are routed to the appropriate support person for the problem. Many companies use a specific team for Domino/Notes support or for particular areas of Domino/Notes support, such as administration, that involve problems too complex or challenging for the typical IS analyst.

In addition, develop a policy for contacting Lotus Customer Support. Encourage users to consult your internal support desk first. Create guidelines for when problems should be elevated to the Lotus Customer Support level. You may want to have your IS staff triage all calls and help requests, attempting to deal with these internally before contacting Lotus.
The need for support will be high as users learn how to use Domino and should decrease after this acclimation period. Consider this high-traffic period in your plan for deploying Domino. You may want to have different parts of your organization transition to Notes and Domino at scheduled intervals — for example, your IS department could move and learn the software first, followed by Sales one week later, followed by Finance one week after that, and so on. As an alternative, you may wish to increase the size of your IS department temporarily to meet the additional demands of a rollout.

Many companies use databases on Domino to track calls to IS and the status of these calls as analysts handle them. Using a database increases familiarity with the software and brings the power of Domino to bear on the complex tasks of tracking, routing, and archiving calls along with the challenge of locating technical information and solutions. In addition, create a mail-in database where users fill out forms for less urgent problems and requests, such as certification requests and hierarchical name changes. The database can automatically route requests to the proper IS analyst, increasing the efficiency of the system.

Consider creating a KnowledgeBase or FAQ (Frequently Asked Questions) database with answers to common questions and problems as well as procedures for contacting support. Users can access this database before calling support, decreasing the workload for your IS analysts.

Remember to plan for support as you increase the size or complexity of your Domino system. If you add new employees to your organization who will use Domino or if you increase greatly the number of databases and applications on your system, consider the need to support problems with and questions about these changes.

---

**Planning for Domino administration**

Domino administration involves maintenance and tasks with the Domino servers, Domino named networks, domains, and databases. For complete information on administration, see *Getting Started with Domino, Extending the Domino System*, and *Maintaining the Domino System* (HELPADMN.NSF). This section is an overview of some of the activities and processes you should consider in planning your deployment.

Consider creating a mail-in database for common requests, such as server access, certification, and name changes. With the workflow capabilities of Domino, you can set up the database to route requests to the correct resource automatically. This reduces the need to sort and resend requests.
About administration tasks
Plan for the following administration tasks as you consider personnel for your rollout:

- Registering new users
  You must create Person documents and mail files for new users and enter information about the users in the Public Address Book. New Notes users require Notes IDs.

- Registering new servers
  You must create server IDs and set up connections, replication, and mail routing for new servers.

- Maintaining the Public Address Book
  You must update the documents in the Public Address Book and remove obsolete documents.

- Scheduling, managing, and troubleshooting replication
  You must set up replication between servers to keep databases current. The complexity of this task varies with your network topology.

- Scheduling, managing, and troubleshooting mail routing
  You must set up mail routing between servers to ensure timely communication. Mail routing is a task similar to replication, but involves routing between different Domino named networks and domains. The complexity of this task varies with the number of domains and Domino named networks in your organization. Lotus recommends you use only one domain for your organization, unless your organization is very large. Using more than one domain requires one of the following:
    - Using a Master Address Book
    - Using cascading Address books
    - Appending domain names to e-mail addresses

  In addition, mail routing requires monitoring dead mail and tracing the path of mail that fails to be delivered.

- Setting up and maintaining calendars and schedules
  You must set up the Schedule Manager, Calendar Connector, and Resource Reservations database if you want to use the calendar and scheduling features in Domino.

- Setting up, updating, and ensuring security
  You must create and maintain a secure Domino environment. This involves software, hardware, and networking considerations. You must manage ID files, ACLs, server access lists, Deny lists, encryption, and electronic signatures.
• Setting up and maintaining remote access
  You must make sure remote and mobile users have access.
• Monitoring system usage and problems
  You must track statistics in the log file to determine the level of system use and system problems. This alerts you to a need for more servers, more hardware, or better distribution of system tasks.
• Maintaining databases
  You must update and maintain Domino databases, including updating designs and full text indexes, and resolve database issues.
• Ensuring system access
  You must make sure critical hardware and software applications are available to users. If necessary, use the clustering feature of Domino Advanced Services for failover.
• Troubleshooting
  You must solve problems as they arise, track their causes and resolution, and work to prevent their recurrence.

---

**Planning for security**

One of the most critical security precautions your organization can take is to create and enforce policies on security procedures. Make this a key focus of your security planning.

Plan for security at the following levels:

• Internet security
  Internet security looks at the connection between your network, your Web site, and the Internet.
• Network security
  Network security looks at external access to your network and controlling internal actions to data, software, and hardware.
• Hierarchical naming for servers and users
  Hierarchical naming looks at controlling access to Domino servers and clients, restricting access for users, and preventing unauthorized individuals from impersonating legitimate users.
• Server security
  Server security looks at protecting the data on your Domino servers.
Notes and client security
Notes and client security looks at preventing unauthorized actions on your workstation and controlling access to local data and Domino servers.

Application security
Application security looks at controlling access to database applications and making sure data can only be viewed by authorized individuals.

Document security
Document security looks at controlling who can create and access documents in a database.

Field security
Field security looks at controlling access to fields on a document containing sensitive or confidential data.

Mail security
Mail security looks at making sure messages cannot be viewed by anyone other than the intended recipients and at validating a sender’s identity.

For information, see Chapter 11.

Naming conventions and requirements
As you plan your deployment, consider the following naming conventions and guidelines:

- Domain names should be a single word or string (maximum of 31 characters). Do not use periods (.) in a domain name as they are reserved characters.

- Organization name is the name of the Certifier ID and is appended to all user and server names. Typically, the organization name is the same as the domain name, and there is only one organization per domain. The name can have a maximum of 64 characters.

- Domino network names denote groups of servers that are physically connected and use the same network protocol. The name can have a maximum of 31 characters. It is helpful to use an identifier such as the location of the Domino named network, the LAN type, or the protocol. For example, Boston_Novell or Singapore_Ethernet are descriptive names.
Domino server names are unique names that identify servers in a domain. Server names can consist of one or more words (a maximum of 79 characters) and can consist of any characters except: parentheses, at (@), slash and backslash (/ and \), equal (=), and plus (+). Using spaces is not recommended. If you use spaces, you must enter that server name in quotes (""") when entering a command at the server console.

**Guidelines for naming a Domino server**

- Choose a name you want to keep. Changing a server name involves recertifying the server ID and changing the name in the Server document, Group documents, database access control lists (ACLs), and Connection documents.
- Choose a name without a space. When you use server console commands, you must use quotation marks around a server name containing spaces.
- Consider that replication and mail routing tasks are usually performed based on numerical rather than alphabetical order. For example, when the router faces multiple choices for a routing path, Domino routes mail to the server 01Finance, then the server Accounting, then the server Research.
- In certain networks the first several characters in a server name must be unique for the network to identify the server. With NetBIOS, the first 15 characters must be unique; with AppleTalk, the first 32 must be unique; and with SPX, the first 47 must be unique.
Chapter 3
Using Domino as a Business Solution

Domino can help your business integrate information, present it to users and to customers, and automate business processes. The explosive growth of the Internet and the advent of sophisticated information technologies makes the challenge of managing information more difficult. Use Domino to meet this challenge.

The advantage of Domino is its ability to act as the central access and distribution point for your organization’s data. The following sections describe how Domino and products based on Domino can meet challenges your business faces.

Creating an intranet based on Domino

A Domino intranet makes information readily available to users. It manages the flow of information and tasks, increasing productivity and reducing overhead. Storing knowledge in databases archives it and makes it accessible. It can integrate the Internet into office tasks. Applications on Domino can automate ordering and order processing, call tracking, human resources functions, approval cycles, and many other business functions.

With the Domino server, Notes clients, and Domino.Broadcast, you can create a fully-featured intranet.

Domino and Notes:

- Provide knowledge sharing using rich text, multimedia, e-mail, discussion and knowledge-base databases, native Internet access, and integrated calendar, scheduling, and task features.
- Create applications that automatically route and process information.
- Use replication to synchronize multiple changes to a document and to work while disconnected from the network — users on the road, in a hotel, at home, or on a plane can still be productive.
- Use Notes clients to integrate office suites like Lotus SmartSuite and Microsoft Office — use Lotus Word Pro® or Microsoft Word as your e-mail editor, and use the Microsoft Internet Explorer component with the Notes Web Navigator to access Internet Explorer through the familiar Notes interface.
• Use Lotus Components, enhanced ActiveX controls, to insert charts, graphs, drawings, and spreadsheets directly into a Notes document.
• Let users work in one environment to accomplish their tasks.

Domino.Broadcast then lets you “push” information in real time to users’ desktops. Send corporate reminders, updates, and questions to users. By clicking a headline or announcement, users access further information from a database. For example, you send a reminder about updating benefits information; when employees click the reminder, Domino opens a Human Resources database and presents them with a form to fill out and update their benefits.

For information on deploying a Domino intranet, see Chapter 6.


Accessing enterprise and legacy data from Domino

Most companies store data in large back-office systems, such as SAP R/3; relational databases, such as IBM DB2®, Informix, or Oracle products; or in transaction processing applications, such as CICS® or Tuxedo. For the user, accessing and manipulating this data can be difficult and requires learning a specialized interface. Moving enterprise data into a client-server three-tier architecture is a challenge many companies face.

Lotus Domino.Connect makes a connection between your workstation and the backend system. You can search for data, modify it, manipulate it, and store it again, all from the familiar interface of your Lotus Notes or Web browser client. Applications employing Domino.Connect access and modify enterprise data seamlessly via standards-based plug-ins, using HTTP, ODBC, and SQL among others. These applications incorporate secure access, messaging, calendar and scheduling features, and the power of replication.

Domino.Connect integrates seamlessly with the following resources:

• Relational Databases

  Relational databases allow companies to manage, search, and manipulate large data volumes with high performance. Domino.Connect lets you access and update data in non-Notes DBMS systems. Domino.Connect includes Lotus NotesPump 2.0, a data distribution server offering high-volume data exchange and synchronization with Access, IBM DB2, Informix, Notes, Oracle, Sybase and ODBC-compliant databases. LotusScript® Data Object (LS:DO) provides real-time data access from Domino via ODBC access to external databases. The Oracle plug-in provides real-time data access via Oracle native protocols.
Enterprise Application Systems
Domino.Connect links to enterprise application systems such as SAP R/3 via a LotusScript BASIC plug-in based on both Remote Function Calls and the SAP R/3 Business API. This plug-in allows bi-directional data exchange and is capable of both synchronous and asynchronous activity. The Plug-in module encapsulates the SAP C-API into LotusScript classes, giving LotusScript programmers an object-oriented framework for calling R/3 function modules through RFC to exchange data bidirectionally with SAP R/3. You can perform this exchange synchronously or asynchronously.
Lotus programs can call any R/3 ABAP/4 program registered as a remotely callable function, including the R/3 Business Application Programming Interfaces (BAPIs).

Transaction Systems
Transaction systems manage the information necessary for purchasing, ordering, and billing in large organizations such as credit card issuers. Domino.Connect applications access more than 18 different platforms and systems via the MQSeries link plug-in from IBM, including AS/400®, CICS, Digital, IMS™, ISAM, HP-UX, Tandem, Tuxedo, and VSAM systems.
Domino.Connect includes a Human Resources self-service application allowing users on Notes clients and Web clients to perform standard human resource functions such as hiring, promotions, terminations, and transfers using ODBC. You can modify Domino.Connect to use SAP R/3 or other products in this application.
Domino.Connect also includes a self-service corporate purchasing application that provides a Notes-based UI with product catalogs, an order form, and integration with an ODBC database containing product catalog information and order information. You can modify Domino.Connect to use SAP R/3 or other products in this application.

Creating an electronic store on the Internet with Domino
Online commerce helps you sell products with low overhead and easy, 24 hour access for consumers. Use Domino.Merchant to create a secure, attractive, and profitable online store front that's easy to use and to maintain. Domino.Merchant is built on the Domino.Action interface and databases, allowing you to set up the site with a GUI and retrieve information from databases.
You create a catalog of products and publish it on the Web. Domino.Merchant maintains the catalog, registers site visitors, accepts and processes orders, and handles online payments using credit cards, purchase order, or CyberCash wallet. Security is assured through SSL and CyberCash. Your online store can interface with banks via CyberCash; for security, Domino.Merchant uses a 768-bit RSA algorithm for security. Domino.Merchant can calculate taxes and shipping costs using tables you define. The software generates orders and delivery information and routes orders to external systems.

Visitors to your Domino.Merchant site use a “virtual shopping basket,” allowing them to add and remove items, review and modify the contents of the basket, and even leave the site and return — the basket is stored in the system. Repeat customers can access their account information and order history. You can allow anonymous shoppers or require visitors to register upon entering the site.

---

**Managing documents in an organization**

Many organizations need to control access and revisions to documents such as specifications, legal drafts, or project plans. With Domino.Doc, you can organize documents, control access to them, and store and retrieve them efficiently. All Domino.Doc features are accessible via a Web browser. You can access documents from a Notes or Web browser client or from ODMA applications.

Domino.Doc stores documents in virtual file cabinets and supports multiple media, including text, graphics, audio, video, and 3D. You set rules on file cabinet access, ownership, and storage. Using the Open Document Management API (ODMA), Domino.Doc allows you to save directly from applications such as Lotus SmartSuite and Microsoft Office to a file cabinet. Users can define document types with global attributes and assign a document to an existing document type.

Domino.Doc security is based on the database access control list (ACL) model and incorporates version control, check-in/check-out features, and audit trails.

Domino.Doc efficiently handles storage and document use. You can replicate file cabinets and control check-in/check-out on a “master-slave” basis, delivering a checked-out document to the user from the nearest file cabinet to minimize network traffic. The Domino.Doc Hierarchical Storage Manager lets administrators shift lower-priority, archived, or older documents to different media such as jukeboxes.
Integrating Domino and Notes with other applications

Domino and Notes integrate with other applications to allow you to accomplish tasks in one place. The Lotus Components are ActiveX controls that integrate with Notes documents to create spreadsheets, drawings, graphics, charts, and product schedules. Anyone who can read or open the document can view the Component, whether they have Lotus Components installed or not. Application developers can use Components in Notes applications; Components have predefined methods and properties and can be modified with LotusScript. Components are available only on Microsoft Windows 95 and Microsoft Windows NT platforms.

The Notes client integrates office suites such as Lotus SmartSuite and Microsoft Office. Use either Lotus Word Pro or Microsoft Word as your e-mail editor. Employees can work with a familiar word processing program while using the document security and routing features of Notes.

For the Internet, the Notes Web Navigator can use the Microsoft Internet Explorer component to retrieve data. This feature presents data in the familiar Notes interface and includes support for frames and animated .GIF files.

Ensuring access to Domino

Many organizations need reliable, 24x7 access to servers, messaging, and databases. Use Domino Advanced Services to achieve this level of performance and reliability. Domino Advanced Services lets you cluster multiple servers with failover capabilities. If one server in the cluster goes down, users trying to access that server are immediately transferred to another clustered server. Databases on the clustered servers replicate in real time, providing failproof data access. Processing and workload can be split among the servers upon reaching administrator-defined thresholds.

Domino Advanced Services allows you to host multiple servers on one computer. These partitioned servers function and appear to users as physically separate computers. Partitioned servers let you fine-tune your resources; for example, you can host multiple Web sites or set up several mail servers on one powerful computer.
Chapter 4
Deploying Applications

The Domino server can host database applications that store knowledge, automate business processes, browse the Web, and interact with enterprise data. Applications can be accessed by Notes and Web browser clients.

Deploying applications on Domino

The Domino server provides the unmatched ability to create and host rich, interactive applications built on databases, HTML Web pages and forms, Java applets, and a wealth of programming tools. Applications help your business reduce overhead, increase workflow efficiency and speed, cut costs, and integrate information. For more information on creating applications, see the Application Developer’s Guide.

You can place an application on an intranet, extranet, or the Internet with equal ease. Domino converts databases into HTML, removing the need to code HTML. Instead of writing CGI or Perl scripts, use forms with automated processing. Use the Domino security architecture to control who can perform which actions in a database, and who has access to information.

Using templates

You can create out-of-the-box applications by using templates, standardized applications that you customize to provide desired functionality. Domino includes application templates for discussion databases, document libraries, Notes Web Navigators, approval cycles, billing, database catalogs, database analysis, Internet search sites, project management, resource reservation databases, and statistics collections.

Programming support

Database applications, with their embedded LotusScript programming language, @formulas, and @commands, have enormous power and flexibility for programmers. Domino supports:

- Lotus C API (Application Programming Interface)
  Provides a set of subroutines and data structures to create programs that access databases.
• Lotus C++ API
  Provides a set of C++ classes that allow programs to access databases.

• Lotus HiTest C API
  Offers a C interface that is faster and requires less code than the C API.

• LotusScript Extensions Toolkit
  Expands LotusScript functionality and lets programmers create extensions (custom modules) that load separately and implement one or more LotusScript classes.

• LotusScript
  Provides a BASIC scripting language with language extensions allowing you to do object-oriented application development. LotusScript interacts with Domino through defined object classes.

• NotesSQL™
  Provides an ODBC driver enabling ODBC-compliant DBMSs and data query tools to access Domino information.

• Lotus NotesPump™
  Lets you create scheduled, event-driven, or on request bi-directional data exchange between data systems including IBM DB2, Notes, Oracle, Sybase, and ODBC databases.

• Lotus Components
  Provide ActiveX controls you can use to create and enhance applications.

• Lotus Notes Global Designer
  Lets you create databases in multiple languages and streamlines maintaining them.

• LotusScript Data Object
  Lets you read and write data from Domino to external ODBC data sources using LotusScript.

• Lotus BeanMachine for Java
  Lets you create and publish Java applets and JavaBean components in a visual authoring environment.

• Java agents on the Domino server

For more information on Domino application development tools, see the RoadMap to Lotus Notes Application Developer’s Documentation and visit the Lotus Developer Central Web site at http://www2.lotus.com/developers/tools.nsf/. 

34 Planning the Domino System
Deploying database applications to the Internet

Use the power of Domino to extend database applications to the Internet. By placing an application on a Domino server and allowing browser access to the server and the database, you enable Internet use of the application. For example, you could place an order-tracking database on the Internet to allow customers to check the status of an order.

Internet database applications have additional security and application development considerations. When you plan to place an application on an Internet-accessible Domino server, consider the following security issues:

- **Anonymous browser access**
  Set the access level that Web browser clients can have to an application without authenticating their identity. If you do not add an Anonymous entry to the application ACL, all Web browser clients have the Default level of access.

- **Maximum Internet name & password access**
  Set the maximum level of access any Web browser client can have to an application.

- **Default access**
  Set the Default level of access to the database for all Notes clients and all Web browser clients. If you add an Anonymous entry in the ACL, this sets the level of access for all Web browser clients that do not authenticate with the Domino server. Web browser clients that do authenticate are granted the Default level of access unless they are individually included in the ACL.

- **Encrypted fields**
  Web browser clients can view encrypted fields. Do not use encrypted fields to protect data in an application to which Web browser clients will have access.

To optimize your application for Web access and viewing, see the *Application Developer's Guide*. 
Designing databases for better performance

Use these design guidelines to improve significantly the performance of a database application.

**Formula design and usage**
- Keep selection formulas, view formulas, and scheduled agents as simple as possible to reduce computation time.
- When using the @ functions @DBLOOKUP and @DBCOLUMN, use the CACHE option if possible. Store the values returned by these functions in a temporary variable or a hidden field if you plan to use them again.
- Make sure functions that are time-consuming to calculate, such as lookup functions, are calculated only as necessary. Wrap these functions in a conditional clause so they are evaluated only when a condition is met.

**View design**
- Maintaining fewer views improves database performance. Use dynamic view sort features to reduce the number of views in a database.
- Allow and encourage document category levels to avoid categories with a large number of documents. This speeds display of categories.
- Views display fastest when categories are either all collapsed or all expanded; choose one of these as a default rather than mixing.
- Avoid categorizing documents in multiple categories. This slows down view navigation and document retrieval.
- Use unread marks at the document level; avoid the Compute and Display at All Levels of View feature. This speeds view and category display.
- Be aware that selection formulas containing time-relative functions such as @NOW or @TODAY are rebuilt each time a view opens.

**Indexing**
- Refreshing a database index takes time. Refresh as infrequently as possible without jeopardizing the integrity of the application.
- Keep key and category values short. Long key values can slow down indexing.
- For databases you use infrequently, save disk space by discarding the index after each use. The performance trade-off is that it takes time to rebuild the index when you next access the database.
Full text indexing

- When databases on a server require frequent full text indexing, performance may suffer during heavy usage. Try changing to a lower priority indexing time on databases, for example, from immediate to hourly, or from hourly to daily. You can also change scheduled indexing to lower usage times.
- When full text indexing a database, use the Whole Word and Case-Insensitive features to use the fewest resources.
- If you plan to full text index a database, consider that protecting documents in a view with read or edit lists or roles slows down the retrieval process.

Database maintenance

- Check databases for corrupted documents. Compact the databases after many deletions and modifications. Database size increases with additions and does not decrease until you compact it. Databases below 90% of capacity may see performance improvements from compacting, but be aware of the time it takes to compact a large database.
- When using the option “Store form in document,” use a mail-in agent to remove the $Body field(s) in a document as it arrives in its destination database. Keep one copy of the form in the destination database to view the documents. This saves disk space and improves the performance of the database.

For more information on maintaining databases, see Chapter 5 in *Maintaining the Domino System*.

Distributing applications on Domino

When you create a database application, place it on one or more Domino servers to make it accessible to users. Before creating a database replica, consider the following:

If a database is heavily used or mission-critical, consider using Domino Advanced Services to cluster servers hosting that database to ensure access. If one replica goes down, users fail over to another.

When to create a replica

- Has the new replica been approved for use in your organization? Establish an approval process for the use of organization resources for databases and database replicas.
- Who will access the application, how frequently will they do so, and from where will they connect?
Can users access a database in the most cost-effective way? If the user can access an existing version of the database across a LAN, you may not need to create replicas. If a group of users accesses the database across a WAN, it is probably more cost-effective and performance-effective to create a replica of the database on a local server for that group.

Is a heavily used database overloading a server? To improve performance, create a replica of the database on another server. Consider clustering the server to balance workloads.

Is the database easily accessible in larger organizations or from the Internet? Consider where to place replicas of the database to ensure accessibility and balance server workloads.

Do users need real-time information? Because replica copies of a database are almost always out of sync with the latest information, users who need access to real-time data should access a single original database. If this is not possible, consider clustering several Domino servers. Clusters provide real-time information for both original databases and replicas.

Are users putting heavy demands on only certain parts of a database? Use selective replication to replicate particular views or documents.

For information on using selective replication, see Chapter 5 in *Getting Started with Domino*. For information about Domino server clusters, see Chapter 9 in *Extending the Domino System*. 
Chapter 5
Deploying Domino to the Internet

Domino is the solution to your business’s Internet needs. With Domino, you can communicate with other organizations using standards-based e-mail, perform and allow directory lookups via the Lightweight Directory Access Protocol (LDAP), create an interactive Web site quickly and without HTML or scripting languages, and incorporate tools like Java into your business. The Domino Mail Server is a complete mail solution for your organization, managing standards-based Internet mail while providing directory information to Internet users through LDAP. Use Domino Mail server as the foundation of your Internet messaging system.

About using Domino on the Internet

The Domino interactive Web applications server is the world’s leading server for messaging, Internet applications, and groupware. Domino provides the following Internet features:

- Notes database applications
  Domino uses powerful Notes database applications to bring fully interactive functionality to the Web: track customer leads, monitor competitors’ Web sites, file and route requests, and deliver customized content to users. Domino agents alert you to Web site updates, bring you information on a given subject, and automatically cache pages for you.

- Web tools
  Domino uses third-party Web tools in addition to its own functionality, giving you the flexibility to work with Java, CGI, Perl, JavaScript, and other options.

