May 1999
Volume 2, Issue 5

Internet Exchange News

Inside this Issue

International Messaging Associates (IMA) Ltd.
Hong Kong Computer Center
54-62 Lockhart Road
Wan Chai, Hong Kong
Tel: +852 2520-0300
Fax: +852 2648-5913

IMA Philippines Inc.
The Peak Tower
15/F 107 Alfaro Street
Salcedo Village
Makati City, Philippines
Tel: +63 (2) 811-3999
Fax: +63 (2) 811-3939

US Support: +1 (408) 481- 9985
US Sales: +1 (408) 481- 9985
US Fax: +1 (888) 562 - 3561

Email: info@ima.com
Website: www.ima.com

NEWS FLASH!!!

Internet Exchange 4.0 Beta program now ready for download: *IMA's new product combines innovative features with easy-to-use Web interfaces*

Internet Exchange 4.0 from International Messaging Associates (IMA) is now available for initial Beta testing. Internet Exchange 4.0 is IMA's latest messaging solution for the Internet community and boasts of a number of features which can easily be configured via user-friendly, Web-based interfaces.

Internet Exchange 4.0 consists of several modules which are in turn made up of different sub-modules for performing specific actions on outbound and inbound messages. Its main components are the Internet Exchange Messaging Server (IEMS), the IMAP4 Optimized Message Store, and the cc:Mail and Lotus Notes Connectors. The IEMS is made of several modules: namely the LDAP-based Directory Server, the Batch SMTP Module, the SMTP Client, the SMTP Daemon, the Distribution List Manager, the Message Switch, and the Preprocessor Unit. The Preprocessor Unit consists of several sub-modules: the Anti-spam and Anti-virus Modules and the Channel Action Matrix, which is used to configure which of the Preprocessor Unit's sub-modules should run for a specific message.

The Message Store consists of the the IMAP4 and POP3 servers and MailSort. The IMAP4 and POP3 servers allow IMAP4- and POP3-capable clients such as Microsoft Outlook, Netscape Mail, and Eudora to receive messages via the IEMS. MailSort, on the other hand, is a mail sorting utility developed by IMA that enables the user to assign incoming messages to predefined folders using information contained in those messages' headers and/or body.

The cc:Mail and Lotus Notes Connectors enable cc:Mail and Lotus Notes users, respectively, to connect to the IEMS and send and receive message to and from the Internet.

Internet Exchange 4.0 comes with a number of highly configurable features. Configuration is carried out by the system administrator via simple Web-based interfaces. The product also comes with troubleshooting tools to spot and fix problems that could affect the performance of the system.

To participate in the Internet Exchange 4.0 Beta program, go to the IMA website at *http://www.ima.com*.

The Internet Exchange Messaging Server Preprocessor: *A sure-fire protection against computer viruses and junk/spam mail*

Internet electronic mail (email) provides both small and large organizations with an inexpensive but reliable tool for communicating with their customers and employees, as well as with other organizations. However, like most technologies, Internet email is not immune to problems. Recently, the Internet community has been the victim of serious virus attacks which were carried out via email. One such virus, named Chernobyl, infected thousands of computers in several countries, particularly in Asia. This virus has the capability to erase hard drives and corrupt a PC's BIOS. Another virus, named Melissa, is launched when a user opens a Microsoft Word document attached to a message. The virus disables Word's usual warning when a Word template is altered and is also capable of sending out email messages to the first 50 people in a victim's Microsoft Outlook address book.

Another problem facing Internet email users is spam mail. Spam mail is an unsolicited mail that are considered a nuisance to email users since they contribute to the delay in the delivery of legitimate email and they consume a considerable amount of storage space.

To provide system administrators with a cost-effective solution protecting their systems against viruses and junk mail, nternet Exchange 4.0 comes with several tools to address these problems. The MTA Preprocessor is made up of three modules, the Anti-virus Module, Anti-spam Module, and Channel Action Matrix.

Anti-virus Module

Internet Exchange 4.0's anti-virus module is a 32-bit multi-threaded standalone pre-processing module capable of performing simultaneous virus scanning for MIME and non-MIME message attachments. Each thread created by the anti-virus engine is responsible for processing one message at a time, allowing high message throughput.

When a message enters the Anti-virus Module (preprocessor), it will first decode the attachment. Then it will scan the said attachment by invoking the anti-virus program indicated by the MTA administrator. Once a virus is detected, the anti-virus module can optionally delete the message right away (with an option to notify the Internet Exchange Administrator that the message has been deleted), bounce back the message to the original sender, or archive the message to a quarantine directory for later manual processing.

