July 2000
Volume 3, Issue 7

Inside this Issue

International Messaging Associates (IMA) Ltd.
The Broadway
20/F, 54-62 Lockhart Road
Wan Chai, Hong Kong
Tel: +852-25200300
Fax: +852-26485913

IMA Philippines Inc.
The Peak Tower
15/F, 107 L. P. Leviste Street
Salcedo Village
Makati City, Philippines
Tel: +63-2-8113999
Fax: +63-2-8113939

US Support: +1-408-4819985
US Sales: +1-408-4819985
US Fax: +1-888-5623561

E-mail: info@ima.com
Website: www.ima.com

Internet Exchange News

NEWS FLASH!!!

Internet Exchange Preprocessor Unit Performs Various Site Operations, Provides System Security

The existence of computer viruses is not the only problem that burden Internet mail users. Unsolicited e-mail (also known as *spam*) also imposes a number of disadvantages to e-mail users. It contributes to the delay in the delivery of legitimate e-mail and consumes a considerable amount of space. There is also the problem regarding the presence of inbound and outbound e-mail with offensive content and information leaks.

The proliferation of these problems forces most organizations to look for secure messaging systems that perform site specific operations, such as virus scanning, spam control and disclaimer generation, among others. **Internet Exchange Messaging Server version 4.1** is equipped with a Preprocessor Unit (see **Figure 1 on page 2**) specially designed to perform said operations. A list of related references, including introductory information, regarding the Preprocessor Unit is found on page 8.

The Preprocessor Unit, which runs the anti-spam and anti-virus plug-in modules, is equipped with a Channel Action Matrix to provide the system administrator with a flexible tool in configuring which channels/connectors should be run for a particular message. Another feature of the Preprocessor Unit is the Auto Text Insertion engine that provides the capability to insert disclaimers into messages that passes through the Internet Exchange.

SYSTEM COMPONENTS

Anti-virus Module

The Preprocessor embodies a plug-in anti-virus module which receives the message, decodes the message attachment and invokes a third-party anti-virus program chosen and defined by the administrator. The Preprocessor is capable of creating multiple threads for fast and reliable virus scanning. Once the anti-virus module detects a virus, it will either bounce the mail, archive the mail to a pre-defined quarantine location/folder or delete the mail, depending on the configuration of the system administrator.

The first step undertaken by the anti-virus module after receiving an e-mail message is *message attachment decoding*. It makes use of decoding procedures that are based on the encoding methods applied in the attachment. The anti-virus module is capable of decoding and performing simultaneous virus scanning on MIME and non-MIME attachments.

The anti-virus module supports the following encoding methods:

- BASE64
- Quoted-Printable
- 7 bit
- 8 bit
- UUENCODE
- BinHex
- AppleSingle
- AppleDouble
- Non-MIME encoded UUENCODE/BinHex
- Embedded UUENCODE/BinHex in MIME text item.

After decoding the attachment, the anti-virus module invokes a *third-party anti-virus software*. The anti-virus module has an open interface, which enables it to support multiple anti-virus softwares. This feature provides the system administrator the ability to use more than one anti-virus package thus, increasing the virus detection capability of the system.

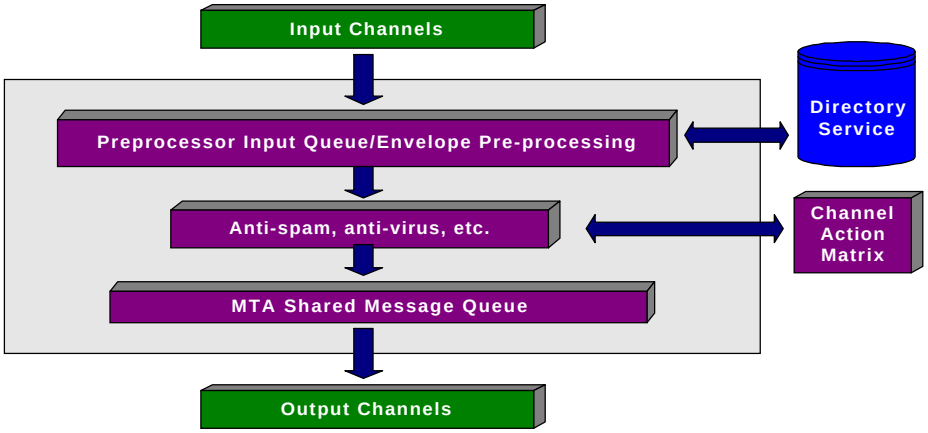

Figure 1: Preprocessor System Architecture

The Preprocessor anti-virus module supports the following anti-virus software:

- F-PROT Anti-Virus
- SOPHOS Anti-Virus
- McAfee Virus Scan

The anti-virus module of Internet Exchange can be *run independently on a remote machine in a distributed environment* via a RPC (Remote Procedure Call) mechanism. This feature is useful on a high traffic system where it is more desirable to run the anti-virus module on a dedicated remote machine, reducing CPU and file I/O loading on the Preprocessor system.

Anti-spam Module

The anti-spam module is designed to protect the integrity of the entire messaging system against unsolicited junk e-mail. This module enables the system administrator to create a list of banned or unwelcome IP address(es) using a configurable GUI (Graphical User Interface). It is also capable of verifying the corresponding name of an IP address during the initial stage of the SMTP session via reverse DNS lookup to filter out forged names, blocking out potential spammers even before they can enter the system. The module has the ability to reject spam messages using SMTP error codes. The anti-spam module supports RBL (Real-Time Blackhole List) for optimum anti-spam protection.