- Web site design
  You can design Web sites in Notes databases from either a Notes client or a Web browser. When you use Notes elements like collapsible sections, database links, and navigators, Domino translates them into HTML. You can create one database on a Domino server and users have the same experience and access to information, regardless of client. Links are maintained and tracked automatically — no more error screens displayed to users when you move a file.
• Internet security
  Domino provides unmatched Internet security by controlling who can access servers, databases, and database elements, and who can perform certain actions in a Web site or database. For example, you can have one access level at your site for all users yet restrict access to parts of your Web site, such as the product discussion databases, to the individual users who are authenticated with a name and password. Domino uses Secure Sockets Layer (SSL) v3.0 to encrypt and protect transactions between Internet users and Domino servers. In addition, Domino can validate X.509 certificates and can act as a Certifying Authority (CA).

• Extranets
  Domino makes it easy to set up an extranet that makes part of your intranet information available outside your company. Use a Domino extranet to make information available to customers, vendors, suppliers, consultants, and others in a controlled, secure fashion.

For more information on using Domino for messaging, see Chapter 10. For more information on security, see Chapter 11.

---

**Using Domino to create an interactive Web site**

Domino provides a variety of tools that lets you easily create and set up a rich, interactive Web site. These tools use the database format (.NSF files) to store HTML code, text, images, Java applets, OLE objects, ActiveX controls, and other constructs. For example, documents in databases support rich text — you can paste in a graphic instead of inserting a file reference, making the image load faster and removing the need to learn HTML code.

Web sites created with Domino use the power of the Domino distributed object store, letting you spread workload over multiple servers — you can host different parts of your site in different databases on different servers — set individual security levels in different areas, ensure failover if a server goes down, and distribute authority and responsibilities for the site.

Each database can have its own design or a single corporate design and can have its own security levels. For example, you can give users access to Product Information but restrict Status Tracking to registered customers. In addition, you can set different access levels and permissions for each database. For example, your Sales manager has Designer access to the Product Information database but only Reader access to the Job Postings database, whereas the Human Resources manager has the opposite. Or you might allow any manager to post a job description in the Job Postings database but require the approval of Human Resources before the description becomes available to outside users.
Sites created with Domino tools are template-based, making it easier and faster to create and customize your Web pages. You can also standardize the look of your site using templates by including the same design elements and graphics in the template for each area of the site. This gives your site a consistent, distinct appearance.

Domino sites are inherently cross-platform; you can design them on one platform and run them on another. Domino tracks page creation and edit dates, allowing you to tell how long a page has been on your site and the last time it was updated. With full text search capability, Domino lets users find specific information on any part of your site that is accessible.

For more information about Domino security, see Chapter 11.

**Using Domino.Action to create a Web site**

Domino provides a tool, Domino.Action, for creating Web sites. Domino.Action sites use the full capabilities of the Domino Web server, including automated workflow and content approval, granular security, and distributed content authoring. You can delegate roles; for example, one person has access to create Web pages, another controls user access levels, and a third approves changes to the global site design. With integrated workflow, you can set up e-mail notifications when someone changes a page and needs approval, a customer fills out a form for more information, or pages are not updated in a certain time period.

Domino.Action lets you easily create and maintain a distinctive site appearance and presentation. Should you need to update a corporate logo, product name, or wish to change the site’s look, you can do so in one place.

Domino.Action lets you set up a Web site without having to know HTML, CGI, Perl, or other Internet tools. Construct the site through a guided, point-and-click interface. Set site standards such as corporate logo, layout, and page appearance.

Domino.Action templates and databases come with the Domino server. Domino.Action is based on the SiteCreator and App Assembler engines and eleven customizable templates, stored in the Library, that correspond to different parts of a corporate Web site, such as Job/Career Opportunities, Products and Services, Discussions, and more. Include any or all of these areas in your site. Use either the Notes client or a Web browser to create your Domino.Action site.

Domino.Action includes documentation for the site creation and maintenance process in the SiteCreator database. For more information, install the Domino.Action templates on your Domino server, open the SiteCreator database, and read “SiteCreator Overview” in the section “Quick Start: SiteCreator.”
Setting up a Domino infrastructure for the Internet

Create an infrastructure to support your Domino Internet presence. Consider the following issues:

- **Staff**
  Assign Internet responsibilities to your personnel; in all but the smallest companies, this means designating or hiring some employees solely for Internet tasks. Domino administrators can handle the SMTP/MIME MTA as part of their duties, but you should assign a Webmaster to oversee your site. You may also want to assign employees who are responsible for content on each part of a larger site. At least one manager should review all content before it is posted to the site. Make sure your Internet staff is attuned to the needs of the company, customers, and employees regarding the Internet.

- **Connection**
  Consider how you connect to the Internet. Many companies use an Internet Service Provider (ISP). Know how reliable the connection is, how much it costs, how much data it can transfer per unit time (bandwidth), and what procedures and backups exist if there is a problem with the connection. Decide whether you want to use the same connection for Internet mail and for your Web site.

- **Physical resources**
  Dedicate resources to an Internet presence. If your Web site will have high utilization (number of hits per day), dedicate a Domino server as your Web site server. For larger companies or for companies with heavy Internet messaging requirements, dedicate a server for the Lotus Domino SMTP/MIME MTA. Factor security into your resource calculations — you may need additional servers or upgraded server resources for such security devices as firewalls.

- **Site architecture**
  Determine how you want your site to look and how you want users to navigate through it. Some companies use a consistent element, like a set of links in a pane or a graphic on the top or bottom of the site, to aid users in determining where they are in the site and in moving within it. Try to have information users need most one or two links away from the main page.
Security

Determine what level of access you want to allow to your Web site and to your servers. A read-only Web site would not allow users to send information by entering it on a form; an interactive site would give general users access to create forms and other documents and could give registered users other permissions. Consider which ports to open in your firewall.

For more information, see Chapter 11.

---

About Internet messaging

Domino’s support for messaging standards helps increase your choice of clients — a full-featured client like Notes, a mail-only client like Lotus cc:Mail™, or a browser. Internet messaging is critical for most businesses, who depend on it for timely information exchange. Messaging comprises e-mail, directory access, and Internet newsgroups. Domino supports all major Internet messaging standards, including SMTP, MIME, POP3, IMAP, NNTP, and LDAP, as well as the proven features of Notes mail. The Domino Mail server provides a messaging-only server for smaller companies or companies that do not need the full power of Domino applications.

Consider the following issues when deploying Internet messaging:

- What e-mail formats does your organization use?
  
  Many organizations use a heterogeneous mix of e-mail systems, combining Internet mail with Notes mail, cc:Mail, and other types. Make sure people in your organization can communicate by deploying Lotus Message Transfer Agents (MTAs). The MTAs are server tools that convert messages between formats, letting you operate in a heterogeneous messaging environment. Lotus offers Domino MTAs for conversion between Notes mail and SMTP/MIME, for cc:Mail, and for X.400. Lotus MTAs are efficient, scalable, multi-threaded, and deliver messages in their native format.

- What e-mail formats do people outside your organization whom you need to communicate with use?

  Your organization may use Notes mail, but your customers or suppliers may use Internet mail based on POP3 or IMAP clients, SMTP routers, and MIME format. Set up MTAs to move messages between Notes mail format and other formats. With the MTAs, you can communicate with customers, suppliers, vendors, and others who use e-mail formats that differ from yours.
• How do people in your organization access mail?
People may need to access mail from a Notes client, from a Web
browser, from a POP3 or IMAP client, or from a combination of these
clients. Use Domino to combine mail from the Internet and your intranet
into a single file accessible from multiple clients. In addition to Notes
mail files, Domino hosts Internet mail files for POP3 and IMAP clients
and allows access to your Notes mail file via these protocols. You can
also access your mail from a Web browser by using the Notes Web mail
template, which allows access to Notes mail, calendar and scheduling
features, and task management from a browser. Domino supports mail
files from a number of profiles.

• How do people inside and outside your organization access directory
information?
You can make the Public Address Book information available or use
LDAP to make directory information accessible. Domino supports LDAP
(Lightweight Directory Access Protocol) for accessing the Public Address
Book. LDAP allows a common means of access for clients, applications,
and servers. With LDAP, you can look up entries in a Public Address
Book, an LDAP server on the Web, or a public resource like 411 or
Bigfoot. Users in your organization can access your Public Address Book
from a browser as easily as from a Notes client. Consider carefully which
LDAP or Public Address Book fields you want to make available to
employees and to people outside your organization.

• How do you guarantee access to e-mail and directory information?
If e-mail is critical to the success of your business, make sure that
employees can read and send mail at all times. With Domino Advanced
Services, you can make sure that e-mail and messaging are always
available to your organization. The clustering and failover features in
Domino Advanced Services allow you to group two or more servers,
which replicate their contents in real time as they change, and configure
this server cluster so that if one server fails, other cluster servers take
over for it. Clustering is invisible to users. You can cluster several mail
servers so that if one server malfunctioned or had to be taken offline, the
other servers would send and deliver mail.

• How do people in your organization share knowledge?
Some organizations use e-mail to share information; others use NNTP
newsgroups or discussion databases. Depending on how your
organization makes knowledge available, concentrate server resources
on e-mail, newsgroups, or other knowledge management systems.
About the Lotus Domino SMTP/MIME MTA

The Lotus Domino SMTP/MIME MTA is a component of the Notes Messaging Services family of products. The SMTP/MIME MTA provides advanced messaging features and extensions to the Domino Server. With the SMTP/MIME MTA, a Domino server transfers Simple Message Transfer Protocol (SMTP) messages between SMTP networks (both Internet and intranets) and Notes, X.400, and cc:Mail users.

The SMTP/MIME MTA provides scalable, bi-directional message transfer with SMTP networks. Through the implementation of standards, such as Multipurpose Internet Mail Extensions (MIME), the MTA ensures state-of-the-art interoperability with other SMTP/MIME implementations. Configuration and management are made easy since the MTA is integrated into the Domino server. Notes networks can be integrated with SMTP networks in a variety of different topologies by installing SMTP/MIME MTA on one or more Domino servers. Customers can use SMTP to send Notes mail messages between Domino servers with no loss of form or content when companies desire an SMTP backbone.

The MTA provides flexible address conversion between the SMTP RFC822 format and the Notes and cc:Mail environments.

An MTA, not just a gateway

The SMTP/MIME MTA is a scalable, high performance component of the Domino Messaging Services. The MTA can translate messages from SMTP/MIME to Notes and vice versa, like a gateway. In addition, the Domino SMTP/MIME MTA operates as a traditional message transfer agent (MTA) when there is a requirement to relay messages, unconverted, from one SMTP/MIME MTA to another.

Some firewalls allow only specific applications, like SMTP, to access the Internet’s TCP/IP capability. In cases like this, where SMTP is the only TCP/IP protocol available between two Domino environments, the MTA can encapsulate Notes mail messages over the SMTP network. This provides high-fidelity transfer of Notes mail messages when connected to an SMTP backbone.

Built on standards

The SMTP/MIME MTA is based on Internet Request for Comments (RFCs). Among the RFCs supported are:

- RFC821 Simple Mail Transfer Protocol
- RFC822 Standard for the Format of ARPA Internet Text Messages
Configuring directory access with LDAP

The Lightweight Directory Access Protocol (LDAP) lets you make the directory information in the Public Address Book available to browsers and Internet clients from the Domino LDAP server. Internet users can search your directory for information about your organization; for example, they can look up the e-mail address for your vice president of marketing without knowing her name or location. The Domino LDAP server uses your Public Address Book under the LIPS (Lightweight Internet Person Schema) model. POP3, IMAP, and X.500 clients can access directory information in this manner. Domino supports search filters (defined in IETF RFC 1558) for client queries. Setting up LDAP in your organization requires upgrading your Public Address books and Master Address Book to the latest template.

Consider the following issues when implementing LDAP in your organization:

- What information do you wish to make available to LDAP queries?
  You can restrict which documents and fields you want LDAP users to see — this applies to all your Domino LDAP servers and allows you to protect some fields, such as phone numbers, from anonymous access.

- Do you want the Domino LDAP server to chase referrals if a search fails?
  If an LDAP search fails, the server can either pass one or more URLs to the client as referrals for further searching or it can chase these referrals itself by searching them without prompting the client.

- Do you want servers to connect to your Domino LDAP server anonymously or with SSL authentication?
  You can let LDAP users submit anonymous queries or, for greater security, require them to identify themselves using SSL.

- How much server capacity do you want to dedicate to LDAP?
  You can limit the maximum time for a search and the maximum number of search results that the Domino LDAP server returns in response to a query.
• What do you want the general Internet e-mail address for your organization to be?
  The Domino LDAP server uses the Global Domain record in your Public Address Book to add the proper address to a user's Internet name.

• What level of LDAP security do you want?
  LDAP security adds to the Domino security model. You can allow LDAP users individual access beyond the anonymous access for users not in the Public Address Book.

---

**Configuring Domino newsgroups**

With the Domino NNTP server, you can participate in Internet newsgroups and create private newsgroups via the NNTP protocol. For example, you might want to read articles in and contribute to USENET groups related to your industry. The NNTP server is a Domino server task that hosts news discussions so Notes, NNTP, and Web browser clients can access and participate in them.

Domino can send content to Internet NNTP servers, such as the USENET servers, via news feeds. Domino provides several levels of security for newsgroups, including anonymous access, password authentication, SSL encryption and authentication, and read-only access for NNTP clients. Set the ACL for individual groups to control access.

When setting up NNTP news groups in your organization, consider the following:

• Policies for posting to news groups
  Establish corporate policies regarding employee postings to news groups. Consider whether employees should be able to post to all groups and what restrictions you want on the content and form of their postings. Documents posted to a newsgroup by employees from your organization identify your company and can affect its image.

• Resources
  If you are hosting or using a number of news groups on your servers, consider establishing separate servers for NNTP groups, which consume significant disk space.
• Personal interest profiles
  Consider working with users to set up personal interest profiles that
  notify them of documents they may be interested in.
• Staff
  You may need a newsgroup administrator responsible for replicating
  content to and from Internet newsgroups and for monitoring newsgroup
  activity and postings.
Intranets are increasingly critical for business communication, collaboration, execution, and success. An intranet links computers together, offering a set of shared resources to an organization. Intranets have security that limits or prohibits access to anyone who is not a member of the organization. In some cases, intranets are completely internal, with no access into the system from outside the organization and no access to the Internet or other intranets from within the system. The most common model for an intranet is client-server protected behind a corporate firewall. Intranets can allow access through the firewall for e-mail and HTTP; some intranets open other ports such as LDAP, NNTP, and FTP.

An intranet can be thought of as a secure meeting room — a place where your organization can share and debate ideas, exchange resources, and communicate privately without worrying about having people outside your company gain access.

Types of Domino intranets

Domino offers you several intranet models: an intranet based on the Domino server and the Notes client; an intranet based on a Web browser, Internet mail client, and the Domino server; or an intranet that is a composite of the first two.

A Notes client - Domino server intranet has unmatched features, security, and scalability. You can run it on multiple protocols and use replication to synchronize the contents of databases on different servers in different locations. With Notes, you can create applications, knowledge management databases, and HTML pages via a GUI interface that does not require programming knowledge. Notes clients have a wider range of participation with applications due to their superior interface, multiple Application Programming Interfaces (APIs), and their ability to work while disconnected from the network. With replication, Notes clients allow you to work while not connected to the intranet — in a meeting, on a plane, at home, or in a hotel — letting you be productive and collaborate in any location, at any time. Notes integrates the software your organization needs — you can use
Lotus Word Pro or Microsoft Word as your e-mail editor; the Notes Web Navigator, Microsoft Internet Explorer, or Netscape Navigator as a Web browser; and Notes as e-mail access to Notes Mail, POP3, or IMAP mail files. A browser - Internet mail - Domino server intranet is simple to set up and learn. However, developing applications for an HTML-based system is difficult; you must create them with a programming language and can deploy them only on the TCP/IP protocol. Working offline is difficult or impossible. Internet mail does not have the features of Notes mail such as rich text, shared mail, replication, delivery reports, priority levels, automatic iterated routing to multiple recipients, integrated calendar and schedule management, and automatic addressing. Since browsers access data via a Universal Resource Locator (URL), your organization must track and manage these links and make a directory of them available to users. Browsers lack the integration with other productivity software, such as office applications, that Notes offers. In addition, the browser security model is not as robust as the Notes client - Domino server RSA public-private key system.

A mixed intranet, with both Notes clients and browsers, blends the two approaches. You can create applications with Notes and use both Notes mail and Internet mail. Domino converts Notes applications to Web applications with no user action necessary. While not as rich in features or security as a Notes client - Domino server intranet, the mixed approach may be best for organizations with different levels of need for intranet functionality. For example, a retail clothing company sets up an intranet with browsers accessing applications on Domino in stores and with Notes clients for headquarters and all regional offices. Sales representatives enter data, query inventories, and send e-mail from the browsers, while administrative employees and managers use the Notes clients to design applications, create reports, and manage the business.

Consider the following issues when deciding on an intranet type:

- **What level of functionality do you need?**

  The three types of intranets have different functionality levels based on the features of their client software. A Notes client - Domino server intranet has the greatest functionality, incorporating e-mail, calendar and scheduling features, integrated Internet access, access to Notes applications, and integration with other productivity software. A browser client - Domino server intranet has less functionality, and a mixed intranet has capabilities midway between the other two types. Decide how much functionality your organization needs in each area and in each group.
• If there are several levels of needed functionality, who needs each type?
Your organization may need different capabilities in different areas. For example, a transportation company needs basic access to applications, information in databases, and e-mail for most employees, with more advanced capabilities for administrators, intranet application designers, and managers. The company deploys Notes clients to personnel who need greater functionality and browser clients to other employees.

• Do employees need to work offline?
If employees travel often or are frequently disconnected from your network, they may need to work and be productive offline. The Notes client is designed for offline use by incorporating replication and locally stored database replicas. Browsers cannot effectively work offline without software like Lotus Weblicator™. If employees need to work offline with intranet applications and e-mail, consider Notes clients.

• What software does your organization already have?
Your organization may want to use software that the company already has, or it may want to upgrade. For example, a company using browsers and Lotus Mail as a POP3 client decides to implement a browser - Internet mail - Domino server intranet, with plans to upgrade to Notes clients over time.

---

**Getting a return on your intranet investment**

Domino intranets offer significant opportunities for enhanced productivity and cost savings. To achieve these results, you must integrate your intranet into your core business processes and ensure that employees take full advantage of the intranet’s capabilities.

• Domino can streamline and automate business functions by routing items to the correct person or department, issuing alerts if timely action is not taken on open items, tracking the status of issues, and removing barriers to information sharing.

• Domino applications improve efficiency and productivity while reducing overhead. Your employees spend less time on tasks such as paperwork and more time working on business issues. Domino messaging lets you communicate with teammates, customers, suppliers, vendors, and others at your convenience.

• With e-mail, archive databases, and discussion databases, you can use Domino to store and share organizational knowledge. With Domino views and full text search, information is easy to find.
For example, you use a single database to hold sales information about current opportunities at a company, the history of past transactions and relationships, key contact names, and information critical to a sale. By centralizing this knowledge, you allow your entire sales force to use it in customer relationships, increasing your success.

- Domino databases and messaging make the concept of a “virtual team” a reality. Use replication and e-mail to communicate among colleagues who are distant geographically. Domino manages document information, allowing you to distinguish revisions, distinguish recent changes from older ones, and enter comments. Use the Calendar and Scheduling features of Domino and the Notes client to schedule meetings, reserve rooms and resources, send announcements, and give others information about the free and busy times in your schedule and theirs.

Intranet security

To ensure the security of your intranet, consider the following:

- How will you protect your intranet from unauthorized external access?
  Set up a firewall between your intranet and other intranets, and your intranet and the Internet. Consider which ports in the firewall need to be open and in which directions. Close all other ports.

- Do you want to allow remote or external intranet access?
  Regulate and monitor remote and external access to your intranet. This helps you determine what resources are needed for remote and external access and to catch security violations.

- How will you authenticate intranet users?
  Set the Server access list in the Server record for each Domino server in your Public Address Book to allow access only to users certified by your company for Notes ID files. You should give users interacting with Domino from a browser a user name that ends with the certification of your company; for example, John Smith/SALES/ACME.

- How will you control access to intranet information?
  Set access control lists on your databases carefully. Consider the level of access needed to the database for different groups. If only a select group needs access to a database, add them explicitly to the ACL and make the Default ACL entry No Access.
• How will users access intranet information?
  Consider the level of access you need Web browsers to have to your databases. If only Notes clients access the databases, set the Maximum Internet name and password access in the ACL to No Access. You may want to set this level to Reader so that browsers can read databases but only Notes clients can create or delete documents within them. This helps to further limit control over the contents of a database.

• What information needs to have restricted access or to be kept confidential?
  Set access restrictions for fields, views, forms, and documents that only selected people and groups should see. For example, you have a Human Resources database with benefit information for employees. All employees can read their benefits, but only Human Resources personnel can create documents for new employees. You give employees access to edit some fields to update personal information — for example, to update the Number of Dependents field when a child is born.

For more information, see Chapter 11.

---

**About intranet applications**

Applications are the most productive and important part of an intranet. You can use applications to store knowledge, process information, track the status of items, collaborate with team members, review project documents, and automate business processes. Domino makes it easy to design, develop, and deploy rich, interactive intranet applications.

When deploying applications on your intranet, consider how and when users will access and use these applications. This helps you decide how many replicas of an application to create and which servers to place them on. For example, a Human Resources application that is used heavily by the HR department but sparsely by other users is placed solely on HR servers, requiring people outside the HR department to access those servers to use the application. A Sales tracking database used by your entire Sales force and most of your organization in multiple countries at different times is replicated to each office’s local server. These replicas send changes to regional hub servers, which exchange updates.

Also consider how users will interact with applications: using Notes clients, browsers, e-mail, or in other ways. This helps you design and implement effective applications.

For more information, see Chapter 4.
About mail on your intranet

E-mail is a critical component of a successful intranet, allowing your employees to communicate in a timely manner, exchange files, and disseminate information widely. Whether you use Internet mail, Notes mail, or a combination, Domino is a reliable, easy to administer mail server. With the Domino Mail server, organizations obtain a mail server that does not include the application hosting and development capabilities of the Domino server. Should needs change in the future, the upgrade path to the Domino server is seamless.

Consider the following issues with intranet mail:

- Which mail features do I need?
  Internet mail, based on IETF standards such as RFC 822, does not have the features of Notes mail. Notes mail has rich text, integrated digital signatures, complete offline capabilities, Object Linking and Embedding (OLE) 2.0 support, and calendar and scheduling features. Decide which features you need in your e-mail system and whether you can best obtain those features with Internet mail or Notes mail.

- What capabilities do I want a mail server to have?
  The Domino Mail server is a messaging server, without application capabilities. If you want to use only mail on your intranet, choose the Domino Mail server. If you also want application development and hosting capabilities, choose the Domino server.

For more information, see Chapter 10.

Pushing information to your users

Domino offers you “push” capabilities to deliver company announcements, updates, requests, and news directly to your employees’ computers. Using Domino.Broadcast, you can integrate information delivery with your Domino server. Domino.Broadcast adds to your intranet by making information active rather than passive — the intranet brings information to employees’ attention, rather than waiting for them to locate and read it.

For example, you send an alert via Domino.Broadcast reminding employees to fill out a survey about a new corporate Web site. By clicking on the alert on their desktop, employees cause Domino to transfer them to the survey form in a database. Employees fill out the survey, save it, and return automatically to their desktops.

Scaling your Domino intranet

A key question businesses face when planning and deploying an intranet is scalability. You want to provide sufficient capacity to ensure good performance while also creating a plan for expansion to meet future needs. Scalability encompasses a number of issues:

- **Server**
  
  How many users and applications can a server host? How much mail can it route efficiently? How often can it replicate databases without suffering significant performance costs?

- **Network**
  
  How much traffic can my network route and process efficiently? What slowdowns exist and how can I eliminate them?

- **Application**
  
  How many users can I host on one application? For example, how many users can use a Notes database at the same time? How large can a database grow before it becomes too large, making replication and performance substandard?

Lotus has developed a tool to address these questions. Domino Server.Planner allows you to gauge how configurations from various vendors and parameters you input based on your system needs will perform. Use Domino Server.Planner to plan hardware and software purchases and to plan server load balancing.

For more information, see Chapter 2.
An extranet exposes part of your intranet to people outside your organization (beyond your firewall). Extranets can add significant value to your business. For example, you can manage your inventories more tightly by letting suppliers detect when items are running low and vendors see what goods are in stock. A shipping company can save on phone costs and support time by opening its intranet to customers, who can then use a Web browser to track where their package is during transit.