Decoding attachments

To ensure that all message attachments are scanned, the Anti-virus Module decodes all attachments according to their encoding. Most MTA's use MIME encoding in attachments, but there are still few sites that use non-MIME encoding. Internet Exchange has solved this problem by using decoding procedures that are based on the encoding method used in the attachment(s). After the attachment has been decoded, the anti-virus engine calls the scan procedure to perform the actual scanning of the attachment.

File attachment scanning

Since most of the virus scanning software use the filename extension to invoke the appropriate virus scan routine, the Internet Exchange 4.0 Anti-virus Module is designed to recognize the original file extension using information available in the message file.

For MIME attachments, the file extension is retrieved from the internal MIME mapping table. This table stores the mapping between Content-type and the associated file extension of the attachments.

For non- MIME messages, the filename is retrieved in the following sequence:

- If the attachment is UUENCODED file, the Anti-virus Module will use the filename from the "BEGIN XXX <filename>" line.
- If the attachment is a BINHEX encoded file, the filename from the decoded BINHEX segment header will be used.
- If the "filename" parameter is present in the "Content-Disposition" header, the Anti-virus Module will use the value of "filename" parameter as the attachment filename.
- If the "name" parameter is present in the "ContentType" header, the value of the "name" parameter will be used as the attachment filename.
- If the attachment cannot be determined even after the checks above, the anti-virus module will do a lookup to find the corresponding filename extension from the Content-type header (if it is present in the MIME message) and assign a dummy name to the attachment.
- If all the above procedures have been performed and the file extension still cannot be determined, the Anti-virus Module will assign a <DEFAULT> value as the file extension. This value is configured by the gateway administrator.

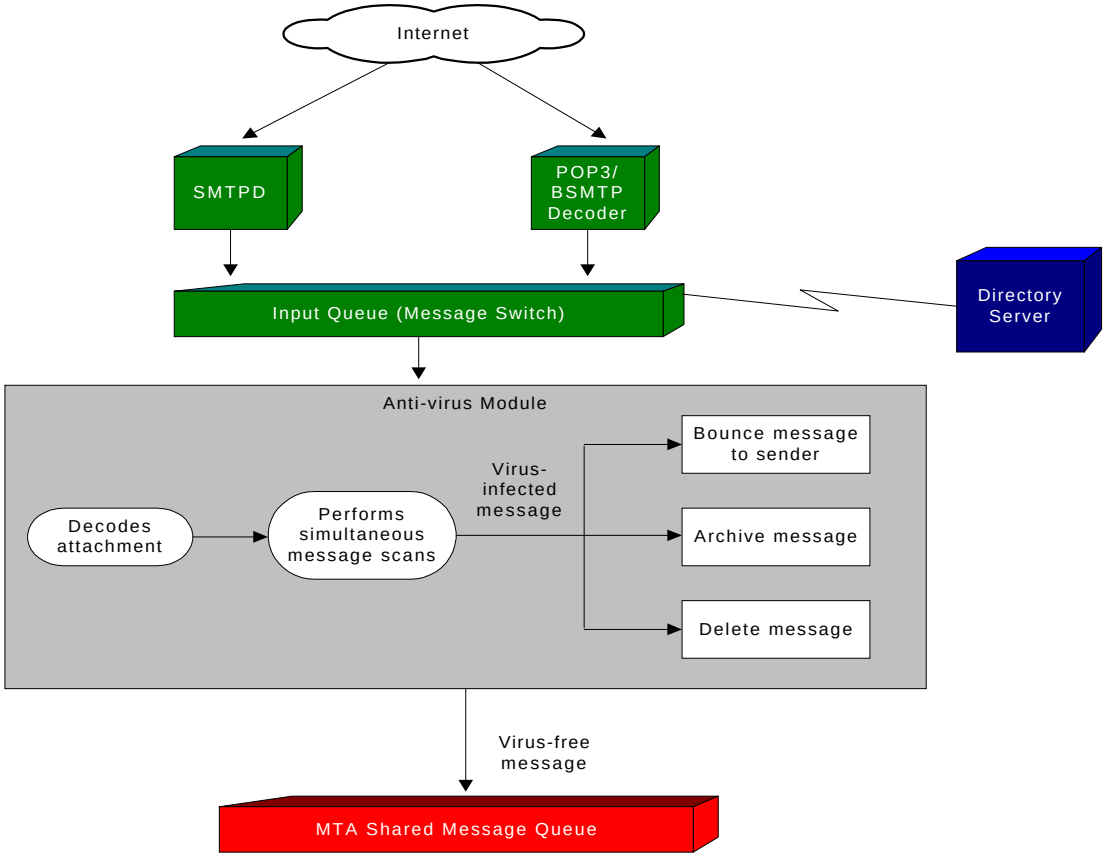


Figure 1. Message flow for the Preprocessor Unit's Anti-virus Module

When viruses are detected, the anti-virus engine handles the message based upon the option chosen by the Internet Exchange administrator.

