Internet Exchange
for cc:Mail and Lotus Notes

Gateway Administrator's Manual

Version 3.0
January 1998

International Messaging Associates Limited
Hong Kong Computer Center, 3/F
54-62 Lockhart Rd
Wanchai
HONG KONG

Tel: +1 (408) 481-9985
+1 (888) 562-3564
+852 2520-0300
+63 (2) 811-3999
Fax: +1 (888) 562-3561
+852 2648-5913
+63 (2) 811-3939
Email: *info@ima.com*
WWW: *http://www.ima.com/*

IMA Philippines, Inc.
The Peak Tower, 15/F
106 Alfaro Street
Salcedo Village, Makati
PHILIPPINES

USA - Sunnyvale, California
USA - Message Center
Hong Kong
Philippines - Makati
USA
Hong Kong
Philippines - Makati

ISBN: 962-8137-02-6

TABLE OF CONTENTS

APPENDICES

PREFACE

OVERVIEW

Internet Exchange is a family of electronic mail gateway/MTA's that connect either Lotus cc:Mail or Lotus Notes Local Area Network email environments to the Internet, and/or to private TCP/IP based Local Area Networks. **Internet Exchange** is the most advanced and complete gateway technology linking cc:Mail and Notes users with the Internet.

This manual describes two versions of **Internet Exchange**: **Internet Exchange for cc:Mail**, and **Internet Exchange for Lotus Notes**. Each version of **Internet Exchange** is available in two editions: the *Enterprise Edition* (unlimited usage), and the *Workgroup Edition* (limit of 100 users). With the exception of the number of users restriction, default address mapping options, and default send/receive permissions, the two versions are identical. The few areas where there are differences are noted in this manual.

Both versions of **Internet Exchange** (the cc:Mail and Notes versions) are very similar, and will be treated identically except where noted in this manual. The main differences between the two versions are in the areas of Installation, Address mapping, and POP3 Server support (not included with the Notes version).

Throughout this manual, the term "Internet" is considered to be interchangeable with any TCP/IP based network or collection of networks.

This manual describes how to configure, use, and administer **Internet Exchange**. It contains the following sections:

- **Part 1**, "*Introduction*" introduces the technologies in **Internet Exchange**. The overall architecture is outlined here.

- **Part 2**, "*Installation*", describes how to install **Internet Exchange** and its components.

- **Part 3**, "*Operation*," describes how to set up and use **Internet Exchange**, including details on such topics as configuration, initialization, rules based addressing, peer domain configuration, Japanese support, remote management and gateway monitoring.

- **Appendices** - The appendices present more detailed information on topics related to **Internet Exchange** including introductions to electronic mail addressing, SMTP, MIME, TCP/IP, Apple Macintosh file structures, Attachment Naming conventions, and the Domain Name System (DNS).

REQUIREMENTS

This section describes the hardware and software requirements necessary to run **Internet Exchange**.

Hardware

The minimum hardware requirements for **Internet Exchange** are:

- **Processor:** 80486-DX or higher
- **Memory (cc:Mail Version):** 16MB for Windows 95 (32MB recommended), 32MB for Windows NT Server (48MB recommended)

- **Memory (Notes Version):** 32MB for Windows 95 (64MB recommended), 48MB for Windows NT Server (96MB recommended)
- **Hard Disk:** 200 MB or more
- **Monitor:** Any Windows VGA resolution or higher monitor
- **Mouse:** Any Windows-supported mouse
- **Network Interface Adapter:** Any network interface board that is hardware compatible with your TCP/IP network, with support for at least one of the following drivers: ODI, NDIS, or packet drivers. This network interface board will communicate with other hosts on your TCP/IP network. In addition, if the connection to your cc:Mail Post Office or Lotus Notes Domain is over a LAN with a different cabling system than your TCP/IP network, you will need a separate Network Interface Adapter for that network as well.

Software

The software requirements for **Internet Exchange** are as follows:

- **Operating System:** One of the following:
    - Microsoft Windows NT Server 3.51 with Service Pack 5 or higher installed
    - Microsoft Windows NT Server 4.0 with Service Pack 3 or higher installed
    - Microsoft Windows 95 with Service Pack 1 and Kernel32 Update installed
- **TCP/IP:** TCP/IP protocol stack compliant with WINSOCK Version 1.1. Microsoft Windows NT Server 3.51 and 4.0 and Windows 95 both come with built-in stacks that meet this requirement.
- **VIM:** (*Internet Exchange for cc:Mail only)* Lotus 32-bit VIM (version 6.03 or later) for cc:Mail. The VIM (Vendor

Independent Messaging) library is used to read from and write to the cc:Mail Post Office.

- **Lotus Notes 4.x Client / Server:** (*Internet Exchange for Lotus Notes only)* The Lotus Notes 4.x Client or Server needs to be installed on the same machine as **Internet Exchange**.

INSTALLATION

Internet Exchange is a network application that operates in a Microsoft Windows environment. It requires the ability to communicate with the TCP/IP network via a WINSOCK Version 1.1 compliant interface. The cc:Mail version of **Internet Exchange** also requires a Lotus cc:Mail 32-bit VIM Version 6.03 or greater interface to communicate with the cc:Mail Post Office, while the Notes version requires the Notes 4.x Client or Server to be co-resident.

To install **Internet Exchange**, the administrator must perform the following tasks:

1. Locate and install all hardware and software shown in the table above.

2. Install and configure the software necessary to communicate with your LAN Network Operating System. Examples of common Network Operating Systems include NetWare®, LANtastic®, LAN Manager®, and others.

3. Install and configure the software necessary to communicate with your TCP/IP network.

4. For cc:Mail installations, make sure the proper VIM cc:Mail libraries have been installed and accessible to the gateway machine. For Notes installations, make sure that either the Notes 4.x Client or 4.x Server have been installed locally.

5. Install **Internet Exchange**.

CONVENTIONS USED IN THIS MANUAL

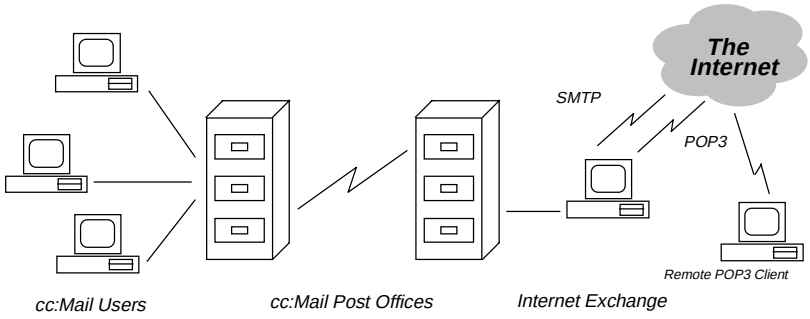
To provide addressing examples, we have taken the case of an organization called Jade Networks, which uses the fully qualified domain name of jade.net, and operates an Internet Exchange gateway with the fully qualified domain name of iegate.jade.net. Examples involving remote sites use a company called XYZ Corp, with a FQDN of xyz.org.

PART 1 INTRODUCTION

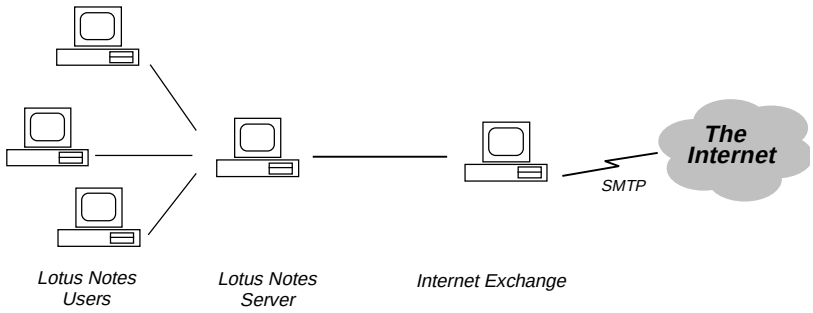
CHAPTER 1
INTERNET EXCHANGE FUNCTIONAL OVERVIEW

INTRODUCTION

Internet Exchange acts as a bridge between either a cc:Mail Post Office or a Lotus Notes Server and the Internet (or any TCP/IP network). The relationship between the **Internet Exchange** gateway/MTA, the cc:Mail or Notes environments and the Internet (or your local TCP/IP network) are shown in the figures below.



Internet Exchange *Bridging cc:Mail and the Internet*



Internet Exchange *Bridging Lotus Notes and the Internet*

Internet Exchange takes messages from the cc:Mail and Notes environments and converts the messages and user addresses into formats understood on the Internet. In the other direction, **Internet Exchange** takes messages and addresses of the format understood on the Internet and converts them into messages and addresses that can be dealt with in either the cc:Mail or Notes environments. This conversion process is transparent to end users on both sides of the gateway. Because of the translation effected at the gateway, cc:Mail and Notes users appear as Internet users on the Internet side of the gateway, and Internet users appear as either cc:Mail or Notes users in the cc:Mail or Notes environments.

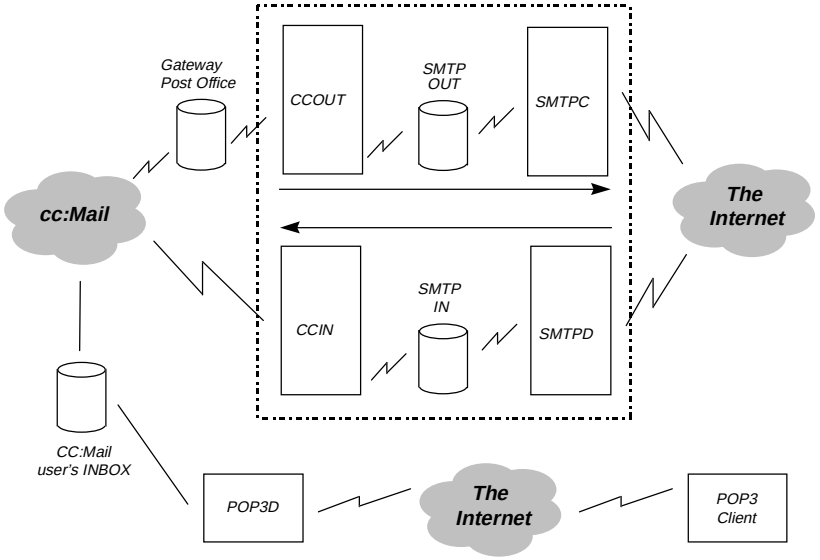
A Post Office Protocol 3 (POP3) server has been integrated into **Internet Exchange for cc:Mail**, making it possible for users to access their mail by using a POP3 mail client. POP3 is discussed in greater detail in Part 3 of this guide. This functionality has not been added for the Notes version of **Internet Exchange** as Lotus Notes already has much of this functionality builtin due to it's inherit client/server architecture.

Internet Exchange possesses a web browser-based *Remote Control* in order to provide administrators with a secure and convenient way to monitor, configure and operate the gateway remotely. The *Remote Control* is discussed in more detail in Part 3 of this guide, while installation procedures are described in Part 2.

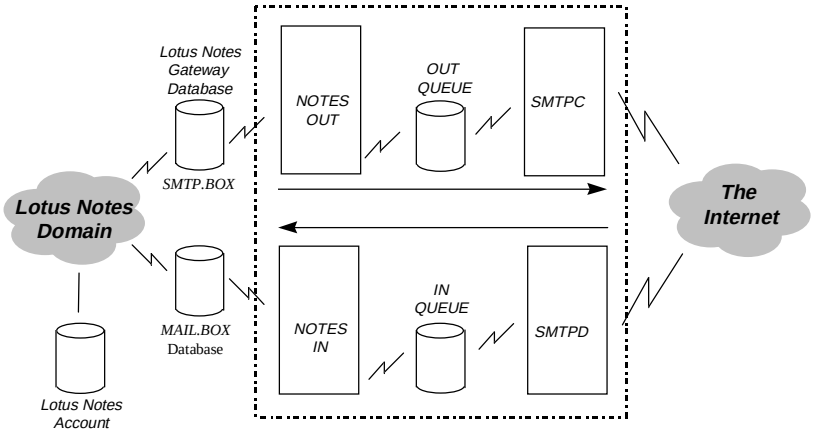
INTERNET EXCHANGE ARCHITECTURE

Internet Exchange is a 32-bit multiprocess, multitasking gateway. Its 32-bit implementation assures greater speed, stability and integration with the Windows 95 and NT operating systems. The various components operate asynchronously with respect to each other, allowing the gateway to handle many tasks simultaneously. Since the communications channels are typically much slower than the host processor, the gateway has the ability to service several channels at the same time. In addition, message and address conversion can be effected while other messages are being transferred. This multiprocessing capability has the effect of maximizing overall gateway throughput.

Internet Exchange is divided into the following functional components:



Internet Exchange for cc:Mail *Functional Block Diagram*



Internet Exchange for Lotus Notes *Functional Block Diagram*

cc:Mail Gateway Post Office *(cc:Mail Version)*

When cc:Mail users send mail to users on the Internet, they do so by sending the mail to the cc:Mail remote post office name that is assigned to the gateway. The cc:Mail post office that acts as the mail forwarder will contain an entry for the gateway post office in its directory. Mail that arrives for the gateway post office will be temporarily stored in the gateway post office mailbox.

In the cc:Mail environment, **Internet Exchange** acts as the gateway post office. Like all other cc:Mail post offices, it is given a unique name, typically *Internet* (although any unique name will work). **Internet Exchange** regularly polls the gateway mailbox on the forwarding post office. This ensures the regular pickup of mail leaving the cc:Mail domain for the Internet.

Internet Exchange is also responsible for regularly checking for inbound messages. It delivers any messages found to the forwarding post office for either final delivery to a user mailbox or for further routing within the cc:Mail domain.

Interaction with the cc:Mail post office

Internet Exchange communicates with cc:Mail using the VIM (Vendor Independent Messaging) protocol. There are two separate programs that talk to the cc:Mail post office, one of which imports messages from the Internet, and one that exports messages from cc:Mail bound for the Internet.

Lotus Notes Gateway Database *(Notes Version)*

When Lotus Notes users send mail to users on the Internet, they do so by sending the mail to the Lotus Notes database that is assigned to the gateway. Mail that arrives for the gateway will be temporarily stored in this database, which is called *SMTP.BOX*.

Internet Exchange regularly checks *SMTP.BOX* to ensure the regular pickup of mail leaving the Lotus Notes domain for the Internet. Incoming mail is placed in a second temporary store, *MAIL.BOX*, also on the Lotus Notes server. For further information see the sections "Outgoing Mail" and "Incoming Mail" later in this chapter.

SMTP.BOX must be configured for Internet Mail and access control lists (ACLs) must be configured for this and for the *MAIL.BOX* database, as described in the sections "Creating a New Database" and "Setting up Access Control" in Chapter 4.

Interaction with Lotus Notes

Internet Exchange communicates with Lotus Notes using the Lotus Notes API (Application Programming Interface). There are two separate programs that talk to Lotus Notes, one of which imports messages from the Internet, and one that exports messages from Lotus Notes bound for the Internet.

Interaction with the Internet

Internet Exchange communicates with mail hosts on the Internet using the **S**imple **M**ail **T**ransfer **P**rotocol (SMTP). This protocol is used for the submission as well as the reception of mail messages. **Internet Exchange** implements SMTP as two separate modules. A client program sends messages from the gateway to the Internet, and a server program receives messages from the Internet bound for the local environment.

Outgoing Mail

Exporting messages from the local Lotus environment to the Internet involves two queue processors: *SMTPC* and either *CCOUT* for the cc:Mail version of **Internet Exchange**, or *NOTESOUT* for the Notes version.

CCOUT

CCOUT obtains messages from cc:Mail by polling the gateway post office. The gateway administrator determines the polling interval, which can be set for as often as once every minute.

The module that performs the polling of the cc:Mail gateway post office and transfers messages into the gateway is *CCOUT*. *CCOUT* logs into the post office using the cc:Mail VIM interface. If messages are present, it will move each message, one at a time out of the gateway post office and into an internal gateway queue (*SMTP OUT*). In the process of moving a message into the *SMTP OUT* queue, *CCOUT* will perform any address and message format translations necessary. *CCOUT* is also responsible for creation of the initial SMTP envelope.

NOTESOUT

NOTESOUT obtains messages from Lotus Notes by polling *SMTP.BOX*. The gateway administrator determines the polling interval, which can be set for as often as once every minute.

NOTESOUT logs into the *SMTP.BOX* using the Lotus Notes API. If messages are present, it will move each message, one at a time out

of *SMTP.BOX* and into an internal gateway queue (*SMTP OUT*). In the process of moving a message into the *SMTP OUT* queue, *NOTESOUT* will perform any address and message format translations necessary. *NOTESOUT* is also responsible for the creation of the initial SMTP envelope.

SMTPC

The SMTP client program (*SMTPC)* is responsible for delivery of messages on the Internet. It does so by regularly checking for messages queued in the *SMTP OUT* queue. When messages are found, it establishes the required number of connections with external SMTP servers (up to a maximum of 120 concurrent connections) and transfers the messages to the appropriate Internet mail hosts. *SMTPC* is multi-threaded, which means that it is able to transmit several mail messages concurrently. In versions of **Internet Exchange** earlier than 3.0, *SMTPC* could only deliver one message at a time; the development of being able to pick up and deliver a number of messages together in the same thread has greatly increased mail transmission efficiency.

The **Internet Exchange** SMTP client program is capable of routing Internet mail messages based on several criteria. The routing options are:

- Domain Name System (DNS) host name lookup
- Host Table lookup of destination host
- DNS followed by Host Table lookup
- Host Table followed by DNS lookup
- Delivery to default mail relay host(s)

Mail routing via the DNS is the preferred method of mail routing in the Internet. The DNS is an Internet network service that provides for the storage and retrieval of information associated with domain names. In the context of Internet mail, the records that are of interest are mail exchanger (MX) records and address (A) records.

MX-records are used to store mail forwarder information for hosts registered in the Internet. An MX-record will contain the name of the host or domain, and a list of one or more mail forwarding hosts and the preference values associated with these hosts. The preference values are used by *SMTPC* to determine the order to attempt delivery in the case where more than one mail forwarder has been identified. MX-records are essential for the proper routing of mail, especially in situations where the destination host is not physically connected to the Internet and has to rely upon a mail forwarder for proper mail delivery. As an example, many organizations rely upon the UUCP communications package which comes with the UNIX operating system to physically exchange mail. These sites, can, by using MX-records, appear to be connected to the Internet even though mail is the only Internet service they use.

A-records are used to store Internet address information for hosts. When configured to use the DNS, **Internet Exchange** attempts to obtain an MX-record for the destination host. If an MX-record is found, the list of mail forwarding hosts is used when the SMTP connection is attempted. If no MX-record can be found, **Internet Exchange** searches for an A-record. If an A-record is found, then this address is used when the SMTP connection is established.

If the SMTP client is configured to use host table lookup, the internal host table, usually a text file, is used to determine the Internet IP address of the recipient host. The exact format and path name of the host table depends upon the TCP implementation. The location of the host table is specified when **Internet Exchange** is installed. This is the equivalent of doing an A-record lookup using the DNS. However most internal host tables are nowhere near as complete databases as that which the DNS can provide.

When configured to use a default mail relay host, all messages will be sent to a primary mail forwarder for further routing. If this mail forwarder cannot be contacted for any reason, and a secondary mail relay host is defined, the gateway will use the secondary mail relay. In this case, It will occasionally check to see if and when it is possible to switch back to use the primary relay host. Use of this option will improve gateway throughput, as mail forwarding hosts are usually on the same network as the gateway. Response time and throughput are typically fast, resulting in little to no backlog of

messages at the gateway. The use of this option, however, places the burden of routing and retries of delayed messages on the mail forwarding machine(s), which will add to existing workload.

Internet Exchange can be configured to use a combination of the above strategies to deliver mail. When not using a mail relay, it is recommended to use a strategy where the DNS is consulted first, and then a local host table in the event of a failure to resolve a name with the DNS. The opposite configuration can also be used if needed. In any event, if the name cannot be resolved using either of the above methods, **Internet Exchange** will fall back to using the mail relay host(s) as the next hop (assuming there is at least one configured), in the hope that resolution can be better handled at that site.

Incoming Mail

Receiving messages from the Internet into the local environment involves two queue processors: *SMTPD* and either *CCIN* for the cc:Mail version of **Internet Exchange** or *NOTESIN* for the Notes version.

SMTPD

The **Internet Exchange** module that receives messages from the Internet is the SMTP daemon *SMTPD*. Unlike the other **Internet Exchange** modules, *SMTPD* is a server process that continuously runs on the gateway machine. This is necessary because there is no way for the gateway to predict the timing or frequency of inbound messages.

SMTPD is a background Windows process that listens for incoming SMTP connections on TCP port 25. When a connection request is detected, it creates a new thread that manages the new connection. *SMTPD* is capable of maintaining several simultaneous SMTP connections, the maximum number of which is a configurable parameter that can be set based upon the performance of the underlying TCP/IP stack. The maximum permitted is 256 concurrent sessions. This ability to handle concurrent SMTP sessions reduces delay in message delivery as remote mail

forwarders do not have to wait for an existing SMTP session to complete.

When a message is received by *SMTPD*, it is placed in the gateway queue *SMTP IN*. *SMTPD* does not perform any message translation. It simply creates the queue entry and goes back to wait for additional connection requests.

CCIN

Mail messages are delivered to the cc:Mail environment by the **Internet Exchange** module *CCIN*. *CCIN* is run by *SYSMAN* at regular intervals, and is responsible for moving messages between the *SMTP IN* queue and the cc:Mail post office. The frequency at which *CCIN* is run is a configuration option set by the gateway administrator.

When *CCIN* is run, it checks the *SMTP IN* queue for any messages. Anti-spam and mail-forwarding are conducted prior to any address and message conversion. Then, for each message that *CCIN* finds in the *SMTP IN* queue, it performs address and possibly message content translation in preparation for submission to cc:Mail. Addresses are converted to a form that can be used in the cc:Mail environment. For messages that are multipart or are encoded non-textual data, message conversion is performed by *CCIN* prior to delivery to cc:Mail.

Once the message is properly converted, *CCIN* logs into the gateway cc:Mail post office, and delivers the message. The message is either directly delivered to a local cc:Mail user, or further routed within the cc:Mail domain.

NOTESIN

Mail messages are delivered to the Lotus Notes environment by the **Internet Exchange** module *NOTESIN*. *NOTESIN* is controlled by the system manager (*SYSMAN)* and is responsible for moving messages between the *SMTP IN* queue and the Lotus Notes environment. The frequency at which *SYSMAN* checks *NOTESIN* is a configuration option set by the gateway administrator.

NOTESIN first checks the *SMTP IN* queue for any messages. For each message that it finds, it performs address and, possibly, message content translation in preparation for submission to Lotus Notes. Addresses are converted to a form that can be used in the Lotus Notes environment. For messages that are multipart or are encoded non-textual data, message conversion is performed by *NOTESIN* prior to delivery to Lotus Notes.

Once the message is properly converted, *NOTESIN* connects to the *MAIL.BOX* database in the Lotus Notes Server, and delivers the message. The message is either delivered directly to a local Lotus Notes user, or further routed within the Lotus Notes domain.

POP3 Server *(cc:Mail Version only)*

Internet Exchange for cc:Mail features a completely functional POP3 (Post Office Protocol version 3) Server which is fully compliant with RFC-1939. The POP3 Server is also referred to as POP3 Daemon, or *POP3D*.

The POP3 implementation permits compliant clients such as Qualcomm's Eudora or Netscape Mail to retrieve cc:Mail post office mail via **Internet Exchange**. It also permits retrieval of e-mail messages via TCP/IP protocol over remote networks (such as the Internet) without the use of cc:Mail For Mobile Users, which renders it indispensable to travelers.

NOTE: POP3 is used solely for retrieving email.

The *POP3D* control panel interfaces seamlessly with **Internet Exchange**'s Graphical User Interface (GUI) and, like *CCIN* and *CCOUT*, uses 32-bit VIM libraries to communicate with, authenticate and retrieve mail messages from the cc:Mail Post Office. This permits full multi-threaded access to the cc:Mail Post Office for faster mailbox access speeds and improved efficiency over conventional methods.

Internet Exchange System Manager

The **Internet Exchange** System Manager (*SYSMAN*), also known as the Control Panel, is the front end that allows configuration of the gateway, as well as the regular scheduling of gateway activity. The System Manager keeps track of the times and frequency at which the various queue managers are run, and is responsible for the launching of these managers.

In addition to being the glue that ties the different **Internet Exchange** modules together, the System Manager is used to configure and administer the gateway. All configuration options, including those associated with the cc:Mail post office/Lotus Notes Server, message routing strategy, Internet host name, scheduling, MIME file mapping, and user address mapping are handled by the System Manager.

SYSMAN also provides views of each of the three gateway queues: *SMTP IN*, *SMTP OUT*, and the outbound cc:Mail post office mailbox or Lotus Notes mailbox. The administrator can obtain detailed information for any message in any queue by selecting the appropriate queue, then double-clicking on the message item. Once selected, individual messages can be forwarded, bounced, delivered, or removed from the queue by simply selecting the appropriate button from the main screen.

ATTACHMENT HANDLING

One of the main differences between the Internet mail environment and either cc:Mail or Lotus Notes is in how attachments and non-text messages are handled. Within the cc:Mail and Lotus Notes environments, users with non-text attachments exchange messages in their native format. It is not necessary to perform any translation on the messages prior to submission to the message transport.

On the Internet, this is not the case. RFC-821 (Simple Mail Transfer Protocol) which defines SMTP, places certain restrictions on messages. These restrictions include certain line length limits as well as the restriction that all data be 7-bit ASCII characters. Because of these restrictions, it is not possible to transfer arbitrary objects using SMTP unless these objects are encoded prior to being submitted to SMTP.

The Internet standard for specifying how to encode non-textual and multipart messages is called MIME (Multipurpose Internet Mail Extensions) and is defined in RFC-1521 (Mechanisms for Specifying and Describing the Format of Internet Message Bodies). This Internet standard not only defines certain encoding and decoding methods, but also the format in which attachments are to be labeled and identified within the message.

When the MIME specification initially came out, it addressed many of the non-textual file attachment problems present within Internet email. One area that was not adequately addressed was the handling of Apple Macintosh file types (see Appendix B for additional information on the differences between these files and DOS or UNIX file types). Shortly after the MIME specification was produced, RFC-1740 (MIME Encapsulation of Macintosh files - MacMIME) was developed to address this shortcoming. By using both the MIME and MacMIME specifications, it is now possible to exchange information between Macintosh and non-Macintosh environments by email.

Prior to MIME, there were no official Internet standards in the areas of encoding standards and multipart message representation. There were some RFCs dealing with multipart message representation, but none of these ever made it to official standard status within the IETF. As a result, several vendors decided to implement one or more of the experimental RFCs covering this area, or to invent their own mechanism for specifying multipart messages.

Internet Exchange is capable of identifying and decoding incoming messages that conform to the MIME and MacMIME standards as well as the convention used in the Lotus gateway. For multipart messages that **Internet Exchange** creates, both MIME as well as non-MIME compliant messages can be generated. Messages that

conform to the MIME/MacMIME standards are produced by default, however it is also possible to define peer domains where different encoding methods can be used for different destination machines or domains. This capability allows **Internet Exchange** to communicate effectively with Internet sites running MIME compliant software as well as with older sites that are not MIME conformant.

INTERNAL DATABASES

Internet Exchange uses several internal Btrieve databases for improved performance. The databases include the following:

Name	**Database File**	**Backup Text File**
Alias Database	smtpadr.btr	smtp.adr
Domain Database	smtppod.btr	smtp.pod
Magic Database	magic.btr	[magic] in ima.ini/ieln.ini
DNS Cache Database	dns.btr	- *none* -
Message Database	mesg.btr	- *none* -
Peer Database	peer.btr	-*none* -
Mail Locking Database	lock.btr	-*none* -
SMTP Locking Database	smlock.btr	-*none* -
Domain Forwarding Database	domfwd.btr	-*none* -
Banned User Databse	banuser.btr	-*none* -
Banned IP Address Database	bannedip.btr	-*none* -
User Forwarding Address Database	userfwd.btr	-*none* -
Directory Database *(cc:Mail Version only)*	rulebadr.btr	- *none* -

Multiple Gateway Locking Database *(cc:Mail Version only)*	ccLock.btr	*-none -*
ASCII ⇔ Lotus Notes Forms *(Notes Version only)*	forms.btr	*-none-*
Fields Filter *(Notes Version)*	items.btr	*-none-*

Alias Database

The Alias Database stores specific cc:Mail or Lotus Notes names to Internet name mappings, as well as the corresponding send and receive permissions and the POP3 access permissions (for the cc:Mail version of **Internet Exchange**) for specific Lotus environment users. The *Workgroup* edition Alias Database has a maximum limit of 100 users. This database is used by *CCIN/NOTESIN* and *CCOUT/NOTESOUT* for cases where either the application of Rules Based Addressing (cc:Mail version) or the default send/receive permissions does not achieve the desired results. The Alias Database takes priority during address translation over the Directory Database (in the case of the cc:Mail version) as well as the Default Encoding method selected for the gateway.

Domain Database

The Domain Database provides the mapping between either downstream (or remote) cc:Mail post offices or Lotus Notes hierarchical certifiers and Internet domain names. This allows downstream post offices (cc:Mail) or Lotus Notes certifiers (Notes) to have unique Internet domain names associated with them.

Magic Database

The Magic Database is used to store the default encoding rules for various types of file attachments. This information is used to prepare MIME headers in outbound attachments, and for file naming in inbound MIME messages.

DNS Cache Database

The DNS Cache Database is used by *SMTPC* to store DNS query results. Each time **Internet Exchange** needs to perform a host name or MX record lookup, this will normally result in a DNS query over the network. When DNS Caching is enabled, the results from these queries are locally stored. The next time a query for the same host is made the **Internet Exchange** DNS resolver code will first check the local cache for the information, eliminating the time consuming network DNS lookup. This both lowers network congestion as well as significantly increasing gateway performance, especially for sites where the DNS server is not connected to a high speed network.

Message Database

The Message Database is used by **Internet Exchange** to store messages as they travel through the gateway. This database manages the inbound as well as outbound SMTP queues. Information stored in this database includes message status, envelope (list of recipients), message ID, and a pointer to the appropriate message, which is stored in a separate flat file (one file per message).

Peer Database

The Peer Database is used to store information about remote hosts or domains that require encoding rules or send / receive permissions different from the defaults specified for the gateway. It is useful when dealing with remote companies or organizations that are still running pre-MIME software and are unable to effectively deal with MIME attachments. It can also be used to restrict email access in one or both directions to / from specific remote sites, to set limits on inbound and outbound message sizes, and set the default attachment types that a remote host is able to handle.

An **Internet Exchange** *peer* is defined as a remote host or domain name. In the case of a domain, the scope of a particular *peer*

definition includes the peer domain name as well as all names and subdomains of that peer.

Peer definitions are processed from the most specific to the most general. A peer definition for the subdomain of a previously defined domain will take precedence over the more general definition.

As an example, let's say you want to configure the mail encoding for a company called XYZ Corp with a domain name of *xyz.org*. Most of the users in this company are still running pre-MIME software and prefer to receive non-MIME encoded messages. One group however, the engineering group, is running MIME compliant software. If the engineering group creates their own subdomain, say *engr.xyz.org*, then you can setup two peer definitions for XYZ Corp.

The first peer definition will define how you want to encode mail for everyone except the Engineering group. You do this by defining a peer *xyz.org*, and specifying non-MIME encoding for this domain. You then setup a second peer for *engr.xyz.org*, where you specify MIME compatible encodings. This has the effect of sending MIME messages to the Engineering Department within XYZ Corp while at the same time sending non-MIME messages to everyone else within the organization.

Hierarchical peer definitions can be added without limit, producing any combination desired. Peer definitions do not have to be associated with domains as in the above example either. The remote peer can be a machine or gateway name, providing configurability all the way down to the individual host level.

Mail Locking Database

The Mail Locking Database stores the mail message ID (the queue ID) to provide exclusive access between modules in **Internet Exchange** (e.g. *SMTPD* versus *CCIN/NOTESIN*, *SMTPC* versus *CCOUT/NOTESOUT*). It is located in the queue directory and is recreated when the gateway is started.

SMTP Locking Database

This database provides a locking mechanism for *SYSMAN* and *SMTPC*, in order to communicate to *SYSMAN* which messages are being processed by *SMTPC*; such a message is indicated by an arrow next to it on the queue screen. The SMTP Locking Database is located in the queue directory and is recreated when the gateway is started.

Domain Forwarding Database

The Domain Forwarding Database is where mappings between recipient and forwarding domains are stored. These mappings are used when the gateway forwards applicable messages from one Internet domain to another, and are also useful in migration from one gateway to another.

Banned User Database

The Banned Used Database stores the Internet addresses of message senders that are not permitted to communicate with or through **Internet Exchange**. The sender name can be checked in either the SMTP dialog session (the envelope) or in the message header itself, which is created by the remote user agent.

Banned Peer IP Address Database

The Banned Peer IP Address Database stores the IP addresses or a range of IP addresses of banned peers for the purpose of disallowing SMTP sessions. Inbound messages from these IP addresses will be rejected by *SMTPD*. If the peer IP address is banned, *SMTPD* will reject the SMTP connection during the HELO session by responding with a permanent SMTP error (553).

User Forwarding Address Database

The Forwarding Address Database stores mappings between forwarding addresses and their particular Internet aliases. *CCIN* and *NOTESIN* use these mappings to find a list of forwarding

addresses for the envelope recipients (an envelope consists of delivery information meaningful to the MTA and is not strictly identical to message headers), and reroutes the messages to the SMTP Out queue for delivery. It is possible for the gateway to function as a generic mailing list generator by configuring these mappings accordingly.

Directory Database *(cc:Mail Version)*

The **Internet Exchange for cc:Mail** *Rules Compiler* produces the Directory Database by compiling the Rules Based Addressing rules. When Rules Based Addressing is selected by the administrator, the selected rules will be applied to the contents of the cc:Mail directory. This results in the creation of the **Internet Exchange** Directory Database, a shadow version of the cc:Mail Directory available from the local Post Office. This database is then consulted by *CCIN* and *CCOUT* when performing routine address translation tasks, eliminating most references to the cc:Mail Directory. This produces higher throughput for the gateway since fewer relatively slow cc:Mail Directory lookups need to be performed.

Multiple Gateway Locking Database *(cc:Mail Version)*

The Multiple Gateway Locking Database provides a locking mechanism for *CCOUT* when the option "Multiple Gateway access to same PO" (see Chapter 7 in Part 3 for more information) is enabled. If this option is not enabled the database is not used. The Multiple Gateway Locking Database is located in the Post Office directory for cc:Mail, which should be accessible by the multiple gateways. The database is recreated when the gateway is started.

ASCII ⇔ Lotus Notes Forms Database *(Notes Version)*

A Notes document is composed of two parts: the FORM Note, which contains the definition of each field in the document that is being composed, and the DATA Note, which is the information

entered for each field. This database stores mappings between the Notes Forms and their equivalent ASCII Forms.

Fields Filter Database *(Notes Version)*

The fields of a Notes document can be static text, images, binary attachments and so on, however they are all stored as binary information in the Lotus Notes environment. If an ASCII Form is unavailable to act as template, a set of Fields can be used to achieve the same goal. The Fields Filter Database contains a list of pre-defined items that are "filtered out" (not exported) when using the Generic mail export function; Fields other than those specified in the filter are exported to the mail body.

ADDRESS TRANSLATION

In order for users to exchange messages between either their cc:Mail or Lotus Notes environments and the Internet it is necessary that they be able to uniquely identify both themselves as well as their intended recipients on both sides of the gateway. Each user on either side of the gateway has an electronic mail address associated with each mailbox. Unfortunately, the formats of these mail addresses are not the same for cc:Mail or Lotus Notes users and Internet mail addresses. Due to the differences between the two addressing formats, it is the job of the gateway to provide address mapping capabilities.

CC:MAIL ADDRESS TRANSLATION

Internet Exchange for cc:Mail offers several different options when it comes to translating between Internet and cc:Mail email addresses. In cc:Mail many if not most users have spaces between their first and last names. This aids in readability and allows users to use their real names, without any artificial limitations on length or case. On the Internet, user addresses are more restricted. Spaces are not allowed, and addresses are case sensitive.

Internet Exchange for cc:Mail has four mechanisms to map between user names in cc:Mail, and the corresponding Internet addresses by which these users will be known to other Internet users:

- Default Mappings
- User Aliases
- Post Office Subdomains
- Rules Based Addressing

The order in which the addressing methods are applied is: user aliasing, rules based addressing, domain mapping, and finally default mapping.

If an outgoing address already contains a separator character before the default mapping is applied, this separator will be doubled. When a reply to such an address is received, the extra separator will be discarded. e.g. if the separator is underscore (_), then the following user:

John_Doe at Remote Sales_PO

will be mapped to:

John__Doe_at_Remote_Sales__PO

Default Mappings

The default method of creating an Internet address from a cc:Mail username is to convert all spaces to underscores. e.g. the user:

John Doe at Main PO

becomes:

John_Doe@iegate.jade.net

Users of cc:Mail on remote Post Offices (the Post Office named *Sales* in the following example) will appear similar to:

Jane_Doe_at_Sales@iegate.jade.net

The remote Post Office name is included so that cc:Mail can reroute replies to this message. Although these address forms are perfectly adequate, often users wish to be known by different Internet addresses. The administrator can achieve this by creating a user alias.

User Aliases

By entering a mapping in the Configure Users screen, an alias can be created for a cc:Mail user. This is a simple textual substitution that happens for both outgoing and incoming messages. For example, an alias for John Doe can be created, mapping him to *johnd*. Any messages from this user will appear to come from johnd@iegate.jade.net. Similarly, replies to such messages will be converted back to the original cc:Mail user name.

These user aliases are most easily created by the Configure Users screen. An alternative method is to edit the file *SMTP.ADR*, which contains these mappings. The above example appears in this file as follows:

John Doe<=>johnd

An equivalent form is

John Doe<=>johnd@iegate.jade.net

Although effectively the same, the first format is preferable, as it will not need changing if the local hostname and/or domain is ever changed. When there is no hostname and domain in an alias, the local values are appended automatically.

Using the manual method can be useful if a list of aliases can be created automatically by a program. Then, the resulting text output can easily be converted into the format needed for *SMTP.ADR*.

Post Office Subdomains

If there are a number of cc:Mail Post Offices in use, then the default method of creating an Internet address produces ungainly results. e.g. John Doe at Sales becomes:

John_Doe_at_Sales@iegate. jade.net

Another mechanism is available that involves mapping remote cc:Mail Post Offices to Internet subdomains. This is set up by the *Configure Domains* screen. e.g. by mapping Sales above to sales.iegate.firm.com, the above address appears as:

John_Doe@sales.iegate. jade.net

These domain mappings are most easily created through the Configure Domains screen. An alternative method is to edit the file *SMTP.POD*, which contains these mappings. The above example appears in this file as follows:

Sales = sales.iegate.jade.net

Using the manual method can be useful if a list of mappings can be created automatically by a program. Then, the resulting text output can easily be converted into the format needed for *SMTP.POD*.

Addressing Options

There are also several options that affect how addresses are formed. They are accessed through the Configure Options screen as follows:

Addressing Separator

This allows the administrator to choose between the underscore ('_') and the dot (.) as the separator used in default mapping. This option should be set initially and not changed, otherwise incoming messages using default addressing will be bounced.

Include cc:Mail Names In Addresses

Setting this option appends the cc:Mail user name in parentheses to any Internet address generated.

Use Hostname In Addresses

This option determines the format of the local hostname used for outgoing Internet addresses. e.g. if set, addresses will look like:

User@iegate.jade.net

and if not set:

User@jade.net

Organizations wishing to hide the internal structure of their network from the outside world often prefer the second format.

Use Remote PO Names

When set, the Post Office name of a user from a remote cc:Mail Post Office is included in the default address mappings. e.g.:

John_Doe_at_Sales@iegate.jade.net

If reset, the above address appears as follows:

John_Doe@iegate.jade.net

This format is much cleaner and is an alternative to using Post Office subdomains. However, if this format is used, the main cc:Mail Post Office must contain entries for all cc:Mail users from other Post Offices. Otherwise, incoming messages will not be able to be routed internally to the correct Post Office. An easy way to ensure this occurs is by running Lotus Automatic Directory Exchange (ADE).

Summary of Default Addressing Formats

The following table lists the options to set depending upon which form of default addressing is preferred. The user here is John Doe at Sales, a remote Post Office:

NAMES	*ADDRESS SEPARATOR*	*USE HOST NAME*	*USE REMOTE PO*
John_Doe_at_Sales@iegate.jade.net	underscore	yes	yes
John_Doe_at_Sales@jade.net	underscore	no	yes
John_Doe@iegate.jade.net	underscore	yes	no
John_Doe@jade.net	underscore	no	no
John.Doe.at.Sales@iegate.jade.net	dot	yes	yes
John.Doe.at.Sales@jade.net	dot	no	yes
John.Doe@iegate.jade.net	dot	yes	no
John.Doe@jade.net	dot	no	no

NOTE: if not using remote PO names, it is best to use ADE.

Rules Based Addressing

For large sites that prefer to map cc:Mail user names to Internet addresses that do not match the rules used by default address translation, it can be inconvenient and time consuming to maintain large alias translation tables. To address this problem, **Internet Exchange for cc:Mail** also makes use of administrator specified address translation rules.

The **Internet Exchange for cc:Mail** *Rules Editor* provides the gateway administrator with the ability to specify an ordered set of rules that the gateway can use when trying to map Internet email addresses to their cc:Mail user name counterparts. The gateway applies each rule in order, allowing a site to effectively support

several different naming conventions without forcing each name mapping to be manually entered into the system.

As an example of how rules based address translation can be used, let's once again look at Jade Networks. The company policy for Jade Networks is that users' Internet email addresses be of a form consisting of first initial followed by the first 7 characters of the last or family name. In addition, some people in the company also want their Internet email address using simply their family name, regardless of length.

Using the *Rules Editor*, which is part of the *Rules Compiler*, the gateway administrator defines two rules. The first specifies the primary company convention of first initial followed by no more than the first 7 characters of the family name. A second rule is then defined to map to the family name, regardless of length. After the rules are entered, the *Rules Compiler* reads the post office directory, applying the rules to produce an **Internet Exchange** shadow directory mapping database.

Once the shadow directory mapping database is created, it will be consulted prior to any attempt to perform default address translation. There are several benefits for this type of configuration:

- Since the rules are defined by the administrator rather than the software, many more combinations are available, decreasing the need for large alias databases.

- Users can accept email addressed to several different Internet email addresses, as long as they conform to the conventions defined by the organization.

- The use of the shadow directory mapping database at runtime significantly reduces the need for the gateway to access the cc:Mail directory. This results in improved performance of the gateway and less overhead for the post office file system.

Additional information on rules based addressing and its configuration can be found in *Chapter 10 - Rules Based Addressing*.

LOTUS NOTES ADDRESS TRANSLATION

Internet Exchange for Lotus Notes offers several different options when it comes to translating between Internet and Lotus Notes email addresses. In Lotus Notes, many if not most users have spaces between their first and last names. This aids in readability and allows users to use their real names, without any artificial limitations on length or case. On the Internet, user addresses are more restricted. Spaces are not allowed, and addresses are case sensitive.

Internet Exchange for Lotus Notes has three mechanisms to map between user names in Lotus Notes, and the corresponding Internet addresses by which these users will be known to other Internet users:

- Default Mappings
- User Aliases
- Certifier Subdomains

The order in which the addressing methods are applied is: user aliasing, domain mapping, and finally default mapping.

Default Mappings

The default method of creating an Internet address from a Lotus Notes username is to replace any spaces with either an underscore or a dot to construct an RFC-822 address. For example:

John Doe/Engineering Department/Jade

will be mapped to:

John_Doe/Engineering_Department/Jade

With the option IncludeCertifier = <NO>/YES, the outgoing address

John Doe/Engineering Department/Jade

may look something like:

John_Doe

Default mapping with a Dot

John Doe/Engineering Department/Jade

maps to:

John.Doe/Engineering.Department/Jade

Without a certifier,

John Doe/Engineering Department/Jade

becomes:

John.Doe

User Aliases

By entering a mapping in the Configure Users screen in *SYSMAN*, an alias can be created for a Lotus Notes user. This is a simple textual substitution that happens for both outgoing and incoming messages. For example, an alias for John Doe can be created, mapping him to *johnd*. Any messages from this user will appear to come from johnd/Jade. Similarly, replies to such messages will be converted back to the original Lotus Notes user name.

These user aliases are most easily created by the Configure Users screen. An alternative method is to edit the file *SMTP.ADR*, which contains these mappings. The above example appears in this file as follows:

John Doe<=>johnd

Equivalent forms are

John Doe < = > jdoe

and

John Doe<=>johnd/Jade

Using the manual method can be useful if a list of aliases can be created automatically by a program. Then, the resulting text output can easily be converted into the format needed for *SMTP.ADR*.

Domain mapping

Internet Exchange for Lotus Notes uses domain mapping to map hierarchical certifiers to specific Internet subdomains, e.g.:

/Sales/Jade

becomes:

sales.jade.net

and

/Engr/Jade

becomes:

engr.jade.net

Once the domain mapping is found for a particular certifier, the option Include Certifier for default mapping will be ignored in order to avoid redundant information contained in both the localpart and domainpart in the RFC-822 address.

Preserving Lotus Notes Domains in an RFC-822 Address

Default mapping, User mapping and Domain mapping provide no means to indicate Lotus Notes Domain information. In order to do

so, **Internet Exchange** uses the option, *Lotus NotesDomainInclusion = NONE / LEFT / RIGHT* to preserve such information, where:

NONE means do not add Lotus Notes domain information.

LEFT means put Lotus Notes Domain information on the left hand side of the @ symbol of the RFC-822 address (localpart), and use a *%* symbol as a delimiter to avoid any conflict with '_' and '.' used in default mapping.

RIGHT means put domain information on the right hand side of the @ symbol in the RFC-822 address and use a dot ('.') as the delimiter.

In general, if a user comes from the same domain as the gateway, *DomainInclusion* will be ignored automatically. For users from other domains, assuming the domain associated with the gateway is 'jade', addresses may look something like the following.

(*LEFT, IncludeCertifier* enabled):

John Doe / Sales @ Sales <=> John_Doe / Sales%Sales@jade.net

(*LEFT, IncludeCertifier* disabled):

John Doe / Sales @ Sales <=> Joe_Wong%Sales@jade.net

(*NONE, IncludeCertifier* disabled):

John Doe / Sales @ Sales <=> John_Doe@jade.net

(*RIGHT, IncludeCertifier* disabled) :

John Doe / Sales @ Sales <=> John_Doe@Sales.jade.net

When a Lotus Notes address comes with explicit domain routing information, outgoing addresses will look like this:

John Doe / Sales @ Sales @ HongKong

<=>

John_Doe%Sales%HongKong@.jade.net (*LEFT*)

John Doe / Sales @ Sales @ HongKong

<=>

John_Doe@Sales.HongKong.jade.net (*RIGHT*)

NOTE: Placing domain information on the *RIGHT* hand side is generally not recommended.

Addressing Options

There are also several options that affect how addresses are formed. They are accessed through the Configure Options screen as follows:

Addressing Separator

This allows the administrator to choose between the underscore (_) and the dot (.) as the separator used in default mapping. This option should be set initially and not changed, otherwise incoming messages using default addressing will be bounced.

Include Lotus Notes Names In Addresses

Setting this option appends the Lotus Notes user name in parentheses to any Internet address generated.

Use Hostname In Addresses

This option determines the format of the local hostname used for outgoing Internet addresses. e.g. if set, addresses will look like:

User@iegate.jade.net

and if not set:

User@jade.net

Organisations that wish to hide the internal structure of their network from the outside world often prefer the second format.

PART 2 INSTALLATION

CHAPTER 2
PLANNING YOUR INTERNET EXCHANGE FOR CC:MAIL INSTALLATION

INSTALLATION REQUIREMENTS

If you are installing Internet Exchange for Notes, please skip ahead to Chapter 4. Before you can install **Internet Exchange for cc:Mail**, all the hardware and software components listed in the *Requirements* section of the *Preface* of this manual need to be properly installed and running.

VIM LIBRARY INSTALLATION

Internet Exchange requires Lotus cc:Mail VIM version 6.0 or later to be present on the system in order to operate properly. At the time of writing, the cc:Mail VIM libraries have reached version 6.03. If you are using a recent version of cc:Mail for Windows operating systems, you probably have the most recent versions of the VIM libraries. To verify that you are running version 6.03, check the following English VIM libraries against the versions you have installed. This can be done by running the *DIR* command from the directory that contains the 32-bit VIM *.dll* set. The name of the directory should be specified in the system PATH environment variable.

```
cdfw800.dll       66048     01-23-97
cdmw800.dll       46592     01-23-97
cfw801.dll        60416     06-12-97
chrset32.dll      17408     10-27-95
ciw801.dll        89600     06-12-97
cmw800.dll        22016     01-23-97
medb632.dll      350720     09-12-96
mew801.dll       751104     06-12-97
vim32.dll        153088     09-19-97
vmefnw32.dll      64000     09-19-97
ccregmod.exe      35840     02-19-97
```

If the files match the ones above or are more recent, then you are running with at least version 6.03 of the VIM libraries and need do nothing more. If they are not as recent as the above files, you can contact cc:Mail technical support to request the proper libraries. Alternatively, you can download them from the Lotus BBS, or you can obtain them by anonymous FTP over the Internet. The cc:Mail BBS can be reached at:

BBS: (415) 691-0401 (Call with any asynchronous package; parameters: 8-N-1)

The files may be obtained by anonymous FTP at the current URL:

ftp://ftp.ccmail.com/pub/comm/ccmail/dev_tools/vdlw32.zip.