About deploying a Domino extranet

With Domino, there is little or no additional work needed to set up an extranet. Domino security allows you to set access to your intranet information as you choose. You can do this in a controlled fashion, by strictly limiting who has access to information and what information they can see, or in a general fashion, which allows anyone with a Web browser to view your organization’s information. Most organizations separate their Internet site, which can be seen by anyone, from their extranet, which is treated as a business resource for customers, suppliers, vendors, consultants, and other trusted firms and people.

For example, you create a Job Postings database on your intranet for your employees to browse and then decide to make this information publicly available. By allowing Web browser access to the server and Job Postings database, you let prospective employees see the open positions in your company. At the same time, the rest of your intranet remains completely secure.

You can also make a database available only to individuals or groups — for example, you give Human Resources and managers access to a Salary database but prevent access by the rest of the company.

There are two types of extranet access: general and individual. General access is based on the Default or Anonymous entries in a database ACL to anyone who views the site. In the ACL for the database, create an entry named Anonymous and assign it the access level, roles, and permissions you want anonymous Web users to have. If you do not create an Anonymous entry, anonymous Web users have the access granted to the Default entry.
Individual access requires specific entries in the ACL, either as individual names or as members of a Group. Groups are managed in the server’s Public Address Book. You can have both general and individual access concurrently. For example, you have an extranet where the Job Postings database is accessible to everyone on the Internet or with a Notes client, but the Software Specifications database is accessible to a few external consultants. Using Notes security, you can have general and individual access to different elements within a single database.

For more information, see Chapter 11.

---

**About administering individual extranet security**

For individual extranet security, you have two choices: add each user to a database ACL individually, or add each user to a Group in the Public Address Book and add the Group to the database ACL. If you use the individual option, you have much finer control of security and access but will engage in more maintenance and administration on each database.

If you use the Group option, you can centralize user administration in the Public Address Book but do not have the same level of control as with the individual option. For example, if you add users to one Group and add that Group to multiple database ACLs, you cannot distinguish among users in that group regarding access. While you may want all members of the group to read documents about corporate policies and training, you may want to restrict access to information about annual reviews. To do this, you must separate users into more than one group or use individual entries.

If you want to have low-level Web security, you can create a single Person record, such as “Guest,” and give out that name and HTTP password to a number of extranet users. This allows some differentiation between extranet users and the general public, but should not be used for confidential information as the name and password may become known.

You can also use Group and individual entries for database elements like forms, views, and fields. For example, you want a team to review plans for a joint construction project but only management of the two companies to see the financial data. You do this by entering each manager’s name in a Read access list for the field or create a Group containing the managers’ names in the Public Address Book, add it to the ACL, and then add it to the Read access list for the field.

**Caution** Field-level encryption does not work on the Web. Be cautious in exposing databases with field-level encryption to browser client access as these clients may be able to read the encrypted fields.
Using an extranet to access Notes mail over the Internet

With Notes remote access and replication features, users can access their mail via the Internet while disconnected from a Domino network. Put the mail files on a Domino server and replace the template with the Web mail template. Have your Domino administrator register users as Web users, with user names and passwords. Make sure that Web users have access to this Domino server. With this configuration, users can access their mail from any Internet-connected browser: they can read and delete mail, and send and delete messages. They don’t need Notes IDs, just user names and passwords.
Chapter 8
Deploying Domino Servers

A major part of planning your deployment is setting up the servers. You may install a mix of Domino Mail servers and Domino servers, depending on your organization’s needs. Consider dedicating servers by use, installing only the tasks necessary for that server’s role. This is important for enterprise organizations that have heavy server demands and many servers; it is less critical for smaller organizations.

Deploying servers is not only installation and setup but also making servers available to users and connecting the servers for optimal information exchange. Consider how to deploy your servers for ease of use and efficient replication and mail routing.

About setting up Domino servers

Be consistent when installing and setting up servers. Consider the following:

- Establish a standard directory structure for Notes. Consider putting the data files in a root-level directory separate from the program files to make future upgrades easier.
- Put the NOTES.INI, SERVER.ID, and DESKTOP.DSK files in the same directory on all servers.
- Create a logical naming convention for servers that is easy to remember. Consider naming servers by functional area, such as Sales1, or geography, such as Los_Angeles1.
- For servers that connect outside your organization, use a naming system that includes your organization name in the server name. This minimizes the possibility of servers with identical names connecting without authorization and breaching security. For example, call a Sales server in the Acme company that connects with servers outside your organization Acme_Sales1.

For more information, see the Domino Install Guide.
About partitioned servers

With Domino Advanced Services, you can install partitioned servers, which allow you to run more than one server on a computer. Domino treats each server as a separate computer with its own system resources. With partitioned servers, you can increase the number of servers in your organization without additional investment in hardware. Partitioned servers can provide independent groups of users with their own domain and server on the same computer. You can set up partitioned servers in different domains on the same machine and can cluster partitioned servers. Each partitioned server has its own administrative client. If you want, you can later easily migrate partitioned servers to separate servers.

Domino supports up to six servers on a single computer. Install the files for each partitioned server to a separate data directory. What happens on one partitioned server does not affect other servers on the same computer.

For more information, see “About partitioned servers” and “Planning a partitioned server configuration” in Chapter 10 of Extending the Domino System.

About server topology and replication

In a Domino system with more than one server, you must plan how to connect your servers to take advantage of replication and mail routing for information updates and exchange. This is known as server topology, the primary goal of which is to set up efficient information exchange by minimizing the number of hops, or connections, information must pass through to reach its destination.

Topology is set up by Connection documents in the Public Address Book. Replication between servers requires one Connection document since replication works bidirectionally, but mail routing requires two Connection documents since it only works in one direction.

The topology that you should adopt varies with organization size. Most small firms use Peer-peer replication, which quickly disseminates changes to all servers but is inefficient for more than a few servers. Mid-size firms may use a combination of Peer-peer and Ring replication, or may implement Hub-spoke replication. Large organizations likely use Hub-spoke replication at several levels (local hub-spoke setups, with local hubs as spokes in a
national hub-spoke setup) for maximum efficiency or may have Ring replication between hub servers. Replication topology normally duplicates the overall server topology of your Domino system.

- **Hub-spoke**
  Establishes one central server as the hub and other servers as the spokes. The spokes update the hub server by replication and mail routing, and the hub in turn updates each spoke. Hub servers replicate with each other or with master hub servers in organizations with more than one hub. You create two Connection documents for each spoke server (spoke to hub, hub to spoke) and two for each hub to hub connection. Hub-spoke is generally the most efficient replication topology and minimizes network traffic, especially in larger organizations.

- **Peer-peer**
  Connects every server in your organization to every other server. This becomes unmanageable in organizations with more than a few servers, but does allow rapid updates in very small organizations.

- **Binary tree**
  Connects servers in a pyramid fashion: the top server connects to two servers below it, each of which connects to two servers below it, and so on. Information travels down the pyramid and then back up.

- **Chain**
  Connects servers one-to-one, end-to-end. Information travels along the chain and then back. Chain replication is less efficient than ring replication but is useful in situations where information only travels in one direction.

- **Ring**
  Connects servers in a circle; it is like chain topology with the ends connected.

- **Cluster**
  This is less a pattern than a way of ensuring server access. Use clustering where you must ensure constant access to data. Clustering is available as part of Domino Advanced Services.
Examples: About server topology and replication

**Hub-spoke**

Hub-spoke replication uses one server as the center (hub) of a ring of spoke servers. The hub coordinates replication for all spoke servers and handles all replication processing, reducing the resource and task load on the spoke servers. With four servers (1, 2, 3, 4) that need to replicate, replication looks like this:

<table>
<thead>
<tr>
<th>2 with 1 (hub)</th>
<th>3 with 1</th>
<th>4 with 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 with 2</td>
<td>1 with 3</td>
<td>1 with 4</td>
</tr>
</tbody>
</table>

The spoke servers send changes to the hub, which then sends changes back to the spokes. While there are six connections, the hub server performs the replication, reducing the load on the spokes. Hub-spoke replication has one Connection document for each hub-spoke connection, with the hub server as the source and the spoke server as the destination. With hub-spoke replication, you can standardize database ACLs with the hub as manager, limit access to the hub, minimize network traffic and maximize network efficiency, centralize replication administration and data backup at the hub, and improve server load balancing. However, network traffic increases on the hub LAN segment. If you have more than 25 servers per hub, establish tiers of hubs. If a hub goes down, replication for that hub and its spokes is disabled until the hub is repaired or replaced.

**Peer-peer**

With peer-peer replication, each server replicates with every other server. With the same four servers, replication looks like this:

<table>
<thead>
<tr>
<th>1 with 2</th>
<th>1 with 3</th>
<th>1 with 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 with 3</td>
<td>2 with 4</td>
<td></td>
</tr>
<tr>
<td>3 with 4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This involves six replication connections to synchronize four servers but allows progressive updates of content. The potential for replication problems decreases because only two servers communicate for each replication, without hub or intermediary servers. However, peer-peer replication requires many Connection documents, increases administration since you must avoid overlap in replication schedules, and prevents you from standardizing ACL requirements.
**Binary Tree**

Binary tree replication connects servers in a pyramid and is normally used in organizations with many servers. A server replicates with two servers beneath it; each of these servers replicates with two servers below it; and so on. Once information has reached the bottom of the tree, two servers at the bottom replicate with one server on the level above. This server and another at its level replicate with a server on the level above them, and so forth. With five servers, replication looks like this:

<table>
<thead>
<tr>
<th>First level down to second</th>
<th>1 (top) with 2</th>
<th>1 (top) with 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second level down to third</td>
<td>2 with 4</td>
<td>3 with 5</td>
</tr>
<tr>
<td>Third level up to second</td>
<td>4 with 2</td>
<td>3 with 5</td>
</tr>
<tr>
<td>Second level up to first</td>
<td>2 with 1 (top)</td>
<td>3 with 1 (top)</td>
</tr>
</tbody>
</table>

Information takes longer to replicate in binary tree replication than in hub-spoke replication and if one server goes down, all servers in that “branch” of the tree fall behind.

**Chain**

Chain replication is end-to-end replication of servers in a line. With the same four servers, replication looks like this:

<table>
<thead>
<tr>
<th>1 with 2</th>
<th>2 with 3</th>
<th>3 with 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 with 3</td>
<td>3 with 2</td>
<td>2 with 1</td>
</tr>
</tbody>
</table>

This increases the time it takes changes to migrate to all servers.

**Ring**

Ring replication is similar to chain replication, but connects the ends of the chains, forming a loop. With the same four servers, replication looks like this:

| 1 with 2 | 2 with 3 | 3 with 4 | 4 with 1 |

Ring replication is more efficient than chain replication.
**About hub-spoke topology**

Hub-spoke topology is the most efficient setup for Domino servers. The hub server replicates with each spoke server in turn according to the schedule you define. You can:

- Install multiple protocols on hub servers to enable communication in organizations using more than one protocol. This places hub servers in multiple Domino named networks, another source of efficiency. Hub servers can connect multiple Domino named networks.
- Bridge parts of a network, such as a LAN and a WAN, with a hub server.
- Centralize administration of the Public Address Book by designating the hub with Manager access and the spokes with Reader access. Making changes in one replica (on the hub) synchronizes the spokes.
- Designate hubs by role; for example, replication hubs and mail hubs.
- Place server programs like Message Transfer Agents on hubs to make them easily accessible.
- Use a hub to connect remote sites to your LAN or WAN.

Often, a single hub server and its spoke servers make up one Domino named network.

---

**Designating servers for tasks**

You can designate servers for specific Domino tasks. This can improve system efficiency, especially in large organizations, and make administration easier. Clustering provides a way to ensure access to any of these types of servers. Some server tasks you may want to designate are:

- **Mail**
  
  Host mail and Address Book databases, the Calendar and Free Time system, and route mail. This reduces network traffic, since mail routes only between mail servers and some mail is sent to recipients on the same mail server.

- **Hub**
  
  Replicate databases and route mail from spoke servers and connect different parts of an organization, such as a LAN and a WAN or remote servers to a LAN.
• MTA
  Route and convert messages between message formats. This is especially useful if you run Notes Mail on your LAN and communicate frequently outside your LAN via Internet mail.

• Application
  Host Notes applications. You can reduce the number of Connection documents in your system if these applications do not use mail, since replication only requires one Connection document while mail routing requires two. You can group applications by use, load, or functional area on the same server.

• Passthru
  Allow users to connect to other servers from one location. Passthru servers connect you to other servers through a single place without requiring you to know routing information for the servers. Remote users can dial in to a passthru server and connect to multiple servers without making additional phone calls. Passthru servers usually do not host applications or mail databases.

• Remote
  Let users access Domino via a modem. With a remote server, you do not need to install and maintain servers in remote locations. You can set up mail and application servers as remote servers. A remote server increases security by acting as a single secure point of entry.

• Billing
  Track and record activity for server sessions, replication, mail, database use, and document use. Use billing to charge internal or external sources for Domino server usage. Billing tasks on the Domino server transfer billing records to a billing database. You can retrieve billing data or send it to a binary file for integration into your organization’s invoice process. Domino billing servers integrate with existing billing processes through APIs and third party applications. Billing is available as part of Domino Advanced Services.

• Gateway
  Connect Notes and foreign systems; for example, Soft-Switch®. Some gateway servers convert Notes documents to another format.

• Backup
  Store critical information. If information is lost on your other Domino servers, you can restore it from the backup servers. In addition, you can copy replicas on backup servers to disk, tape, or other removable media.
About passthru servers

Use passthru servers so remote users and servers can connect to your Domino servers from one location without multiple phone calls. Passthru servers running multiple protocols can connect to other servers or clients that do not share a common protocol. You can also use a passthru server as a remote services server.

Users can define a default passthru server in the Location document for their Notes client and can use multiple passthru servers by creating passthru Connection documents in their Personal Address Book. You can define a default passthru server for a Domino server in the Server document in the Public Address Book.

To balance workloads among passthru servers, set up hunt groups, groups of servers with the same phone number. Incoming phone calls are distributed among the hunt group to balance server workload. If one server is down, calls are routed to other servers in the hunt group.

Control passthru security in the Server document in the Public Address Book by configuring the fields “Access this server through passthru” and “Use this server as a passthru server.”

You can use passthru servers for replication.

About Domino and file servers

With some network operating systems, such as IBM LAN Server or Windows NT, Domino servers can run concurrently with the network file server. Some network operating systems, such as Novell NetWare, require that Domino servers run concurrently with a file server.

However, if your system does not require it, avoid running Domino servers concurrently with a file server because:

- Security may be circumvented by network file server users if the Domino data directories are inadvertently shared. Restrict all access to Domino data directories from network users.
- Performance of either the file server or the Domino server will suffer if one uses a lot of processing time.
- Stability of the file server or of Domino may be affected. For example, if a file server program or a Domino program is restarted, all other programs or processes must also be restarted.

For more information on security, see Chapter 11.
Deploying Domino in multi-protocol environments

If your network infrastructure uses more than one protocol, consider the following:

- Bridge Domino named networks by repeating one server in all networks. For example, to bridge Trout, running TCP/IP, and Salmon, running SPX, install both TCP/IP and SPX on server Guppy and include Guppy in both Domino named networks. This allows the server Guppy to exchange mail and replicate updates between the Domino named networks Trout and Salmon.

- Use a hub server running multiple protocols to ease replication between Domino named networks. This minimizes the number of Connection documents you need and simplifies administration.

About integrating Domino with Microsoft Windows NT

If you are using Windows NT, you can use either Windows NT or Domino to perform many of the administration tasks in both products. For example, you can:

- Register a new user in Domino or in Windows NT and automatically register the user in the other product as well.

- Register existing Windows NT users in Domino. Optionally, you can assign Windows NT users to a Domino group when you register them in Domino.

- Create a new group in Windows NT and automatically create the group in Domino. Optionally, you can register the group members in Domino.

- Add existing Windows NT groups to Domino. Optionally, you can register the group members in Domino.

- Delete a user from either product and automatically delete the user from the other product as well.

- Delete a group from either product and automatically delete the group from the other product as well.

- Rename Windows NT user accounts when you rename Notes users.

- Synchronize existing Windows NT and Notes users when user information changes. Optionally, synchronize passwords so that existing users have the same password for Windows NT and for their Notes Internet password. (When you create new users, you can assign them the same password for Windows NT, for Notes, and for their Notes Internet password.)
• Use Windows NT to create Notes Internet-only users.
• Assign users Internet mail when you use Windows NT to register them in Domino.

Planning for replication

Replication is a task that requires significant CPU and network resources. Plan your replication topology carefully to eliminate unnecessary connections and make the most of each replication while keeping databases as up to date as possible. Replication depends on your network and server topology and varies greatly with organization size. For small businesses, replication involves only a few servers — reducing the number of connections is less important due to the small number of total connections. For mid-size and enterprise organizations dealing with many servers, multiple sites, modems, and LAN and WAN connections, planning replication carefully is critical.

Domino and Notes use a distributed content object store, which means that Domino maintains content in multiple places simultaneously. A database (content) can reside on several servers at the same time. Each iteration of this database is known as a replica. All replicas initially have identical content. Since people can make changes to the database replica on each server, the database replicas quickly become different — their content is no longer the same. Replication is the process of synchronizing the different replicas so that they are again identical.

Replication gives multiple sites, teams, and people the ability to make changes easily to a database and share these changes with everyone else who has access to the database. Replication ensures that you see the latest information in a database. It is also an advantage for mobile users, who can keep a local replica of a database on a laptop and then replicate with a server database via a modem. Mobile users can dial in, replicate, hang up, work offline, then replicate their changes back to a server. Replication also reduces network traffic by providing access to databases from local servers; people do not need to attach to a central server to work with a database.

Domino replication is superior to other means of synchronizing databases in that you can control globally which replicas can make changes that propagate to other replicas. In addition, Domino offers a variety of replication strategies instead of limiting you to a superior-subordinate replication mode. Domino field-level replication greatly reduces replication time and the network and computer resources needed to accomplish this task.
About using replication in an organization

Replication can make your business more efficient and your employees more productive.

- Administrators can set up network resources to allow users to create new databases only on certain servers, or only after participating in a review process.
- A sales representative on the road can dial in to her mail database, replicate, and read her messages. She can replicate with a database containing a new presentation that wasn’t ready when she left the office a week ago.
- In the office, replication ensures backups. If one server goes down, you can work on another replica, then send changes so that information is up to date.
- If you have teams working in multiple places, replication can ensure that they have the most up to date information to work with. If the testing team in Austin enters bug reports into a tracking database, the development team in Chicago will learn about it after the next replication.
- It can reduce network traffic at the same time that it reliably updates key information. To see the latest information from manufacturing, check the orders database — no need to send a round of e-mail.

Replication makes the concept of a “virtual team” a reality — workers in different locations, working at different times, can seamlessly collaborate, revise, and create. Replication allows you to distribute content for easy local access while ensuring that it stays current with the latest information.

About database replicas and database copies

If you want to update the content of a database from another iteration of it, create a new replica. If you want its content to be unique and not alter the content of other iterations of that database, create a new copy.

Replica databases have the same replica ID, a number which allows the Domino server to identify all the iterations of a database and update their content. Replica databases can have different file names; Domino examines only the replica ID.

Database copies differ from database replicas in that they cannot exchange updates. Database copies have different replica IDs.
About replicating servers

Replication is a server task that occurs between two servers in one direction. One server at a time calls a second server and checks for changes in common databases. The server then either sends changes to the other server or receives changes from it. This highlights the three types of replication: Push, Pull, and Push-Pull. Push replication sends changes from the first server to the second. Pull replication receives changes from the second server to the first. Push-Pull replication sends changes from the first server to the second, then pulls updates from the second server to the first.

Controlling replication is a vital challenge. For example, a corporate policies database is controlled from a central office, with replica copies in all field offices. The company wants to restrict access to and replication of the database such that changes can only be made in the replica in the central office. The firm accomplishes this with Push replication so that the field office replicas receive changes from the central office replica, but cannot send changes to it. Or, a company has replicas of a database both inside and outside its firewall, such as a customer comment database accessible via the Web. The company wants to prevent internal information and status tracking from replicating to the outside database, so it uses Pull replication to bring information from the database outside the firewall into the company.

When planning replication, consider the following questions:

- Do replicating servers have appropriate access to each other’s data?
  Do they share a common certificate? Are they listed correctly in the server access list?

Replication control begins with server access. When Server 1 calls Server 2 with a replication request, Server 2 checks whether Server 1 has been granted access in the Server Access field of the Server document for Server 2 in the Public Address Book. If Server 1 does not have access to Server 2, replication cannot begin. If Server 1 does have access to Server 2, the two servers begin the process of authentication (checking for a common certificate so that the servers can “trust” each other). Server 1 authenticates Server 2. If this happens successfully, Server 2 authenticates Server 1. Without authentication, replication cannot take place. Once the servers successfully authenticate each other, they compare databases to determine which have changed since the last replication (exchange of information and changes).
Does each server have access correctly set in the ACL of replicating databases?

Servers check the database access control list (ACL) for each replicating database. The ACL determines what actions each server can perform upon the database. Access levels range from No Access, which does not allow the server to view or modify the contents of the database, to Manager, which allows the server to modify content in the database and the ACL. Checking the ACL tells the servers what content they can replicate and update. For example, a server with Reader access to a replica on another server can receive (read) updates from that replica but cannot send changes to that replica.

Are servers replicating too frequently based on the information in the replication history?

After determining what access each server has to the other server’s replica, the servers examine the replication history of the database to find out which documents have changed since the last replication. Then the servers check the replication settings for the database to see which documents can replicate. The replication settings may only allow a subset of documents to replicate; for example, documents in a certain folder or documents which meet the criteria established in a formula.

Have document authors prevented their documents from replicating?

Servers check all of the documents that are eligible for replication to ensure that they have access to each document. Authors can restrict access to a document or a form (from which documents are created) with a Readers field that limits who can read the document. If there is a Readers field and the server is not listed in it, the server cannot replicate that document.

For more information on replication, see chapter 5 of *Getting Started with Domino* and chapter 4 of the *Database Manager’s Guide*.

---

**Planning replication scheduling**

Because replication can involve moving large amounts of data, how you set up and schedule replication can have a significant impact on performance. After you develop a basic replication strategy, consider some of these tips to help you fine-tune your system:

- To use your server resources efficiently, run multiple replicators on a single server so that replication among servers will be faster. Each replicator must replicate with a different server; you cannot use multiple replicators to replicate with multiple databases on the same server.
• Use selective replication to replicate only certain items instead of automatically replicating an entire database.

• To save money on connection costs to remote sites, specify a time limit for replication in the Server Connection document.

• Keep the number of hops in a replication route to a minimum. The number of hops results directly from how you connect servers with Connection documents. Generally, when you get beyond a few servers, the most effective arrangement for servers is hub-spoke, where the hub initiates replication by calling the spokes and passing the replication data along.

• Because replication can affect response time on a server, limit replication on servers where users are attached. Heavy replication schedules should be restricted to dedicated replication servers or to hubs.

• Don’t run server tasks such as AGMGR, UPDALL and UPDATE on a hub server. These tasks slow the server because they require CPU resources and affect most databases.

• Don’t build or store full text indexes on a hub server. Full text indexes take up disk space and must be updated. Build and store full text indexes on spoke servers.

• Don’t put hub servers in the same Domino named network as any other servers. Hub servers should not participate in mail routing and should not appear in a user’s Open Database dialog box. The server access list of a hub server should enforce these restrictions.

• When a replica is placed on a hub, it should be a complete replica. This allows spoke servers to selectively replicate from any hub server. Exceptions should be carefully managed.

• It is tempting to try to schedule replications at different levels of the hub-spoke arrangement to predict the movement of data up to the central hub and then back down to the spokes, but this does not result in any benefit. Each hub serves its spokes best by conducting a simple “round robin” schedule among them, repeating as often as practical. This distributes all data within a hub’s sphere of influence as quickly as possible.

• An exception to hub-spoke replication is if you have a very large database (500MB or larger) that is supported on only two or three servers. In this case, the servers should replicate directly with each other so that the hubs do not need 500MB of space to support the database.

• In a tree structure, any problem with a hub server partitions the network into two pieces that don’t communicate with each other. To alleviate this risk, have a backup server available and configure it so that it can be substituted for any hub server in fewer than 10 minutes.