Once a message has been detected and tagged as spam by the anti-spam module, any of the following actions can be applied:

- Send notification to postmaster
- Delete the mail
- Move the mail to the designated SPAM directory
- Bounce the mail to the original envelope sender
- Include a signature text in a file for the bounced message

Channel Action Matrix

The Channel Action Matrix provides the system administrator with a flexible tool for configuring which modules the Preprocessor Unit should run for a particular message and exactly under what conditions it should be run. The Preprocessor engine consists of several modules: AntiVirus, SpamArchive, SpamDelete, SpamBounce, LoopDetection and AutoInsertion. The system administrator can select from these modules when routing messages to or from the Internet into the Internet Exchange. After a specific Preprocessor module has been selected, the different channels and connectors in the Channel Action Matrix will run the specific Preprocessor module for the messages to be routed in the Internet Exchange.

Auto Text Insertion Engine

The Auto Text Insertion Engine provides the capability to insert disclaimer messages into messages that passes through the Internet Exchange. Using this feature, messages created by users will automatically include a disclaimer stating the confidentiality of the message and limiting the liability of the company that maintains the mail system where the message originated. The system administrator can add different disclaimer messages based on the message source channel. With this feature, it is possible for messages generated in the cc:Mail environment to have different disclaimer from those that came from the Lotus Notes environment. The engine allows the system administrator to use plain text and/or HTML file for insertion process. It also supports non-MIME and MIME message structure types.

KEY FEATURES

Enhanced Queue Management Utility

Internet Exchange provides an enhanced Queue Management utility for the system administrator to view pending messages that has not yet been processed by the corresponding channel (DL, BSMTPOUT, Notes, ccMail, Local, SMTPC).

The system administrator may sort the pending messages for a particular channel according to one of the following criteria:

Priority, Sender and *Size*. The messages can also be searched according to *Sender's Address* or *Recipient's Address*. When the sorting/searching criteria is specified, the queue management utility searches all the messages for the specified criteria. The results are displayed on a new page, which shows all the messages that matched the criteria. The system administrator may either view the headers of the message, delete/bounce the message or re-set the queue.

Domain Forwarding

The Domain Forwarding feature provides the necessary information about the different domain/channel mappings for a domain-based mail routing. A sample entry of the Domain Forwarding is shown below.

Domain	Channel	Channel Identifier
smallcorp.com	BSMTPOUT	smallcorp@domain.com
othernet.org	BSMTPOUT	othernet@domain.com

Using the sample above, once messages enter the Preprocessor module it determines if there is a Domain Forwarding defined for the domain name in the recipient address. If the Domain Forwarding is defined, the Preprocessor will forward the mail message to the defined BSMTP channel. The BSMTP Encoder will encode the mail messages using the domain address (e.g. smallcorp.com) and then re-submit them to the Message Switch for further routing and delivery to the address defined in the Channel Identifier (e.g. smallcorp@domain.com).

In the above example, all messages destined for smallcorp.com will be forwarded to the BSMTP channel with the BSMTP identifier's address *smallcorp@domain.com*, while messages destined for othernet.org will be routed to *othernet@domain.com*.

Loop Detection

The Loop Detection feature enables the system administrator to configure the different parameters for defining the rules of message loops in the Internet Exchange. The system administrator may specify the maximum number of received lines (that show the FQDN of the MTA machine) allowed in an incoming message. Only lines containing the MTA FQDN are counted. If this number exceeds, the message will be bounced. If set, any looping messages will be bounced to the local postmaster instead of being returned to the remote sender.

Build Alias Table

The Build Alias Table feature enables the system administrator to extract all mail aliases from the LDAP-enabled Directory Server into a separate database. After extracting all mail aliases, the Preprocessor module will update an internal database that holds all the e-mail aliases available in the Directory. This database is required by the Preprocessor to recognize recipients who use an alias name.

An alias is like a multiple identity of a user. You can create your mail alias in the Directory Server configuration page using a different e-mail address. Let's say your original e-mail address is *username@domain.com* and your alias name is *username@mail.domain.com*. When a message is sent to username@mail.domain.com, the Preprocessor will route the message to username@domain.com.

CONFIGURING THE PREPROCESSOR UNIT

The system administrator can configure the different Preprocessor controls via the *System Administrator Web Interface*. To go to the System Administrator Web Interface, the system administrator must click on the *System Administrator* link from the *Internet Exchange Main Web Interface.* After clicking the System Administrator link, the system administrator will be asked to type in his username and password for proper authentication. Once he is successfully logged in, the *System Administrator Main Web Interface* displaying the various icons of the Internet Exchange components on the Top Menu will appear. The system administrator must click on the *Preprocessor* icon to display the different Preprocessor controls.

By using the web interface, the system administrator can perform the following functions:

- view the number of pending messages
- configure the domain forwarding
- view module list
- configure the channel action matrix
- configure the anti-virus and anti-spam modules
- configure the auto text insertion engine
- configure the loop detection
- build alias table

Queue Status

The Queue Status link displays the different Input Channels with corresponding pending messages. The system administrator may select a specific Input Channel (e.g. SMTPC) to view its details. Once a specific channel is selected, the new screen will display the sender's domain and the number of pending messages.

To read the messages of the particular domain, select the check box beside the particular message that you would like to view. Choose from the pull-down menu your preferred sorting criteria: *Priority*, *Sender* or *Size*. Click on the *Show Messages* button.

