October 2000
Volume 3, Issue 10

Inside this Issue

International Messaging Associates (IMA) Ltd.
27/F, China Resources Building
26 Harbour Road
Wan Chai, Hong Kong
Tel: +852-2520-0300
Fax: +852-2648-5913

IMA Philippines Inc.
6/F, Hanston Building
Emerald Avenue, Ortigas Center
Pasig City, Philippines
Tel: +63 (2) 637-9090
Fax: +63 (2) 637-9898

US Toll Free No.: +1 (800) 549-2762
US Fax No.: +1 (888) 562-3561

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

Internet Exchange News

NEWS FLASH!!!

Internet Exchange 4.11 Allows Access to Mailing List Archives, Handles TNEF Attachments

To allow access to the mailing list archives and enable the efficient handling of message file formats, **Internet Exchange Messaging Server version 4.11** now features the Distribution List (DL) Archive and Transport Neutral Encapsulation Format (TNEF) Expander.

The DL Archive allows both mailing list members and non-members to access the open mailing list archives, but limits the access of the closed mailing list archives to its members (either local or remote users) only. Local users are those users defined in the Directory Service. Remote users, on the other hand, are those users not defined in the Directory Service, but are members of the closed mailing list.

All closed mailing list members are required to go through the DL Authentication procedure before they can access the list archives. The authentication procedure requires the mailing list members to enter his username and password as defined in the Directory Service. However, remote users must first undergo registration procedure before the authentication. To register, remote users must enter their username and password in the DL Archive registration page. This process verifies if the e-mail address entered is a member of the list. Once verified, an e-mail will be sent to the list member confirming his request. The user must reply to the confirmation e-mail before he will be registered.

Continued on page 2 --->

Internet Exchange Offers an Innovative Approach to Message Transfer with SMTPC and SMTPD

Focusing support for Internet protocols and standards, specifically SMTP (Simple Mail Transfer Protocol), through innovative design features, Internet Exchange incorporated two modules, the SMTPC (Simple Mail Transfer Protocol Client) and the SMTPD (Simple Mail Transfer Protocol Daemon) into its system design. The two Internet Exchange modules carry features that enhance the message transfer process through multi-threading, message priority handling and mail routing.

Remote messaging systems that have messages destined to Internet Exchange send connection requests to the SMTPD. Once the SMTPD detects a connection request, it creates a new thread that will establish a new SMTP connection with the remote messaging system. After the connection is established, the SMTPD will receive messages from the remote messaging system through the SMTP connection and create a new queue entry for each message received.

The SMTPC module, on the other hand, is responsible for sending messages from Internet Exchange to the Internet. The first thing that the SMTPC does is to retrieve the messages bound to the Internet from the Internet

Continued on page 2--->

The DL Archive sorts messages based on any of the following sorting criteria: *Date*, *Author* or *Thread*. *Archive by Date* sorts all messages on a daily basis. Messages that were sent on the same day will be grouped together. *Archive by Author* sorts all messages by author, based on the *From* field of the archived message. *Archive by Thread* sorts all messages by subject, based on the *Subject* field of the archived message. A subject thread is created whenever a message generates one or more reply messages.

The Distribution List Archive can be accessed by clicking the *Internet Exchange Messaging Server 4.11 Main Web Administration interface*. For more information, please see *http://www.ima.com/pdf/dlarchive.pdf*.

Internet Exchange 4.11 also incorporates a Preprocessor plug-in expander responsible for handling TNEF attachments. TNEF is a proprietary format used by the Microsoft Exchange and Outlook e-mail clients when sending messages in RTF (Rich Text Format). Although TNEF attachments can effectively contain Word documents, Excel spreadsheets, video clips, programs, among others, only Microsoft mail products can properly recognize and read it. Most non-Microsoft e-mail clients cannot translate TNEF blocks. Thus, whenever a TNEF-encoded message sent using a non-Microsoft e-mail client, the TNEF part appears as a long sequence of hexadecimal digits, either in the message itself or as an attached file (usually named WINMAIL.DAT). This WINMAIL.DAT file serves no purpose and can be deleted.