For more information, see Chapter 5 in Getting Started with Domino.
About improving replication performance

- Be careful about over scheduling the server. When the server becomes overloaded, calls back up, mail is not delivered, and users may receive poor service from the server.
- Check the log file (LOG.NSF) to see that databases are replicating properly, mail is routing promptly, and that the server is not overloaded. If necessary, modify the Connection documents and make adjustments until the problem is solved.
- Use selective replication to replicate only documents from a certain person, about a certain topic, or subsets of databases.
- If replications are taking too long, change the schedule to replicate more often so there are fewer updates per replication.
- Schedule replication at off-peak hours. If you are replicating internationally, consider the time zones for the source and destination servers and plan accordingly.
- For the most dramatic improvement in performance, set up multiple replications so that a server, such as the hub, can replicate with multiple servers simultaneously. This should improve replication performance immediately.
- Use replication options to shorten replication times. For example, if a hub server replicates to 50 servers and you want to make sure an entire replication cycle occurs twice a day, limit the time the hub connects to each server. Be sure to check the log to see which databases replicate completely and which do not.
- Set the replication priority to high, medium, or low to replicate databases of different priorities at different times. Set up replication groups based on replication priority.
- Develop a policy that controls how database replicas get placed on servers. Creating unnecessary replicas consumes system resources.
- Check the Statistics & Events database for events indicating server problems.

For more information on managing scheduled replication, see Chapter 5 in Getting Started with Domino.
About using replicas on Notes workstations

Users can create database replicas, called local replicas, on their Notes workstations if they have access to the database. With local replicas, users can work offline and then send changes back to the replicas on the servers. This reduces network traffic and allows you to be productive when the network is busy or down. Remote users can work without a modem connection, saving costs and increasing mobility. Users can decide which changes to send to the server and can force replication to send them the latest changes and to update the server replica.

About planning replication policies

Replication is a resource-intensive task. Users and administrators can force replication from a workstation or from the server console. Thus, you must plan to minimize the replication load upon your servers while also keeping databases up to date. Consider the following policies:

- Limit the creation of new replica databases by limiting which servers users can place replicas on
- Route requests for new replicas through an administrator or team
- Limit access to creating replicas by creating a Group in the Public Address Book listing users with this authority. List this group in the Restrictions field.
- Create new replicas only as necessary.
- Test the need for a replica database by monitoring usage of existing replicas. If usage is high, or users at one site frequently access and change content in a replica, consider new replicas — for example, at the site with heavy usage.

About replication conflicts

With field-level replication, changes in documents can be merged as long as the same field has not been modified in each replica. If this happens, replication produces a replication conflict. For example, if an administrator in Key West modifies the Time field for a conference call on July 11, and a vice president in San Diego modifies the Time field for the same call before the Key West change replicates to her server, future replication will produce a replication conflict. Domino cannot tell which Time entry is the correct one, so it produces two versions of the conference call document and signals the
conflict with a diamond next to the second document. You must resolve these conflicts by deciding which document version is correct. Copy the correct information into the main document and delete the second (and other) documents.

You can avoid replication conflicts by:

- Selecting to merge replication conflicts in the Form Properties InfoBox
  Selecting to merge replication conflicts allows Domino to compare the fields of two documents that have a potential replication conflict. If the two documents do not have any changed fields in common (there are no fields which have been changed on both documents since the last replication), Domino merges the documents by updating each field with the latest information. If the two documents do have fields which have changed on each document, Domino creates a replication conflict. Domino’s field level replication greatly reduces replication conflicts.

- Specifying a versioning option when creating a form
  You can further reduce conflicts by designing versioning into forms. This prevents conflicts by storing each iteration as a new version of the document.

- Using LotusScript to create a program to handle conflicts
- Assigning users Author access or lower so that they cannot edit documents

### About save conflicts

Save conflicts occur independently of replication but cause replication conflicts. Users create a save conflict by opening and editing the same field or fields in a document at the same time. If a vice president and her administrative assistant open a Meeting document at the same time, modify the Location field, and then save the document, they will create a save conflict. Domino cannot tell which version of the saved document is the correct one, so it saves one as the main document and the second as a save conflict. Domino indicates the conflict with a diamond next to the save conflict document. Selecting to merge replication conflicts has no effect on save conflicts.
About monitoring replication

Domino provides a database, LOG.NSF, that logs replication events for a server. Using the log, you can track the following items:

- Disconnection between network or remote servers
- Certification problems
- Documents damaged in replication
- Problems resulting from insufficient ACL access

Each database also maintains a replication history that is useful for tracking replication problems. The database manager is generally responsible for monitoring the replication history. View by clicking the Replication History button on the Basics tab of the Database Properties InfoBox.

Deploying the Public Address Book

The Public Address Book is the center of a Domino system. It contains all of the directory information your system needs about each server, user, group, server connection, certificate, domain, Domino named network, cluster, and configuration. It is also involved in each aspect of a Domino system, including mail routing, security, and replication. You create the Public Address Book for a domain when you set up the first server in that domain. The Public Address Book is a database (NAMES.NSF by default) that resides on every server in its domain. Maintaining accurate information in the Public Address Book and ensuring that it replicates successfully and frequently is essential to the proper functioning of your system. With the Public Address Book, you can efficiently administer multiple servers remotely from one location.

Documents, or records, in the Public Address Book track all parts of the Domino system. Domino creates some documents automatically when you perform certain actions such as setting up a server or creating a new user ID file. Some of the documents in the Public Address Book are:

- Person documents
  
  Domino creates a Person document for each Notes user. You can create additional Person documents for Internet users who access Domino from other clients. Person documents contain information on a user’s name, home/mail server, personal information such as phone number and office, domain, mail system, HTTP password (encrypted), and public key.
• Server documents
  Domino creates a Server document for each Domino server in the domain. A Server document includes a server’s public key and information on the domain, Domino named network, location, who can access the server, who can create databases and replicas on a server, server routing tasks, network and proxy configuration, message transfer agents, security, and Internet processes.

• Connection documents
  You create Connection documents to allow Domino servers to connect to replicate common databases and exchange mail. There are different Connection documents for remote, LAN, modem, and protocol connections.

• Certificate documents
  Domino creates a Certificate document for each certifier ID you create. The document lists the certifier name, which certifier created it, who to contact for certification, and contains a public key for the certifier.

• Group documents
  You create Group documents as lists of users, servers, and other groups who have a common characteristic, such as working on the same project or attending the same meeting. Use Groups in server access lists, e-mail addressing, and ACLs for greater efficiency. You can create several types of groups: e-mail only, ACL use only, server Deny list only, or multiple purposes. Assigning a group type simplifies views in the Public Address Book.

• Cluster documents
  Domino creates Cluster documents when you set up clustering using Domino Advanced Services. Cluster documents list the cluster name, cluster servers, cluster title, and cluster administrator.

• Configuration documents
  You create Configuration documents to manage and administer Domino servers remotely from the Public Address Book. Configuration documents set the NOTES.INI variables for a server, group of servers, or all servers in a domain. Individual configuration settings take precedence over group settings, which take precedence over domain settings. You modify settings in Configuration documents with the administration panel. You do not need to restart the servers for the new settings to take effect.
• Domain documents
  Domino creates Domain documents to set up and configure Domino domains. You can create Global domains, which group Domino domains into a single Internet domain; Adjacent domains, which are connected to each other; Non-adjacent domains, which act as intermediaries between two unconnected domains; and Foreign domains, which use different mail systems from Notes mail.
  For more information on Global Domain documents, see Chapter 11.

• Network documents
  Domino creates a Network document for each Domino named network you set up. Network documents list the network name, servers in the network, network title, and network administrator.

• Program documents
  You create Program documents to schedule and run server programs. Program documents give you greater control over when a program runs than you have by modifying the server NOTES.INI file. Run OS/2 command files, Domino server programs, API programs, UNIX shell scripts, or UNIX programs with Program documents.

• Setup Profile documents
  You create Setup Profile documents to configure Notes workstation settings for users. Use profiles to set up batches of users who have the same default settings.

To ensure system security and efficiency, limit access to the Public Address Book through the database ACL by using access levels, permissions, and roles. With roles, you can decentralize and delegate administration securely.

---

About improving Public Address Book performance

**Improving the lookup time**

To speed the lookup time for the Public Address Book, create a group called Frequent Users. Groups are processed faster than either views or server access lists. Add the Frequent Users group to the Access server field in the appropriate Server document. If Domino finds the user in the Frequent Users group first, it doesn't look for that user in the Public Address Book.

**Improving performance of the Administration server**

Processing a request to rename a server in the Public Address Book may slow down the performance of the Administration server. To minimize this, perform the following steps on the Administration server for the Public
Address Book when the Rename Server in Address Book request appears in the Administration Request database.

- Shut down the Update, Router, and Replicate server tasks.
- Enter a Tell Adminp Process New command from the server console.
- When the status of the Administration Process is idle, load the Updater task to update the view indexes of the Public Address Book.
- When the Updater is idle, restart the Router and Replicator tasks.
- Use the Push server command with the name of the server whose name is changing to force replication of the modified Public Address Book to the upgraded server.

For more information on setting up the Administration Process and on server tasks, see chapter 7 in *Getting Started with Domino*. For more information on creating groups in the Public Address Book, see Chapter 3 in *Getting Started with Domino*. 
Chapter 9
Deploying Clients

Domino supports a wide variety of clients, from basic Web browsers to the Notes client, the industry’s most fully-featured client. You can deploy Domino in your organization and take advantage of existing applications like POP3 and IMAP e-mail clients, news readers based on NNTP, browsers, as well as leveraging the features of Notes. Many organizations use a heterogeneous client mix.

About deploying clients

Once you have selected and purchased clients, deploy them to users. There are several ways to distribute clients, depending on your organization and its infrastructure. Some employees may be using network computers; to make the software available to them, place it on their servers and let them know how to access it. If you are using UNIX servers and workstations, distributing clients via a network can save time. Do security and access restrictions on UNIX machines need to be modified to allow administrators to install and configure the software on different hosts? For PCs, you can place client software on a file server, distribute CD-ROMs or disks, or use a node install (on certain platforms). In addition, you can use systems management software to deploy Notes clients. For more information, see http://www.lotus.com/systems/.

For more information on installing Notes client software, see the Notes Designer for Domino Install Guide and the Domino Install Guide.

All Domino users require the following:

- A mail file on a Domino server, known as the user’s home or mail server. Your Domino administrator creates a mail file for each user. Users who access Domino only via news reader clients and who do not use e-mail do not need mail files.
- A Person record in the Public Address Book, regardless of client. This allows you to control access to servers, databases, and database elements. Person records are created for Notes users automatically when you create a Notes user ID file.
- Information on what protocol and connection type users have to access Domino servers.
• Information on how users connect to the Internet, including Domino server name or Web server address, browser type, proxy configuration, and Internet e-mail address.
• Training on how to use the client software, any messaging product such as Lotus Mail, and Notes databases.

For more information, see Chapter 2.

**Deploying Notes clients and creating Notes users**

Notes users and clients enjoy increased functionality and enhanced security compared to other client software. Before setting up Notes on a workstation, create a Notes user ID file for the user is the primary user for that workstation. A Domino administrator creates ID files from the Administration Control panel of a Domino server, specifying the following:

• Certifier used to certify the ID, verifying the association of its public and private key
• Home/mail server
• Security encryption type (North American or International encryption algorithm)
• ID expiration date (when the user’s ID must be recertified by)
• User name (first, last, middle initial)
• Minimum password length
• Initial password (which can be changed by the user)
• Mail file name and whether to create it now or when the user sets up the workstation
• Where the ID file is stored (in the Public Address Book or in a file, such as on a disk)
• On Windows NT platforms, whether to create an NT user account and synchronize the NT and Notes passwords

Administrators can register (create user IDs for and enter into Person records in the Public Address Book) users by file, by profile, or use automated installations for increased efficiency. This lets you standardize user and workstation configuration, reducing maintenance and user confusion. In addition, automated installation lets users or software distribution programs install Notes without requiring the attention of an administrator for each installation.
**Common Setup Profile**

You can create a Setup Profile to configure workstation default options for users. Create a Setup Profile in the Public Address Book and specify an Internet browser, how Web pages should be retrieved, a default passthru server, databases to add to the workspace, default remote servers, Java applet security options, proxy configuration settings, and secondary NDS and TCP/IP servers. Use profiles to set up batches of users who have the same default settings. For example, you create user IDs and set up workstation defaults for your Sales force, who access the same remote server and need the same databases on their desktop. Create a profile called Sales with these options and use it to create these users. You can create multiple profiles.

**Register multiple users**

Registering users from a text file lets you decide on options and then go through the setup process with the Administration Control Panel only once. You can generate lists of users from existing lists to save time. For example, you copy a human resources list of employees in one group and use this list to create a text file to create user IDs for these employees. As with creating users individually, you can set up Windows NT accounts at the same time you create Notes user IDs.

All users in a registration file must be registered with the same certifier. You must create a separate text file for each organizational unit (OU) certifier you will use.

**Automated installation**

With automated installation, you can have options automatically selected during the Notes workstation installation and setup. Edit the installation response file (.RSP extension) provided with the Notes software. You can create multiple response files for different customized installations. Users select the appropriate response file during installation and no further user interaction is needed for installation and setup. In addition, you can use response files with software distribution programs to install the Notes workstation, appropriately configured, automatically. Installation and setup using response files are available for Windows and OS/2 workstations.

To aid users in adding the correct databases to their desktop, create portfolios or database libraries containing the desired databases. You can put portfolios and libraries on a server and instruct users to access them after workstation setup.
**About distributing Notes IDs**

When you create user ID files for Notes users, you can store the IDs in each user’s Person document in the Public Address Book or store the ID as a file on a computer or disk. ID files stored in Person documents must be protected by a password. Consider how to distribute passwords to users in a secure fashion.

When you create passwords for Notes ID files, make each password using unique random alphanumeric passwords at least 13 characters long for maximum security. Have users change their password upon receiving the ID file, and instruct them not to use names, birthdays, employee numbers, social security numbers, or other items as passwords. Passwords using these prompts are easily guessed. If users want to use words, have them incorporate several words into a phrase. This is easy to remember and reduces security risk. Caution users not to write down passwords.

You can retain a backup copy of each user’s ID file in case that user forgets the password or leaves the company. However, multiple copies of Notes ID files present a significant security risk; the public-private key Notes encryption and security algorithm depends on the protection of the private key on the Notes ID file. If you create backup ID files, implement a security plan to protect the IDs. If they have passwords, store the passwords and ID files separately and do not give anyone access to both passwords and IDs. If you create backup IDs without passwords, store them so that no one can access the files alone. Set up a monitoring system to audit access to the IDs.

**About communication**

Domino servers and Notes clients are connected over a network. Server-to-server and client-to-server connections can take one or a combination of these forms:

- Always connected through a local area network (LAN) or a wide area network (WAN)
- Sometimes connected through a communications port used for dial-up connections
- Sometimes connected via remote LAN service
- Connected through both LAN/WAN and a dial-up port

For information on network configurations, see *Configuring the Domino Network*. 

---

86 Planning the Domino System
E-mail allows organizations to share information, exchange files, and work together while separated by time and space. Many organizations use a mix of e-mail products: LAN-based products like cc:Mail, mainframe systems, Internet mail, and Notes mail. Domino works as a messaging server and allows you to host a heterogeneous mix of mail programs and clients. Your mail deployment varies depending on which types of mail you are using and the clients that you want to access Domino servers. You can purchase migration tools to help you move your organization from older mail products to Domino.

About deploying mail

The purpose of e-mail is to broaden communication. This means considering the e-mail strategies of your clients, partners, suppliers, vendors, and others with whom you wish to communicate - you will almost certainly need to translate between different formats and programs. Domino makes this easy with Message Transfer Agents (MTAs), scalable server tasks that are superior to gateways. The MTAs route messages in their native format without having to convert messages to an intermediate form. Lotus offers MTAs for SMTP/MIME, cc:Mail, and X.400. Using Domino and MTAs, you can communicate easily in an organization that uses multiple mail programs and with people outside your organization who use different e-mail formats.

Notes mail has rich features including support for graphics, images, audio, video, Java applets, OLE, and ActiveX. Security features include digital signatures, encryption based on a public-private key RSA cryptosystem, and an Execution Control List (ECL) that protects against viruses and embedded programs. You can use full text indexing to search your mail and intelligent agent technology to manage it.
About deploying Domino as a mail server

Domino is designed to be a full-featured, multi-protocol mail server. For businesses that want a mail server without running applications, Lotus offers the Domino Mail server. Organizations looking to leverage Domino applications on their intranet and Internet choose the Domino server, which includes all of the capabilities of a Mail server with the ability to host applications. Deploying mail is identical for both servers.

Smaller companies with only a few servers host a variety of tasks on each Domino server. Larger organizations, especially enterprise-scale ones, typically dedicate servers as mail servers due to the large volume of mail they encounter. Dedicating mail servers lets you use all of a server’s resources to handle mail, streamline mail administration and troubleshooting, and minimize mail disruption. Organizations frequently cluster mail servers with Domino Advanced Services to ensure mail availability.

Domino allows you to establish a single mail file for all of your mail, whether Notes mail or Internet mail. You can access your mail from a Notes client, a browser using the Web mail template, or a POP3 client. This gives you the flexibility to manage your mail from multiple locations and with different clients.

Domino hosts mail files and routes the mail sent from them. A server task called Router moves sent mail from the outgoing message store to the Inbox of the recipient’s mail file. If necessary, an MTA converts the e-mail between formats, such as from Notes Mail to MIME. Mail routing depends on where the message’s author and recipient have their mail files, the priority level of the message, and the message format.

Planning mail routing in a Domino system

Mail routing depends on the mail infrastructure, the destination of a message, and the priority. To plan for mail routing, you must consider the following concepts:

- A domain groups Domino servers, allowing you to administrate and control them easily. All servers in a domain have the same Public Address Book, which is the Domain’s control center, containing all of the documents necessary to route mail, connect servers, administer users, and configure servers. To send mail to another user in the same domain, enter the person’s name in the To field of a memo. To send mail to a user in another domain, enter the person’s name and the domain in the To field.
A Domino named network is a subgroup of Domino servers that are physically connected. Domino treats a Domino named network as physically separate and distinct, even if it is connected to other servers and other Domino named networks. Mail routes automatically in a Domino named network and does not require Connection documents for delivery. A server’s Domino named network is listed in its Server record in the Public Address Book.

A Connection document specifies how and when two servers connect, usually to exchange mail and to update common databases through replication. You need a Connection document from each server to the other to route mail.

A routing table is a list of connections from a Domino server to all other servers it can contact. Domino assembles this table when the server starts by searching the Server, Connection, and Domain documents in the Public Address Book. Domino uses the routing table to determine the best, least-cost path to deliver mail.

A router is the Domino server task that moves mail messages between the sender’s mail file and the recipient’s mail file.

A MAIL.BOX file is the Domino mailbox; all outgoing and incoming mail on a server is held in MAIL.BOX until it is delivered. Mail is transferred from the sender’s mail file to MAIL.BOX before being routed. Routing moves the message from MAIL.BOX on the sender’s server to MAIL.BOX on the recipient’s server. Domino then moves the message from MAIL.BOX to the recipient’s mail file.

A home server for a given user is the server on which that user’s mail file is located.

A Message Transfer Agent (MTA) routes and converts messages from different formats, such as MIME and Notes mail.

Mail routing occurs on the backbone of your mail infrastructure, including your domain and Domino named network setup. When planning mail routing, consider the following tips:

- Designate one server in each domain to connect to other domains.
- Designate one server in each Domino named network to connect to other Domino named networks.
- Use shared mail to reduce network traffic and the space needed to store mail.
- Use the mail trace feature in Domino to see the fastest route for mail and to debug routing problems.
- Schedule mail routing and replication together as tasks in Connection documents. This minimizes the number of Connection documents you need to create and reduces network traffic.
**About mail routing and the Internet**

Internet mail routes on the Domino mail infrastructure. Mail routing and transport take place via SMTP with messages in MIME format. You must set up the SMTP/MIME MTA on at least one server in your organization to use Internet mail.

Notes mail users can send mail easily to Internet mail users and vice versa. Domino supports POP3 and IMAP. These protocols specify how mail is stored on a server and how a client retrieves it. Users whose mail files reside on a Domino server can send Internet mail to one of two destinations: to a recipient outside their organization, or to a recipient inside their organization.

If the mail is intended for a recipient outside an organization, Domino moves the message via the router to a server running the SMTP/MIME MTA. Mail routing to the MTA takes place on the Notes mail infrastructure as though the message were a Notes mail message intended for the SMTP/MIME MTA as a destination server. Once the message reaches the MTA, the MTA contacts the recipient’s POP3/IMAP server and delivers the message to it via SMTP. You can install the SMTP/MIME MTA on any Domino 4.6 server in your organization.

If the mail is intended for a recipient inside an organization, Domino routes the mail to the SMTP/MIME MTA, which looks in its Public Address Book to find the server on which the recipient’s mail file is located. The MTA routes mail on the Notes mail infrastructure to the destination server. This takes place whether the recipient uses Internet mail or Notes mail.

**Note** Users who have POP3 or IMAP mail files cannot receive or read encrypted mail.

**How mail travels between Notes and the Internet**

- A Notes user addresses a Notes message to an SMTP address — for example, Joe@acme.com.
- The Notes Mail Router identifies the address as an SMTP address based on the syntax. It looks in the Public Address Book at the Foreign SMTP Domain documents and the SMTP Connection documents to determine the Notes server running the appropriate SMTP/MIME MTA.
- The Notes Mail Router then routes the message to the SMTP MTA server, where the SMTP.BOX database stores the message.
- The Outbound Conversion Handler task polls SMTP.BOX at regular intervals for new messages. When it finds a message, it converts it from Notes format to RFC822 format and writes it to the Outbound Work Queue. It also updates the message in SMTP.BOX to indicate that it is pending transmission.
The Outbound Session Controller reads the message from the Outbound Work Queue and notifies (or creates) an Outbound Session Handler task passing the message ID. The Outbound Session Controller can launch up to three handlers by default; however, you can configure it to launch a maximum of eight handlers. If possible, the controller groups message for the same host to reduce overhead.

The Outbound Session Handler retrieves the message from the work queue. It resolves the specified Destination Host to an IP address, opens a connection to the destination, and sends the message through the SMTP protocol driver. It then changes the state of the message in the Outbound Work Queue to Sent.

The Delivery Report Task removes the message from the Outbound Work Queue and SMTP.BOX. If the message experiences a temporary failure — for example, if the destination was unavailable — the message will be requeued to be resent later. If the message experiences a permanent failure — for example, if the destination host is unknown or the user on that host is unknown — the Delivery Report Task generates and sends a Non-delivery Report to the sender and removes the original message from the Work Queue and SMTP.BOX.

How mail travels from the Internet to Notes

- The Inbound Session Controller Task listens on the well-known SMTP socket to respond to connection requests. When a connection request comes in, the Inbound Session Controller notifies (or creates) an Inbound Session Handler to process the message. The Controller can launch up to three handlers by default; however, you can configure it to launch a maximum of eight.
- The Inbound Session Handler receives the SMTP message and writes it to the inbound work queue in RFC822 format.
- The Inbound Message Conversion task reads the message out of the Inbound Work Queue. If the message is not addressed to a configured list of Internet domains in the Global Domain document(s), it passes the message on to the outbound work queue to be sent to the correct destination. If the address is recognized, the address is converted to a Notes address. If the message is deliverable, it is converted to Notes format and placed in MAIL.BOX for the Notes Mail Router to deliver. If the message fails to be routed to a destination or fails conversion, the conversion task will indicate this in the message so that Delivery Report Task can take appropriate action.
- The Delivery Report Task polls the Inbound Work Queue and deals with the message accordingly, either deleting it or placing a Non-Delivery Report in the Outbound Work Queue.
About the components of the SMTP MTA

When the SMTP/MIME MTA runs on a Domino server, it uses a number of tasks and databases to process messages. Below is a picture of the components of the SMTP/MIME MTA.

Add-in Controller

The Add-in Controller (task name: SMTPMTA) is the task that is loaded on the Domino server. It acts as a control point for all the other tasks. All commands for the MTA are sent to the Add-in Controller and it notifies the necessary child processes — for example, Tell SMTPMTA Quit.