INTERNET EXCHANGE FOR CC:MAIL INSTALLATION

Before you run the **Internet Exchange** *INSTALL* program, it is necessary to assemble all the information needed for the installation. This includes information about where to install **Internet Exchange**, and details about the cc:Mail gateway post office as well as your TCP / IP configuration.

To assist with the installation of the gateway software, please review and fill out the installation worksheet provided at the end of this chapter prior to the start of the installation. Each item in the worksheet will be discussed in the following sections.

Gateway Parameters

The Gateway Parameters sections of the installation worksheet identify parameters that are associated with either the installation and/or the overall operation of the gateway.

Program Directory

The default location in which **Internet Exchange** is installed is c:\ieccmail. This is where the programs and libraries reside. The directory can be located anywhere, however it is strongly recommended that it be placed on a local hard drive for performance and reliability reasons.

Queue Directory

The default location where **Internet Exchange** stores temporary files is c:\ieccmail\queue. This is where the messages and log files reside. This directory can be placed anywhere, however it is strongly recommended that it be placed on a local hard drive for performance and reliability reasons. The program and queue directories do not have to be on the same disk. This allows a more flexible installation.

Temporary Directory

The directory in which **Internet Exchange** will store messages. It is usually configured to be a subdirectory of the queue directory, but it can be set to a different directory and/or drive depending upon local disk availability.

Local Character Set

The ISO character set to be used. Most Anglo-Saxon countries can select US-ASCII, while others will prefer to choose a different character set. All outgoing email will be tagged as using the selected character set.

Local Time Zone

The time zone in which the local machine resides. Whether this time zone uses daylight saving or not should also be noted. There are many locations configured in the system, including the USA, much of Europe, and Asia. If the local time zone is not listed, it will have to be entered manually into IMA.INI (IELN.INI for Notes Versino) with an editor as follows:

[Gateway]
Timezone=*tzn*[[+ | -]]*hh*[[:*mm*[[:*ss*]]]][[*dzn*]]

The *tzn* must be a three-letter time-zone name, such as PST, followed by an optionally signed number, *hh*, giving the difference in hours between UCT and local time. To specify the exact local time, the hours can be followed by minutes, *:mm*; seconds, *:ss*; and a three-letter daylight-saving-time zone, *dzn*, such as PDT. Separate hours, minutes, and seconds with colons (:). If daylight saving time is never in effect, as is the case in certain states and localities, set *Timezone* without a value, for *dzn*. If the *Timezone* value is not currently set, the default is PST8PDT, which corresponds to the Pacific time zone of the USA.

If the time zone "Use system TZ variable" is selected, the timezone information will be obtained from the user defined TZ environment variable. Under Windows 95, this can be set in the *autoexec.bat* system startup file. Under Windows NT it is usually set in the system registry. In either case, the machine must be rebooted in order to make the change effective.

cc:Mail Parameters

The cc:Mail section of the installation worksheet identifies parameters associated with the gateway post office. This is the post office that is queuing messages on behalf of **Internet Exchange**.

Local Post Office Name

The name of the post office that **Internet Exchange** will log into to retrieve messages.

Internet Post Office Name

The name which **Internet Exchange** uses to log into the cc:Mail Post Office. This name must exist in the cc:Mail directory, and must be defined as a Post Office. Although any unique name may be used here, it is recommended that *Internet* be used for clarity.

Post Office Path

The path name for the directory where the local post office resides.

Post Office Password

The password that **Internet Exchange** should use when logging into the local post office.

Post Office Postmaster

Internet mail standards require that each site have a mail account that receives messages addressed to "postmaster." The postmaster typically receives notices about mail problems, network problems, and inquiries about users and mailboxes. It should be set to the cc:Mail address of the person responsible for the Internet mail gateway.

TCP/IP Parameters

The TCP/IP parameters section of the installation worksheet identifies parameters associated with the local TCP/IP network.

Host Name

Each host on the Internet must have a unique identifier so that email bound for that site has a single unambiguous destination. This identifier is known as the Fully Qualified Domain Name (FQDN).

The host name parameter is the name component of the gateway machine FQDN. For example, if the FQDN of the gateway is *iegate.jade.net* then the host name would simply be *iegate.*

Domain Name

The domain component of the gateway machine FQDN. For example, if the FQDN of the gateway is *iegate.jade.net* then the domain component would be *jade.net*.

Host File Location

This is the full path name of the TCP/IP host file. Even if the Domain Name System (DNS) is used for host name to address translation, it is recommended that a host file be present that contains addresses for the following hosts: loopback, gateway machine, and your mail relay host.

Mail Relay Host

The mail relay host is the name of the machine that is used to send mail that cannot be resolved by either host table lookup or by DNS queries (or if you have configured **Internet Exchange** to use a default mail relay host only). It is required that this host have an entry in the local host table in the event that the DNS cannot be contacted.

Name Server Addresses

This is the list of name servers to contact for performing MX record and Address record lookups using the Domain Name System (DNS).

Internet Exchange For cc:Mail

Installation Worksheet

Gateway Parameters

Program Directory _____

Queue Directory _____

Temporary Directory _____

Local Character Set _____

Local Time Zone _____

cc:Mail

Local Post Office Name _____

Internet Post Office Name _____

Post Office Path _____

Post Office Password _____

Post Office Postmaster _____

TCP/IP Configuration

Host Name _____

Domain Name _____

Host File Location _____

Mail Relay Host _____

Name Server Addresses _____

CHAPTER 3
INTERNET EXCHANGE FOR CC:MAIL INSTALLATION

PREPARING THE CC:MAIL POST OFFICE

Internet Exchange requires that a gateway post office be established within cc:Mail. The following instructions provide a step-by-step approach to the creation of this gateway post office.

1) Start up cc:Mail's **admin** utility. First enter the DOS environment, change your current working directory to the directory containing the above program, e.g., c:\ccadmin, and then type **admin** followed by **Enter**.

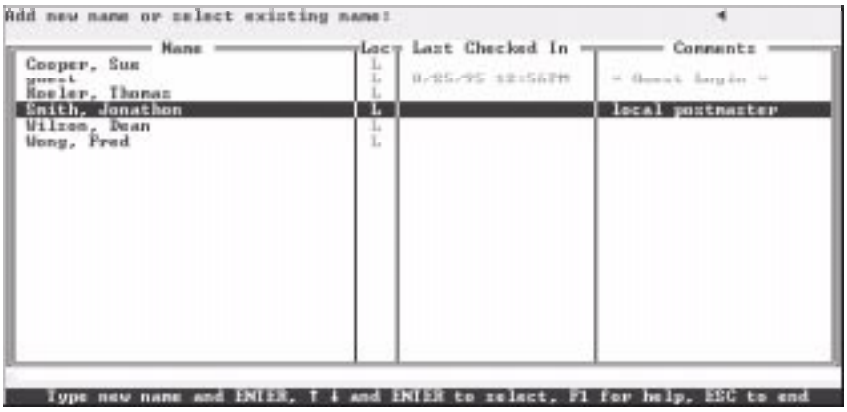
2) Enter the local post office directory, e.g. c:\ccdata, and press **Enter**.

3) Enter the name of the local post office - in our example, *Jade Networks*, and press **Enter**.

4) Enter the password for the post office and press **Enter**.

The following screen will be presented:

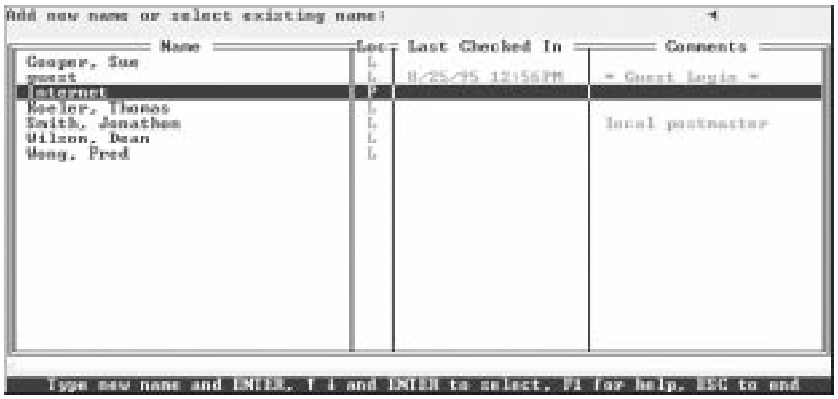
5) Choose “manage Mail directory” (as above) by selecting it and pressing **Enter**.



6) Type in the name of the new gateway post office, e.g. Internet, and press **Enter**.

7) When prompted for the location status of the new post office enter a "**P**" followed by **Enter**.

8) You can now enter an optional comment (e.g., "Internet Exchange post office"), followed by **Enter**. The new entry now appears in the menu:



9) After verifying that the above information is correct press **Enter** followed by **Esc** to return to the main menu, then enter an **X** followed by **Enter** to save and exit **admin**.

INSTALLING INTERNET EXCHANGE FOR CC:MAIL

Once the Installation Worksheet is complete, you are ready to perform the actual installation.

The CD Installer

The **Internet Exchange** Compact Disc Installer is a front-end program designed to facilitate and automate gateway installation. In addition, it also provides the option to install Adobe Acrobat Reader in order to view various Portable Document Format (PDF)

files included on the CD such as the administrator's guide, product comparison documents, benchmarking reports, **Internet Exchange** Whitepapers and so on.

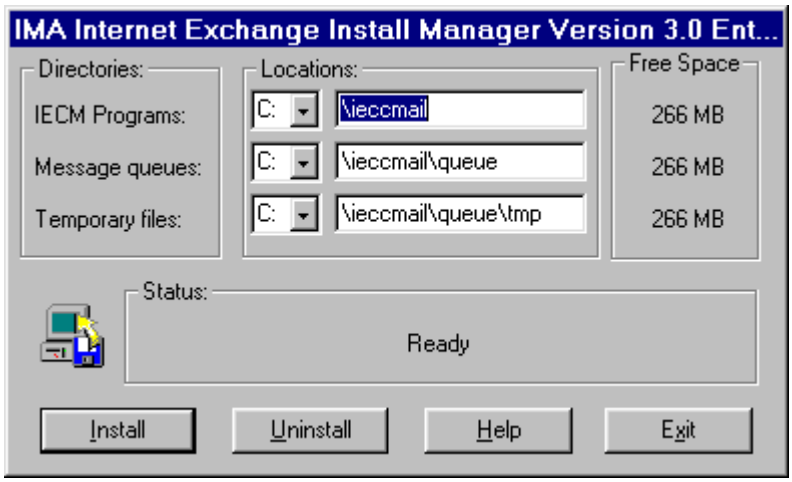
To install **Internet Exchange** perform the following tasks:

1. Make sure your computer and monitor are turned on and the Windows environment is running.
2. Insert the **Internet Exchange** CD into an available CD-ROM drive.
3. The *install.exe* file is located on the CD under one of the following directories depending upon which product you are installing:

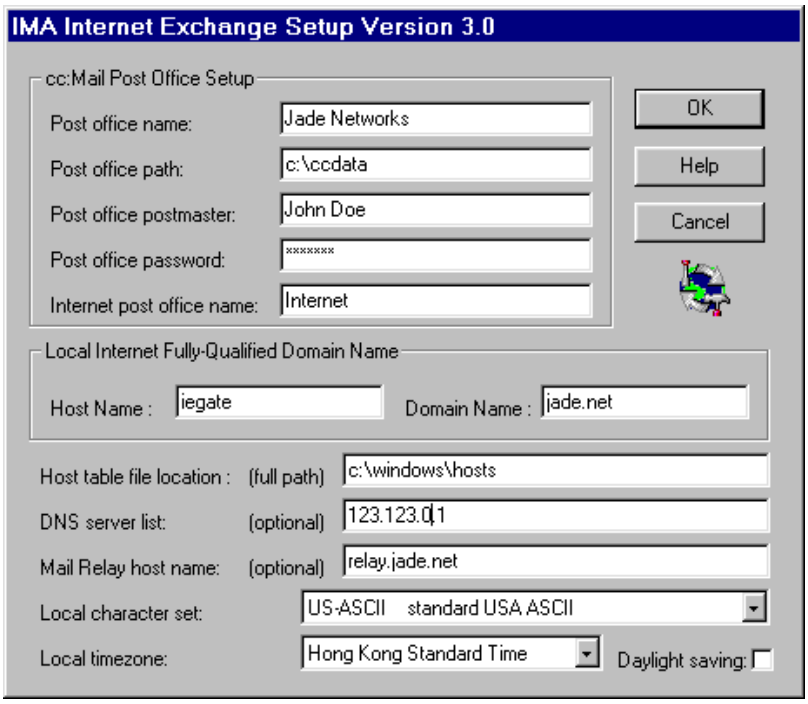
\IECM-ENTERPRISE	**Internet Exchange for cc:Mail**, *Enterprise Edition*
\IECM-WORKGROUP	**Internet Exchange for cc:Mail**, *Workgroup Edition*
\IELN-ENTERPRISE	**Internet Exchange for Lotus Notes**, *Enterprise Edition*
\IELN-WORKGROUP	**Internet Exchange for Lotus Notes**, *Workgroup Edition*

   In order to run the installation without the assistance of the CD Installer, locate the appropriate installation program and run it.
4. Choose the option to install **Internet Exchange** on your system.

Install will then present the following screen:



Press the default *Install* button to install **Internet Exchange**. A progress dialog showing how the installation process is going will be displayed. Once all the files have been copied over and the **Internet Exchange** Program Group has been created, the *Setup* program will be automatically executed and will display the following screen:

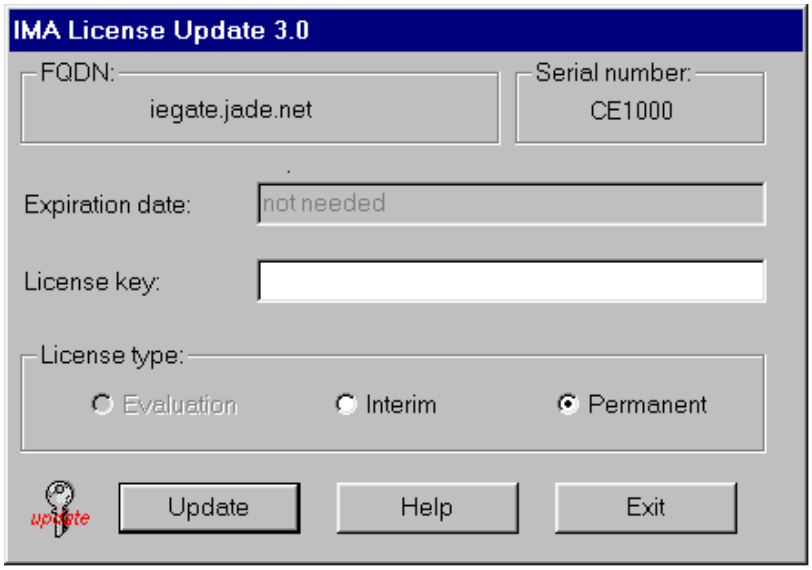


This screen shows the basic parameters that are necessary to start up **Internet Exchange**. The above example is for the machine *iegate.jade.net*, connecting to the cc:Mail post office *Jade Networks* located in c:\ccdata. The Internet cc:Mail Post Office name is *Internet.* Please refer to the Installation Worksheet completed earlier, and ensure that all the entries above are properly set for your site. When all fields are correct, click on the *OK* button for the selections to take effect.

If **Internet Exchange** is being installed on top of an existing installation, it may be necessary to perform certain conversions from the previous version. If necessary, the following utilities will be automatically started during the installation process: *MIME Magic Mapping Utility, Message Conversion Utility, Domain Conversion Utility,* and the *Address Conversion Utility*. Detailed information regarding each of these utilities can be found in Chapter 11.

Once *Setup* is complete, it will offer to update the gateway license. If desired, the *License Update* program will be automatically started. This program can also be run at any time by selecting the *License Update* program from the *Internet Exchange for cc:Mail* Program Group.

After License Update is started, the following screen will be displayed:



There are two read only fields that appear when the *License Update* program starts - the FQDN and Serial Number. The FQDN, or fully qualified domain name, is the official name for the gateway. The Serial Number field displays the unique serial number built into the current copy of *Internet Exchange.* These are the two fields that need to be provided to your supplier or IMA to generate a license key as described below.

There are three types of software licenses that can be generated for *Internet Exchange.* They are:

Evaluation License

If this copy of *Internet Exchange* was obtained from a public access site (anonymous FTP, the Web or a commercial service), it is not possible to permanently enable the gateway. For these versions of the gateway, the evaluation license radio button will be the only option.

To obtain an evaluation license, it is necessary to contact your supplier or IMA, either by phone, fax, or email. Email requests should be sent to:

eval-auth@ima.com

When requesting an evaluation license, please provide a completed registration form, which can be found in the Internet Exchange for cc:Mail program group.

After obtaining the evaluation license, it is necessary to enter both the expiration date of the license as well as the license key. The expiration date is entered in the form mm/dd/yy. The license key should be entered exactly as obtained from your supplier or IMA. After entering the appropriate expiration date and license key, press the *Update* button to store the registration information.

Interim License

Interim licenses are similar to Evaluation licenses, with the exception that an Interim license can be updated to a Permanent license at a later date. To obtain and apply for an Interim license, follow the same procedure outlined for an Evaluation license. Instead of sending email to *eval-auth*, please contact either your supplier or IMA, or send email containing full registration information to:

auth@ima.com

Permanent License

Unlike Evaluation and Interim licenses, Permanent licenses do not have expiration dates. These licenses are based upon the **Internet Exchange** serial number and the Fully Qualified Domain Name

(FQDN) of the gateway machine. To obtain a Permanent license key, please contact either your supplier or IMA, or send email containing full registration information to:

auth@ima.com

Since there is no termination date to a permanent license, the only information you need to enter for a Permanent license is the license key. Enter the key and press the *Update* button to store the registration information.

After storing the license information with License Update, the installation and licensing of **Internet Exchange** is complete and the gateway is ready for use. You may wish to perform further configuration of the users, subdomains or the MIME Mapping Database.

INSTALLING THE REMOTE CONTROL

The Remote Control uses HTTP, HTML and CGI in order to allow administrators to monitor, configure and operate **Internet Exchange**. A web server has to be installed on the machine running the gateway for the Remote Control to operate (for best results the web server should be dedicated solely to the Remote Control). **WebSite Professional** from O'Reilly Software (*http://website.ora.com*) was successfully tested, and it is recommended by our technical staff. Accepted web browsers are Netscape Navigator 3.01 or higher and Internet Explorer 3.02 or higher. A screen resolution setting of at least 800x600 pixels is required.

The Setup Program

The setup program *INSTRC.EXE* will automatically install Remote Control modules on to the gateway system with only a minimum of information required. The HTML files and CGI programs required for remote access are automatically copied to their corresponding physical directories on the gateway system. If you are using

O'Reilly's WebSite, the Setup program will also automatically add the URL and CGI mappings to the web server's configuration.

Shut down the web server prior to running the Setup program.

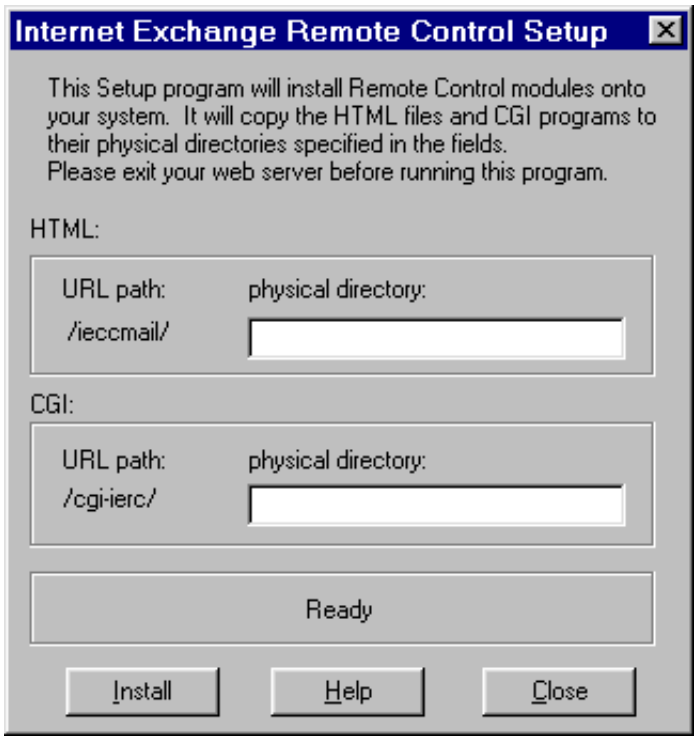
The URL path for the HTML files is:

/ieccmail/

And the URL path for the CGI programs is:

/cgi-ierc/

It is strongly recommended that security protection be applied to these URLs.



HTML Physical Directory

Specifies the physical directory in which to store the HTML files required by the Remote Control. If WebSite is used the default directory will be *c:\website\ieccmail*, where *c:\website* is the root directory of WebSite.

CGI Physical Directory

Specifies the physical directory in which to store the CGI programs required by the remote Control. If WebSite is used the default directory will be *c:\website\cgi-erc*, where *c:\website* is the root directory of WebSite.

Install

Starts the setup process and installs the Remote Control.

Help

Displays the help file on Remote Control Setup.

Close

Exits the setup program.

After the Setup process is complete, start the web server. To remotely access the gateway from any PC, establish an Internet connection and enter this path into your web browser's location field:

http://web.server.name/ieccmail/index.htm

where web.server.name is the name of your web server. A window allowing remote operation, configuration and monitoring of the gateway will load.

INSTALLING INTERNET EXCHANGE AS A WINDOWS NT SERVICE

In order to install **Internet Exchange** as an NT Service, simply run the Service Installer **INSTSRV.EXE**. This program is designed both to install **Internet Exchange Service** on an NT system and to remove it should the need arise. You are required to login to the Windows NT account with Administrator privileges before running the Service Installer.

Install

Installs **Internet Exchange** as a Windows NT Service.

Uninstall

Removes **Internet Exchange** as a Service from the system.

Help

Displays information and notes about installation.

Close

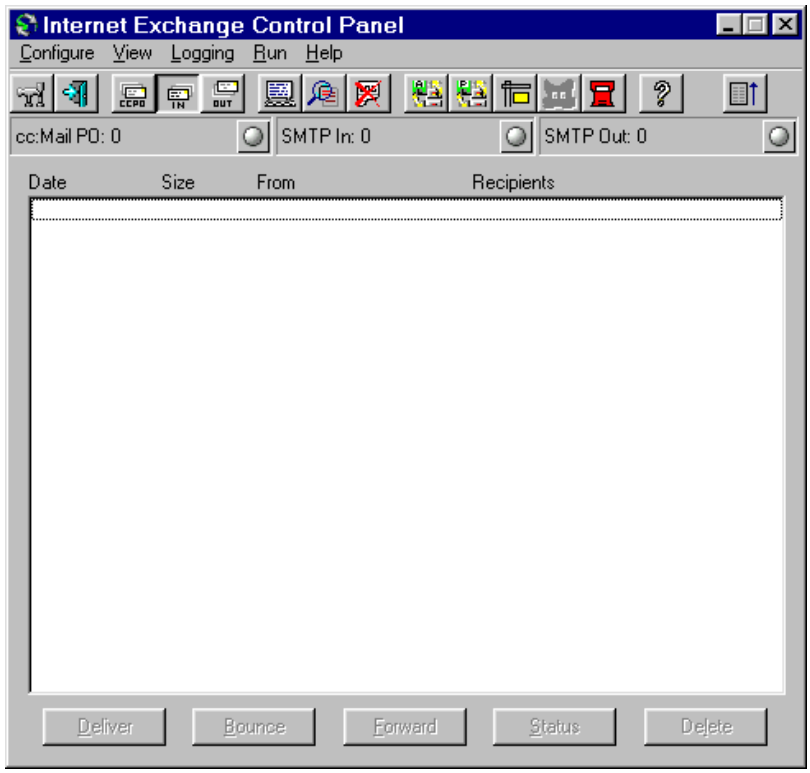
Exits the Service Installer program.

When the installation is complete, you may configure the manner in which **Internet Exchange** as an NT Service is started up (manual or automatic) by clicking on the "Service" icon in the Windows Control Panel. In order to start up the Service automatically, the path of the VIM32 library must be added to the system path; it is possible to do this in the "System" menu of the Control Panel.

In order to configure the service to be started up automatically along with the NT machine, all the network paths (such as PO path) used by the gateway have to be specified in UNC (Universal Naming Convention) instead of the regular network drive letters.

STARTING INTERNET EXCHANGE FOR CC:MAIL

During the **Internet Exchange** installation process, the program group ***Internet Exchange*** is created and the icons for the following programs are set up: *SYSMAN*, *CCIN*, *CCOUT*, *SMTPD*, *SMTPC* and *POP3D*. To start **Internet Exchange**, double click on the System Manager icon with the title *IMA Internet Exchange.* The system manager will then start, along with the SMTP Daemon, and the following window will be displayed:



The rotating globe that appears on the Windows Taskbar indicates normal operation of the gateway, although its rate of rotation may vary. When the System Manager is started, the SMTP daemon icon is placed on the Taskbar; the existence of this icon indicates that the

SMTP Daemon is running and listening for incoming SMTP requests:

At this point, **Internet Exchange** is up and running, ready to exchange messages between cc:Mail and the Internet.

If the SMTP daemon should fail for any reason, the icon will disappear, and the *Restart SMTP* button on the System Manager will become activated.

CHAPTER 4
CONFIGURING LOTUS NOTES

INSTALLATION REQUIREMENTS

Before you can install **Internet Exchange for Notes**, all the hardware and software components listed in the Preface need to be properly installed and running. You should also be familiar with configuration processes for the Lotus Notes Server. In addition, it is necessary to assemble all the information needed for the installation.

This chapter deals with setting up the Lotus Notes Server so that it can communicate properly with **Internet Exchange.** You must follow the procedures described in this chapter before attempting to install **Internet Exchange.**

If you are not familiar with the Notes Server setup process, you should refer to the Lotus Notes Server Administrator's Manual.

Special note: if using Domino 4.6, the following preliminary steps have to be taken:

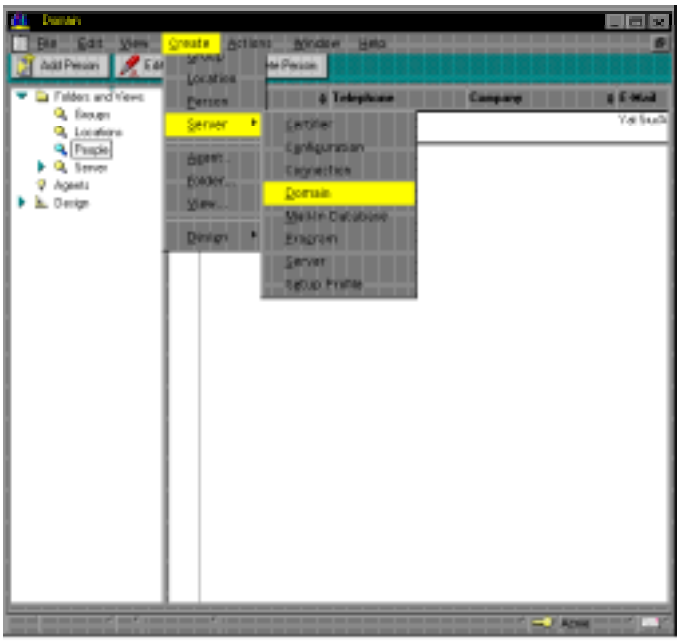
- remove the entry "SMTPMTA" in the *ServerTasks* option from the *NOTES.INI* file. This prevents default startup of the Lotus SMTP MTA.

- Delete the file *SMTP.BOX* created by the Lotus SMTP MTA and re-create one using the standard "mail router mailbox" template, as **Internet Exchange** does not understand the format of the one created by the Lotus SMTP MTA.

Installing SMTP settings for Internet Exchange on the Notes Server

Creating your Domain

You must first install a new SMTP Domain on the Notes Server. This can be done in the Public Address Book in Lotus Notes by selecting the Create Server Option where you may then select a Domain.

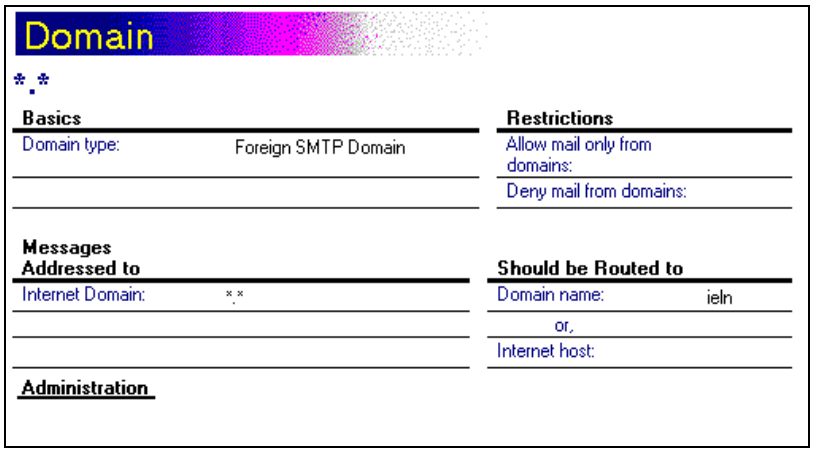


Lotus Notes Image

In the Domain Menu the Domain type should be configured as *Foreign SMTP Domain*, which is one of the default domain type keywords. The Internet Domain must then be configured to

identify which domain addresses are to be sent via a Foreign SMTP Domain such as Internet Exchange. Wildcards such as *.* are permitted which would mean ALL domains.

If you enter something like *.com then any domain with the extension .com, e.g., lotus.com, would be sent via the Internet through Internet Exchange.

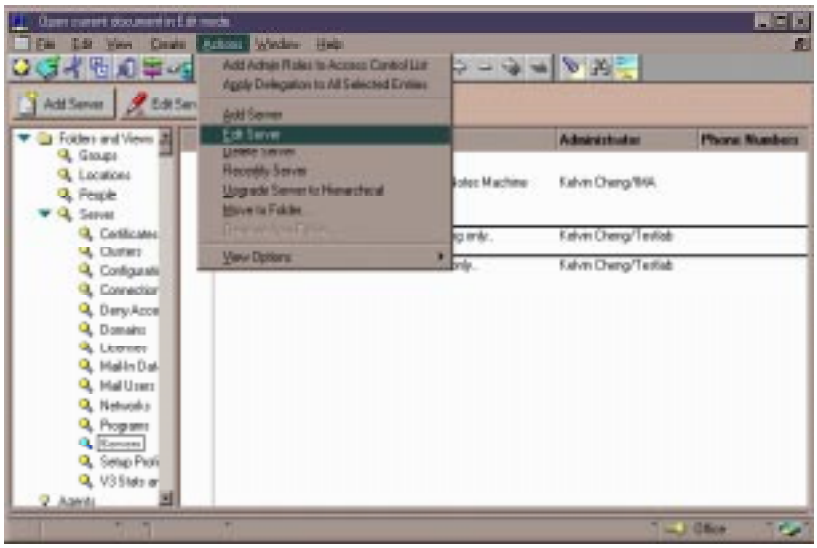


Lotus Notes Image

In the option *Should be Routed to*, you specify a hypothetical Domain Name which we call *ieln* (for Internet Exchange for Lotus Notes) in this example. This field is used to specify all outgoing SMTP Mail. You may choose to call it any name you like. Once you are finished, save and exit this menu.

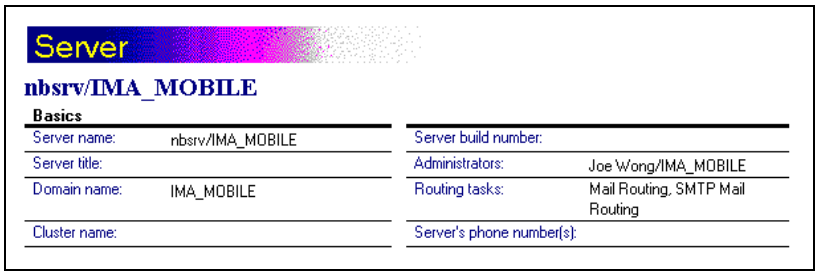
Modifying the Server Document

Once you have finished with the domain setting you must configure the Server options under *Action/Edit Server*. This is shown in Fig 5.3. The server configures the Routing logic and tasks for your mail destined for SMTP routing via the Internet.



Lotus Notes Image

In Routing tasks you should add the additional keyword *SMTP Mail Routing*



Lotus Notes Image

The Server connection provides information to Lotus Notes on how to route the Internet Mail by defining the Connection Type as SMTP. The Source Server and Source domain is the Notes Server and Domain from which mail is sent. The Destination Server and Destination Domain is the location to which all Source Mail is routed. In the following example we have given this the name *ieln*, the same name that we defined earlier as the domain in the *Should*

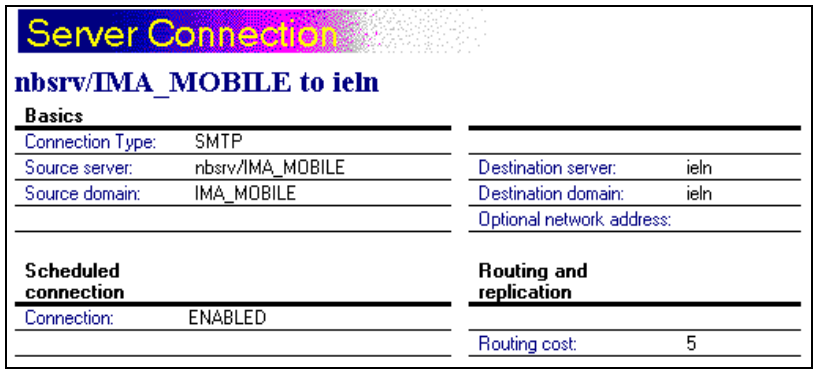
Be Routed To field. This will route the mail to the Internet Exchange Mail gateway and send it via the Internet. The Domain Name setting is case sensitive which means you must adhere to exactly the same case syntax that you have used before.

The Destination Server and the Destination Domain itself can be called anything as long as they are called the same. It will not influence the setting of **Internet Exchange** at all if you change the name to anything else. Make sure it is the same name as in the Domain settings.

If you already have this setup from a previous installation you will most likely only need to add an additional Routing Task which would be SMTP Mail Routing and then save and close the menu.

Configuring the Gateway Server Connection

Open the Server Connection in *Create/Server/Connection*.



Lotus Notes Image

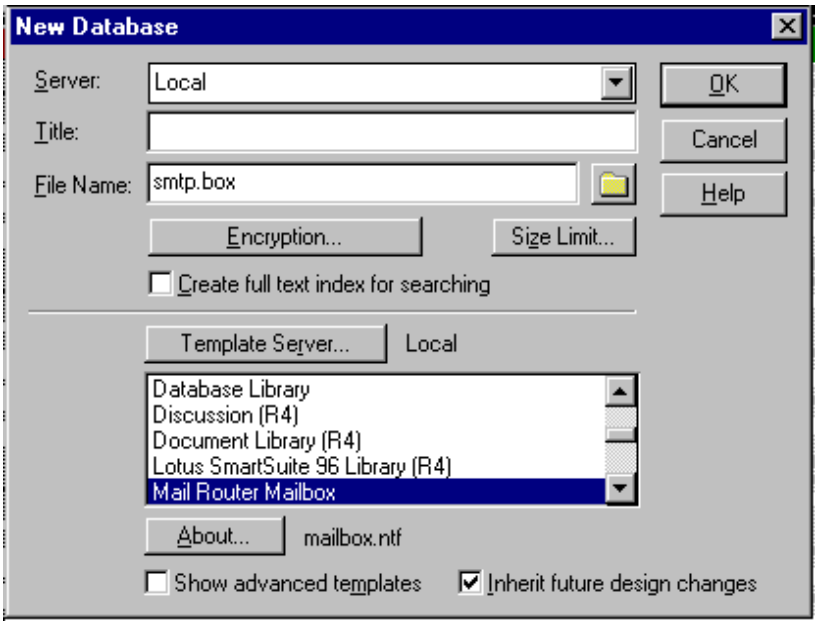
Your scheduled connection should be set as *ENABLED*, and the routing and replication to an integer value (e.g., *5*). Routing cost is the measurement used for determining the best route between servers to servers. You may enter any value at will. If you have a large network, ask your administrator what the best routing cost value would be. The Source Server must be the name of the system / Notes Domain.

Setting up the Notes Server for Internet Mail

Notes requires that a new database be configured for Internet Mail as well as additional configuration for access control to the database.

Creating a new database

In the New Database option under *File/Database/New* or using the shortcut *[CTRL]-N* you may create the new database. The following dialogue box will open.



Lotus Notes Image

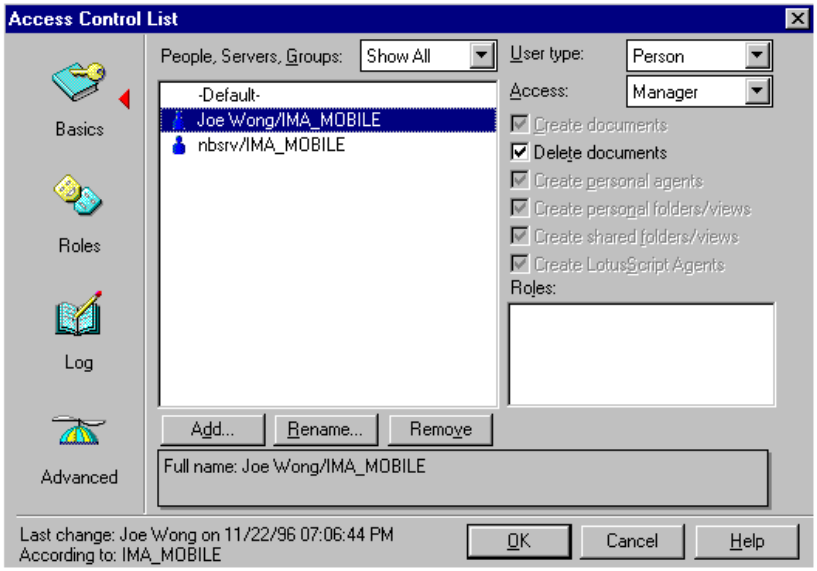
In most cases the Notes Server is Local as this will be the server where SMTP mail is being configured to run. The filename for Internet Mail should be called *SMTP.BOX*. The template used for this database is *Mail Router Mailbox* which can be selected by scrolling down the template options.

The *Mail Router Mailbox* template is a special Notes template used to automatically create a database that holds mail in transit to other servers or users. This database will manage and hold all your outgoing Internet mail with Internet Exchange.

Once this has been setup a new workspace icon should appear with a label such as *Smtp on Local.*

Setting up Access Control

Every database includes an access control list (ACL) which Notes uses to determine the level of access that users and servers have to a database. You must now configure the mail database *SMTP* with the correct access permissions. The Access Control List dialogue box is in *File/Database/Access Control* once you have selected your new database (in this case SMTP.BOX).



Lotus Notes Image

Although the names of access levels are the same for users and servers, those assigned to users determine the tasks that users can perform on a database while those assigned to servers determine what information within the database the servers can replicate. In

this example we have entered the user *John Doe/JADE_MOBILE*. The requirement is that the Access be set to *Manager* and with the permission to *Delete documents.* This step is important as this will be the user that Internet Exchange uses to control this particular mail database as the Gateway Administrator.

Repeat the same steps for the mail database *MAIL.BOX* and make sure that you are editing the access control of that particular database. The User with access control in *MAIL.BOX* should be the same with access control as *SMTP.BOX*, in our example it would be *John Doe/JADE_MOBILE.*

After you have performed all these basic installation steps your Notes server is now ready to send mail through to the Internet via **Internet Exchange**.

Differences Between Lotus Notes Server and Workstation Versions

If you are using **Internet Exchange** with a Notes server then you may skip this section. If you are using Lotus Notes Workstation and installing the **Internet Exchange** on such, some minor modifications need to be made.

In the section *Creating a new database*, we explained how to set up a new database for SMTP mail which we called *SMTP.BOX* with the template server *Mail Router Mailbox.* For the Workstation version of Internet Exchange, follow the same steps to configure *SMTP.BOX* except replace that same value with *MAIL.BOX*, then go to the Access Control list and add permissions to that same user for *MAIL.BOX*.

CHAPTER 5
INTERNET EXCHANGE FOR NOTES INSTALLATION

INSTALLING INTERNET EXCHANGE FOR NOTES

Before attempting to install **Internet Exchange for Lotus Notes** you must set up the Notes server as described in Chapter 4.

You should then prepare the worksheet provided in this chapter to ensure that you have essential installation information ready to hand when you begin. Please read the following instructions carefully before installation and then use them as a tutorial during installation.

Once the Installation Worksheet is complete, you are ready to perform the actual installation.

What is included in the Installation Files?

INSTALL.EXE
The Internet Exchange for Lotus Notes Installation Program to be run under Microsoft Windows 95 or Windows NT.

IMASETUP.EXE
The Internet Exchange setup program - this is launched by *install.exe*, and need not be run separately.

REGISTER.WRI
Internet Exchange Registration Form in Microsoft Write format.

RELNOTE.WRI
Internet Exchange Release Notes in Microsoft Write format.

LICENSE.WRI
Evaluation License text in Microsoft Write format.

CHECK THAT ALL IS READY FOR THE INSTALLATION

Before you run the **Internet Exchange** *INSTALL* program, it is necessary to assemble all the information needed for the installation, including information about where to install **Internet Exchange**. You must also prepare Lotus Notes as described in Chapter 4.

To assist with the installation of the gateway software, please review and fill out the installation worksheet on the following two pages prior to the start of the installation. Each item in the worksheet will be discussed in the following sections.

Internet Exchange for Notes

Installation Worksheet

Gateway Parameters

Program Directory	
Queue Directory	
Temporary Directory	
Forms Directory	
Local Character Set	
Local Time Zone	

Lotus Notes

Notes Mail Server	
User / Server ID File in Use	
Password for the ID File	
Gateway Administrator	
Local Notes Mail Domain	
Local Internet Hostname	
Local Internet Domain	
Host Table Filename Location	
DNS Server List	
Mail Relay Host Name	
Local Character Set	
Local Timezone	
Daylight Saving	

contd …

Installation Worksheet continued

TCP/IP

Host Name	
Domain Name	
Host File Location	
Mail Relay Host	
Name Server Addresses	

Gateway Parameters

The Gateway Parameters sections of the installation worksheet identify parameters that are associated with either the installation and/or the overall operation of the gateway.

Program Directory

The default location for **Internet Exchange** to be installed is c:\ienotes. This is where the programs and libraries reside. This directory can be located anywhere, however it is strongly recommended that it be placed on a local hard drive for performance and reliability reasons.

Queue Directory

The default location for **Internet Exchange** to store temporary files is c:\ienotes\queue. This is where the messages and log files reside. This directory can be located anywhere, however it is strongly recommended that it be placed on a local hard drive for performance and reliability reasons. However, the program and queue directories do not have to be on the same disk. This allows for a more flexible installation.

Temporary Directory

This is the directory in which **Internet Exchange** will store messages. It is usually configured to be a subdirectory of the queue directory. However, it can be set to a different directory and/or drive depending upon local disk availability.

Forms Directory

This directory is used **by Internet Exchange** to store Lotus Notes forms in ASCII representation. For further information see *Forms* configuration in *Chapter 7*.

Local Character Set

The ISO character set to be used. Most Anglo-Saxon countries can select US-ASCII, while others will prefer to choose a different character set. All outgoing email will be tagged as using the selected character set.

Local Time Zone

This is the time zone in which the local machine resides. Whether this time zone uses daylight saving or not should also be noted. There are many locations configured in the system, including the USA, much of Europe, and Asia. If the local time zone is not listed, then it will have to be entered manually into *IELN.INI* with an editor as follows:

[Gateway]
Timezone=*tzn*[[+ | -]]*hh*[[:*mm*[[:*ss*]]]][[*dzn*]]

The *tzn* must be a three-letter time-zone name, such as PST, followed by an optionally signed number, *hh*, giving the difference in hours between UCT and local time. To specify the exact local time, the hours can be followed by minutes, *:mm*; seconds, *:ss*; and a three-letter daylight-saving-time zone, *dzn*, such as PDT. Separate hours, minutes, and seconds with colons (:). If daylight saving time is never in effect, as is the case in certain states and localities, set *Timezone* without a value, for *dzn*. If the *Timezone* value is not currently set, the default is PST8PDT, which corresponds to the Pacific time zone of the USA.

If the time zone "Use system TZ variable" is selected, the timezone information will be obtained from the user defined TZ environment variable. Under Windows 95, this can be set in the *autoexec.bat* system startup file. Under Windows NT it is usually set in the system registry. In either case, the machine must be rebooted in order to make the change effective.

Lotus Notes Parameters

The Lotus Notes section of the installation worksheet identifies parameters used in setting up the exchange of messages between Lotus Notes and the gateway.

Notes Mail Server

This is the name of the Notes server to which the gateway will be connected, e.g.,

User / Server ID file in use

This is the name of the ID file specified in the entry *"KeyFileName="* of NOTES.INI. **Internet Exchange** uses the owner of this ID file to access SMTP.BOX and MAIL.BOX in the Notes Server. Normally, this file will be created in the data directory of Lotus Notes Server / Workstation during installation process. If KeyFileName does not contain any path information, **Internet Exchange** will automatically append the data directory specified in *"Directory="* from NOTES.INI as the prefix, e.g.,

c:\notes\data\user.id for normal Notes Workstation Installation

c:\notes\data\server.id for normal Notes Server Installation

Password for the ID file

This is the password for ID file specified above. The password will appear as a row of asterisks (****) for security reasons.

Gateway Administrator

This is the user name for the gateway administrator. By default, **Internet Exchange** uses the owner of the ID file specified above as the name of the Gateway Administrator. Also, this is the alias for the Internet Postmaster. All Internet sites are required to support the Postmaster alias. When **Internet Exchange** receives a message addressed to Postmaster, it will be sent to this Notes user, e.g.,

postmaster/Crop.

Local Notes Mail Domain

This is the local Notes Mail domain name that the gateway should be connected to. This Mail Domain name will be created

automatically in the server during the first installation of the Notes Server, e.g.,

Jade

SMTP Domain Name

This is the domain name to which **Internet Exchange** is attached, defined in the "Foreign SMTP domain" Notes Document of the Notes Public Address Book. Select the correct entry to enable concurrent multiple SMTP server operation for the same Notes environment, e.g.,

ieln

Local Internet Hostname

The Internet hostname for the local machine which is running **Internet Exchange**. This is the leftmost part of the fully qualified domain name for this host, and should contain no dots, e.g.,

iegate

Local Internet Domain

The Internet domain for the local machine which is running Internet Exchange. This is the remaining part of the FQDN for this host after the above hostname is removed, e.g.,

jade.net

Host table filename location

The full path for the host table. This must include both the drive, directory and name of the file, e.g.,

c:\etc\hosts

DNS server list

A comma separated list of Internet DNS servers, if DNS is being used, e.g.,

192.0.0.1, 192.0.0.2

If just a single DNS server will be used, just enter it alone, e.g.,

192.0.0.1

Note: this field is optional.

Mail Relay host name

The hostname of a smart Internet site which can be used as a last resort for hostname resolution. If a hostname cannot be resolved via either DNS or a local host table, then the message will be passed to the mail relay host for delivery. If needed, a secondary mail relay host may be configured within SYSMAN, for use when the primary mail relay host is inaccessible, e.g.,

relay.jade.net

Note: this field is optional.

Local character set

The ISO character set to be used. Most Anglo-Saxon countries can select US-ASCII, while others will prefer to choose a different character set. All outgoing email will be tagged as using the selected character set.

Local Timezone

Select the local timezone from those in the combo box.

Daylight saving

Set this checkbox if the local timezone uses daylight saving in the summertime.

TCP/IP Parameters

The TCP/IP parameters section of the installation worksheet identifies parameters associated with the local TCP/IP network.

Host Name

Each host on the Internet must have a unique identifier so that email bound for that site has a single unambiguous destination. This identifier is known as the Fully Qualified Domain Name (FQDN).

The host name parameter is the name component of the gateway machine FQDN. For example, if the FQDN of the gateway is *iegate.jade.net* then the host name would simply be *iegate*.

Domain Name

This is the domain component of the gateway machine FQDN. For example, if the FQDN of the gateway is *iegate.jade.net* then the domain component would be *jade.net*.

