Internet Exchange

for cc:Mail and Lotus Notes

Gateway Administrator's Manual Version 3.1 Addendum

August, 1998

International Messaging Associates Ltd
Hong Kong Computer Center, 20/F
54-62 Lockhart Road
Wanchai
HONG KONG

Phone:	+852 2520-0300	(Direct)
	+1 (888) 562-3564	(USA Message Center)
Fax:	+852 2648-5913	(Direct)
	+1 (888) 562-3561	(USA Toll Free)

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

Phone:	+63 (2) 811-3999	(Direct)
	+1 (408) 481-9985	(USA – Direct)
Fax:	+63 (2) 811-3939	(Direct)
	+1 (888) 562-3561	(USA Toll Free)

Email: info@ima.com
WWW: http://www.ima.com/

TABLE OF CONTENTS

INTRODUCTION 1

INTERNET EXCHANGE FOR CC:MAIL INSTALLATION (CHAPTER 3) 3

INSTALLING INTERNET EXCHANGE 3.1 FOR CC:MAIL 3
THE CD INSTALLER 3
INTERNET EXCHANGE LICENSING 6
Evaluation License 6
Interim License 7
Permanent license *7*

CONFIGURING INTERNET EXCHANGE (CHAPTER 7) 8

CONFIGURE SCHEDULES 8
CCIN/NOTESIN Interval 9
CCOUT/NOTESOUT Interval 9
SMTPC Interval 9
System Interval 9
Sync Mode 9
Enable Autoshutdown 10
Remote Access Service 10
RAS CONFIGURATION 11
DIALUP SCHEDULER 12
Connection Profile Setting 13
Enable ETRN support 13
ETRN support for alternate name list 14
Send ETRN to a list of hosts when SMTPC starts up (Active ETRN) 14
Send "Keep Alive" packets 15
Run a program when connection is established 15
Wait For Program To Terminate Before Disconnecting 15
Status Information 15
CONFIGURE GATEWAY 16

ANTI-SPAM (CHAPTER 8) 19

INTRODUCTION 19
INCOMING SMTP CONNECTION 19
Allowed and Denied IP lists 20
MAIL RELAY FILTERING 23

REAL TIME LOG ANALYZER 24

INTRODUCTION 24
Log Message 25
Errors Only 25
Messaging Logging 25
SMTP Session 25
Diagnostic 25
List box buffer 25
Clear Log Buffer 25
GENERAL GATEWAY STATISTICS *26*
ANTI-SPAM STATISTICS *26*
SECURITY AND PERMISSION STATISTICS 27

INTRODUCTION

OVERVIEW

This is an Addendum to ***Internet Exchange 3.0 Users Manual.*** This Addendum describes the differences between Version 3.0 of ***Internet Exchange*** and Version 3.1. Each chapter in this addendum is intended as an update to the corresponding chapter in the Version 3.0 *Gateway Administrator's Manual.*

Internet Exchange Version 3.1 contains many functional and performance enhancements over the previous Version 3.0. Included in the new release are the following new features:

- **Active ETRN:** Used during dialup connections, this new option allows the gateway to send ETRN requests, which specify the FQDN of the gateway, to all remote SMTP servers that may be holding queued email during establishment of the dialup connection. These requests can be sent to multiple remote servers, and regardless of if outbound mail is destined for the remote server(s).

- **Dialup Scheduler:** Versions of Internet Exchange prior to 3.1, in order to facilitate the establishment of dialup connections, had to shut the gateway down and then restart, using external schedulers such as *IMACRON*. Version 3.1 has incorporated dialup scheduling internal to Internet Exchange, removing the need to employ external schedulers to stop/restart the gateway. The *Dialup Scheduler* works in conjunction with RAS.

- **Enhanced ESMTP Support:** Version 3.1 adds support for the *ESMTP SIZE* service extension. By using the *Peer Configuration* capabilities, the Internet Exchange administrator can specify a global maximum inbound message size to accept, as well as maximum sizes on a peer-by-peer basis. When communicating with remote ESMTP servers, Internet Exchange will use this information in order to determine when to send or

receive large messages prior to the actual message being sent across the Internet, resulting in significant bandwidth savings for large undesirable messages.

- **Mail Relay Filtering:** The new *Mail Relay Filtering* controls enable the gateway administrator to stop spammers or any other undesirable source from using the Internet Exchange MTA as a mail relay. By using this tool, the administrator can deny external sources the use of the gateway to propagate spam or junk mail, while at the same time allowing well known hosts (such as local POP3 clients) to relay mail.

- **New Logfile Tools:** Internet Exchange 3.1 standardizes the internal logfile format, and features a new *Real Time Log Analyzer* to let administrators analyze gateway-related information such as log message, general gateway statistics, anti-spam statistics, and permission statistics. Using the *Real Time Log Analyzer*, administrators can easily monitor all gateway activities and anticipate any messaging problems. Additionally, Version 3.1 includes a logfile API and DLL's that give application programmers a standard interface to the logfile data for more advanced data analysis.

- **New Licensing Options:** New licensing options are available for the *Workgroup Edition* - adding support for 250 and 400 user configurations. *Workgroup Edition* licenses are also now fully upgradable to *Enterprise Edition* without having to install a new version of Internet Exchange, making upgrading simpler than ever.

For programmers wishing to build additional logfile analysis tools, please refer to the *Internet Exchange 3.1 Logfile Analyzer API* document found on the 3.1 CDROM. It is also available for downloading from the IMA web site.

INTERNET EXCHANGE FOR cc:MAIL INSTALLATION (CHAPTER 3)

INSTALLING INTERNET EXCHANGE 3.1 FOR cc:MAIL

Once the **Installation Worksheet** has been filled in, installation of *Internet Exchange 3.1* can be initiated.

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 users 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, bench-marking reports, and *Internet Exchange* related white papers.

To install *Internet Exchange:*

1. Turn on the computer and run the Windows environment.

2. Insert the *Internet Exchange* CD into the CD-ROM drive.

3. On machines configured to automatically launch the CD auto-run feature, the Internet Exchange Installation tool will be started. If this does not happen, run the file *cinst.exe* found in the root directory of the CD.