Outbound Message Conversion

The Outbound Message Conversion task (task name: SMTPMTA OMSGCNV) converts Notes messages into a SMTP/MIME format ready for transmission. The format of the SMTP message and the conversion of Notes addresses to SMTP Addresses is fully configurable.

Outbound Session Controller

The Outbound Session Controller (task name: SMTPMTA OSESCTL) controls the transport of the converted messages to their respective SMTP destinations. It launches or notifies one or more session handlers to perform the transport of the message or messages to a particular destination.
Outbound Session Handler(s)

The Outbound Session Handler(s) (task name: SMTPMTA OSESHLRn) are child processes of the Outbound Session Controller. The handlers perform the actual tasks of connecting to the destination or next hop in the SMTP system, delivering the message(s) and passing back any errors, either temporary or permanent.

Inbound Message Conversion

The Inbound Message Conversion Task (task name: SMTPMTA IMSGCNV) converts messages received by the Inbound Sessions Handler(s) to a Notes format. It also converts the destination user address to a Notes format and checks that this address is deliverable. If the message is not convertible or the address not deliverable, the Inbound Message Conversion Task indicates the message has failed delivery so that a Non-delivery Report can be generated. If the message is not destined for Notes, it puts the message into the work queue for the Outbound Transport.

Inbound Session Controller

The Inbound Session Controller (task name: SMTPMTA ISESCTL) controls the receiving of messages from other SMTP systems. It listens on the SMTP port 25 and accepts the initial incoming connection. It then launches or notifies an Inbound Session Handler to take the connection so that it can listen for a new connection.

Inbound Session Handler(s)

The Inbound Sessions Handler(s) (task name: SMTPMTA ISESHLRn) accept incoming connections from the Inbound Session Controller. They perform the SMTP protocol handshaking with the sending system and write the incoming data to the work queue.

Delivery Report Task

All the other SMTP MTA tasks perform specific functions. For each message, each task indicates whether or not that task was successful and whether a temporary or permanent error occurred. The Delivery Report Task processes the messages in the work queues depending on their status. The Delivery Report Task deletes all messages that have been successfully sent or received. For messages that have a permanent failure, the Delivery Report Task generates a Non-delivery Report or Undeliverable Message Notification back to the sender and also notifies the administrator.
About databases that the SMTP MTA uses

The transient message databases (SMTP.BOX, SMTPOBWQ.NSF, SMTPIBWQ.NSF) are compacted automatically once a day by the Add-in Controller at a specified time, defined in the Perform daily housekeeping at: field on the Server document.

SMTP mail box (SMTP.BOX)

The install program creates the SMTP.BOX database from the SMTPBOX.NTF. The Domino Router places Notes messages in this database to be converted. The Outbound Message Conversion task polls this database for work at a configurable interval. Messages are not removed from this database by the Delivery Report Task until they are successfully sent or a Non-Delivery report is generated for them.

Outbound work queue (SMTPOBWQ.NSF)

The SMTP Outbound Work Queue is used a temporary storage area for messages that have been converted by the Outbound Message Conversion task and are pending transport, or transport has been attempted and are pending processing by the Delivery Report Task.

Inbound work queue (SMTPIBWQ.NSF)

The SMTP Inbound Work Queue is used as a temporary storage area for messages that have been received by an Inbound Session Handler and are either pending conversion or pending processing by the Delivery Report Task.

MTA Tables database (MTATABLES.NSF)

Both the SMTP/MIME MTA and X400 MTA use the MTA Tables database. It acts as a lookup table for character set and file type identification routines in the MTAs and also as a cross reference table between MIME type/subtypes and file extensions.

MTA Forms database (MTAFORMS.NSF)

The MTA Forms database is built from the Mail template (MAIL46.NTF) at install time. It is used to render Message content in outbound messages. If your organization is using custom letterhead subforms then they need to be added to this database to allow the message to be rendered, even though the letterhead doesn’t appear in the resulting message.

For more information, see Appendix B in *Maintaining the Domino System.*
About configuring the SMTP/MIME MTA

Depending on your needs, the type of topology you plan to use affects how you configure your MTA(s). All configuration changes are made within the Public Address Book. All configurations require a minimum of one each of the following documents:

- The Global Domain document contains the name(s) of your organization as it is known by to the outside world. Most companies want to be known by one name (for example, ACME.COM), and they register that with their Internet provider. In some cases, a company may have more than one name. This is a common practice of companies that have merged with other companies having an historical domain name.

- The Foreign SMTP Domain document defines which addresses are to be considered Internet Addresses and to which Domino domains (real or virtual) these messages should be sent. It also allows you to restrict access through your server, thus creating a more secure environment.

- The Server Connection document creates a logical link between the MTA and the Foreign SMTP domain.

- The Server document identifies the MTA to the server upon which it resides. It also links to the Global Domain document, so that the MTA is identified with the Global Domain.

Note that for each scenario, the number of documents or the fields used within a document may change. For example, some scenarios require key changes to the Server document, while others might require changes only to the Server Connection document.

For the purpose of illustration, all examples are built on the same basic scenario. Only documents with changes are shown in each scenario.

Preparing to configure the MTA

Before you configure the SMTP/MIME MTA:

1. Use the Ping utility to test your LAN and WAN connections.

2. Determine the local host name for the server where the SMTP MTA resides by typing hostname at the operating system prompt.

3. Define a list of the inbound Internet addresses your organization is known by and from which the SMTP MTA accepts mail. In some cases, a company may have multiple Internet addresses, for example companies that have been absorbed other companies may use an historical domain name.
4. Decide the format your organization uses for inbound address, for example:
   - @acme.com
   - @sales.acme.com
   - @mail.acme.com

5. Make sure that the inbound Internet mail addresses for the MTA server are defined in the Domain Name System (DNS).

6. If your company site uses a mail relay system or a firewall for security reasons, find out the full name or IP address for that system (for example, 130.000.00.00). Ensure you have connectivity to that system.

**Using the Ping utility to test connectivity**

Use the Ping utility to check LAN and WAN (to Internet) communications connectivity before you send Notes SMTP mail. The Ping utility (part of the TCP/IP) initiates a basic connectivity test between your computer and the destination computer’s communications protocol software. The Ping utility indicates whether there has been a successful packet transfer between SMTP hosts.

If you have Internet connectivity through an Internet Service Provider, test the communications path to a node on the Internet. Before running the Ping utility to test the WAN connection, you must define the destination host system with which you wish to communicate in either the local hosts file or the Domain Name System (DNS). Either the local hosts file or the DNS provides mapping between the destination host’s domain name and its IP address.

To run the Ping utility, type ping, followed by the domain name. For example, type:

```
ping xyz.com
```

If successful, the Ping utility returns a message in a format similar to the following:

```
64 bytes from 130.000.00.00: icmp_seq=4, time=0, ms
```

**About connecting SMTP/MIME MTAs**

Before configuring your SMTP/MIME MTA, consider these scenarios:

- Connecting one SMTP/MIME MTA directly to the Internet
- Accessing the Internet through a firewall or other mail relay system
- Accessing the Internet through a firewall with intranet messages delivered directly to the SMTP/MIME MTA
- Using one MTA for Internet messages and one MTA for intranet messages
About connecting one SMTP/MIME MTA directly to the Internet

A company can send mail back and forth between Domino and the Internet using a single SMTP/MIME MTA that has access directly to the Internet. To do this, the company must:

- Be registered with an Internet service provider (ISP).
- Have their domain name service (DNS) set up to have a mail exchange (MX) record for their Internet address (if required) and an Address (A) record to the server where the MTA resides.
- Configure the Public Address Book to contain the minimum documents required to install an SMTP/MIME MTA.

Example: Connecting one SMTP/MIME MTA directly to the Internet

Acme Company has a working SMTP connection and is registered with the Internet service provider as acme.com. They have one Notes domain called SEAFOOD. SEAFOOD contains several Domino servers (Lobster, Crayfish, and Shrimp), but only Lobster/SEAFOOD contains an SMTP/MIME MTA. Therefore, any mail originating in Crayfish or Shrimp that is using SMTP to send messages to the Internet must route through the MTA on Lobster.

So that all mail from the Internet can get to the MTA on Lobster/SEAFOOD, SEAFOOD is a member of the global domain, ACMEGlobal. All Internet mail to and from the SMTP/MIME MTA global domain is addressed @acme.com. All messages that have an address containing a period after the @ sign are seen as an Internet address by Domino and are routed to the MTA.

Public Address Book Requirements

For this scenario, you can generally use the default field values in each document.
One Global Domain document. You may need to create a new
document. You must complete or add information in the following
fields: Domain type, Global Domain name, Global domain tasks, and
the Internet domain suffix(es). The X.400 address conversion fields are
not applicable unless you are also configuring an X.400 MTA on the
same server.

**DOMAIN: AcmeGlobal**

<table>
<thead>
<tr>
<th>Basics</th>
<th>Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain type</td>
<td>Global Domain</td>
</tr>
<tr>
<td>Global domain name</td>
<td>AcmeGlobal</td>
</tr>
<tr>
<td>Global domain role</td>
<td>SMTP MTA</td>
</tr>
</tbody>
</table>

**SMTP Address Conversion**

- Outbound mail restriction: Unrestricted
- Address domain: acme.com
- Internet address lookup: Disabled
- Local mail enabled: Full name
- Notes domain(s) included: All
- Notes domain(s) positions: Left of @
- Notes domain separation: `%`
- Address example: JOE%JOE%JOE@acme.com

**X.400 Address Conversion**

- Outbound mail restriction: Restrict to global domain
- Country name: 
- ADM name: 
- FRM name: 
- Notes domain attribute: 

One Foreign Domain document. You may need to create a new
document. You must complete the following fields: Domain type and
the Domain name (under Should be Routed to). In this configuration,
messages addressed to Internet Domain are wildcarded (`*.*`). This means
that any mail message having an Internet address should be routed to
the domain name chosen for the configuration; for example TheInternet.

**DOMAIN: *.***

<table>
<thead>
<tr>
<th>Basics</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain type</td>
<td>Foreign SMTP Domain</td>
</tr>
</tbody>
</table>

**Messages Addressed to**

- Internet Domain: `*.*`

**Should be Routed to**

- Domain name: TheInternet

98 Planning the Domino System
- One Server Connection document. You may need to create a new document. You must complete the following fields: Connection Type, Source server, Destination server, Destination domain. The Destination domain is defined as the target for the Foreign SMTP domain. The name in this field is arbitrary and should not be the same name chosen for the Source server.

**SERVER CONNECTION: Lobster/Seafood to All Internet Hosts**

<table>
<thead>
<tr>
<th>Basics</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection type</td>
<td>SMTP</td>
<td></td>
</tr>
<tr>
<td>Source server</td>
<td>Lobster/Seafood</td>
<td>Seafood</td>
</tr>
<tr>
<td>Source domain</td>
<td>Seafood</td>
<td></td>
</tr>
<tr>
<td>Direct connection</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scheduled Connection</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection</td>
<td>ENABLED</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Routing and Replication</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing cost</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

- One Server document. You must edit the server document for the server containing the MTA. You must complete the following fields: Routing tasks, Global domain name, and Fully qualified Internet host name.

**SERVER: Lobster**

<table>
<thead>
<tr>
<th>Basics</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Server name</td>
<td>Lobster</td>
<td></td>
</tr>
<tr>
<td>Server title</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain name</td>
<td>Seafood</td>
<td></td>
</tr>
<tr>
<td>Cluster name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Master address book name</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Internet Message Transfer Agent (SMTP MTA)</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Global domain name</td>
<td>AcmeGlobal</td>
<td></td>
</tr>
<tr>
<td>Fully qualified Internet host name</td>
<td>Lobster.Acme.com</td>
<td></td>
</tr>
<tr>
<td>MTA administrator</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Control</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Poll for new messages every</td>
<td>120</td>
<td></td>
</tr>
<tr>
<td>MTA work poll</td>
<td>c:Waste&amp;mailwork</td>
<td></td>
</tr>
<tr>
<td>Debug level</td>
<td>Normal</td>
<td></td>
</tr>
<tr>
<td>Enable daily housekeeping</td>
<td>Enable</td>
<td></td>
</tr>
<tr>
<td>Perform daily housekeeping at</td>
<td>07:00 AM</td>
<td></td>
</tr>
</tbody>
</table>

Chapter 10: Deploying Mail  99
About accessing the Internet through a firewall or other mail relay

For security reasons, a company can set up a firewall or use a mail relay system to forward the mail between the MTA and the Internet. As is true with a direct connection to the Internet, the organization must be registered with a Internet service provider, and their DNS must be set up to have a mail exchange (MX) record for their Internet address to the Relay/Firewall (if required for inbound mail) and an Address (A) record to the server where the MTA resides. You must configure the Public Address Book to contain the minimum documents required to install an SMTP/MIME MTA.

Example: Accessing the Internet through a firewall or other mail relay system

Acme Company has a working SMTP connection and is registered with the Internet service provider as acme.com. They have one Domino domain called SEAFOOD. SEAFOOD contains several Domino servers (Lobster, Crayfish, and Shrimp), but only Lobster/SEAFOOD contains an SMTP/MIME MTA. Therefore, any mail originating in Crayfish or Shrimp that is using SMTP to send messages to the Internet must route through the MTA on Lobster.

This configuration differs from Example 1 (Connecting one SMTP/MIME MTA directly to the Internet) in that mail needs to route to another system (for example, 130.000.00.00) rather than connect directly to the Internet. This other system does not need to be part of the Domino network, but it does need to have a direct connection to the MTA server.

Public Address Book requirements

For this scenario, you can generally use the default field values in each document, except where specified.
• One Global Domain document. You may need to create a new document. You must enter information in the following fields: Domain type, Global Domain name, Global domain tasks, and the Internet domain suffix(es).

• One Foreign Domain document. You may need to create a new document. You must enter information in the following fields: Domain type and the Domain name (under Should be Routed to).

• One Server Connection document. You may need to create a new document. You must enter information in the following fields: Connection Type, Source server, Destination server, Destination domain. To indicate the firewall or relay to be used, you must also indicate the Optional network address name or the IP address of that system.

SERVER CONNECTION: Lobster/Seafood

<table>
<thead>
<tr>
<th>Basics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection type</td>
<td>SMTP</td>
</tr>
<tr>
<td>Source server</td>
<td>Lobster/Seafood</td>
</tr>
<tr>
<td>Connect via</td>
<td>Direct connection</td>
</tr>
<tr>
<td>Usage priority</td>
<td>Normal</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Delivery domain</th>
<th>TheInternet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relay/exit</td>
<td>192.0.0.1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scheduled Connection</th>
<th>Routing and Replication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection:</td>
<td>Tasks:</td>
</tr>
<tr>
<td>enabled</td>
<td>SMTP Mail Routing</td>
</tr>
<tr>
<td>Calls at Night</td>
<td>Route at Once:</td>
</tr>
<tr>
<td>00:00:00 AM - 10:00:00 PM each day</td>
<td>5 messages pending</td>
</tr>
<tr>
<td>Repeat interval:</td>
<td></td>
</tr>
<tr>
<td>360 minutes</td>
<td></td>
</tr>
<tr>
<td>Days of Week:</td>
<td></td>
</tr>
<tr>
<td>Sun, Mon, Tue, Wed, Thu, Fri, Sat</td>
<td></td>
</tr>
</tbody>
</table>

• One Server document. You must edit the server document for server containing the MTA. You must enter information in the following fields: Routing tasks, Global domain name, and Fully qualified Internet host name.

About accessing the Internet through a firewall with Intranet messages delivered directly

What if your organization needs to access an internal network (an intranet), as well the Internet? You still want to set up a firewall or use a mail relay system to forward the mail between the MTA and the Internet because that keeps your systems secure. However, you may want to access your Intranet directly without going through a firewall.

You still must register your organization with an Internet service provider, and their DNS must be set up to have a mail exchange (MX) record for their Internet address to the Relay/Firewall (if required for inbound mail) and an
Address (A) record to the server where the MTA resides. They must then configure the Public Address Book to contain the minimum documents required to install an SMTP/MIME MTA.

**Example: Accessing the Internet through a firewall with Intranet messages delivered directly**

Acme Company has a working SMTP connection and is registered with the Internet service provider as acme.com. They have one Domino domain called SEAFOOD. SEAFOOD contains several Domino servers (Lobster, Crayfish, and Shrimp), but only Lobster/SEAFOOD contains an SMTP/MIME MTA. Therefore, any mail originating in Crayfish or Shrimp that is using SMTP to send messages to the Internet must route through the MTA on Lobster.

Additionally, Acme has an Intranet, where Notes messages can be transferred without going through the firewall. Because these messages have an SMTP address, they are also processed through the SMTP/MIME MTA on Lobster.

**Public Address Book requirements**

For this scenario, you can generally use the default field values in each document, except where specified.

102 Planning the Domino System
- One Global Domain document. You may need to create a new document. You must enter information in the following fields: Domain type, Global Domain name, Global domain tasks, and the Internet domain suffix(es).

- Two Foreign SMTP Domain documents.
  - One Foreign SMTP Domain document routing to the Internet. All SMTP mail that is addressed to the Internet domain *. automatically routes to the virtual domain name, TheInternet.
  - One Foreign SMTP Domain document routing to the Intranet. All SMTP mail that is addressed to the domain *.acme.com automatically routes to the virtual domain name, TheIntranet. The MTA recognizes that acme.com is internal and therefore routes the mail to the Intranet rather than sending it outside to the Internet.

### DOMAIN: *.acme.com

<table>
<thead>
<tr>
<th>Basics</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain type: Foreign SMTP Domain</td>
<td>Allow mail only from domains:</td>
</tr>
<tr>
<td>Deny mail from domains:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Messages Addressed to:</th>
<th>Should be Routed to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Domain: *.acme.com</td>
<td>Domain name: TheIntranet</td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Internet host:</td>
<td></td>
</tr>
</tbody>
</table>

### DOMAIN: *.*

<table>
<thead>
<tr>
<th>Basics</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain type: Foreign SMTP Domain</td>
<td>Allow mail only from domains:</td>
</tr>
<tr>
<td>Deny mail from domains:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Messages Addressed to:</th>
<th>Should be Routed to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Domain: *</td>
<td>Domain name: TheInternet</td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Internet host:</td>
<td></td>
</tr>
</tbody>
</table>
Two Server Connection documents.

One Server Connection document for the Internet. You may need to create a new document. You must enter information in the Connection Type and Source server fields. The Destination domain must match the domain entered in the foreign domain document (TheInternet). This field should not be the same name chosen for the Source server. You can give a virtual name for the Destination server (All Internet Hosts). To indicate the firewall or relay to be used, you must also indicate the Optional network address name or the IP address of that system.

One Server Connection document for the Intranet. You must create a new document. You must enter information in the Connection Type and Source server fields. The Destination domain must match the domain entered in the foreign domain document (TheIntranet). This field should not be the same name chosen for the Source server. You can give a virtual name for the Destination server (Local SMTP Hosts).

**SERVER CONNECTION: Lobster/Seafood**

<table>
<thead>
<tr>
<th>Basics</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection type</td>
<td>SMTP</td>
<td></td>
</tr>
<tr>
<td>Source server</td>
<td>Lobster/Seafood</td>
<td></td>
</tr>
<tr>
<td>Connects</td>
<td>Direct connection</td>
<td></td>
</tr>
<tr>
<td>Usage priority</td>
<td>Normal</td>
<td></td>
</tr>
<tr>
<td>Destination domain</td>
<td>TheInternet</td>
<td></td>
</tr>
<tr>
<td>Relay host</td>
<td>123.45.67.89</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scheduled</th>
<th></th>
<th>Routing and Replication</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection</td>
<td>ENABLED</td>
<td>Protocol</td>
<td>SMTP Mail Routing</td>
</tr>
<tr>
<td>Call at</td>
<td>08:00 AM - 10:00 PM each day</td>
<td>Route at once if</td>
<td>5 messages pending</td>
</tr>
<tr>
<td>Repeat interval</td>
<td>360 minutes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Days of week</td>
<td>Sun, Mon, Tue, Wed, Thu, Fri, Sat</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
One Server document. You must edit the server document for the server containing the MTA. You must enter information in the following fields: Routing tasks, Global domain name, and Fully qualified Internet host name.

About using one MTA for Internet messages and one MTA for Intranet messages

This scenario is similar to accessing the Internet through a firewall with Intranet messages delivered directly, except that two MTAs are used to handle the messaging load. In this example, Internet message traffic should not impact the throughput of messages to other local systems. For this configuration to work correctly, there are two ways you can set up the DNS.

You can register your organization with an Internet service provider, and their DNS must be set up to have a mail exchange (MX) record for the Internet address to the Relay/Firewall (if required for inbound mail) and an Address (A) record to the each server where an SMTP/MIME MTA resides. You must then configure the Public Address Book on each MTA server, to contain the minimum documents required to install an SMTP/MIME MTA.

For more information, see “Using one MTA for Internet messages and one MTA for Intranet messages.”

Example: Using one MTA for Internet messages and one MTA for Intranet messages

Acme Company has a working SMTP connection and is registered with the Internet service provider as acme.com. It has one Domino domain called SEAFOOD. SEAFOOD contains several Domino servers (Lobster, Crayfish, and Shrimp). Lobster/SEAFOOD and Shrimp/SEAFOOD each contain an SMTP/MIME MTA.
Lobster/SEAFOOD is configured to send and receive mail to the Internet. This scenario could be configured for either a direct connection or to pass through a firewall. Shrimp/SEAFOOD is configured to send and receive SMTP mail from the Intranet. Any messages received from the Internet destined for any of the servers, must go through Lobster/SEAFOOD. Any messages received from the Intranet destined for any of the servers, must go through Shrimp/SEAFOOD.

Public Address Book requirements
For this scenario, you can generally use the field values in each document, except where specified.

- One Global Domain document. You may need to create a new document. You must enter information in the following fields: Domain type, Global Domain name, Global domain tasks, and the Internet domain suffix(es).
- Two Foreign SMTP Domain documents.
  - One Foreign SMTP Domain document routing to the Internet. All SMTP mail that is addressed to the Internet domain *. automatically routes to the virtual domain name, TheInternet.
• One Foreign SMTP Domain document routing to the Intranet. All SMTP mail that is addressed to the domain *.acme.com automatically routes to the virtual domain name, TheIntranet. The MTA recognizes that acme.com is internal and therefore routes the mail to the Intranet rather than sending it outside to the Internet.

<table>
<thead>
<tr>
<th>Domain: *.acme.com</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basics</strong></td>
</tr>
<tr>
<td>Domain type</td>
</tr>
<tr>
<td><strong>Restrictions</strong></td>
</tr>
</tbody>
</table>
| Allow mail only from
  domains:           |
| *Deny mail from domains: |

<table>
<thead>
<tr>
<th>Messages Addressed to:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internet Domain</strong></td>
</tr>
<tr>
<td>*acme.com</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Should be Routed to:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain name</strong></td>
</tr>
<tr>
<td>TheIntranet</td>
</tr>
</tbody>
</table>

| Or: |
| Internet host: |

• Two Server Connection documents.

• One Server Connection document for the Internet: You may need to create a new document. You must enter information in the Connection Type. The Source server fields must reflect the name of the server on which the MTA resides (Lobster/Seafood). The Destination domain must match the domain entered in the foreign domain document (TheInternet). This field should not be the same name chosen for the Source server. You can give a virtual name for the Destination server (All Internet Hosts). To indicate the firewall or relay to be used, you must also indicate the Optional network address name or the IP address of that system.
• One Server Connection document for the Intranet. You need to create a new document. You must enter information in the Connection Type. The Source server fields must reflect the name of the server on which the MTA resides (Shrimp/Seafood). The Destination domain must match the domain entered in the foreign domain document (TheIntranet). This field should not be the same name chosen for the Source server. You can give a virtual name for the Destination server (Local SMTP Hosts).