With the Internet Exchange TNEF expander, TNEF attachments are extracted as early as the pre-processing phase and submitted again in a separate message to the original recipient. This means that when you retrieve your message with TNEF attachments, you will receive two messages. The first message will contain the original message, while the second message will contain the extracted attachments.

With the two new features, Internet Exchange 4.11 provides powerful messaging solutions to enterprise messaging needs.

Internet Exchange Offers...

Continued from page 1

Exchange MTA Shared Message Queue. Then, the messages are transferred either to the Pending Queue or to the Deferred Queue (*please see page 3 for a detailed description of these queues*) while SMTPC establishes the required number of connections with the external SMTP servers. After the connection is established, SMTPC will retrieve the messages either from the Pending or Deferred Queue. The messages will then be transferred to the appropriate Internet mail hosts.

SMTPD KEY FEATURES

Multi-threaded Architecture

The SMTPD features a multi-threaded architecture (see **Figure 1**), which enables SMTPD to create multiple threads that can handle multiple connections and manage simultaneous processing of messages. This multi-threaded architecture is made up of the following components:

- *Master Thread Manager*
  Continuously listens to the SMTP port for incoming connection requests. Upon receipt of a connection request, the master thread manager creates a new worker thread to establish a new connection.

- *Worker Thread*
  Manages the connection and the transfer of messages between the Internet Exchange and the external SMTP servers.

Spam Control

SMTPD performs anti-spam checks on messages before routing them to the MTA Shared Message Queue. Using this feature, Internet Exchange can detect and act upon junk and spam messages even before they enter your system. Currently, the SMTPD module applies the following connection-based detection methods:

- *Site/Network Blacklisting*
  Internet Exchange allows the system administrator to create a list of all the IP addresses/IP ranges that are authorized to send messages to the Internet Exchange. If the SMTPD receives a connection request from a remote host whose IP address is not included in list, SMTPD will automatically deny the connection.

- *Third-party relay prevention*
  The Internet Exchange SMTPD module has a list of remote sites that are authorized to relay messages to the Internet Exchange. During the SMTP transaction, where the message recipients are identified, Internet Exchange checks if the remote site is included in the list of sites authorized to relay messages. If the remote site is not included in the list, the SMTP connection is rejected.

- *Remote Name Verification*
  During SMTP start up, Internet Exchange identifies the remote machine that sent a connection request. Via the SMTP-HELO command, the remote machine sends its FQDN (Fully Qualified Domain Name). Internet Exchange, using the supplied FQDN, can perform reverse DNS lookup based upon the known network address of