Host File Location

This is the full path name of the TCP/IP host file. Even if the Domain Name System (DNS) is used for host name to address translation, it is recommended that a host file be present that contains addresses for the following hosts: loopback, gateway machine, and your mail relay host.

Mail Relay Host

The mail relay host is the name of the machine that is used to send mail that cannot be resolved by either host table lookup or by DNS queries (or if you have configured **Internet Exchange** to use a default mail relay host only). It is required that this host have an entry in the local host table in the event that the DNS cannot be contacted.

Name Server Addresses

This is the list of name servers to contact for performing MX record and Address record lookups using the Domain Name System (DNS).

Internet Exchange For Notes Installation Procedures

Internet Exchange provides the user with the ability to customize the location of various components of the gateway. When specifying the various locations, be sure to choose paths with sufficient diskspace. IELN Programs is where the program executables are stored, Message Queues is where the internet mail is stored before being sent, and template forms is where forms are stored.

The CD Installer

The **Internet Exchange** Compact Disc Installer is a front-end program designed to facilitate and automate gateway installation. In addition, it also provides the option to install Adobe Acrobat Reader in order to view various Portable Document Format (PDF) files included on the CD such as the instruction manual, product comparison documents, benchmarking reports, **Internet Exchange** Whitepapers and so on.

To install **Internet Exchange**, perform the following tasks:

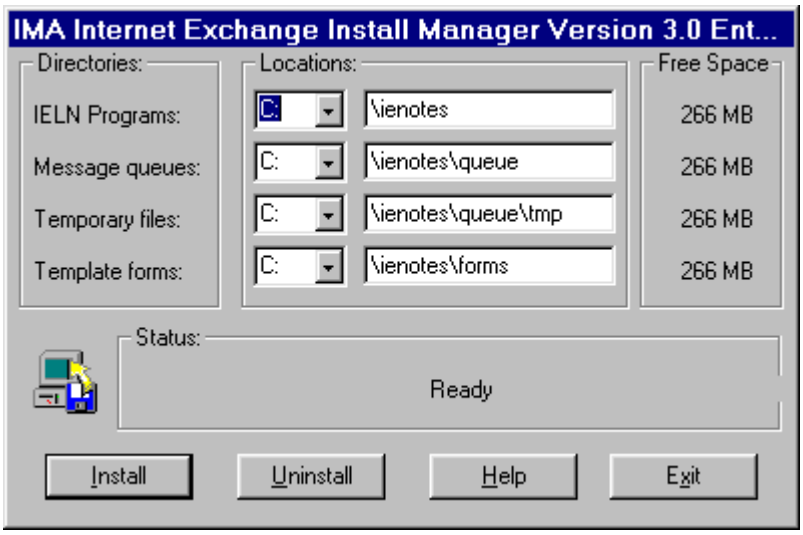
1. Make sure your computer and monitor are turned on and the Windows environment is running.
2. Shut down the Notes Server if it is already running.
3. Before you run the installation program you must define the full path of the *nnotes.dll* (eg. *C:\notes\nnotes.dll*), which is included in the Notes directory. Under Windows95 you must include this in your *autoexec.bat* file and append it to your path directory, then reboot. In Windows NT you may edit the full path in the *system.cpl* file which is located in the Control Panel. If you do not know what the full path is, you may use *find* to search for the directory where this file is located.
4. You should also have a hosts file which maps your Internet IP address with your server's Internet Host and Domain Name.
5. Insert the **Internet Exchange** Compact Disc into an available CD-ROM. The *install.exe* file is located on the CD under one of the following directories depending upon which product you are installing:

\IECM-ENTERPRISE	**Internet Exchange for cc:Mail**, *Enterprise Edition*
\IECM-WORKGROUP	**Internet Exchange for cc:Mail**, *Workgroup Edition*
\IELN-ENTERPRISE	**Internet Exchange for Lotus Notes**, *Enterprise Edition*
\IELN-WORKGROUP	**Internet Exchange for Lotus Notes**, *Workgroup Edition*

In order to run the installation without the assistance of the CD Installer, locate the appropriate installation program and run it.

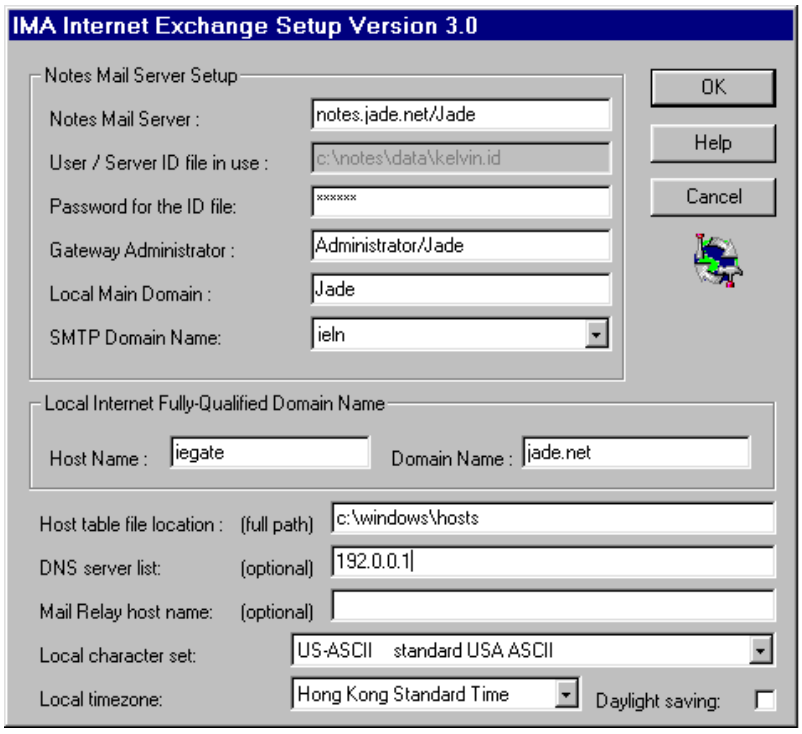
5. Choose the option to install **Internet Exchange** on your system.

Install will then present the Install Manager screen.



Simply follow the instructions that will then pop up to install the **Internet Exchange** Lotus Notes Gateway. You will then be prompted by the IMA **Internet Exchange** Setup dialogue box (see

next page) where most of the settings should coincide with your previous Lotus Notes Server settings.



The options *Notes Mail Server*, *User / Server ID file in use* and *Local Main Domain* should all already be setup automatically and coincide with your Lotus Notes Server or Workstation installation for Foreign SMTP Mail. The Gateway Administrator is the user you have already set up in with manager access to *SMTP.BOX* and delete documents permissions.

The *Password for the ID file* is the password for the ID file specified above. If there is no password set for the specified ID file, just leave this entry blank.

You now need to provide additional information for the Internet Exchange Setup program for it to function properly.

Local Internet Fully-Qualified Domain Name (FQDN) is the Internet domain and hostname for your gateway system that is connected to the Internet to send Internet Mail. If you are not sure what this is, please contact your system administrator. The hostname and domain name must be mentioned in the hosts table of your operating system. This is traditionally already configured in Windows NT 4.0, however in Windows NT3.5x and Windows 95 a host file may not be present, and must be set up.

To create a hosts file (you may use EDIT or Notepad), please make sure that the following information is included:

```
#
# This is a sample HOSTS file used by Microsoft TCP/IP
# for Windows 95
#

127.0.0.1           localhost

your.ip.address     hostname.internet-domain-
                    name.organisation
```

your.ip.address is your real IP address on the Internet such as 202.75.0.3 and *hostname.internet-domain-name.organisation* is your real internet domain name. In our example in 5.2 this is *nbsrv.ima.com.*

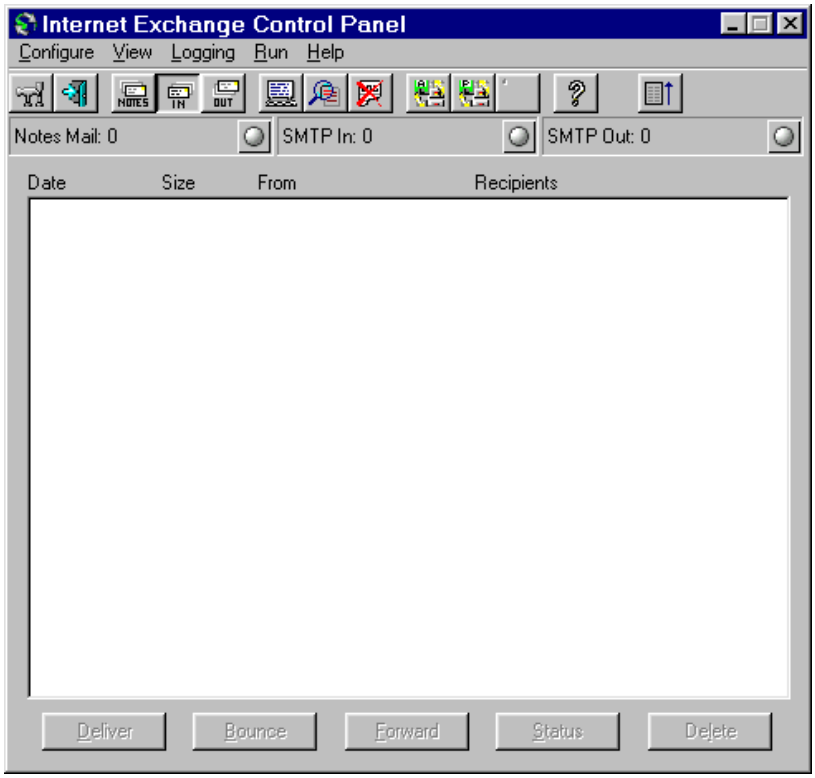
Once the host file has been created, the location of this file needs to be entered into *Host table file location*. Traditional locations would be c:\windows\hosts or c:\hosts.txt (make sure that the file exists in the path that is defined).

If you are using the DNS for address to name mapping, this must be setup next. The IP address or addresses of the name servers you wish to use are entered into the DNS Server list. If you do not know which IP addresses to use, please consult your system administrator our your internet network provider. The Mail relay host setting is an alternative option that permits you to send mail routing all your mail through a mail relay host. It may be left blank for most purposes.

> ***NOTE***: For sites connected via dialup IP to a service provider, it is recommended that the Mail Relay host be set to the ISP mail relay.

The installation program will now restart the Lotus Notes Server. During the **Internet Exchange** installation process, the program group ***Internet Exchange*** is created and the icons for the following programs are set up: *SYSMAN*, *NOTESIN*, *NOTESOUT*, *SMTPD*, and *SMTPC*.

After the appropriate licensing information has been entered, start up Internet Exchange by clicking on *sysman.exe* or on Internet Exchange in your newly created Program Manager group. The Internet Exchange System Manager will then be started.

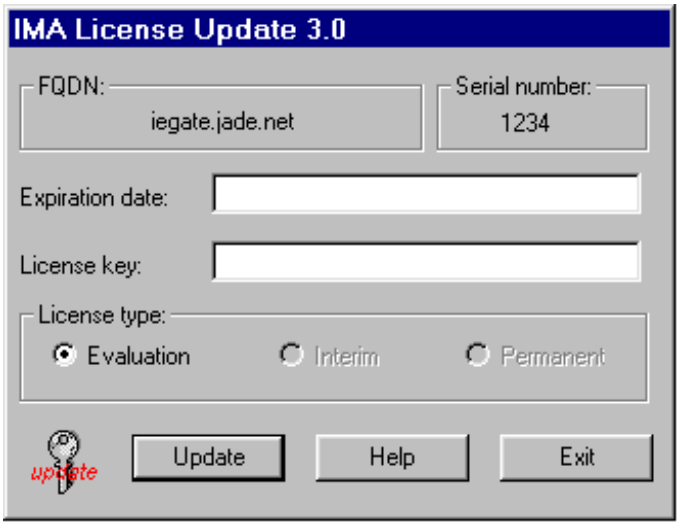


Internet Exchange is now fully configured and ready to go. There are many extra options and features which are explained in detail in the online *HELP*. The base installation is already configured to send and receive electronic mail via the internet.

You may now send electronic mail via the Internet to test Internet Exchange. If you have successfully set up the program you may send your first message to IMA Technical Support by clicking on *HELP* and *IMA Technical Support* and we will respond to you as soon as possible.

Once *Setup* is complete, it will offer to update the gateway license. If desired, the *License Update* program will be automatically started. This program can also be run at any time by selecting the *License Update* program from the *Internet Exchange for Lotus Notes* Program Group.

After License Update is started, the following screen will be displayed:



There are two read only fields that appear when the *License Update* program starts - the FQDN and Serial Number. The FQDN, or fully qualified domain name, is the official name for the gateway. The

Serial Number field displays the unique serial number built into the current copy of *Internet Exchange*. These are the two fields that need to be provided by your supplier or IMA to generate a license key as described below.

There are three types of software licenses that can be generated for *Internet Exchange*. They are:

Evaluation License

If this copy of *Internet Exchange* was obtained from a public access site (anonymous FTP, the Web or a commercial service), it is not possible to permanently enable the gateway. For these versions of the gateway, the evaluation license radio button will be the only option.

To obtain an evaluation license, it is necessary to contact your supplier or IMA, either by phone, fax, or email. Email requests should be sent to:

eval-auth@ima.com

When requesting an evaluation license, please provide a completed registration form, which can be found in the Internet Exchange for Lotus Notes program group.

After obtaining the evaluation license, it is necessary to enter both the expiration date of the license as well as the license key. The expiration date is entered in the form mm/dd/yy. The license key should be entered exactly as obtained from your supplier or IMA. After entering the appropriate expiration date and license key, press the *Update* button to store the registration information.

Interim License

Interim licenses are similar to Evaluation licenses, with the exception that Interim licenses can be updated in the field to a Permanent license at a later date. To obtain and apply an Interim license, follow the same procedure as outlined for an Evaluation license. Instead of sending email to *eval-auth*, please contact either your supplier or IMA, or send email containing full registration information to:

auth@ima.com

Permanent License

Unlike Evaluation and Interim licenses, Permanent licenses do not have any expiry date associated with them. These licenses are based upon the **Internet Exchange** serial number and the Fully Qualified Domain Name (FQDN) of the gateway machine. To obtain a Permanent license key, please contact either your supplier or IMA, or send email containing full registration information to:

auth@ima.com

Since there is no termination date to a permanent license, the only information you need to enter for a Permanent license is the license key. Enter the key and press the *Update* button to store the registration information.

After storing the license information with License Update, the installation and licensing of **Internet Exchange** is complete and the gateway is ready for use.

INSTALLING THE REMOTE CONTROL

The Remote Control uses HTTP, HTML and CGI in order to allow administrators to monitor, configure and operate **Internet Exchange**. A web server has to be installed on the machine running the gateway for the Remote Control to operate (for best results the web server should be dedicated solely to the Remote Control). **WebSite Professional** from O'Reilly Software (*http://website.ora.com*) was successfully tested, and it is recommended by our technical staff. Accepted web browsers are Netscape Navigator 3.01 or higher and Internet Explorer 3.02 or higher. A screen resolution setting of at least 800x600 pixels is required.

The Setup Program

The setup program **INSTRC.EXE** will automatically install Remote Control modules on to the gateway system with only a minimum of

information required. The HTML files and CGI programs required for remote access are automatically copied to their corresponding physical directories on the gateway system. If you are using O'Reilly's WebSite, the Setup program will also automatically add the URL and CGI mappings to the web server's configuration.

Shut down the web server prior to running the Setup program.

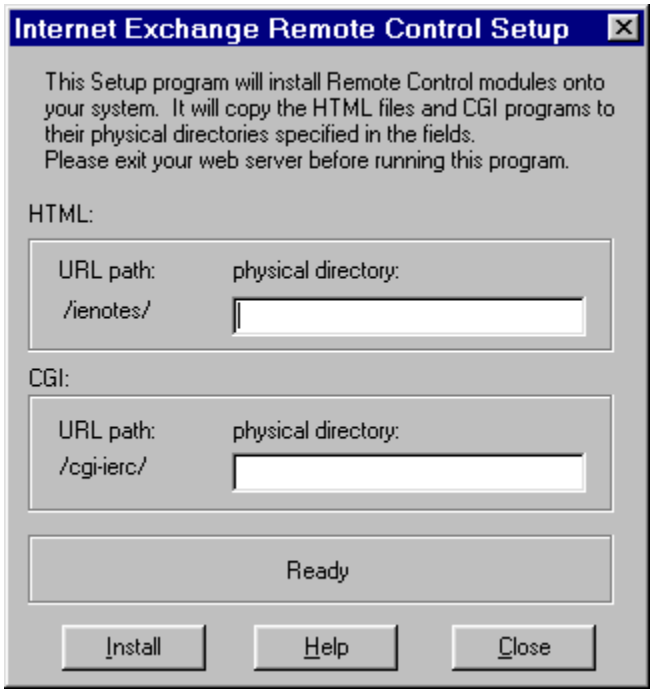
The URL path for the HTML files is:

/ienotes/

And the URL path for the CGI programs is:

/cgi-ierc/

It is strongly recommended that you apply security protection to these URLs.



HTML Physical Directory

Specifies the physical directory in which to store the HTML files required by the Remote Control. If WebSite is used the default directory will be *c:\website\ienotes*, where *c:\website* is the root directory of WebSite.

CGI Physical Directory

Specifies the physical directory in which to store the CGI programs required by the remote Control. If WebSite is used the default directory will be *c:\website\cgi-erc*, where *c:\website* is the root directory of WebSite.

Install

Starts the setup process and installs the Remote Control.

Help

Displays the help file on Remote Control Setup.

Close

Exits the setup program.

After the Setup process is complete, start the web server. To remotely access the gateway from any PC, establish an Internet connection and enter this path into your web browser's location field:

http://web.server.name/ienotes/index.htm

where web.server.name is the name of your web server. A window allowing remote operation, configuration and monitoring of the gateway will load.

INSTALLING INTERNET EXCHANGE FOR NOTES AS A WINDOWS NT SERVICE

In order to install **Internet Exchange** as an NT Service, simply run the Service Installer **INSTSRV.EXE**. This program is designed both to install **Internet Exchange Service** on an NT system and to remove it should the need arise. You are required to login to the Windows NT account with Administrator privileges before running the Service Installer.

Install

Installs **Internet Exchange** as a Windows NT Service.

Uninstall

Removes **Internet Exchange** as a Service from the system.

Help

Displays information and notes about installation.

Close

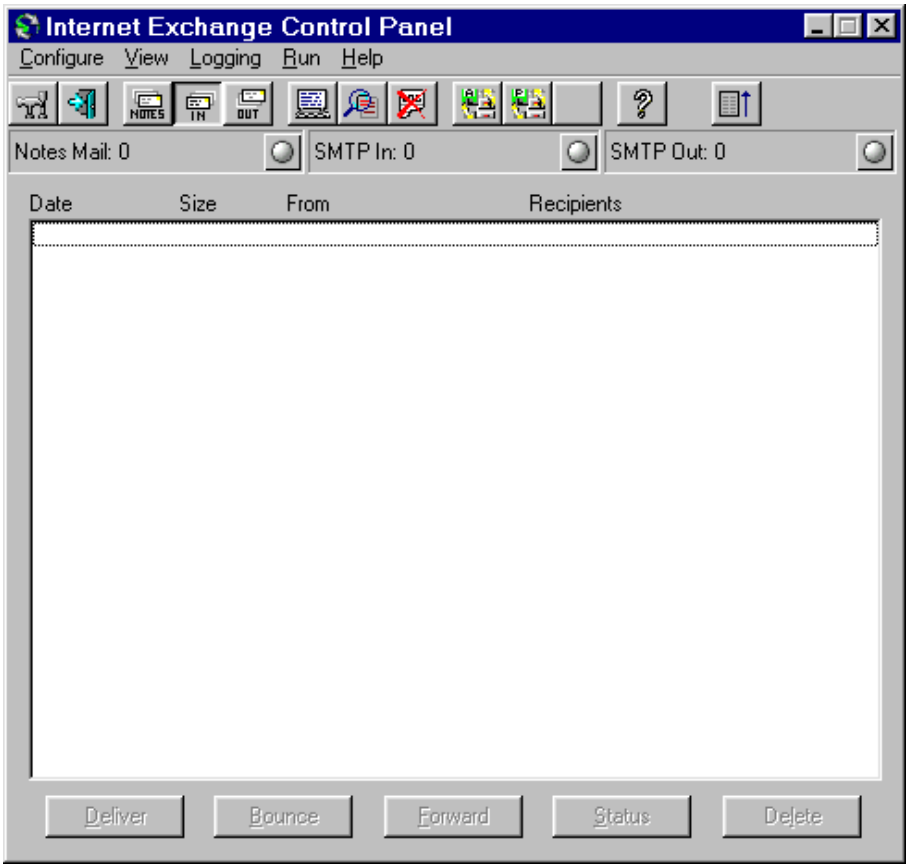
Exits the Service Installer program.

When the installation is complete, you may configure the manner in which **Internet Exchange** as an NT Service is started up (manual or automatic) by clicking on the "Service" icon in the Windows Control Panel. In order to start up the Service automatically, the path of the Notes client/server installation directory must be added to the system path; it is possible to do this in the "System" menu of the Control Panel. The Notes client/server installation directory contains *nnotes.dll*, which is used by the gateway to communicate with the Notes environment.

In order to configure the service to be started up automatically along with the NT machine, all the network paths used by the gateway have to be specified in UNC (Universal Naming Convention) instead of the regular network drive letters.

STARTING INTERNET EXCHANGE FOR NOTES

During the **Internet Exchange** installation process, the program group ***Internet Exchange*** is created and the icons for the following programs are set up: *SYSMAN*, *NOTESIN*, *NOTESOUT*, *SMTPD* and *SMTPC*. To start **Internet Exchange**, double click on the System Manager icon with the title *IMA Internet Exchange*. The system manager will then start, along with the SMTP Daemon, and the following window will be displayed:



The rotating globe that appears on the Windows Taskbar indicates normal operation of the gateway, although its rate of rotation may vary. When the System Manager is started, the SMTP daemon icon is placed on the Taskbar; the existence of this icon indicates that the SMTP Daemon is running and listening for incoming SMTP requests:

At this point, **Internet Exchange** is up and running, ready to exchange messages between Lotus Notes and the Internet.

If the SMTP daemon should fail for any reason, the icon will disappear, and the *Restart SMTP* button on the System Manager will become activated.

PART 3 OPERATION

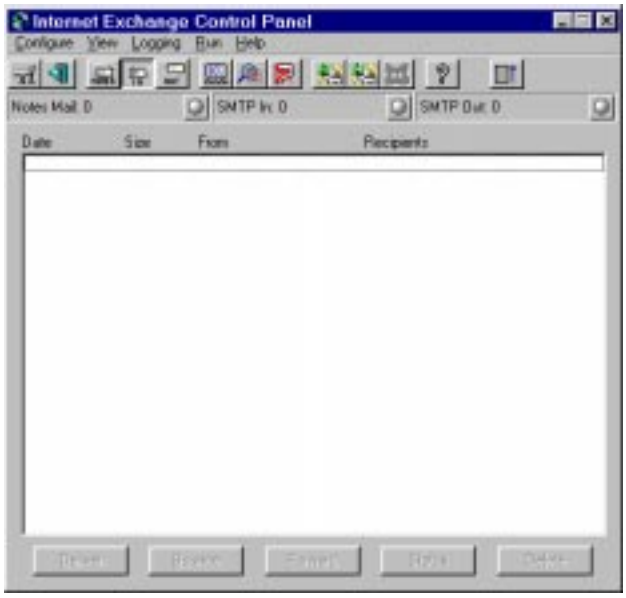
CHAPTER 6
GATEWAY MANAGEMENT

SYSMAN

The **Internet Exchange** System Manager (*SYSMAN*), or Control Panel, is the main user module responsible for gateway activity scheduling, configuration and individual queue tracking. *SYSMAN* binds the different modules together and keeps track of the time and frequency at which the various queue managers are run, and is responsible for launching these managers at the appropriate time.

SYSMAN is also used to configure and operate **Internet Exchange**. All configuration options are handled by and accessed via *SYSMAN*. It provides visual displays of the three gateway queues: *SMTP IN*, *SMTP OUT* and either the outbound cc:Mail post office mailbox (cc:Mail version), or the outbound Lotus Notes *SMTP.BOX* mailbox (Notes version). Detailed information for any message in these queues is obtained by selecting the appropriate queue and double-clicking on the message item. Selected messages can be forwarded, bounced, delivered or removed from the queue by clicking the desired button on the *SYSMAN* console.

Sysman Console: Internet Exchange for cc:Mail



Sysman Console: Internet Exchange for Notes

MESSAGE QUEUES

As detailed in *Chapter 1 - Internet Exchange Functional Overview*, **Internet Exchange** maintains three separate message queues:

cc:Mail Post Office / Lotus Notes Database  / 	These are the queues that are internal to the respective mail systems. For cc:Mail, this is the queue in the *Internet* Post Office, and for Notes, this is the *SMTP.BOX* Notes queue.
SMTP IN 	Stores messages received from the Internet by *SMTPD* and bound for local cc:Mail or Notes users.
SMTP OUT 	Stores messages bound for the Internet that have been exported from the local cc:Mail Post Office or Notes Server by *CCOUT* or *NOTESOUT*.

Each of the above queues can be viewed separately by selecting the appropriate button, or by using the pull-down *View* menu of **Internet Exchange** Control Panel's main screen.

When selected, any entries present in the queue are displayed in the information area located immediately below the toolbar and queue counters. The number of entries in the queue should match the number given in the corresponding queue counter. Under certain circumstances, such as when the system is under heavy load, the queue entry counters may become unsynchronized with the displayed information. In such situations the System Manager can appear to be unresponsive to user input. This is considered normal behavior as it is a side-effect produced by the Windows and VIM or Notes API implementations.

NOTE: In such situations ***DO NOT*** attempt to gain the attention of the system by repeatedly clicking on various boxes. These interrupts are queued for processing when a time slice becomes available and, when processed, may result in an action or actions being taken which were not desired. The

responsiveness of the System Manager under these conditions (and the throughput of the system in general) can be improved by turning off *Regular Screen Updates* in the *Options* configuration window.

Queue indicator button states:

Gray: either there are no messages in the queue or the queue is currently active, processing messages.

Green: the queue is currently idle and awaiting the next scheduled processing for that queue. Pressing this button will begin the processing of messages in this queue immediately.

MESSAGE FUNCTIONS

Circumstances can arise which require administrator intervention. It may be necessary to delete, forward, or inquire about the status of a message. The message function buttons at the bottom of the queue list provide an interface that gives the administrator complete control over all messages passing through the gateway. Note that these actions can only be performed on messages that are waiting to be delivered. Once delivered to either cc:Mail or the Internet, they are out of reach.

It is generally desirable to make sure sync mode is switched off and that the queue run time is set to some large number (e.g. 1000 minutes) before attempting operations on a given message. Otherwise, the queue may be processed too fast to allow individual messages to be selected. Queue run times can be set in the *Schedules* configuration window.

Deliver

Selecting this option forces immediate delivery of the selected message.

Bounce

The bounce option lets the administrator return a message to the sender with an optional explanation. Once the bounce operation is selected, the administrator can enter a reason for returning the message in the *Reason:* field. The message is then bounced after the *OK* button is selected.

Forward

This option calls up a screen allowing the administrator to forward a selected message to another recipient. Once the forward operation is selected, the gateway administrator needs to enter the recipient address in the *Forward To:* field. The recipient address is different depending on which queue the message currently resides. If the message is in either the cc:Mail Post Office or Notes mailbox queues, the recipient address must be a valid cc:Mail or Notes address, whereas if the message is in either the *SMTPIN* or *SMTPOUT* queues, the recipient must be an Internet address. However, this is not a limiting factor. To forward a cc:Mail message for instance to an Internet user, specify:

user@host.domain AT Internet-PO-Name

e.g. *jim@xyz.org AT Internet*

To forward an Internet message to cc:Mail, specify:

user@cchost.domain

e.g. *J_Smith@sales.jade.net*

Only one recipient may be entered. Select the OK button to perform the forwarding operation.

Status

The status of a message can be determined either by selecting a message and then clicking on the *Status* button or by double-clicking on the desired message.

Delete

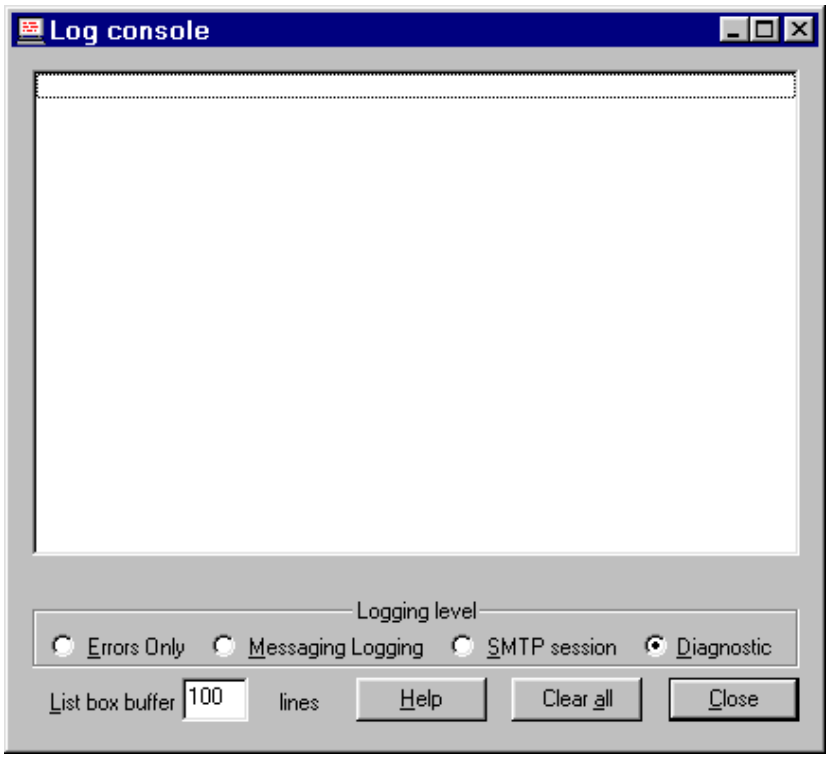
The *Delete* option deletes a message from the message queue after confirmation is provided. This protects against accidental deletion of messages. After the delete action is verified the system responds with confirmation of the deletion.

LOG FILES

Internet Exchange maintains four levels of logging information. This information can be very useful and may be required in order to determine the causes of certain email or network related problems that may occur. **Internet Exchange** logs all SMTP session level information by default. In general, this is both desirable and sufficient, but in rare cases more diagnostic information may be required. Logging at diagnostic level is too voluminous for general use and significantly reduces system performance.

Log console 

The Log Console can be viewed by selecting the *Show Log Console* button on the *Internet Exchange Control Panel* window or via the *Logging* pull-down menu. The log console allows the administrator to view varying types of gateway activity. The console view is built up from the larger log file, which keeps a record of all gateway activity. Four levels of logging are available, from basic (showing Errors only), to diagnostic level (showing all gateway activity). Viewing the diagnostic level can be quite helpful when experiencing any messaging problems.



Errors Only

Displays only erroneous activity related to gateway or message problems.

Messaging Logging

Displays all incoming and outgoing message related activity including any errors reported. Each queue processor adds a line to the log file for each message it processes.

SMTP Session

Displays any SMTP conversations into and out of the gateway as well as messaging and error activity.

Diagnostic

Displays the maximum level of information regarding gateway activity. This option is for debugging and is not normally required. Owing to the large amount of debugging information produced, this level of logging is only recommended for situations where very detailed logging information is needed. Such extensive logging will noticeably slow down the operation of the gateway.

List box buffer

Configures the maximum number of lines to be displayed on the list. This value cannot be larger than 1000.

Clear all

Removes all entries on the logging list.

Logfile 

The information contained in the log file can be viewed by selecting the *View Logfile* button on the *Internet Exchange Control Panel* window or via the *Logging* pull-down menu. The Windows default viewer (typically the *WordPad* application) is invoked.

By default, **Internet Exchange** logs all transactions in the file *IECCMAIL.LOG* (*IENOTES.LOG* for the Notes version) located in the gateway queue directory. The software will continue to log information until the file size reaches the maximum configured value. This value is defined with the *Logfile size* option under the *Gateway* configuration window; its default is 50,000 bytes (50K). When this limit is reached the log file is renamed and a new *IECCMAIL.LOG* (*IENOTES.LOG* for the Notes version) file is created to continue logging. The naming convention for old log files is:

ddmmmnnn.log

Where *dd* is the day of the month, *mmm* is the month, and *nnn* is a three digit number starting at zero, and increasing for each old log

file generated during that day. For example, on March 5th, the first few old log files to be renamed would appear as:

05Mar000.log, 05Mar001.log, 05Mar002.log, ...

If the *Send old logfile to postmaster* option is set, in the *Advanced Options* configuration window, old log files are automatically mailed to the local postmaster. The *Keep old logfile on disk* option in the same window controls whether old log files are kept on disk or deleted.

NOTE: if not deleted, log files continue to accumulate until manually archived or removed by the gateway administrator. If left unattended, they can grow to consume a significant amount of disk space.

When the *IECCMAIL.LOG* file is in use by another application, such as the WordPad application, messages are not logged to the log file and gateway activity information is discarded.

Clear Logfile 

Selection of this button clears the current log file. A dialog appears asking for confirmation if the *Confirm logfile deletion* option in the *Options Advanced* configuration window is checked.

UTILITIES

These utilities can be launched from the *Run* pull-down menu or with the following buttons:

 Address Conversion Utility

 Domain Conversion Utility

 Rule-based Address Generator (cc:Mail Version)

Address conversion utility

This utility converts information between the address file, an ASCII file that contains permissions and mappings between cc:Mail or Notes user names and Internet addresses, and the Alias Database, which stores specific local name to Internet name mappings, including their associated permissions and options. An alternative to running this manually is to enable the *Automatically update alias database* option within the *Dynamic Conversion* configuration screen. This enables *SYSMAN* to regularly check for changes in *SMTP.ADR* and run this conversion program automatically if any changes are detected. Setting this option greatly reduces the workload associated with maintaining the Alias Database.

This utility is explained in greater detail in *Chapter 11 - Utilities*.

Domain conversion utility

This utility converts between the *SMTP.POD* text file and the Domain Mapping Database, which stores mappings between cc:Mail Post Offices or Notes domains and Internet subdomains. An alternative to running this manually is to enable the *Automatically update domain database* option in the *Dynamic Conversion* configuration screen. This enables *SYSMAN* to regularly check for changes in *SMTP.POD* and run this conversion program automatically if any changes are detected. Setting this option greatly reduces the workload associated with maintaining the Domain Mapping Database.

This utility is explained in greater detail in *Chapter 11 - Utilities*.

Rules based address generator *(cc:Mail Version Only)*

The use of rules based addressing (RBA) allows increased flexibility with the types of Internet addresses that are used in **Internet Exchange**. While a very simple method of address formatting is provided by way of the default separator, the use of rules based addressing is much more powerful. Rules can be setup so that a number of incoming address formats are accepted, allowing many different addresses to be delivered correctly. In the same manner, a preferred format can be selected for translating outgoing cc:Mail addresses into Internet addresses.

Rules based addressing acts as a fallback for determining Internet to cc:Mail address mapping for all users of the gateway. Mappings found in the *Users* configuration take precedence over these rules. If no rules have been set up the gateway default mappings are subsequently used.

Running this utility allows configuration of new rules as well as compilation of the Directory Database. An alternative to running this manually is to check the *Enable scheduled compilation* checkbox in the *Rules-based addressing* window. This enables *SYSMAN* to run the database compilation automatically at regular intervals defined by the administrator. Setting this option greatly reduces the workload associated with maintaining the Directory Database.

This utility is explained in greater detail in *Chapter 10 - Rules Based Addressing*.

SMTPD 

The SMTP Daemon is the process which receives messages from the Internet for cc:Mail or Notes users. Unlike the other **Internet Exchange** modules, *SMTPD* is always running on the gateway machine. This is necessary because there is no way that the gateway can predict the timing or frequency of inbound messages.

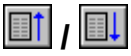
NOTE: SMTPD can be set to be manually turned on and off, which is useful in a dialup environment. In the *Setup* menu, under the *Options* tag, uncheck the box *Auto SMTPD restart* in order to enable manual starting and stopping of this daemon.

POP3 *(CC:MAIL VERSION ONLY)* 

The Post Office Protocol Version 3 (POP3) Server implementation allows access to the cc:Mail environment via POP3 clients such as Eudora, Netscape Mail, Microsoft Internet Explorer, and many others.

The POP3 server does not automatically start up with the gateway but is initiated manually via the *Run* pull-down menu or the POP3 button. Otherwise, POP3 can be configured to start automatically along with the gateway by checking the *Start with Gateway* checkbox in the *POP3 Setup* window. It is recommended to check the *Shutdown with Gateway* checkbox as well.

Further information regarding POP3 is available in *Chapter 12 - POP3*.

HIDE / DISPLAY MESSAGE QUEUE 

Toggles the **Internet Exchange** Control Panel display to show or hide the messaging queues. This partially minimizes or restores the Control Panel and is helpful if the gateway machine is non-dedicated, or if gateway administration is being conducted and gateway activity needs to be observed.

HELP AND SUPPORT

In addition to using the  button and operation sensitive help on each configuration screen to obtain on-line help, additional help can be accessed via the *Help* pull-down menu.

Contents

Displays the main Contents page for the on-line help. Links to all help topics for all the major **Internet Exchange** functions are available from here.

Search

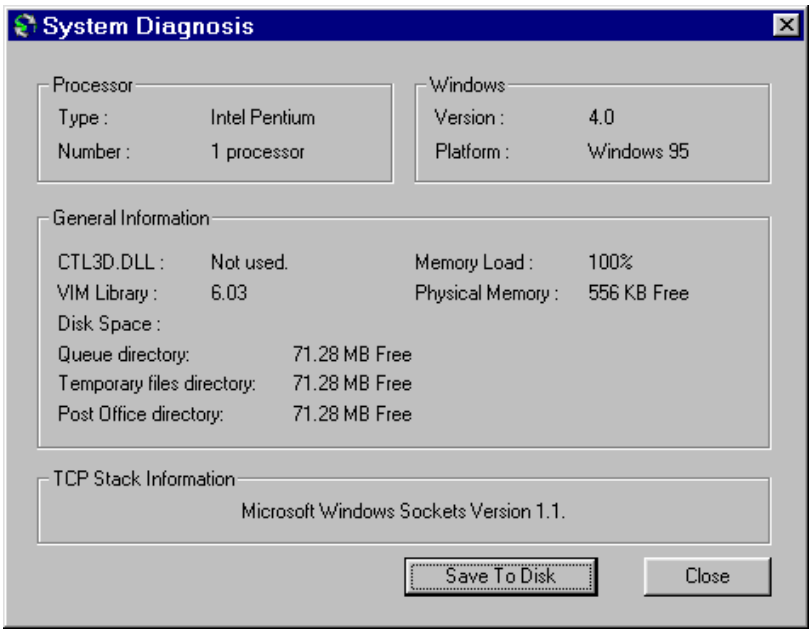
Provides a searchable index for all on-line help topics as well as the Windows *Find* utility to search the entire on-line help for a character string.

What's new

Displays the on-line help page with a list of the features added in the newest version of **Internet Exchange**.

System diagnosis

Displays the hardware and software specifications of the equipment on which the gateway is currently installed.



Processor type

The CPU make and model, e.g. Intel Pentium.

Processor number

The number of CPUs currently installed.

Windows version

The version number of the Microsoft Windows operating system.

Windows Platform

The type of Windows operating system in use, e.g. Windows NT.

CTL3D.DLL

The version of the Microsoft Windows 3D Windows Library, if used.

VIM Library *(cc:Mail Version Only)*

The version of the Lotus 32-bit VIM library. The VIM files can be located anywhere within the file system provided that the system's *PATH* includes this location.

Memory load

The percentage of memory currently in use by the system.

Physical memory

The available physical memory in Kilobytes.

Disk space - Queue directory

The available disk space on the hard drive containing the **Internet Exchange** queue directory.

Disk space - Temporary file directory

The available disk space on the hard drive containing the directory allocated for **Internet Exchange** temporary files.

Disk space - Post Office directory *(cc:Mail Version)*

The available disk space on the hard drive containing the cc:Mail Post Office directory.

TCP stack information

The type and version of the TCP stack installed on the system, e.g. Microsoft Windows Socket Version 1.1.

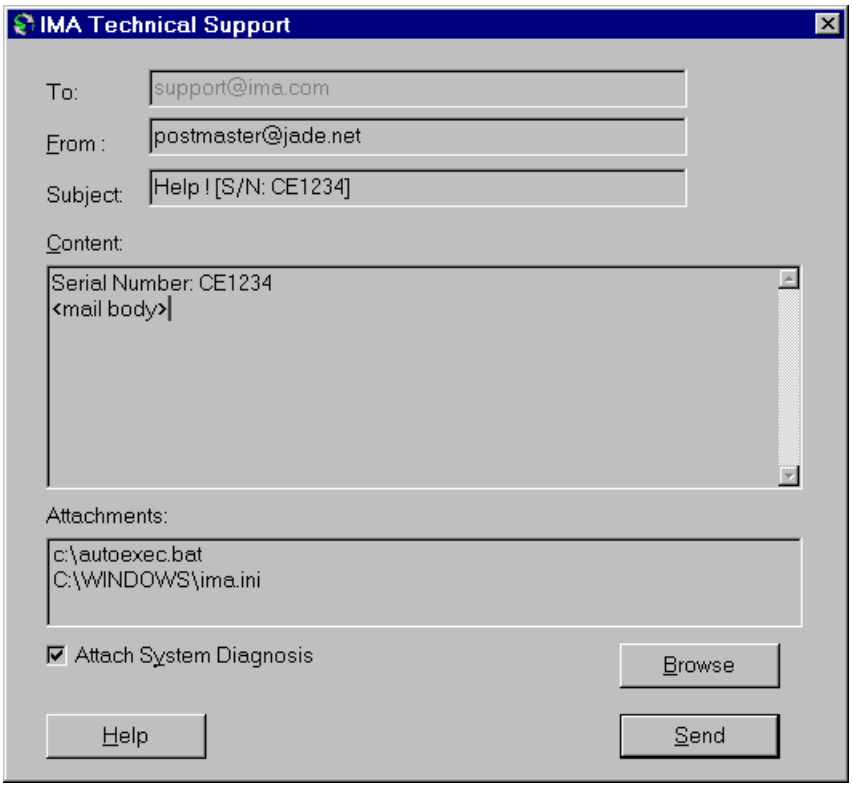
Save to Disk

Saves the current *System Diagnosis* information to a log file in the **Internet Exchange** queue directory,

E.g. *c:\ieccmail\queue\sysinfo.log.*

IMA Technical Support

Provides a simple method of sending email to IMA's Technical Support division. It automatically attaches pertinent files and allows additional information to be included.



The *To, From and Subject* fields are automatically filled. Additional support information can be added to the *Content* section. Use the *Browse* button to include additional files apart from those automatically included: *AUTOEXEC.BAT, CONFIG.SYS* and *IMA.INI/IELN.INI.* The *Attach System Diagnosis* checkbox determines whether to attach the hardware and software information regarding the gateway system as explained above. Once the *Technical Support* window has been filled, click the *Send*

button to forward this information to the IMA Technical Support department.

About Internet Exchange

Provides information regarding the current **Internet Exchange** version installed. Information presented includes:

Version number.

Edition : Enterprise or Workgroup, including the Beta status (if running Beta version).

License status : *Evaluation, Interim* or *Permanent.*

Copyright information.

Serial number : The 4/5 digit serial number, or displays *Evaluation* during the trial period.

Current date and time.

VIM Library version : At the time of writing, 6.03 is the latest 32-bit VIM tested. *(cc:Mail Version Only)*

TCP Stack Info : The socket version currently in use by Microsoft Windows. Socket version 1.1 or above are compatible with **Internet Exchange**. The standard WinSock used by Windows NT is version 2.0.

CHAPTER 7
CONFIGURING INTERNET EXCHANGE

CONFIGURATION OPTIONS

Ordinary configuration of **Internet Exchange** is conducted during gateway operation. The operating of both Internet Exchange for cc:Mail and Internet Exchange for Notes are identical in most areas. The exceptions are primarily in the areas of address conversions as the two environments support different local addressing conventions. In addition, Internet Exchange for cc:Mail has a POP3 Server and Rules Based Address Generator, while the Notes version has included support for automatic Forms conversion. The configuration and operation of both versions of Internet Exchange are documented here, with differences between the two versions being noted when applicable.

Configuration of **Internet Exchange** is accessed by clicking either the  button or on *Setup* in the *Configure* pull-down menu. Configuration of **Internet Exchange** is broken down into several functional groups. These are identified in the *Setup* window as various tabs and are made up of the following:

Post Office	Configures the name and location of the local cc:Mail post office. Also stores the local post office password and identifies the postmaster. *(cc:Mail Version)*
Lotus Notes Domain	Configures the name and location of the local Lotus Notes Mail Server. Also stores the User / Server ID file, ID file password, local Lotus Notes mail Domain and identifies the Gateway administrator *(Notes Version)*
Schedules	Configures the frequency at which the various queue managers are launched, and includes the RAS setup.
Gateway	Configures general gateway parameters including mode of operation, logging levels, system maximum sizes, and queue directory location.
Connection	Configures the host name, domain name, and location of the host table, and alternate names by which the gateway may be known.
Routing	Configures the list of DNS hosts to check for name resolution. Also identifies the name of the mail relay host(s) for default mail routing.
Options	Configures the default MIME encoding method, the default addressing separator as well as various options used in message delivery to cc:Mail.
Japanese Support	Configures the conversion of inbound and outbound messages between a Japanese cc:Mail environment and the Internet.
Anti-spam	Defines rules to trap spam mail attacking the mail system, and subsequent actions to be taken.
Peers	Defines capabilities of peer systems with which the gateway communicates.
MIME	Defines the mapping between DOS file extensions and MIME Content-Type and Content-Subtype identifiers.

Domains	Defines mappings between cc:Mail Post Offices or Lotus Notes Domains and Internet subdomains.

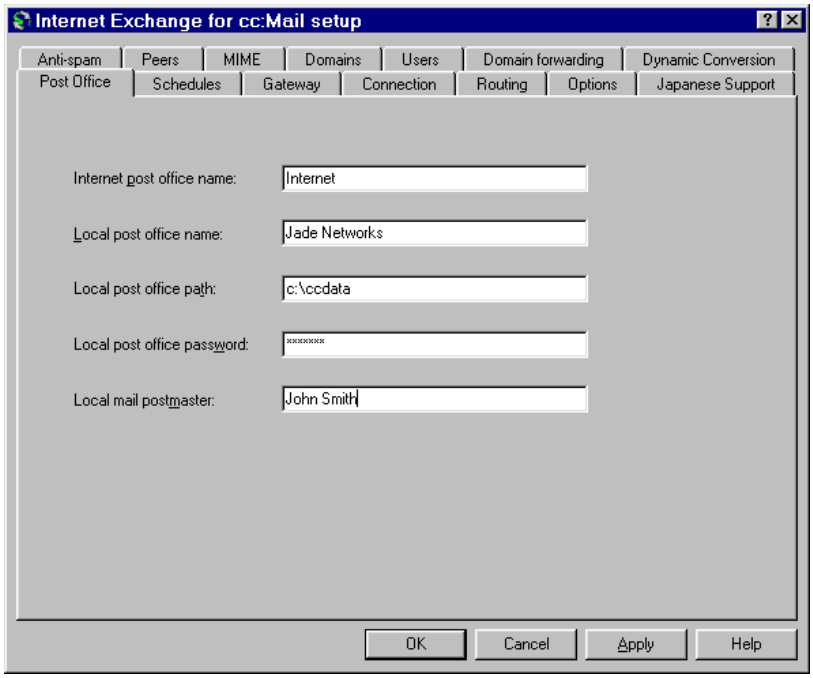
Users	Defines special cc:Mail or Notes username to Internet address mappings as well as forwarding incoming messages to one or more addresses.
Domain Forwarding	Configures forwarding of incoming messages to another domain.
Forms	Defines Lotus Notes form templates used for converting the Notes Form based message (internal format) into the appropriate Internet format. *(Notes Version)*
Dynamic Conversion	Allows automatic updating of alias and domain databases.

Additionally, the main *SYSMAN* window offers three utilities which can be configured by clicking the respective icon on the toolbar or via the *Run* pull-down menu.

Address Conversion Utility	Allows conversion of user alias information back and forth between the address file (in ASCII format) and the Alias Database.
Domain Conversion Utility	Allows conversion of domain address mapping information back and forth between the address file (in ASCII format) and the Domain Mapping Database.
Rules-based Address Generator	Configures the mappings of cc:Mail account names with corresponding Internet addresses. *(cc:Mail Version)*

CONFIGURE POST OFFICE *(CC:MAIL VERSION)*

This screen allows entry of the information required to permit **Internet Exchange** to communicate with the cc:Mail post office.



Internet Post Office Name

The name which **Internet Exchange** uses to log into the cc:Mail Post Office. This name must exist in the cc:Mail directory, and must be defined as a Post Office. Although any unique name may be used here, it is recommended that *Internet* be used for clarity. **Internet Exchange** uses this information to access the local cc:Mail Post Office.