4. From the *Internet Exchange* installation screen, select the button ***Install Products From*** *IMA*.

5. From the install menu, select the appropriate version of Internet Exchange for your location.

The *Internet Exchange* **Install Manager** screen will appear as shown in Figure 1:

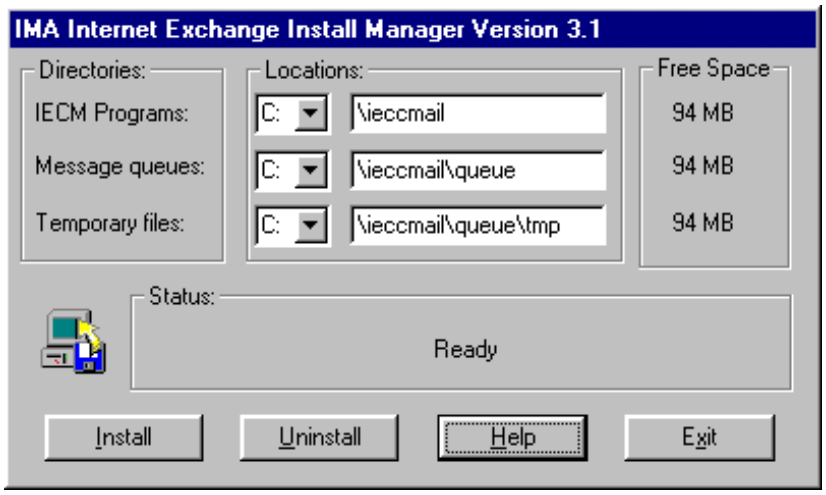

Figure 1. *Internet Exchange* **Install Manager** GUI

Press the ***Install*** button to install *Internet Exchange*. A dialog box showing the progress of the installation process will appear. Once all the files have been copied and the *Internet Exchange* program group has been created, the **Setup** program is automatically executed, displaying a new screen as shown in Figure 2:

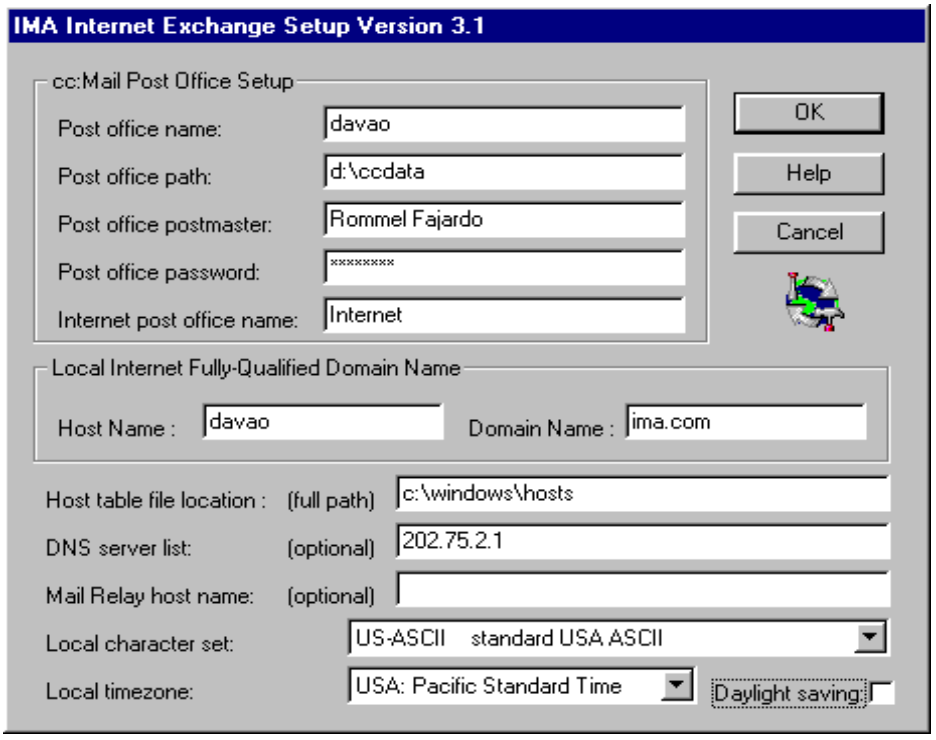

Figure 2. *Internet Exchange* **Setup** GUI

Figure 2 illustrates the basic parameters needed to start *Internet Exchange*. The figure is for the machine *davao.ima.com*, connecting to the cc:Mail post office *davao* located in d:\ccdata. The Internet cc:Mail Post Office name is *Internet*. Refer to the **Installation Worksheet** to ensure that all the entries are correct. Then click on the ***OK*** button to save the changes made to the screen.

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

After the **License Update** is run, a screen as shown in Figure 3 will be displayed:

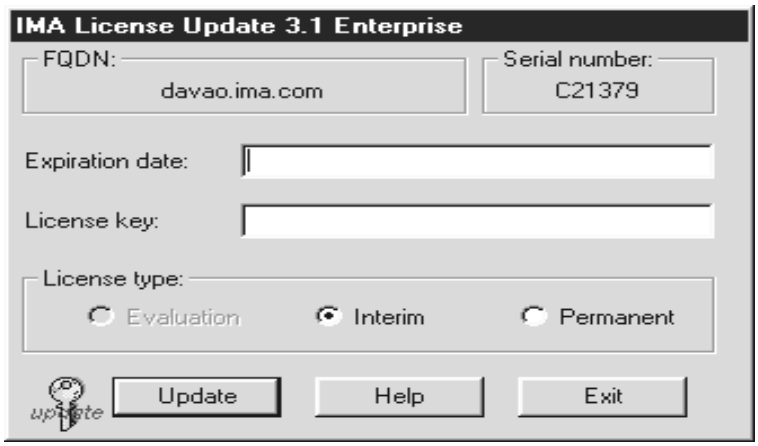

Figure 3. IMA **License Update** GUI

The version 3.0 license system for *Internet Exchange* was divided into two editions, namely Enterprise Edition and Workgroup. This system has been eliminated. Instead, a new licensing system is introduced for *Internet Exchange 3.1* onwards. It implements a Workgroup-100, Workgroup-250, Workgroup-400 and Enterprise (unlimited) users licenses. The license type is automatically derived from the supplied permanent or interim license keys.

There are two "read-only" fields in the **License Update** screen - the *FQDN* and *Serial Number* fields. 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 two fields

must be provided to your *Internet Exchange* supplier or IMA to generate a license key as described below.

To install *Internet Exchange 3.1* on top of an earlier version, it may be necessary to perform certain conversions. 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 of the *Internet Exchange 3.0* **Users Manual**.