**SERVER CONNECTION: Lobster/Seafood**

<table>
<thead>
<tr>
<th>Basics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection type</td>
<td>SMTP</td>
</tr>
<tr>
<td>Source server</td>
<td>Lobster/Seafood</td>
</tr>
<tr>
<td>Connect via</td>
<td>Direct connection</td>
</tr>
<tr>
<td>Usage priority</td>
<td>Normal</td>
</tr>
<tr>
<td>Destination domain</td>
<td>TheIntranet</td>
</tr>
<tr>
<td>Filter host</td>
<td>132.00.00.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scheduled Connection</th>
<th>Routing and Replication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connections</td>
<td>Tasks</td>
</tr>
<tr>
<td>Enabled</td>
<td>SMTP Mail Routing</td>
</tr>
<tr>
<td>Days of week</td>
<td>Route at once</td>
</tr>
<tr>
<td>Sun, Mon, Tue, Wed, Thu, Fri, Sat</td>
<td>5 messages pending</td>
</tr>
</tbody>
</table>

**SERVER CONNECTION: Lobster/Seafood**

<table>
<thead>
<tr>
<th>Basics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection type</td>
<td>SMTP</td>
</tr>
<tr>
<td>Source server</td>
<td>Shrimp/Seafood</td>
</tr>
<tr>
<td>Connect via</td>
<td>Direct connection</td>
</tr>
<tr>
<td>Usage priority</td>
<td>Normal</td>
</tr>
<tr>
<td>Destination domain</td>
<td>TheIntranet</td>
</tr>
<tr>
<td>Filter host</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scheduled Connection</th>
<th>Routing and Replication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connections</td>
<td>Tasks</td>
</tr>
<tr>
<td>Enabled</td>
<td>SMTP Mail Routing</td>
</tr>
<tr>
<td>Days of week</td>
<td>Route at once</td>
</tr>
<tr>
<td>Sun, Mon, Tue, Wed, Thu, Fri, Sat</td>
<td>5 messages pending</td>
</tr>
</tbody>
</table>

• Two Server documents.

• One Server document for the SMTP/MIME MTA connected directly to the Internet. You must edit the server document for server Lobster/SEAFOOD. You must enter information in the Routing tasks, and the Global domain name. The Fully qualified Internet host name represents your full Internet address for this server.
One Server document for the SMTP/MIME MTA connected to the Intranet. You must edit the server document for the server Shrimp/SEAFOOD. You must enter information in the Routing tasks, and the Global domain name. The Fully qualified Internet host name represents your full Intranet address for this server.

**SERVER: Lobster**

<table>
<thead>
<tr>
<th>Basics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Server name:</td>
<td>Lobster</td>
</tr>
<tr>
<td>Server title:</td>
<td></td>
</tr>
<tr>
<td>Domain name:</td>
<td>Seafood</td>
</tr>
<tr>
<td>Cluster name:</td>
<td></td>
</tr>
<tr>
<td>Master address book name:</td>
<td></td>
</tr>
</tbody>
</table>

**Internet Message Transfer Agent (SMTP MTA)**

<table>
<thead>
<tr>
<th>General</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Global domain name:</td>
<td>AcresGlobal</td>
</tr>
<tr>
<td>Full qualified Internet host name:</td>
<td>lobsters.acres.com</td>
</tr>
<tr>
<td>MTA administrator:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Control</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Pull for new messages every:</td>
<td>120 seconds</td>
</tr>
<tr>
<td>MTA wait path:</td>
<td>c://Wd/SMTPwork</td>
</tr>
<tr>
<td>Log level:</td>
<td>Normal</td>
</tr>
<tr>
<td>Enable daily housekeeping:</td>
<td>Enable</td>
</tr>
<tr>
<td>Perform daily housekeeping at:</td>
<td>01:00 AM</td>
</tr>
</tbody>
</table>

**SERVER: Lobster**

<table>
<thead>
<tr>
<th>Basics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Server name:</td>
<td>Shrimp</td>
</tr>
<tr>
<td>Server title:</td>
<td></td>
</tr>
<tr>
<td>Domain name:</td>
<td>Seafood</td>
</tr>
<tr>
<td>Cluster name:</td>
<td></td>
</tr>
<tr>
<td>Master address book name:</td>
<td></td>
</tr>
</tbody>
</table>

**Internet Message Transfer Agent (SMTP MTA)**

<table>
<thead>
<tr>
<th>General</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Global domain name:</td>
<td>AcresGlobal</td>
</tr>
<tr>
<td>Full qualified Internet host name:</td>
<td>shrimp.acres.com</td>
</tr>
<tr>
<td>MTA administrator:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Control</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Pull for new messages every:</td>
<td>120 seconds</td>
</tr>
<tr>
<td>MTA wait path:</td>
<td>c://Wd/SMTPwork</td>
</tr>
<tr>
<td>Log level:</td>
<td>Normal</td>
</tr>
<tr>
<td>Enable daily housekeeping:</td>
<td>Enable</td>
</tr>
<tr>
<td>Perform daily housekeeping at:</td>
<td>01:00 AM</td>
</tr>
</tbody>
</table>
About mail routing and domains

Most organizations use a single domain. Consider the following issues in deciding between a single or multiple domains:

- **Mail routing**
  With a single domain, users specify the recipient’s name in a mail message. Domino checks a single Public Address Book and routes the message. With multiple domains, you must set up a Master Address Book, cascading Address books, or users must specify the recipient’s domain.

- **Public Address Book administration**
  With a single domain, you only administer and make changes to one Public Address Book, but that Address book may be large. With multiple domains, you make changes and administer several Address books, which are smaller than a single Address book would be for the same system.

- **Server administration**
  With a single domain, server administration is centralized in one Public Address Book. With multiple domains, server administration is divided among more than one Address book. This lets you decentralize tasks but also means you must make changes in several places.

If the sender and recipient of a mail message are in the same domain, the message is routed based on information in that domain’s Public Address Book. The transfer may take place on the same server, on different servers within the same Domino named network, or on different servers in different Domino named networks.

If the sender and recipient of a mail message are in different domains, Domino routes mail between domains. First, Domino determines which domain the recipient is in.

- The sender specifies a domain in the e-mail message; for example, “John Jones@North.”

- The sender does not specify a domain path and the organization is using either Directory Assistance with a Master Address Book or cascading Address books. Domino checks the sender’s Public Address Book and does not find a listing for the recipient.

- With Directory Assistance, Domino consults the Master Address Book for replicas of Address books for other domains and searches them for the recipient’s name.

- With cascading Address books, Domino checks replicas of other Address books in the order in which they are listed in the NOTES.INI file.
Second, Domino must decide how to move the message from the sender’s server to the recipient’s server by finding a connection between domains.

- Servers in the two domains are connected by Connection documents, allowing mail routing and replication between the domains. Domino moves the message from the sender’s server to the connected server in that domain, then to the connected server in the second domain, then to the recipient’s server.
- There is no direct connection between the two domains, but other domains server as intermediaries. Domino looks in the Public Address Book of the sender’s domain for a Non-adjacent Domain document, which gives a path specifying the domains through which a message must pass to reach the destination domain. Domino then checks for a connection between a server in the sender’s domain and the first domain in the Non-adjacent Domain document. Domino moves the message from the sender’s server to the server connected to the intermediate domain. When this connected server contacts the server in the intermediate domain, it transfers the message. Domino repeats this transfer process between domains until the message reaches the target domain, where it is moved to the recipient’s server.

---

About mail routing and multiple Public Address books

When you work with multiple domains, each domain has its own Public Address Book. To route mail between domains, use any of the following methods.

**Separate Public Address books**

Using this strategy, a server stores only a replica of its primary Public Address Book (the one associated with its domain). Separate Public Address books are easier to maintain and don’t need to be replicated across domains.

**Directory assistance**

Directory assistance allows users to select names from secondary Public Address books.
Cascading Public Address books

You set up cascading Public Address books by using the NOTES.INI setting NAMES= on servers to point to a replica of secondary Address books. With this approach, users can use the Addressing dialog box to select names from secondary Public Address Books. Be aware that:

- Domino searches the secondary Public Address Books in the order they are listed in the NAMES= setting.
- It doesn’t resolve names from secondary Public Address Books entered in memos before sending them.
- You are limited in the number of domains you can set up for cascading Public Address Books by the NOTES.INI NAMES setting, which has a maximum of 256 characters.
- A user cannot automatically access a replica when the server storing a secondary Public Address Book (NAMES= points to) is unavailable.

There are two ways to set up cascading Public Address Books:

**Replicate secondary Public Address books within a domain**

With this arrangement, servers in a domain store replicas of secondary Public Address books as well as a replica of their primary Public Address Book. Storing replicas of secondary Public Address books provides the type-ahead addressing feature. However, this arrangement requires additional disk space and regular replication of secondary Public Address books.

**Access secondary Public Address books over the network**

With this arrangement, most or all servers in a domain store only replicas of their primary Public Address books and point to replicas of secondary Public Address books on another server which are accessed over the network. This arrangement requires less disk space and less Public Address Book replication than replicating secondary Public Address books. However, the type-ahead addressing feature doesn’t search secondary Public Address Books accessed over the network and a server session is kept open permanently for each server configured in NAMES= to be accessed over the network.
Summary of methods for managing multi-domain Public Address books

The following table summarizes the features of each approach to managing Public Address books in a multiple-domain environment:

<table>
<thead>
<tr>
<th>Features</th>
<th>Separate Public Address books</th>
<th>Directory assistance</th>
<th>Cascading Public Address books (Public Address books replicated across domains)</th>
<th>Cascading Public Address books (Public Address books accessed over the network)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users can use addressing feature to select names from secondary Public Address books</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Users can use the type-ahead mail addressing to search names from secondary Public Address books</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Name of a recipient from a secondary Public Address Book resolved before memos sent</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Low disk space usage</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Failover to another replica of a secondary Public Address Book</td>
<td>Not Available</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Permanently open server sessions</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Public Address books replicated primarily or exclusively within their domains only</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Uses rules for more efficient searching of secondary Public Address books</td>
<td>Not Available</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Mail routing within a Domino named network

Mail routes in a Domino named network automatically and without Connection documents. If there are two servers, the sending server and the destination server, Domino moves the message from the MAIL.BOX file on the sending server to the MAIL.BOX file on the destination server, using the path specified in the routing table that has the least cost.

If the sender’s mail file and the recipient’s mail file are on the same server, Domino moves the message from the sender’s mail file to the recipient’s mail file.

Chapter 10: Deploying Mail 113
Mail routing between Domino named networks

With multiple Domino named networks, there are several possibilities for routing mail. For maximum efficiency, connect Domino named networks by including one server in both networks. This server must run the protocol for each Domino named network.

Domino checks the Public Address Book for the domain and finds that the sending server and the receiving server are in different Domino named networks. There are several possibilities:

- The Domino named networks have a server in common (a server running the protocol for each Domino named network). Domino checks the routing table and moves the message from the sending server to the common server. This effectively transfers the message between Domino named networks. The common server moves the message to the destination server.

- The Domino named networks do not have a server in common but are directly connected. Domino checks the Connection records in the Domino named network to find a server in the sending Domino named network that connects to a server in the destination Domino named network. Domino moves the message to the connected server in the sending Domino named network. When this server contacts the server in the destination Domino named network, it transfers the message. The connected server in the destination Domino named network moves the message to the destination server.

- The Domino named networks do not have a server in common and are not directly connected. Domino checks the routing table for a path to the destination Domino named network and routes the message along that path through intermediary Domino named networks.

About server connections for mail routing

Servers connect to route mail and to replicate databases based on parameters set up in Connection documents in the Public Address Book. Replication requires only one Connection document, but mail routing requires two — one document for each direction. You can schedule connections at intervals and set a routing threshold — when a certain number of messages are waiting to be delivered, the servers connect even if a connection is not scheduled. Make sure you replicate the Public Address Book between servers in a domain so that Connection documents are kept up to date.
About mail routing and priority levels

You can designate a mail message as High, Normal, or Low priority. A message’s priority determines how quickly it routes.

- High priority mail routes immediately, even if mail routing is not scheduled.
- Normal priority mail routes during the next scheduled connection or when the number of messages reaches the threshold level defined in the Connection document. Mail is designated Normal priority by default.
- Low priority mail routes only between 12:00 AM and 6:00 AM, regardless of when other mail routes. You can configure when low priority mail is delivered by modifying the NOTES.INI file on the Domino server.

You can disable mail priority, setting all mail as Normal, by modifying the NOTES.INI file on the Domino server.

About mail files

Notes mail files are Notes databases (.NSF files) based on a mail template. You can access a Notes mail file from Notes, from a browser, and from POP3 and IMAP clients. Domino can host multi-client mail files (for example, you access your mail from Notes at work and from a POP3 client at home) as well as files accessed only from Notes or only from POP3 or IMAP.

Consider how you want to store messages. Messages based on Internet protocols can be stored in Notes format, in MIME format, or in both formats. If you store the messages in MIME format, Notes displays a file attachment that you can read with the attachment viewer. Storing the messages in both Notes and MIME format takes more disk space but is the best option for users who access their mail from both Internet clients and Notes and offers the best performance during mail retrieval because no format conversion is necessary.

For more information, see “Creating a Person document for a POP3 or IMAP user” in Getting Started with Domino.

Consider setting size limits on mail files by setting a database quota. This improves your ability to plan demands on and manage server space. If a mail database reaches its quota, Domino continues to deliver mail but does not allow that database user to create or save new messages. In addition, consider whether to allow users to create full text indexes for their mail files. While full text indexing is a powerful feature, it takes up disk space and CPU processing time.
About accessing mail from Internet clients

To access your mail from Internet clients compliant with MIME and either POP3 or IMAP, you must have a Domino SMTP/MIME MTA on at least one server in your organization and must be running TCP/IP on the MTA server and on the mail server you wish to access. Authentication takes place on the challenge/response model and can use SSL if the Domino server has an X.509 certificate. Lotus recommends setting the POP3 client to delete mail from the POP3 mail file automatically after the client copies it locally. This saves server disk space; however, do not set this option if the user also accesses the mail file from Notes.

Notes folders appear in IMAP as IMAP mailboxes. Adding or deleting documents in an IMAP mailbox changes the contents of the folder in Notes and vice versa.

About shared mail

Shared mail reduces the disk space needed to store mail that is sent to multiple recipients. When you send a mail message to multiple recipients and several of those recipients have the same mail server, Domino puts a copy of the message in a database named MAILOBJ.NSF on that mail server. Each recipient accesses that copy of the message via a pointer message that is sent to their mail file. There is no difference between a shared mail message and an individual mail message. This eliminates the need to deliver and store multiple copies of the same message on the same server. If a recipient edits the message, Domino copies it to the mail server so that it can be edited.

About accessing mail from MAPI clients

Domino allows you to access and send mail from MAPI clients like Microsoft Exchange, Microsoft Outlook, and Microsoft Office. You can also access mail on an Exchange server from a Notes client.

For more information on setting up and configuring MAPI with the Notes MAPI Service Providers, see Chapter 1 in the Notes Designer for Domino Install Guide.

For more information on setting up and configuring MAPI, see the index entry “MAPI” in Notes Help (HELP4.NSF).
Setting up the Calendar and scheduling across your organization

Using Domino and Notes to manage your employees’ calendars and schedule meetings offers significant reduction in overhead and improvements in efficiency. You no longer need to call or e-mail people to determine whether they are available for a meeting. You can reserve a room and all the resources you need from your computer.

The Notes client includes powerful features for managing your calendar and scheduling meetings. Each Notes mail file contains a Calendar view. By creating a Calendar Profile, users enable scheduling and can set up meetings, schedule appointments, and reserve resources such as conference rooms. Users set who can look up information on their free and busy times in the Calendar Profile. With the Free Time system on Domino servers, you can search users’ free time slots to find the best time for scheduling a meeting. The Calendar and scheduling features in Notes integrate with other calendar systems such as Lotus Organizer® and IBM OfficeVision®.

The Free Time system, which manages calendars, schedules, resource reservations, and free time lookups, consists of two server programs: Schedule Manager and Calendar Connector. Schedule Manager creates a Free Time database (BUSYTIME.NSF) that stores information about the free time of every user whose mail file is on that server. Calendar Connector enables Free Time lookups across multiple Notes domains and determines the path between servers for queries.

You can set up a Resource Reservations database to allocate resources to meetings and appointments. This allows users to reserve conference rooms, overhead projectors, videoconferencing equipment, and other resources for a particular time. A Resource Reservations database automates and centralized the process of obtaining a meeting room and other resources.

In large organizations in multiple locations, using the Notes calendar, Free Time system, and Resource Reservations database reduces the administration and time needed for scheduling.
Securing your data against unauthorized access is one of the most important challenges your organization faces. Use the security features of Domino to defeat hacking and to compartmentalize information within your organization. Domino provides security from the Internet down to the individual fields in a document. This chapter gives an overview of how to protect the information in your Domino system.

About security in a Domino System

Domino provides robust, proven security at multiple levels. To maximize the security of your network, Web site, applications, and servers, you must develop and implement security policies at an organizational level. By setting requirements for security concerns like remote access, passwords, modem access, administration, and firewall access, you protect your system from human error and technical weaknesses. By creating a clear policy on information distribution and employee identification, you can help eliminate unauthorized access to your system.

To develop security policies, examine each level of Domino security and determine how you want to implement it in your organization. Consider weaknesses from outside your company and from inside it. Examine the tradeoffs between increased security and increased accessibility and ease of use. Also, create a plan to react to and repair breaches in security.

Domino security covers multiple levels, from Internet and network security down to protecting the fields in a document in a database. These levels are complementary — using a level reinforces the security above and below it. In addition to security for your network protocols, server operating systems, and client operating systems, consider the following areas:

- Internet security
- Network security
- Hierarchical naming for servers and users
- Domino server security
- Notes client security
- Web browser client security
About Internet security

Connecting to the Internet offers your company many opportunities but also creates a number of security risks. Domino allows you to control many of these risks. In developing Internet security policies, you must balance the need for communication and information transfer between your company and customers, vendors, suppliers, and the public, with the potential for harm that this access creates. Examples of weak points include password length and expiration, transferring information over the Internet without using encryption such as the Notes RSA algorithm or SSL, open ports through your corporate firewall, directory access to servers (critically important for UNIX servers and Windows NT), and receiving files from the Internet via e-mail, File Transfer Protocol (FTP), or the World Wide Web. In evaluating whether to open a port in your firewall, for example, you must weigh the value of allowing your employees to send and receive information through this port with the possibility that people can infiltrate your system through this opening or introduce harmful programs such as viruses by using it as an access point.

In addition, the Internet poses risks that involve both your system and the larger Internet infrastructure, such as DNS spoofing and denial of service attacks. Browsers may contain security flaws that allow foreign programs and users to interact with your network. Such risks are difficult to combat on your own — work with your Internet Service Provider (ISP) to guard against problems.

A good resource for Internet security is the Computer Emergency Response Team, a unit of the National Computer Security Agency. Visit their Web page, which gives updates on known problems and solutions, at http://www.ncsa.com/ncsacert.html.

Firewalls

Consider carefully how you connect to the Internet. Many organizations install firewall software that protects their intranet from unauthorized external access. A firewall works at a hardware or software level to control access to your system. Firewalls implement such security measures as packet filtering, application-level gateways, circuit gateways, and are often used in conjunction with a proxy server. The Domino server and Notes workstation do not rely on a firewall. The Domino registered TCP socket (1352) can be
left open in your firewall if you take appropriate security measures at the
server and database level. Firewalls are useful to protect other parts of your
system such as FTP and Internet mail.

**Proxy servers**

You can use a proxy server for your organization to mediate between client
requests in your company, such as HTTP requests from a browser, and
servers outside your firewall. Proxies mask the return address of the
requesting computer, providing secure anonymity for users and denying
any potential targets.

Proxies can implement protocol-specific security and allow you to filter
incoming requests to the various protocols on your system. For example,
you block all HTTP requests to objectionable Web sites using a proxy, or
prevent users from downloading files via FTP except from specified trusted
hosts. Some proxies run virus detection programs on incoming packets.

Proxies improve performance by caching information. If a user requests
www.lotus.com through a proxy, the proxy will cache the HTTP information
from www.lotus.com. Other users who request this site are sent the cached
page information from the proxy, eliminating the need to transfer the data
from www.lotus.com again. This conserves bandwidth and results in faster
rendering of sites for your users. You can use a proxy to mediate requests
from outside your firewall. For example, you make some internal documents
available to public request by caching them on a proxy server outside your
firewall.

**Encryption**

You should create a corporate policy instructing users to be cautious in
transmitting any personal or company information over the Internet. Unless
encrypted, this data is easily intercepted. This protection is particularly
important for data such as user names, passwords, confidential product
information, and electronic commerce information like credit card numbers.

While browsers allow you to verify attaching to a secure server, there is no
way to be certain of the identity of this server without using other means:
a user might connect to an unsecure server, believing that it was in fact
another, secure computer.

Domino supports version 3.0 of the Secure Sockets Layer (SSL) protocol,
which allows secure encrypted communications in HTTP transactions. SSL
is a public/private key RSA cryptographic system that uses key ring files
to store the encryption codes needed for private communications. If you
connect to a Domino server using SSL, information exchange is highly
secure. Domino Directory Services, POP3 server, Web Navigator, and News
Discussion server all use SSL for enhanced security. Domino can act as a
Certifying Authority (CA) for SSL certificates.
Internet activity tracking

Domino can create log files, in either text file or Notes database (.NSF) format, to track Internet activity on a server. The log stores information on what parts of a site or server are accessed, which browsers are used, which URLs are used, and any CGI errors that may occur. You can use these files to monitor activity on your sites and on your servers and to check for suspicious actions.

Notes client

With the Notes client, Domino uses an RSA public-private key algorithm that is even more secure than SSL and that virtually eliminates the possibility of data interception or packet sniffing. The Domino - Notes combination is the most secure client - server package available and has a security model that has been proven through time and use.

You can use Notes features such as Read access lists, Edit access lists, Authors fields, and Readers fields in your Internet databases to control access to documents.

Note  Field-level encryption does not work on the Web. Be cautious in exposing databases with field-level encryption to browser client access as these clients may be able to read the encrypted fields.

For information on extranet security, see Chapter 7.

About network security

Your network comprises the infrastructure behind your firewall, the firewall and any proxy servers, and computers outside the firewall that you use to communicate with the Internet. Key network security issues are guarding against unauthorized network access and authenticating user identities, protecting against viruses, and ensuring the physical security of the network.

Guarding against unauthorized access

Guarding against unauthorized network access involves, at a minimum, installing a layer of challenge - response that must be passed before access is allowed. Typically, this involves providing a user name and password, which should be encrypted. Further challenge - response points can be used to protect server access or access to particularly confidential information. An enhanced form of this security uses digital signatures to authenticate user identities. The Notes client has a digital signature based on the RSA public - private key algorithm. With browsers or other Web clients, X.509 certificates play the same role. Establish policies on keeping passwords and user names confidential and instructing users to guard their digital signatures. Instruct
users to use long alphanumeric passwords to defeat dictionary attacks, where a program attempts to crack passwords by running combinations of letters against the password challenge, and remind them not to write down passwords.

The major concern for network security is intentional, malicious access by unauthorized users. Following the security precautions in these sections aids in protecting your network against these attacks. Monitor server log files for suspicious queries or attempts to access your system. Limit root access to servers and protect system files carefully. Remove unneeded services and protocols from your firewall to deny potential access points. Both firewalls and proxies can log activity, which helps you detect suspicious actions. Use a tool such as SATAN (System Administrator Tool for Analyzing Networks) to check your network for security flaws.

Remote access is often a source of risk. Ensure that modems and remote servers have the same access protections as the other access points in your organization. Utilize dial-back and password protections for modems.

Domino can encrypt data that travels through its system and over your network. This option encrypts data packets at the port level. If you are using the Internet to transfer data, encrypt the data by choosing File - Tools - User Preferences, clicking the Ports tab, and selecting Encrypt Network Data.

Guard against viruses

Viruses have the potential to cripple your network by destroying or corrupting data and interfering with applications and communications. Viruses are commonly introduced by users who receive programs from outside the network or who connect with a contaminated source, such as a disk with a virus. E-mail is often a source of viruses. Set up a network-wide virus scanner that checks all file attachments in e-mail and that searches for viruses on the network. In addition, install virus-scanning software on all computers and configure it to run frequent scans. Instruct users not to bring disks from outside the network into it. Warn users to be cautious of files received via or downloaded from the Internet; some are disguised viruses. Macro viruses hide inside files created by programs that allow macro scripting. Familiarize users with the security features of their applications and encourage them to use these features. When installing applications, set security defaults to a high level of protection. Viruses and other similar programs, such as Trojan horses, are data driven attacks: they operate inside a firewall when a user runs them. There are a number of products that work with Domino to scan your system for viruses. For more information, contact your Lotus authorized reseller.
The Notes client has a security feature called the Execution Control List (ECL) that guards against the unauthorized execution of programs received via e-mail or in a database. The ECL allows you to restrict the access and execution rights of programs depending on the digital signature of the document’s author. You can allow programs created or sent by a colleague to run without restrictions but deny programs received via the Internet. If you receive a file from an unknown sender, you can choose not to run the file, to run it once but not to trust the sender, or to trust the sender and run programs sent by the same person in the future.