Local Post Office Name

The name of the local cc:Mail Post Office. This will be the same as the name parameter given to the *chkstat* and *reclaim* programs for cc:Mail. **Internet Exchange** uses this information to resolve local email addresses.

Local Post Office Path

The path where the local cc:Mail Post Office resides. This will be the same as the path parameter given to the *chkstat* and *reclaim* programs for cc:Mail. **Internet Exchange** uses this information to access the local cc:Mail Post Office.

Local Post Office Password

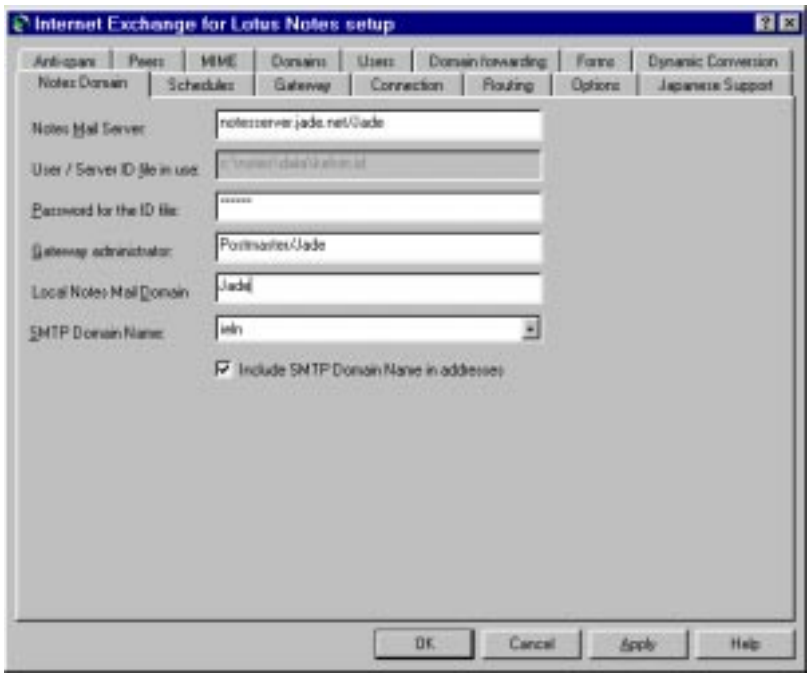
The password for the local cc:Mail Post Office. This will be the same as the password parameter given to the *chkstat* and *reclaim* programs for cc:Mail. **Internet Exchange** uses this information to access the local cc:Mail Post Office.

Local Mail Postmaster

The alias for the Internet Postmaster name. All Internet sites are required to support the Postmaster alias. When **Internet Exchange** receives a message addressed to Postmaster, it is sent to this cc:Mail user.

CONFIGURE LOTUS NOTES DOMAIN *(NOTES VERSION)*

This screen allows entry of the information required to permit **Internet Exchange** to communicate with the Lotus Notes domain.



Notes Mail Server

The name of the Notes Server to which the gateway is connected. This name consists of the Lotus Notes server's name and certifier name in the form:

servername/certifiername

This field is filled in automatically to match the values set up during your installation of Lotus Notes Server or Workstation installation.

User / Server ID file in use

This is the name of the ID file specified in the entry, *KeyFileName=* of the *NOTES.INI* file. **Internet Exchange** uses the owner of this ID file to access *SMTP.BOX* and *MAIL.BOX* in the Notes Server. Normally, this file is created in the data directory of Lotus Notes Server / Workstation during the installation process. If the *KeyFileName* does not contain any path information, **Internet Exchange** will automatically append the data directory specified in *NOTES.INI* under *Directory=* as the prefix.

e.g. *c:\notes\data\user.id* for standard Notes Workstation Installation

c:\notes\data\server.id for standard Notes Server Installation

This field is filled in automatically to match the values set up during your installation of Lotus Notes Server or Workstation installation.

Password for the ID file

This is the password for the User / Server ID file specified above. The password will appear as a row of asterisks (****) for security reasons. If no password has been set for the specified ID file, this field should be left blank.

Gateway administrator

This is the user name for the gateway administrator. By default, Internet Exchange for Lotus Notes will use the owner of the ID file specified above as the name of the gateway administrator. The gateway administrator is the user that is set up with manager access to *SMTP.BOX*, including document deletion permissions.

This is also the alias for the Internet Postmaster. All Internet sites are required to support the Postmaster alias. When Internet

Exchange receives a message addressed to Postmaster, it will be sent to this Notes user.

e.g. *postmaster/Corp.*

Local Notes Mail Domain

This is the local Notes Mail domain name to which the gateway should be connected. This Mail Domain name is generated during the first installation of the Notes Server.

e.g. *Jade*

SMTP Domain Name

This is the domain name defined in the Foreign SMTP Domain document of the Notes Public Address Book. Enter the domain name of the corresponding gateway; this permits multiple SMTP servers to run on a single Notes environment.

Include SMTP Domain Name in addresses

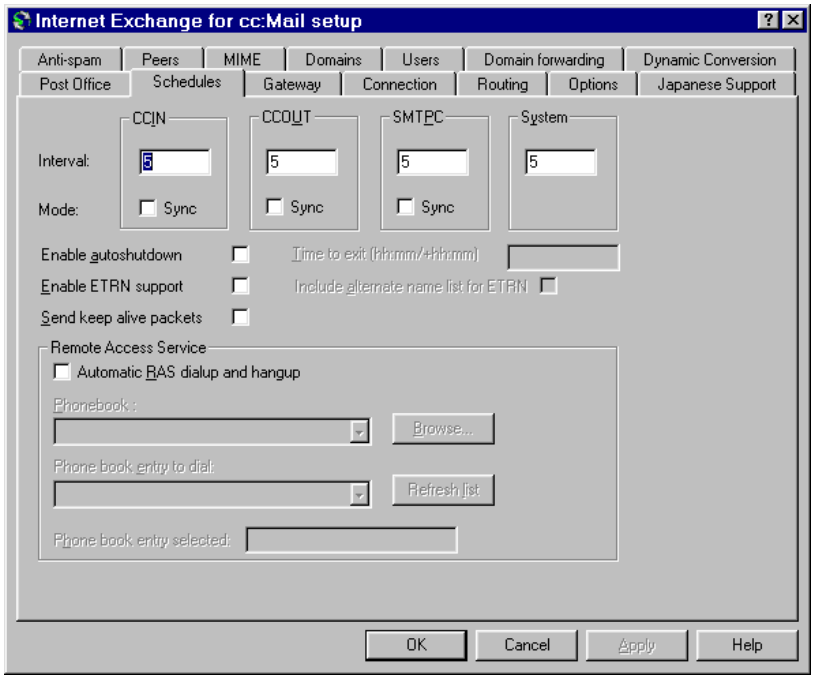
This enables the selected SMTP domain name to be appended to the Internet address of inbound messages. If the Notes environment contains more than one SMTP domain, replies to inbound messages are then forced through the **Internet Exchange** gateway. e.g.

user@iegate.jade.net becomes *user@iegate.jade.net @ ieln*

when this option is enabled.

CONFIGURE SCHEDULES

This screen allows entry of scheduling information for **Internet Exchange**:



Both versions of Internet Exchange are identical in appearance and functionality, with the exception that the Notes version controls the starting of *NOTESIN* and *NOTESOUT*.

CCIN / NOTESIN Interval

The interval for activating *CCIN / NOTESIN*, measured in minutes. *CCIN / NOTESIN* are the processes responsible for the transfer of messages from the *SMTP IN* queue into either cc:Mail or Lotus Notes.

CCOUT / NOTESOUT Interval

The interval for activating *CCOUT / NOTESOUT*, measured in minutes. *CCOUT / NOTESOUT* are the processes responsible for the transfer of messages out of either the cc:Mail post office or the Notes *SMTP.BOX* into the *SMTP OUT* queue.

SMTPC Interval

The interval for activating *SMTPC*, measured in minutes. *SMTPC* is the process responsible for the transfer of messages from the *SMTP OUT* queue to remote Internet hosts via SMTP.

System Interval

The interval for starting up system checking, measured in minutes. If auto-conversion is enabled, this time interval determines how often **Internet Exchange** checks the time stamps of *SMTP.ADR* and *SMTP.POD*. If changes have been effected to either of these files they are auto-converted to their corresponding databases (*SMTPADR.BTR* and *SMTPPOD.BTR*, used for user alias mapping and Post Office to Internet subdomain mapping, respectively). The default value is 5 minutes.

Sync Mode

Messages flow through **Internet Exchange** by way of the various different queue managers. For messages originating within either cc:Mail or Notes, these managers are *CCOUT / NOTESOUT* and *SMTPC*. For messages originating on the Internet side of Internet Exchange, the corresponding managers are *SMTPD* and either *CCIN* or *NOTESIN*. These queue managers operate independently of each other and are run by *SYSMAN* at regular intervals as outlined above.

Selecting the *Sync* checkbox for each of the above will cause the corresponding queue manager to be started as soon as a message is available. For instance, if the *CCIN / NOTESIN Sync* box is checked and a message is received by *SMTPD*, *CCIN / NOTESIN* will be started in order to deliver the message to cc:Mail or Notes. For most installations, it is recommended to run with sync mode selected for all queue managers.

Enable Autoshutdown

This option will enable an automatic shutdown of **Internet Exchange** at the given time (24 hour time format). When set, the gateway will shut down at the requested time.

A relative shutdown time can also be given, in the format of +hh:mm. This will shut the gateway down a defined number of hours and minutes from the time that *SYSMAN* was last started.

There is no maximum time limit for a scheduled gateway shutdown.

Enable ETRN Support

ETRN (RFC 1985 - SMTP service Extension for Remote Message Queue Starting) is an SMTP command issued by SMTPC when connecting to a remote SMTP server. This command, which includes the FQDN of the **Internet Exchange** gateway, requests that the remote SMTP server start processing its mail queues for messages there that are addressed to the gateway's FQDN. If any such messages are at the server, the server creates a new SMTP session and sends the messages at that time. This can be especially useful in a dialup environment where SMTP servers usually send mail only at specific intervals.

When *Include alternate name list for ETRN* is checked, SMTPC will also include entries defined in the alternate name list in addition to the gateway's FQDN when sending out ETRN commands to remote SMTP hosts. The SMTP server will immediately send any messages addressed to the gateway FQDN as well as the alternative domain names mentioned in the ETRN command.

The ETRN Support option is only useful when communicating with SMTP servers that support ETRN commands.

Send keep alive packets

For TCP connections that are made over a dialup connection (typically PPP or some ISDN connections) some TCP/IP stacks can be configured to time out and automatically disconnect after a predetermined period of no network activity. Under these

conditions, it is necessary for the gateway to keep the stack active if *SMTPD* is to continue to be able to receive incoming mail. If the *KeepAlive* option is enabled, *SMTPD* will send keepalive packets (a single UDP packet) to the discard port (9) of a remote host. The gateway will look for a DNS server, then conduct a sequential search for any host (other than the gateway itself) in the hosts file to send the keepalive packets to. The keepalives are sent at the rate of one packet approximately every 10 seconds.

Remote Access Services (RAS)

RAS is the Remote Access Service for Windows, actively supported on all WIN32 platforms. It is a useful feature not only for dial-up issues, but for any Windows-supported dial-up mechanism: these include direct leased lines to Windows systems, dial-up connections, ISDN connections, TAPI applications that comply to the RAS API (e.g. Video Conferencing Devices) and the WAN protocol X.25.

The RAS implementation is fully integrated into **Internet Exchange**, which means that use of dial-up is no longer exclusive to English Windows 95 and can be used on any language version of Windows 95, NT 3.5X and 4.0. Support for dial-up scripting and secure RAS is also included.

When *Automatic RAS dialup and hangup* is enabled, **Internet Exchange** will automatically start a RAS connection during gateway startup. Upon gateway termination, the RAS connection will terminate automatically.

Once RAS is enabled, Windows 95 Phonebook information can be entered. *Phonebook* allows specification of the phone book used by Internet Exchange for RAS connection. If Internet Exchange is running on Windows 95, the only possible entry is "System Phone Book". More than one phonebook can be chosen under Windows NT; use the *Browse* button to search through the file system for other phonebooks (files with the *.PBK* extension).

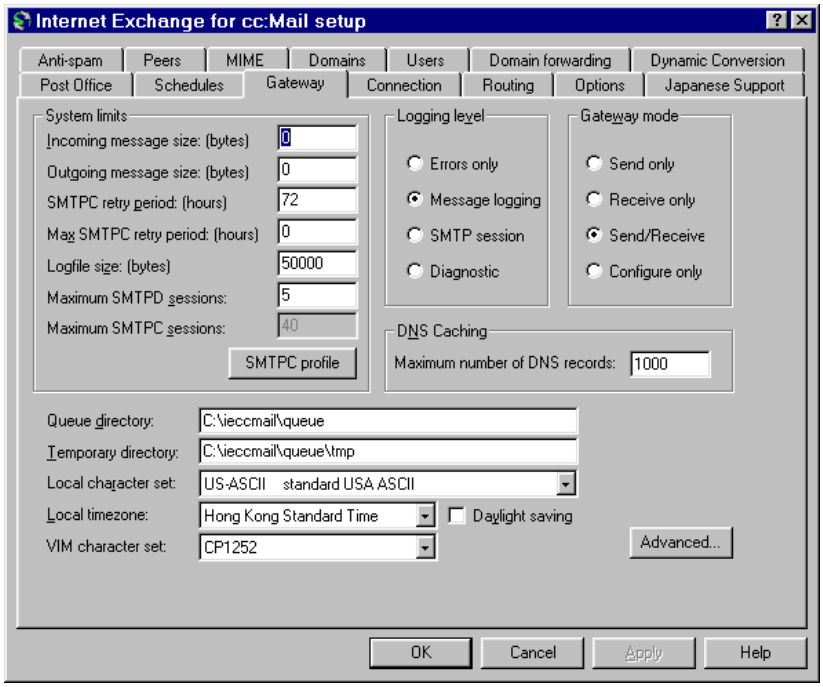
Phone book entry to dial allows the selection of the appropriate RAS profile name. Internet Exchange uses this name for making RAS connection during startup. The current entry selected in the

list is shown in the *Phone book entry selected* field. When running Windows NT, where more than one Phonebook can be selected, use the *Refresh* button after changing Phonebooks to refresh the list of Phonebook entries.

RAS is discussed in greater detail in *Chapter 14 - Remote Access Service.*

CONFIGURE GATEWAY

This screen allows entry of information related to the general operation of **Internet Exchange**.



System Limits

Incoming Message Size: (bytes)	The largest Internet message size in bytes that the gateway will accept. Setting this field to the default of zero will disable any limits on the size of incoming messages. This is a display only and the actual variable must be accessed in the *Peers Configuration* screen.

Outgoing Message Size: (bytes)	The largest cc:Mail message size in bytes that can be sent out. Setting this field to the default of zero will disable any limits for outgoing messages. This is a display only and the actual variable must be accessed in the *Peers Configuration* screen.
SMTPC Retry Period: (hours)	The number of hours that SMTPC tries to deliver a message before returning it to sender. If SMTPC cannot deliver a message, it waits for a minute before trying again. If unsuccessful after that, the delay doubles, until the retry time is reached. The default is 72 hours. (3 days). Setting this value to zero indicates the default time will be used.
Maximum SMTPC Retry Period: (hours)	The maximum number of hours before SMTPC attempts to deliver a delayed message. SMTPC uses an exponential backoff algorithm to avoid retrying a host too often. Each retry is attempted after a delay twice as long as the last delay. This parameter puts a limit on this delay, so that it does not get too large. The default is zero which indicates no maximum limit..
Logfile size:	The largest log file size allowed before the gateway saves it to another name and starts a new one. The default limit is 50,000 bytes which allows the Windows *notepad* application to read the file. Acceptable values that may be entered range between 10240 bytes (10 K) and 2000000000 bytes (roughly 2 G). A value of zero indicates that the default value.

Maximum SMTPD Sessions:	Some stacks have trouble when too many incoming SMTPD sessions are active. This parameter limits the number of incoming simultaneous sessions. The default is 15 and maximum is 256. A value of zero indicates the maximum will be used.
Maximum SMTPC Sessions:	Some stacks have trouble when too many outgoing SMTPC sessions are active. This parameter limits the number of outgoing simultaneous SMTP sessions. This value cannot be altered directly but is based on the configuration in *SMTPC profile*. The default is 15 and maximum is 120.

Logging Level

Internet Exchange offers four levels of debugging:

Errors Only	Only erroneous activity is logged.
Message Logging	Information about the delivery of all messages is logged.
SMTP Session	All SMTP conversations are logged.
Diagnostic	Logs the maximum level of information regarding gateway activity, including all details on core operations.

The logging levels are cumulative: e.g. at message logging level errors are also logged.

Gateway Mode

Internet Exchange can operate in either send mode, receive mode, send/receive mode, or configure only mode. Send/Receive mode is the normal method of operation. Configure only mode can be used to completely shut down all gateway operations while configuration takes place. While this

is not necessary, it may be desirable if gateway problems are identified. The radio buttons allow the gateway mode to be changed to any of these values.

DNS Caching

The *Maximum number of DNS records* entry records the maximum number of DNS records cached. The DNS cache greatly improves throughput of **Internet Exchange**, particularly when the DNS server(s) are not on a local LAN. The default is 1000, which balances increased throughput against greater disk space used for the cache.

Queue Directory

Internet Exchange stores messages in this directory. The log file is stored as *IECCMAIL.LOG* (*IENOTES.LOG* for the Notes Version). The queue subdirectories are:

in:	messages coming in from the Internet.
out:	messages waiting to be delivered to the Internet.
bad:	directory for any malformed messages. These are occasionally created if an SMTP session does not finish cleanly.
spam:	spam messages identified and caught (if Anti-Spam is enabled).

The default is *c:\ieccmail\queue* for the cc:Mail Version and *c:\ienotes\queue* for the Notes Version.

Gateway Temporary Directory

This is the directory in which **Internet Exchange** stores temporary files. Usually it is a subdirectory of the queue directory. It can be set to a different directory or drive depending upon local disk availability. The default is *c:\ieccmail\queue\tmp* for the cc:Mail Version, and *c:\ienotes\queue\tmp* for the Notes Version.

Local Character Set

The ISO character set to be used. Those in most Anglo Saxon countries can select US-ASCII, while others will prefer to choose

a different character set. For Japanese users, ISO-2022-JP should be used. All outgoing email will be tagged as using the selected character set.

VIM Character Set *(cc:Mail Version)*

Select from the list of character sets to be used to login to the cc:Mail Post Office. By default, only CP1252 is available. If **Internet Exchange** detects that the Japanese VIM interface is being used, CP932 can also be selected from the list.

Local time zone

This is the time zone in which the local machine resides. Whether this time zone uses daylight saving or not should be specified in the *Daylight saving* checkbox. There are many locations configured in the system, including the USA, much of Europe, and Asia. If the local time zone is not listed, then it will have to be entered manually into *IMA.INI/IELN.INI* with an editor as follows:

[Gateway]
Timezone=*tzn*[+ | -]*hh*[:*mm*[:*ss*]] [*dzn*]

The *tzn* must be a three-letter time-zone name, such as PST, followed by an optionally signed number, *hh,* giving the difference in hours between UCT and local time. To specify the exact local time, the hours can be followed by minutes, *:mm*; seconds, *:ss*; and a three-letter daylight-saving-time zone, *dzn*, such as PDT. Hours, minutes, and seconds should be separated by colons (:). If daylight saving time is never in effect, as is the case in certain states and localities, set *Timezone* without a value, for *dzn.* If the *Timezone* value is not currently set, the default is PST8PDT, which corresponds to the Pacific time zone of the USA.

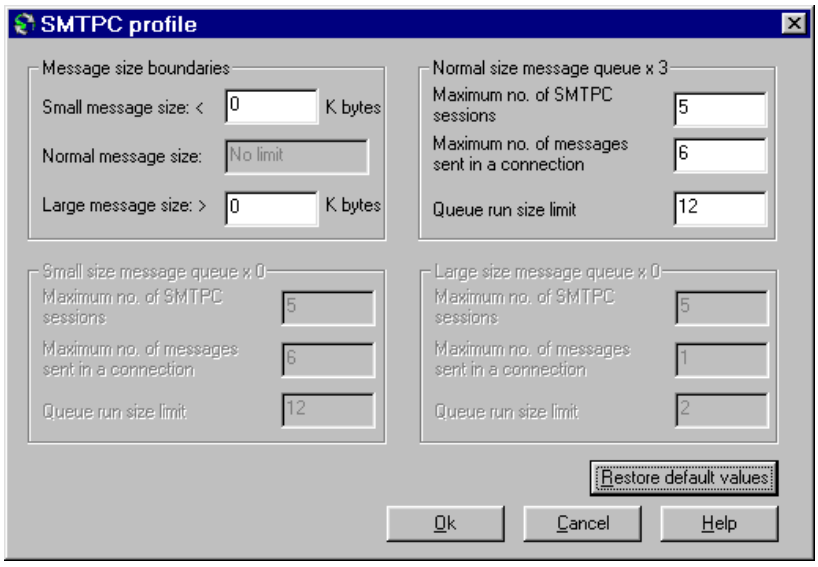
If the time zone "Use system TZ variable" is selected, the timezone information will be obtained from the user defined TZ environment variable. Under Windows 95, this can be set in the *AUTOEXEC.BAT* system startup file. Under Windows NT it is usually set in the system registry. In either case, the machine must be rebooted in order to make the change effective.

Daylight saving

This field is set to indicate whether the local time zone uses daylight saving in the summer.

SMTPC Profile

The SMTP client program *SMTPC* is responsible for the delivery of messages to the Internet. It checks the *SMTP OUT* queue for messages and, if any are found, it establishes one or more connections with external SMTP servers in order to transfer the messages to the appropriate Internet mail hosts.



SMTPC supports three queue processors that are capable of producing different profiles depending on their configurations: three identical and independent queue processors are created to process messages of any size, and there are no defined size boundaries by default. When the small and large size boundaries are defined, *SMTPC* creates three different queue processors: one to process small messages, one to process large messages, and one to process normal messages, which are defined as having a range of sizes greater than or equal to the "small" boundary but less than or equal to the "large" boundaries. The processing of any one range of messages is therefore independent of the other two.

Small message size boundary

This value marks the boundary (measured in Kilobytes) between small and normal messages. Any message of size lower than the value specified is considered small. If this value is set to -1 the small message queue processor is not created. If the value defined is greater than 0 a queue processor for messages between 0 and the specified value is created. The default value is 0, which means that a queue processor is created and not assigned to a specific "small" range, but reserved for messages of normal size range.

Normal message size boundary

This value is derived from information entered into the other two message size boundaries and cannot be altered directly.

Large message size boundary

This value marks the boundary (measured in Kilobytes) between large and normal messages. Any message of size larger than the value specified is considered large. If this value is set to -1 the large message queue processor is not created. If the value defined is greater than 0 a queue processor for messages of size greater than the specified value is created. The default value is 0, which means that a queue processor is created and not assigned to a specific "large" range, but reserved for messages of normal size range.

The profiles of each of the queue processors can be tuned individually by using respective sets of three options:

Maximum number of SMTPC sessions

This integer specifies the highest number of concurrent outbound SMTP connections allowed per queue processor. Utilized system resources increase as this limit is raised, and overall gateway performance may be affected, along with the performance of any other applications running on the same machine. It is, however, useful to raise the limit when there are outbound messages that comprise a large variety of destination domains, as more simultaneous SMTP connections are established and the queue is processed more rapidly. The default value is 5, and the maximum is 40 (per queue processor).

Maximum number of messages sent in a connection

Specifies the highest number of messages that can be sent using a single SMTP connection. When this number is increased, more messages can be sent to a remote SMTP server on each connection; because the total number of SMTP connections required actually decreases as this limit is increased, the drain on system resources is kept to a relative minimum. Note that this is only the case if the majority of queued messages share common domains as destinations; it is more efficient to process several outbound messages through the same SMTP connection rather than establishing a separate connection for each message. Altering this value generally has no significant effect (please see below for exceptions and particulars) if the destinations of outbound messages include a wide variety of domains. The default is 6 and the maximum is 40. For the large message size queue processor the default is 1.

NOTE: Altering this value *does* have an effect when a queue processor is configured to handle messages of large size. In this case the default is 1 (one message per SMTP connection) because this forces new SMTP connections to be opened rather than sending large messages sequentially through one connection, thus alleviating accumulation and backup of outbound mail.

Queue run size limit

Specifies the maximum number of messages that can be processed in each queue run. Setting a high value for this option increases gateway performance significantly, but may be detrimental to system resources. The default is 12 and the maximum is 40. For the large message size queue processor the default is 2.

NOTE: When configuring a queue processor for large messages, reducing the number of messages to be processed at each queue run generally results in significant savings of system resources, thus improving overall gateway performance.

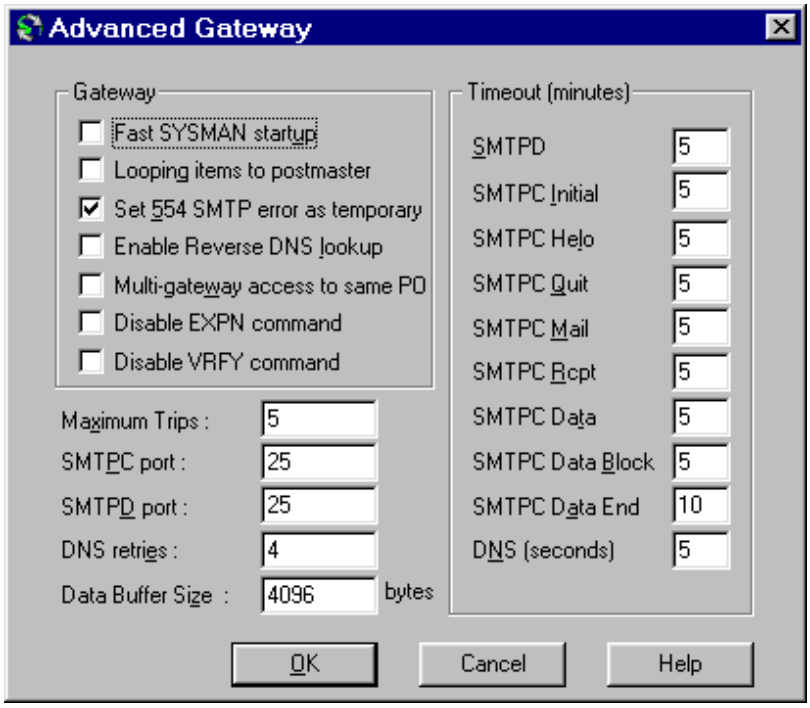
Restore default values

All default values for the options displayed are restored by the use of this button. Press OK to save the changes.

It is important to note that changing the settings of *SMTPC* profiles will affect the general performance of the gateway. The default values are intended for standard gateway usage; adjustments to these values should take into account variables such as quantity, number of recipients and size of messages.

Advanced

This dialog box allows many of the advanced gateway parameters to be changed. Normally the default values will work perfectly well, and should not be changed without full understanding of the consequences.



There are several functions that are controlled within the gateway section. They are:

Fast SYSMAN startup

If a problem with the network arises, a large queue of messages can build up in the cc:Mail Post Office or Notes *SMTP.BOX*. In that case gateway startup will be very slow. By setting this variable, the queue counter update does not occur until either a key has been pressed or the mouse has been moved. The queue messages display is not updated until the next time a key is

pressed or the mouse is moved. This greatly increases the speed of gateway startup. This option should be set if running unattended dialup PPP. The default is *NO*.

Looping items to postmaster

If set, any looping messages are routed to the local postmaster instead of being returned to the remote sender. This is often useful to stop infinite email loops from occurring. The default is *NO*.

Set 554 SMTP error as temporary

RFC821 on SMTP is not clear as to whether the error *554 transaction failed* during the DATA phase should be regarded as a permanent error. Usually 5xx errors are permanent, but some SMTP servers return 554 errors for temporary errors. **Internet Exchange** takes the conservative approach and retries such messages later. If this option is set to *NO*, then such messages will be bounced instead of retried. The default is *YES*.

Enable reverse DNS lookup

This is a security feature. When a remote host issues a HELO command, *SMTPD* has the capability to perform a reverse DNS query in order to verify whether the name that the remote host has issued as its own matches its DNS hostname. If the two do not match a warning response is issued to the peer and the event (along with the real hostname) is logged.

Multi-gateway access to same PO *(cc:Mail Version)*

Checking this option guarantees that no multiple copies of the same outbound message are sent when multiple gateways share the same Post Office. When one gateway processes an outbound (cc:Mail to Internet) message, exclusive mail message locking is performed on the message (in the common Post Office) in order to restrict other gateways' access to the same message at the same time; the other gateways will export the next messages in line instead.

Disable EXPN command *(cc:Mail Version)*

For security reasons, the "EXPN" (expand mailing list) command is sometimes considered too intrusive: a remote host may confirm whether a certain mailing list exists in a certain post office. Disabling the "EXPN" command causes *SMTPD* to respond with "550 command disabled" when a remote SMTP client issues this command.

Disable VRFY command *(cc:Mail Version)*

For security reasons, the "VRFY" (verify user) command is sometimes considered too intrusive: a remote host may confirm whether a particular user exists in a certain post office. Disabling the "VRFY" command causes *SMTPD* to respond with "252 command disabled" when a remote SMTP client issues this command.

Timeouts

There are a large number of timeout values that can be altered if needed. The defaults (normally 5 minutes) are usually adequate, and should be changed only if Internet Exchange is experiencing a lot of timeouts. The variable timeouts are:

SMTPD	how long *SMTPD* waits on an open socket during an SMTP session.
SMTPC Initial	how long *SMTPC* waits for a reply when starting a new session.
SMTPC Helo	how long *SMTPC* waits for the remote system to respond to the HELO command.
SMTPC Mail	how long *SMTPC* waits for the remote system to respond to the MAIL command.
SMTPC Rcpt	how long *SMTPC* waits for the remote system to respond to the RCPT command.
SMTPC Data	how long *SMTPC* waits for the remote system to respond to the DATA command.

SMTPC Data Block	how long *SMTPC* waits for the remote system to acknowledge each block of data sent.
SMTPC Data End	how long *SMTPC* waits for the remote system to respond to the dot (.) command after all the data has been sent.
SMTPC Quit	how long *SMTPC* waits for the remote system to respond to the QUIT command.
DNS	how long to wait before a DNS request times out (default is 5 seconds).

Maximum Trips

Specifies the maximum number of Received lines allowed in an incoming message that show the FQDN of the gateway machine. Only lines containing the gateway's FQDN are counted. If this number is exceeded, the message is bounced. This option is useful in preventing message loops. The default is 5.

SMTPC port

Specifies the port which SMTPC uses, and can be useful when running the gateway behind a firewall or any other non-standard setup. The default is 25.

SMTPD port

Specifies the port which SMTPD uses, and can be useful when running the gateway behind a firewall, or any other non standard setup. The default is 25.

DNS retries

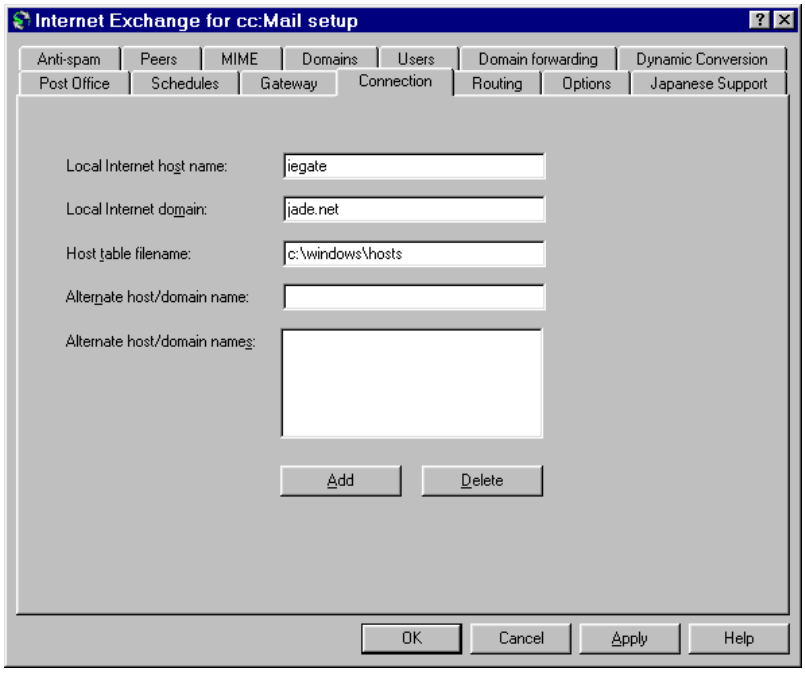
Specifies the number of times a DNS query is retried after a timeout. DNS retries utilize an exponential back-off timer to vary the period between retries. The default is 4.

Data Buffer Size

This is the size, in bytes, of the data buffer used by the SMTP programs to read data from the Internet. If the gateway machine uses disk caching, set this option to the size of the read ahead buffer. The default value is 4096 (4K); the maximum limit is 32768 (32 K).

CONFIGURE CONNECTION

This screen allows the entry of connection and alternate host / domain name information for **Internet Exchange**:



Local Internet Hostname

This field records the Internet hostname of the gateway machine. In the above example, if the FQDN for the gateway machine is *iegate.jade.net*, the Local Internet Hostname would be *iegate.*

Local Internet Domain

This field records the Internet domain of the gateway machine. In the above example, if the FQDN for the gateway is *iegate.jade.net,* the Local Internet Domain would be *jade.net.*

Host Table Filename

This field records the location of the Internet host table for address resolution. Even if the DNS is used for name resolution, it is necessary to configure a host table that contains at least the name and address for the gateway machine as well as for the default mail relay host. This will allow **Internet Exchange** to send mail to the default mail relay host for further routing in the event problems communicating with the name server(s) occur.

The default configured into **Internet Exchange** is *c:\ieccmail\hosts* (*c:\ienotes\hosts* for the Notes Version). For Windows 95 this value should be set to *c:\windows\hosts* while for Windows NT it should be set to

c:\windows\system32\drivers\etc\hosts

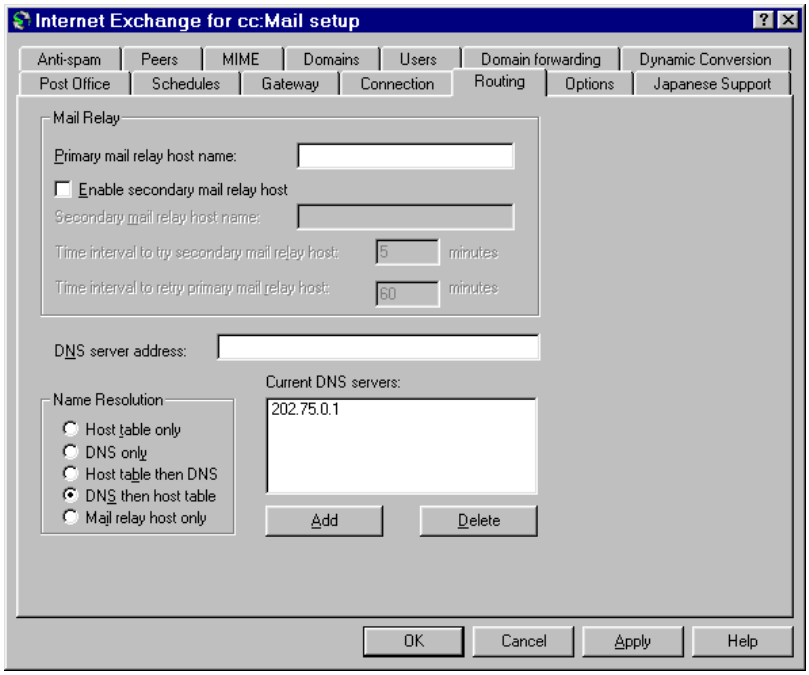
if using the default locations (where c:\windows is the topmost directory in the Windows system).

Alternate Host/Domain Name

Sometimes it is desirable for a gateway machine to be known by more than one fully qualified domain name. This field is used to add additional names by which the gateway host is known. This list of alternate names contains entries that can be added to or deleted by using the appropriate buttons. All messages addressed to users at hosts identified in this list will be considered local when received by the gateway and will be sent to cc:Mail or Notes.

CONFIGURE ROUTING

This screen allows entry of routing information for **Internet Exchange**:



Primary mail relay host name

If *SMTPC* is unable to resolve a hostname by either DNS or host table lookup, it routes messages to this host for forwarding. This option is also used if routing is configured to mail relay host only.

Enable secondary mail relay host

If this checkbox is checked, a secondary mail relay host can be configured for use when the primary mail relay host is unavailable.

Secondary mail relay host name

If the primary mail relay host is down, then the gateway routes messages to this host instead.

Time interval to try secondary mail relay host

Number of minutes of unavailability after which the primary mail relay is considered offline and the secondary, if enabled, is attempted.

Time interval to retry primary mail relay host

The number of minutes before the gateway attempts to revert to the primary mail relay host once the latter has been confirmed unavailable.

DNS Server Address

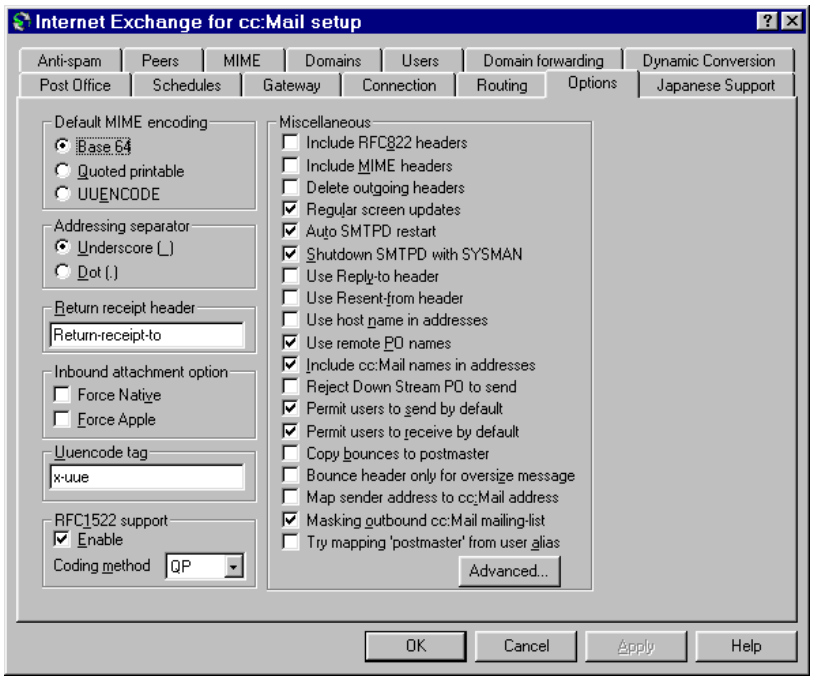
SMTPC will try contacting the list of configured DNS servers. Each address must be of the form a.b.c.d, where each number is between 0 and 255. (See Appendix E on TCP / IP for a discussion of IP addressing.)

Name Resolution

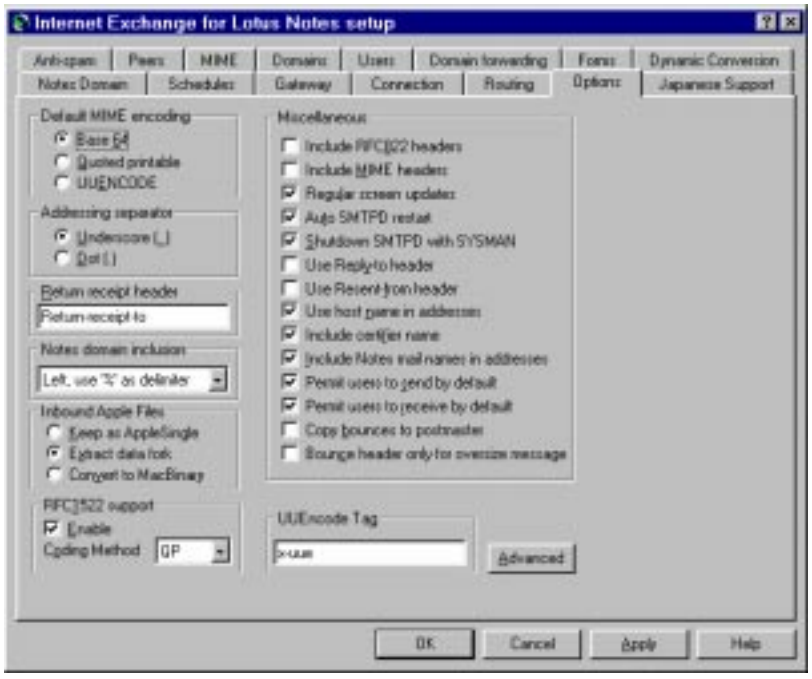
Any combination of DNS or host table lookup can be used, in any order. Where "mail relay host only" routing is not used, it is recommended that DNS be used if at all possible, as this usually results in the most reliable routing and greatest throughput.

CONFIGURE OPTIONS

This screen allows entry of various options for **Internet Exchange**. The following shows the default values for the cc:Mail and Notes versions:



Configure Options: Internet Exchange for cc:Mail



Configure Options: Internet Exchange for Notes

Default MIME Encoding

When encoding cc:Mail or Notes messages, *CCOUT / NOTESOUT* uses the MIME encoding information configured into **Internet Exchange** (see the section on MIME for details). When a non- Macintosh file with an unknown extension is encountered, it is encoded using the default binary encoding. Choose the appropriate radio button based upon the capabilities of those sites with which you communicate most. Base64 is preferable for communicating with MIME-capable sites. UUENCODE should be specified as the default if you intend on communicating with many sites that are not MIME-compliant. However, as UUENCODE/UUDECODE are not part of the MIME specification their widespread use is discouraged.

Addressing Separator

When constructing Internet addresses for cc:Mail or Notes users without an explicit entry in the *SMTP.ADR* file, all spaces are usually converted to underscores (spaces are not valid in Internet mail addresses). Some sites prefer to use dots instead of underscores—this option allows to choose between the two.

Return Receipt Header

This parameter specifies the value of the Internet Return Receipt header. Using the default value of *Return-Receipt-To:* allows compatibility with the UNIX *Sendmail* program and various other MTA's found on the Internet. There are however problems involved with this approach. S*endmail* uses the header to request notification of message delivery at the transport level, while some other products (SMTPLINK from Lotus is one example) uses it to signify that the message has been opened (and possibly read) by the recipient.

Choosing a different value will sidestep this problem, but will also ensure that the return receipt function is portable only between IMA gateways that settle upon the same value to use.

Lotus Notes domain inclusion *(Notes Version)*

User mapping and Domain mapping provide no means to indicate Lotus Notes Domain information. This option allows the preservation of such information.

The special character '@' is used in Notes environments to specify Notes domain. However, this special character '@' has different meaning in Internet addresses. There are three built-in methods in Internet Exchange to handle the Notes domain : NONE, LEFT (uses "%" as the delimiter) and RIGHT (uses "." as the delimiter).

e.g. *John Smith/Sales/Jade @ Sales @ Jade*
(Notes mail address)

will become

John_Smith/Sales/Jade@jade.net
(NONE)

or

John_Smith/Sales/Jade%Sales@jade.net (LEFT)

or

John_Smith/Sales/Jade@sales.jade.net
(RIGHT)

Inbound attachment option - Force Native *(cc:Mail Version)*

By checking this option, inbound Macintosh attachments (in BinHex, MacMIME or uuencoded AppleSingle format) are stripped of their header and (if present) resource fork before being attached to messages in the cc:Mail Post Office. If this is not done, some applications may refuse to open the resulting file. See *Appendix B* for a more detailed discussion of this issue.

Inbound attachment option - Force Apple *(cc:Mail Version)*

By checking this option, inbound non-Macintosh attachments are given a dummy header and converted into AppleSingle cc:Mail attachments before being attached to messages in the cc:Mail Post Office. The type and creator are obtained from the MIME table prepared with the *Configure MIME* dialogue box. See *Appendix B* for a more detailed discussion of this issue.

Uuencode tag

Internet Exchange generates an “x-uue” tag in the content-transfer-encoding header by default when an outbound MIME uuencoded message is processed, but some electronic mail agents require the tag “x-uuencode” in the message header. This entry field is used to change the tag name. Both “x-uue” as well as “x-uuencode” are automatically recognized on all messages received by **Internet Exchange**.

Inbound Apple files - Keep as AppleSingle *(Notes Version)*

By checking this option, inbound Macintosh attachments will be kept in AppleSingle format after decoding. Attachments received by Lotus Notes may require a third part application in order to correctly convert the attached file to the native system format before viewing. For example, if the attachment is an Adobe Acrobat file, no third party application is required because the Adobe Acrobat Viewer for Microsoft Windows can automatically understand the file in AppleSingle format. This option is best checked if the Lotus Notes environment is comprised of a mixed environment of Macintosh users and non-Macintosh users. See *Appendix B - Apple Macintosh File Structure* for a more detailed discussion of this issue.

Inbound Apple files - Extract data fork *(Notes Version)*

By checking this option, only the data fork of the Macintosh attachment will be used after decoding. The Macintosh resource fork associated with the attachment will be stripped from the file, thus guaranteeing that the attachment will be viewed correctly using any non-Macintosh Lotus Notes client. This option is best checked if the Lotus Notes environment is comprised of non-Macintosh users. See *Appendix B - Apple Macintosh File Structure* for a more detailed discussion of this issue.

Inbound Apple files - Convert to MacBinary *(Notes Version)*

By checking this option, the decoded MAC MIME attachment will be converted to MacBinary II format before importing to the Notes server. This will guarantee that the attachment will be viewed correctly under the Lotus Notes client for Macintosh. This option is best checked if the Lotus Notes environment is comprised of Macintosh users. See *Appendix B - Apple Macintosh File Structure* for a more detailed discussion of this issue.

RFC1522 Support

When this is enabled, *CCOUT / NOTESOUT* encodes any message header that contains non-ASCII characters according to the definition of RFC 1522 (MIME part II, Message Header Extensions for Non-ASCII Text).

RFC1522 Support—Coding method

It is possible to choose between Quoted-Printable and Base64 as methods for encoding non-ASCII characters in message headers. If the gateway is generating mainly European characters it is recommended to use Quoted-Printable, while Base64 is suggested for Japanese or any double-byte character-set environment.

Include RFC822 Headers

In normal operation, **Internet Exchange** discards RFC822 headers after messages have been imported into either cc:Mail or Notes. This option allows all such headers to be retained in messages as separate attachments.

Include MIME Headers

In normal operation, **Internet Exchange** discards MIME bodypart headers after they have been processed. This option allows all such headers to be retained in messages as separate attachments.

Delete Outgoing Headers *(cc:Mail Version)*

When a MIME message is imported into cc:Mail, and either RFC822 and / or MIME headers are included, extra text items are created containing these headers. When such messages are resent out to the Internet, these text items are not useful and often confuse the recipient. Setting this option automatically deletes these header attachments from outgoing messages.

Regular Screen Updates

Screen updates occur at regular intervals (once per minute) during normal gateway operations. If one or more of the mail queues grows very large, *Regular Screen Updates* should be turned off. Otherwise the system will spend too much time re-reading and re-displaying the queues.

Auto SMTPD Restart

This allows *SYSMAN* to automatically restart the SMTP daemon if and when it exits. The default is on.

Shutdown SMTPD With SYSMAN

If set, this will shut down the SMTP daemon when the *SYSMAN* program is exited.

Use Reply-To Header

This option makes use of the *Reply-to:* field by copying it to the *From:* field on all incoming mail. Otherwise this information is lost, as neither cc:Mail or Notes have any concept of *Reply-to:* fields. Use of this option will result in the loss of the original *From* field, if this field is different from the *Reply-to* field.

Use Resent-from header

In the versions of **Internet Exchange** prior to 2.0, if a *Resent-From:* header was present on the incoming message, it was used for the cc:Mail / Notes *From* field instead of the *From:* header. This option allows this behavior to be turned on or off as needed. Use of this option will result in the loss of the original *From* field, if this field is different from the *Resent-from* field.

Use Hostname In Address

This option determines whether the local hostname is included in Internet addresses for cc:Mail users. As an example, the user John Smith might appear to the outside world as *John_Smith@iegate.jade.net* with this option set, and as *John_Smith@jade.net* with the option not set.

Additionally, the local domain should be added to the *Alternate host name/domain* list in the *Connection* configuration window. This ensures that incoming mail of this form is recognized as local. All MX records for this domain should be forwarded to Internet Exchange.

Use Remote PO Names *(cc:Mail Version)*

Using default address mapping, a message from a user at a remote Post Office of "Sales" will appear to be sent from a user in the following form:

John_Smith_at_Sales@iegate.jade.net

This is not attractive. By disabling this parameter, the message will appear to come from:

John_Smith@iegate.jade.net

which is much more presentable. To ensure that replies to this message will be returned to the sender, there must be an entry in the gateway Post Office for the user. This can most easily be accomplished by using Lotus ADE (Automatic Directory Exchange).

Include cc:Mail names in Addresses *(cc:Mail Version)*

Turning this option off removes the cc:Mail user name from Address field leaving only the user's Internet address. The default is *on*.