Handling virus-infected messages

When a message is found to be infected with a virus, the infected message can be acted upon as follows:

- *Delete* – this tells the anti-virus plug-in to delete the message from the Internet Exchange Messaging Server (IEMS).
- *Archive* – this tells the anti-virus plug-in to move the message file from the IEMS to the virus archive directory. The file extension of the archived mail is .VIR.
- *Bounce back to sender* – this tells the anti-virus plug-in to bounce the infected message back to the original SMTP envelope sender. The bounced message body indicates that the message's attachment contains a virus and is being returned by IEMS.

Anti-virus engines supported

Internet Exchange 4.0's Anti-virus Module supports several anti-virus engines. The system administrator has the option to use a single anti-virus engine or install several anti-virus applications in case he/she wants several layers of anti-virus protection. Internet Exchange 4.0 supports the following:

- *McAfee VirusScan* – this software engine supports the following platforms: DOS, Windows 95, Windows 98, and Windows NT.
- *Sophos Anti-Virus for Windows 95/98* – this application has the capability to automatically eliminate many common viruses and can easily be installed. It can be updated monthly with the latest anti-virus technology via the World Wide Web or via a CD or floppy disk.
- *Sophos for Windows NT* - this application is specifically designed for the Windows NT platform and has the same features found in Sophos Anti-Virus for Windows 95/98.

- *F-PROT Professional Anti-Virus Toolkit* – this anti-virus engine supports the following platforms: DOS, Windows 3.1, Windows 95, and Windows NT.

- Anti-virus packages from Computer Associates.

Anti-spam Module

The Anti-spam Module of Internet Exchange 4.0 provides the administrator with options to control the reception of unsolicited and unwanted SPAM mail messages. In addition to providing control over what sites can use Internet Exchange 4.0 as mail relay, the system can be defined to reject mail during the SMTP exchange from:

- Any number of hosts and domains.
- IP addresses.
- IP address ranges.
- Hosts with supplied names that cannot be verified via the DNS.

or even based on the following message headers after message reception:

- From:
- Sender:
- Reply-To:
- Resent-From:
- Return-Path:

Connection-based Detection

Spam messages can be detected and acted upon either during the SMTP transaction with the remote site, or once received by the Anti-SPAM preprocessor module. Connection-based detection includes the automatic rejection during the initial stage of the SMTP connection based upon pre-defined IP addresses or names, non-verifiable host names during the HELO startup, or the unauthorized routing of third-party traffic. This blocks out potential spammers even before they can enter the system. Connection characteristics that can be analyzed during the SMTP transaction as a basis for denying service include:

- Remote IP Address
- Supplied Remote Host Name (SMTP HELO Command)
- Supplied Sender Address (SMTP MAIL FROM Command)

Site/network blacklisting

Unsolicited or spam messages usually originate from known networks. These networks are either owned by the spammers, or by careless service providers who allow their networks to be abused in this manner. If either the network address of the spammers machine or network (range of addresses) are known, SMTPD can shutdown the connection request (with an error code 553) before the SMTP transaction ever starts.

The MTA administrator defines what IP addresses or IP address ranges are authorized to send messages to Internet Exchange. When a new incoming SMTP connection is requested, SMTPD will scan the IP address list and check if the IP address of the remote host is in the unauthorized list. If a match is found, SMTPD will reject the connection and respond with an error stating that the peer host is not authorized to send mail to this MTA. This has the advantage of detection and control of abusive messages before any local or network resources are consumed.

Third-party relay prevention

Many spamming organizations rely upon innocent third parties to carry and distribute their junk mail. For this to work, the spammer relies upon the unsuspecting MTA to accept and relay its traffic, usually generating far more outgoing traffic than inbound. This technique not only shifts the costs of delivery (both in terms of machine and bandwidth resources) to the third party, but can also be used to conceal the true identity of the spammer.