INTERNET EXCHANGE LICENSING

There are three types of software licenses that can be generated for *Internet Exchange*: evaluation, interim, and permanent licenses.

Evaluation License

If the 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 a supplier or IMA, either by phone, fax, or email. Email requests should be sent to:

eval-auth@ima.com

When requesting for 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/yyyy. The license key should be entered exactly as obtained from the 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 used in applying for an evaluation license. Instead of sending email to *eval-auth*, please contact either the 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 *FQDN* of the gateway machine. To obtain a permanent license key, contact the supplier or IMA, or send email containing full registration information to:

auth@ima.com

Since a permanent license has no termination date, the only information needed to apply for a permanent license is the license key. Enter the license key and press the ***Update*** button to store the registration information.

After storing the license information in the **License Update** screen, *Internet Exchange* is ready for use.

CONFIGURE SCHEDULES

The **Configure Schedules** screen (see Figure 4) allows the gateway administrator to enter scheduling information needed for running *Internet Exchange*:

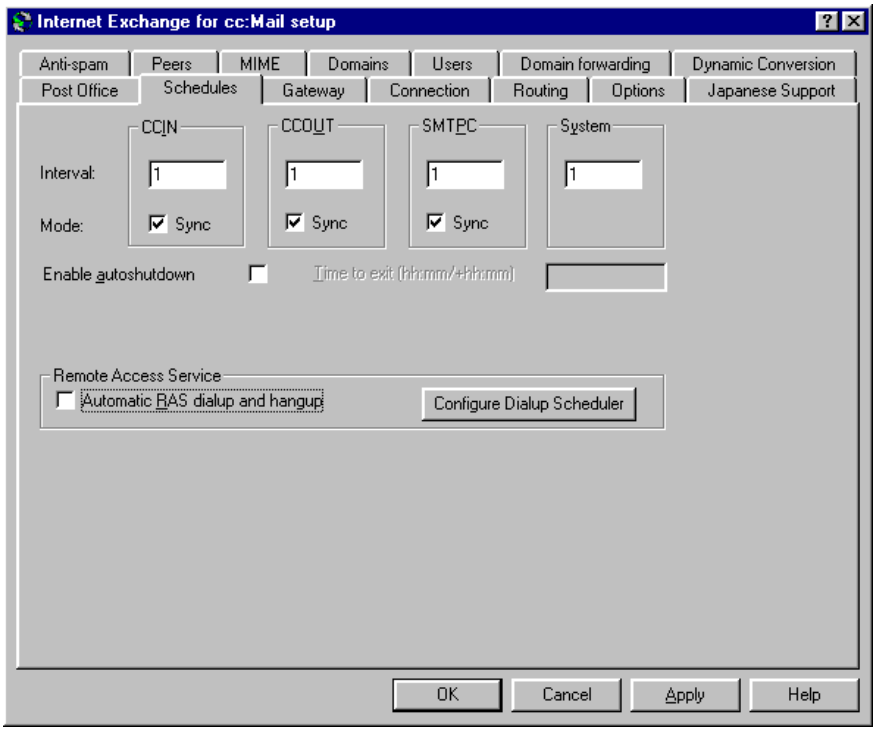

Figure 4. **Configure Schedules** screen

The most common configuration when using the *Internet Exchange 3.1* gateway is to have a permanent connection to the Internet. However, in certain cases, this setup may be impossible or impractical. In such cases, it is desirable to be able to schedule *Internet Exchange* to dial up an ISP at a particular time of the day so as to download and upload messages from and to the Internet.

Internet Exchange 3.1 features the **Dialup Scheduler,** which eliminates the need to use additional add-on products for dialup scheduling. With the **Dialup Scheduler**, a complete dialup and scheduling facility is integrated into a single product.

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 *SMTP*, measured in minutes. *SMTPC is* responsible for the tranfer 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 made 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 from either cc: Mail or Notes, these managers are *CCOUT/NOTESOUT* and *SMTPC*. For messages from 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.

Enabling the **Sync** option for each of the above parameters prompts the corresponding queue manager to start up as soon as a message is available. For instance, if the *CCIN/NOTESIN* **Sync** option is activated and a message is received by *SMTPD*, *CCIN/NOTESIN* will immediately start delivering the message to cc:Mail or Notes. For most installations, it is recommended to enable the **Sync** mode for all queue managers.

Enable Autoshutdown

This option enables automatic shutdown of *Internet Exchange* at the given time (24 hour time format). When a predetermined time is 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 option shuts the gateway down after a defined number of hours and minutes have been reached from the time that SYSMAN was last started.

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

Remote Access Service

RAS is the remote access service for Windows and is actively supported on all WIN32 platforms. It is a useful feature not only for dialup issues, but also for any Windows supported dial-up mechanism. With *Internet Exchange 3.1*, IMA introduces a new **RAS Dialup Scheduler.** The **RAS Dialup Scheduler** not only takes care of dial-up needs with ETRN but goes a step further by managing the dial-up scheduling as well.

To enable the **RAS Dialup Scheduler,** click on the ***Config Dialup Scheduler*** button on the **Schedules** screen. A screen for modifying **RAS** configuration and **Dialup Schedule** configuration will appear (see Figure 5).

