Troubleshooting SMTP Routing

Chris Miller
Director of Messaging/Collab
Connectria

What We'll Cover …

- Following the breadcrumbs in the forest
- Planning to be an archeologist
- Running relay races, jumping hurdles and the javelin technique
- Looking for trouble – or -- Oh sorry, that was my error
- Shaking hands – or -- Have we met before?

Overview

- There are so many areas of SMTP that tips and techniques are easily presented. Remember that each environment is unique and some or maybe all of this might apply to your architecture
- Feel free to bring up unique points and questions about how your infrastructure operates
- Be sure to think about the flow of mail as we go through the sections and how it applies to you

What We'll Cover …

- Following the breadcrumbs in the forest – Or Inbound Messaging
- Planning to be an archeologist
- Running relay races, jumping hurdles and the javelin technique
- Looking for trouble – or -- Oh sorry, that was my error
- Shaking hands – or -- Have we met before?

Where Do I Find a Message?

- Real time monitoring does not exist
  - Unless you have time to watch a scrolling console
- The log.nsf is a time delay and does not give all the necessary information
- The mail.box shows the live messages but cannot show the path a message has taken
- MTC (message tracking) is partially the answer!

Following a Message in From the Internet

- In most environments there is at least one dedicated SMTP server (Domino or non-Domino based)
  - Now add in spam/virus servers and following the mail can be a daunting task
- Always start from the furthest point possible and work backwards
  - Start at your Internet facing server and work in
  - Verify the message flow at each step to save valuable troubleshooting time

Following a Message in From the Internet (cont.)

- As an administrator you must have a basic understanding of DNS and MX records to effectively troubleshoot
  - This actually applies for mail both inbound and outbound
  - MX records control your destiny on inbound mail, as well as redundancy and failover
    - ✓The first host that is attempted is the lowest weight
    - ✓Servers may have the same MX weight for load balancing
  - If you don’t know which host it came in you can’t start tracking the message

Mapping a Message in From the Internet

- SMTPDebug
  - Capture of inbound SMTP protocol conversations. This is for all messages received by the SMTP listener from all clients and servers via the SMTP protocol
  - You may set this variable from a value of 1-4
    - ✓1 gives minimal logging for the listener
    - ✓2 logs commands and responses and number of bytes, but not the text being transmitted
    - ✓3 logs everything in 2 plus all text (not the body) of a message
    - ✓4 is undocumented and provides the most verbose

Mapping a Message in From the Internet (cont.)

- SMTPDebugIO
  - Enables the logging of all data received by the SMTP listener task
  - You may set this variable from a value of 1-4
    - ✓1 logs the number of bytes
    - ✓But there is no 2 !!!
    - ✓3 logs all data received by the SMTP task
    - ✓RFC822 data – message data

Heads Up!

  - Caution Use SMTPDebugIO only when necessary and disable it again as soon as possible. It can cause the log file to grow very large, and logs the contents of received messages

Mapping a Message in From the Internet (cont.)

- SMTPSaveImportErrors
  - Cause the SMTP listener to save the message context exactly as it is received
  - The files are saved at STXXXXXX.tmp in the system temp directory
  - You may set this variable from a value of 1-3
    - ✓Beware if you leave this variable running and forget about it. You may accumulate a lot of .tmp files on heavily loaded servers
    - ✓1 logs messages that fail to import
    - ✓2 logs all message context
    - ✓3 logs all message context, deleting successful messages and keeping ones that fail to import

Tips Around the Debug Parameters

- The SMTPClientDebug parameter does not require the use of the NOTES.INI parameter DEBUG_OUTFILE
  - All information will be written to the Miscellaneous section of the LOG.NSF by default
    - ✓We will cover this more for outbound mail
- SMTPDebug and SMTPDebugIO do not write their outfile to the LOG.NSF
  - So *DEBUG_OUTFILE=path/filename.txt* must be in the notes.ini

Too Much Information to Sort Through?

- Many messages in today's world originate in MIME and the Domino router shows the conversion both ways (MIME to CD or back)
  - You may suppress this message with a notes.ini variable
    - ✓converter_log_level=10
  - These console messages are informational only and do not provide much troubleshooting
  - The message itself will contain the conversion information in the document properties

Now That the Message is in…

- You have choices in the way your environment was established for NRPC and SMTP routing
- Server to server
  - NRPC
  - SMTP
  - Domain documents
    - ✓Foreign
    - ✓Adjacent
    - ✓Non-adjacent
- If you can’t map server to server flow you will be hard pressed to find the message
  - Back to MTC

Bonus SMTP Notes.ini Setting

- SMTPGreeting= string
  - This gives you the ability to hide the Domino version and customize what the sender receives
  - The message must contain the “%S” string which identifies the date and time
  - The Domino default gives far too much information about the server for any SMTP conversation

What We'll Cover …

- Following the breadcrumbs in the forest
- Planning to be an archeologist – Or Outbound Messaging
- Running relay races, jumping hurdles and the javelin technique
- Looking for trouble – or -- Oh sorry, that was my error
- Shaking hands – or -- Have we met before?