The system administrator may also search for a particular message using the *Sender's Address* or *Recipient's Address*. To search according to Sender's Address or Recipient's Address, enter the recipient or sender's address of the particular message (e.g. *username@domain.com*) and click on the *Search* button.

Configuration

The Configuration link enables the system administrator to set the following parameters:

- Local Domains
  Refer to the Internet domain names recognized by the

Internet Exchange as local. Local refers to the recipient's domain name (e.g. domain.com) that is listed in the local domain listing under the Preprocessor settings. The Preprocessor performs LDAP lookup on any local recipient to find out the corresponding connector. If the domain name does not exist in the domain listing, the Preprocessor will route the message to the default non-local channel, which is the SMTPC, to complete the routing. Local Domains also refer to the domains that the MTA take the responsibility for handling their messages. The MTA will either do the final delivery to the recipient or bounce the message if the message is undeliverable.

A domain name may begin with an asterisk (*) to denote all sub-domains, not including the main domain. For example, the entry *.domain.com will match entries that contains the local domain name as domain.com (e.g. machinename.domain.com). The MTA will accept the mail for all the domains listed even if the recipient may not have an entry in the LDAP directory. To configure the system to accept all mail for the primary domain plus all sub-domains, two entries are required (i.e., domain.com and *.domain.com).

- Default Local Delivery Channel
  Defines the channel processor that will handle non-mappable local recipients.

  Example: username@domain.com is local because “domain.com” is defined in the local domains list. If username@domain.com does not have an entry in the Directory Server, the Preprocessor will route the message to the default local delivery channel, which can be local, ccMail or Notes. If the default channel finds out that recipient does not exist in any of these channels, the message will be bounced. If the MTA receives a message for a local recipient who does not have an LDAP entry, the MTA will deliver the message to the default local delivery channel. If the recipient has an LDAP entry but does not have any connectors defined, the MTA will deliver the message to the default local delivery channel.

  At present, only Notes, ccMail and SMTPC connectors can process messages for recipients who does not have LDAP entries. For the Notes and ccMail connectors, it is necessary to have the “unlimited user” license to enable the default mapping functionality.

- Internet Delivery Channel
  Refers to the channel (e.g. SMTPC) used by the Preprocessor to deliver a message to the Internet. Although the entry is configurable, Internet Exchange makes use of the SMTPC channel as the default Internet delivery channel. It is recommended not to change the default setting.

- Message Queue Server
  Refers to the NetBIOS name of the machine where the MQ (Message Queue) is located. The MQ Server can reside on any NetBIOS compatible host, but the entry should correspond to the NetBIOS name of this server. The NetBIOS name must be the same as the Internet host name. It is possible to configure Microsoft Windows to have two different names for NetBIOS and the Internet name, but this will not work for the system designated as the MQ Server.

- Message Queue Server Access Mask
  Refers to a list of IP addresses describing the systems which are permitted to access the Preprocessor queues. Each entry can either consist of a single dotted IP address (e.g. 192.55.89.10), a range of IP addresses (e.g. 192.55.89.10-192.55.89.12), or an IP address with a mask (e.g. 192.55.89.00/28). The Preprocessor will log an error in the system log file, without listing the IP address, if an application tries to access the channels/queues.

- Message Queue Local Directory
  Refers to the directory path (e.g. c:\msgqueue) where the message queue databases and the sub-directories for the message files are installed. This directory is used by all connectors running on the same system.

- Message Queue Remote Access Directory
  Refers to the directory path (e.g. \\Station1\msgqueue) where the message queue can be accessed remotely. This directory is used by all connectors which are not running on the same system as the MQ Server.

  Example: If the MQ Server was running on a machine named Station1, a connector on machine named Station 2 could access the queued messages using this directory prefix.

  The system will not operate correctly across a network if the entries MQ Local Directory and MQ Remote Access Directory are not pointing to the same directory. If all the connectors, Preprocessor and the MQ Server are running on the same system, this directory will not be used.

- Message Queue Server Account Name
  Refers to an account name (e.g. Account Name) used to access the MQ Server. It also serves as the authentication information to be able to acccess the MQ Remote Access Directory.

  If the remote connector could not access the MQ Remote Access Directory, which uses a UNC (Universal Naming Convention) entry, then the entry provided is not properly stored in the MQ databases. If this entry is not filled up, the connector will use the credentials as previously configured on the current system to access the remote directory.

- Message Queue Server Password
  Refers to the password used for the MQ Server account name. The password must be at least four characters long. The password will appear as a row of asterisks (****) for security reasons.

- Notification Messages Sent To
  Allows the system administrator to enter the e-mail address of the person whom he would like to be able to receive such notification messages.

- Notify Postmaster on Corrupt Messages
  Provides the system administrator an option whether he would like to receive notificaton messages on corrupted messages or not. To be able to receive the notification messages on corrupted messages, tick on the check box otherwise, leave the field blank.

  Click on the *Update* button to change the current settings.

Domain Forwarding
This link allows the system administrator to define a domain forwarding mapping. If the Domain Forwarding is defined, the Preprocessor will forward the mail message to the defined channel. A sample entry of the Domain Forwarding is shown on page 3.