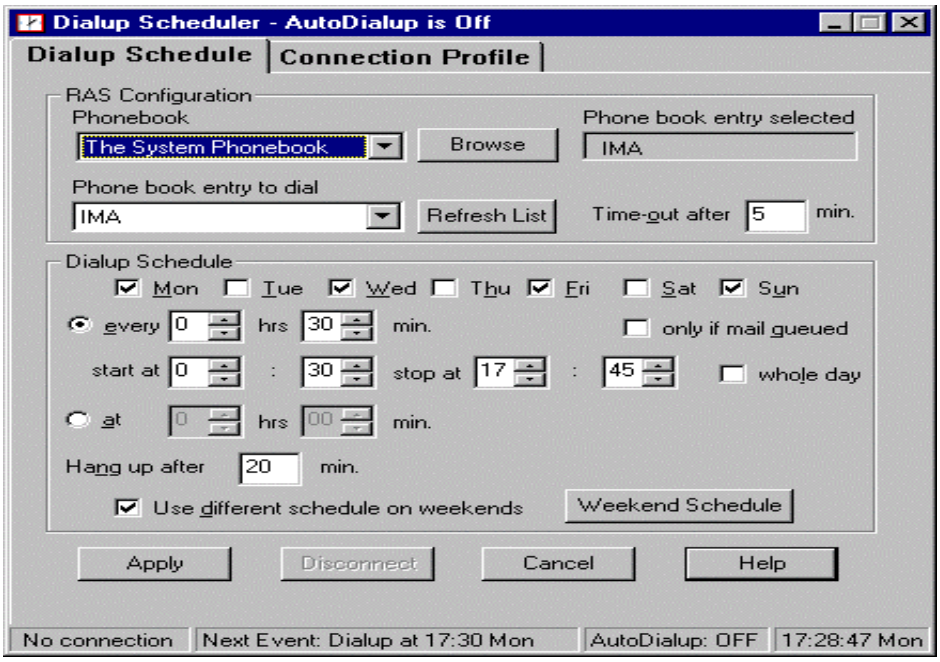

Figure 5. **Dialup Schedule** GUI

RAS CONFIGURATION

RAS configuration allows the gateway administrator to select the phonebook and the phonebook entry to use in the RAS dialup. In addition, it enables the administrator to specify a timeout value should the **Dialup Scheduler** fails to establish RAS dialup connection.

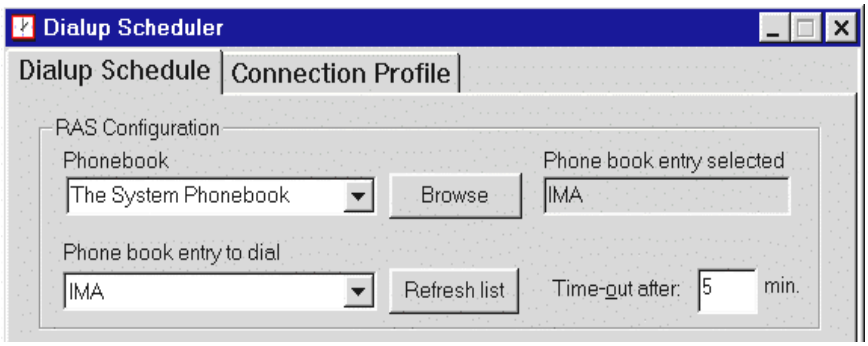

Figure 6. **RAS Profile** Configuration GUI

Figure 6 shows the layout of a section of the IMA **Dialup Scheduler** screen that allows the gateway administrator to configure these settings. It shows that the system phone book is

selected, and the entry to dial is IMA. It also shows that a time out value of 5 minutes is selected. Thus, if RAS dialup connection is not established after 5 minutes, the **Dialup Scheduler** aborts the dialup operation and waits for the next dialup event to occur.

DIALUP SCHEDULER

The **Dialup Scheduler** allows the gateway administrator to choose which days of the week to run the schedule. In addition, there is an option that allows for a different schedule to be used on weekends.

Figure 5 shows the different fields on the **Dialup Scheduler** screen for configuring various scheduling options. In the figure, periodic scheduling has been configured to run every 30 minutes between 00:30 hours and 17:45 hours every Monday, Wednesday, and Friday. However, dialup will only be activated if there are mail queued in the SMTP Out queue. Each dialup session will last for 20 minutes, after which the dialup connection is terminated. A different dialup schedule is also configured to be applied on weekends. The weekend dialup schedule will run on Sundays.

The ***APPLY*** button is used to implement new dialup schedules, including the weekend dialup schedules, and save the changes made on the screen. By clicking on the ***CANCEL*** button, any changes made to the **Dialup Schedule** GUI are discarded. The ***DISCONNECT*** button allows manual disconnection of any established connection.

To configure the weekend schedules, the **Weekend Dialup Scheduling** configuration GUI, as shown in Figure 7, is used. In the figure, the gateway is configured to perform dialups at 1015 hrs on a predetermined day on weekends (in this case, the scheduled day for running dialups is Sunday, as configured in Figure 5). Each dialup session will last for 60 minutes, after which the dialup connection is terminated.

To save the changes made to the **Weekend Dialup Schedule** configuration GUI, click on the ***OK*** button. The **Dialup Schedule** screen (see Figure 5) will appear. By clicking on the ***APPLY*** button, all changes made to this screen are saved and a new weekend schedule is implemented.

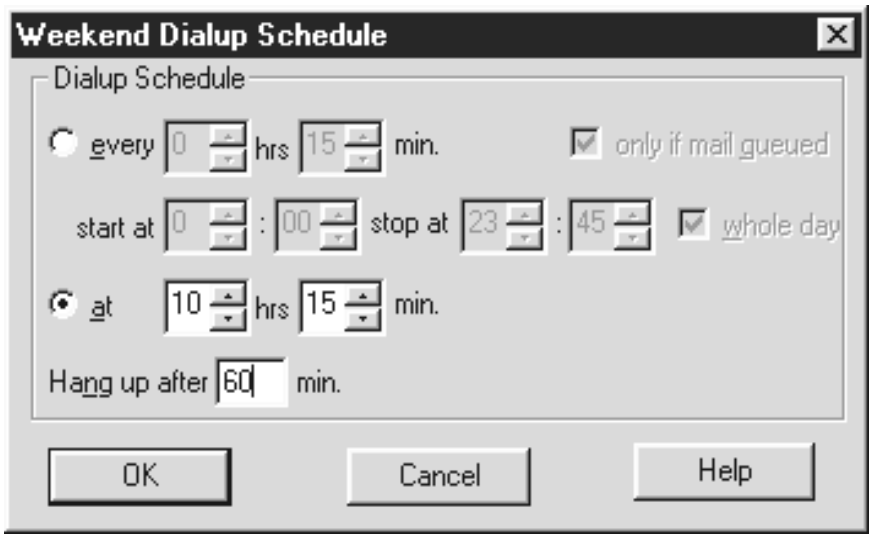

Figure 7. **Weekend Dialup Schedule** screen

Connection Profile Setting

The **Connection Profile** GUI (see Figure 8) allows the gateway administrator to configure the various parameters for the dialup connection. Some of the options under this setup are consistent with earlier versions of *Internet Exchange*. Figure 8 shows the **Connection Profile** configuration GUI. In the figure, the **ETRN Support** option is enabled with both the ETRN for alternate host name list option and the active ETRN option activated. The **Send keep alive packets** option is also enabled as well as the option for executing a program when connection is established. The program to run is *ping.exe* and the command line parameter for the program is *mail1.jade.net*.

To save the changes made to the **Connection Profile** screen, click on the ***APPLY*** button. To discard the changes, click on the ***CANCEL*** button.