Tracking the Outbound Message

- The Domino router handles outbound SMTP traffic generated from NRPC
  - The router makes direct connections via native SMTP to the remote destination
- SMTPClientDebug
  - Captures outbound SMTP protocol conversations, both Domino to Domino and Internet
  - Message content is not included
    - ✓You enable this when attempting to troubleshoot outbound communications

Tracking the Outbound Message (cont.)

- General mail logging for the Notes environment
  - What is the best setting for Log_MailRouting?
    - ✓Zero through 40 (in increments of 10) are the available options with the lower number performing less logging
    - ✓The most common setting is 10 and it gives minimal information sufficient to watch mail flow
  - MTC works for internal mail flow as well as external
    - ✓It actually provides more as you can follow a server hop to hop if MTC is enabled on each server
    - ✓Once a message hits the Internet you lose tracking ability

Tracking the Outbound Message (cont.)

- SmtpSaveOutboundToFile
  - Traps outbound MIME information
    - ✓This may be set as 0 or 1
  - Here is an example of how it would show in the miscellaneous view of log.nsf
    - ✓mm/dd/yyyy 12:53:41 PM [07A0:0006-0790] SMTPClient: RFC822 message outbound stream saved to C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\notesC839B6\st867538.TMP
  - Note where the file is stored, not easy to find!
    - ✓The directory might be hidden through the OS folder properties

Modifying the Outbound Message

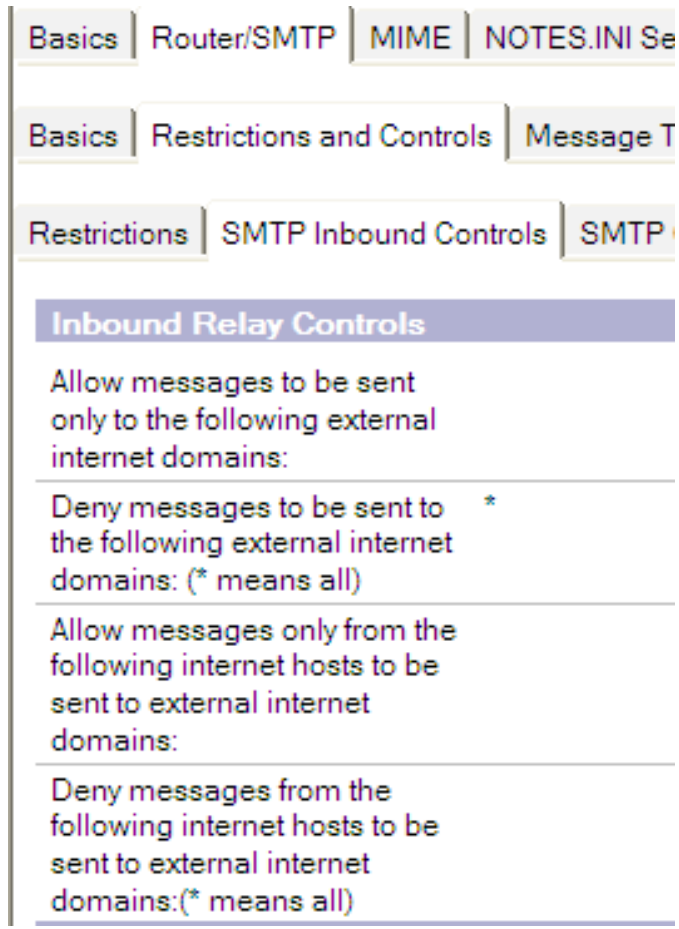
- Disclaimers
  - Outbound disclaimers are not available by default prior to Domino 7
  - Prior to Domino 7 you must modify the mail template, message or use a third party product
- Blocking Domino from identifying itself as the type of sending server
  - *SMTPNoVersionInRcvdHdr=1* will hide the Domino information from being shown in the received header

What We'll Cover …

- Following the breadcrumbs in the forest
- Planning to be an archeologist
- Running relay races, jumping hurdles and the javelin technique
- Looking for trouble – or -- Oh sorry, that was my error
- Shaking hands – or -- Have we met before?