Reject Down Stream PO to send *(cc:Mail Version)*

Setting this option will disable users from downstream post offices to send messages to the Internet. Thus, only users from the local post office can send messages to Internet.

Include certifier name *(Notes Version)*

If there is no address mapping for outbound Notes addresses found in the alias database, default mapping will be used. If the certifier name is not required for the Internet address, this option should be turned off.

e.g. certifer name included: *John_Smith/Sales/Jade@jade.net*

certifier name not included: *John_Smith@jade.net*

Include Lotus Notes names in addresses *(Notes Version)*

Checking this option will include the Lotus Notes names in the comment part of outgoing Internet addresses.

e.g. names included: *Jonathan_Smith@jade.net (Jonathan Smith)*

names not included: *Jonathan_Smith@jade.net*

Permit users to send by default

If send permission is not set for a user in the alias database and directory database, this option determines whether the user can send messages to the Internet.

NOTE: Internet Exchange Workgroup Edition does not permit the configuration of this parameter, and the default is *NO*.

Permit users to receive by default

If receive permission is not set for a user in the alias database and directory database, this option determines whether the user can receive messages from the Internet.

NOTE: Internet Exchange Workgroup Edition does not allow for the configuration of this parameter, and the default is *NO*.

IMPORTANT: When the default permission to receive is set to "NO", Internet addresses can only be converted into a corresponding cc:Mail or Lotus Notes user names if a corresponding entry is present in either the Alias or the Rules-Based databases (in the case of the cc:Mail Version). This implies that some cc:Mail or Notes users that are mentioned as recipients (either "To:", or "Cc:") on outgoing messages may not have any associated valid Internet address. By default, they are not considered for conversion while building the recipient headers of the resulting Internet message. In order to enable **Internet**

Exchange to generate references to these users, the following variable should be changed in the *IMA.INI/IELN.INI* file:

[Options]
IncludeNonRepliableAddresses=YES

By setting this option to *YES*, the default mapping will be used anyway for giving visibility over the original list of recipients. Any attempt to reply from the Internet side without editing out the unrepliable addresses will result in bounces (without affecting the delivery to the repliable ones).

Copy Bounces To Postmaster

Setting this option directs all bounced messages to the local postmaster, as well as the original sender of the message.

Bounce header only for oversized message

Setting this option causes inbound and outbound messages in excess of the maximum size limit to be stripped of their bodies and bounced back to their senders as headers only.

Map sender address to cc:Mail address *(cc:Mail Version)*

Setting this option causes **Internet Exchange** to attempt to map a sender's Internet address to a valid cc:Mail user address; if a match is found *CCIN* replaces the Internet address in the "From:" header with the corresponding cc:Mail user name.

Masking outbound cc:Mail mailing list *(cc:Mail Version)*

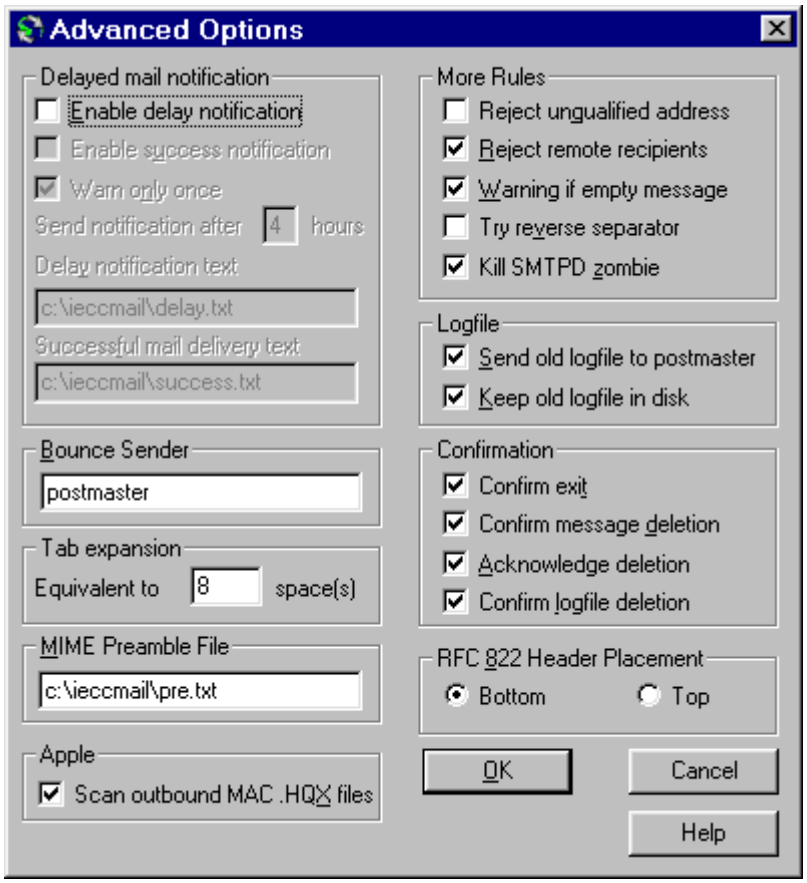
If this option is set *CCOUT* will ignore any mailing list entries when generating message headers. This means that if a message is addressed to a mailing list and to addresses external to the mailing list, only the mailing list recipients will be able to see the entire list of recipients, while the external addressees will not receive indication that the message was also sent to a cc:Mail mailing list. It is also useful to avoid duplicate replies being sent to the same cc:Mail recipient/s if that recipient is also addressed in the cc:Mail mailing list.

Try mapping 'postmaster' from user alias *(cc:Mail Version)*

Messages addressed to the Postmaster are sent by default to the "local mail postmaster", defined in the Post Office setup screen; the "Internet address" field for the prospective postmaster in the Users setup screen must be set as "postmaster". Enabling this option allows users to map "postmaster" to another user; if no valid entry can be mapped from the user aliases, **Internet Exchange** uses the local mail postmaster name for mail delivery.

Advanced Options

A set of advanced options can be accessed through the *Advanced* button:



The *Delayed mail notification* section allows the setting of many options related to handling messages that cannot be delivered on the first attempt:

Enable delay notification

With this option activated, **Internet Exchange** warns the sender if a message cannot be delivered for a period of time. This time is defined by the *Send notification after ... hours* option described below.

Enable success notification

If this option is set, **Internet Exchange** notifies the sender when a delayed message has been successfully sent.

Warn only once

If this option is set, the gateway does not send additional notifications for repeated delays of the same message. Otherwise, delay notifications are sent regularly until the message is successfully delivered.

Send notification after ... hours

Defines the threshold of what should be considered delayed delivery.

Delay notification text

The pathname of the file containing the message to be used to notify of a delayed message delivery. If no file name is specified or no file is found at the specified path, the following default warning message text is used:

> The Internet Exchange gateway (localhost.domain) has come across problems delivering to the following Internet recipient(s): recip1, recip2. This mail message has been delayed for *n* hours. The gateway will continue to retry the message and may send it back if it cannot be eventually delivered.

Successful mail delivery text

The pathname of the file containing the message that will be sent to postmaster when the gateway eventually delivers a delayed message. If none is specified or if no file is found at that path, the following default message text will be sent:

> The Internet Exchange gateway (localhost.domain) has successfully delivered your delayed message to the Internet recipient(s): recip1, recip2, ...

Bounce Sender

When messages are bounced, the user defined in this field receives notification, generated by the **Internet Exchange** MTA, to warn of undelivered mail. A copy of the message is included in the notification. The default is postmaster (highly recommended).

Tab expansion

The number of spaces used to replace tab characters in incoming text messages. If set to zero, tabs will not be replaced. As some clients have trouble displaying tab characters, this option allows them to be replaced by spaces.

MIME Preamble File

MIME multipart messages contain an initial section known as the preamble, where a short optional text useful to non-MIME gateways and user agents can be stored. This section resides between the RFC822 headers and the first MIME body part. If this option identifies an existing file, the contents of this file are used as the preamble in outgoing messages. If set to a nonexistent file, no preamble is used. If not set, no preamble is used.

Scan outbound MACINTOSH .HQX files *(cc:Mail Version)*

In outgoing messages, checks whether the message body contains files in BinHex format and, if found, uses the information in the header to prepare the proper MIME headers.

Reject Unqualified Addresses

When this is set *SMTPD* checks recipient and sender addresses for a proper domain part, refusing to receive messages where it is absent. e.g. *user@host.com* is accepted but *user* is rejected. This option can be useful in encouraging users to always use FQDNs when sending mail to the Internet.

Reject Remote Recipients

When this is set *SMTPD* rejects incoming messages for remote Internet recipients. This is to prevent remote sites from trying to spoof messages by rerouting them through the gateway back out to the Internet.

Warning if empty message

This causes empty outbound messages to trigger a warning to the local postmaster. The warning text is:

> *Warning: your message went out the [cc:Mail / Lotus Notes] gateway with an empty message body.*
>
> *If you intentionally sent an empty message, disregard this warning. If you included a reply in an old header body part, it was purged.*
>
> *Key headers from the message that was sent follow*.

Try reverse separator

This causes both address separators (dot / underscore) to be tried with incoming addresses during default address translation. This can be useful if the local site changes its preferred separator and still wishes addresses with the old separator to be valid.

Kill SMTPD zombie

When this option is set, *SMTPD* checks the value of the SMTPDmainSocket option in the config section of *IMA.INI/IELN.INI* upon startup. If this is *not* set to NONE, the number indicates the main socket used by *SMTPD* when it last shut down prematurely shut down prematurely. An attempt to close this socket is performed, so that *SMTPD* does not get an *address already in use* error when restarted.

Send old logfile to postmaster

If checked, all old logfiles are automatically mailed to the postmaster.

Keep old logfile on disk

If checked, prevents the deletion of old log files.

Confirm exit

Setting this option results in the gateway asking for confirmation before a manual shutdown.

Confirm message deletion

If checked the gateway asks for confirmation before deleting a message.

Acknowledge deletion

Setting this option results in the gateway presenting acknowledgment after successfully deleting a message.

Confirm logfile deletion

Setting this option results in the gateway asking for confirmation before deleting the log file.

RFC 822 Header Placement *(cc:Mail Version)*

Controls where the RFC822 headers will be attached from an incoming message, i.e. before the first attachment or after the last.

JAPANESE SUPPORT

From version 2.03beta3 onwards, Internet Exchange for cc:Mail includes Japanese language support.

Operating System Requirements

In order to run Internet Exchange with Japanese language support a Japanese operating system (Windows 95, NT 3.51 or 4.0) is required in conjunction with a Japanese post office (DB6 or DB8) in the case of cc:Mail, or a Japanese Lotus Notes client or server in the case of Notes.

Japanese Character Set Standards

There are three basic Japanese encoding methods: JIS, Shifted-JIS and EUC. JIS encoding is typically used for electronic transmission, Shifted-JIS encoding is used on MS-DOS based machines, and EUC encoding on UNIX-based machines. Therefore, **Internet Exchange** only needs to support the conversion between JIS and Shifted-JIS.

The standard for JIS encoding is known as ISO-2022-JP and handles several types of character sets. For text that contains embedded Japanese characters, the encoding of the Japanese characters will start through a special escape sequence upon detection of the first Japanese character. To switch back to ASCII, another escape sequence is used again to signal the end of the sequence of Japanese characters. The following table shows the escape sequences and the corresponding character sets.

Escape Sequence	**Character Set**
ESC (B	ASCII
ESC (J	JIS X 0201-1976 (“Roman” set)
ESC $ @	JIS X 0208-1978
ESC $ B	JIS X 0208-1983

There is a newer character set, JIS X 0212-1990, which has two more characters than the older character sets. However, owing to its rare usage, Internet Exchange does not support it.

Moreover, current Shifted-JIS encoding also does not support the new characters defined in JIS X 0212-1990.

The “Roman” character set of JIS X 0201-1976 is the same as ASCII except for backslash and tilde. The backslash is replaced by the Yen sign, and the tilde is replaced by overline. The JIS X 0208 character set consists of Kanji, Hiragana, Katakana, and other symbols and characters, all of which are 7-bit. Each character consists of two bytes. Shifted-JIS encoding consists of 8-bit characters and no escape sequences are involved in switching between ASCII and Japanese. Both JIS and Shifted-JIS support half-width katakana, which is not frequently used.

Conversion criteria

Internet Exchange for cc:Mail

In order to support Japanese language, Internet Exchange for cc:Mail converts between the Shift-JIS character set used in Japanese Post Offices (Codepage 932) and the ISO-2022-JP used on the Internet, as recommended by RFC 1468.

Internet Exchange for Notes

In order to support Japanese language, Internet Exchange for Lotus Notes converts between the Lotus Notes Multi-byte Character Set (LMBCS) and the Shift-JIS character set used in the Japanese Windows operating system. This is then converted between the Shift-JIS character set and the ISO-2022-JP used on the Internet, as recommended by RFC 1468.

Limitations of Conversions

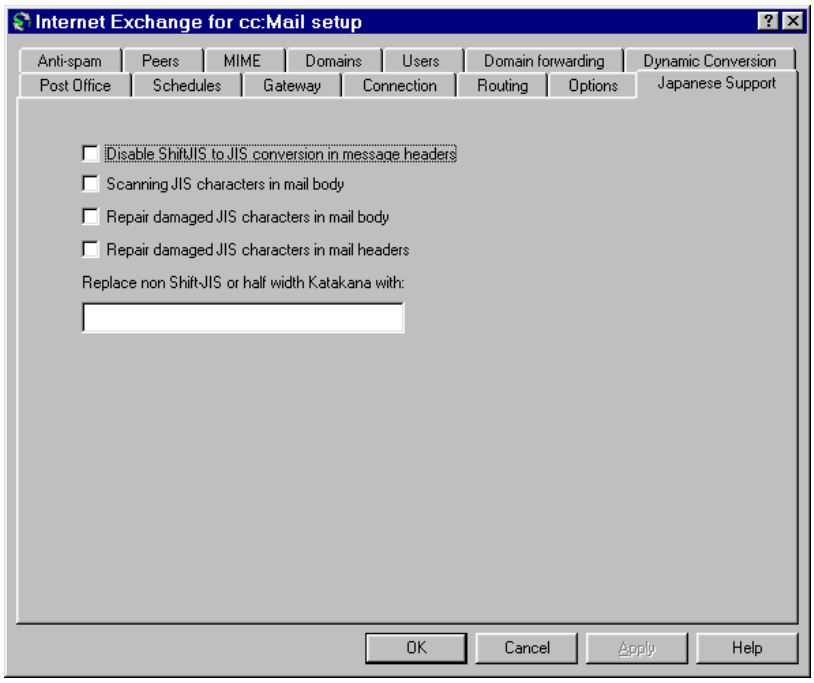
From cc:Mail or Lotus Notes to the Internet

Messages originating from a Japanese cc:Mail Post Office or a Japanese Lotus Notes server are Shifted-JIS encoded when they are composed in cc:Mail. Therefore, a conversion from Shifted-JIS to JIS is required in order for the message to be transmitted through the Internet. If a Japanese message created in cc:Mail or

Notes contains half-width Katakana, this will be changed to full-width Katakana before the full conversion takes place. Since not all 8-bit characters are Shifted-JIS encoded Japanese, they will be checked against the valid range of the Shifted-JIS encoding. However some characters (for example, some European characters) share the same coding range of Shifted-JIS encoding. In that case, those overlapping encoded characters may be mistakenly interpreted as Japanese. If any 8-bit non-Japanese characters are detected in a message, either they will be copied out for further processing or some specified error messages will be issued. In order to achieve a unique standard, all the Shifted-JIS encoded messages are converted into JIS encoded messages having JIS X 0208-1983 as their character set. Therefore, only the escape sequence of ESC $ B and ESC (J are seen in the properly encoded outgoing messages.

From the Internet to cc:Mail or Lotus Notes

All messages must be 7-bit when they are transmitted through the Internet. Therefore, a conversion from JIS to Shifted-JIS is required in order for the message to be transported into cc:Mail for proper reading. The JIS encoded messages are checked to see whether they are JIS X 0208-1978 or JIS X 0208-1983 by examining the escape sequences. Then all the escape sequences are removed and the messages are converted into proper Shifted-JIS encoded messages. The function will also check if there are any incomplete escape sequences indicating the existence of JIS-encoded characters. Since every line must end in ASCII with a carriage return and newline character, scanning for incomplete escape sequences is done on a per-line basis. If “$ B” and “(J” or “$ @” and “(J” are detected at the same time within a line, the text between the pair is treated as JIS encoded Japanese and converted into Shifted-JIS encoded Japanese. The broken escape sequence is removed. So if it happens that the message is intended to have “$ B” and “(J” in the same line as ASCII characters only, the text is erroneously treated as Japanese.



Outbound (cc:Mail / Notes to Internet) messages

If "ISO-2022-JP" is selected in the gateway setup as the local character set, the gateway assumes that all the messages in the Internet queue are encoded in a mixture of ASCII and Shift-JIS. Codes higher than 128 trigger a Shift-JIS to ISO-2022-JP conversion, instead of the QP encoding used when the character set is ASCII or ISO-8859-X.

NOTE: This implies that it is not possible to export from the same Internet PO or Notes server mixes of messages containing Japanese characters and messages containing ISO-8859-X characters. At the time of writing the only solution for mixed Japanese/European environments is the use of two gateways serving one Internet PO or Notes server each (say, INTERNET-I for messages whose 8-bit codes should be QP-encoded, and INTERNET-J for messages whose 8-bit codes should be transcoded into ISO-2022-JP 7-bit JIS).

Replace non Shift-JIS or half-width Katakana with:

Defines a string (e.g. "*invalid character mark*") with which to replace any non Shift-JIS or half-width Katakana characters that the gateway fails to identify during outbound message conversions. If the field is left empty the gateway copies the original message content to the outbound message.

Inbound (Internet to cc:Mail) messages

Scanning for JIS characters in mail body

Enabling this option causes message text to be converted from 7-bit JIS to Shift-JIS before being imported into either cc:Mail or Notes. The default is (enabled) if the local gateway character set is
ISO-2022-JP, and (disabled) if the character set is something else.

Repair damaged JIS characters in mail body

If this is enabled the gateway attempts to recover JIS messages without Escape characters (ESC, ASCII code 27—some mail transports filter them out). This feature uses heuristic criteria, and might produce incorrect results in certain cases. The default is (enabled) if the local gateway character set is ISO-2022-JP.

Repair damaged JIS characters in mail body

If the escape characters in a message have been removed by other mail routers or MTAs, **Internet Exchange** can attempt a recovery of JIS characters without ESC characters. By default, the automatic recovery of ISO-2022-JP escape sequences lacking the escape character will not be attempted.

Inbound and Outbound messages

Disable Shift-JIS to JIS conversion in message headers

The conversion between Shift-JIS and ISO-2022-JP also affects message headers. Should this cause problems, it is possible to disable the bi-directional conversion between 8-bit JIS and 7-bit

JIS character sets in message headers with this option. The conversion takes place by default.

Using Japanese VIM *(cc:Mail Version)*

The recommended platform for Japanese language support is based on the Japanese VIM library and Japanese Microsoft Windows (95 or NT). Japanese VIM may be downloaded from:

ftp://ftp.louts.co.jp/pub/comm/ccmail/update/vdlw32.lzh

The local Post Office should be created by Japanese ADMIN

IMPORTANT: in order to use the Japanese VIM, the VIM character set CP932 must be selected in the Gateway setup page, in the VIM character set field.

Using English VIM 6.x *(cc:Mail Version)*

A kit for the latest version (6.03 at the time of writing) is available free of charge from Lotus's ftp site:

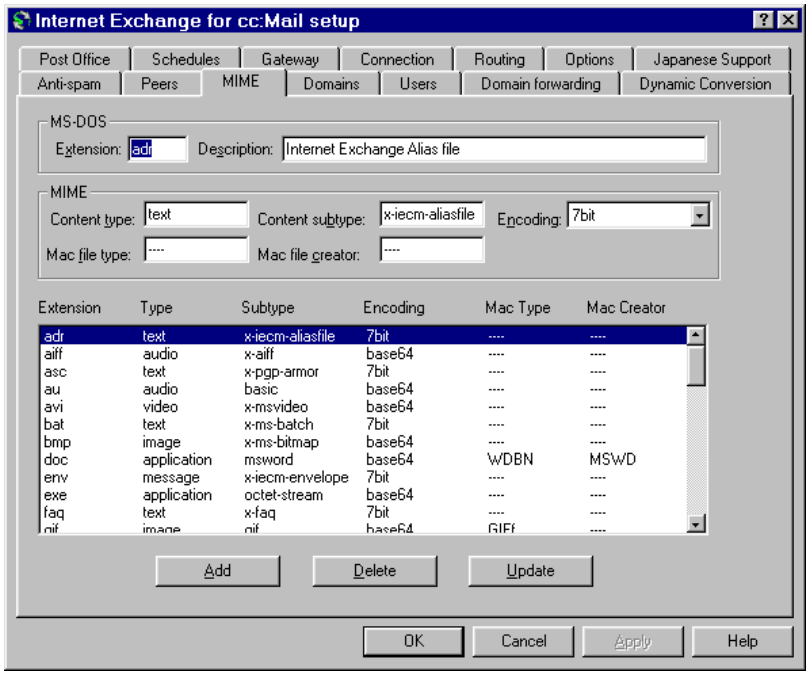
ftp://ftp.ccmail.com/pub/comm/ccmail/dev_tools/vdlw32.zip

This version of VIM has been found to handle Japanese characters on Japanese Windows 95, NT 3.51 and 4.0. This configuration is discouraged, and it is recommend to use Japanese VIM instead.

CONFIGURE MIME

When cc:Mail or Lotus Notes users send messages containing attachments to recipients on the Internet, it is necessary to encode the message and attachments according to the MIME standard. The MIME standard provides a framework for both the encapsulation of attachments within a single message, as well as the encoding of these attachments.

Internet Exchange gives the gateway administrator full control over how file attachments are encoded for messages originating within cc:Mail. An internal table is maintained by the gateway that provides the mapping between DOS file extensions and MIME content type/subtype and encoding methods. Information is also maintained for communicating with Macintosh computers.



The *MIME* configuration screen gives the administrator the ability to modify the manner in which the gateway handles

specific file types and to extend its abilities by adding new file types. **Internet Exchange** comes with the standard set of MIME types and subtypes as defined by the Internet Assigned Numbers Authority (IANA) pursuant to RFC-1590 (Media Type Registration Procedure). This set, which is periodically updated, is available at:

ftp://ftp.isi.edu/in-notes/iana/assignments/media-types/media-types

To enter new MIME mapping rules, the gateway administrator simply fills in the fields *Extension*, *Description*, *Content type*, *Content subtype*, *Encoding*, *Macintosh file type* and *Macintosh file creator* and saves the entry by pushing the *Add* button. Existing entries can be edited by double clicking, and then modifying the appropriate fields. As with a new entry, the modified entry is finalized by pushing the *Add* button. Mapping rules can be removed by selecting the appropriate rule and then pushing the *Delete* button. For more information on how to construct MIME content types / subtypes, please refer to Appendices.

Using the above information, an outgoing GIF attachment will result in the following MIME header:

Content-Type: image / gif; name="world.gif"

In the case of an outgoing GIF sent from a Macintosh, the result might appear as follows:

Content-Type: image / gif; name="world.gif"; type="GIFP:MGIF"

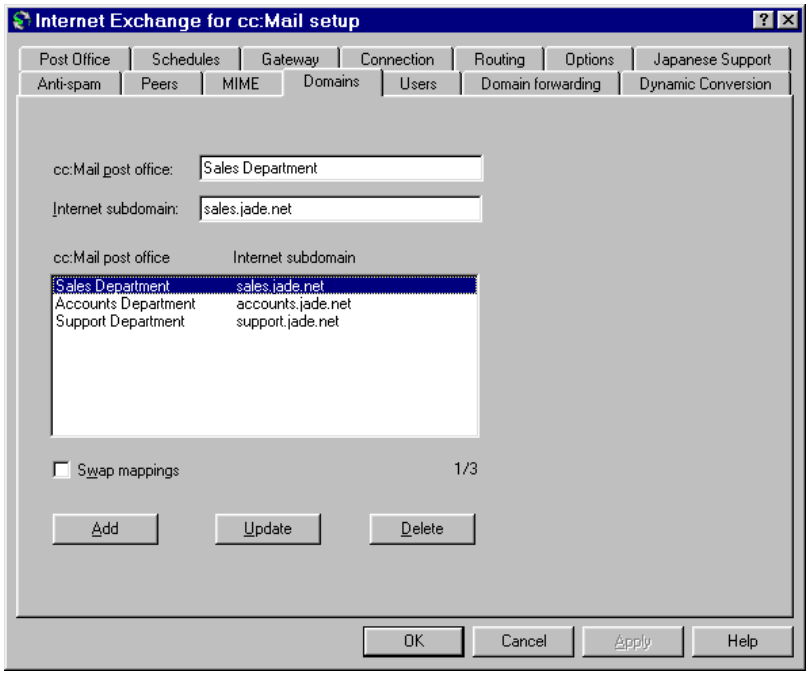
This presumes that the Macintosh file type and creator are *GIFP* and *MGIF* respectively.

When the gateway comes across an attachment type that is not in the MIME mapping table, it applies the default binary encoding method specified in the *Configure Options* screen. The resulting MIME header would look similar to:

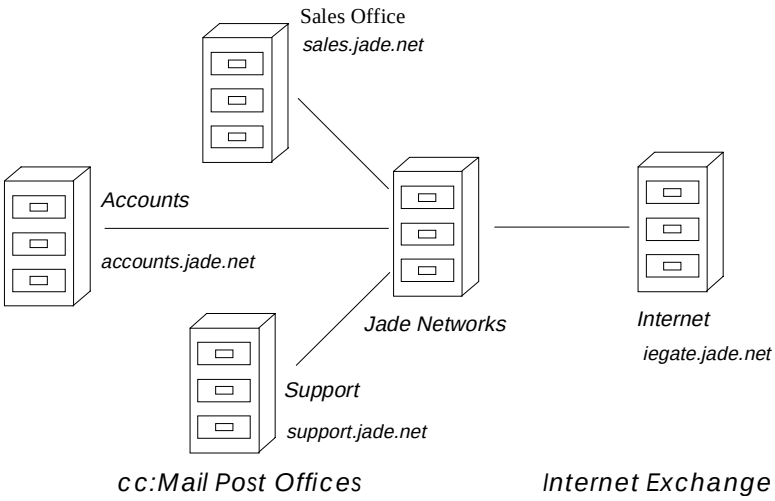
Content-Type: application / octet-stream; name="test.abc"

CONFIGURE DOMAINS *(CC:MAIL VERSION)*

This screen allows the creation of Internet-style subdomains within the local cc:Mail environment. These subdomains are mapped to cc:Mail Post Offices (connected through Router to the main PO) which are hidden from the Internet by the gateway. This style of post office to Internet subdomain name mapping is useful when remote post offices are communicating with the gateway and the cc:Mail post office routing information needs to be maintained across the gateway.



In the following example, three cc:Mail post offices are hidden behind the main post office (*Jade Networks*). The hidden cc:Mail post office names are *Sales Office, Accounts,* and *Support.*



cc:Mail Subdomain Name Mapping

While the cc:Mail post office names are descriptive and legal in the cc:Mail domain, they do not make for good domain name components on the Internet, due to the frequent use of spaces. Since the fully qualified domain name of the **Internet Exchange** gateway machine is *iegate.jade.net*, the remote post offices will appear as subdomains within this domain.

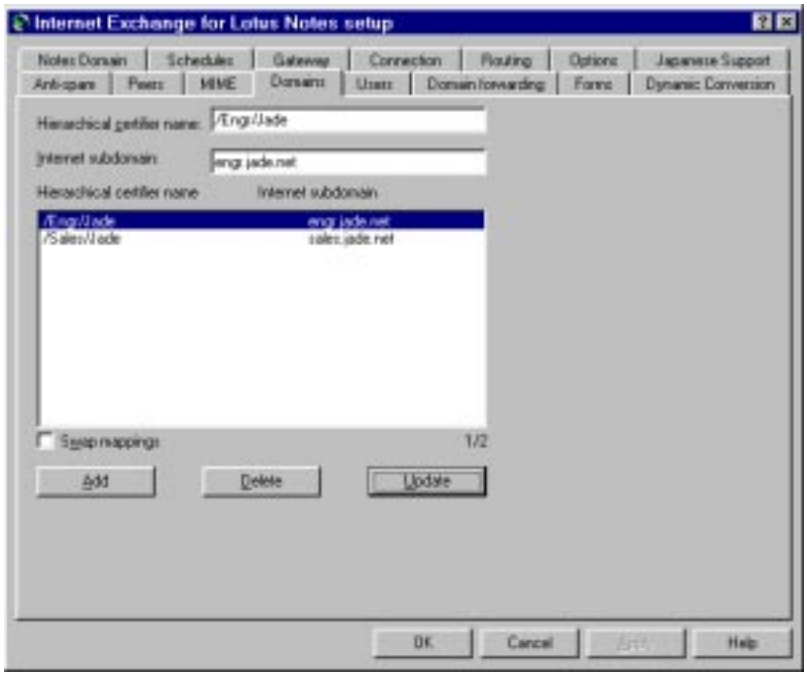
The *Configure Domains* screen gives the gateway administrator the ability to perform these post office to subdomain mappings. When configured as above, cc:Mail messages that originate in the *Sales Office* post office appear to have come from *user@sales.jade.net* once they reach the Internet. Internet messages delivered to *iegate.jade.net* with a recipient address on *sales.jade.net* are delivered to the post office *Jade Networks* for further routing within the cc:Mail domain to the post office *Sales Office*.

Swap mappings

When this option is checked, the position of subdomain mappings can be changed. This is done by highlighting a specific entry, and using Up arrow, Down arrow, Home, End, Page up and Page Down. These keys will move the selected entry in that direction.

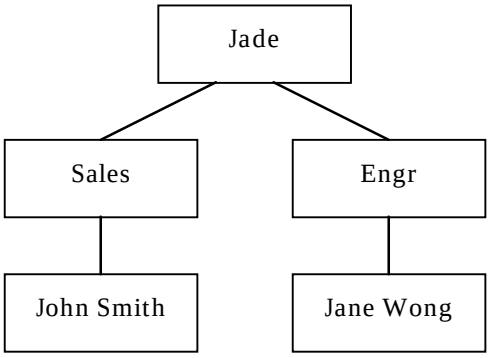
CONFIGURE DOMAINS *(NOTES VERSION)*

This window allows the creation of Internet-style subdomains within the local Lotus Notes environment. These subdomains are mapped to Lotus Notes User's ID Certifiers.



Since the fully qualified domain name of the **Internet Exchange** gateway machine is *iegate.jade.net*, the remote hierarchical certifiers will appear as subdomains within this domain.

In the following example, two Lotus Notes hierarchical certifiers exist in the Lotus Notes environment. These hierarchical certifiers are called */Sales/Jade* and */Engr/Jade.*



Hierarchical Certifier Name Mapping

The *Domains* configuration window gives the gateway administrator the ability to perform these Lotus Notes hierarchical certifier to subdomain mappings. When configured as above, Lotus Notes messages that originate in the */Sales/Jade* hierarchical certifier will appear to have come from *user@sales.jade.net* when they reach the Internet. Internet messages delivered to *iegate.jade.net* with a recipient address on *sales.jade.net* will be mapped back to the */Sale/Jade* hierarchical certifier for further routing within Lotus Notes.

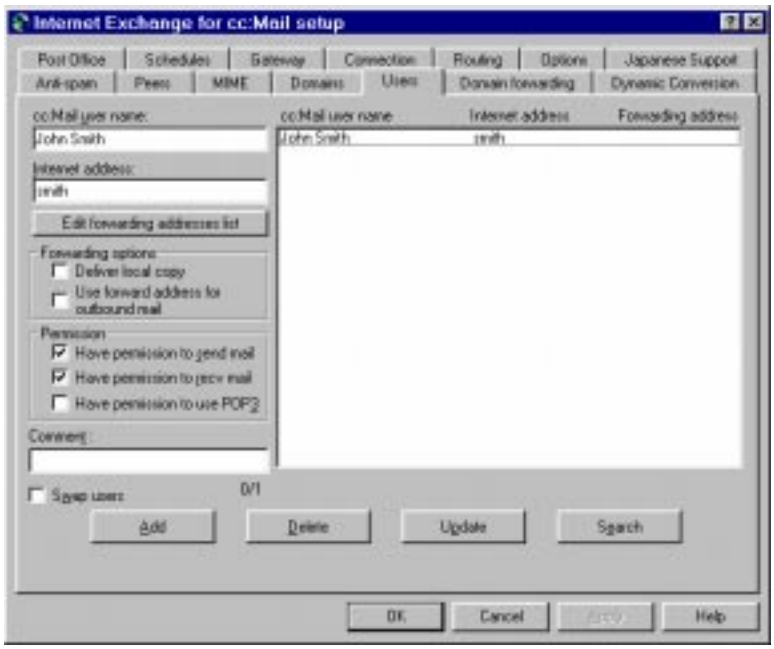
Swap mappings

When this option is checked, the position of subdomain mappings can be changed. This is done by highlighting a specific entry, and using Up arrow, Down arrow, Home, End, Page up and Page Down. These keys will move the selected entry in that direction.

CONFIGURE USERS

This screen allows configuration of cc:Mail or Notes usernames to Internet address mapping on a per user basis. In the absence of an entry in the *SMTPADR.BTR* file, **Internet Exchange** applies the addressing rules. If still unsuccessful, it applies the default address mapping (*Enterprise Edition* only), which converts the cc:Mail or Notes username to:

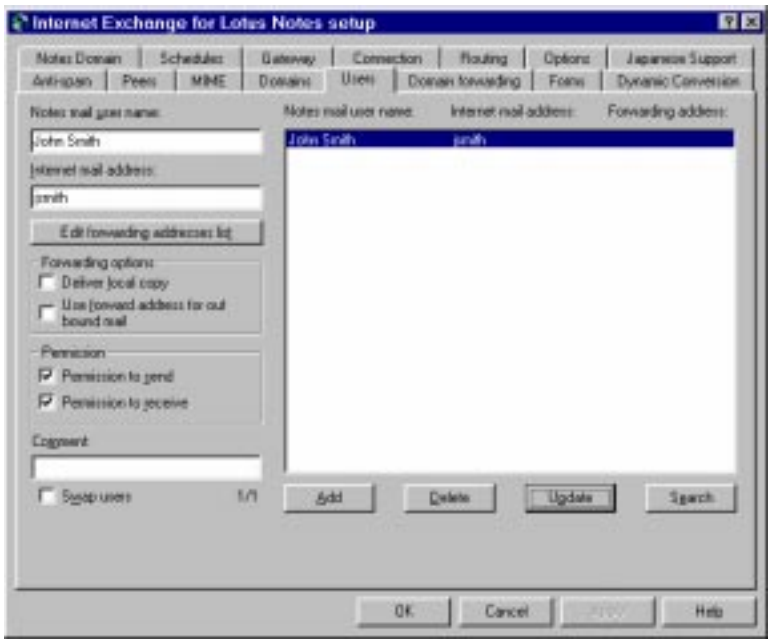
firstname_lastname@gateway.domain



Configure Users: Internet Exchange for cc:Mail

When messages are received through SMTP for delivery into either cc:Mail or Notes, **Internet Exchange** consults the Alias Database for per user address translation rules. If an entry is found the corresponding cc:Mail/Notes address is used for submission into cc:Mail/Notes. If an entry is not found, rules based addressing is attempted (Internet Exchange for cc:Mail

version). If no entries are still not found, the default address translation rule described above is used.



Configure Users: Internet Exchange for Notes

When messages are sent from cc:Mail / Notes to the Internet, **Internet Exchange** consults the Alias Database to match possible *To:*, *From:*, and *Cc:* addresses. If matches are found, these addresses are replaced with the corresponding Internet address prior to submission to the Internet. For the cc:Mail version of Internet Exchange, if an entry is not found, rules based addressing is attempted. If unsuccessful, the default address translation rule is applied in order to construct a valid Internet address.

To add a new entry, enter the cc:Mail or Notes username, the Internet address, and an optional comment. The following can also be checked on a user basis:

Deliver local copy

The inbound message is delivered to the corresponding cc:Mail/Notes user as well as being forwarded to the associated forwarding address. Enabling this option allows replication of inbound mail between a cc:Mail or Notes environment and an external e-mail system.

Use forward address for outbound mail

In general, when a cc:Mail/Notes user sends out an e-mail message to the Internet via Internet Exchange, the cc:Mail or Notes address will be mapped to the Internet alias defined in the Internet address field. If this option is enabled, Internet Exchange attempts to find the associated forwarding address of that Internet alias and, if a match can be found, the first entry in the forwarding addressee list will be used instead. By using this the mail will be sent directly to the forwarding address instead of going back to the original cc:Mail or Notes sender.

Have permission to send mail

Enables the user in question to send mail to the Internet.

Have permission to receive mail

Enables the user in question to receive mail from the Internet.

NOTE: Internet Exchange *Workgroup Edition* supports a maximum of 100 registered users of the gateway. This number is determined by adding the number of unique cc:Mail or Notes users found in the Alias database (and Rules Based Addressing database for the cc:Mail version of Internet Exchange). The gateway will check for the limits when either of the above databases are modified. If the number of users exceeds the maximum allowed, the respective database update will not be made. Manual regeneration of either database which results in an error will result in a dialog box to the administrator indicating the problem. Errors detected during Dynamic Conversion will result in the error

message being mailed to the gateway administrator.

Have permission to use POP3 *(cc:Mail Version Only)*

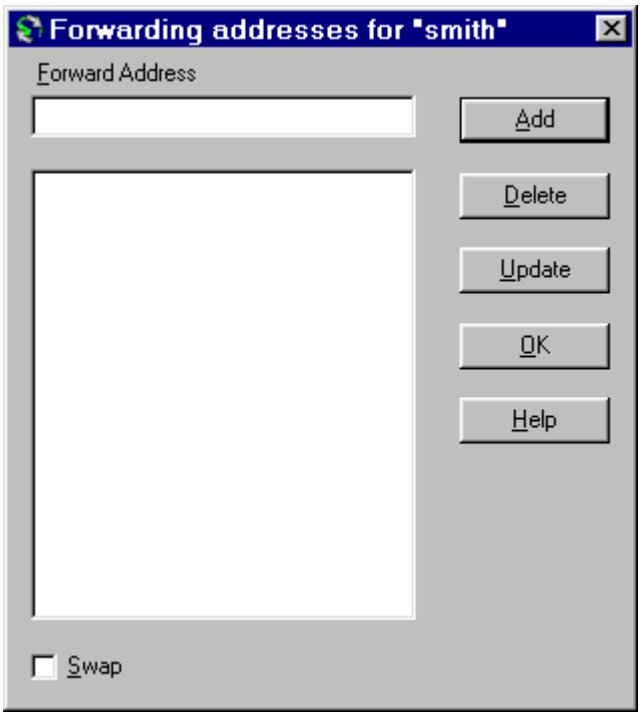
Enables the user in question to access his cc:Mail mail box via the **Internet Exchange** POP3 server.

Swap users

When this option is checked, the position of user mappings can be changed. This is done by highlighting a specific entry, and using Up arrow, Down arrow, Home, End, Page Up and Page Down. These keys move the selected entry in their respective directions. The first entry for a particular cc:Mail user has the highest priority and is used for outgoing address translation.

Edit forwarding address list

For a particular user, highlight their entry and click the *Edit forwarding address list* button. A windows appears where a simple mailing list can be established and managed.



This function allows the manipulation of the database which stores forwarding addresses associated to a particular Internet alias. *CCIN/NOTESIN* uses this mapping to find a list of forwarding addresses for the envelope recipient and reroute the message from the SMTP OUT queue to those forward addresses. Manipulation of this mapping enables the gateway to function as a generic mailing list generator by adding multiple entries for a particular user entry.

This can also be used for migration of individual accounts from **Internet Exchange** to another gateway such as another **Internet Exchange** gateway (Notes or cc:Mail) or other mail systems. On a user basis, a forwarding Internet address with the domain of another gateway can be added. When a forwarding address has been configured, the *Users* configuration should have the *Forwarding options* mentioned above appropriately checked.

Migration is addressed in at greater length in *Chapter 15 - Migration*.

NOTE: There is a manually configurable option which causes **Internet Exchange** to check for the existence of entries in the Domain Forwarding Database *if* no User Address Forwarding information has been found (without this option set messages are sent directly to the cc:Mail or Notes user account). In case **Internet Exchange** finds relevant information in the Domain Forwarding Database the mail is forwarded accordingly; otherwise it is sent to its cc:Mail or Notes alias as normal. To enable this option the following line must be added to *IMA.INI/IELN.INI*:

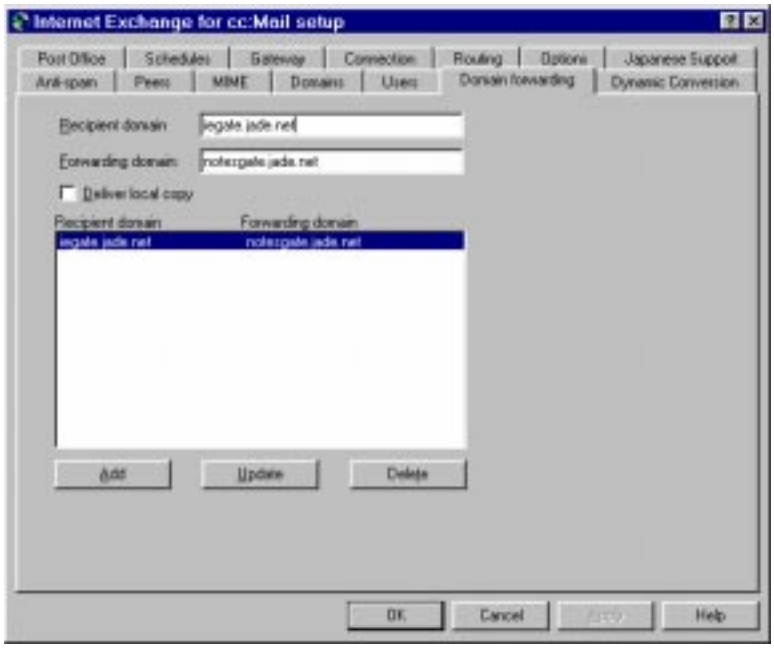
```
[options]
TryDomainForwardingIfAliasLookupFail=YES
```

For received inbound messages the gateway checks for entries in the Domain Forwarding Database; this takes place only after it has been determined that the recipient cc:Mail or Notes user has no user address forwarding configured (configured in the *Users* window). By default this line does not exist, and the default is *NO*.

CONFIGURE DOMAIN FORWARDING

This screen allows the maintenance of the Domain Forwarding Database. This database stores mappings between the recipient domain and forwarding domain. These mappings are used to forward incoming messages of all users from one Internet domain to another Internet domain by the gateway. This can also be used to migrate all users from the current gateway to another messaging environment, which is explained at greater length in *Chapter 15 - Migration.*

NOTE: **Internet Exchange** only supports a *N-1* mapping between each recipient domain and forwarding domain; i.e. you cannot define multiple forwarding domains to a particular recipient domain.



Recipient domain

Enter the full Internet host / domain name (FQDN) of the recipient domain. This is not always necessarily the current **Internet Exchange** gateway domain. Sometimes the gateway is used as an SMTP router for another domain or gateway.

Forwarding domain

Defines a domain name to redirect all incoming messages addressed to that recipient domain.

Delivery local copy

If this option is checked, the message is delivered to the original recipient domain as well as being rerouted to SMTP Out queue.

Note regarding migration

The Domain Forwarding features can be used for migration from the local **Internet Exchange** gateway to another gateway or messaging environment such as another **Internet Exchange** system. This is commonly used to migrate users from cc:Mail to Lotus Notes in a transparent manner. By entering the FQDN of the local gateway as the *Recipient domain* and the FQDN of the remote gateway as the *Forwarding domain*, all incoming mail headed for the local environment (cc:Mail or Notes) is redirected to the remote environment (via the remote gateway). This is not an overnight procedure. A "teething in" period can be accommodated by selecting *Deliver local copy*. Thus, both cc:Mail and Notes environments are supported simultaneously during the migration period. More information regarding Migration strategies can be found in *Chapter 15 - Migration.*

NOTE: For Domain Forwarding there is no on-line option similar to the *Users* configuration window's *Use forward address for outbound mail.* It is possible to achieve a similar result by manually editing the *IMA.INI/IELN.INI* file found in the Windows directory. To do this, the following line must be added to *IMA.INI/IELN.INI*:

[options]
UseForwardAddress=YES

This globally sets the "*FROM*" field in the header of gateway users' outbound messages to include the users' forwarded Internet address rather than their previous local Internet address. By default this line does not exist, and the default is *NO*.

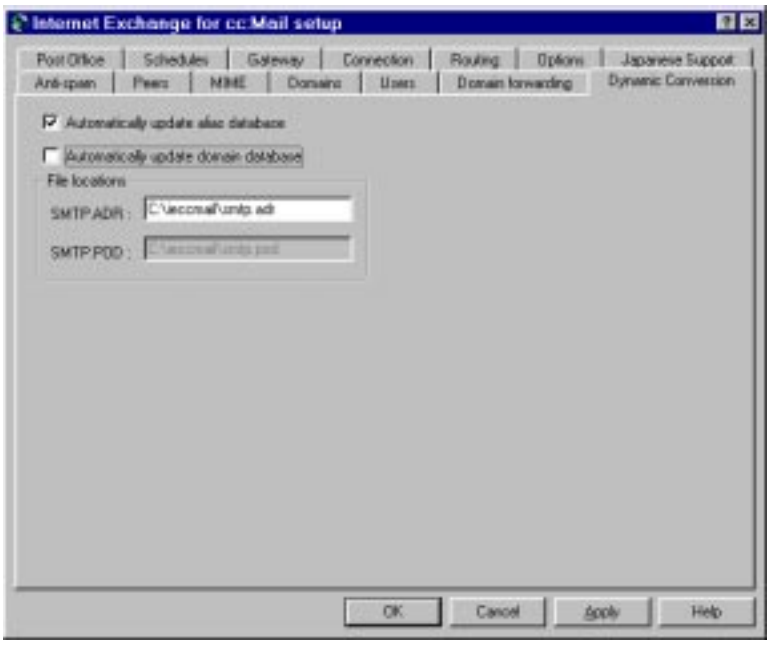
FURTHER NOTE: Another option, manually configurable by modification of the *IMA.INI/IELN.INI* file, causes the gateway to check for the existence of entries in the Domain Forwarding Database *if* no User Address Forwarding information has been found (without this option set messages are sent directly to the cc:Mail or Notes user account). In case the gateway finds relevant information in the Domain Forwarding Database the mail is forwarded accordingly; otherwise it is sent to its cc:Mail or Notes alias as normal. To enable this option the following line must be added to *IMA.INI/IELN.INI*:

[options]
TryDomainForwardingIfAliasLookupFail=YES

For received inbound messages the gateway checks for entries in the Domain Forwarding Database; this takes place only after it has been determined that the recipient cc:Mail or Notes user has no user address forwarding configured (configured in the *Users* window). By default this line does not exist, and the default is *NO*.

CONFIGURE DYNAMIC CONVERSION

The **Internet Exchange** System Manager (*SYSMAN)* program can automatically check the time stamps of the *SMTP.ADR* and *SMTP.POD* files, and if changes are detected, will run the conversion utilities automatically to rebuild the related databases. To change how often these checks are made, change the *System* option in the *Schedules* configuration screen. This function can be useful for systems that have written programs to update the *SMTP.ADR* and *SMTP.POD* automatically.



Automatically update alias database

Enables or disables the routine checking on the *SMTP.ADR* file.

NOTE: Internet Exchange *Workgroup Edition* supports a maximum of 100 registered users of the gateway. This number is determined by adding the number of unique cc:Mail or Notes users found

in the Alias database (and Rules Based Addressing database for the cc:Mail version of Internet Exchange). The gateway will check for the limits when either of the above databases are modified. If the number of users exceeds the maximum allowed, the respective database update will not be made. Manual regeneration of either database which results in an error will result in a dialog box to the administrator indicating the problem. Errors detected during Dynamic Conversion will result in the error message being mailed to the gateway administrator.

Automatically update domain database

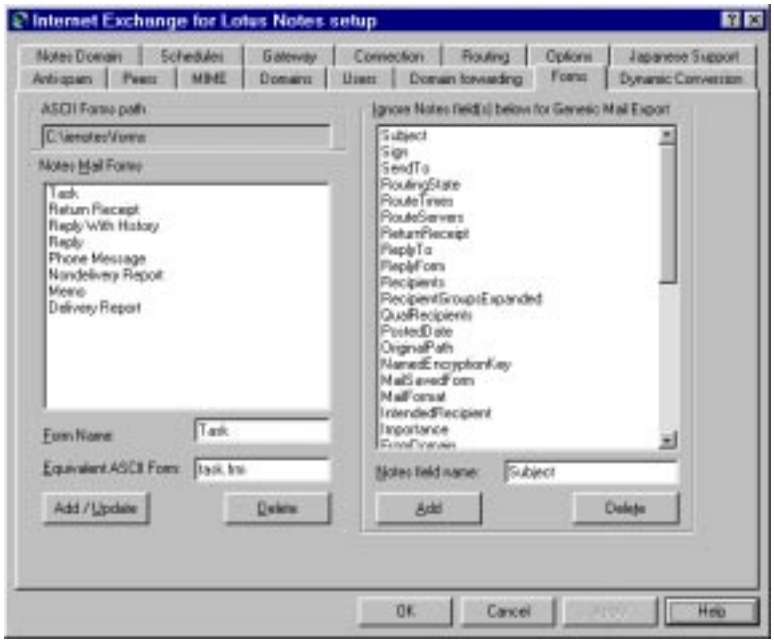
Enables / disables the routine checking on the *SMTP.POD* file.