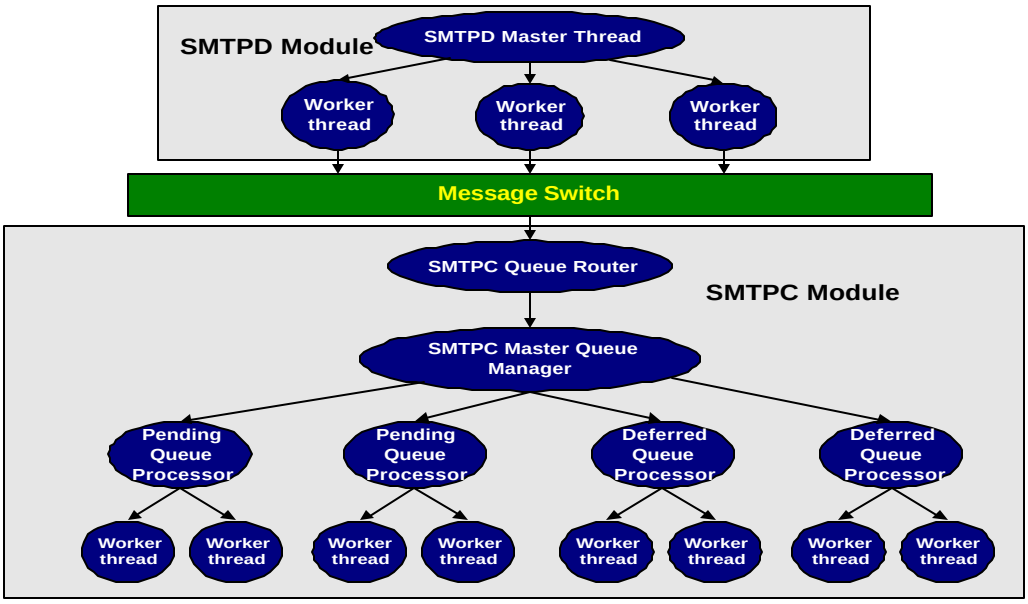

Figure 1: SMTPD and SMTPC Modular Design

the sending site to verify the name. If the supplied name and verified name do not match, SMTPD can terminate the connection.

SMTPC KEY FEATURES

Hierarchical Multi-threaded Architecture

SMTPC features a hierarchical multi-threaded architecture (see **Figure 1**), which assures high scalability and performance. This hierarchical multi-threaded architecture consists of two components:

- *SMTPC Queue Router*
  Retrieves messages from the Internet Exchange MTA Shared Queue and determines whether the messages should be routed to the Pending Queue or Deferred Queue.

- *SMTPC Master Queue Manager*
  Controls and synchronizes the following queues:

  Pending Queue
  Temporarily stores the messages that have to be sent out immediately to the Internet. The Pending Queue has one or more pending queue processors, which process the messages. The pending queue processors are responsible for establishing connections with the external SMTP servers and delivering the mail messages to the remote hosts via SMTP. If the delivery of a message in the Pending Queue is unsuccessful, it is passed on to the Deferred Queue so that it can be delivered at a later time.

  Deferred Queue
  Contains messages that are either intentionally deferred or whose previous delivery attempts have failed. These messages will be stored in the Deferred Queue and will not be delivered immediately. The delivery attempts are considered "failed" when any of the following conditions are encountered:

  - The option *queue mail before attempting delivery* is enabled. When this option is enabled, messages will be placed to the Deferred Queue and will not be delivered immediately. This is particularly useful if the destination domain is an ETRN SMTP domain. Dialup SMTP hosts connect to the Internet intermittently, and an attempt to deliver messages to such hosts when they are not connected to the Internet will usually fail.
  - There is a temporary DNS error during the domain name resolution process.
  - A destination host is found, but the SMTP connection cannot be established.
  - The destination SMTP server issues a temporary SMTP response code.
  - The SMTP connection is aborted prematurely due to network problems.
  - The destination SMTP server did not reply within the configured time.

  Messages in the Deferred Queue are further grouped into different SMTP domain channels using the information in the recipient addresses. This allows server side ETRN support and prevents the deferred messages from delaying the processing of new messages. Like the Pending Queue, the Deferred

Queue is also equipped with Deferred Queue Processors which process the messages on a per channel basis. During each scheduled queue run time, one or more deferred queue processors are created for every SMTPC domain channel by the SMTPC to handle deferred outgoing messages. Messages for each SMTPC domain channel are processed according to their message priority weight.

After the priority weight for each message is determined and the messages are arranged according to their priorities, SMTPC will attempt to deliver the first message from each SMTPC channel. If the first message in the SMTPC channel is delivered successfully, the Deferred Queue processor will create another thread to deliver the subsequent messages in the channel. If the delivery attempt for the first message failed, the subsequent messages in the entire channel will remain queued. This approach increases the efficiency of the system by eliminating unnecessary message delivery attempts.

Message Priority Handling

SMTPC features a mechanism for message priority handling which guarantees not only high throughput but also the orderly handling of messages with different priorities. This mechanism basically allows the SMTPC to assign a priority weight for each message based upon three factors:

- The pre-defined message precedence
- The message size
- The total deferred time

The message priority weight is calculated using the formula:

*Priority Weight = (precedence*Mp)+(size*Ms)+(deferred_time*Md)*

where:

Mp is the precedence multiplier;
Ms is the size multiplier; and
Md is the deferred time multiplier

The priority weight is an integer value. The lower the priority weight, the higher the priority level and the sooner the message is processed. The message precedence and size multiplier are configurable parameters that the system administrator can define, whereas the deferred time multiplier is system generated since it denotes how long the message has been in the Deferred Queue. A message with a longer total deferred time is given higher priority over the messages that arrived recently.