Guard the physical system

Your network must be physically secure. Protect servers by requiring passwords to access them and keep the server machines in a locked room with controlled access. Most operating systems allow you to password-protect keyboard access. For UNIX servers, password-protect the server account and limit permission to the data directory and program files. The Domino SET SECURE server command lets you set a password that limits access for some administration tasks, such as adding or deleting users. Password-protect workstations if possible. Establish security procedures that prevent unauthorized individuals from gaining access to your network.

About hierarchical naming

Hierarchical naming gives users and servers ID files with names that are based on a cascading series of certificates. It helps differentiate users and servers, increases your control over access and authentication, allows for decentralized administration, and helps you manage your extranet. Use an organizational map to help you plan and implement hierarchical naming. When you set up the first Domino server in your organization, Domino creates an organization-level certifier (CERT.ID), a binary file which it uses to certify, or stamp, the server’s ID and an administrator’s user ID. ID files contain a private key, used for authentication and digital signatures, and a series of certificates that help authenticate the ID. These certificates are the stamps created by certifier IDs and are central to hierarchical naming. While hierarchical naming requires planning and knowledge of your organizational hierarchy, it confers significant security and administration advantages.

Verifying identities

Certification allows Domino to verify the identities of users and servers. An ID file is like a passport; certification is the border control process that stamps passports. If a user or server possesses a passport with the correct stamp, they can enter the destination. Cross-certificates are like visas; they
allow controlled access to areas outside your organization, or permit you to give people outside your organization controlled access to certain parts of it. With cross-certificates, Notes users from different organizations can authenticate with your servers. Each organization cross-certifies one ID file from the other and stores the cross-certificate in its Public Address Book. Cross-certification can occur at all levels of certification and can limit access to a given OU level. Cross-certification does not have to be at the same level in both directions. To restrict access by other organizations to certain servers, use Server access lists. Both certificates and cross-certificates can have expiration dates, limiting the risk of a lost or compromised ID file. This forces users and servers to have their ID files restamped at set intervals or by a certain date.

Certification affects server and user registration, server access, and electronic signatures. It verifies users and servers securely in both directions. Users and servers are referred to in Domino and Notes by their hierarchical names, or their user/server name plus their certificates. Judy Smith, who works for Acme and whose certificates are /ACME and /SALES/ACME, would be recognized as Judy Smith/SALES/ACME. Always use hierarchical names in access control lists and Server access lists to prevent people with the same given name but different hierarchical names from accessing each other’s files.

Organize the company

You use two types of certifiers for hierarchical naming, one organizational certifier (O) and up to three organizational unit certifiers (OU). Certifiers are analogous to families; lower-level certifiers inherit the characteristics of the certifiers above them. For example, the OU certifier /SALES/EAST/ACME has a stamp for the organizational unit certifier /EAST/ACME, which is certified by the organizational certifier /ACME. Large organizations need more levels of certifiers than smaller organizations.

Organization certifiers generally use the company name as the stamp, such as /ACME for the Acme Corporation, and have the file name CERT.ID. Organizational unit certifiers are commonly used to differentiate business units or geographic locations, such as /FINANCE/ACME or /SOUTH/ACME, and take the name of the OU for their file, such as FINANCE.ID. OU certifiers are commonly referred to by their OU name, such as the “Finance OU” for /FINANCE/ACME. Each additional OU allows you to add another level with which you can distinguish users and servers. Use your first OU certifier based on the primary groups in your organization, which are frequently distinguished by geographic location or business function. For example, Acme might use geographic location for its first OU certifiers, /WEST/ACME and /NORTH/ACME, then use business units for the second OU certifiers, /SALES/WEST/ACME and
/ACCOUNTING/WEST/ACME, and a third business unit for the individual office in which a server or user is located, such as /PHOENIX/ACCOUNTING/WEST/ACME. With these certifiers, Acme can limit access to the Sales servers to employees with the /SALES certificate on their IDs.

Lotus recommends reserving one OU to distinguish servers; for example, /H/ACME could identify a hub server and /M/ACME a mail server. Guard certifiers vigilantly — if compromised, they could allow unwanted access to your system.

You can set multiple passwords on certifier ID files and require that a certain number of those passwords be entered before the ID can be used. For example, if you had four administrators with access to the certifier ID, you could set four passwords on the ID, give one to each administrator, and require a minimum of two passwords to use the ID. This prevents a single person from misusing the certifier.

You can create organizational unit certifiers to decentralize administration, improve security in case a certifier is compromised, to provide context for servers and users, and to distinguish people with the same name. By creating multiple certifiers, you allow more than one person to create and certify new users. You can use wildcards in access control lists (ACLs), such as */ACME, which would allow anyone with the /ACME certificate to access a database. Should an OU certifier file be lost or compromised, there is less work to recertify users than if an O certifier is lost, since you only recertify the employees and servers stamped with that certifier. If a certifier is lost, recertify all servers and users stamped with that certifier and then deny access for IDs with that certificate to all servers. Certificates help provide context to the function of a server or user; the certified name of the server Data1/Finance/Boston/Acme indicates what the server’s role is. Multiple certifiers reduce the risk of having multiple people with the same name and the same certificates. For example, Domino regards Jane Doe in Marketing and Jane Doe in Administration as separate people, even though they have the same name, because they have different certificates: Jane Doe/MARKETING and Jane Doe/ADMIN. In addition, certificates conform to the X.500 naming convention.

Domino maintains a certification log with a document for each user and server with their name, license type, ID number, and date of certification and expiration. You create additional certifiers in the Public Address Book.

**Caution** Do not use the failure to certify an ID as an access control mechanism. Use database ACLs to control data access. Certifying IDs enables authentication, which allows checks on access control.
About Domino server security

Domino provides the most advanced, proven security available. In addition to the physical and password security, Domino servers use a server access list to determine who can access the information on that server. The server access list is configured in the Server document in the Public Address Book. You can allow or deny access to users, servers, and groups on an individual level, permit everyone to access the server, or deny all access. In addition, you can set the server to permit only users in the Public Address Book. Setting this limit denies anonymous browser access.

The access lists controls who can create databases and replicas on the server and how the server works with passthru. Passthru controls whether users can route requests through the server to another server as a steppingstone. Denying passthru limits internal access to servers and can help reduce network traffic. By using the server access list on each Domino server in your organization, you can leave the Notes port in your firewall open without concern. Domino does not allow passthru for Web browsers, who are restricted to viewing databases for which they have access on the server they are connected to.

However, you can allow anonymous Notes access to your servers by selecting Yes in the Allow Anonymous Notes Access field in the Security section of the Server document in the Public Address Book. If you allow this access, close the Notes port in your firewall, do not allow passthru access to this server, and do not allow further access from this server to the rest of your network. With this option, Server access lists and database ACLs control access to data on the server.

Domino servers authenticate with one another in the same way that Notes clients authenticate with Domino: via public - private key encryption based on an RSA algorithm. The private key is stored in the user ID file or in the server ID file. Secure connections and data integrity are assured by this method.

You can control the default level of access that Notes clients allow to executable files via the ECL. The Public Address Book contains an Administration ECL that Domino copies automatically to the Notes workstation during workstation setup. Use the Edit Administration ECL agent in the Public Address Book to update this default ECL. You can send updates of the ECL to users via Notes mail.

For administrator and server IDs, you can set multiple passwords on the ID file and require that a certain number of those passwords be entered before the ID can be used. For example, if you had four administrators with access to the server ID for a server with confidential data, you could set four passwords on the ID, give one to each administrator, and require a minimum of two passwords to use the ID. This prevents a single person from misusing critical information.
About Web browser client security

Browser clients participate interactively with all Domino features. Domino provides extensive security that allows you to control which Internet users can view and use each part of your site and who has access to your servers from browsers. Create Person documents in the Public Address Book for each Internet user whom you wish to identify individually. Person documents include HTTP passwords, which are encrypted. Authentication between a Domino server and a Web browser takes place via challenge-response and occurs when the browser tries to perform an action for which access is restricted. The browser client must provide the user name and password that match those in a user’s Person document. To gain access to data, that user must be included in the database ACL as an individual or a member of a group. You can force users to supply a name and password by appending “&Login” to a URL command, but this is not a true security feature since users can delete &Login from the URL.

Domino allows SSL connections for secure communication with browsers and can act as a Certifying Authority (CA) for SSL certificates. Domino can also send certification requests to third-party CAs.

To prevent anonymous browser access to your Domino servers, select No in the Allow anonymous HTTP connections field of the Security section in the Server document. This negative setting overrides greater permissions for anonymous users in the ACLs of individual databases. To prevent anonymous access to a database, create an entry for Anonymous in the ACL and assign it No Access. You can control the maximum level of access for any user from a browser client with the Maximum Internet name & password access field, which overrides greater permissions in the ACL.

Domino does not allow passthru by browser clients. Browsers can only access databases on the Domino server with which they are connected.

About Notes client security

The Notes client is the most secure client available. The Notes client security model interacts with the Domino server security framework. When a Notes client attempts to access a Domino server, the server validates the client ID file by establishing that it trusts the client public key, then authenticates the ID through a challenge-response procedure using the public and private keys of the client and server. Trust validating a common certificate on the two IDs. The certificates on the active user ID for the client determine whether the server authenticates it. Certificates generate a code associated with the name of the certifier, such as /FINANCE/ACME, and consist of the association of that name plus the code. Authentication is possible when two entities, such as a server and a client, have common certificates.
The association between public and private keys created by certificates avoids the problem of public key spoofing, where a user attempts to convince another user or server that a valid public key belonging to someone else belongs to that user. Certificates can be compared to notarized messages stating that a public key is associated with a particular name. If an entity has a certificate signed by a certifier and can determine the certifier’s public key, it can verify the signature on the certificate.

Notes public keys are used both for authentication and for mail encryption. You can create new public keys for users but must recertify the ID files for those users. Domino can keep clients from using the old public key and can be set to authenticate only clients whose public keys match the public keys in the Public Address Book.

Notes client ID files contain a private key that is mathematically related to the public key stored in the Public Address Book. Information encrypted with one key can be decrypted with the other. Lotus strongly recommends that you protect all ID files with passwords. Encourage users to use long alphanumeric passwords. Passwords should be at least 13 characters in length. Using mixed uppercase and lowercase letters and numbers improves password security. Using a phrase for a password makes the password easier to remember and reduces the chance that an attacker could guess it. It is important for users to remember their passwords and to keep backup copies of their ID files; if they forget the password or lose their ID file permanently, they can no longer access data encrypted with that password.

To defeat dictionary or brute force attacks on ID file passwords and to reduce the risk of password capture, Notes employs an anti-spoofing password dialog box. If users enter an incorrect password, Notes waits for several seconds before allowing them to try again. This delay increases with each incorrect attempt to a maximum of thirty seconds. The delay feature makes it difficult to try rapidly many passwords in succession in the hope of guessing the right combination. Also, the dialog box has a series of hieroglyphic symbols on the left side that change as users enter their password. These dynamic symbols make it more difficult to substitute a false dialog box that captures passwords in place of the Notes dialog box. Tell users to be alert to the symbols as they enter their passwords — if they notice that the symbols do not change or are not present, they should stop entering their password and click Cancel.

ID files allow Notes clients to create verifiable digital signatures on documents. These signatures assure readers of the identity of the document author and confirm that the document has not been tampered with since it was created. For example, digital signatures allow you to be sure that a mail message is really from a colleague and not from an untrusted third party.
About database security

Database security begins with the database access control list (ACL), the checkpoint which governs access to the database. The ACL lists users, servers, and groups who have varying levels of access to the database. Entities not listed explicitly have the access granted to the Default entry. Each ACL entry has a type (Unspecified, Person, Server, Person Group, Server Group, Mixed Group) and an access level (Manager, Designer, Editor, Author, Reader, Depositor, No Access). The type designation prevents two entities with the same name from accessing a database with the same permissions. For example, by designating the server Sales as a Server and the group Sales as a Person Group, you can give the server and the group different levels of access. Using groups can help make access and administration easier — by entering a group in the ACL and then adding members to that group in the Public Address Book, you can make changes in one place and eliminate the need for adding individual entries to multiple databases.

Access levels

Access levels control the type of actions an entity can perform on the contents of a database and on the database itself. Each access level has the permissions of those below it; for example, authors can perform all of the functions of a Depositor and a Reader. No Access denies access to an entity. Depositor does not allow an entity to view the contents of the database but allows them to create certain documents in it. Readers can read documents in the database that do not have Readers fields and Authors can create documents that do not have specific access restrictions. Editors can change the content of saved documents. Designers can modify the design of all database elements and Managers can change the ACL itself.

Entities may have different levels of access in an ACL if they appear in multiple groups or as individual entries and as members of a group. The access granted in an individual entry takes precedence over that granted through a group entry. If in multiple groups, the group with the highest level of access controls. If an entity has one level of access in the ACL and another level in a Read list or View access list, the element (document, view, etc.) list can lower that entity’s access.

Permissions

You can control what actions entities can take in a database with ACL Permissions. Permissions include the ability to create documents, delete documents, create personal agents, create personal folders/views, create shared folders/views, create LotusScript agents, read public documents, and write public documents. Public documents are documents designed
to be accessed by a wide audience, such as the busy and free times in your personal calendar. Users with the Write public documents permission can read, create, edit, and delete public documents from a database.

**Roles**

The ACL structure described above applies to all databases. However, you may want to create permissions that apply only to one database. Use roles to accomplish this. Roles grant access to individual elements in a database, such as forms or views. For example, your company has a phone number database with two forms: a Phone Number form and a Request Change form. You want all employees to create a Request form, but only the office manager to create a Phone Number form. You create a Role called Phone and change the security on the Phone Number form so that only users with the Phone role can create documents with that form. You can leave employees with Author access, knowing that only the office manager can create the Phone Number form.

You can ensure that all replicas of a database have the same ACL by selecting the Enforce consistent ACL across all replicas option on the Advanced panel of the ACL. This prevents users from creating a replica and modifying its ACL to gain access to confidential information.

**Internet**

Use the Maximum Internet name & password access field to choose the maximum level of access users have when accessing a database from a Web browser. This access overrides individual levels set in the ACL.

Domino logs all ACL changes for auditing.

---

**About database encryption**

You can encrypt databases to protect them from unauthorized access from the operating system level or on a server. The three encryption types are: Strong, Medium, or Simple. Strong encryption is the most secure, but documents in the database take longer to open. Medium security offers both good security and fast access. Simple encryption offers limited security but the fastest access. Disk compression utilities can compress databases with Simple encryption but not those with Strong or Medium encryption.
About controlling access to database design elements

You can control access to forms, fields, views, folders, sections, and documents without using the database ACL.

- Forms
  You can control who can read a form, create documents with a form, set up default encryption keys for a form, allow users with the “Write public documents” permission to create documents with the form, and prevent users from printing, forwarding, or copying the document to the Clipboard. You can also generate encryption keys for a form, encrypt it, and then distribute the keys to people whom you want to have access.

- Fields
  You can control who can view and enter data into a field by encrypting it with an encryption key.

- Views
  You can control who can use a view and whether users with access to public documents can see it.

- Folders
  You can control who can use a folder, whether users with access to public documents can see it, and who can update the contents of the folder.

- Sections
  You can control who can edit the contents of a section.

- Documents
  You can control who can read a particular document with a Readers field. This allows you to control readers on a document-by-document basis instead of for all documents created with a form. With a Readers field, three types of users can read the document: those listed in the Readers field, those listed in the read access list for the form with which the document was created, and those listed in an Authors field on the document.

  You can control who can edit a particular document with an Authors field. Authors fields allow you to grant editing privileges on a document-by-document basis. An Authors field affects only entities with Author access to a database. Users with lower access cannot edit a document; users with higher access can edit a document regardless of the contents of an Authors field.

  You can use an existing encryption key to encrypt a document.
About mail security

Domino works with standards-based Internet mail, Notes mail, cc:Mail, and X.400 mail. Mail security is a critical concern for most organizations, who need to ensure that messages are not read or tampered with by people other than the intended recipients and to verify the identity of the message author. For Internet mail, Domino supports Secure Sockets Layer version 3.0, which allows for mail encryption, digital signatures, and message content validation.

Notes mail has proven security features which offer unmatched security and features. Notes mail users can encrypt mail with the public - private key algorithm in Domino, attach digital signatures to messages to ensure that the contents are not tampered with, encrypt their mail databases, encrypt saved mail, and generate return receipts that notify the sender when the recipient has read the message. To encrypt mail, you must have the public key of the recipient stored in either the Public Address Book or your Personal Address Book.

Your Domino administrator can control how mail routes within the system by not allowing mail to route from a domain to other domains.
Chapter 12
Administering Domino

To maintain full efficiency and ensure user access to mail, databases, and Web sites, you must carefully administer your Domino system, especially the Domino servers. This chapter provides an overview of common administration tasks and tips on improving administration. For more information on administration, see Getting Started with Domino, Extending the Domino System, and Maintaining the Domino System.

About administering Domino servers

Administering Domino servers is one of the most critical tasks in a Domino system. Your system depends on maintaining easy, reliable access for users. Be sure to have enough administrators for your servers and consider creating an administration team to handle server issues at a company level and to work on improving the efficiency and success of server administration. Administrators should be responsible for the following tasks:

- Running, monitoring, and troubleshooting Domino servers.
  Lotus provides an SNMP NotesView® agent to assist administrators in monitoring activity on their network and with their servers. For more information, see the Lotus Web site at http://www.lotus.com/systems/.
- Installing and setting up new servers.
- Optimizing server performance.
  Administrators set and configure the NOTES.INI settings on the Domino server, compact databases, fix corrupted files, and enable the server to run at maximum efficiency.
- Setting up multi-database searching.
- Managing the Public Address Book.
  Administrators create and update Person records, Groups, and the documents related to servers in the Public Address Book. In addition, they make the Address Book useful to users by overseeing directory assistance, managing cascading address books, and administrating LDAP.
• Configuring, monitoring, and troubleshooting replication and mail routing.
  Administrators set up and maintain shared mail, schedule and configure replication, set mail thresholds, reroute dead mail, configure POP3 clients and files, and set replication access levels among servers.
• Setting up and monitoring scheduling, free time lookups, and the resource reservations database to enable calendaring and scheduling at an organizational level.
• Setting up, monitoring, testing, and ensuring server and network security.
• Dealing with remote connections to servers, including access issues, passthru, and hunt groups.
• If your company uses Domino Advanced Services, setting up clustering, billing and monitoring, failover, load balancing, and partitioned servers.
• Managing users.
  Administrators add, remove, and certify users, as well as manage moves from one home server to another or from one domain to another.
• Responding to user requests, problems, and suggestions.
• Monitoring the Log and statistics databases.
• Monitoring Internet access and ensuring a stable, reliable connection to the Internet.
• Backing up databases and files.

You can administer Domino servers from a Lotus Notes Designer for Domino client, a Web browser via the Web Server Administration Tool, and from an administration-only Notes client which is included with each Domino server license. With the Web Server Administration tool, you administer a Domino server from a browser through a URL that accesses an administration database. Domino provides access control to the database with challenge-response password authentication and optional SSL encryption and authentication. The administration-only Notes client lets you use the server administration panel, the Administration menu, and your mail file.

---

**Optimizing server performance**

Consider the following factors when working to maximize server performance:

• Minimize Domino logging
• Configure NOTES.INI settings
• Configure server tasks and scheduling
Monitor performance of the server (especially on Windows NT)

Optimize views and full text indexing

Select a type for Groups. You can designate a Group as Access Control List only, Mail only, Deny list only, or Multipurpose. Designating Group types reduces view size since Groups appear only in the appropriate views, improving the speed of view display.

Dividing administration responsibilities

Because numerous tasks fall under the heading of administration, coordinating activities and setting up clear divisions of responsibility greatly improves the proper functioning and efficiency of your system. Domino server administrators, database managers, and support can all help.

The database manager handles most database responsibilities that include granting database access, monitoring database usage and participation, archiving documents, and updating database design. Administrators should work with databases as entities without being involved in database-specific activities. Administration responsibilities include fixing corrupted databases, approving requests for new databases or new replicas, monitoring server load from database usage, granting server access to users if necessary, and creating database backups.

Administration responsibilities included user registration, server setup, and certification. You can use roles in the Public Address Book to delegate responsibilities while maintaining security and control. For example, one administrator creates new users while a second creates new connections between servers. You must balance the need for security (for example, by having multiple passwords on a certifier ID file and giving only one password to each administrator) with the need to delegate tasks.

User issues and requests to Support relating to servers are generally dealt with by Domino administrators.

Administration guidelines for better server performance

- Monitor database size and usage. Use database quotas to set maximum sizes for databases and enforce archiving.
- Dedicate servers to specific tasks, such as mail routing, replication, or dial-in requests. Reducing the number of tasks a server performs improves the server response time.

Chapter 12: Administering Domino  137
• Avoid using a file server concurrently as a Domino server. Performance of either the file server or the Domino server suffers if one uses a lot of processing time. Additionally, if a program on the file server must be restarted, you must restart all other programs or processes, including Domino.

• Restart the server on a regular schedule. Many databases that are always open on a server, such as the Server Log, the Public Address Book, and the Statistics Reporting database, build up deletion stubs that do not get purged until the server is restarted. If you wait too long between restarts, the purge process will slow down server startup.

• Configure the server to run as many sessions as possible. The Domino server establishes a session for each task, such as replication and mail routing, and for each user who accesses the server. Domino allows users to access the server even after the maximum number of configured sessions is reached. When a new user tries to access the server, Domino drops the session for the user who has accessed the server least recently. Dropped users aren’t affected since when they access the server again, they experience only a slight delay as a new session is established. However, if the server is consistently pushed to the limits of its sessions, users may complain about slow performance. To avoid this, be sure that the server is configured to allow as many sessions as possible. If the server is still overloaded, consider adding another server or reducing the number of users who access the overloaded server.

For more information on monitoring server performance, see Chapter 3 in *Maintaining the Domino System.*

---

**Monitoring and maintaining servers**

Domino provides a wide range of tools for gathering information about a server and for diagnosing and fixing problems.

Include the following maintenance tasks in your administration plan:

• Back up the server.
• Check for dead mail.
• Use the Administration Process to remove users names globally from access control lists.
• If necessary, run the Database Fixup utility manually to fix corrupted databases and prevent server crashes.
• Check the log file for problems with replication, mail routing, scheduling, database integrity, and communication links.
• Monitor server statistics and events to track disk space, server load, memory, swap space, and to head off server trouble.
• Monitor database replication and ACL changes using event monitors.
• Periodically run the Compact utility to keep wasted database free space to a minimum.

For more information on monitoring and maintaining servers, see Chapters 3 and 4 in *Maintaining the Domino System*. For information on using the Administration Process to make global changes to access control lists, see Chapter 2 in *Getting Started with Domino*.

---

### Checking for dead mail

To ensure that mail is being routed and delivered efficiently, check for dead mail daily. Dead mail is mail that fails to route within one day. The failure might be the result of a server or gateway being down.

You can check for dead mail by:

- Checking the statistic MAIL.DEAD in the Statistics Reporting database. You can use an event to notify you automatically when you have dead mail on a server.
- Looking at the Dead Mail view of a server MAIL.BOX.
- Using the server command SHOW TASKS to list dead mail.

After you identify and resolve a mail routing problem, you can release the mail for delivery to the recipient or return it to the sender using the Release Dead Messages action in MAIL.BOX.

For more information on checking for dead mail, see Chapter 4 in *Maintaining the Domino System*.

---

### About the Database Fixup utility

The Fixup server task checks databases for corrupted documents and, if possible, fixes them to prevent server crashes. The first database that Fixup checks and repairs is the log file so that all subsequent repairs can be documented. You can run Fixup one of two ways:

- Automatically, each time the server starts.
- On demand as a command from the server console. You can check all databases on the server or specify one or more databases.

For more information on the Fixup server task, see Chapter 5 in *Maintaining the Domino System*.
About the Log database
The log file (LOG.NSF) records server events, such as replications performed, mail routed, and databases used. The server creates the log file automatically and starts recording information when the server starts.