File locations

Specifies the locations of *SMTP.ADR* and *SMTP.POD* files.

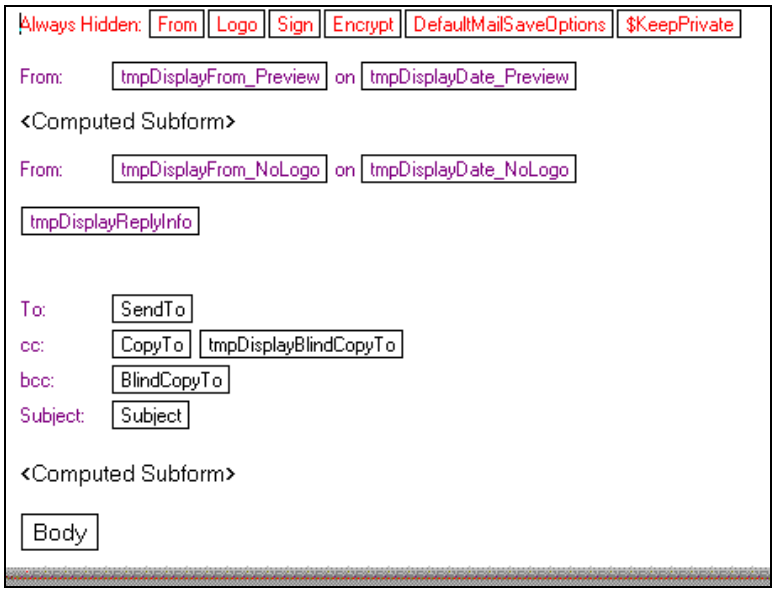
CONFIGURE FORMS

All Notes mail documents are composed of two parts: the FORM note and the DATA note. The FORM note contains the definition of each field in the mail document. These fields can be static text, images, or binary attachments. However, all of these fields are stored as binary information under the Lotus Notes environment. As a result, Internet Exchange requires the form templates so that the gateway can export the information to the correct fields in the pre-defined format in the Internet email message.



Forms handling in Internet Exchange

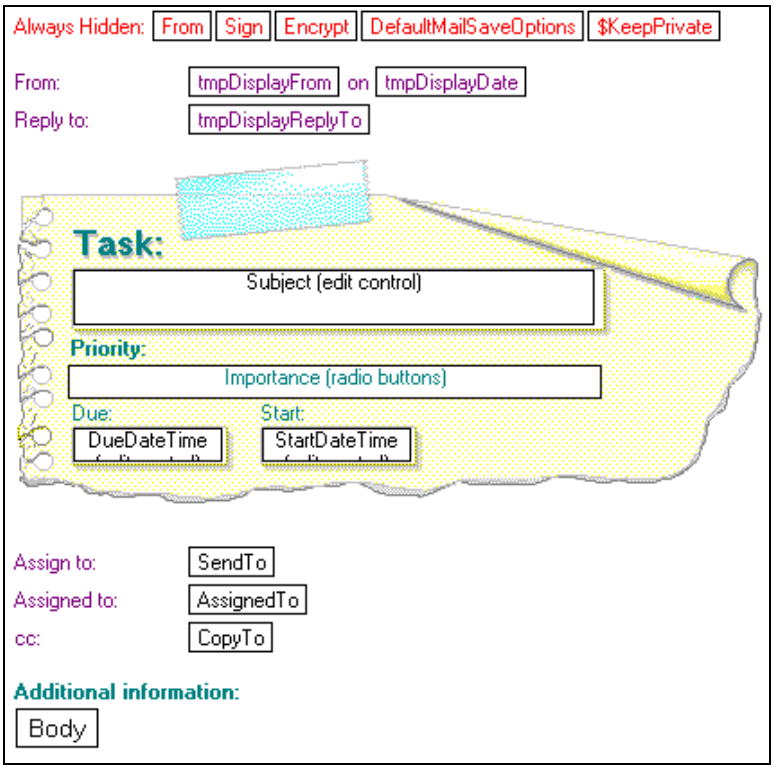
Our first example concerns a standard MEMO form in Lotus Notes:



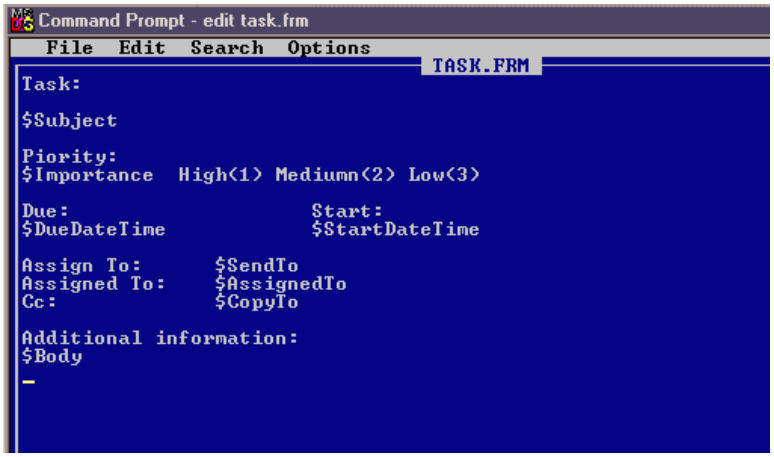
For **Internet Exchange**, the only important information that needs to be exported is the *Body* field. There is no need to include fields such as *SendTo* or *CopyTo* in the mail message body, because they are already in the RFC-822 headers. **Internet Exchange** uses an ASCII form template to do the filtering and mapping for mail export; an ASCII template text file called *MEMO.FRM* is located in the forms directory containing only:

$Body.

A second example is the TASK form:



The ASCII form template, *TASK.FRM* may look like this:



The outbound process will first determine which ASCII form is used for mail export. After getting the suitable ASCII form template, it will perform *Fill in the Blanks*. Each word bearing the prefix '$' is treated as a field, e.g. *$Subject*. The content of the *Subject* field in the Lotus Notes document will be extracted and written back to the mail body. A word *w*ithout a '$' prefix, such as *Task,* will be treated as a *STATIC* text label. This label will be directly written back in the mail body. The final mail body should look something like this:

```
Task:

Cleanup your mailbox

Priority:
2      High(1) Medium(2) Low(3)

Due:                  Start:
12/12/96              12/11/96

Assign To:            johndoe @ ima.com
Assigned To:          johndoe @ ima.com
Cc:

Additional information:
Send me a message when you have finished.
```

NOTE: Only fields of the following types will be exported:

TYPE_TEXT
TYPE_TEXT_LIST
TYPE_NUMBER
TYPE_NUMBER_RANGE
TYPE_TIME
TYPE_TIME_RANGE
TYPE_COMPOSITE *(Rich text)*

For a rich text field, only the text portions (without attributes) can be exported. Embedded objects will be ignored.

What if there is no ASCII form template for certain mail messages?

Suppose that the *TASK.FRM* template has been deleted. When the gateway picks up a mail message composed by the *TASK* form it cannot use the *ASCII* template for export, but there is another way to handle generic mail export. In the *Forms* configuration window the right-hand column contains a list of pre-defined items that will not be exported when using Generic mail export function. Fields other than those specified in the filter will be exported in the mail body like this:

[Field 1]
<Data of Field1>
[Field 2]
<Data of Field2>
:
:
etc.

Only field types that are described above can be exported. Field types that cannot be represented in ASCII format are ignored.

Forms configuration fields

ASCII forms path

This is the directory under which Internet Exchange will store the ASCII forms. By default, this is located in the directory *\ienotes\forms*.

Notes Mail Forms

A list of forms currently known by the gateway by default. Items can added, updated or deleted by the corresponding buttons.

Form Name

The name of the Notes Form that is currently selected.

Equivalent ASCII Form

This is the name of the equivalent ASCII form template file (*.FRM*). This file must be located in the **Internet Exchange** ASCII form path mentioned above.

New or updated Notes Mail forms can be added by entering/editing names to the *Notes Form* and *Equivalent ASCII Form* fields and pressing the *Add / Update* button.

To delete a current Notes Mail form, select an entry from the *Notes Mail Forms* list and press the *Delete* button.

Ignore Notes fields for generic mail export

This list box contains the field names which are not necessary to export from the Notes mail to the mail body of Internet messages. For example, the item "Address" will not be exported to the **Internet Exchange**, provided that this field is shown in the list.

When the gateway cannot find an equivalent ASCII form template to handle the mapping, **Internet Exchange** will export it into a format as follows:

[Item Name]
Item Value

For example,

[Name]
Peter Pan
[TelNo]
852-1234-5678
[Address]
Room 103 Tall Building, Somewhere.

To enable a particular field from Notes Mail to be imported to the main body of the Internet message, select that field from the list and press the *Delete* button.

Notes field name

If an existing form has been customized with an additional field it can be added to the list by entering the field's name in the *Notes field name* field and pressing the *Add* button.

CHAPTER 8
ANTI-SPAM

INTRODUCTION

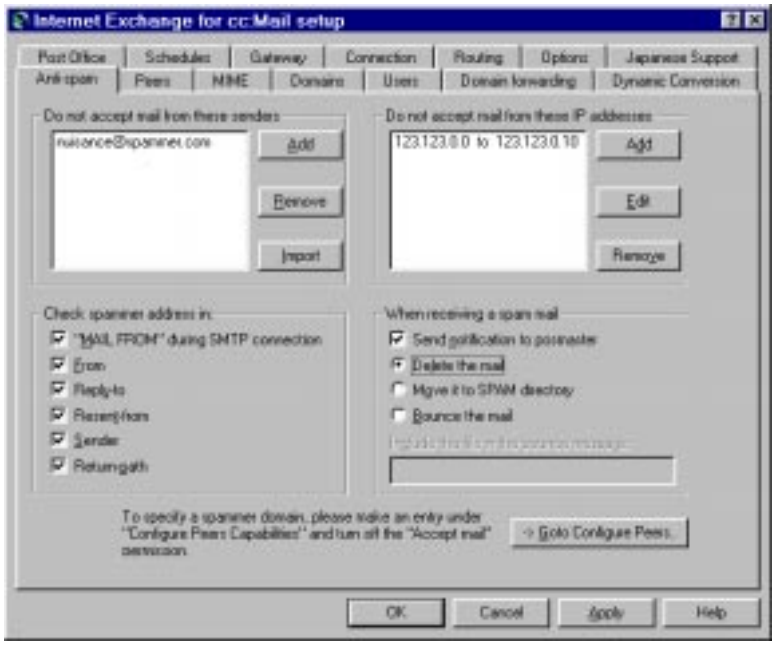
There are several built-in functions that enable gateway administrators to prevent "spammers" (undesirable senders of unsolicited electronic mail) from attacking their mail system. **Internet Exchange** is able to identify spam messages and initiate predefined action against them. The following criteria are employed in the identification of a spam message:

- banned IP address or IP address range on inbound SMTP connection
- banned Internet host or domain
- banned sender's address

Once a spam message is identified it can be:

- rejected by *SMTPD*
- deleted from the Queue directory
- moved from the Queue directory to the */SPAM* directory
- bounced back to the sender

The various functions and configuration of Anti-spam are discussed below.



Specifying spammers' Internet email addresses

A list of spammers' addresses is maintained in the list box named *Do not accept mail from these senders.* To add to this list, click the *add* button, enter the undesired sender's full email address in the pop-up window and click the *add* button on it to finalize the entry. To import a list of spammers from a text file (please note: the file must be in ASCII with one address per carriage return) click *import* and browse for the appropriate file, then click *open.* To remove an entry from the list box, highlight the correct line and click *remove*; a pop-up box will ask for confirmation. Duplicate addresses are not permitted.

Specifying remote spam hosts' IP addresses

A list of undesired mail senders IP addresses are maintained in the *Do not accept mail from these IP addresses* list box. Every time a new SMTP connection is requested *SMTPD* checks it against this list: if a match is made an SMTP error 553 warning is sent to the remote mail host and the connection is dropped. To add to this list, click the *add* button and a pop-up window will appear: to specify just one spammer IP address, enter it in the *start address* field; to specify a range of spammer IP addresses, use both *start address* and *end address* fields. It is possible to modify a list box entry (whether single address or range of addresses) by highlighting it and pressing the *edit* button. To delete an entry highlight it and press *remove*; a pop-up box will ask for confirmation.

Rules to check for spammer address or domain

The gateway is able to check for a spammer address or domain in various parts of a message; to define the rules by which this process is conducted the *Check spammer address in* section must be configured. When the *"MAIL FROM" during SMTP connection* button is checked, *SMTPD* scans for any spammer address or domain during the MAIL FROM session; if a match is found it returns an error 553 warning to the remote sendmail host. The rest of the buttons in the section define the locations in which *CCIN/NOTESIN* scans for spammer addresses or domains: in the *Message From:*, *Reply-To:*, *Resent-From:*, *Sender:* and *Return-Path:* mail message headers. When a spammer address or domain is identified in one or more of these fields, the gateway will proceed to implement one or more of several courses of action defined by the administrator.

Action to be taken in response to spam mail

A number of options to deal with spam mail are provided in the *When receiving a spam mail* section:

Send notification to postmaster

A short notification message is sent to the gateway's postmaster, including details regarding the spammer's address or domain and the action taken by the gateway in response.

Action to be taken with each spam message

(only one may be selected)

- **delete the mail:** the spam mail message is deleted
- **move it to */SPAM* directory:** the spam mail message is moved to the */SPAM* directory, located in the Queue directory of the gateway
- **bounce the mail:** bounces the spam mail message back to the original envelope sender. It is possible to use the *Include this file in the bounced message* edit box in order to specify a filename the contents of which are copied to the bounced message.

Blocking a spammer's domain

This is not an option present in the Anti-Spam configuration screen, but in the *Peers* configuration screen (see *Chapter 9 – Peer Domain Configuration*).

In order to block a spammer from sending mail through the gateway, enter the domain name of the offender in the *Peer Domain Name* field, and click *Save* to add the spammer to the list of peer domains. Select the spammer's domain name in the list box and uncheck the *Accept Mail* checkbox in the *SMTP Connection* section, just to the left of the list box.

CHAPTER 9
PEER DOMAIN CONFIGURATION

INTRODUCTION

The Internet hosts with which **Internet Exchange** communicates will often have different capabilities, such as the email formats that they can accept. The *Peers* Configuration screen allows such information to be recorded and used in preparing outgoing messages for the Internet. This will ensure that messages sent to the Internet are able to be successfully decoded by recipients.

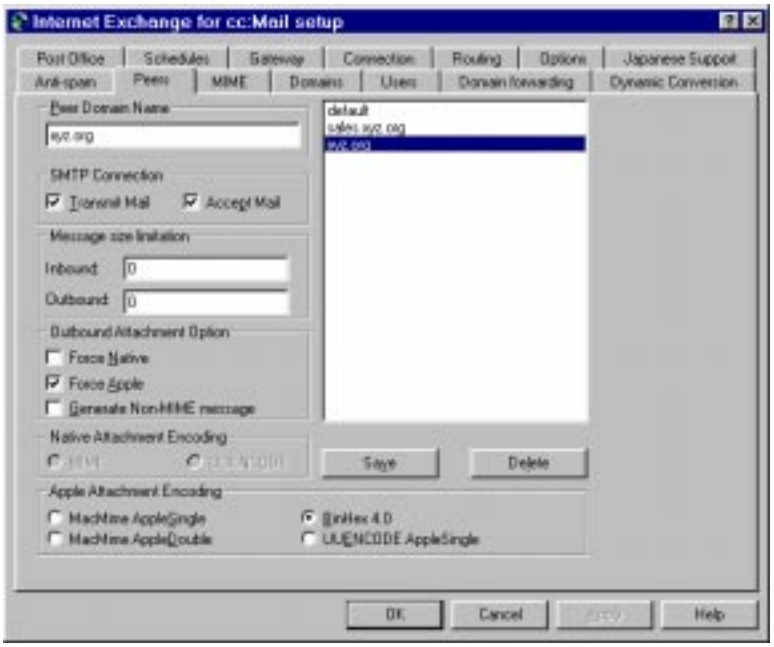
This information is stored as a list of peers for which certain capabilities apply. These capabilities apply to a specific domain and all its subdomains, unless a more specific capability exists within the database. Consider, for example, the following capabilities:

Peer	***Capability***
xyz.org	Uuencode AppleSingle
sales.xyz.org	MacMime AppleDouble

For outgoing messages with Macintosh attachments, any message sent to xyz.org will be encoded with Uuencode AppleSingle. Messages going to test.xyz.org will also be encoded with Uuencode AppleSingle. However, messages

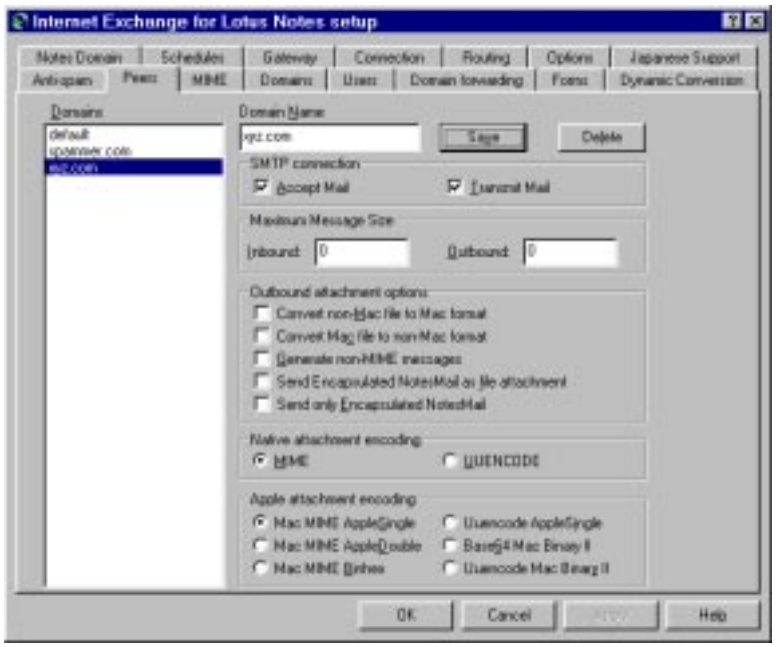
going to sales.xyz.org will be encoded using MacMime AppleDouble, as will messages to m1.sales.xyz.org.

CONFIGURING PEER CAPABILITIES



Configure Peers: Internet Exchange for cc:Mail

The *Peer Domain Name* field allows entry of the required domain. On the right hand side, there is a list box showing all domains for which a peer capability has been defined. By selecting an existing peer from this list box, all the capabilities for it will be displayed in the dialog box. These capabilities can be divided into the following groups.



Configure Peers: Internet Exchange for Notes

SMTP connection

A checkbox is provided to indicate whether **Internet Exchange** is allowed to send to and/or receive messages from the selected domain. If **Internet Exchange** is not allowed to transmit mail to a remote site, *CCOUT/NOTESOUT* will bounce any message destined for that host back to the original cc:Mail or Notes sender. If **Internet Exchange** is not allowed to receive mail from a remote host, *SMTPD* will reject a HELO command from that host with the following response:

> *550 host sales.xyz.org is not authorized to connect to iegate.jade.net*

Message size limitation

The largest message size, in bytes, that can be sent to and received from the selected domain. The smallest size allowed is 8192 bytes (8K). A value of zero indicates no limitations. If the *Inbound* limitation is exceeded, *CCIN/NOTESIN* will bounce the message back to the Internet domain with the following response:

> *Message too big (M bytes). Local limit is N bytes.*

Where *M* is the original message size and *N* is the local size limitation.

If the *Outbound* limitation is exceeded, *SMTPC* will bounce the message back to the originating cc:Mail or Notes user with the following response:

> *This message was returned to you for the following reasons:*
>
> *Can not send message to recipient:<recipient's Internet address> Message (M bytes) too big for peer domain <domain name> local limit is N bytes.*

Where *M* is the original message size and *N* is the local size limitation.

NOTE: By default, attachments are also be bounced. Checking the *Bounce header only for oversize message* checkbox, in the *Options* configuration window, will cause the attachment and body to be dropped from the bounced message.

Outbound Attachment Options *(cc:Mail Version)*

Three checkboxes are offered, specifying how to encode general attachments in outgoing messages. These are:

Force Native

This option will result in all Apple attachments being stripped of their headers and resource fork, allowing non-Macintosh sites to access the information easily.

Force Apple

This option will result in all non-Apple attachments being changed to Apple format. This involves adding a header and an empty resource fork, and then encoding using the Apple encoding specified below. This option might be useful when **Internet Exchange** is communicating primarily with a network of Macintosh computers.

Generate Non-MIME message

This option ensures that no MIME messages are generated for this peer. This can be useful when communicating with older email systems that do not understand MIME. In this case, either UUENCODE or BinHex 4.0 is used to encode binary attachments; if the peer does not contain any Macintosh recipients, it is advised to select UUENCODE encoding.

Outbound Attachment Options *(Notes Version)*

Five checkboxes are offered, specifying how to encode general attachments in outgoing messages. These are:

Convert non-MAC file to MAC format

This option should be checked if the peer domain and subdomains are comprised in large part of Macintosh users. For non-Apple Notes mail attachments, dummy Apple header with empty resource forks are created and Apple-compatible encoding is used (see below).

Convert MAC file to non-MAC format

This option should be checked if the peer is a gateway to a network with a sizeable percentage of non-Macintosh recipients.

Internet Exchange will then strip Apple Notes mail attachments of their headers and resource forks (if any).

Generate Non-MIME message

This option should be checked if the peer is not a MIME compatible gateway. This is useful when communicating with older email systems that do not understand MIME. In this case, either UUENCODE AppleSingle or UUENCODE Mac Binary II can be used to encode binary attachments. If the peer does not contain any Macintosh recipients, it is advised to select *Convert MAC file to non-MAC format* as well.

Send Encapsulated NotesMail as File Attachment

Checking this option will cause the native Lotus Notes *.NSF* file to be attached to a message, along with message text and any attachments. As a result, the outbound message becomes a Multipart/Alternative MIME message. This is useful when recipients consist of a mixture of Lotus Notes users and users of other mail clients. When the peer network is using **Internet Exchange** for Lotus Notes, this option can be used to set up a "Virtual Intranet" Notes network via **Internet Exchange**. That is, **Internet Exchange** at the recipient peer will be able to reuse the attached *.NSF* file to render the original message in the native Lotus Notes format.

Send only Encapsulated NotesMail

Checking this option will cause only the native Lotus Notes *.NSF* file to be attached to the message, stripping the message of text and any attachments. This is only useful if the recipient is also a Lotus Notes user. When the peer network is using **Internet Exchange** for Lotus Notes, this option can be used to set up a "Virtual Intranet' Notes network via **Internet Exchange**. That is, **Internet Exchange** at the recipient peer will be able to reuse the attached *.NSF* file to render the original message in the native Lotus Notes format.

Native Attachment Encoding

MIME

Specifies that non-Apple attachments are to be encoded using the MIME standard.

UUENCODE

Specifies that non Apple attachments are to be encoded using the older UUENCODE format. The *Generate non MIME message* checkbox determines whether MIME headers are generated for messages.

Apple Attachment Encoding

MacMime AppleSingle

Specifies that outgoing Macintosh attachments are to be encoded using the MacMime AppleSingle standard.

MacMime AppleDouble

Specifies that outgoing Macintosh attachments are to be encoded using the MacMime AppleDouble standard.

BinHex 4.0 *(cc:Mail Version)*

Specifies that outgoing Macintosh attachments are encoded using the BinHex 4.0 standard. The *Generate non MIME message* checkbox determines whether MIME headers are generated for messages.

MacMIME BinHex *(Notes Version)*

Specifies that outgoing Macintosh attachments are to be encoded using the BinHex 4.0 standard specified in RFC-1741, also used by the Stuffit(TM) utility.

UUENCODE AppleSingle

Specifies that outgoing Macintosh attachments are to be encoded using the AppleSingle standard, using UUENCODE instead of MacMime. The *Generate non MIME message* checkbox determines whether MIME headers are generated for messages.

Base64 Mac Binary II *(Notes Version)*

Specifies that outgoing Macintosh attachments are to be encoded using the Mac Binary II standard with the base-64 encoding scheme.

Uuencode Mac Binary II *(Notes Version)*

Specifies that outgoing Macintosh attachments are to be encoded using the Mac Binary II standard with UNIX-style x-uue Content-Transfer-Encoding. The *Generate non MIME message* checkbox determines whether MIME headers are generated for messages.

CHAPTER 10
RULES BASED ADDRESSING

INTRODUCTION

The use of rules based addressing allows increased flexibility with the types of Internet addresses that are used with **Internet Exchange for cc:Mail**. While a very simple method of address formatting is provided by way of the default separator, the use of rules based addressing is much more powerful. Rules can be setup so that a number of incoming address formats are accepted, allowing many different addresses to be delivered correctly. In the same spirit, a preferred format can be selected for translating outgoing cc:Mail addresses into Internet addresses.

NOTE: Rules Based Addressing is only present in **Internet Exchange for cc:Mail**.

HOW RULES BASED ADDRESSING WORKS

An addressing rule specifies how to translate between a cc:Mail username and the corresponding Internet address. It is composed of different combinations of the first, middle and last names, in either partial or full form, as well as an optional separator of underscore (_) or dot (.).

Here are some examples of addressing rules, with the resulting address corresponding to a cc:Mail username of Jonathan Andrew Smith:

Address Rule	***Example Name***
FA_M1_LA	Jonathan_A_Smith
F1M1LA	JASmith
F1_MA_LA	J_Andrew_Smith
F1.LA	J.Smith

In the first example above, if an Internet message addressed to Jonathan_A_Smith@jade.net is received, it is delivered to the local user Jonathan Andrew Smith. If there are many addressing rules specified, then each format of incoming addresses is recognized. i.e. any of the addresses on the above right will be translated into Jonathan Andrew Smith, assuming there are no name collisions.

It is not necessary to understand the abbreviated format on the above left of the list, as the creation of addressing rules is conducted via a detailed dialog box, as explained in the next section.

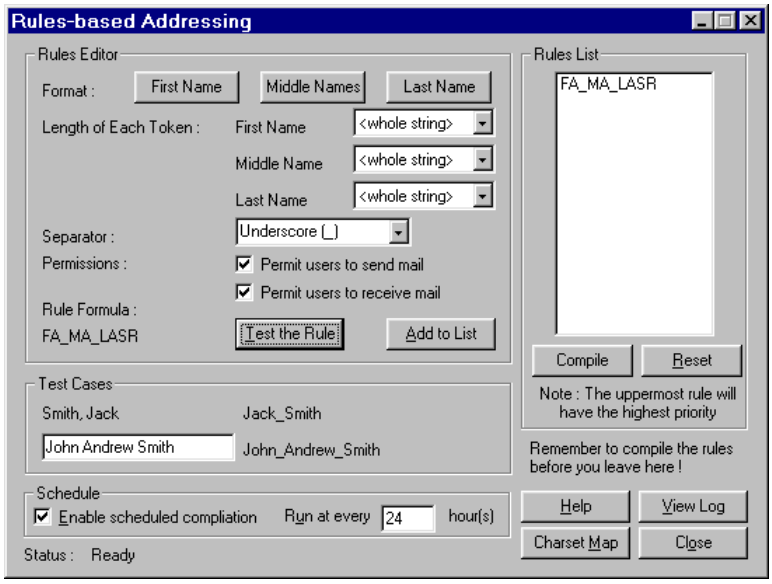
At the end of each rule are optional characters, indicating whether the cc:Mail user has send and/or receive permission. The letters represent the following permissions:

Permissions	***Send***	***Receive***
Allowed	S	R
Banned	X	X

Once the addressing rules have been established, they must be compiled to produce an address directory database. This greatly increases the speed with which **Internet Exchange** is able to process messages. If any changes are made to either the cc:Mail directory or the addressing rules, a new compilation *must* be run by the administrator. **Internet Exchange** will not use the changes until a new compilation occurs.

CONFIGURING RULES BASED ADDRESSING

Rules-based Addressing configuration is accessed directly from the *Internet Exchange Control Panel* via the button or from the *Rules* pull-down menu. The *Rules-based Addressing* configuration dialog box allows easy maintenance of the rules based address system. The first step is to decide upon the preferred format of outgoing addresses. This will look similar to the examples given above. Each rule can be built from up to three separate name parts, optionally separated by either a dot (.) or an underscore (_). The three name parts are FirstName, LastName, and MiddleName(s). If there are more than three parts to the name, then each extra name is added to the MiddleNames(s) part. Any name in the standard cc:Mail format of *LastName,FirstName* will initially be reversed to appear as *FirstName LastName.*



Each of the three buttons on the *format* line can be cycled through the available name parts: first name, middle names, last name, or not used. However, these can only be used in the rule once; the first name cannot be included twice in a single rule.

After selecting which parts of the cc:Mail username to use, the length of these name parts can be chosen by the set of combo boxes below. Each name part can be either the full name, or up to nine initial characters.

Next, the type of separator can be chosen, either the underscore (_), the dot (.) or no separator.

Next, the send/receive permissions can be specified using the appropriate checkboxes.

The current rule can be tested at any time by pushing the *test* button. This shows the results of applying the current rule on two test cases at the bottom of the screen. One of the test cases is fixed, while the other can be changed.

Once the addressing rule is complete, it can be added to the rules list by pushing the *Add to List* button. The new rule will be appended to the list of current rules in the list box on the righthand side of the screen. The R*eset* button can be pushed at any time to delete all the current addressing rules.

NOTE: the first rule in the list is used to generate outgoing Internet addresses.

After all new rules have been added, the *Compile* button must be pushed to compile the addressing rules into the address directory database. If this operation is not done, newly added addressing rules are ignored. A logfile is kept showing the results of the compilation process, and can be examined by pushing the *View Log* button.

Enable scheduled compilation allows automatic compilation of the list of rules into the address directory database, thereby reducing this administrative task, and is especially useful when the cc:Mail address list is changed frequently. Initially the gateway is set to compile once every 24 hours, but other frequencies can be configured.

NOTE: Internet Exchange *Workgroup Edition* supports a maximum of 100 registered users of the gateway. This number is determined by adding the number of unique cc:Mail users found in the Alias and Rules Based Addressing databases. The gateway will check for the limits when either the User Alias or Rules Based Addressing databases are modified. If the number of users exceeds the maximum allowed, the respective database update will not be made. Manual regeneration of either database which results in an error will result in a dialog box to the administrator indicating the problem. Errors detected during Dynamic Conversion will result in the error message being mailed to the gateway administrator.

Name Collisions

In some cases, rule compilation produces a clash in names. There are several situations in which this can occur: For example:

rules:	F1M1LA F1M2LA
user:	Barry Dilmann
mappings:	BDilmann (twice)

In this case, the duplicate mapping is discarded, leaving a single mapping. If two rules produce the same mapping with two separate users, the mapping with the highest priority will used.

Sometimes a single rule will produce a clash for two users: For example:

rule:	F1LA
users:	John Quentin Thompson

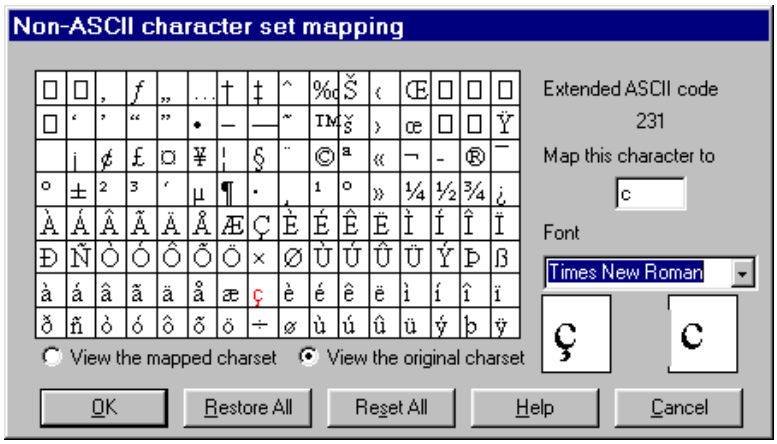
John Martin Thompson.

mapping: JThompson

Here, the mapping is discarded completely, so it would be necessary to add entries in SMTP.ADR so that each user has a unique mapping.

CHARACTER SET MAPPING

Extended ASCII characters (codes 128 - 255) are not allowed in headers of Internet messages. **Internet Exchange** allows these to be converted into standard ASCII characters (codes 0 - 127) by selecting the *Charset Map* dialog box. The administrator can build a customized mapping to convert any Extended ASCII characters into standard ASCII characters to be used in outgoing message headers. This is particularly useful when using international character sets within cc:Mail.



The main character set display in the dialog can display either extended ASCII, or the set of characters that it is mapped to. This can be changed by selecting the appropriate radio button underneath the character set display.

A new mapping may be added by selecting an extended ASCII character in the character set display and typing a corresponding standard ASCII character into the *Map this character to* text box. Once this has been done, the corresponding character is displayed in the box after the small hand. An extended ASCII character can be mapped to a string of, at most, two standard ASCII characters.

The *Font* pull-down list permits a different character set to be displayed. This is useful when working with international character sets.

There are two buttons that allow recent changes to be discarded: *Restore All* returns settings to how they were before this editing session, and *Reset All* removes all character mappings.

NOTE: Character set mapping can only be configured if at least one addressing rule has been defined. Once defined, it is valid across all rules.

CHAPTER 11
UTILITIES

All utilities are accessible via the *Windows Program Manager* in the *Internet Exchange* program group, and the *Address Conversion* and *Domain Conversion* utilities are also accessible via buttons on the *Internet Exchange Control Panel*, as they are used relatively more often. These utilities can be accessed via the *Run* pull-down menu or the following buttons:

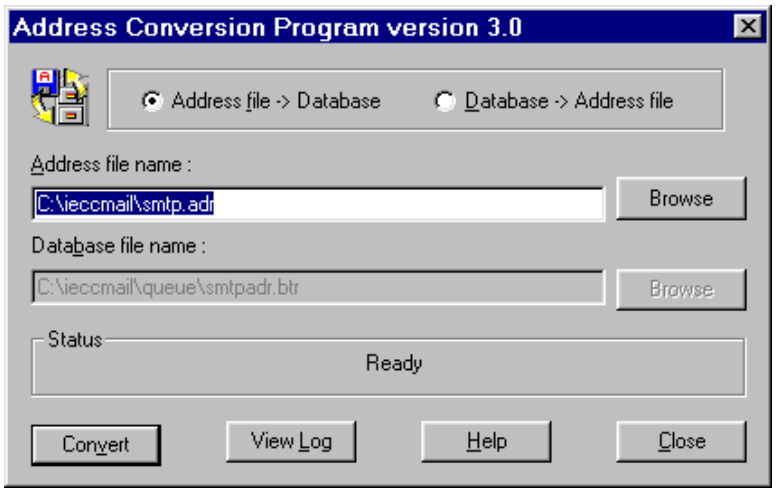
 Address Conversion Utility

 Domain Conversion Utility

ADDRESS CONVERSION UTILITY

The *CONVADR* program converts between the text *SMTP.ADR* file and the Alias Database. It is most useful when an external program has been written to regularly create a new version of *SMTP.ADR*. Once generated, this new version of *SMTP.ADR* needs to be converted to the Alias Database, using this tool. An alternative to running this manually is to enable the *Automatically update alias database* option in the *Dynamic Conversion* configuration screen. This enables *SYSMAN* to regularly check for changes in *SMTP.ADR* and run this conversion program automatically if any changes are

detected. Setting this option greatly reduces the workload associated with maintaining the alias database.



The two radio buttons at the top of the screen indicate the direction in which the conversion will run:

Address file to Database

Converts the old *SMTP.ADR* alias file into the indexed Alias Database, deleting any current information.

Database to Address file

Converts the information from either the Alias Database (see *Users* configuration) or the Directory Database (cc:Mail version only - see *Rules Based Addressing*) to an ASCII file in the same format as *SMTP.ADR*. The destination file is overwritten. A current address ASCII file can serve as a backup in case the Alias or Directory Databases ever become corrupted. To convert the Alias Database, in the *Database file name* field, enter the name as *SMTPADR.BTR* (default). To convert the **Internet Exchange for cc:Mail** rules-based Directory Database, enter *RULEBADR.BTR* in the *Database file name* field.

When doing this latter conversion, it is recommended to rename the *Address file name* from *SMTP.ADR*, as this address file name will be overwritten. Once the Directory Database has been converted to ASCII file, it can be manually manipulated and restored back to database format using the *Address file -> Database* conversion. However, this can only be converted back into the Alias Database, which will overwrite any currently existing Alias Database. This procedure can be useful if the administrator wishes to copy and manually update the user entries from the Directory Database (as a result of running the *Rules-based Address Generator*) to the Alias Database.

NOTE: An easier way to perform this operation is to simply rename the *RULEBADR.BTR* file to *SMTPADR.BTR*. Individual alterations to the globally based address rules can then be modified in the *Users* configuration window.

Convert

Performs the conversion.

View Log

Errors and related information during conversion are logged to the text file *SMTPADR.LOG* in the main directory, which is viewed with this command.

SMTP.ADR Format

There are three formats with which this utility can work. The older formats of *SMTP.ADR* were used in older versions of **Internet Exchange**. However, since **Internet Exchange** version 2.0 the send/receive permissions and comment field have been added to the databases. **Internet Exchange** 3.0 has added *permission to use POP3 (cc:Mail Version)*; *deliver local copy* and *forward address for outbound mail.* This conversion utility handles all three formats.

The old format of SMTP.ADR implemented with **Internet Exchange** version 1.04b or earlier :

cc:Mail_Name<=>Internet_Name

e.g. John_Smith<=>J_Smith

The format of SMTP.ADR introduced with **Internet Exchange** version 2.0:

cc:Mail_Name<=>Internet_Name;<S/X><R/X>;<comment>

e.g. John_Smith<=>J_Smith;SR;Accountant
(John Smith is permitted to send and receive mail)

The format of *SMTP.ADR* introduced with **Internet Exchange** version 3.0:

cc:Mail_Name<=>Internet_Name;<S/X><R/X><P/X><D/X><F/X>;<comment>

- or –

Lotus_Notes_Name<=>Internet_Name;<S/X><R/X><D/X><F/X>;<comment>

where the permissions and options are as follows:

Permissions	***On***	***Off***
Send	S	X
Receive	R	X
Use POP3 (*cc:Mail Version*)	P	X
Deliver local copy	D	X
Forward address for outbound mail	F	X

e.g. John_Smith<=>J_Smith;SRXXX;Accountant
(John Smith is permitted to send and receive mail but not permitted to use POP3. If a forwarding address is provided does not receive a local copy of inbound mail or have his forwarding address contained in his outbound mail)

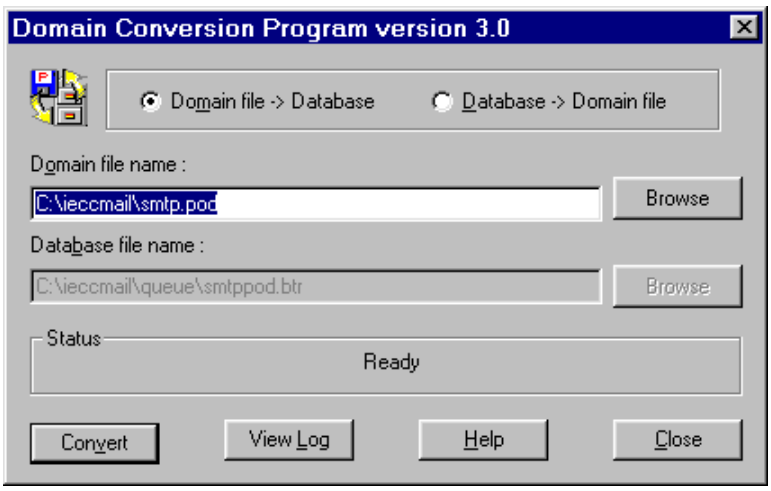
When an earlier than 2.0 format *SMTP.ADR* is converted to the new Alias Database, the send and receive permissions are enabled but all

other permissions and options are switched off and the comment field is left blank. When converting from the 2.x format *SMTP.ADR*, the send and receive permissions and comment field are ported over but the new version 3.0 permission and options are switched off. Conversion of the *SMTP.ADR* file will always be to the new **Internet Exchange** version 3.0 format.

NOTE: **Internet Exchange** *Workgroup Edition* supports a maximum of 100 registered users of the gateway. This number is determined by adding the number of unique cc:Mail or Notes users found in the Alias database (and Rules Based Addressing database for the cc:Mail version of Internet Exchange). The gateway will check for the limits when either of the above databases are modified. If the number of users exceeds the maximum allowed, the respective database update will not be made. Manual regeneration of either database which results in an error will result in a dialog box to the administrator indicating the problem. Errors detected during Dynamic Conversion will result in the error message being mailed to the gateway administrator.

DOMAIN CONVERSION UTILITY

The *CONVPOD* program will convert between the old text *SMTP.POD* file and the Domain Mapping Database, introduced with **Internet Exchange** version 2.0. It is most useful when an external program has been written to create a new version of *SMTP.POD* regularly. Once generated, this new version of *SMTP.POD* needs to be converted to the Domain Mapping Database, using this tool. An alternative to running this manually is to enable the *Automatically update domain database* option within the *Dynamic Conversion* configuration screen. This will enable *SYSMAN* to regularly check for changes in *SMTP.POD* and run this conversion program automatically if any changes are detected. Setting this option greatly reduces the workload associated with maintaining the Domain Mapping Database.



The two radio buttons at the top of the screen indicate which direction the conversion will run:

Domain file -> Database

Converts the *SMTP.POD* user mapping file into the new indexed Domain Mapping Database, deleting any current information.

Database -> Domain file

Saves the information from the Domain Mapping Databases to an ASCII file in the same format as *SMTP.POD*. The destination file is overwritten. An updated *SMTP.POD* file can serve as a backup in case the Domain Mapping Database becomes corrupted.

Convert

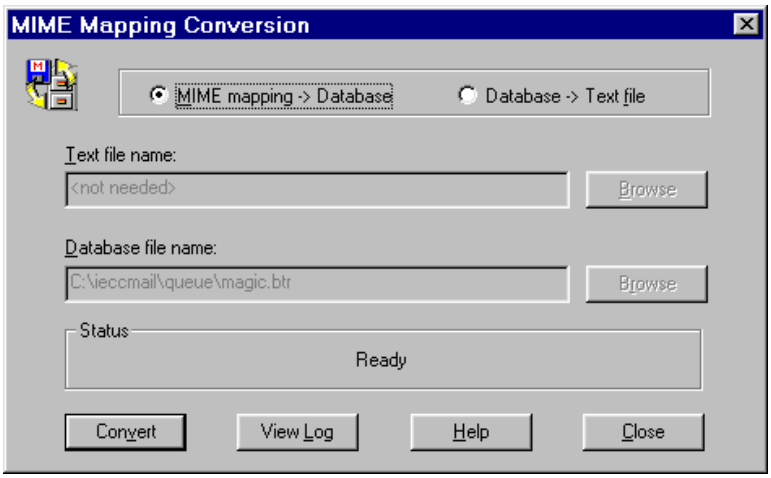
Performs the conversion.

View Log

Errors and related information during conversion are logged to the text file *SMTPPOD.LOG* in the main directory.

MIME CONVERSION UTILITY

This utility is not accessed from the **Internet Exchange** *Control Panel*, but is a separate application launched from the *Internet Exchange* program group in the Windows *Program Manager*. The *CONVMIME* program converts between the text found in the Mime section of *IMA.INI* and the new MIME Mapping Database, introduced with **Internet Exchange** version 2.0. It can convert in either direction, and produces an external text file containing the mappings. This utility is largely unnecessary since the MIME table information had been kept in the *IMA.INI* file only prior to **Internet Exchange** version 2.0. The main application of this utility is the upgrading of a release of **Internet Exchange** earlier than version 2.0. It can also be used to create a backup of the MIME Mapping Database by performing a reverse conversion of the database back to the *IMA.INI* file, which can then be stored elsewhere.



MIME Mapping -> Database

Deletes any existing MIME Mapping Database and creates one based on the MIME mapping information found in the Magic section of the *IMA.INI/IELN.INI* file. The new database fields for which there is no information are left empty.

Database -> Text File

Saves the information contained in the MIME Mapping Database to an ASCII file, suitable for inclusion in the Magic section of the IMA.INI/IELN.INI file. An uptodate text file can serve as a backup in case the MIME Mapping Database becomes corrupted.

Convert

Performs the conversion.

View Log

Errors and related information during conversion are logged to the text file *MAGIC.LOG* in the installation directory, which is viewed with this command.

MESSAGE DATABASE RECOVERY UTILITY

Internet Exchange versions 2.0 and later incorporate a new database backend engine designed to improve gateway performance. Unlike previous versions, which stored message status and envelope information in separate DOS files, versions since 2.0 now store this information in the message database (*MESG.BTR*). For reliability, the message file, which used to contain only the message contents, now also contains redundant envelope information, in the unlikely event that problems are ever encountered with the message database.

If the message database file (*MESG.BTR*) should ever get removed or corrupted, the *Message Database Recovery* utility can be used to read the envelope information from the message files and create a new *MESG.BTR* database file.

The *Message Database Recovery* utility can only be started from the Windows *Program Manager* in the *Internet Exchange* program group. Upon execution, the following message is presented:

To create a new message database, simply click the *Rebuild* button. Upon successful completion of the operation, the message "*Recovered message database successfully!*" is displayed in the window status line.

CHAPTER 12
POP 3 (POST OFFICE PROTOCOL VERSION 3)

The **Internet Exchange** integrated POP3 (Post Office Protocol version 3) server makes it possible for the users of a local cc:Mail post office (as defined in the *Post Office* tab of the configuration window) to access their mail by using a POP3 mail client. The completely functional POP3 Server, fully compliant with RFC-1939, is also referred to as POP3 Daemon, or *POP3D*.

The POP3 implementation permits compliant clients to retrieve cc:Mail Post Office mail via **Internet Exchange**. It also permits retrieval of electronic mail messages via TCP/IP protocol over remote networks (such as the Internet) without the use of cc:Mail For Mobile Users. Please note that POP3 is used solely for retrieving mail.

The *POP3D* control panel interfaces seamlessly with **Internet Exchange**'s Graphical User Interface (GUI) and uses 32-bit VIM libraries to communicate with, authenticate and retrieve mail messages from the cc:Mail Post Office. This permits full multi-threaded access to the cc:Mail Post Office for faster mailbox access speeds and improved efficiency over conventional methods (such as Import/Export, which is 16-bit).

The POP3 Server supports both DB6 and DB8 post office formats, however VIM does not support unique message numbers for DB6 PO types. This means that the UIDL command (Unique-ID Listing)

is not supported in conjunction with a DB6 post office. Because UIDL is an optional implementation under RFC-1939, POP3 mail clients normally have a work-around solution around this problem and no difficulties should be encountered.

Multiple log-ins

It is important to note that a single user may not log in for more than one concurrent session; multiple concurrent use by the same user is not permitted.

Attachment encoding

Non-text attachments are encoded in Base64 format for transmission through the Internet.

Message deletion

When a message is deleted using POP3, it is permanently removed from the cc:Mail PO and is not moved to the TRASH folder. A user who is logged into the POP3 Server will find that if a message is deleted in the background (e.g. by a background cc:Mail session), attempting to retrieve it using POP3 will cause the server to respond to the client with an error message.

SETTING UP A USER TO ACCESS POP3

Server setup

1. From the *Setup* menu of the *Internet Exchange Control Panel*, click on the *User* configuration tab.

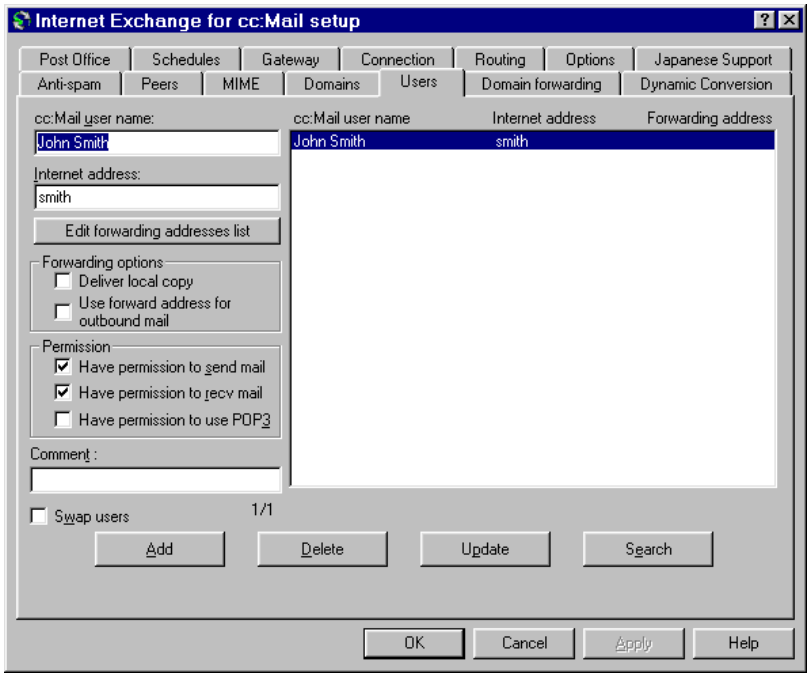
2. If the record of the user to be configured to use POP3 is not present in the table displayed, an appropriate entry must be added (refer to the section *Configure Users* for details). Note that the user must be present in the local post office (configured in *Post Office Configuration*).