To add a new domain mapping, click on the *New* button. A new screen will appear where you will be required to enter the values for the following parameters:

- Domain
- Channel
- Channel Identifier

The *Domain* can be the second, third, fourth part of a FQDN (Fully Qualified Domain Name) to which the defined domain forwarding rule will apply. The format should be similar to "domain.com". For example, the domain name of the FQDN *hostname.domain.com* is *domain.com*. The *Channel* indicates the different Input/Output Channels, which are listed in the file 'queue.cfg' of the system. These Channels are created upon installation of the system. All of the messages in these Channels are listed in the status page as one entry. The *Channel Identifier* specifies the address of the channel you have selected from the Queue Selection List.

Module List
This link displays the various Preprocessor modules, such as the AntiVirus, SpamArchive, SpamDelete, SpamBounce, LoopDetection and AutoInsertion. This page also displays the full pathname of the module, module version number and brief description of each module. Each module name is linked to its corresponding Channel Action Matrix.

To configure the Channel Action Matrix for each module name, click a specific module name. A new screen will display the Channel Action Matrix for that module in table format (see **Figure 2**). The table lists the names of the Input Channels (i.e., SMTPD, BSMTPIN, DSN, DLOUT, WEBCLIENT) on the left-hand side, and the names of all the Output Channels (i.e., LOCAL, SMTPC, BSMTPOUT, DL) on the top. Tick the check box of the corresponding entry in the Channel Action Matrix. A check mark indicates that the Preprocessor module will execute the specific function. For example, as shown in Figure 2, the anti-virus module will scan the messages coming from the Input Channel (e.g. SMTPD) destined for the Output Channel (e.g. LOCAL) for possible viruses.

Anti-virus plug-in Configuration
This link enables the system administrator to view the different anti-virus profiles as well as create, edit or delete the different profiles (see **Figure 3 on page 6**). This page also presents several options on what to do with infected and suspicious messages.

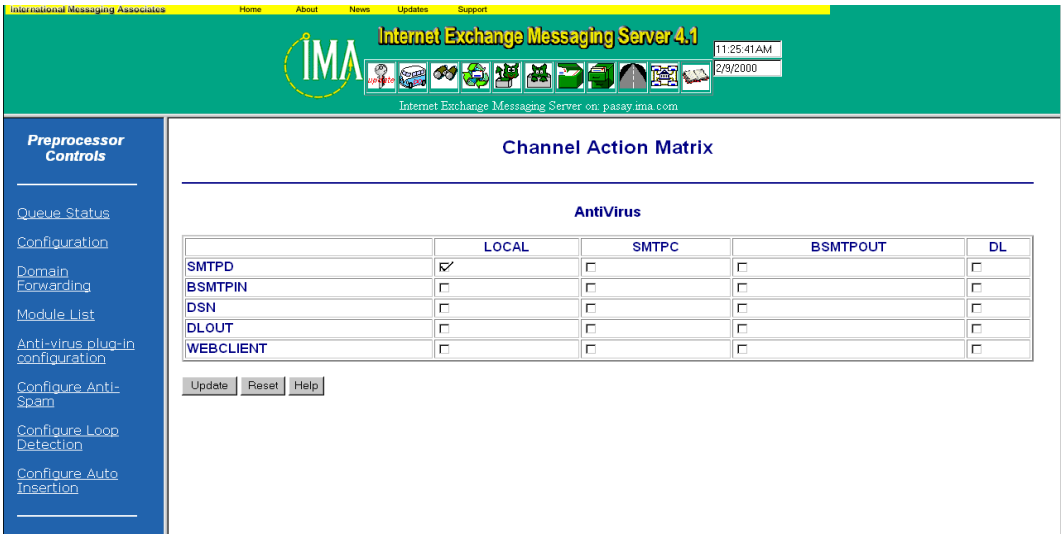

Figure 2: Channel Action Matrix configuration screen

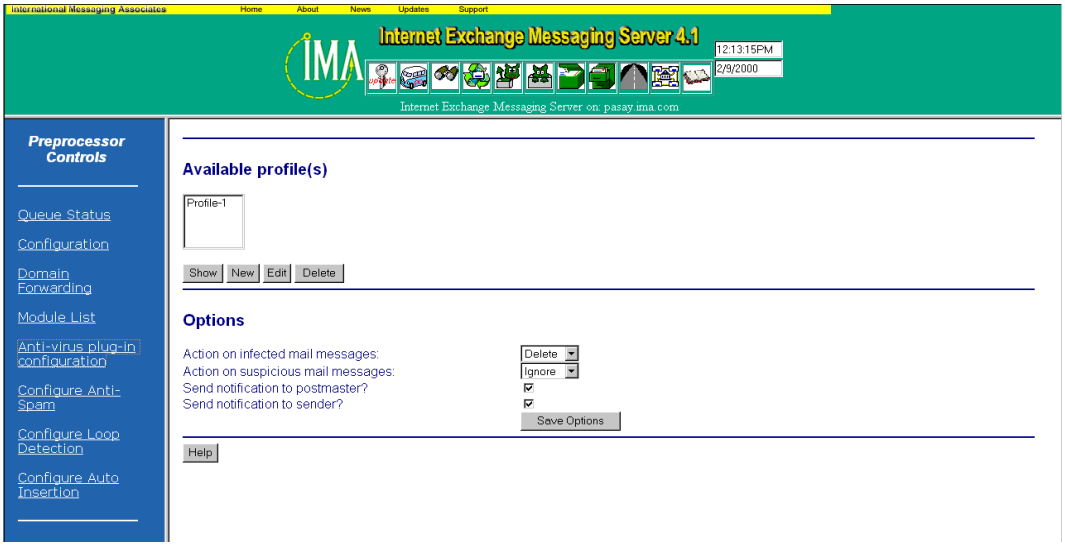

Figure 3: Anti-virus configuration screen

To view the anti-virus profiles, select a profile from the *Available Profile(s)* list box. Click on the *Show* button and the anti-virus profile attributes will be displayed.