Relay Races

- Starting in Domino 6, relays are blocked with a simple * in the appropriate fields
  - Older domain installations carried forward were open by default
  - You may allow certain internal hosts to relay which overrides the deny all
  - If you include any relay hosts, the deny is not necessary as it will allow ONLY what is in the field



Hurdles

- Balancing a proper relay and protected system is becoming more common
  - If you can use internal host names or IP addresses it is easier to manage
  - Never open your site to ranges of public IP space
  - In Domino 5 you could either have an authenticated SMTP server, or non-authenticated
    - ✓In Domino 6 and on they can co-exist!

The 100 Meter Hurdles

- Next you may want to provide encrypted traffic across the mail ports
  - This is easily accomplished in the server document under port settings
  - However, you must create a certificate for the SSL ports
    - ✓The certificate may either be self signed by Domino or from a third party
    - ✓The certificate would then be utilized for everyone connecting for encrypted traffic

The Javelin Technique

- This technique allows one (or more) servers to act as a secure SMTP reception server plus an internal server for secure relay ability only
  - This relies on proper DNS administration and domain architecture
  - While not difficult to manage, if not implemented properly you can create security holes in your mail infrastructure
    - ✓You could open an outside server to relays
    - ✓You could deny mail from outside sources
    - ✓Mail may not route properly without correct reverse DNS entries

What We'll Cover …

- Following the breadcrumbs in the forest
- Planning to be an archeologist
- Running relay races, jumping hurdles and the javelin technique
- Looking for trouble – or -- Oh sorry, that was my error
- Shaking hands – or -- Have we met before?

Outbound Connection Issues

- *Connection terminated with status: 2055* is a common outbound error in log.nsf
  - Network Router having issues resolving addresses
  - Proxy misdirecting traffic over port 25 to wrong or nonexistent servers
  - Firewall blocking outbound port 25
  - Firewall/Mail Relay Host server overloaded or otherwise unresponsive
  - Using an incorrectly configured multi-homed NIC or dual NICs

Coloring (errors) By Numbers

- Error 500
  - Syntax or bad command
  - Could be an input line was too long
- Error 501
  - Most commonly a malformed To field or From field.
  - Look for extra spaces or bizarre characters that you would not normally see in an email address
- Errors 502-504
  - Commands not recognized, implemented on the SMTP server or a bad sequence

Coloring (Errors) By Numbers

- Errors 450 and 550
  - Mailbox is unavailable
  - Usually busy, no access or non-existent
- Error 452 and 552
  - Not enough local storage
  - Exceeded storage limit (quota)
- Error 554
  - Transaction failed
    - ✓Possibly my favorite!!
    - ✓Out of disk space
    - ✓Policy reasons

What We'll Cover …

- Following the breadcrumbs in the forest
- Planning to be an archeologist
- Running relay races, jumping hurdles and the javelin technique
- Looking for trouble – or -- Oh sorry, that was my error
- Shaking hands – or -- Have we met before?

Basic SMTP Authentication

- SMTP authentication in Domino currently relies on a username/password
  - Encrypted traffic over SSL and lookups are not authenticated
  - Domino would rely on the user or server to send a username/password combination in order to send SMTP mail through the server
- There is a new notes.ini variable in 6.0.3 and 6.5 to enforce the senders Internet Address
  - SMTPVerifyAuthenticatedServer
    - ✓Variables are from 0-2, with 0 not requiring the sender to use their Internet Address

Options to Block Relays and Attempts

- Verify sender's domain in DNS
  - While great at verifying that sending domains exist in DNS, the possibility to pause incoming mail exists
    - ✓*SMTPVerifySendersDomainTimeout=* was added as a notes.ini variable
    - ✓The default value was also reduced from 120 seconds to 30 seconds in 6.0.3 and 6.5

More on Verify with DNS

- Verify sender's domain in DNS
  - This only verifies that the Internet Address for the sender exists in DNS
  - On spam/spoofed email they often use verifiable domains
- Verify connecting hostname in DNS
  - This only verifies that the hostname connecting to send the message exists in DNS
- Neither of these authenticate the sender, block spam entirely or confirm a valid email

Verify Sender or Hostname in DNS

- Both of these options also present unique issues
  - If DNS is not responding, this will slow all inbound Internet mail
  - If there is a new hostname connecting that has not propagated through DNS the message can be refused
  - If the sender is a spammer using a known domain or host, the message may be accepted