Mail Routing Handling

SMTPC uses several criteria when routing Internet mail messages. The routing options are:

- *Domain Name System (DNS) host name lookup*
  Used to locate and translate an Internet domain name into an IP address. A domain name is a meaningful and easy-to-remember "handle" for an Internet address (i.e., *domain.com).*

- *Host Table lookup of destination host*
  An internal host table, usually a text file, is used by the

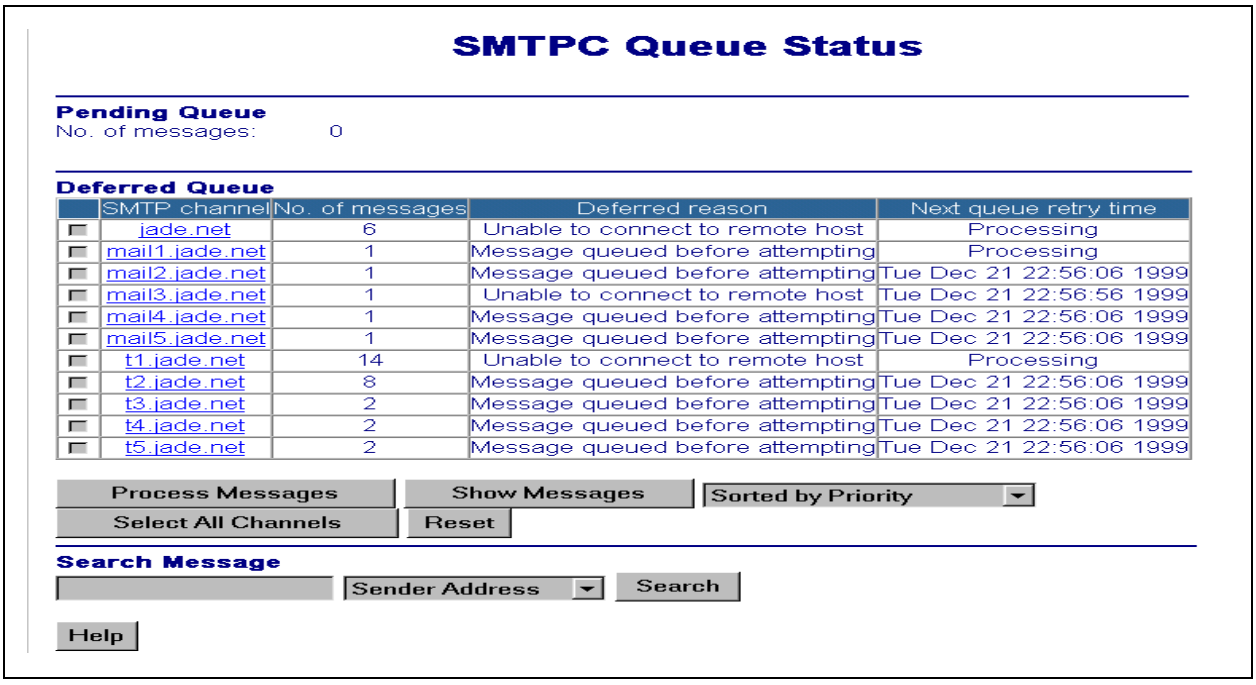

Figure 2: SMTPC Queue Status for Pending and Deferred Queues

SMTPC to determine the IP address of the recipient host. The exact format of the host table depends upon the TCP implementation. The location of the host table should be specified upon the installation of Internet Exchange.

- *DNS then Host Table lookup*
  In the event of a failure to locate and translate an Internet domain name into an IP address, Internet Exchange will perform a *Host Table lookup* to determine the IP address of the recipient host.