To create a new anti-virus profile, click on the *New* button. A new screen will be displayed. Enter the *virus scanner type, program path, commandline parameters, no error codes, error codes* and *detected virus codes* in the appropriate fields. Click on the *Add* button to install the new anti-virus profile.

To edit your existing anti-virus profile, select an existing profile and click on the *Edit* button. A new screen for modifying the attributes of that profile will appear. Again enter the appropriate values on the specified fields and then click on the *Save* button to implement the new settings.

To delete an existing anti-virus profile, select the profile and click on the *Delete* button.

Anti-spam Module

The anti-spam configuration is in two-column table format (see **Figure 4 on page 7**). The left column contains the Spammer Address/Domain Restriction parameters, while the right column contains the IP Address Access Control parameters.

You can activate the parameters in *Spammer Address/Domain Restriction* column by ticking the check box of the following:

- MAIL FROM during SMTP connection
  If enabled, SMTPD will scan any spammer address or domain during the “MAIL FROM” session; and will return a 553 error to the remote sendmail host if a match is found.

- From
  If enabled, the anti-spam module will scan any spammer's address or domain in the “From” header.

- Reply-To
  If enabled, the anti-spam module will scan any spammer's address or domain in the “Reply-to” header.

- Resent-from
  If enabled, the anti-spam module will scan any spammer's address or domain in the “Resent-from” header.

- Sender
  If enabled, the anti-spam module will scan any spammer's address or domain in the “Sender” header.

- Return-path
  If enabled, the anti-spam module will scan any spammer's address or domain in the “Return-path” header.

- Reject Domain without MX/A Record
  The system administrator may choose to reject mail messages if the domain does not contain a MX or A record either Temporary or Permament

- Enable RBL Lookup
  If this option is enabled, SMTPD will try to find and match find an IP address in the RBL, which is a list of IP addresses that are known to send spam mail, be friendly to spammers, and/or totally open to mail relaying.

  The anti-spam module also allows the system administrator to specify whether to reject spam messages with a Permanent or Temporary *SMTP Error Code*. If the *Permanent* radio button is selected, the messages will be rejected by SMTPD with a Permanent SMTP error code, and will usually be bounced back to the original sender by the peer MTA. On the other hand, if the *Temporary* radio button is selected, the messages will be rejected by SMTPD with a Temporary SMTP error code and will usually be queued up and re-tried by the

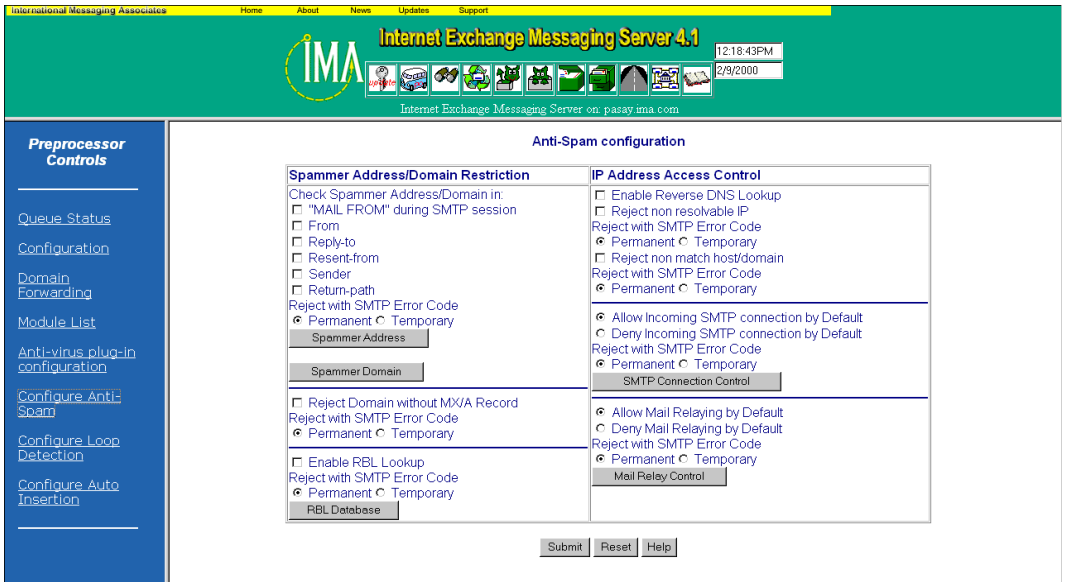

Figure 4: Anti-spam configuration screen

peer MTA later on to the recipients.

The *Spammer Address* button, once clicked, displays the e-mail addresses of potential spammers. To add a new e-mail address to the list, click on the *New* button. A new screen for adding spammer addresses will appear. Enter the e-mail address of the spammer on the blank field and click on the *Add* button. To delete an e-mail address from the list, select that particular address and click on the *Delete* button.