During the SMTP transaction where the message recipients are identified, Internet Exchange will check to see if the remote site (based upon its network address as above) is authorized to relay messages through the local MTA. If the remote site is not authorized, the message will be rejected during the SMTP dialog.

Internet Exchange can be fully configured so that sites or networks that are known to be unfriendly are not allowed relay authorization, while at the same time allowing relaying for desirable machines or networks, such as local POP3 or IMAP4 mail clients.

Remote name verification

The first operation that two connecting SMTP machines perform when starting up is to identify the name of the calling machine. This is done via the SMTP HELO command where the originating site supplies its fully qualified domain name. At this stage, Internet Exchange has the option of performing a reverse lookup based upon the known network address of the sending site in order to verify this name. This is to make sure that the originating site is who they claim to be and not attempting to masquerade as another site. If the supplied name and the verified name do not match, Internet Exchange can be configured to terminate the connection.

Sender address verification

The message sender address (envelope) is conveyed in

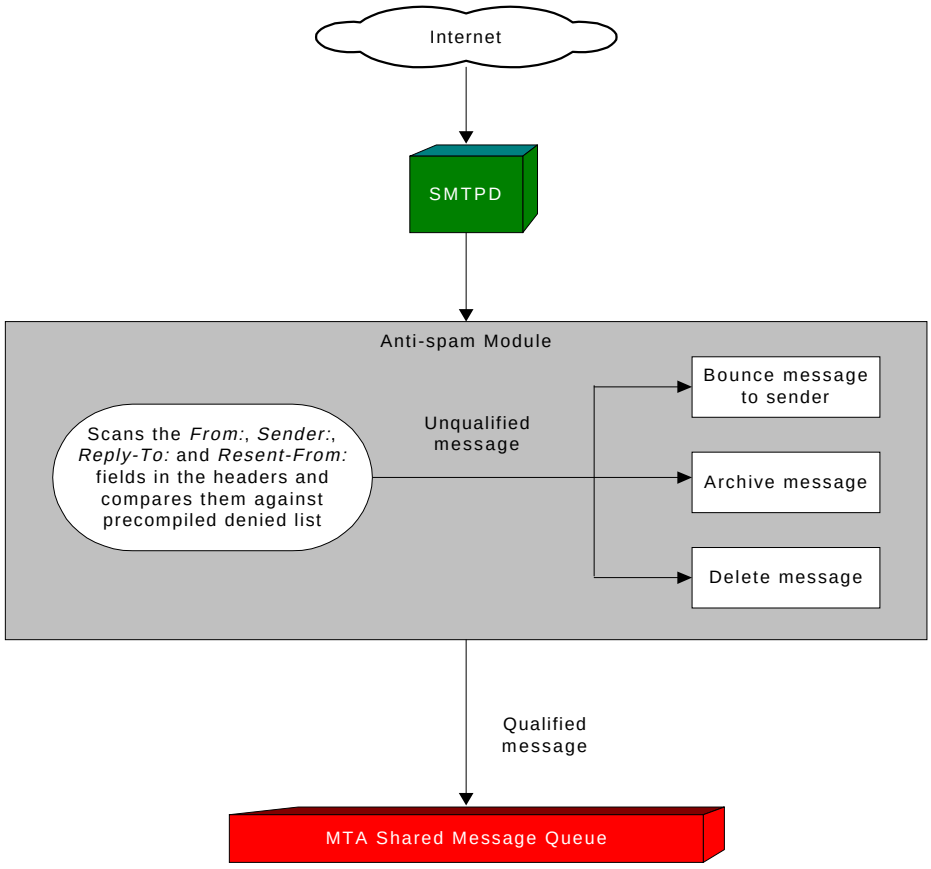


Figure 1. Message flow for the Preprocessor Unit's Anti-spam Module

the SMTP MAIL FROM command prior to the actual transmission of the message. If the originator has not forged this address, it will point back to the original spammer. Internet Exchange allows for the configuration of known addresses that correspond to unfriendly addresses. When an address of this type is encountered during the SMTP MAIL FROM dialog, the message is rejected before it has a chance to be sent across the network.

Preprocessor-based Detection

If a spam message makes it past the connection-based controls, rules can be applied using the Preprocessor Unit's Anti-spam Module to perform additional checks by analyzing information found in the RFC-822 message headers. Once detected by the Anti-spam Module, the offending message(s) can optionally be moved to a pre-defined directory, bounced back the message sender, or deleted silently.