- *Host Table then DNS lookup*
  When the IP address of the recipient host cannot be determined, Internet Exchange will perform a *DNS lookup* to locate and translate an Internet domain name into an IP address.

- *Delivery to Default Mail Relay Host*
  When the Internet Exchange is configured to use a default mail relay host, messages will be sent to a primary mail forwarder for further routing. If this mail forwarder cannot be contacted for some reason and the secondary mail relay host is defined, the machine will use the secondary mail relay host. In this case, it will occasionally check to see if and when it is possible to switch back to use the primary relay host.

Internal Database Storage
SMTPC uses several databases to store messages and peer information. The *MESG.BTR* is used to store the envelope, priority value and status information of messages. The *CHANNEL.BTR* is used to store the status information for the SMTP Domain channel. The *PEER.BTR* is used to store the SMTP Domain Profile configuration information, such as queue run interval, queue run size, maxSMTP sessions, maxMsgPerSession and retryPeriod for each peer domain. Another database, the *DNS.BTR* is used to store the resolved DNS information.

SAMPLE SCENARIO

An Internet mail user *johndoe@jade.net* sends a message to an Internet Exchange user *jdoe@ima.com.* The mailer of the remote host (*jade.net*) will first establish a connection with the Internet Exchange SMTPD. Once the connection is established, the remote host transfers the message to the SMTPD, which will receive the message and later submit it to the MTA input queue for further processing.

After receiving the mail from *johndoe@jade.net*, *jdoe@ima.com* sends an e-mail reply to *johndoe@jade.net* on the Internet. The module that will facilitate the sending process of this message will be the Internet Exchange SMTPC. The SMTPC will initiate a connection with the remote host, which will eventually send the message to the external host *jade.net.* Once the connection is established, SMTPC sends the message to the remote host on the Internet.

Question and Answer.....

Continued from page 8

Q: We are having major problems with our Internet Exchange for cc:Mail 3.13 gateway and are in need immediate help. Our main concern is, after every few messages received, the system generates a VIM error stating that it is related to the WIN.INI file. Below is a portion of the log file with the error messages generated.

Mon Apr 10 12:09:20 ccIn: [Error] VIMSendMessage failed: 2/1

Mon Apr 10 12:09:20 ccIn: [Error] VIM error message: A fatal error occurred.

Mon Apr 10 12:09:20 ccIn: [Error] VIM extended message: WIN.INI

Mon Apr 10 12:09:20 ccIn: [Error] VIM extended message: WIN.INI

A: The two log messages, "A fatal error occurred" and "WIN.INI", are the corresponding text for the VIM error 2/1. These two strings are returned from the VIM DLL. Lotus does not offer that much information on the VIM API explaining the cause of this error. Past experiences told us that these error messages are related to cc:Mail database problems. Running the post office maintenance utility “reclaim” resolves this problem most of the time.

Internet Exchange News

A monthly publication of International Messaging Associates, Ltd.

Staff

Editor..... Ana Cruz
Writers..... Rio Peralta, Karen Madrid
Editorial Consultant..... Tim Kehres
Graphic Artists..... Ana Cruz, Rio Peralta
Contributors.....Ogie dela Cruz, Ramiro Belialba

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

Highlight of the Month

Troubleshooting Network and SMTP Connectivity Using Network Diagnostic Tools

There are instances when your messaging server may fail to send messages to a remote host. The following diagnostic tools can help you troubleshoot the problem: *Nslookup*, *Ping*, *Traceroute* and *Telnet*. The *Nslookup* utility helps you identify the hostname or IP address of the remote host you are trying to send a message to. The *Ping* or *Traceroute* diagnostic tools enables you to check the remote host's network connectivity. The *Telnet* utility helps you verify the SMTP connectivity of the remote host you are trying to send a message to.

Identifying the Hostname or IP Address Using the Nslookup Utility

The *Nslookup* utility is a tool used in identifying the hostname or IP (Internet Protocol) address of the remote host (e.g. domain.com) you are trying to send a message to. It can also be used to query the DNS (Domain Name System) for certain types of records, such as MX (Mail Exchanger).