The *Spammer Domain* button, once clicked, enables the system administrator to add, delete and edit the peer domain attributes. To add a new spammer domain, click on the *New* button. A new screen for creating a peer domain and configuring its various options (i.e., Domain Name, SMTP Connection, SMTPC Profile, Native Attachment Encoding, among others) will be displayed. Enter the appropriate values for each parameter and then, click on the *Add* button to implement the settings of the new peer domain. To view an existing peer domain, select an entry from the list box. Click on the *Show* button and a new screen for modifying the peer domain's various attributes will appear. To edit an existing peer domain, select an entry from the list box. Click on the *Edit* button. A new screen for modifying the peer domain's various options will appear. To remove an existing peer domain, select an entry from the list box and click on the *Delete* button.

The *RBL Database* button, once clicked, enables the system administrator to view the list of the databases used by Internet Exchange to match IP addresses with those of potential spammers. Each database in the list contains blacklisted IP addresses. To add a new RBL database file to the list, click on the *New* button. A new screen will appear. To delete any of the RBL database files, select the file and click on the *Delete* button.

All the parameters in the *IP Address Access Control* column can be configured by also ticking the check box of the following:

- Enable Reverse DNS lookup
  By activating this option, reverse DNS lookup during the SMTP session is enabled. During the HELO/EHLO session, the SMTP client identifies itself to the SMTP server (SMTPD) through the HELO/EHLO parameter. The SMTP server verifies if the domain name corresponds to the IP address of the SMTP client host by performing Reverse DNS lookup.

- Reject Non-Resolvable IP
  When enabled, SMTPD rejects the connection if the incoming IP address is non-resolvable, which means that the DNS server/mail relay host cannot resolve the IP address.

- Reject Non-Match Host/Domain
  When enabled, SMTPD matches the resolved domain name with the one declared by SMTP client. If the two do not match, the connection is denied. It is also used to compare the reverse address look-up values and does not continue to check for possible CNAME entries.

- Allow/Deny Incoming SMTP connection by default
  If the “Allow Incoming” option is selected, SMTPD accepts every IP address except for those mentioned in the Deny IP address list. On the other hand, if “Deny Incoming” option is selected, every IP address except for those mentioned in the Allow IP address list is rejected.

- Allow/Deny Mail Relaying by default
  If “Allow Mail Relaying” option is selected, SMTPD

allows mail relaying for all IP addresses except for those mentioned in the Deny IP address list. On the other hand, if "Deny Mail Relaying" is selected, every IP address except for those mentioned in the Allow IP address list is prohibited for mail relaying.

The *SMTP Connection Control* button, once clicked, enables the system administrator to view the list of IP address range of potential spammers. Potential spammers are prevented from establishing SMTP connection with Internet Exchange. Clicking the *New* button will allow you to add a new IP address range. A new screen will be displayed. Enter the IP address range and click on the *Add* button to include that particular IP address range in the list of banned IP addresses. To remove an existing entry, select a particular entry and click on the *Delete* button.

The *Mail Relay Control* button, once clicked, enables the system administrator to list down the IP address(es) that are allowed to perform mail relay.

Configure Loop Detection

This link enables the system administrator to configure the different parameters for defining the rules of message loops in the Internet Exchange.

- Maximum trips
  Specifies the maximum number of received lines (that show the FQDN of the MTA machine) allowed in an incoming message. Only lines containing the MTA FQDN are counted. If this number exceeds, the message will be bounced. This option is useful in preventing message loops.

- Looping items to postmaster
  If set, any looping messages will be bounced to the local postmaster instead of being returned to the remote sender. This is often useful in preventing infinite mail looping.

  Click on the *Submit* button to implement the new settings.

Configuring Auto Insertion

This link allows the system administrator to create a new Auto Insertion setting. To create new settings, click on the *New* button. A new screen will be displayed where you should enter the values for the following fields:

- Source Channel
  A disclaimer will automatically be attached by the Auto Insertion Engine to messages coming from this channel.

- Text file
  The path to the *.txt file that contains the disclaimer to be attached to outgoing messages (e.g. c:\autoinsert\disclaimer.txt).

- HTML file
  The system administrator is provided with the option to use an HTML file as a disclaimer for outgoing messages. This is the full path specification of a single HTML file to be used (e.g. c:\autoinsert\disclaimer.html).

To store the auto insertion settings, click on the *Save* button. To edit the auto insertion files, click on the *Edit* button. To delete the auto insertion settings, click on the *Delete* button.

Building Alias Table

This link allows the system administrator to extract all mail aliases available in the Directory Server and build a separate database, which is required by the Preprocessor to recognize recipients using an alias name. To extract all aliases, click on the *Build Alias Table* button. This will enforce the Preprocessor module to update an internal database that holds all the e-mail alias available in the Directory.

For more information about the Preprocessor, please go to the following references:

- *http://www.ima.com/pdf/adminman2.pdf*
  (Messaging Server Administrator's Guide)
- *http://www.ima.com/faq/msgsrv/av/setup.html*
  (Internet Exchange Messaging Server Anti-virus Module Configuration)
- *http://www.ima.com/faq/msgsrv/av/advanced.html*
  (Configuring the Anti-virus Module To Run On Its Own Machine)
- *http://www.ima.com/product/v4/antivirus/index.html*
  (The Internet Exchange Anti-virus Module)
- *http://www.ima.com/pdf/ienews/vol2no12.pdf*
  (Internet Exchange Anti-virus Module Supports Virus Engines Inoculated for the Coming Millenium)
- *http://www.ima.com/pdf/ienews/vol2no5.pdf/*
  (The Internet Exchange Messaging Server Preprocessor: A sure fire protection against computer viruses and junk/spam mail)
- *http://www.ima.com/product/v4/antispam/index.html*
  (The Internet Exchange Anti-spam Module)
- *http://www.ima.com/pdf/ienews/vol3no5.pdf*
  (Preprocessor Auto Text Insertion Engine Inserts Disclaimer to Text and HTML Messages)

Highlight of the Month

Configuring the Internet Exchange Messaging Server to Work with IMAP4-capable Clients

IMAP (Internet Message Access Protocol) is a method of accessing electronic mail that are stored on a (possibly shared) mail server. It permits a "client" e-mail program to access stored remote message as if they were local. For example, e-mail stored on an IMAP server can be manipulated from a desktop computer at home, a workstation in the office and a notebook computer while traveling, without the need to transfer messages or files back and forth between these computers.