The Internet Exchange administrator can maintain a list of spammers' email addresses, enabling the MTA to reject any messages coming from any of the configured addresses. When Internet Exchange receives a new message, it will check the "From:" header of the incoming message and check if it is included in the denied list. If a match is made, the MTA will perform the necessary action on the message as defined earlier by the Internet Exchange administrator.

The spammer's address or domain can be compared to information found in any of the following RFC-822 message headers:

- From:
- Sender:
- Reply-To:
- Resent-From:
- Return-Path:

Actions on Spam Mail

Once a message has been tagged as spam by the Anti-SPAM preprocessor module, several options exist for it's handling. These options are:

- 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

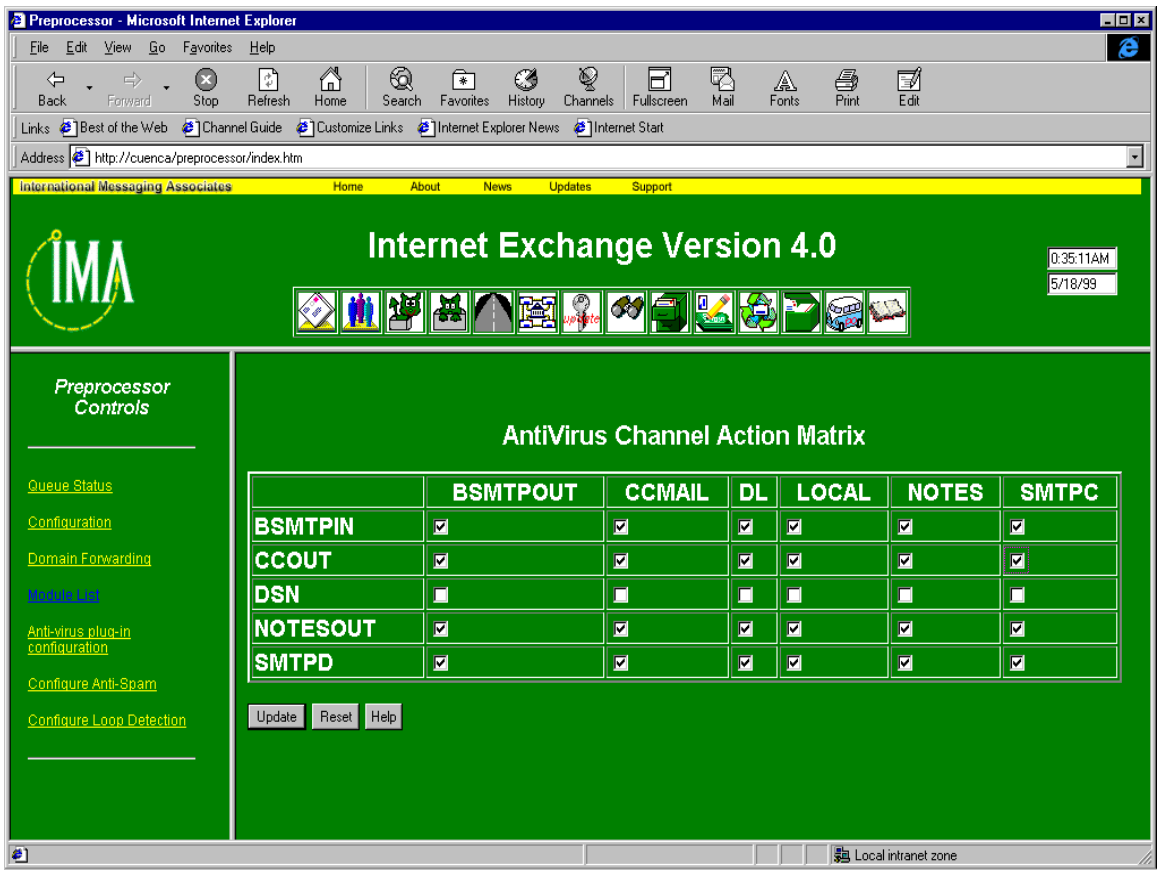
Channel Action Matrix

Internet Exchange 4.0 provides a Channel Action Matrix for each module in the Preprocessor Unit. With the Channel Action Matrix, system administrators are provided with a flexible tool for configuring which modules in the Preprocessor Unit should run for a particular message, based upon message flow or routing within the MTA. For example, to minimize delay in message delivery, the system administrator may not want to run the Anti-virus for messages coming from a cc:Mail user and destined to another cc:Mail user or to a Lotus Notes user within the system. Or he may want to run the Anti-virus Module only for messages coming from the Internet and not for messages bound for the Internet. These controls are easily configured by the system administrator in the Channel Action Matrix. The figure below shows a screen that displays information from the Channel Action Matrix configuration file as configured by the system administrator.