For example, to identify the hostname or IP address of the remote host "*domain.com*", go the MS DOS prompt and type "*nslookup*". Then, press the *Enter* key. Type "*set type=mx*" to instruct nslookup to query the MX records. Afterwards, type the domain name "*domain.com*" (you may replace domain.com with the name of the machine you wish to test) then press the *Enter* key. The results will be displayed on your screen. Using the example (see **Figure 1**), the default mail server for the peer domain is set to "mail.domain.com", which means that all the mail sent to "domain.com" is sent via "mail.domain.com". This procedure can help verify if the MX records are set properly and if the mail is being sent to the correct remote host to help resolve mail routing problems.

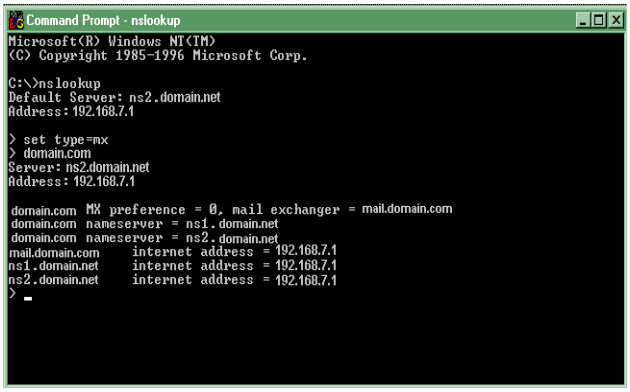

Figure 1: Running the Nslookup Utility

Checking the Network Connectivity Using Ping or Traceroute

To check the network connectivity of the remote host "*domain.com*", you may use *Ping* or *Traceroute*. *Ping* (Packet Internet Groper) is a basic Internet program that lets you verify if a particular IP address exists and can accept requests. It is used diagnostically to ensure that the host computer you are trying to reach is actually operating and responding to ICMP (Internet Control Message Protocol) requests.

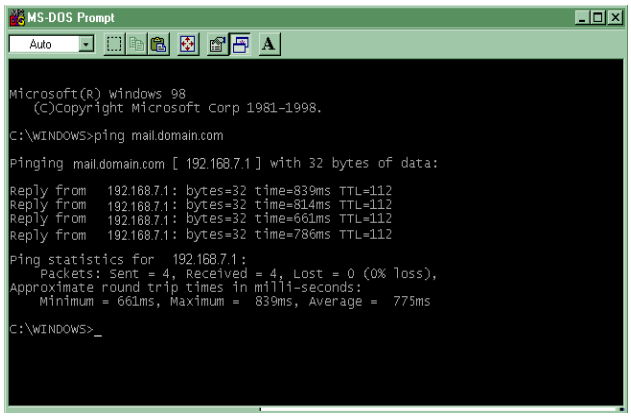

Figure 2: Running the Ping Diagnostic Tool

Traceroute, meanwhile, provides you with more detailed information on where a problem might lie. It records the route (the specific gateway for each hop packets take) between your computer and the destination host. It also calculates and displays the amount of time each hop took.

To run the *ping* diagnostic tool, open the MS DOS command prompt. Type "ping hostname" (e.g. mail.domain.com) and then click the *Enter* key (see **Figure 2**).

The *ping* diagnostic tool returns either "*Unknown host*", "*Request timed out*" or *Reply from*. If "*Unknown host*" is returned, the local DNS cannot resolve the name because the host is invalid or does not exist. Receiving "*Request timed out*" does not necessarily mean that there is a network connectivity problem. A possible cause could be that the remote host is temporarily down, busy or is behind a firewall. Receiving "*Reply from*" means there is no connectivity problem.

Note: The hostname *mail.domain.com* was obtained from the *mail exchanger* field of the nslookup utility (see **Figure 1**).