Advanced SMTP Authentication

- Error 505 – authentication required
  - This is a basic error letting the attempting sender know that you must provide some username/password combination in order to us the SMTP task

Security Checklist

- By default, Domino 6 started securing basic relays
  - If you have older systems that have been around then you need to reverify relay fields
- Ranges of IP addresses used for open relay and trusted sources should be limited to the last octet
  - For example [192.168.1.X]
- Authenticated users and servers shold communicate over TLS or encryption
  - The overhead is minor on the server performance
- Anti-relay enforcement should be enabled for all connecting hosts if possible

Relay Tests That Show an Open Host

FIGURE 1

Sample SMTP server conversation

You type:	And the system responds:
Telnet mail.xyz.com 25	220 mail.xyz.com Lotus Domino R5 SMTP Service Ready
HELO testing.com	250 mail.xyz.com Hello testing.com ([192.168.100.1]) pleased to meet you
MAIL FROM:<test_user@testing.com>	250 test_user@testing.com ..... Sender OK
RCPT TO:<actual_user@mail.xyz.com.com>	250 actual_user@mail.xyz.com .... Recipient OK
DATA	354 Enter Mail, end by a line with only '.'
[Press ENTER] Hello World . (This is a period)	250 Message accepted for delivery.
QUIT	221 Goodbye

Relay Tests Denied!

FIGURE 2

Sample SMTP relay conversation

You type:	And the system responds:
Telnet mail.xyz.com 25	220 mail.xyz.com Lotus Domino R5 SMTP Service Ready
HELO testing.com	250 mail.xyz.com Hello testing.com ([192.168.100.1]) pleased to meet you
MAIL FROM:<test_user@testing.com>	250 test_user@testing.com ..... Sender OK
RCPT TO:<relay_test@fakecompany.com>	554 Relay rejected for policy reasons.

Resources

- RFC 821 error codes
  - http://www.ietf.org
- RFC 1893 error codes (delivery failure)
  - http://www.ietf.org
- Lotus Knowledgebase
  - Technote #1153776 has the SMTP reply codes
- Lotus Knowledgebase
  - Technote #1157257 has a step by step plan for troubleshooting mail routing
- My previous E-Pro article has step-by-step info
  - http://www.e-promag.com/eparchive//index.cfm?fuseaction=viewarticle&ContentID=1999&publicationid=19&PageView=Search&channel=2

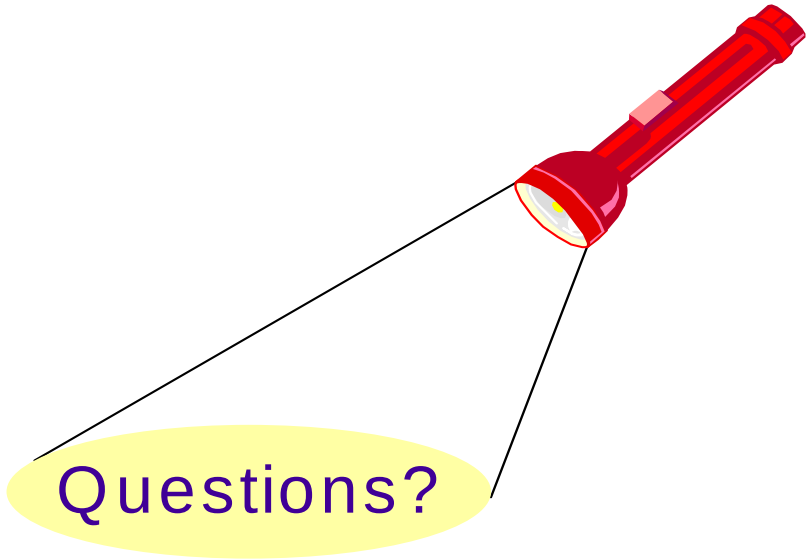
7 Key Points to Take Home

- Understanding DNS and MX records is a basic knowledge required for any mail administrator
- Diagramming your infrastructure will help you go step by step through the mail flow path
  - Unknown relay or spam servers can cause your troubleshooting time to grow
- Become aware of the optional debugging and logging options to help troubleshoot
  - Do not leave these options enabled long term!
- Secure the relays on the servers immediately

7 Key Points to Take Home

- Utilize the ability to force relayed mail to be through authentication only
- Create a reference site or database containing the SMTP error codes to ease troubleshooting
- Create and configure SSL for the appropriate ports to secure mail transactions

Your Turn!



How to contact me:
Chris Miller
IdoNotes@netscape.net
AOL IM: IdoNotes
Blogging at
http://www.IdoNotes.com