3. Ensure that the *Have permission to use POP3* box in the user record is checked.

4. Click the *Add/Update* button to add to or update the user record, and then click *OK* to save changes and close the *Setup* menu.

5. The POP3 Server is initiated on the *Internet Exchange Control Panel* via the *Run* pull-down menu or the button.

The server setup is now completed.



Setting up the POP3 mail client

When setting up the POP3 mail client you will be asked for account and server information.

Account information

For the user name, the Internet name mapped in the **Internet Exchange** *User* configuration is recommended. Alternatively, the cc:Mail name may also be used, but note that it is expected that cc:Mail user names be normalized according to the Default Mapping rules. For example, in the case of the entry shown in the screenshot above, the user John_Smith can enter his user name as *smith* or *John Smith*.

Server information

The host and domain names of the machine where the POP3 server resides should be entered.

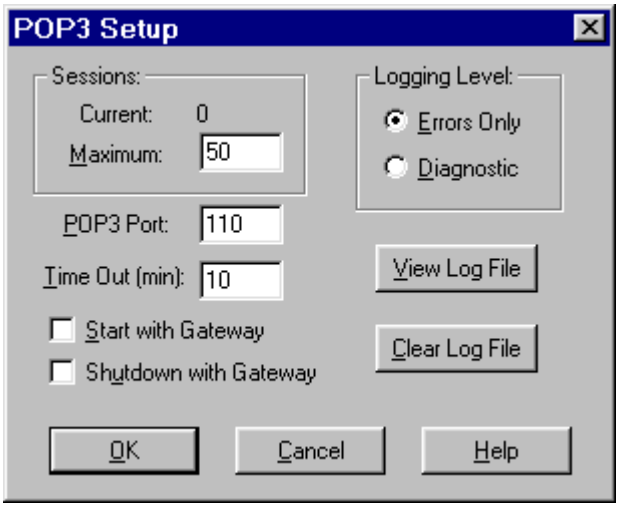
The setup is thus complete.

It is now possible for the POP3 mail client to establish a connection to the server and check for new mail.

CONFIGURING THE POP3 SERVER

The POP3 icon in the System Tray of the Windows Taskbar indicates operation of the POP3 module. Right click on this icon to bring up a menu containing the *POP3 Setup* and *Quit POP3* options.

POP3 Setup



The following parameters can be adjusted to customize your environment:

Current Sessions

Indicates the number of POP3 sessions currently established (note: this is a display only and not an option)

Maximum Sessions

Specifies the maximum number of concurrent POP3 sessions allowed: when this limit is reached further connection requests are refused. New connections can be established only when the Current Sessions number falls below the Maximum Sessions value. The default value is 50.

POP3 Port

This is the listening TCP port number to be used for POP3. The default value is 110.

Time Out (min)

Defines the period (in minutes) during which each POP3 server thread waits for the POP3 client to issue the next command. Upon time-out the server closes the connection. The default value is 10 minutes.

Start with Gateway

If this box is checked the POP3 server is automatically launched when the Gateway is started.

Shutdown with Gateway

If this box is checked the POP3 server will be exited when the gateway is shut down.

Logging Level

Defines the log file logging level. **Internet Exchange** POP3 Server offers two levels of debugging:

Errors Only	Only errors are logged
Diagnostic	The logging mechanism records all activity in the POP3 Server

The diagnostic level is only required when particularly problematic issues arise, as the log will be needed by Technical Support staff. The default logging level is the Error level, which only logs an event when an error occurs.

View Log File

This starts a Windows Wordpad session and displays the current log file. The information displayed and the level of activity recorded are dependent on the logging level previously selected.

Clear Log File

Deletes the contents of the current log file.

CHAPTER 13
REMOTE CONTROL

INTRODUCTION

The primary purpose of the **Internet Exchange** Remote Control is to provide a convenient and secure medium for gateway administrators to monitor, configure and operate **Internet Exchange** remotely. The Remote Control makes use of HTTP as the communication protocol and HTML as the presentation interface to users, which means that a web browser is required to operate it (Netscape and Internet Explorer are both supported). A third party web server that supports the CGI interface and SSL (Secure Socket Layer) are required to provide remote service and ensure a secure transmission channel; **WebSite Professional**, produced *by O'Reilly Software*, meets all these requirements and is recommended for use with **Internet Exchange**.

The Remote Control consists of three components: the *Remote Admin Client* (Netscape 3.01 or later and Internet Explorer 3.02 or later), *web server*, and *CGI programs*. The Remote Admin Client is designed to run on a remote machine and connect to the web server over a TCP/IP network such as the Internet, while the presence of the web server and CGI programs is required on the machine that is running the gateway. A basic description of functionality for these three components follows:

Remote Admin Client

The Remote Admin Client, or web browser, is the main external user interface for gateway administrators. It exchanges data with the web server using HTTP and presents it in HTML format. Netscape and Internet Explorer are both fully supported and suited to be Remote Admin Clients for the **Internet Exchange** Remote Control.

Web Server

A web server that supports CGI and SSL is required to exchange data between the Remote Admin Client and the CGI programs. Its functions are to output the appropriate HTML information to the web browser and invoke the appropriate CGI program when a CGI action is submitted from the web browser.

CGI Programs

These are 32-bit console applications that conform to the standard CGI interface; they are invoked by the Remote Admin Client to perform actions accordingly, and also generate data in HTML format for the web server, which then outputs them to the Remote Admin Client.

REMOTE CONTROL OPERATION

Internet Exchange for cc:Mail – Remote Control

To set up the Remote Control, please refer to *Internet Exchange Installation* in Part 2 of this manual. There are three functional categories for the Remote Control: *Monitoring*, *Configuration* and *Operation*. Please note that the categories and subordinate options listed below are discussed in greater detail in their relevant chapters. The categories are shown on the main web page at *http://web.server.name/ieccmail/index.htm* (cc:Mail version) and *http://web.serve.name/ienotes/index.htm* (Notes version).

Monitoring

Gateway Status

Shows the current gateway status, including the queue counters and status of the various processes (*CCIN/NOTESIN*, *CCOUT/NOTESOUT*, *SMTPC*, *SMTPD* and *POP3D*). The display is refreshed automatically at every lapse of the set time interval. The default time interval is 10 seconds.

Internet Exchange for Notes – Remote Control

System Status

Shows the gateway system status, including the FQDN of the machine on which the gateway is running, license information, local time, up time, memory information, disk space information, VIM library version (*cc:Mail Version)* and TCP stack information.

Configuration

Post Office *(cc:Mail Version)*

Accesses the post office configuration information, including Internet and local post office names, local post office path, password and mail administrator.

Notes Domain *(Notes Version)*

Accesses the Lotus Notes domain configuration information, including Notes Mail Server name, user / server ID file in use, ID password, gateway administrator, Local Notes Mail domain and SMTP domain name.

Schedules

Allows to configure the various schedules of gateway activity.

Gateway

Displays the configuration screen for standard gateway settings.

Advanced Gateway

Displays the configuration screen for advanced gateway features.

SMTPC Profile

Accesses configuration of the SMTPC profiles for message size and various message size queues (please refer to *Chapter 7* for a discussion of SMTPC Profiles).

Connection

Allows to configure host and domain connections.

Routing

Displays the configuration screen for mail relay host routing, DNS server addresses and name resolution.

Options

Accesses configuration of optional settings for message encoding, address separators and other miscellaneous options.

Advanced Options

Configuration of advanced optional settings for delayed mail notification, rules, confirmations and the like.

Japanese Support

Allows to configure Japanese language support settings.

Dynamic Conversion

Displays the configuration screen for dynamic conversion of the alias and domain databases as well as the file locations of the SMTP.ADR and SMTP.POD files.

Operation

Gateway Operations

Displays a list of gateway operations such as start Internet Exchange, shut down Internet Exchange, start *SMTPD*, quit *SMTPD* and so on. To select an operation, highlight it and press the *Submit* button.

View Log File

Shows a listing of all the gateway log files located in the queue directory. The cc:Mail version of **Internet Exchange** also shows the POP3 log files, which are located in their own subdirectory called */POP3* (also in the */queue* directory).

CHAPTER 14
REMOTE ACCESS SERVICE (RAS)

Remote Access Service (RAS) is the service by which the Windows operating system allows the local system to dial and connect to another peer over the Internet. For Windows 95, RAS is more commonly known as Dial-up Networking, but for Windows NT 3.5x and 4.0, this function has been introduced as Remote Access Service.

To facilitate the remote access, scripts are required that replace the manual procedure of entering connectivity and access information such as username and password. This chapter outlines how scripting for use with **Internet Exchange** for Windows 95, Windows NT 3.5x and Windows NT 4.0 is accomplished.

DIAL-UP NETWORKING SCRIPTING FOR WINDOWS 95

The following information in this section on Dial-up Networking Scripting for Windows 95 is copyright © Steve Jenkins 1995 and used with permission. The most uptodate version is available at:

http://www.windows95.com/connect/dscript.html

Note about the Microsoft Scripting Tool

Many scripting users have been having trouble getting some of the Microsoft scripting commands to work. This is because there are two versions of the scripting tool available. The basic scripting tool (which ships on the Windows 95 CD-ROM) supports simple scripts only, like the sample script provided in this tutorial. The default scripting tool should be sufficient for the majority of script users.

Using the more advanced scripting commands requires the scripting tool available in Microsoft PLUS!, which is available at your local software retailer. Any script that uses the integer command requires the Microsoft PLUS! version of the scripting tool.

Step 1: Create a Dial-up Connection

Before writing your script, make sure that you have a working dial-up connection to your Internet provider. If you do not, use the information on the *Windows95.com TCP/IP Setup Page* to help you set one up. Once you have a working connection, proceed to Step 2.

Step 2: Create a Login Script

Using a text editor (Notepad will work fine), create a script that will issue the commands necessary to log you into your Internet provider. If you have a PPP connection, many providers do not require manual log in steps - your *username* and *password* in the *Connect To* dialog box will be sufficient, and you won't need dial-up scripting at all. However, all SLIP/CSLIP connections, some PPP connections, and any other connection that requires menu selections, advanced input, or that does not strip information from the initial dialog box will require a script.

If you have a PPP connection that you think requires a script, try putting *ppp:your_username* in the username text area in the *Connect To* dialog box. Some providers will accept this to initiate a PPP connection. If that doesn't work, try a script. In most cases, you will most probably be able to modify an existing script to connect successfully with your provider. Sample scripts are available here.

All scripts must begin with the following line:

```
proc main
```

and end with:

endproc

These are the commands to tell Windows 95 to start and stop the script. Use the *waitfor* and *transmit* commands to wait for certain information from your provider (such as a login: prompt or a password: prompt) and to transmit your *username*, *password*, and any other necessary information. The variables *$USERID* and *$PASSWORD* will send the username and password entered in the *Connect To* dialog box at the beginning of the dial-up session. To send a carriage return to you provider, use a ^*M*. To wait for any amount of time, use *delay* followed by the number of seconds. You can put comment lines in your scripts by beginning the line with a semicolon (;). For example: a simple script that starts, waits for a *login:* prompt, sends your *username*, hits *ENTER*, waits for a *password* prompt, sends your password, hits *ENTER* then ends, would look like this:

;This will begin the script

proc main

;Enable the following to delay for 3 seconds first to
;allow host time to send initial characters (not needed by many ISPs).

delay 3

;Sometimes, ISP's need a carriage return to initiate the login process.
;If your ISP requires this, uncomment the following line:

;transmit "^M"

;Wait for the login prompt before entering the user ID and carriage return
;(I left off the first letter since login is case-sensitive)
;The $USERID variable is taken from the dial-up connection dialog box

```
waitfor "ogin:"
transmit $USERID
transmit "^M"

;Enter your password (I left off the first letter since login is case-
sensitive)
;and send a carriage return

waitfor "assword:"
transmit $PASSWORD
transmit "^M"

;Finish the script!

endproc
```

In fact, the above is the exact script I use to connect to my provider! If you use the integer command in your script, you will need the version of the *Dial-up Scripting Tool* available in Microsoft PLUS!.

If your provider requires PPP callback, try inserting these lines into your script:

```
delay 1
transmit "++++"
delay 1
transmit "at&c0q0o^M"
```

Once you're finished with your script, save it in the *\Program\Files\Accessories* folder, with a file extension of *scp* (i.e. *ppp.scp*).

Step 3: Verify that the Dial-up Scripting Tool is Installed

Press the *Start* button under Windows 95, select *Programs*, then *Accessories*. If the *Dial-Up Scripting Tool* shows up, you're ready to proceed to step 4.

If it is not there, and you have the Windows 95 CD, press the *Start* button, select *Settings...*, then *Control Panel*. Double-click the *Add/Remove Programs* icon. Select the *Windows Setup* tab, then click on the *Have Disk* option. Assuming your CD-ROM drive is E:, enter

the path of *e:\Admin\Apptools\Dscript*. Press *OK* and the *SLIP/CSLIP* drivers and *Dial-up Scripting Tool* will be installed.

If you have Windows 95 on floppies, you can download the *Dial-up Scripting Tool* and *SLIP* drivers directly from Microsoft (be aware, however, that their server is VERY busy). Then install the *Dial-up Scripting Tool* as shown in the above paragraph.

Step 4: Attach Your Script to a Dial-up Profile

Press the *Start* button under Windows 95, select *Programs, Accessories*, then *Dial-Up Scripting Tool*. You'll see the utility's dialog box.

Your current dial-up profile(s) will be listed in the text area on the left. Select the profile for which you wrote the script, and then press the *Browse* button. If you saved your script in the *Accessories* folder, it should appear in the dialog box. Select it and press *Open*.

If you'd like to troubleshoot your script (recommended for the first time through), select the *Step through* script option. Upon connection, this will allow you to "step through" each line of your script and see the result in a terminal screen. When your script is working properly, select the *Start terminal screen minimized* option to keep the script window minimized when you connect.

Press the *Apply* button (it's best to keep the *Dial-up Scripting Tool* dialog box open until you finish troubleshooting your script) and get ready to try your script! When you are certain it works, you can press *OK* to close the *Dial-up Scripting Tool*. It does not have to be open when you connect for the script to work.

Step 5: Connect and Troubleshoot your Script

IMPORTANT! Before you connect and use your script, go to *My Computer*, double-click *Dial-up Networking*, select your dial-up profile, click the right mouse button, and select *Properties*. Underneath your modem (in the *Connect using* section), press the *Configure* button. Select the *Options* tab and make sure that in the *Connection Control* area, NEITHER OPTION IS SELECTED. Even though you probably had the *Bring up terminal window after dialing* option selected previously, the *Dial-up Scripting Tool* opens a

terminal window anyway. Leaving this option checked will cause your script to fail.

Using *Dial-up Networking*, connect to your Internet service provider. Make sure your *username* and *password* are entered into the dialog box, since your script will need these variables to connect. If you chose to step through the script, a terminal window will appear upon connect and let you step through your script by pressing *F7*. Watch the result closely to track down errors in your script. You can press *F3* during this process to cancel at any time.

Once your script connects reliably, turn off the *Step through script* option in the *Dial-up Scripting Tool* dialog box. You can also close the *Dial-up Scripting Tool*. It does not need to be open for the script to run. It will run automatically with your dial-up connection as long as it is attached properly.

Example Scripts

I have put together a collection of sample scripts that work with Internet Service Providers around the world. You can find them in my Sample Scripts page. All of them are easily modifiable to work with your particular provider

RAS SCRIPTING FOR WINDOWS NT 3.5X

To automate the Remote Access Server (RAS) login procedure, create a login script and store it in the file:

%SYSTEMROOT%\system32\ras\switch.inf

where *%SYSTEMROOT%* is path of the topmost directory of the Windows NT installation, e.g. *C:\WINNT35*. Windows NT comes with the sample script file (*SWITCH.INF*), so it is recommended to first copy the file to *SWITCH.INF.BAK* then edit the original file in Notepad.

The *SWITCH.INF* may contain more than one connection script. The individual scripts are delimited by their section header, represented by square brackets [ ] followed by the command and response

entries. The entry contained in the section header describes the subsequent script which is then associated with a particular RAS phone book entry.

Determine exactly what is expected to be sent and received in order to connect to the peer network during the login process. To get this information, use the RAS Terminal interface and conduct the login process manually. Comments, starting with a semicolon, should be added to your script in order to simplify future administration.

The available RAS script commands are shown below.

<cr>	Carriage return.
<lf>	Line feed.
<match>"abcdef"	Waits for match to "abcdef".
<ignore>	Ignores the rest of the response.
<?>	Wildcard character.
<hNN>	Used to represent a hexadecimal value containing the digits NN.
<diagnostics>	Displays a diagnostic message box.
OK=value	Defines the expected response.
COMMAND=value<cr>	Sends the text string "value".
NoResponse	No response is expected.
CONNECT=value	Terminates the script when the "value" is received.
ERROR_NO_CARRIER=value	Checks for the loss of the modem carrier.

ERROR_DIAGNOSTICS=value	Checks for diagnostic messages.
LOOP=value	Loop waiting for a match value.

The following is a typical RAS script used to access an ISP. Replace the "*sername*" and "*assword*" with your own username and password. It is important to ensure that the syntax of each command is correct in order to have a successful script.

NOTE: it is necessary to leave a blank line after the script header, or the script will not work.

; this is the header section
[My ISP Login Script]

; wait for the USERNAME prompt
OK=<match>"sername:"
LOOP=<ignore>
COMMAND=your_username<cr>

; wait for the PASSWORD prompt
OK=<match>"assword:"
LOOP=<ignore>
COMMAND=your_password<cr>

; If your ISP requires more prompts and responses, enter them below
…

; the model above then issues the final command below
OK=<ignore>

Associating the RAS Script with the RAS phonebook entry

Once the login script (*SWITCH.INF*) is complete, it must be associated with the RAS phone book entry. When RAS is launched it will activate the script and thereby automate the login process. The following steps explain how to achieve this:

1. Start the *Remote Access* applet.

2. *Edit* an existing phone book entry or *Add* a new entry.

3. Ensure this entry is capable of connecting to the ISP manually.

4. Uncheck the *Authenticate using the current username and password* checkbox.

5. Click the *Security* button; if it is not visible click the *Advanced* >> button to access it.

6. Check the box *Accept any authentication including clear text*.

7. In the *After Dialing* list box, select the entry of the section header of the script added to the *SWITCH.INF* file.

8. Click *OK* to confirm and then close the *Remote Access* window.

9. Restart the *Remote Access* applet, selecting the appropriate phone book entry, and click the *Dial* button to test the RAS configuration.

Troubleshooting the RAS Script

Troubleshooting a RAS login script is possible by reviewing the *DEVICE.LOG* file, which records all connection activity. After a failed login, this log file indicates how the *SWITCH.INF* script should be modified to enable the correct connection. To activate logging of the connection attempt (the log is stored in the *DEVICE.LOG* file):

1. Run the *REGEDT32.EXE* registry editor program.

2. Modify *HKEY_LOCAL_MACHINE \ SYSTEM \ Current ControlSet \ Services \ RasMan \ Parameters*.

3. Change the value of Logging to 1.

Restart the RAS applet in order to start logging. The commands sent during connection and their responses will be logged to the *DEVICE.LOG* file in the *%SYSTEMROOT%\SYSTEM32\RAS* directory.
After troubleshooting is complete, reset the Registry option to disable RAS logging.

RAS SCRIPTING FOR WINDOWS NT 4.0

Microsoft Windows NT 4.0 supports both Windows 95 dialup scripting files (files with the *.SCP* extension) and the Windows NT 3.5x RAS scripting file (*SWITCH.INF*). Please refer to the previous sections for the formats of these script files.

Associating the RAS Script with the RAS phonebook entry

After a scripting file is created it must be associated with the RAS phone book entry. RAS will then activate the script when its phone book entry is launched, thereby automating the login process; before associating the RAS script, it is useful to manually ensure that it can connect to the ISP. Script association is achieved with the following steps:

1. Start *Dial-Up Networking.*

2. Select the appropriate phonebook entry from the pull-down combo box *Phonebook entry to dial.* If an entry has not yet been recorded, use the following steps:
   a) Click the *More* button.
   b) Under the *Basic* tab, fill the fields for *Entry name*, *Phone number* and other settings as required.
   c) Under the *Script* tab, choose the *Run this script* radio button and select your script from the pull-down list
   d) Change the settings under the other tabs as required.

3. Click the button *More* and select the option *Edit entry and modem properties.*

4. Select the *Script* tag and click the option *Run this script*. Then choose the appropriate script from the pull-down list and click *OK*.
5. Click the *Dial* button to connect to the ISP and test the RAS configuration.

Troubleshooting the RAS Script

The troubleshooting procedure is the same as for Windows NT 3.5x, described in the previous section.

CHAPTER 15
MIGRATION

INTRODUCTION

As more cc:Mail-using organizations make the transition to Lotus Notes or other messaging environments, the need to seamlessly migrate users from one product to the other has become more and more evident. **Internet Exchange** Version 3.0 includes numerous features that far surpass those of its predecessors. This includes migration functionality developed to resolve issues related to the conversion from Lotus cc:Mail to Notes or to other messaging environments, as well as mail address aliasing within the gateway.

This means that present users of Lotus cc:Mail and **Internet Exchange** can now seamlessly cross over to Lotus Notes and **Internet Exchange** for Notes, or other messaging environments, without disturbing their messaging requirements. Both cc:Mail and Notes environments can be kept running concurrently for a "teething-in" period.

Figure 1 shows the relationship between each of the **Internet Exchange** gateways, the Internet and the Lotus mail applications:

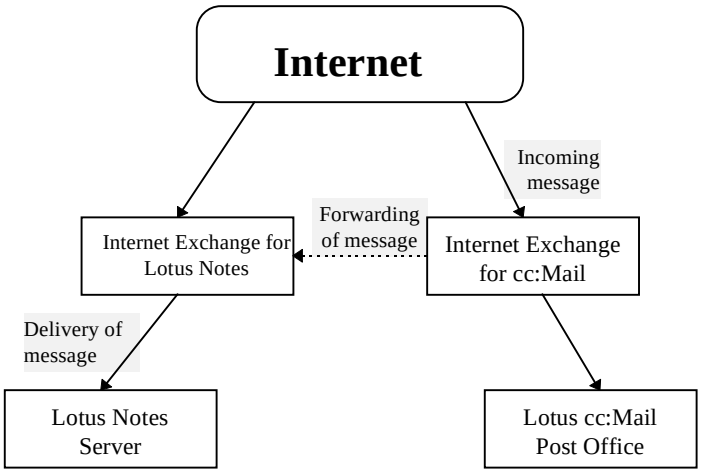


Figure 1 - Address Migration

ISSUES RELATED TO MIGRATION

There are a large number of factors to take into consideration when making the transition from Lotus cc:Mail to Notes. It is certainly not an overnight procedure and there is more to consider than simply the movement of mail directories and addresses. Much planning is required, and the process can take weeks and sometimes months to complete. This means, inevitably, that the usage of both mail systems will overlap and, for this reason, the administrator should think of this procedure not merely as a migration but as a coexistence of systems.

From the Lotus product viewpoint, the Notes environment needs to be configured with user accounts, directories, mailboxes and so forth. This can be completed by the *cc:Notes* migration utility offered by Lotus. Information regarding *cc:Notes* can be found in the Lotus documentation. With the Notes environment in place and the new **Internet Exchange for Notes** product installed, users can begin the process of moving over to their new mail system. The problem facing them is that this process will, more than likely, take some time depending on the size of the organization. Not only will the testing phase and the "teething" process be time-consuming, but

users will want to be able to use the old cc:Mail client while they familiarize themselves with their new mail system.

This scenario could be problematic for mail administrators: there might be users still running cc:Mail, others that have been shifted to Notes and others yet opting to continue with both systems. Appropriate addressing for each user, not only in order to receive mail from the Internet, but also to be able to choose what information to display in the "From" field in the outbound message headers, would become somewhat difficult. **Internet Exchange** is designed with a migration and coexistence functionality. As will be explained, many configurations are available to administrators to cater for all migratory situations and eventually reach the point at which a complete shift to Lotus Notes has occurred.

Examples

The first and clearest example implements migration using **Domain Forwarding**. When testing has been completed and both cc:Mail and Notes gateways are fully operational, the mail administrator can implement Domain Forwarding to move all users in a sub-domain over to Lotus Notes. All incoming mail to the cc:Mail gateway for a particular sub-domain is redirected over to the Notes gateway and promptly forwarded to the respective Notes user. The mail administrator can choose to copy all incoming mail for that sub-domain to the local cc:Mail Post Office as well. This added option allows a coexistence between the two systems for an intermediate period, and can be revoked when cc:Mail support is discontinued.

The next example utilizes Per User migration which is where the movement over to Lotus Notes is not an approach across the board but is stepped, on the basis of individuals. In this instance, mail administrators can choose which individual users will move over to Lotus Notes and whether they will continue to receive a local cc:Mail copy of inbound mail. Once users are comfortable with Notes and the full transition is complete, mail administrators can suspend the cc:Mail copy.

When configuring migration on a per user basis, the mail administrator has an additional option to set up a mailing list for incoming mail: mail directed at a particular address can be

forwarded to multiple destinations, thus enabling an incoming mail address list. This is appropriate as part of a migration strategy when users wish to receive mail from Lotus Notes, while using a different mail client off-site; this is also useful if the organization is considering additional mail application options.

MIGRATING INTERNET ADDRESSES TO INTERNET EXCHANGE FOR LOTUS NOTES

There are two methods of migrating Internet → cc:Mail gateway messages on to a Notes gateway. The *per user* basis defines the new Internet address for the Notes **Internet Exchange** gateway for individual users only. The *domain forwarding* basis allows to specify multiple users by redirecting Internet mail addressed to a particular domain on to a new specified domain name.

Per User Migration

From the *Setup* menu, choose the *Users* tag. A list of current users is displayed, showing users' cc:Mail user name and corresponding Internet addresses. To migrate a user to **Internet Exchange for Lotus Notes**, highlight the user to be migrated and press the *Edit forwarding address list* button. The *Forwarding addresses for <user>* window will appear where the user's new address is entered in the *Forward address* field. Press *Add* to update the new forwarding address to the list. This entry can be deleted or updated at a later time. Press *OK* to apply these changes.

To enable mail to continue to be directed to the current local cc:Mail account as well as forwarded to the Lotus Notes **Internet Exchange** gateway, check the *Deliver local copy* box. In addition, checking the *Use forward address for outbound mail* box will cause the "From" field in the header of outbound messages to include the users' forwarded Internet address on Notes rather than their previous local Internet address on cc:Mail.

NOTE: Adding more than one Internet address to the list of forwarding addresses causes incoming mail to be redirected

to all addresses specified. It is therefore possible to enable a simple mailing list for incoming mail. The *Swap* button here can be used to alter the order of domains as they appear in the list. This can be useful when the forwarding address is included in the "From" field of outbound message headers because only the first address of the simple mailing list is included in the header.

Domain Forwarding Migration

From the *Setup* menu, choose the *Domain Forwarding* tag. To migrate all incoming mail addressed to users in a particular domain, enter the domain's Fully Qualified Domain Name (FQDN) in the *Recipient domain* field. The FQDN of the new **Internet Exchange for Lotus Notes** gateway should then be entered in the *Forwarding domain* field. When finished, pressing the *Add* button will append the FQDN to the list of destination domains. The FQDN consists of the gateway's host name as well as the organization's domain name in the form <*hostname*>.<*domain name*> (i.e.: *cchost.company.com*).

To enable incoming mail to be directed to the current local cc:Mail account as well as forwarded to the Lotus Notes gateway, highlight the appropriate domain and check the *Deliver local copy* box. Press *OK* to apply the changes.

NOTE: For Domain Forwarding there is no on-line option similar to the *Users* configuration window's *Use forward address for outbound mail.* It is possible to achieve a similar result by manually editing the *IMA.INI/IELN.INI* file found in the Windows directory. To do this, the following line must be added to *IMA.INI/IELN.INI*:

[options]
UseForwardAddress=YES

This globally sets the "*FROM*" field in the header of gateway users' outbound messages to include the users' forwarded Internet address rather than their previous local

Internet address. By default this line does not exist, and the default is *NO*.

It is possible to concurrently enable Per User and Domain Forwarding migration for forwarding addresses of individual users. In this case when messages arrive and the gateway is determining where to forward an address, the Per User forwarding takes precedence over Domain Forwarding.

NOTE: Another option, manually configurable by modification of the *IMA.INI/IELN.INI* file, causes the gateway to check for the existence of entries in the Domain Forwarding Database *if* no User Address Forwarding information has been found (without this option set messages are sent directly to the cc:Mail user account). In case the gateway finds relevant information in the Domain Forwarding Database the mail is forwarded accordingly; otherwise it is sent to its cc:Mail alias as normal. To enable this option the following line must be added to *IMA.INI/IELN.INI*:

```
[options]
TryDomainForwardingIfAliasLookupFail=YES
```

For received inbound messages the gateway checks for entries in the Domain Forwarding Database; this takes place only after it has been determined that the recipient cc:Mail user has no user address forwarding configured (configured in the *Users* window). By default this line does not exist, and the default is *NO*.

APPENDICES

APPENDIX A
ELECTRONIC MAIL ADDRESSING

INTERNET MAIL ADDRESSING AND ROUTING

RFC-822 Message Format

An RFC-822 message is the standard unit of electronic mail on the Internet and with mail gateways that exchange mail with Internet-connected systems. When the basic Internet mail standards were published in 1982, RFC-821 (Simple Mail Transport Protocol) defined the method of exchanging messages among Internet hosts. RFC-822 (Standard for the Format of ARPA Internet Text Messages) defined the overall format of the messages themselves, as well as the syntax and semantics of mail addressing.

Each RFC-822 message is made up of simple ASCII text consisting of two parts: a header and a body. This entire message is enclosed in a so-called "envelope," which the SMTP client and server use to route and deliver the message. The message header consists of lines of keywords, usually individually called "headers," followed by a colon (':') and a text or numeric string value. The full list of keywords can be found in RFC-822, and is further extended by the MIME specification (see *Appendix D* on MIME). The headers are separated from the message body by a blank line; the body is an ASCII text of arbitrary length.

Of the required RFC-822 headers, the most important for mail addressing and routing are the From:, To:, Cc: and Bcc:, Sender:, and Reply-To: headers (and variations on these indicating a re-sent [forwarded] message). Each of these is expected to contain one or more valid mailbox names (e-mail addresses) in the form specified by RFC-822.

From: / Resent-From:	Identity of the person or process that caused this message to be sent. Should be a single mail address. "Resent-From:" indicates a forwarded message.
Sender: / Resent-Sender:	Identity of the person or process actually sending the message (this could be a secretary or a software agent). Optional if the contents of the field would be identical to the "From:" line.
Reply-To: / Resent-Reply-To:	The address to which replies to this message should be sent. Redundant if contents would be the same as the "From:" header.
To: / Resent-To:	Identity of the primary recipients of the message.
Cc: / Resent-Cc:	Identity of the secondary (informational) recipients of the message.

Bcc:	Identity of additional ("blind") recipients of the message. The contents of the field are not included in the message header but are processed separately by the sender's mail agent.

Some additional RFC-822 header fields of interest include "Message-ID" (which uniquely identifies the message, usually by combining a time-stamp and serial number with the sender's system's domain name); "Received" (a time-stamped "postmark" added by each system that the message passes through, for tracing and debugging purposes); "Subject" (the topic of the message); and "Date" (a time-stamp for the message).

In addition, users may define additional header fields for private use and place them in the header. These headers begin with the letters "X-", e.g., "X-Full-Name", and are guaranteed not to conflict with RFC-822 headers defined in the future.

Since RFC-822 was published there have been some extensions to the set of defined header fields. The most important of these are the MIME headers, which are discussed in the Appendices.

RFC-822 Addresses

An RFC-822 mailbox address is made up of two parts — on the left is the "local-part", and on the right is the "domain-part". They are joined in the middle by the "@" symbol, pronounced "at". (Example: roger@wilco.org.) The domain-part specifies how the message should be routed on the Internet, and the local-part specifies how it should be delivered when it arrives at its destination. SMTP clients and servers and other mail transport agents and gateways normally only deal with the domain-part. Other programs called *local delivery agents* use the local-part to determine how to deliver the message to a particular mailbox, program, or mail filter. Sometimes further transport of the message

to another mail system is “hidden” in the local-part. This is discussed below.

The content of the domain-part determines how the message will be routed on the Internet. RFC-822 discusses a number of domain ideas, but predates the adoption of the Domain Name System (DNS). It thus should not be used as an authority for domain syntax and semantics, in which it has been superseded by STD 13, (RFC-1034 and RFC-1035).

RFC-822 permits comments and explanatory material in the contents of originator and recipient header fields. These are often used to note the actual names of users corresponding to mailbox addresses, the names of mailing lists or mail aliases, or the names or versions of programs that send or receive mail. Strings inside parentheses are always comments; arbitrary strings not containing syntactically significant characters may also appear as comments on a line, so long as the actual address is enclosed in angle brackets (<>).

Some examples of RFC-822 header lines include the following

```
From: bill@bloom-county.outland.com (Bill the Cat)

To: “Wayne Gretzky” <gretzky@la-kings.nhl.org>

From: MCP@TRON.NET (Master Control Program v1.0)

To: larry@startup.com (formerly larry@bigcorp.com)
```

Note that in the example the address in parentheses is treated as a comment and will not be used for delivery.

The domain-part of RFC-822 addresses is case-insensitive; “user@bigcorp.com”, “user@BIGCORP.COM”, and “user@BigCorp.Com” are equivalent. The local-part of the address, since it is interpreted by a wide set of different local delivery agents on different operating systems, *is* case-sensitive, and should never be modified by mail transport programs.

UUCP Addresses

UUCP is a set of protocols intended to serve as a method of transporting files, executing remote commands, and transporting mail among UNIX systems. This was used to build the first large-scale electronic mail network as well as the Usenet News network. It is very commonly seen in the UNIX world, and there are implementations of UUCP for DOS/Windows systems and other platforms. Many Internet sites also use UUCP, and messages from one UUCP site to another may use the Internet as a backbone network.

UUCP mail addresses are of the form "site!user", where "site" is the UUCP name of a particular system, and "user" is a mailbox. A chain of site names, called a "path", can be used to explicitly state the route to the recipient's site. e.g., *violet!topaz!ruby!jane* means, "send the message to *violet*, then *topaz*, then *ruby*, which will deliver it to mailbox "jane." The namespace of UUCP sites is flat, and there is no provision for centrally assigned site names. There is, however, a central registry that attempts to both prevent name collisions and provide a routing database. The UUCP mail network is implemented as a number of individual, site-to-site connections.

In recent years there have been some modifications and extensions to UUCP mail addressing and routing. First, many UUCP sites have registered DNS domain names, and use normal RFC-822/DNS addresses. In most cases, these sites have an Internet mail exchanger that accepts mail for the domain and forwards it via UUCP. Outgoing messages are sent to a default UUCP connection for delivery to the Internet or elsewhere.

Furthermore, it is possible to use the data provided in the centrally maintained UUCP routing/site maps to produce a routing database that will look up an address like *ruby!jane* and turn it into the appropriate path address. e.g. *violet!topaz!ruby!jane*, or alternatively forward the message to an Internet forwarder that may transform the address into a domain-type address like *jane@ruby.xyz.edu*.

Finally, if a site is in the UUCP map database, it may be possible to route mail to it by using the unofficial ".uucp" pseudo-domain, e.g., *jane@ruby.uucp*. This is functionally equivalent to *ruby!jane*, and

requires that the sending system either use the UUCP map database or forward all outgoing messages to a mail relay system that does.

Hybrid Addresses

Because of the way certain sites are connected to mail relays, it is not uncommon to see addresses that mix different addressing formats. The most common of these is the so-called "percent-sign hack", in which a non-Internet mail route is "hidden" inside the local-part of an RFC-822 domain-type address. Instead of a simple mailbox, the local-part would contain an unofficial "user@site.network" type address. However, it is a syntax error for there to be more than one "@" in an RFC-822 address, so the "hidden" @ is turned into a "%". E.g.:

jane%ruby.uucp@relay.xyz.edu

In this case, the message will be delivered to *relay.xyz.edu*, whose mailer is expected to decode the local-part and deliver it on to *ruby!jane* by UUCP.

Another type of hybrid address is a mixture of a UUCP path address with a domain address, e.g.:

ruby!jane@topaz.xyz.edu

This is commonly seen, but has the problem of being ambiguous. It could mean either, "deliver the message to *topaz.xyz.edu* for forwarding to jane at the UUCP site *ruby*", or "deliver the message to UUCP site *ruby* for forwarding to jane at the domain *topaz.xyz.edu*." Unfortunately, there is no universal standard that covers these situations: Internet hosts will generally follow the former interpretation ("@" takes precedence) while UUCP-only hosts will follow the latter interpretation. This type of address format should be avoided wherever possible in favor of either a true domain address or, if necessary, a UUCP path address including the host in the domain-part, e.g.:

topaz.xyz.edu!ruby!jane

Lastly, it is possible to encapsulate other types of address formats completely unrelated to RFC-822 or UUCP inside the local-part of a domain address. In this case, the entire local-part should be enclosed in double quotes (“ “). This is useful for sending messages via X.400 gateways, e.g.:

```
“/C=US/PRMD=StarMail/O=HiTechCorp/G=Mickey/S=Jones/”@hitech.com
```

which indicates that the message is to be delivered to “hitech.com” via normal Internet methods (i.e., SMTP). The mail transport agent at hitech.com will then hand it off to a X.400 gateway for further delivery using the local-part.

Internet Mail Routing

With a properly formed domain address, the task of mail routing is relatively simple. When the sender’s mail transport agent attempts to deliver the message on the Internet, it first “resolves” the address. After determining that the address is not local (in which case it will simply pass the message to a local delivery agent), it makes a DNS query asking for the host name and Internet address of a mail exchanger (MX) for the recipient’s domain.

A mail exchanger is an Internet host that is registered as accepting mail for a particular host (including itself) or entire domain. When queried for an MX record for a domain, the DNS server will return records containing the host names and IP addresses of the mail forwarders and a priority number indicating which forwarder is to be tried first. The sending system will attempt to open an SMTP connection with the MX host with lowest-numbered priority, and if unsuccessful, will try each other MX in order of increasing numerical priority.

If there are no MX records for a particular host/domain, then the sending system will make a DNS query for the actual IP address of the recipient's host, and if successful, will attempt to open an SMTP connection directly with it.

MX records are typically used for two purposes. First, to provide a back-up capability for receipt of mail when a host is unavailable on

the network. Secondly, when a host acts as a mail relay for systems that are not directly connected to the Internet.

In the first case, incoming messages may be re-directed to another host at the same site. Here, the messages might be deliverable by a different method, or at least could be queued locally until the original host is back on the network.

In the second case, a host acting as a mail relay will accept messages for one or more systems or sites that are not directly connected. It may either simply send the message on through an internal IP route (as in the case of systems behind security fire walls), or may forward the message onward by another type of transport, such as UUCP. In either case, the complexities of routing the mail are hidden from the sender of the message, who merely needs to know the proper domain address.

APPENDIX B
APPLE MACINTOSH FILE STRUCTURE

The filesystem used by MacOS (the operating system running on Apple Macintosh computers) has a different file structure than MSDOS, UNIX or most other operating systems. On the latter, files can be seen as simple sequential unstructured streams of bytes, while Macintosh files consist of three parts:

- A *header*, containing information about the file (e.g., *true* filename, identity of the application that created and can subsequently open the file, file type (*TEXT* or more specific qualifiers), creation and last modification time, etc.

- Optionally, a *Resource fork* containing Macintosh-specific data (such as icons and other resources)

- Optionally, a *Data fork* containing the actual file data.

These three parts may be stored together in *AppleSingle* format, introduced in 1990 for Apple's version of UNIX called A/UX, and now considered Apple's official export format to other platforms. This is a sequential byte stream that can be passed to other operating systems (like DOS or UNIX). However, its direct use by applications on those platforms can be difficult, because the header and data fork are generally seen by the application as unrecognizable data. It is customary to discard the header and resource fork and pass only the data fork to applications running on non-Macintosh platforms.

Shipping Apple files over non-8-bit-clean channels

Another way to handle Macintosh files in foreign environments is to convert them into a sequence of printable ASCII characters. This operation is especially important if the files have to be transmitted over a 7-bit communications channel, such as the old X.25 links or the SMTP Internet mail protocol. Various solutions can be chosen: UUENCODEing an AppleSingle stream, using the BinHex encoding format made popular by the *StuffIt* utility, or preferably the MacMIME standard as specified by the Internet document RFC1740 (for MIME AppleSingle and AppleDouble) and RFC1741 (for MIME Binhex).

MIME AppleSingle is simply a base64 (or otherwise) encoded AppleSingle binary, labeled as *Content-Type: application/applefile*. AppleDouble is a more flexible example of the MIME *Multipart* content type. It consists of a pair of MIME bodyparts, the first being an AppleSingle file derived from the original minus the data fork, and the second an application-specific MIME type (e.g., image / gif) containing the data fork information. That allows easy separation of the data fork on non-Macintosh platforms, at the same time preserving the Macintosh-specific information.

Macintosh files and cc:Mail / Lotus Notes

cc:Mail can store Macintosh files in the Post Office in AppleSingle binary format. Clients running on various platforms will get the complete file or just the Data fork. The cc:Mail client for Windows automatically strips away header and resource fork, whereas the client for Macintosh makes good use of the complete file.

When handling Apple messages, Lotus Notes uses the MacBinary II format instead of AppleSingle. **Internet Exchange for Lotus Notes** understands this format and performs the necessary translation of AppleSingle format messages into MacBinary II for processing by Lotus Notes.

When the Macintosh client (cc:Mail or Lotus Notes) processes a non-AppleSingle attachment, it creates a dummy header and an empty Resource fork. The resulting document may or may not be readable by the original application running on the Macintosh. For example, Microsoft Excel® 5 does not recognize these rebuilt files, but Microsoft Excel 6 does and opens them normally.

Internet Exchange Macintosh file handling

From the above discussion, it is generally advisable to preserve as much file information as possible. This is the default behavior of **Internet Exchange**: outgoing cc:Mail AppleSingle and outgoing Lotus Notes MacBinary attachments are encoded in MacMime or BinHex format, and all other Apple attachment types are encoded as simple MIME or uuencoded.

For incoming messages: MacMime and BinHex produce AppleSingle for cc:Mail attachments, and the other formats produce native cc:Mail attachments (*cc:Mail Version).* For the Notes version, the Configure Options screen provides the facility to keep the files as AppleSingle, to extract the data fork or, y default, convert to MacBinary. Other formats produce native Lotus Notes attachments.

There are situations when the administrator may want to modify this behavior. For example, if many of the clients fed by the gateway are not Macintoshes, storing the header and resource fork wastes disk space. Conversely, heavily Macintosh-oriented sites may want to synthesize either AppleSingle attachments (cc:Mail environments) or MacBinary II attachments (Lotus Notes environments) out of non-Macintosh MIME messages, using parameters (Creator and Type) determined by the MIME Content-Type headers. This might be preferable to delegating the job to local mail client when the mail is read, by which time the information contained in the MIME headers is lost. This may make the difference between being able to open a spreadsheet with Excel 5 or being stuck with an unreadable document.

To allow this choice with **Internet Exchange for Lotus Notes**, there are three mutually exclusive options in the *Configure Options* screen. The first, *Keep as AppleSingle,* preserves the incoming format. The

second, *Extract data fork*, strips the header and resource fork from incoming MacMIME or BinHex messages and imports the messages as native, i.e., non-Macintosh. The third, *Convert to MacBinary* converts the file to the MacBinary format normally used to store Apple files in **Internet Exchange for Lotus Notes**.

To allow this choice with **Internet Exchange for cc:Mail**, there are two mutually exclusive options in the *Configure Options* screen. The first is *Force Native* that strips the header and Resource fork from incoming MacMIME or BinHex messages and imports the messages as native, i.e. non-Macintosh. The alternative is *Force Apple* which creates an empty Resource fork and a synthetic header (based on the MIME headers) for non-Macintosh MIME or non-BinHex incoming messages, and imports the messages in AppleSingle format. For outgoing mail, the same two options apply to each peer in the *Configure Peer* screen.

In summary:

- If primarily running Macintoshes and/or there is plenty of free disk space where the local post office resides, set *Force Apple* in the *Configure Options* screen, otherwise set *Force Native*.
- If a certain domain has mainly PCs or UNIX boxes, and/or wants to eliminate unnecessary traffic, select *Force Native* in the *Configure Peer* screen for that domain.
- If a certain domain has mainly Macintoshes, select *Force Apple* in the *Configure Peer* screen for the corresponding domain.
- In all other case, use the defaults.

Where To Find More Information

Macintosh file types

The manual for the *Fetch* utility:

http://www.dartmouth.edu/pages/softdev/fetchhelp/index.html

Information about BinHex and pointers to related documents:

http://www.natural-innovations.com/boo/binhex.html

Macintosh and MIME RFCs

MIME Encapsulation of Macintosh files - MacMIME - also contains information on AppleSingle and AppleDouble formats:

http://www.internic.net/rfc/rfc1740.txt

MIME Content Type for BinHex Encoded Files:

http://www.internic.net/rfc/rfc1741.txt

Tools For General Users

StuffIt utility to handle BinHex files, by Aladdin Systems:

http://www.aladdinsys.com/obstufex.htm

APPENDIX C
ATTACHMENT NAMING CONVENTIONS

Internet Exchange uses several different methods to communicate attachment names in outgoing messages. This allows the names of cc:Mail attachments to be preserved when being sent to users on the Internet. In a similar manner, the same methods are used to extract attachment names from incoming Internet messages.

The Name parameter

This parameter is optional in the first MIME specification RFC-1341 and is deprecated by RFC1521, but is still used by many mail programs. It is generated by **Internet Exchange** by checking the MIME configuration information available through the *Configure MIME* screen. The parameter is appended to the MIME *content-type* header. For example:

Content-Type: image / gif; name="world.gif"

For incoming messages, any present name parameter is used to name the corresponding attachment when imported into cc:Mail. If absent, a unique filename *MIMEnn.ext* will be generated, *nn* being a small decimal number, and *ext* an extension determined by the MIME mappings or, if these do not help, the default extension *raw*. For example:

Content-Type: application / octet-stream; name="mime01.raw"

The content-disposition header

This header is defined in RFC1806 and is an alternative way of defining attachment names. For example:

Content-Disposition: attachment; filename="test.doc"

This specifies that the MIME bodypart is an attachment, as well as its original filename. For incoming messages, this information is again used to generate a name for cc:Mail attachments.

Macintosh header information

For incoming attachments in either AppleSingle or BinHex format, the attachment name will be taken from the Macintosh header resource. This takes precedence over either of the above methods of attachment naming.

APPENDIX D
MIME

INTRODUCTION

MIME, which stands for Multipurpose Internet Mail Extensions, is a standard that extends the functionality of basic Internet mail (RFC-822 message format) to allow additional types of message contents to be transported by Internet mail services.

The previous standards, RFC-821 (SMTP) and RFC-822 (Text message format) were published in 1982 and have been very widely implemented, even among non-Internet mail systems. However, these standards impose a very strict limitation on what can be included in an Internet mail message: the content is limited to 7-bit ASCII text (with lines shorter than 1000 characters). MIME permits this to be extended to include message contents such as:

- Images and graphics files
- Text in non-ASCII character sets
- Text in fonts
- Text with arbitrary-length lines
- Sound and video messages or files
- Multi-part messages
- Binary and application-specific files
- References to documents stored elsewhere

In general, these content objects are (when required) encoded to permit them to travel through existing Internet mail systems. MIME messages are downward-compatible with RFC-822 and will interoperate seamlessly even with mail systems that have not been upgraded to special MIME capabilities. This means that MIME messages can be transported through the 7-bit ASCII path provided by SMTP; that MIME messages will not cause RFC-822 mail user agents to break; and that MIME mail user agents will be able to handle normal RFC-822 messages as well. (It is also possible for sets of hosts that are MIME-capable to communicate using an extension to SMTP that allows some MIME messages to be transported without encoding. This is called ESMTP and is discussed below.)

Conceptually, MIME works by defining some additional RFC-822-type headers that describe the structure of the message. The single message body of RFC-822 messages is extended to multiple message bodies in MIME, each of which can contain a different content type. And each content type can be either transported in native form (if compatible with RFC-821 and RFC-822) or encoded to be compatible.