IMAP provides support for *online*, *offline* and *disconnected* access modes. It also supports concurrent updates and access to shared mailboxes. IMAP's capability does not only include the ability to name and access different incoming and archive message folders, but it also has the ability to list, create, delete and re-name the different folders.

The **Internet Exchange Messaging Server 4.x** supports the IMAP4 to allow you to access your mail from the IMAP4 Server using IMAP4-capable clients, such as Microsoft Outlook Express, Netscape Communicator and Pegasus Mail, among others. Using IMAP4, you can manipulate your mail on the server without having to download them to a local hard disk. You can also create multi-level mailboxes as well as shared mailboxes on the server that can be viewed concurrently, easily re-named, moved or deleted across multiple operating systems.

Pre-configuration Procedure:
Before you can configure the different IMAP4-capable clients to work with the Internet Exchange, you must install the Internet Exchange software in your system. After installing the software, you need to configure the different Internet Exchange components (i.e., Preprocessor, Directory Server, among others). For a detailed instruction on configuring the different Internet Exchange components, please go to *http://www.ima.com/pdf/adminman2.pdf*.

After configuring the different Internet Exchange components, follow the procedure below:

1. On the top menu of the Internet Exchange Main Web Interface, click on the Message Store icon. The Main Message Store web interface will appear.

2. Create a new user by clicking on the *Add User* button. Fill up the necessary fields with information and then click on the *Add* button. This will automatically create a local channel/connector for the IMAP4 account.

Note: The system administrator may also create a shared account. Using a shared account, the system administrator can manage users, groups and other shared data with just a single e-mail account. To create a shared account, click the "Add Shared" button. A new screen will appear where you should create an e-mail address for the shared account. Select the users that you want to include in the shared account. Click on the "Add" button to create a local channel/connector for the IMAP4 account.

Now, you are ready to configure your IMAP4-capable clients to work with Internet Exchange 4.1.

Configuring the IMAP4-capable Clients
To configure the different IMAP4-capable clients to work with the Internet Exchange, follow the steps listed below.

Creating an IMAP account in Outlook Express (v.4/v.5)
1. Open the Outlook Express.

2. Go to *Tools* pull-down menu and select *Accounts*. The *Internet Accounts* screen will appear.

3. Click on the *Add* button then, select *Mail*. The *Internet Connection Wizard* screen will appear.

4. Type your Display Name (i.e., John Doe) and click on the *Next* button.

5. Enter the e-mail address that you created in the Internet Exchange Message Store. Click on the *Next* button.

6. Choose IMAP server from the pull-down menu for the incoming mail server. Type the FQDN of your incoming and outgoing mail server on its respective field. Click on the *Next* button.

7. In the *account name* field, type in the e-mail address that you created in the Message Store and the associated password in the *password* field. Click on the *Next* button. A dialog box stating that you have successfully entered all the information required to set up your account will appear. Click on the *Finish* button. The *Internet Accounts* screen displaying the account you created will appear.

8. Click on the *Close* button. A dialog box will appear where you will be asked to download folders from mail server. Click on *Yes* button. The different folders of your IMAP account will be shown. Highlight the shared folders and click on the *Show* button to make them visible in Outlook Express' main window. Then, click on the *OK* button.

Creating an IMAP account in Eudora (v. 4.x)
1. Open the Eudora Mail Client.

2. Go to *Tools* pull-down menu and select *Options*. The *Options* screen will appear. You will be required to provide

information on the following parameters:

- Real name
- Return address
- Incoming Mail Server
- Login Name
- Outgoing SMTP Server

3. On left-hand side of the screen, click on the *Incoming Mail* icon. Select IMAP for your *server configuration*. Then, click on the *OK* button. A password box will appear. Enter your password.

4. On the Eudora main page, the <Dominant> is the newly created account's server. The shared folder(s) will also be shown if you have created a shared account on the Internet Exchange Message Store.

Creating an IMAP account in Pegasus Mail (v. 3.x)

1. Open the Pegasus Mail

2. Go to *Tools* pull-down menu and select *IMAP profile*s. The *IMAP Profiles* window will appear. Click on the *New* button. A new screen will appear. You will be required to provide information on the following parameters:

   - Profile name
   - IMAP Server address
   - Server port
   - Login name
   - Password

3. After you have filled up the necessary information, click on the *OK* button. The *Manage IMAP Profiles* screen displaying your existing IMAP Profiles will appear.

4. To download your messages from IMAP server, click on the *Connect* button or just double click the newly created IMAP username.