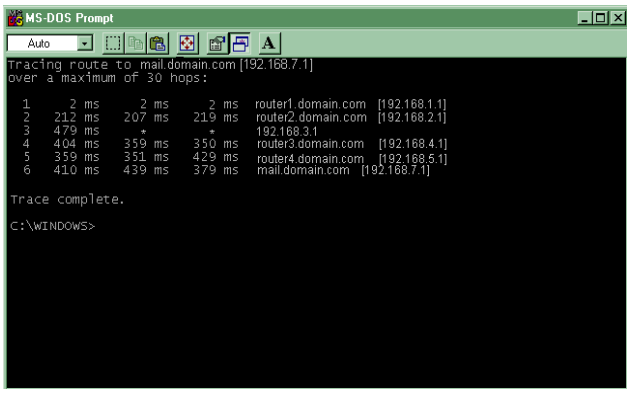

Figure 3: Running the Traceroute Utility

To run the traceroute utility, go to the MS DOS Prompt, and type in "*tracert mail.domain.com*". You can also enter the equivalent numeric form of the remote host's IP address.

Using the given example (see **Figure 3**), the traceroute utility recorded that it took 6 hops to reach the destination host *mail.domain.com*. The first hop took an average of 2 milliseconds to reach the first router, *router1.domain.com*. Then, another ICMP packet was sent to the second router, *router2.domain.com*. Traceroute continues to record the different hops and the time it took for each router to send a time exceeded message until the ICMP packet reaches the destination host.

If the traceroute displays a "*Destination host unreachable*" error reply or a row of three asterisks (***) during the first and second hop, it means that there may be a connection problem between your local network and ISP (Internet Service Provider). To determine if you have a problem, it is recommended that you perform a traceroute using another remote host's hostname or IP address. If the other remote host returns a positive value (e.g. *212ms 207ms 219ms router2. domain.com [192.168.2.1]*), it means that you do not have a network connection problem. If you still receive a "*Destination host unreachable*" error message or a row of three asterisks, then we suggest that you log off and then log again to your ISP to see if you can get a different connection route. If you see long connection time intervals (consistently in excess of 400ms), the server on that hop may be busy servicing other packets or the connection may be across a large distance (i.e., an ocean). This traceroute is only indicative of network traffic at that moment. It should be run several times to determine the pattern of the traffic. You may contact the network administrator of your local ISP to determine if they have a problem with their Internet connection.

The asterisk (*) on the third hop means that a packet was placed by two servers on a network wire at the same time and overwrote each other (commonly called a data collision). This is indicative of heavy traffic on that network.

If the traceroute displays three asterisks (***) during the third and succeeding hops, the following are the possible reasons:

- the remote destination host's server may be down
- the IP address does not exist
- the network is behind a firewall.

You may contact the system administrator of the remote destination host to determine the specific network problem.

A confirmation message "*Trace complete*" will be displayed indicating that there are no network connectivity problems and that the host can be reached.

Verifying the Host's Capability to Receive Mail Using the Telnet Utility

To verify if the remote host you are trying to send a message to is capable of receiving mail messages, use the Telnet utility.

Telnet allows you to access someone else's remote computer, assuming you have a permission to do so. You can also use telnet to verify or test if other services (e.g. mail services, FTP, web servers) are running on the machine.

To use the Telnet utility in determining whether the mail host *mail.domain.com* is capable of receiving mail, go the *Start* menu and click the *Run* command. Type *Telnet* and click the *OK* button. The telnet utility will be displayed. Click the *Connect* menu and select *Remote System*. On the *Host Name* field, type "mail.domain.com". On the Port field, type "25". Then, click the *Connect* button.

A confirmation message will be displayed (see **Figure 4**). Receiving this kind of message means that the mail host is capable of receiving messages. Otherwise, an error message "*Could not open a connection to mail.domain.com*" will appear, which means that the host you are connecting to is not capable of receiving messages.