Enable ETRN support

This option, when activated, enables *Internet Exchange* to send ETRN requests to all remote *SMTP* hosts during the dialup connection when the gateway is sending out mail. The ETRN requests specify the *FQDN* of the gateway.

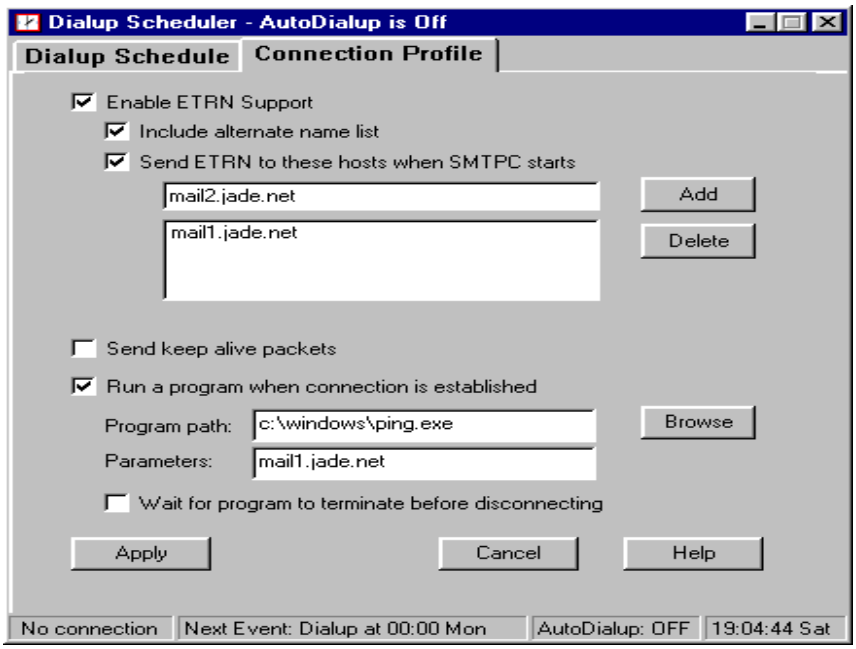

Figure 8. **Connection Profile** Configuration GUI

ETRN support for alternate name list

In addition to specifying the *FQDN* of the gateway, ETRN requests that specify the alternate name list of the gateway can also be sent to all remote hosts during the SMTP session by enabling this option.

Send ETRN to a list of hosts when *SMTPC* starts up (Active ETRN)

Sometimes it is necessary to send ETRN requests to several hosts even if there is no mail bound for these hosts. It is possible that these hosts are holding mail for the gateway.

By activating this option, ETRN requests are sent to specific hosts even if there is no mail bound for these hosts. This option allows the gateway administrator to specify the host(s) to which ETRN requests will be sent. Each host name specified is checked against the host table and is accepted if a match is found. Otherwise, the host name is rejected. An ***ADD*** button and a ***DELETE*** button are provided to enable the gateway administrator to add or remove host names from the list.

> **NOTE:** Active ETRN hosts have to be listed in the *hosts* file which is configured from the *Configure Connection* screen (this may be different from the system *hosts* file).

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 zero network activity. Under this condition, it is necessary for the gateway to keep the stack active if *SMTPD* is to continue to receive incoming mail.

If the **Send keep alive** option is enabled, *SMTPD* sends “**keep alive**” packets (which are single UDP packets) to the discard port of a remote host. The gateway looks for a DNS server, then conducts a sequential search for any host (other than the gateway itself) in the host file to send the “**keep alive**” packets to. The packets are sent at the rate of one packet approximately every 10 seconds.

Run a program when connection is established

It might be necessary for the gateway to execute a particular program, such as the finger utility, once the RAS dialup connection is established. This new option allows the gateway administrator to specify the program to run and the command line parameter for the program.

Wait For Program To Terminate Before Disconnecting

This option, when enabled, forces the dialup scheduler to wait for the execution of the program to terminate before it disconnects the RAS connection.

Status Information

The **Dialup Scheduler** configuration GUI includes a status bar (see Figure 9) showing the state of the **Dialup Scheduler**. In the figure, the status bar shows the RAS status with possible indications such as no connection, dialing, connected, and shutting down. The scheduled time for the next event is also shown. Possible events include dialup, hang up, and time out. The state of the **Automatic RAS dialup and hang up** option is also indicated on the status bar, so there is no need to open the **Configure Schedules** screen on SYSMAN to check whether this option is enabled or not. The current system time is also shown.

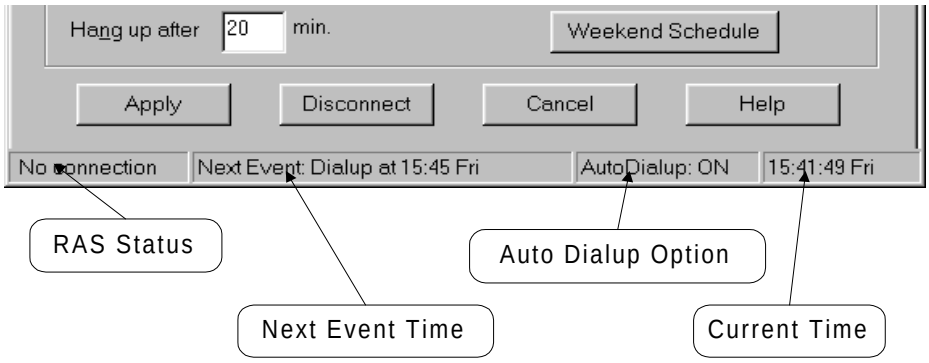

Figure 9. Status bar for **Dialup Scheduler**

CONFIGURE GATEWAY

The **Configure Gateway** screen (see Figure 10) allows the gateway administrator to enter information related to the general operation of *Internet Exchange 3.1*.