Conclusion

Electronic mail or email is one of the most widely utilized Internet technologies today, and its use is likely to become more widespread in the future as we gradually move on to a paperless society. However, the usefulness of Internet email is being threatened by the proliferation of such irritants as spam mail and computer viruses. The latter can create serious damage not only to stored data but also to the hardware itself. The former, on the other hand, can lead to misallocation of precious bandwidth and storage resources.

IMA recognizes these problems and has come up with a solution for protecting email systems against junk and virus-infected messages transmitted over the Internet. IMA's Internet Exchange Messaging Server features the Preprocessor Unit, which consists of the Anti-spam and Anti-virus Modules. Both modules are highly configurable and can be programmed to scan outgoing and incoming email based on a wide range of message parameters. In addition, the Anti-virus and Anti-spam modules are both multithreaded applications, thereby ensuring high throughput and fast message delivery. With these features, the Internet Exchange Messaging Server is able to detect junk and virus-infected messages and prevent them from harming the system.



Questions & Answers

Q: Recently, there were reports that a virus, known as Melissa, has infected hundreds (probably thousands) of computers via email and destroyed important files. What is the Melissa virus? Is there a way for us to protect our messaging system against this virus?

A: The Melissa virus is spread over the Internet via a file attachment called LIST.DOC. When users open this file in Word 97 or Word 2000, the Melissa virus is launched. It then prompts Microsoft's Outlook email program to send an infected message to the first 50 addresses listed in the user's Microsoft Outlook address book. The email is made to appear to come from the user and the subject line reads "Important Message From (name of infected user)". The message body reads "Here is that document you asked for ... don't show anyone else."

After sending an infected message to other users, the virus proceeds to infect other Word documents. It is activated when the minute of the hour matches the day of the month (e.g. the time is 12:21 and it is the 21st of February). It inserts the following Bart Simpson quote into the active Word document: "Twenty-two points, plus triple-word score, plus fifty points for using all my letters. Game's over. I'm outta here."

The Melissa virus spreads rapidly and can crash email servers by flooding them with infected messages. It can also send out infected but confidential files to other users without the knowledge of the owner of those files.

The Anti-virus Module in Internet Exchange 4.0 provides system administrators with a tool for fighting viruses like Melissa. The Anti-virus Module can be configured to perform virus scans on outgoing and incoming messages. To download the beta version of Internet Exchange 4.0, go to the IMA website at *http://www.ima.com*.

Q: We usually enounter the "VIMOPenSession Failed" error. How do I solve this problem?

A: When you encounter this kind of error, shut down Internet Exchange and delete all files in your system's TEMP directory (not the Internet Exchange TEMP directory). Then do the following:

1. Check the iecc-mail\queue\bad directory for corrupted messages. Then move such messages to the appropriate IN or OUT queue directory and rename them to *.msg.
2. Delete MESG.BTR and LOCK.BTR under the iecc-mail\queue directory.
3. Run the MESG.EXE utility and click on the Rebuild button. Close this utility after the rebuild process is completed.
4. Restart Internet Exchange.

This will get rid of the "VIMOpenSession Failed" error.

"Debugging is anticipated with distaste, performed with reluctance, and bragged about forever." **– Anonymous.**

This Month's Tip

Fast SYSMAN Startup for Internet Exchange 3.x

When a network problem occurs, a large queue of messages can build up in the cc:Mail Post Office or Notes SMTP.BOX. When this happens, gateway startup can become very slow. To enable fast gateway starup, do the following:

1. Click on the  button on the Internet Exchange Control Panel.
2. On the next screen, click on the *Gateway* tab. A screen for configuring various gateway options will appear.
3. Click on the *Advanced...* button at the bottom of the Gateway Configuration interface to view the screen for configuring advanced gateway options.
4. Enable the *Fast SYSMAN startup* option by checking the appropriate box.
5. Click on the *OK* button to implement the changes made.

When the *Fast SYSMAN startup* option is activated, the queue counter update does not occur until either a key has been pressed or the mouse has been moved. Also, the queue messages display is not updated until the next time a key is pressed or the mouse is moved. This significantly increases the speed of gateway startup.

NOTE: This option should not be set when running unattended dialup PPP.