As part of server maintenance activities, check the log every day to learn about server problems, including replication, mail routing, and modem problems. The log is also an important tool for analyzing your system because it tracks such information as database size and usage, and calls to and from a server.

You can customize what information gets logged through setup options and log views. Your maintenance plan should include what standard information should be logged for a server and some guidelines on how to deal with log data.

Identifying problems with the Log Analysis tool
You can search the log using the Log Analysis tool on the administration panel. The Log Analysis tool allows you to search multiple servers for keywords you specify and direct the search output to an output database you specify. Searching for words such as “error,” “failed,” and “cannot” will lead you to most system problems and help you to isolate potential problems. For example, you use the tool to search the Miscellaneous Event view of several specified servers for all occurrences of the word “corrupt.” You can direct the output to a local copy of a results database to allow for central administration with minimal network traffic.

For more information about the log file and the Log Analysis tool, see Chapter 3 in Maintaining the Domino Server.

Monitoring server events and statistics
Gathering information about server activities falls into two areas: events and statistics. Server events are the errors and alarms for a monitored server. Server statistics track information about a wide range of server activity, such as available memory, disk space usage, mail activity, and communications port activity. By monitoring the statistics for certain conditions, such as low disk space, you can set alarms to head off trouble. Events and statistics are not generated by default; you must run server tasks to collect information at intervals you specify.

You can collect statistics and events data by running a Report task on each server or running a Collector task on a centrally located server. The Collector task collects data for the server running the task plus a number of other servers. Each task stores data in a statistics database and generates alarms based on the contents of a configuration database.
Guidelines for monitoring statistics and events

- Choose a standard set of statistics that you want all server administrators to monitor. Establish alarm thresholds for various server configurations.

- Centralize statistic and event monitoring to reduce administrative overhead. Not every server needs its own Report task and Statistics Reporting database. Instead, run the Collector on a central server and store statistics from various servers in one central database where one administrator can monitor the information.

- Decide how to handle alarms generated by statistic monitoring. For example, you might specify that alarms trigger trouble-tickets that are sent either to a mail-in database or directly to an administrator.

- Use Event Monitors and Message to Event Mapping documents in the Statistics & Events database to automatically monitor messages that get logged to the log file.

- Use access control list (ACL) and Replication Monitors to monitor the ACL and replication schedules of key databases.

- Use the Statistic Analysis reports to look for trends, slow-downs, and peak usage periods over a period of time.

For more information on monitoring statistics and events, see Chapter 3 in *Maintaining the Domino System*. 
Appendix A
Improving Domino Server Performance

Use the following tips to improve the performance of your Domino servers. For more information on technical aspects of server performance, see Getting Started with Domino, Extending the Domino System, and Maintaining the Domino System.

About editing the NOTES.INI file to improve performance

This table lists some of the variables in the NOTES.INI file that you can customize to improve server performance.

<table>
<thead>
<tr>
<th>NOTES.INI variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MailMaxThreads</td>
<td>Determines the maximum number of threads that the mail Router can create to perform its mail transfers efficiently. Without this variable, the default is one thread per server port.</td>
</tr>
<tr>
<td>Memory_Quota</td>
<td>Determines the maximum number of megabytes of virtual memory that Domino is permitted to allocate. Administrators gain more control over the growth of the swap file.</td>
</tr>
<tr>
<td>MinNewMailPoll</td>
<td>Determines how often workstations can contact the server to see if new mail has arrived for the user. This setting overrides the user’s selection in the Mail Setup dialog box. No default is set during server setup.</td>
</tr>
<tr>
<td>NSF_Buffer_Pool_Size</td>
<td>Sets the size of the NSF buffer pool, a section of memory used for buffering I/O transfers between the NSF and NIF indexing functions and disk storage. The default value is usually sufficient, but if users get an error telling them to increase the value of this variable, increase the value a few megabytes at a time. You can use a performance monitor to find out if a larger value is causing too much swapping or paging.</td>
</tr>
</tbody>
</table>

continued
### NOTES.INI variable Description

<table>
<thead>
<tr>
<th>NOTES.INI variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSF_DbCache_Disable</td>
<td>Enables (=0) or disables (=1) database caching. The database cache stores data required to open recently opened databases. A database stored in the cache can be opened more quickly than one not stored in the cache.</td>
</tr>
<tr>
<td>NSF_DbCache_Maxentries</td>
<td>Sets the maximum number of databases stored in the database cache (if enabled). For short intervals Domino will store up to 1.5 times the number entered for this variable. Increasing the maximum number of databases improves performance but requires more memory.</td>
</tr>
<tr>
<td>ServerTasks</td>
<td>Controls the tasks that the server runs. These tasks start automatically at server startup and continue until the server is shut down. Improve performance by removing tasks that aren't appropriate to the server if it is a specialized server. Do not remove the update task from a server. If you do so, the Public Address Book will not update.</td>
</tr>
</tbody>
</table>

For more information on editing system variables in the NOTES.INI file, see Appendix A in *Getting Started with Domino*.

---

### About improving NLM server performance

Since there is no virtual memory in Novell NetWare, install memory for every application or process on the machine. To run Domino, you need a minimum 24MB of memory. 32MB is recommended for 64 users; 48MB is recommended for 128 users. Other NLM servers running on the file server may need additional memory.

To improve performance on an existing Domino server, increase disk space and add more memory. For optimal performance, run the Domino server for NetWare on a dedicated NetWare file server.

### Improving STARTUP.NCF

For good performance on the NLM server, include this line in STARTUP.NCF to ensure that the file server keeps enough network data packets in memory to respond promptly to requests for transferring data across the network:

```
set minimum packet receive buffers=X
```

where X is a number between 10 and 1000, with 10 being the default. Use the NetWare Monitor to check the server's current setting.
Improving AUTOEXEC.NCF

In the AUTOEXEC.NCF file or at the NetWare console, load the Domino server for NetWare before loading the NetWare Monitor. Due to a known problem in the NetWare Monitor program, processor use can approach 100% if you load the Monitor program before loading the Domino server. Modify the AUTOEXEC.NCF file as follows:

- `load notessrv`
- `load monitor`

<table>
<thead>
<tr>
<th>NLM Setting in AUTOEXEC.NCF</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set maximum packet receive buffers=1000</td>
<td>To avoid using all available memory on the server, limit the number of network data packets that can be stored in memory. Specify 1000 when a high number of network transactions is expected. Default is 100. Use the NetWare MONITOR to check the server’s current setting.</td>
</tr>
<tr>
<td>set dirty disk cache delay time=7.5</td>
<td>The dirty disk cache is information in memory that is written to disk shortly. The delay time specifies how long the operating system waits before writing the information to disk. Specify 7.5 seconds to make disk operations more efficient. The range for this variable is between 0.1 seconds and 10 seconds, with 3.3 seconds being the default.</td>
</tr>
<tr>
<td>set minimum file cache buffers=1000</td>
<td>File caching improves file access time by taking the most recently read data from the disk and keeping it in file cache buffers in memory until it's needed. Establishing a minimum number of file cache buffers ensures that a certain amount of memory is dedicated to file caching. Specify 1000 to ensure that Notes users can access files quickly. The range for this variable is between 20 and 1000, with 20 being the default.</td>
</tr>
<tr>
<td>NLM setting in AUTOEXEC.NCF</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>set maximum alloc short term memory=5000000</td>
<td>If you are running NetWare 3.12, you don’t need to change this variable. The default of 8MB should be adequate. The Alloc Short Term Memory pool is a block of memory set aside for the temporary use of the operating system and loadable modules. Specify 5MB to ensure that the NLM server has enough short-term memory to use for its normal operations.</td>
</tr>
<tr>
<td>set immediate purge of deleted file=on</td>
<td>Determines whether you can recover accidentally deleted files using the NetWare FILER’s “Salvage deleted file” option. The default is OFF, which allows recovery of deleted files. Set to ON increases the amount of disk space available, but can cause users inconvenience.</td>
</tr>
<tr>
<td>set reply to get nearest server=off</td>
<td>When set to ON, the server must respond to “Get Nearest Server” requests from workstations. Set the default setting (OFF) to conserve server processing time.</td>
</tr>
<tr>
<td>set enable disk read after write verify=off</td>
<td>When information is written to disk, this setting determines whether the information is compared against the same information held in memory. The default setting is ON, which ensures the integrity of the data. Setting to OFF speeds up disk operations, but increases the risk of corrupted files.</td>
</tr>
</tbody>
</table>

**About improving OS/2 Warp server performance**

To improve performance on existing Domino OS/2 Warp servers, increase disk space and add more memory (a minimum of 16MB of memory is recommended). Buy a LOCALBUS disk controller to achieve faster data transfer rates than with a PC/AT bus.

**Choosing a file system**

OS/2 Warp provides a choice for the Domino server file system. The File Allocation Table (FAT) system is the traditional system used in DOS. High Performance File System (HPFS) is an OS/2 Warp-specific system. Domino works equally well on both file systems.
HPFS systems are usually three times faster than FAT systems and allow for better storage of small files, although the drive is not shareable with DOS and requires a long boot time after a crash. FAT systems allow you to share a drive with DOS so systems can be dual-boot, but they are slower and provide poorer storage for small files.

**Disk swapping**

OS/2 Warp makes extensive use of disk swap space. Be sure that the drive where OS2\SYSTEM\SWAPPER.DAT resides has at least 5MB to 10MB free for normal expansion by OS/2 Warp. OS/2 Warp uses this file as virtual memory.

To enable disk swapping, Domino requires the following statement in the CONFIG.SYS file:

```
MEMMAN=SWAP,MOVE
```

When the swap file becomes too big, which is usually due to low memory conditions, server performance deteriorates and the server may crash. Restart the server to clear the swap file and then automatically reset the file to the default value of 512KB.

If the swap file consistently exceeds 20 percent or more of RAM, increase system memory to the maximum size allowed by OS/2 Warp. For example, with 6MB RAM and a swap file of 1.5MB, the swap file is 25 percent of RAM. To improve performance, add 2MB of RAM.

**Disk caching**

Disk caching keeps the most recently read data in RAM until it's needed again. By setting up a disk cache, you can dramatically improve the time it takes for Domino to read data from the disk.

**HPFS**

Set the HPFS cache to 10 to 15 percent of the total available RAM, up to a maximum disk cache of 2048K. To set the DISKCACHE to 1536 blocks (1 block=1K), enter the following IFS and RUN statements in the CONFIG.SYS file:

```
IFS=C:\LANMAN\NETPROG\HPFS386.IFS /I:C:\LANMAN /AUTOCHECK:DE
RUN=C:\LANMAN \NETPROG\CACHE386.EXE /LAZY:ON /MAXAGE:5000
 /BUFFERIDLE:500
```

**FAT**

Set DISKCACHE between 512 to 1024 blocks. To set DISKCACHE to 1024 blocks (1 block=1K), enter the following statement in the CONFIG.SYS file:

```
DISKCACHE=1024 blocks
```

Appendix A: Improving Domino Server Performance 147
Configuring memory

Good server performance depends on adequate memory. Configure a new server with the maximum amount of memory you can afford. If you have a performance problem with an existing server, increasing memory should help.

Note  OS/2 2.x can handle more than 16MB of RAM. To force Domino to take advantage of more than 6MB, set the NOTES.INI variable NSF_Buffer_Pool_Size.

Configuring your disk

Follow these guidelines for optimal disk performance:

- Use many small disks rather than one large disk. For example, four 300MB drives are preferable to one 1.2GB drive.
- If you have more than one drive, do not put databases on the same drive as the swap file. You can, however, put the Domino program and library files on the drive with the swap file.
- Defragment your disks regularly.
- Allow for growth on the disk that contains the LOG.NSF and STATREP.NSF databases, as well as on disks that contain any databases that could grow large.

For more information on monitoring server performance, see Chapter 3 in Maintaining the Domino System. For information on editing system variables in the NOTES.INI file, see Appendix A in Getting Started with Domino.

About improving Windows NT and Windows 95 performance

If you experience a high page fault rate and a high page I/O as a result of Domino server processes running on a Windows NT Advanced Server configuration, check the configuration file. You will probably find that the following Registry entry in the configuration file is non-zero:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\LargeSystemCache
```

This entry specifies that the Windows NT system should work as a file server rather than an application server because Windows NT will favor the system-cache working set rather than the processes working set. On a Windows NT workstation, the setting for that Registry entry is zero.

If you are running a Domino server on a Windows NT system set as a file server, the excessive page faults and paging activities can result from memory-intensive processes. For example, rebuilding the index for a large
database might result in an undesirable level of paging, causing users to experience poor response times.

To correct the problem, reset the Registry entry to zero and reboot the system.

For more information on monitoring server performance, see Chapter 3 in *Maintaining the Domino System*.

---

**About improving UNIX server performance**

When a UNIX system runs Domino server software, the server must have enough disk space for program and data files and enough memory to handle swapping and the number of processes. You can also change several system parameters to improve server performance.

For information on system requirements and improving performance on a UNIX server, see the Release Notes for your UNIX platform.
Index

A
Access
planning for, 31
Access Control Lists
and database security, 130
Access levels
described, 130
ACL
and database security, 130
Address Book
Public and LDAP planning, 46
Administration
about planning for, 21
and performance guidelines, 137
tasks, 135
Administration Process
described, 138
Administration server
performance, 80
Advanced Services
and messaging, 43
described, 62
planning, 31
APIs
and applications, 33
Applications
creating, 33
deploying, 33
deploying to Internet, 35
distributing on servers, 37
Internet security and, 35
intranets and, 53
programming tools and, 33
security planning, 23
using on intranets, 53
Assessing
business needs, 8
employee capabilities, 9
employee needs, 9
organizational needs, 7
technical issues, 8
AUTOEXEC.NCF, using to improve performance, 145

B
Binary tree, 63
Browsers
security in a Domino system, 128
Business processes
reengineering, 7
refining, 7
C
Caching
disk, 147
Calendar
setting up, 117
Capacity
intranets and, 55
planning for, 14
CERT.ID, 124
Certificates
described, 124
Certification
described, 124
Certifiers
described, 125
Chain, 63
Clients
automated installation, 85
deploying, 83
deploying Notes, 84
security planning, 23
Cluster, 63
CONFIG.SYS
disk swapping, 147
Configuration scenarios
SMTP/MIME MTA,
97, 100-101, 105
Configuring
SMTP/MIME MTA,
95-97, 100-102, 105
Conflicts
replication, 76
save, 77
Connection documents
described, 88
mail routing and, 114
Connections
testing, 96
Conventions
naming, 24
Creating
an intranet, 49
Cross-certificates
described, 124
Cross-certification
described, 124

D
Databases
copies, 71
deploying, 33
deploying to Internet, 35
design, 36
distributing on servers, 37
encryption and, 131
Fixup program, 139
maintenance, 37
replicas, 71
security, 132
security of design
elements, 132
system administration, 137
Dead mail, 139
Deployment
clients, 83
multiple protocols and, 69
Notes, 84
Public Address Book, 78
replication planning and, 70
Directory assistance, 111
Disk
caching on OS/2 Warp
server, 147
configuring for OS/2 Warp
server, 148
running on a file server, 68
SAP R/3 and, 28
security overview, 119
server administration tasks, 135
server performance
guidelines, 137
server security, 127
server topology and
replication, 62
setting up, 61, 72
TCP socket, 120
transaction processing and, 28
using, 1
Web sites, 40
Web tools, 40
Domino.Action
creating a Web site with, 41
Domino.Broadcast
and Domino intranet, 27
Domino named networks
described, 88
mail routing and, 114
Domino newsgroups, 47
Domino NNTP server
planning, 47
Domino Server.Planner
capacity planning and, 14
NotesBench and, 15
scalability and, 14

F
Fields
security, 132
File servers
running Domino on, 68
Firewalls
described, 120
Internet and, 100
Folders
security, 132
Forms
security, 132
Formulas
performance, 36

G
Growth
planning for, 13

H
Hierarchical naming, 124
Hub, 62
Hub-spoke, 63

I
IDs
security and, 86, 128
storing, 86
IMAP
mail access, 116
Inbound work queue, 94
Indexes
performance and, 37
Indexing
performance, 36
Information
on Lotus Web sites, 4
Integration
Domino and Windows NT, 69
Internet
creating a Domino
Web site, 40, 41
Domino features, 39
infrastructure planning, 42
messaging planning, 43
planning, 16
security planning, 23
SMTP/MIME MTA,
97, 100-101, 105
using Domino, 39
Internet commerce
and Domino.Merchant, 29
Internet mail
IMAP, 90
POP3, 90
Internet security
types, 120
Intranets
applications, 53
capacity, 55
creating, 27
creating with Domino, 49
Domino.Broadcast and, 54
Domino Server.Planner and, 55
features, 51
mail and, 54
Notes and, 49
planning, 17, 49
push technology and, 54
return on investment and, 51
scalability, 55
security, 52
SMTP/MIME MTA, 101, 105
types of, 49
using, 51
Web browsers and, 49

L
LDAP
planning, 43, 46
security, 46
Links
to Lotus Web sites, 4
Log
described, 140
replication monitoring, 78
Log.NSF
described, 140
Log analysis tool
described, 140
Log files
described, 140

M
Mail
accessing from POP3
or IMAP, 116
concepts described, 88
dead, 139
deploying, 87
extranets and, 59
Internet and, 90
Internet clients, 116
intranets and, 54
MAPI clients and, 116
MIME, 90
multiple format planning, 43
priority levels, 115
routing, 110, 113, 114
routing planning, 88
security, 133
security planning, 23
shared, 116
storage formats, 115
terms described, 88
MAIL.BOX and, 89
Mail routing
Connection documents and, 114
different domains, 110
Domino named
network and, 113, 114
Internet-to-Notes, 90
Notes-to-Internet, 90
overview, 90
planning, 89
Public Address Books and, 111
same domains, 110
Maintenance
checking log file, 140
databases and, 37
running Fixup, 139
MAPI
and accessing mail, 116
Memory
performance and, 144, 148
Message Transfer Agents
multiple mail programs and, 87
using, 43
Messaging
planning, 43
MIME
described, 45
MTA tables database, 94
MTAs
using, 43
MTATABLES.NSF, 94
NAMES.NSF
described, 78
Naming
conventions, 24
NetWare servers
performance and, 144
Network
security planning, 23
NNTP
and Domino newsgroups, 47
Notes
automated installation, 85
creating users, 84
deploying, 84
ECL and, 128
security and, 128
NOTES.INI file
ingo, 143
NotesBench, 15

O
OS/2 Warp
disk swapping, 147
OS/2 Warp servers
performance, 146
Outbound work queue, 94

P
Partitioned servers
described, 62
Passthru, 68
Passwords and Notes, 128
Peer-peer, 63
Performance
AUTOEXEC.NCF and, 145
configuring OS/2 Warp
servers, 148
database, 36
full text search and, 37
guidelines, 137
NetWare servers, 144
optimizing server, 136
OS/2 Warp disk
swapping and, 147
OS/2 Warp servers, 147
Public Address Book and, 80
replication, 75
STARTUP.NCF and, 144
UNIX servers, 149
Windows 95 servers, 148
Windows NT servers, 148
Permissions
and database security, 130
Pilot project
planning, 19
Ping utility
using, 95, 96

Index-3
Planning
  administration tasks, 22
  Advanced Services, 31
capacity, 15
clients and, 17
database replicas, 37
deployment, 10, 18, 19
Domino and the Internet, 16
Domino integration, 12
Domino newsgroups, 47
Domino rollout, 10, 18, 19
extranet security, 58
failproof access, 31
growth, 13
information systems, 12
integrating Domino into activities, 19
Internet, 16
Internet infrastructure, 42
intranet, 17
LDAP access to the Public Address Book, 46
messaging, 43
moving to Domino, 10
Notes clients, 17
NotesBench and, 15
organization level, 10
organizational needs, 7
pilot project, 19
replication, 70
replication policies, 76
replication scheduling, 73
rollout support, 20
rollout team, 11
scalability, 13
security, 23
server administration, 21
workgroup rollout, 18
Planning the Domino System
  about using, 3
Policies
  replication, 76
POP3
  mail access, 116
Priority levels
  and mail, 115
Programming tools
  and applications, 33
Protocols
  and Domino, 69
Proxy servers
  security, 121
Public Address Book
  cascading, 112
deploying, 78
described, 78
directory assistance, 111
docs, 78
LDAP planning and, 46
mail routing and, 111
managing, 111
performance and, 80
Replica IDs
defined, 71
Replicas
creating, 37
local, 76
Notes workstations and, 76
using, 76
Replicating servers, 72
Replication
  access, 72
  conflicts, 76
  control, 72
  history, 72
  local replicas and, 76
  monitoring, 78
  organization and, 71
  performance and, 75
  planning, 37, 70
  planning scheduling, 73
  policies, 76
  scheduling, 73
  server topology and, 62
  servers and, 72
RFCs
  supported in SMTP MTA, 45
Ring, 63
Roles
  and database security, 131
Rollout
  clients, 83
  multiple protocols and, 69
  Notes, 84
  Public Address Book, 78
router
described, 88
Routing table
described, 88
S
Save
  conflicts, 77
Scalability
  Domino Server.Planner and, 14
  intranets and, 55
  NotesBench and, 15
  planning for, 13, 15
  planning with Domino Server.Planner, 14
  protocols and, 13
  servers and, 13
Scheduling
  replication, 73
  setting up, 117
Sections
  security, 132
Security
  access control for servers, 127
  access control list, 130
  considerations, 119
  database, 130, 132
  database encryption and, 131
digital signatures and, 123
  encryption and, 121
  extranets and, 58
  firewalls, 120
  Internet, 120
  Internet users and, 128
  intranets, 52
  mail and, 133
  network, 122
  Notes client and, 128
  Notes ECL and, 124
  overview, 119
physical, 124
  proxy servers, 121
remote access and, 123
  servers, 127
viruses, 123
Web browser clients and, 128
Server access list
described, 127
Server administration
  planning for, 21
Servers
  administrator tasks, 135
  authentication and, 127
  capacity planning, 14
  checking for dead mail, 139
  connecting for mail routing, 114
  designating by task, 66
Servers (continued)

- dividing administration tasks, 137
- editing NOTES.INI for performance, 143
- events, 140
- installing, 61
- monitoring, 138
- naming guidelines, 25
- optimizing performance, 136
- passthru, 68
- performance guidelines and, 137
- planning for growth, 13
- replicating, 72
- replication and, 62
- scalability, 14
- scheduling replication, 73
- security planning, 23
- setting up, 61
- statistics, 140
- system administration, 137
- UNIX performance and, 149

Setting up

- Domino servers, 61

Setup Profile

- creating, 85

Shared mail

- described, 116

Sharing information

- Sites, Lotus Web, 4

SMTP.BOX

- overview, 94

SMTP/MIME MTA

- components, 92
- configuring, 95
- databases used, 94
- Internet mail access and, 116
- overview, 45
- tasks, 92

SMTP/MIME MTA configuration scenarios

- examples, 96
- Internet and, 97, 100-101, 105
- intranet and, 101, 105

SMTP/BWQ.NSF, 94

SMTPMTA server tasks

- IMSGCNV, 92
- ISESCTL, 92
- ISESHLRn, 92
- OMSGCNV, 92
- OSESCTL, 92
- OSESHLRn, 92
- SMTP/BWQ.NSF, 94

SSL

- and Internet clients, 128

Statistics

- server, 140
- Support and Domino, 20

Synchronization

- Domino and Windows NT, 69

T

Tasks

- Add-in Controller, 92
- administration, 135
- Delivery Report, 92
- Inbound Message Conversion, 92
- Inbound Session Controller, 92
- Inbound Session Handler, 92
- Outbound Message Conversion, 92
- Outbound Session Controller, 92
- Outbound Session Handler, 92
- overview, 92
- servers and, 66
- SMTPMTA server, 92
- Testing connections, 96
- Topology and replication, 62

U

UNIX servers

- performance and, 149

URLs

- to Lotus Web sites, 4

Users

- registering, 85

V

Views

- performance, 36
- security, 132

W

- Web browsers security and, 128
- Web sites, 4
- Windows 95 servers
  
- performance and, 148
- Windows NT
  
- integration with Domino, 69
- Windows NT servers
  
- performance and, 148
- Workgroup and rolling out Domino, 18