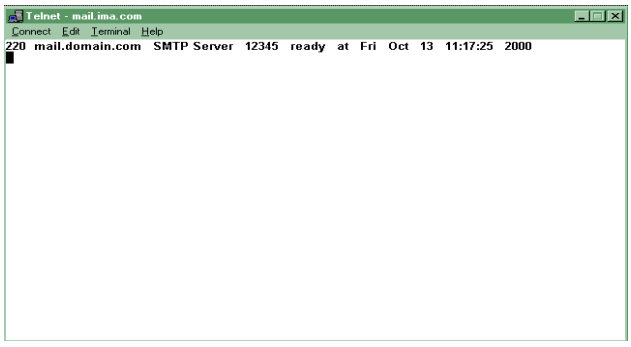

Figure 4: Running the Telnet Utility

Questions & Answers

Q: We are using Internet Exchange Messaging Server 4.1 with cc:Mail and Notes connectors installed. I successfully migrated all the cc:Mail users to the LDAP directory using the cc:Mail migration tool. However, I am having a problem migrating our Notes users to Internet Exchange. I encountered an error message which states that, "The VIM32.dll in your system path is not usable by the Notes PAB Converter. Please make sure you put the Notes install directory in the path". I am sure that I have included the Notes installation directory in the path. Currently the system path is set to "C:\Winnt; C:\Winnt\System32; C:\Lotus\Notes". The Lotus VIM 6.30 files needed by the cc:Mail connector to communicate with our cc:Mail PO is located at the "C:\Winnt\System 32" folder. How do I go about this?

A: The Internet Exchange Messaging Server's Notes migration utility makes use of the "VIM32.dll" file located in the Notes installation directory (i.e., C:\Lotus\Notes). Without this file migration will not continue. In your scenario, the Notes migration tool was able to locate the "VIM32.dll" file included with the Lotus VIM 6.30 files installed in the "C:\Winnt\System32" folder instead of the "VIM32.dll" file in the Notes installation directory. The located file is incompatible with the Notes migration tool that is why an error message was generated.

To solve this problem, temporarily rename the Lotus VIM 6.30 file "VIM 32.dll" located in the "C:\Winnt\ System32" folder to, say, "ccMailVIM32. dll". Then, proceed with the Notes migration. After Notes migration, rename the "ccMailVIM32.dll" file back to its original name "VIM32.dll".

Q: Currently, there are looping messages clogging our Internet Exchange Messaging Server 4.1, resulting in backlog of messages. It turns out that one of our disabled Message Store user accounts is trying to send a message to an invalid Internet user which resulted to a message loop. Is there any setting/s in Internet Exchange Messaging Server 4.1 that I can enable to prevent this problem?

A: Yes, you can enable the Loop Detection feature of the Internet Exchange Preprocessor module. If enabled, the Preprocessor module performs loop detection on all incoming messages based on the number of received lines (5 lines by default) of the message. Only lines containing the MTA FQDN are counted. If this number exceeds, the message will be bounced back to the sender. You can optionally set the Loop Detection feature to bounce the message to the local postmaster instead of bouncing the message back to the remote sender.

To enable the Loop Detection feature, go to the System Administrator Preprocessor web interface, select Module List and click on the Loop Detection Channel Action Matrix page. Tick the boxes of all the channels where you wish this feature to be enabled. For example, if you wish to enable the Loop Detection for messages originating from the Internet destined to your Notes environment, tick the box in between the STMPD and NOTES channels.

Continued on page 5-->

"The World Wide Web offers the clearest vision of what computer networking and communication, in general, is going to be like in the future."

-- American Scientist

This Month's Tip

Running Apache Web Server as an NT Service

Internet Exchange uses the Apache Web Server as its default web server. Apache which runs in a DOS console window, can also be run as an NT service. Running Apache as an NT service allows you to automatically start the Apache web server when your machine boots.

To install Apache as a Windows NT service, go to the DOS command prompt. From the DOS command prompt, go to the directory where the *apache.exe* file is located (e.g. C:\Program Files\IMA\Internet Exchange 4.1\Apache). Type *"`apache -i`"*

To start the Apache service, go to the *Windows NT Control Panel* and select *Services*. Click on the Apache and press the *Start* button to start the Apache service.

Note: Running Apache as an NT service is only possible if you are using the Windows NT/2000 platforms.

For more information on the Apache Web Server, you may visit *http://www.apache.org.*