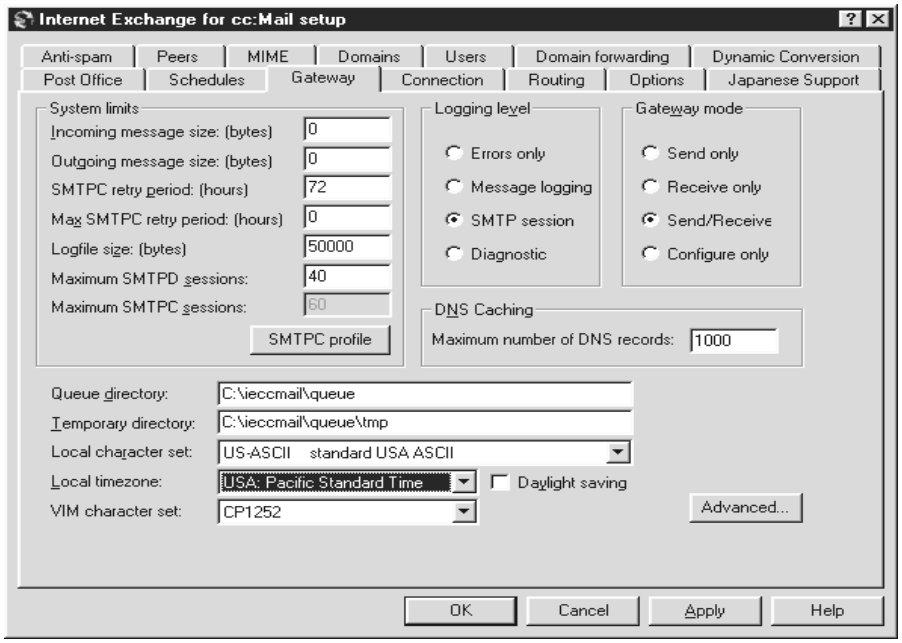

Figure 10. **Gateway** Configuration GUI

The features in the *Internet Exchange 3.1's* **Configure Gateway** GUI are the same as those in previous versions with the exception of one new function in the **Advanced Gateway** configuration window, namely *ESMTP* support.

Previous versions of *Internet Exchange* supports only *SMTP*, which is defined by RFC821 as the Internet message transfer protocol. But with *ESMTP*, *SMTP's* Service Extension, now becoming more and more popular in the Internet community, IMA has included *ESMTP* support in *Internet Exchange 3.1* onwards.

The service extensions available for ESMTP support in *Internet Exchange 3.1* are SIZE and ETRN. The **Advanced Gateway** configuration screen (see Figure 11) allows the gateway administrator to enable *ESMTP* support and the *ESMTP SIZE* Extension.

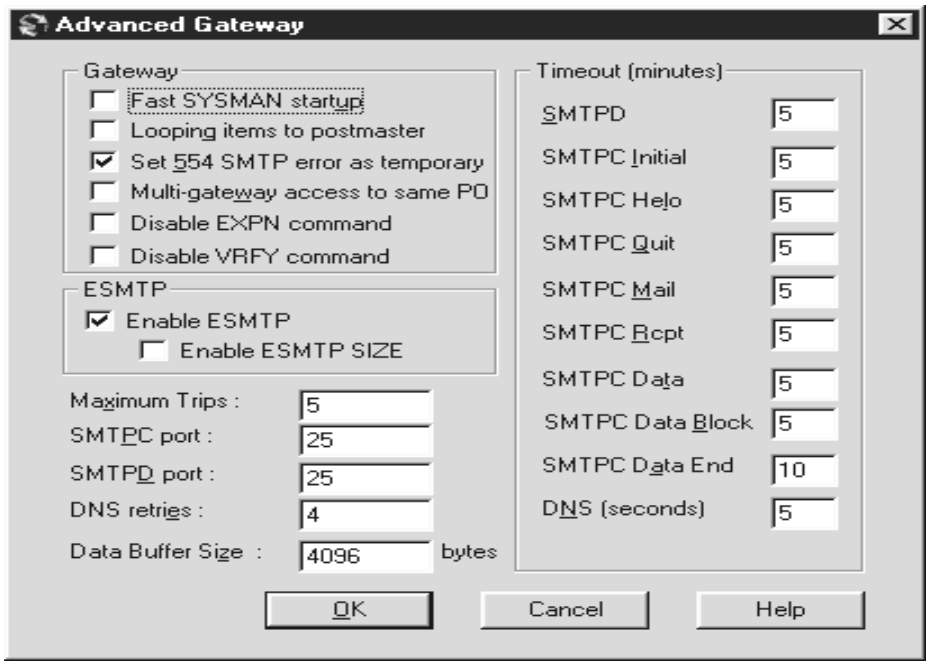

Figure 11. **Advanced Gateway** Configuration GUI

To enable *ESMTP* support, check the **Enable ESMTP** box. By default, this option is enabled. With this option activated, *SMTPD* accepts EHLO command and *SMTPC* issues EHLO command instead of HELO command to the peer side, otherwise, both *SMTPC* and *SMTPD* will only support *SMTP*. If the peer *SMTP* server does not support *ESMTP*, *SMTPC* reissues the HELO command and behaves as an unextended *SMTP* client.

By checking the **Enable ESMTP SIZE** box, the SIZE extension service is activated. By default, this option is enabled.

When **Enable ESMTP SIZE** is activated, *SMTPD* advertises the EHLO keyword SIZE in response to the EHLO command. The maximum inbound message size for each peer domain and the default maximum size can be configured via the **Peer** configuration GUI. The optional parameter for the keyword SIZE, which is used to specify the fixed maximum size, can be determined from the **Peer** configuration window by taking the maximum values of the size limits for all the peer domains.

In previous versions of *Internet Exchange*, the maximum inbound message size checking, which is performed by CCIN, is based on the domain specified in the envelope sender address (this follows the MAIL FROM command). If the peer *SMTP* client also supports SIZE service extension, it may indicate the estimated size of the message that is going to be transmitted in the MAIL FROM command (i.e. MAIL FROM: user@pattaya.ima.com SIZE=500000).

In *Internet Exchange 3.1*, maximum size checking can be moved forward to the *SMTPD* module under the MAIL FROM command. Under this setup, *SMTPD* accepts the extended version of MAIL FROM command, parses this string, retrieves the value specified by SIZE, and checks again the sender domain as defined in the **Peer** configuration window. If the declared size exceeds the maximum size for the sender domain, *SMTPD* rejects the message.

Similarly, if the peer *SMTP* server supports ESTMP and the **Enable ESMTP SIZE** option is enabled, *SMTPC* parses the EHLO keywords returned by the *SMTP* server.

For any outgoing message, if the actual message size exceeds the fixed maximum message size, *SMTPC* will not attempt to transmit the message. The message is marked as bounced.

SMTPC also supports the extended version of MAIL FROM by specifying the actual size of the message in the MAIL FROM command. All other consequent *SMTP* sessions and return *SMTP* code handling are classified as unextended *SMTP*.