Creating an IMAP account in Netscape Messenger (v4.x)

1. Open the Netscape Messenger

2. Go to *Edit* pull-down menu and select *Preferences*. The *Preferences* window will appear. Double click the *Mail & Newsgroups* folder and select *Mail Servers*. You will be required to provide information on the following parameters:

   - Incoming Mail Server
   - Outgoing mail (SMTP) server
   - Outgoing mail server username

3. Click on the *Add* button. The *Mail Server General Properties* will appear. You will be required to provide information on the following parameters:

   - Server name
   - Server Type (Choose the IMAP server)
   - Username

   After providing the information, click the *Advanced* folder. Uncheck the "Show only subscribed folders" to view the *Shared* folders and check the "server supports folders that contain sub-folders and messages" option. Then, click on the *OK* button.

Question and Answer.....

Continued from page 11

2. Start the LDAP Server manually

3. Open MS-DOS prompt and go to C:\ProgramFiles\IMA\Internet Exchange 4 folder

4. Run the *dbupdate -r* command

5. Re-start Internet Exchange

If there are still stuck messages in the SMTPC Queue folder after doing the procedure mentioned above, you may have to manually force the delivery of the stuck messages by going to the SMTPC Queue Status web administration interface. To go to the SMTPC Queue Status page. Click the SMTPC icon on the Top Menu of the Internet Exchange Main Web Interface. The SMTPC Main Web Interface will appear. On the left-hand side of the screen, click the Queue Status link. The SMTPC Queue Status page will apper. Once here, select all the messages and then click on the *Process Messages* button.

Internet Exchange News

A monthly publication of International Messaging Associates, Ltd.

Staff

Editors..... Rio Peralta, Ana Cruz, Karen Madrid
Editorial Consultant..... Tim Kehres
Graphic Artist..... Ana Cruz, Rio Peralta
Contributor..... Ogie dela Cruz, Cesar Chiong

Please send your comments and suggestions to doc@ima.com

Questions & Answers

Q: I am using the vacation utility of Internet Exchange Messaging Server 4.1. I created a message filter and defined this filter to reply with a vacation message to incoming messages from my hotmail account. I used my hotmail account to send a test message and I successfully received a vacation message in response. Minutes later, using the same hotmail account, I sent another test message, but was not able to receive another vacation message. Am I missing something?

A: The Mailsort Vacation Utility by default, is configured to send a vacation message to a specific sender once within seven days. Thus, if the vacation utility already replied to your hotmail account, it will not send any more messages to the same hotmail account until after seven days. This is the reason why on your second trial, you no longer received a response from the vacation utility. If you wish, you may modify the default interval of seven days to your choice of time interval (e.g. 1 day) in the [LocalMail] section of the IEMTA.INI file. To modify the time interval, simply change the default setting from "ReplyInterval=7" to "ReplyInterval=1".

Q: Our Corporate Audit Department run several security scanning tools to examine our SMTP mail gateway. The tools identified two problems:

1. **SMTP allows VRFY remote command**
2. **SMTP allows EXPN remote command**

What does VRFY/EXPN command mean? How are we going to disable these commands?

A: The VRFY (verify user) command allows a remote host to confirm whether a particular user exists in a certain post office, while the EXPN (expand mailing list) command allows a remote host to confirm whether a certain mailing list exists in a certain post office. To disable these commands, go to Internet Exchange system administrator web configuration screen. Click on the SMTPD icon on top of the configuration screen. The SMTPD Control screen will appear. Select the SMTPD Options link. From the SMTPD Options screen, tick the check box of the following:

- Disable VRFY command
- Disable EXPN command

Q: We have approximately 1,500 messages stuck in the C:\Program Files\IMA\Internet Exchange 4.1\Msgqueue\smtpc folder. Deleting the *.btr files and all *.ccmail files had no effect. When I re-started the Internet Exchange, the messages were still in the queue folder. The "Queue Status" page on the Preprocessor web interface does not reflect any messages, when there are hundreds of messages in the actual SMTPC queue folder. How do we solve this problem?

A: To reflect the number of pending messages to the SMTPC Queue Status page of the Preprocessor web interface, follow the procedure below:

1. Shutdown all the Internet Exchange Modules

Continued on page 10 -->

"The Internet is like a giant jellyfish. You can not step on it. You can not go around it. You have to get through it."

-John Evans

This Month's Tip

Subscribing to/Unsubscribing from the Available Mailing Lists via the Internet Exchange Free Lists Page

The Free Lists Web Administration Interface of the Internet Exchange 4.1 allows the end users to subscribe to or unsubscribe from the open mailing lists available on the Messaging Server.

To access the list of open mailing lists, click the *Free Lists* link from the *Main Web Administration Interface*. A screen displaying the list of open mailing lists, with short description as provided by the system administrator, will appear. To subscribe/unsubscribe to the list, click the link of a particular mailing list address (e.g. jazz@ima.com). The Mailing List Subscription Form will appear. To subscribe to the preferred mailing list, enter your e-mail address on the input text box. Select the mode of delivery either immediate or digest. In immediate mode, when messages are posted to a mailing list, the DL Manager sends them immediately to the mailing list's subcribers. In the digest mode, posted messages are allowed to accumulate in the local archive of the member(s) who selected this mode and are sent to the subscriber based on a pre-determined schedule set by the list owner/system administrator as requested by the subscriber. Then, click on the *Submit* button. The subscription request will then be forwarded to the DL Manager. A confirmation message is then sent to the new member informing him that his subscription request has been approved. Upon receipt of the confirmation message from the subscriber, the subscriber will be automatically added to the requested list.