MIME HEADER FIELDS

The additional header fields defined by MIME are the following:

MIME-Version	Version of the MIME standard used by the message. Currently 1.0.
Content-Transfer-Encoding	Method used to encode the content data for transport
Content-Type	Data type of the contents. There are numerous subtype and option fields

Content-Description	Description of the message body data
Content-ID	Unique identifier (similar to the Message-ID) for message body parts

MIME was designed to be extensible; the set of content types, subtypes, and options is easily extensible, as well as the set of transfer encodings. The MIME standard (RFC-1521) requires that new values for these basic types be registered with the Internet Assigned Numbers Authority (IANA) to prevent confusion and name collision.

When a MIME message contains a single message body part, the main (RFC-822) message header will contain the required Content-Type and Content-Transfer-Encoding headers with the appropriate value. The RFC-822 message body will contain the MIME message body, either as a simple text message, or in the specified encoding. A simple MIME message with a message body with a Content-Transfer-Encoding of "7-bit" (the default) and of Type "text/plain" will simply appear as an RFC-822 message.

When a MIME message has multiple message bodies, however, the Content-Type header in the RFC-822 message header will specify

```
Content-Type: multipart/mixed;
      boundary="unique-boundary"
```

This means that the individual message bodies will be set apart with the string

```
--unique boundary
```

alone on a line. Each message body must then contain its own Content-Type header that defines the type and subtype of the message body part. It is possible to nest multipart messages (as long as the nested levels use uniquely defined boundaries).

This simple example multipart message consists of two message body parts:

```
From: milo@bloom-county.outland.com (Milo)
```

```
To: charlie-brown@peanuts.comic.com (Charlie
      Brown)
Subject: Simple example
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="unique-
1a7GHq5cm"

This is a preamble to the message, ignored by MIME mail
user agents.

By convention a message to non-MIME user agents is
placed here explaining that this is a MIME message.

--unique-1a7GHq5cm

This is part 1 of the message.  There was no Content-
type or Content-transfer-encoding header, so it
defaults to type "text/plain" and encoding "7bit".

--unique-1a7GHq5cm
Content-type: text/plain; charset=US-ASCII

This is part 2 of the message.  It is explicitly typed
as "text/plain".
Its default encoding is also "7bit".

--unique-1a7GHq5cm
This area is the message epilogue, also ignored by MIME
mail user agents since it is beyond the boundary of the
last message part.
```

There are multipart subtypes other than "mixed", indicating other ways that the multiple message bodies are to be interpreted.

Content Types

There are 7 top-level content types defined in the MIME standard. Additional supported content types are expected to be included by defining additional subtypes of the top-level types. The seven top-level types and their currently defined subtypes are:

Type	Subtype	Remarks
application	(various)	Binary data specific to an application. A full list of subtypes can be found in RFC-1521.
Audio	basic	8-bit ISDN u-law, single channel, 8000 Hz

image	gif	GIF (Graphics Interchange Format)
	jpeg	JPEG (Joint Photography Experts Group) format
message	rfc822	Encapsulated RFC-822 message, with headers
	partial	Partial message, with identifier and part number. Used to fragment and reassemble large MIME messages
	external-body	Reference to a document or file stored elsewhere, with access method and identifier
multipart	mixed	Multiple independent message body parts, separated by unique boundary, designed to be viewed serially
	alternative	Same as multipart/mixed, but each part is an alternative version of the same information; the mail user agent should choose the most appropriate type

	parallel	Same as "multipart/mixed", but the parts are meant to be presented simultaneously, as in a multimedia message (e.g., graphics plus audio)
	digest	Each part is an RFC-822 mail message, collected into a digest
text	plain	Plain, unformatted text; default character set is US-ASCII
	richtext	A simple marked-up formatting language for text, defined in the standard
video	mpeg	MPEG (Motion Picture Expertise Group) format video
x-*typename*	(as defined)	Privately defined content type used between cooperating mail systems; analogous to RFC-822 "X-" headers

The Name parameter

This parameter was optional in the first MIME RFC (RFC-1341) and is deprecated by RFC1521, but is still used by many mail programs. Its purpose is to suggest a filename for the attachment, in case the user decide to save it to disk. When present, it is used by **Internet Exchange** as name of the cc:Mail file attachment created from a MIME bodypart. If absent, a unique filename *MIMEnn.ext* will be

generated, *nn* being a small decimal number, and *ext* an extension determined by the MIME mappings or, if these do not help, the default extension *raw*.

CONTENT TRANSFER ENCODINGS

As shown above, a number of the content types possible in MIME are represented in their native format by binary (8-bit) data, which cannot be transported by SMTP or represented in a standard RFC-822 message.

In order to permit binary data to be transported over standard mail systems, MIME supports a number of encoding formats that reduce the binary data to a manner that is acceptable for transport. This is done through the Content-transfer-encoding header field. The values are as follows:

base64	Basic binary encoding — three 8-bit octets are represented as four printable ASCII characters. Lines are limited to 76 characters
quoted-printable	Lines of mostly printable text, with non-printable characters escaped using "=" as a quote
8bit	Unencoded 8-bit data that is line-oriented (less than 1000 characters per line).
7bit	Unencoded, plain 7-bit characters, less than 1000 characters per line. This is the default format.
binary	Arbitrary-format unencoded binary, no specified line length
x-*encoding*	Privately defined encoding used between cooperating mail systems

Note that 8bit and binary are in fact unencoded forms, and generally cannot be used as such using SMTP transport, except as

noted below. 7bit is also unencoded, and is the default format for simple text messages.

As noted above, the set of subtypes is expected to grow in the future; consult the STD version of the MIME RFC for the currently defined subtypes.

OTHER MIME HEADERS

MIME also defines two other headers: Content-ID and Content-Description. These fields are optional. Content-ID is used to label a message body, where it may be useful to refer to it elsewhere, such as in another header field or message body. Content-Description merely associates a text description of the subject or contents of a (possibly non-textual) message body; this could be used by a mail user agent to display a caption for an image, for example.

EXTENSIONS TO SMTP (ESMTP)

While MIME provides a method of encoding arbitrary types of message contents for transport through Internet standard mail systems, it is also desirable for systems with the capability of exchanging binary data in mail messages to be able to do so (to avoid the overhead of encoding and decoding of 7-bit representations of binary data), in a way that is compatible with the MIME standard.

The extensions to SMTP defined in RFC-1651 are optional and are not required to be implemented by Internet mail systems. Basically, they provide a framework for systems that use various enhancements to be able to identify themselves to each other and discover which extended capabilities they mutually possess. This is similar to the options negotiation in the TELNET protocol. The extended capabilities discussed in the RFC include a maximum

message size negotiation and a negotiation for use of 8-bit MIME transport. The 8-bit MIME transport itself is specified in RFC-1426.

If an ESMTP-capable SMTP client wishes to initiate an ESMTP session with a server, it uses the new EHLO command (instead of HELO) to identify itself at the outset of the connection. An ESMTP-capable server will respond to the EHLO command with a response consisting of a list of extended commands (beyond the set required in RFC-821) that it supports. Obviously, early non-ESMTP-capable servers will not even recognize the EHLO command, and will return an "unknown command" error. In this case the client will know that the server is not ESMTP-capable, and the session will continue as a normal SMTP session.

The initial set of extended commands defined by RFC-1651 are:

SEND	Send message to terminal
SOML	Send message to terminal, or mail
SAML	Send message to terminal and mail
EXPN	Expand mail list or alias
HELP	Return a help message
TURN	Client and server exchange roles

Note that all of these were originally defined in RFC-821 as SMTP commands, but were not widely implemented. This standard makes them optional extensions.

RFC-1426 defines an optional extension named 8BITMIME, which can be used if the ESMTP server is able to support 8-bit binary mail transport. The client, upon receiving the 8BITMIME keyword in response to a EHLO command, may send an 8-bit MIME message by extending the SMTP MAIL command with the BODY parameter (with a value of 8BITMIME). Without the BODY parameter, or if it has the value 7BIT, the type will default to 7-bit ASCII text.

The following example from RFC-1426 shows use of 8BITMIME in an ESMTP session:

```
Server: <wait for connection on TCP port 25>
Client: <open connection to server>
Server: 220 dbc.mtview.ca.us SMTP service ready
Client: EHLO ymir.claremont.edu
```

```
Server: 250-dbc.mtview.ca.us says hello
Server: 250 8BITMIME
Client: MAIL FROM:<ned@ymir.claremont.edu>
BODY=8BITMIME
Server: 250 <ned@ymir.claremont.edu>... Sender and 8BITMIME ok
Client: RCPT TO:<mrose@dbc.mtview.ca.us>
Server: 250 <mrose@dbc.mtview.ca.us>... Recipient ok
Client: DATA
Server: 354 Send 8BITMIME message, ending in CRLF.CRLF.
           ...
Client: .
Server: 250 OK
Client: QUIT
Server: 250 Goodbye
```

APPENDIX E
TCP/IP

WHAT IS TCP/IP?

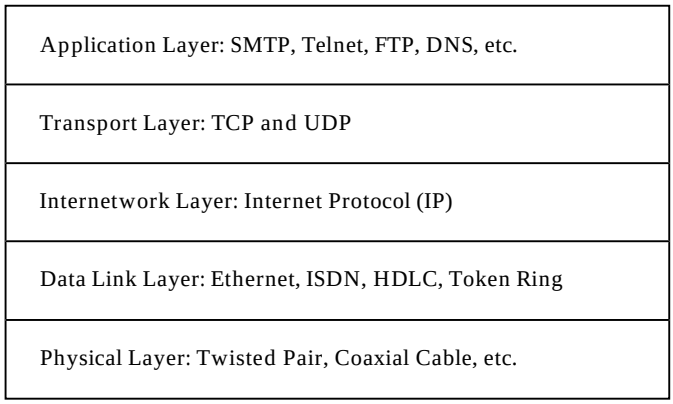
TCP/IP (which stands for Transmission Control Protocol/Internet Protocol) has become the most widely used network protocol suite in the world. It is the basis for the global Internet, which by early 1994 consisted of approximately 22,000 connected networks with 1.75 million hosts and about 13 million users. While the Internet can support a number of other networking protocols, TCP/IP is used by the vast majority and forms the basis for Internet routing and addressing.

A network protocol suite is a set of individual protocols (communication standards) that have been designed to work together to support a range of network applications. Each protocol in the suite handles a different part of the entire networking scheme. So called low-level protocols handle matters such as routing or creating virtual circuits, while higher-level protocols may handle data presentation or specific network applications like e-mail or file transfer. A protocol suite is sometimes referred to as a "stack" — a reference to diagrams that illustrate the suite as a stacked set boxes in which protocols performing similar functions are grouped into layers.

TCP/IP is now supported on almost every hardware platform and operating system. In the MS-DOS and Microsoft Windows user community, acceptance was initially slow because of the availability of less complex, turnkey solutions. However, there are now a number of easy-to-install commercial packages that implement TCP/IP for DOS and Windows systems, and are compatible with the WINSOCK standard. Some of these include Novell LAN

WorkPlace for DOS, Frontier Technology's Super-TCP, and The Wollongong Group's PathWay.

A complete TCP/IP implementation can be thought of as a "stack" with five levels, of which only the top three are provided by the TCP/IP suite itself.



The Physical layer is essentially merely the actual cabling (or wireless carrier) that carries the electrical signals that are recognized by network equipment as data. It is not part of the protocol suite, but TCP/IP networks are carried on a very wide variety of physical carriers, including twisted-pair cable, coaxial cable, fiber-optic cable, microwave, etc.,

The Data Link layer, sometimes (confusingly) called the Network layer, are a collection of low-level protocols appropriate to various physical cabling schemes. Examples include Ethernet protocols for various coaxial cable and twisted-pair schemes, FDDI for fiber-optic cabling, X.25, V.35 and HDLC for high-speed serial lines, ISDN over circuit-switched telephone lines, token-ring and broad-band protocols, etc. These are also not part of the TCP/IP suite itself, and can be used (often simultaneously) by other network protocol suites, such as NetWare IPX/SPX, DECnet, etc.

The Internetwork layer is the most important to the TCP/IP suite. This is where overall Internet addressing and routing are handled by IP (Internet Protocol).

The Transport layer is concerned with data integrity and consistency. TCP/IP provides two protocols -- TCP (Transmission Control Protocol), which assures a reliable communication stream between processes on two network hosts, with retransmission of lost data, presentation of data packets in the correct order, etc.; and UDP (User Datagram Protocol), which simply transmits packets of data without guarantee of delivery or ordering.

The Application layer is where protocols that implement specific network services are grouped. Most complex and interactive applications use TCP, which will handle the details of reliability and ordering of the communications stream. Examples of TCP-based application protocols include Telnet (the virtual terminal protocol), FTP (File Transfer Protocol), and, of course, SMTP (Simple Mail Transport Protocol). Examples of UDP-based applications include Domain Name System (DNS) queries and the Sun Network File System (NFS) which is the most widely used standard for file sharing on workstation networks.

IP, TCP, and UDP, along with the supplementary protocols used for network control and routing in TCP/IP, will be described below.

INTERNET ADDRESSING

Each system (known as a "host") connected to the Internet has a unique IP address. (Actually, hosts may have more than one address, since they may be connected to more than one physical network, and addresses are actually assigned to the network interface rather than the host CPU.) Unlike addressing schemes for local-area networks, or hardware-based address schemes, IP addresses are assigned by a central numbering authority. This is to ensure the uniqueness of IP addresses in the global Internet, and to make sure that packets will be routed to the correct site network from other parts of the Internet. Obtaining IP addresses for your Internet-connected systems is handled in different ways in different

organizations. Some large organizations have been assigned a large "chunk" of IP addresses that are allocated internally by an administrative authority. Other organizations use addresses allocated to them by their Internet service provider. Still others will need to arrange for their own block of IP addresses directly. This manual assumes that you have already obtained an IP address assignment for the systems on which you will operate **Internet Exchange** gateways.

IP addresses are 32 bits long, divided into four 8-bit segments known as octets. Addresses are conventionally written in "dotted-decimal" notation, with each octet expressed as a decimal number, with dots separating each octet. (You may see IP addresses written in hexadecimal or undotted decimal in some programs, mostly involved with installing network adapters or drivers. This is relatively uncommon, however.) The leftmost octet of the address are the high-order 8 bits of the address, followed by the next 8 bits, and so on, with the rightmost octet being the lowest-order 8 bits of the address.

Examples of IP addresses are 192.12.17.2, 36.3.150.9, and 190.9.200.254.

IP Address Classes

Since the Internet is not a single network but a "network of networks," part of the IP address designates a *network number* and part a *host address* on that network. In an attempt to strike a balance between networks of different sizes on the Internet, the IP addressing scheme defines several *classes* of IP addresses. The underlying idea of address classes was to efficiently use the IP address space by recognizing that there will be a very small number of huge networks, a reasonably large number of medium-size networks, and a huge number of very small networks. In addition, provision has been made for two special types of addressing, broadcasts and multicasts.

Class	Address Range	Number of networks in class (theoretical)	Possible hosts per network (theoretical)
A	0.0.0.0 — 127.255.255.255	128	16,777,216
B	128.0.0.0 — 191.255.255.255	16,384	65,536
C	192.0.0.0 — 223.255.255.255	2,097,152	256
D	224.0.0.0 — 239.255.255.255	N / A	N / A
E	240.0.0.0 — 255.255.255.255	N / A	N / A

The number of networks and hosts is shown as "theoretical," since in the actual Internet standards the numbers 0 and 255 in each octet are always reserved for special uses and are not available for use in normal host addresses.

Addresses in classes A, B, and C are used for normal host-to-host communications. Class D addresses are reserved for *multicasting*, that is, messages sent from one host to a group of hosts. Applications for multicasting include routing messages, network status messages, conference calls, and delivery of real-time audio and video data across the Internet. Class E addresses (with one exception) are reserved for future applications. (The exception is the address 255.255.255.255, which is a *broadcast* address. Broadcast addresses are discussed below.)

IP Subnet Addressing

Large organizations are usually assigned blocks of IP addresses that are allocated internally according to an administrative plan. To make IP addressing and routing easier inside a large organization network, it is possible to subdivide a large IP address space into a number of *subnets*. Subnets have the characteristics of networks for internal routing purposes, but the collection of subnets appears as one large network to hosts outside the organization.

Subnet addressing is achieved by taking the host number part of an IP address, and further dividing it into a subnet number and a host number. For example, many Class B networks are divided into (up to) 254 subnets, each of which can have up to 254 hosts each. (This is equivalent to having obtained assignment of 254 contiguous Class C networks, but is easier to administer, since they appear to be one large network to the outside world.)

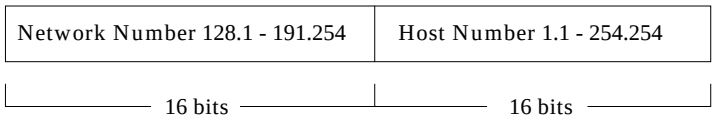


Figure B.1 : an unsubnetted Class B address

By using the third octet of the address as a subnet number, the organization's numbering authority can assign subnets to individual LANs that are connected by internal routers.

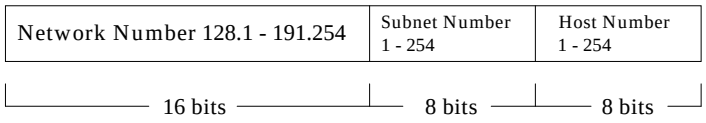


Figure B.2: a Class B address with 8-bit subnets

The value of subnets, besides ease of administration, is in simplification of network routing from outside the organization. Without subnets, routing information for each of the organization's internal LANs would have to be maintained by the Internet trunk routers. Using subnets, however, a single route for all the organization's subnets is the only one that needs to be known outside the organization.

When installing network software on a host in a subnetted environment, it is necessary to enter the appropriate *subnet mask* so that the host's address is properly interpreted. IP uses the subnet mask to determine which parts of the IP address should be treated as the network/subnet number and which as the host number. In a subnet mask, 1-bits are used for the network/subnet number, and 0-bits as the host number. Thus an unsubnetted Class B network

would have the subnet mask 255.255.0.0 (upper 16 bits are network number, lower 16 bits are host number), while a Class B network using the third octet of the address as a subnet number would have the mask 255.255.255.0 (upper 24 bits are network/subnet number, lower 8 bits are host number). It is not necessary for the number of bits used for the subnet to be evenly divisible by 8. Organizations can declare larger or smaller subnets as necessary; however, 8-bit subnets are by far the most common and make dotted-decimal addresses easy to interpret. In the typical Class B subnetted scheme with a subnet mask of 255.255.255.0 the address 128.32.100.5 would be read as "Network 128.32, subnet 100, host 5."

Broadcast addresses

A host may often need to send a particular message to all the hosts on its local network, or all the hosts on a larger organization network. This is known as a *broadcast*. Uses for broadcasts include network status messages, routing messages, requests for a host's own IP address during rebooting, etc.

The basic broadcast destination address is 255.255.255.255, which means "all hosts on this local network". (Broadcast messages are not forwarded by routers, except for subnet broadcasts.) In a subnetted environment, the broadcast address 128.32.255.255 would mean "all hosts on all subnets of network 128.32." This broadcast would be carrier by internal routers to all subnet LANs on network 128.32. In practice, however, broadcasting is usually limited to a local network.

In earlier implementations, a host number of all 0-bits (e.g., 128.32.0.0) was used as the broadcast address. Though the standard has changed to a host number of all 1-bits (e.g., 128.32.255.255), most current implementations recognize the earlier form as well.

Future IP addressing issues

The IP 32-bit address model has proven to be very flexible and has served the Internet well, even during its recent explosive growth. However, it has become clear that for some purposes the current system will be inadequate in the future. One of the most pressing

problems is the rapid increase in the number of individual networks in the Internet. Since IP routing requires that Internet trunk routers exchange nearly complete information about the gateway routers for each site, the burden of doing so may become unmanageable in the future. In addition, some IP address types — notably Class B addresses — are in danger of becoming scarce because of their finite availability. A number of solutions for these problems have been proposed, some of them requiring replacement of IP with another protocol at the Internetwork layer; some provide for extension of the 32-bit address space; still others propose changes to the IP routing model. Any change that is made will need to provide adequate backward compatibility for the very large number of hosts that cannot easily adopt a new protocol implementation because of vendor or service provider issues.

While waiting for the implementation and deployment of IP v6 that sports a vastly enlarged addressing space, the most promising stopgap solution seems to rely on the so-called classless addressing (CIDR: Classless Inter-Domain Routing), as documented in RFC1517/1518/1519/1520. CIDR is based on the suppression of the concept of "network class" and, besides allowing network sizes more closely tailored to real needs, greatly simplifies the routing aggregating groups of old networks under "prefixes" of variable bit length. For example, IMA's prefix 202.75.0.0/18 includes four "classic" class C networks from 202.75.0.0 to 202.75.3.0; each route mentioning it replaces four routes in the old-style arrangement. This addressing space may be subnetted under the exclusive control of the local administration, without burdening the backbone core routers. With shorter prefixes, of course, the savings are even more impressive.

THE TCP/IP PROTOCOLS

Internet Protocol (IP)

The key feature of IP is its ability to route packets containing arbitrary higher-level protocol data throughout an internetwork that may consist of many different kinds of data-link and physical layers. This is done by *encapsulating* a transport-layer (i.e., TCP or

UDP message) into an IP packet, adding sufficient header information to allow the packet to be correctly routed to a destination, and then preparing whatever framing information is necessary for the data-link layer to process the packet, and finally handing it off to the driver for the data-link layer implementation (e.g., Ethernet).

An important function of IP beyond message encapsulation is fragmentation and reassembly of packets, where the size of the encapsulated message is larger than that which can be handled by the underlying data-link layer network.

An IP packet consists of a header, the fields of which are shown below, and data, which is an arbitrary-length (up to 64K bytes) bit string consisting of a message prepared by a higher-level protocol.

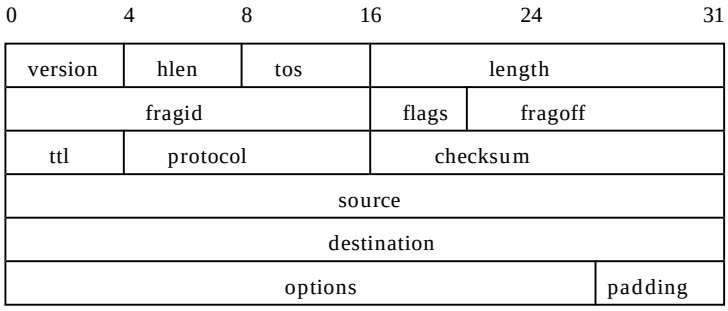


Figure B.3: IP packet header

The meaning of the header fields is shown below.

version	IP (protocol) version number
hlen	Header length in 32-bit words
tos	Type of service — usually unused
length	Length of entire packet, including header, in bytes

fragid, flags, fragoff	Fragment ID, fragment flags, and fragment offset — used for fragmentation and reassembly of large packets
ttl	Time-to-live — maximum lifetime of this packet, in seconds. Decremented by each router the packet passes through; effectively a maximum hop count, to prevent looping.
protocol	The protocol responsible for the encapsulated message, e.g., TCP, UDP, or others
checksum	A 16-bit checksum of the header only. Other error checking is performed by higher-level protocols on the encapsulated data field of the packet.
source	IP address of the source (originator) of the packet
destination	IP address of the ultimate destination of the packet
options	Various IP processing options, including source routing, route recording, time stamping, and security. Rarely used except for special purposes.
padding	Padding to bring the header to an even multiple of 32 bits

After IP receives a message from a transport-layer protocol, encapsulates it into an IP packet, and creates the IP packet header, IP determines which network interface will be used (possibly by consulting a routing table), then the packet is *framed* in the format appropriate for the data-link layer of that interface, and passed to a driver that arranges for submission of the packet onto the physical network.

In this process, the IP packet may be fragmented in order to comply with the maximum frame size of the data-link layer. While the maximum size of an IP packet is 64K bytes (because of the 16-bit

field used to store the packet length), data-link layer protocols may allow only shorter frames; for example, the maximum transmission unit (MTU) of an Ethernet network is 1500 bytes (excluding headers).

In order to send a large IP packet through a network with smaller MTU's, IP will fragment the packet into two or more packets, and use the *fragid*, *flags*, and *fragoff* header fields to identify the size and order of the fragmented packet. The IP implementation receiving the packet holds the fragmented packets in a reassembly queue, and using the information in the header, will re-assemble the packets before presenting them to a higher-level protocol for processing.

Fragmentation and reassembly of packets is a relatively costly operation. IP uses various strategies to avoid fragmentation when sending packets across networks where the MTU is known in advance, and reducing packet size to a known minimum where the destination is many hops away.

Support Protocols for IP

Internet Control Message Protocol (ICMP)

ICMP is a support protocol for IP that is implemented by encapsulation into an IP packet. It is used for exchanging network control and informational messages among hosts and routers, and for diagnosis and debugging of network problems. Each ICMP packet contains a *type* and *code* field that specify particular queries, responses, or conditions. Some frequently used ICMP packet types are the following:

echo request, echo reply	The echo request is a packet with a small amount of data directed at a particular host, with a request to echo it (send it back); the echo reply contains the return data.

destination unreachable	Sent by a router to indicate the destination of an IP packet is not available (no route)
redirect	Sent by a router to indicate a better route to the destination host
source quench	Indicates network congestion or overflow; directs the source (sender of packets) to decrease the rate of transmission
time exceeded	Indicates that a packet's *ttl* has expired, usually because of a routing problem or loop

Address Resolution Protocol (ARP)

ARP is used to discover the mapping between IP addresses and hardware-based addresses of an underlying data-link layer network, such as Ethernet. IP addresses are assigned by a central numbering authority, and are implemented in software. However, some data-link network schemes, including Ethernet, token ring, and FDDI, use addresses that are embedded in network adapters. When IP sends a packet to another host on the same local network, it needs to construct a frame to be given to the lower-level network driver. Part of this frame is the hardware address of the destination IP host.

In order to obtain the hardware address of the destination host, the sending host looks the address up in its local *ARP cache* (table in memory of address mappings), and if it is not found, creates an ARP request packet, frames it with the proper data-link layer header, and broadcasts it to all hosts on the local network. The ARP packet contains fields for the sender's IP and hardware address, and the recipient's IP and hardware address. (The recipient's hardware address, being unknown, is set to all zeros.)

When each host receives the broadcast, it matches its IP address with the destination address, and if it is the same, it fills in its

hardware address in the recipient field, and sends the packet back to the sender address. The sender receives and decodes the packet and updates its ARP cache.

Reverse Address Resolution Protocol (RARP)

RARP is used almost exclusively for diskless workstations or intelligent terminals to discover their own IP address since they do not store it between operating sessions. In this case, a host will know its own hardware address (which is embedded in a ROM, for example), and needs to learn its IP address in order to receive a bootstrap image and engage in further IP protocol traffic.

Use of RARP requires setting up a RARP server that contains hardware address to IP address mappings. RARP packets are analogous to ARP packets — that is, the sending host will fill in the fields of the packet, frame it with the proper data-link layer header, and broadcast it on the local network.

Any RARP server can accept and decode the packet, fill in the requested IP address from its table, and return the packet to the sender.

IP ROUTING

Routing in IP is done on a per-network basis, that is, IP uses only the network number portion of an IP address to make routing decisions. This makes routing relatively simpler, since there is no need to keep a list of the location of all hosts in an internetwork (which would be practically impossible in the global Internet).

The basic element of IP routing is the routing table kept by each host, which is basically a list of network numbers and the IP address of a gateway (router) to which packets for that network should be sent. There is also usually a third field, a set of flags that indicate the status of the network and whether it is directly connected to the sending host.

For each IP packet to be sent, the sending host looks up the network number of the destination in the routing table, and determines

whether the network number is that of the local, directly connected network. If so, the packet is sent directly to the destination (possibly using ARP to discover the hardware address of the destination on the local network). If the network number is not local, but there is an entry for it, the packet will be sent to the gateway listed for that network. Finally, if there is no entry matching the destination network number, the packet is discarded and a failure message is returned.

This basic routing algorithm is used by all IP hosts and routers. However, in practice, most hosts have a very small routing table, consisting of only three entries: an entry for itself (usually known as the "localhost" or "loopback" address; this is used for debugging and some software applications); an entry for its directly attached local network, for which the gateway field will be its own IP address — indicating that the packet should be delivered directly via the data-link layer; and an entry labeled "default," which means all other packets that are non-local, for which the gateway field will be the IP address of the router that connects the local network to the Internet.

Routing Protocols

In the early days of the Internet, overall routing was managed by a set of core routers, known as the *mailbridges*, which contained routing table entries for every known connected network in the Internet. Every site network communicated directly with these core routers and propagated their routes throughout the Internet; some sites with limited capacity used the core routers as default routers. Because of the dramatic increase in the size of the connected Internet, it is no longer possible to maintain this method of routing.

The present Internet is divided into a collection of Autonomous Systems (AS) which are a set of routers that are under a single administration and exchange routing information among themselves using a specific routing protocol. The routing protocol shared by routers inside an AS is called an Interior Gateway Protocol; (IGP). Examples of IGPs are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).

Each AS has one or more exterior routers, which communicate with routers belonging to another AS. This involves the use of Exterior Gateway Protocols (EGP). Examples of EGPs are the original Exterior Gateway Protocol itself (EGP) and Border Gateway Protocol, version 4 (BGP4).

Routing Information Protocol (RIP)

RIP is a simple routing protocol appropriate for a small network that is stable, homogeneous, and having a simple topology, such as a LAN router with two or more external WAN connections. RIP is a "distance vector" protocol, that is, it maintains a "cost" or "distance" metric for routes to distant networks.

While RIP supports requests for routing tables from remote routers, it is most commonly used as a system of updates whereby routers broadcast their routing tables in a form consisting of a network number and a distance metric. This distance metric is a hop count, that is, the number of intermediate routers through which a packet to that network must pass. Routers and hosts receiving RIP updates simply update their tables with this new information, and use the hop count to determine a "best" route to each network.

Open Shortest Path First (OSPF)

OSPF is suitable for large, complex autonomous systems that need to exchange routing information where network topology changes rapidly, or where there are multiple, different-cost paths to various locations. OSPF is relatively new to the Internet (deployed 1991) and is not in as wide use as RIP.

Routers using OSPF receive routing updates that include link-state and bandwidth information as well as distance vectors. This information is used to build internal graphs of internetwork topology that are used to generate shortest-path network routes.

OSPF also allows the definition of "routing areas" within an AS — in some ways the analog of IP subnets. This hides the details of complex routing inside parts of an AS.

Unlike RIP, OSPF requires the resources of a high-capacity dedicated router and therefore is usually only used when required by the complexity or criticality of a network.

Exterior Gateway Protocol (EGP)

EGP is a simple "reachability" protocol that allows AS routers to exchange information about which networks can be reached through their respective AS gateways. In EGP, there is a "core" AS that communicates directly with each other AS (which are known as "stubs"). Each stub AS supplies the core with information indicating what networks it handles traffic for, and the core redistributes this information to each other stub.

Border Gateway Protocol (BGP4)

BGP is an extension to EGP that allows for AS's to be connected in other than a strict core-stub topology. The EGP "core" is redefined as a "Transit AS", that is, a network (or collection of networks) that permits transit traffic — connections where neither the source nor destination is on that AS. In addition, AS's can be stated to be either stubs or multi-homed; this allows for more complex reachability routing information.

The most important feature of BGP, besides additional robustness, is that it permits an AS to accept or reject transit traffic. This is used to implement so-called *policy-based routing*, where IP routing decisions are made on externally described policy factors such as type of traffic, as well as strictly on reachability and best-path factors.

TRANSPORT-LAYER PROTOCOLS

Transmission Control Protocol (TCP)

TCP is the most heavily used of the transport protocols in the TCP/IP suite. A TCP connection is a reliable, sequenced, bi-

directional data stream between processes on two Internet hosts. This means that lost data will be retransmitted, the messages are guaranteed to arrive in the proper order, and communications can take place in either direction.

A TCP message is encapsulated inside an IP packet, and routed to its ultimate destination by IP, locally or through an arbitrary number of routers. The TCP message consists of a header, shown below, and data, which is a stream of bits prepared by (and meaningful to) an application-layer protocol (such as FTP or Telnet).

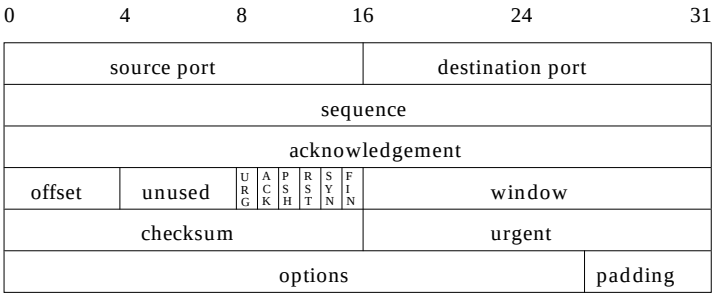


Figure B.4: TCP packet header

The meaning of the header fields is shown below.

source port	Port number of the source application. A list of port numbers used in TCP is in Figure B.5
destination port	Port number of the destination application
sequence number	Sequence number of this segment — used to assure correct ordering
acknowledgment number	Contains next segment number which is also used as acknowledgment of previous segments
data offset	Location of the data portion of packet (e.g., length of TCP header) in 32-bit words

URG bit	Notes “urgent data” is present
ACK bit	Notes Acknowledgment field is valid
PSH bit	Causes this data to be pushed through to application instead of buffered
RST bit	Causes connection to be reset
SYN bit	Causes sequence numbers to be resynchronized
FIN bit	Notes end of source data stream
window size	Size of flow control window
checksum	16-bit header and data checksum
urgent pointer	Location of “urgent data” inside packet
options	TCP options including maximum segment size, security, etc.
padding	Padding to next multiple of 32 bits.

The application on the originating host (called the client) and the application on the destination host (called the server) must establish a *connection* in order to communicate using TCP. This is done by a somewhat complex initiation procedure that sets up the sequence numbers, window size, and other connection parameters. First, the client sends a message with the SYN bit set and includes a sequence number (this is generated by software using a real-time clock, to prevent sequence numbers from being reused too often).

The server accepts the SYN message, replies with a SYN message, includes its own sequence number, and sets the ACK bit as well. The client and server then negotiate other parameters of the connection, such as the window size (number of unacknowledged packets-in-flight that are permitted), and begin communicating

according to whatever higher-level protocol data is being exchanged. During the connection, each side continues to increment the sequence number of their packets, and issues acknowledgments for packets it has received; in this way lost data will be recognized and re-transmitted after a time-out. For the purposes of flow control, either side may re-set the window size to more efficiently react to the speed and congestion of the network connection.

Finally, when one side proposes ending the connection, it sends a message with the FIN bit set; communication continues until the other side sends a FIN message as well.

TCP is probably the most complex protocol of the TCP/IP suite, because efficient network usage, high throughput, and reliability all depend on TCP's flow control and retransmission algorithms. For additional information on TCP specifics, see RFC-793.

Protocol	Port No.	Service
tcpmux	1	TCP port service multiplexer (RFC-1078)
rje (old)	5	Remote job entry (former)
echo	7	Echo (used for testing)
discard	9	Discard (used for testing)
systat	11	System status & users
daytime	13	Time of day
netstat	15	Network status
chargen	19	Character generator
ftp-data	20	File Transfer Protocol — data channel
ftp	21	File Transfer Protocol — control channel
telnet	23	TELNET protocol
smtp	25	Simple Mail Transfer Protocol
time	37	Time server
whois	43	NICname server
domain	53	Domain Name Service

gopher	70	Gopher information service
rje	77	Remote Job Entry
finger	79	Finger (user information) service
link	87	Terminal linking
supdup	95	SUPDUP (enhanced) Telnet protocol
hostnames	101	NIC hostname service (old)
x400	103	X.400 messaging
x400-snd	104	X.400 messaging
pop2	109	Post Office Protocol, Version 2
pop3	110	Post Office Protocol, Version 3
sunrpc	111	Sun Remote Procedure Call protocol
nntp	119	Network News Transport Protocol (Usenet)
ntp	123	Network Time Protocol
news	144	Network-extensible Window System
xdm	177	X Display Manager protocol
wais	210	Wide-Area Information Service
exec	512	Remote program execution (UNIX rexec)
login	513	Remote login (UNIX rlogin)
shell	514	Remote shell (UNIX rsh)
printer	515	Printer service (UNIX lpd)
courier	530	Courier remote procedure call protocol
uucp	540	UUCP over TCP

Figure B.5: TCP port assignments (partial list)

User Datagram Protocol (UDP)

UDP is a connectionless protocol that is useful when an application does not require 100% reliable delivery and sequencing of packets. This could be for one of two reasons — first, where the application performs error checking and sequencing itself, and arranges for re-transmission of lost data, and secondly, where integrity of every single packet of a voluminous stream is not needed. Examples of the former include the Network File System (NFS) where NFS itself employs numerous reliability and integrity checks; examples of the latter include broadcast-stream applications like voice or video distribution. Other services using UDP include Domain Name System (DNS) queries and replies, RIP routing updates, and services based on Sun's Remote Procedure Call (SunRPC) interface.

The UDP packet header is very simple compared with TCP. UDP also uses the abstraction of port numbers to identify various services. Since port numbers exist on a per-protocol basis, it is possible for UDP and TCP to have the same port number for the same or even a different service. As can be seen in Figure B.5, a number of UDP port numbers are the same as TCP port numbers; in this case, implementations of a protocol can choose whether to use TCP or UDP for the application. (For example, while DNS queries normally use UDP, most implementations can be configured to use TCP if requested by the user.)

The UDP header has only four parts, analogous to the same fields in TCP.

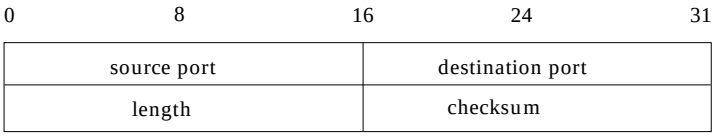


Figure B.6: UDP packet header

The meaning of the header fields is shown below.

source port	Port number of the source application. A list of port numbers used in UDP is in Figure B.7
destination port	Port number of the destination application
length	Length of the packet, including data
checksum	16-bit checksum of header and data

In practice, the UDP header source port field need not be filled in, since (as a connectionless protocol) there is no requirement that the destination's UDP server process reply to the source. Additionally, the checksum is optional and for the sake of further streamlining may not be decoded and computed by the destination.

Protocol	Port No.	Service
echo	7	Echo (used for testing)
discard	9	Discard (used for testing)
daytime	13	Network status
chargen	19	Character generator
time	37	Time server
name	42	NICname server
domain	53	Domain Name Service
tftp	69	Trivial File Transfer Protocol
sunrpc	111	Sun Remote Procedure Call protocol
snmp	161	Simple Network Monitoring Protocol
snmp-trap	162	SNMP Trap (event log)
biff	512	Mail arrival notification
who	513	Number of users and load average (UNIX)
syslog	514	System log messages
talk	517	Terminal-to-terminal chat (old)

ntalk	518	Terminal-to-terminal chat (new)
route	520	Routing Information Protocol (RIP)
new-rwho	550	Number of users/load (experimental)
rmonitor	560	Remote host monitoring (experimental)
monitor	561	Host monitoring (experimental)

Figure B.7: UDP port assignments (partial list)

APPLICATION PROTOCOLS

Telnet

The telnet protocol is the basic means of logging into a remote host over a TCP/IP network. The protocol is designed to be both robust enough to maintain a connection over a noisy transcontinental Internet link, while at the same time efficient enough not to slow down a user logging into a host on the same LAN. Telnet is a TCP-based protocol.

The telnet client is a program on the user's local system, often a personal computer or workstation. The telnet server is a program on a destination system that is able to accept login connections (normally a time-sharing system, but single-user personal computers may also have telnet servers). The telnet server listens for connection requests on TCP port 23. The session begins when a telnet client sends a request to open a connection.

The server accepts the connection request for processing, and the client and server negotiate telnet options (parameters for the connection). There are numerous telnet options, including whether the connection should be character-oriented (the normal case) or line-oriented; what characters should be used for special purposes like *interrupt* or *flush output*; carriage-return/line-feed mapping

options; debugging information; what type of terminal is being emulated, etc. This negotiation is performed by exchanging a number of telnet protocol commands and assertions in the form WILL <option> / WONT <option> and DO <option> / DONT <option>. For example, a client may assert WILL FLUSH (flush output when an interrupt occurs), and the server may reply either DO FLUSH or DONT FLUSH indicating acceptance or rejection of that parameter.

At the end of the negotiation procedure, the server starts a login session for the client, and according to the parameters negotiated, the client and server programs pass characters back and forth, possibly interpreting or translating special characters or escape sequences. The protocol provides for re negotiation of options during the session if requested by either side.

When the session is ended, the client and server exchange closing messages and the connection is closed. The TCP implementation will detect the closing of the telnet session and terminate the underlying TCP connection.

File Transfer Protocol (FTP)

FTP is a method of copying files across TCP/IP networks. It is designed to interoperate among a very wide range of operating systems and file formats. FTP is mostly used between dissimilar hosts or host on different networks; on LANs, it is often simpler and more efficient to use a protocol such as *rcp* (UNIX remote copy) or a file-sharing scheme (such as NFS) where network file transfers are transparent to users. FTP is also commonly used where the user does not have an account on the remote host, but certain files have been made available for public copying (anonymous FTP).

The FTP protocol and client-server model are somewhat complex, in that FTP sets up *two* TCP connections between the client and server. One connection carries commands and responses; the other carries the actual file data. The FTP protocol is interactive, in that the FTP user opens a connection to a remote server, set a number of options establishing the parameters of the connection, and then upload or

download files or groups of files, and possibly navigate among directories on the server host.

FTP clients understand a number of user commands that are passed to the FTP server. These commands are usually typed to a command processor (in the case of DOS or UNIX) or may be buttons or fill-in fields in a graphical user interface such as Microsoft Windows. These commands are used to manage the connection with the remote host, supply required login and password information, move among directories and file systems; get lists of files and directories; determine the format of file presentation and transfer; upload and download files; determine if special processing of the files is required; rename, move, or delete remote files; and manage the local user interface.

FTP is implemented by submitting commands and protocol requests over the FTP control TCP connection; the server will reply over the same channel with protocol responses. Some commands / responses will result in data being transferred (in either direction) over the data TCP connection.

Each protocol response has an assigned numerical code, which is used by the client software. The verbal portion of the response code may or may not be seen directly by the user. The first digit of the response code indicates the family of the response, according to the following rules:

Leading digit	Meaning
1 _ _	Positive preliminary reply. The requested action is being initiated; expect another reply before proceeding with a new command.
2 _ _	Positive completion reply. The requested action has been successfully completed.
3 _ _	Positive intermediate reply. The command has been accepted, but the requested action is being held in abeyance, pending receipt of further information.

4 _ _	Transient negative completion reply. The command was not accepted and the requested action did not take place, but the error condition is temporary and the action may be requested again.
5 _ _	Permanent negative completion reply. The command was not accepted and the requested action did not take place. The user is discouraged from repeating the exact request (in the same sequence).

The second digit of the response code indicates the type of the response message:

Second digit	Meaning
_ 0 _	Syntax error
_ 1 _	Informational message
_ 2 _	Connection message
_ 3 _	Authentication / accounting message
_ 4 _	(reserved for future use)
_ 5 _	File system message

A complete list of FTP server response codes appears below.

110 Restart marker reply.
120 Service ready in nnn minutes.
125 Data connection already open; transfer starting.
150 File status okay; about to open data connection.

200 Command okay.
202 Command not implemented, superfluous at this site.
211 System status, or system help reply.
212 Directory status.
213 File status.
214 Help message.
215 NAME system type.
220 Service ready for new user.
221 Service closing control connection (user is logged

out if appropriate).
225 Data connection open; no transfer in progress.
226 Closing data connection; requested file action successful.
227 Entering Passive Mode.
230 User logged in, proceed.
250 Requested file action okay, completed.
257 “PATHNAME” created.

331 User name okay, need password.
332 Need account for login.
350 Requested file action pending further information.

421 Service not available, closing control connection.
425 Can't open data connection.
426 Connection closed; transfer aborted.
450 Requested file action not taken; e.g., file not present.
451 Requested action aborted: local error in processing.
452 Requested action not taken: insufficient storage space in system.

500 Syntax error, command unrecognized.
501 Syntax error in parameters or arguments.
502 Command not implemented.
503 Bad sequence of commands.
504 Command not implemented for that parameter.
530 Not logged in.
532 Need account for storing files.
550 Requested action not taken: file unavailable
551 Requested action aborted: page type unknown.
552 Requested file action aborted: exceeded storage allocation
553 Requested action not taken: file name not allowed.

Simple Mail Transfer Protocol (SMTP)

SMTP is the protocol used to transport electronic mail on the Internet. In addition to transporting mail between and among

directly connected Internet sites, SMTP can also be used as a common mail backbone between organizations that use other types of mail systems, with the intermediate transport performed over Internet mail relays. **Internet Exchange** uses SMTP to send and receive messages over the Internet.

SMTP is closely associated with a specific message format, known as RFC822 format, which is the basic mail message type used in the Internet. Until the arrival of MIME (see Appendix D), RFC822 messages were the only standard message type carried by SMTP.

SMTP itself is a relatively simple "lock-step" protocol implemented using TCP. (Several non-TCP/IP implementations exist for SMTP, but are not in general use on the Internet.) Hosts that can receive SMTP messages run a SMTP server daemon that listens for connection requests on TCP port 25. Hosts wishing to send a SMTP message use a SMTP client program that opens a connection with an SMTP server on the destination host or a mail relay, and the client and server communicate in a series of protocol commands and responses. SMTP is called a "lock-step" protocol since every command has a finite number of protocol responses, and each side waits, synchronously, for the end of a protocol request or response before continuing.

When a user sends an Internet mail message (from a directly connected system), his mail program (user agent) will pass it to a mail transport program, which determines (by consulting the Domain Name System), which Internet host the message should be delivered to. The system's SMTP client then initiates a connection with the SMTP server on that host. (If the user is using a mail gateway such as **Internet Exchange**, there may be a number of intermediate steps before the message is given to an SMTP client for Internet delivery.)

After the connection is initiated and the client identifies its domain name (with the HELO command), it communicates the address of the sender of the message (with the MAIL command), and the addresses of the recipient of the messages (with the RCPT command). The SMTP server acknowledges each recipient address as either valid or invalid. When the list of recipients is complete, the client uses the DATA command to indicate that the message

itself is ready to be sent. The server receives and acknowledges the message, and the client closes the connection. The server agrees to the close of connection and this is detected by the TCP implementation that terminates the connection. At this point, if the original message has further recipients elsewhere, the SMTP client will open a connection to another host and repeat the process until all recipients have been delivered to.

The SMTP command set is relatively small.

HELO <domain>	Client identifies itself to the server with its domain name
MAIL FROM:<reverse-path>	Identifies sender of the message
RCPT TO:<forward-path>	Identifies a recipient address
DATA	Message text follows, terminated by a line with a dot (".") by itself
RSET	Abort the current mail transaction and reset the connection
SEND FROM:<reverse-path>	Deliver message to a terminal (now considered an optional extension)
SOML FROM:<reverse-path>	Deliver message to terminal or mail it (now considered an optional extension)
SAML FROM:<reverse-path>	Deliver message to terminal and mail it (now considered an optional extension)
VRFY <string>	Confirm that <string> is a valid address

EXPN <string>	Expand (show the addresses in) a local mail alias or mailing list (now considered an optional extension)
HELP	Return a list of SMTP commands and meanings (now considered an optional extension)
NOOP	No operation; requires acknowledgment
QUIT	Request to close connection
TURN	Request for server and client to exchange roles so that client can receive mail queued on server host (now considered an optional extension)

The SMTP server response codes are similar in form to those used in FTP, but because of the relative simplicity of the protocol, are a smaller set.

211 System status, or system help reply
214 Help message
220 <domain> Service ready
221 <domain> Service closing transmission channel
250 Requested mail action okay, completed
251 User not local; will forward to <forward-path>

354 Start mail input; end with <CRLF>.<CRLF>

421 <domain> Service not available, closing transmission channel
450 Requested mail action not taken: mailbox

unavailable
451 Requested action aborted: local error in processing
452 Requested action not taken: insufficient system storage

500 Syntax error, command unrecognized
501 Syntax error in parameters or arguments
502 Command not implemented
503 Bad sequence of commands
504 Command parameter not implemented
550 Requested action not taken: mailbox unavailable
551 User not local; please try <forward-path>
552 Requested mail action aborted: exceeded storage allocation
553 Requested action not taken: mailbox name not allowed
554 Transaction failed

Since the original implementation and deployment of SMTP, there have been a number of proposals to extend the SMTP command set and range of services, including adding the capability of handling messages that are not 7-bit ASCII text. The standards document RFC-1651, “SMTP Service Extensions” (February 1993), defines a method of extending SMTP by registering additional capabilities with the central Internet naming authority, and listing them as part of a simple extensions negotiation at the beginning of an SMTP session. This extended SMTP protocol is called ESMTP.

INDEX

N

O

P

Q

R

S

T

U

V

W

X