ANTI-SPAM (CHAPTER 8)

INTRODUCTION

Internet Exchange 3.1 has several built-in functions that enable gateway administrators to prevent "spammers" (undesirable senders of unsolicited electronic mail) from attacking their mail systems. Using these functions, the gateway is able to identify spam messages and initiate predefined action against them. The following criteria are employed in identifying spam messages:

- Banned IP address/IP address range on inbound *SMTP* connection
- Banned Internet host/domain
- Banned user address

Once a spam message is identified, the message can be:

- Rejected by *SMTPD*
- Deleted from the Queue directory
- Moved from the Queue directory to the SPAM directory
- Bounced back to the spammer

Internet Exchange 3.1 features all the anti-spam options found in *Internet Exchange 3.0* (see Figure 12) plus enhanced **Incoming SMTP Connection** configuration and **Mail Relay Filtering**.

INCOMING SMTP CONNECTION

Internet Exchange versions 3.0 and 3.01 allow the gateway administrator to define a group of IP addresses in such a way that *SMTPD* rejects all incoming connection from those hosts. While this is a useful tool to reject unwelcome hosts, it requires the gateway administrator to identify unwanted IP addresses beforehand. *Internet Exchange 3.1* offers a another alternative

by providing gateway administrators with a tool that allows them to define a list of IP addresses that must be accepted by the gateway. All IP addresses not on the list are automatically rejected.

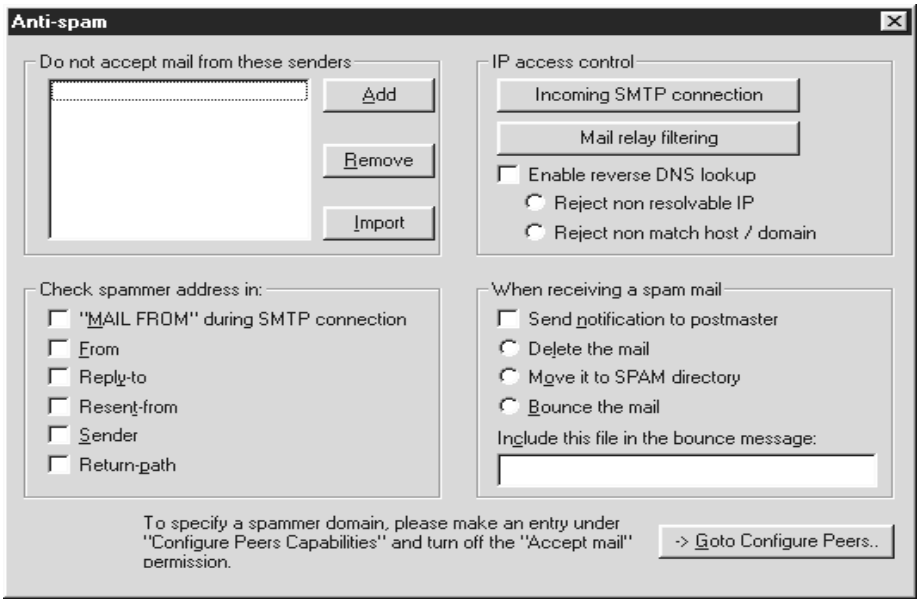

Figure 12. **Anti-spam** Configuration GUI

NOTE: In *Internet Exchange 3.0*, the option Enable reverse DNS lookup is enabled/disabled using the Advanced Gateway configuration GUI. In *Internet Exchange 3.1*, this option is moved to the Anti-spam configuration screen and grouped with the two other anti-spam options, the **Reject non resolvable IP** and **Reject non match host/domain** options (see Figure 12).

Allowed and Denied IP lists

Using the **Allow IP addresses** option in *Internet Exchange 3.1*, this new **Anti-spam** feature enables the gateway administrator to define which remote hosts or networks can establish SMTP connections with SMTPD by their host/network IP addresses.

The *Internet Exchange* administrator has full control over IP access control through the configuration of either one of the following:

- ⇨ *Allowing access to all hosts except those specified in a Denied IP access control list, or*
- ⇨ *Denying access to all hosts except those specified in an Allowed IP access control list.*

When *SMTPD* accepts a new connection, it checks whether the peer IP address is permitted to connect and issues a "553" response to any unauthorized hosts.

To configure the **Allow IP addresses** list in *Internet Exchange 3.1*, click on the ***Incoming SMTP connection*** button on the **Anti-spam** configuration screen. The **Incoming SMTP connection** GUI as shown in Figure 13 will appear.

Figure 13. **Incoming SMTP connection** GUI

Depending upon which default IP access restrictions are selected (either allow or deny access by default), only one of the access control lists will be active. If access is allowed by default, then it will be possible to specify the addresses that you wish to exclude from the default of allowing access to everyone. If access is denied by default, then the access control list that will be accessible will be the one that allows the configuration of sites that you explicitly desire to be able to establish SMTP connections with you.

To add entries to either list, click on the ***ADD*** button. The **Add IP address** screen will appear (see Figure 14), which will allow for the specification of either a single IP address, or a range of addresses.

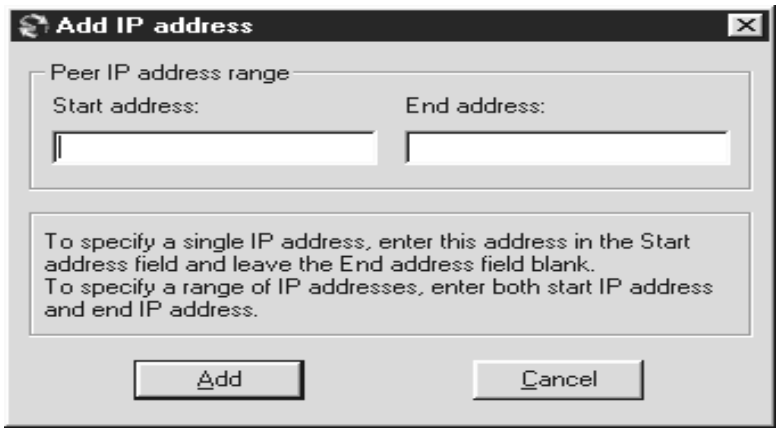

Figure 14. GUI for adding IP addresses to allowed/denied list

To edit an existing entry, simply select the entry, and click on the ***EDIT*** button. The **Edit IP address** screen will now appear (Figure 15), which will allow for the modification of existing configuration data.

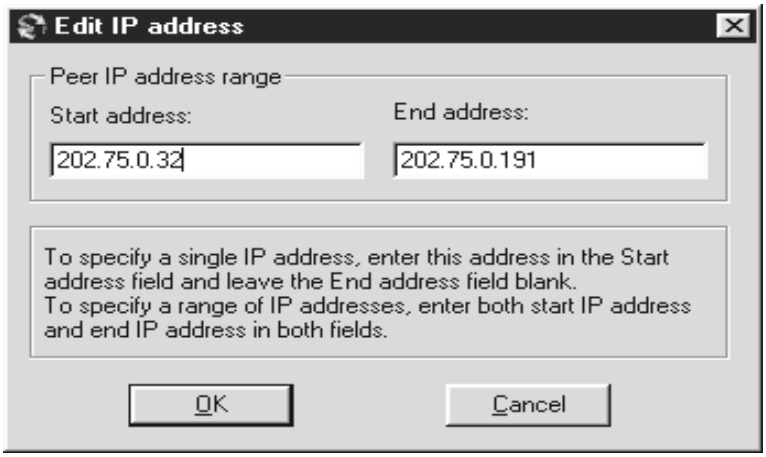

Figure 15. GUI for modifying IP addresses in allowed/denied list

MAIL RELAY FILTERING

Mail Relay Filtering is included as part of the Anti-spam features of *Internet Exchange 3.1* for cc:Mail and Lotus Notes. This option is aimed at stopping spammers from using *Internet Exchange SMTP MTA* modules to route their spam mail. By using this feature, only well-known hosts are allowed to relay mail.

The same procedure used in the **Incoming SMTP Connection** configuration is used to configure the **Mail relay filtering** GUI as (see Figure 16).

Figure 16. **Mail relay filtering** GUI

The above two utilities are combined in *Internet Exchange 3.1* to provide the gateway with a solid Anti Spam functionality.

NOTE: In order to allow mail relay, the global option "*Reject non-local users*" under the "*Advanced Options*" section must be turned off.

INTRODUCTION

The Real Time Log Analyzer allows the administrator to analyze various types of gateway activities and related information based on four distinct categories:

- Log Message
- General Gateway Statistics
- Anti-Spam Statistics
- Security and Permission Statistics

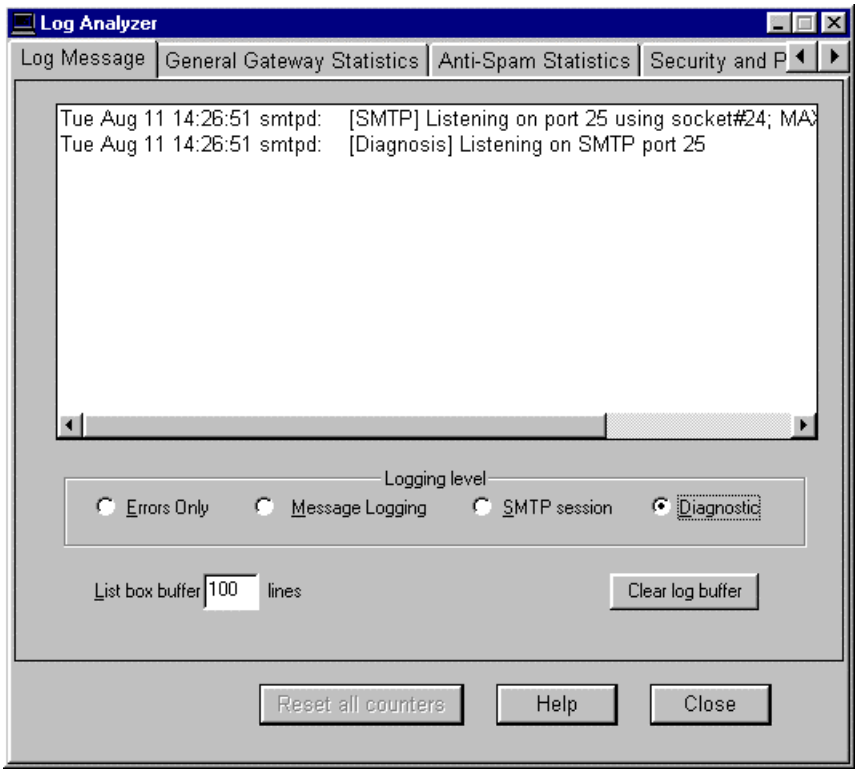

Figure 17. **Log File Analyzer**

Log Message

The Log Message view is derived from the larger log file that keeps a record of all gateway activity. Four activity levels are available: from the most basic level, called Error Only, to the Diagnostic level, which shows all gateway logging. Viewing the Diagnostic level can be quite helpful when experiencing messaging problems.

Errors Only

Only erroneous activity related to gateway or messaging problems are displayed.

Messaging Logging

Displays all incoming and outgoing message-related activity, including the errors reported in the first level. 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 1,000.

Clear Log Buffer

Removes all entries on the logging list.

GENERAL GATEWAY STATISTICS

This option provides the administrator with detailed gateway statistics regarding General functionality. Following are some examples of general gateway statistics:

- Mail received from Internet
- Mail delivered to Internet
- Mail imported to post office
- Mail exported to post office
- Mail bounced to post office
- Mail bounced to out queue
- Mail bounced to in queue
- Mail rerouted to out queue
- Mail rerouted to in queue
- Mail relocated to bad queue

To reset the above parameters, click on the Reset Counters button.

ANTI-SPAM STATISTICS

This option provides the administrator with detailed gateway statistics regarding Anti-Spam. Following are some examples of anti-spam statistics:

- Banned domain detected by SMTPD
- Banned sender address detected by SMTPD
- Banned domain detected by CCIN
- Banned sender address detected by CCIN
- Banned IP address
- Banned IP address for mail relaying
- Banned unresolved IP address
- Banned mismatched IP / host

To reset the above parameters, click on the Reset Counters button.

SECURITY AND PERMISSION STATISTICS

This option provides the administrator with detailed gateway statistics regarding Permission and Security. Following are some examples of security and permission statistics:

- Unauthorized local sender by CCOUT
- Unauthorized remote sender by CCOUT
- Banned domain by CCOUT
- Unauthorized local recipient SMTPD
- Unauthorized remote recipient by SMTPD

To reset the above parameters, click on the Reset Counters button.