
Lotusphere®
2007

BP402 Demystifying IBM Lotus Domino and SMTP Messaging

Daniel Nashed, CTO - Nash!Com Germany

About the Speaker

- Daniel Nashed
  - Nash!Com - IBM/Lotus Advanced Business Partner/ISV
  - Member of The Penumbra group
    - an international consortium of selected Business Partners pooling their talent and resources
  - focused on Cross-Platform C-API, Domino® Infrastructure, Administration, Integration and Troubleshooting
  - Platform Focus: W32, xLinux, zLinux, AIX® and Solaris®
  - nsh@nashcom.de
  - http://www.nashcom.de

Lotus software

Nash!Com Communication Systems

Lotusphere 2007

Agenda

- How does Messaging work?
- Notes Client & Messaging
- Domino Server Configuration
- Messaging Infrastructure Scenarios
- Best Practices
- Q&A

Disclaimer:

- The session has way too much slides but I think all is important to know
- I might skip some details on slides or special debug parameter slides and keep them in the presentation for reference

How does Mail-Routing work?

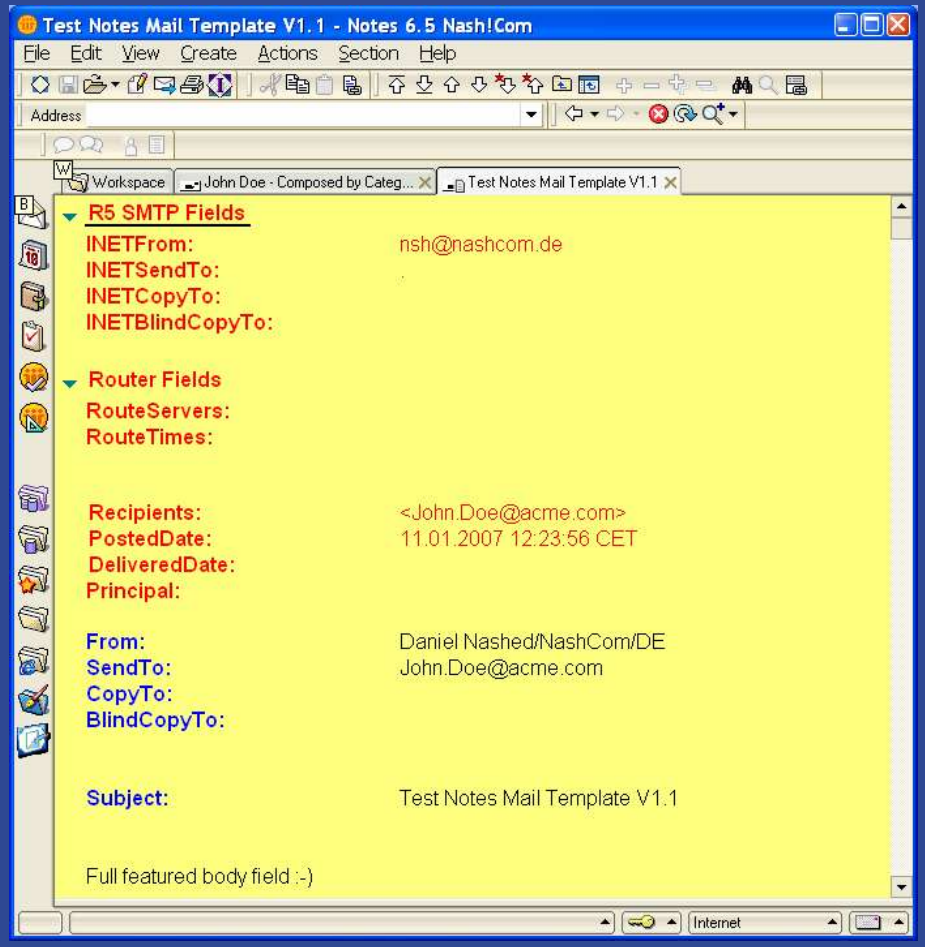
- Notes Client Mail-Routing is based on
  - Notes Mailer component
  - mail.box (local or server)
  - Local names and Domino Directory
    - Also LDAP directories
- Notes Server Mail-Routing is based on
  - Mail-Router
  - SMTP Task
  - mail.box
  - Domino Directory (routing table ...)
    - Also Directory Assistance(DA), Directory Catalog, LDAP Directories configured in DA

Notes Mailer Component

- Notes Mailer is part of the Notes Client and responsible for
  - Addressbook-Lookup / Name-Resolution, Type-ahead, Group-Expansion, ...
  - Calculation of the Recipients field (even with server groups)
    - Other fields are only for display. Group Expansion is determined by
    - $ExpandGroups: 0=no groups, 1=local groups, 2=public groups, 3=all groups
  - Formats the message for Notes Recipients (CD-Records) and separately for Internet Recipients (MIME Messages)
    - Separate Mails are send to Internet and Notes Recipients
  - Sets the "PostedDate"
  - Encryption and Signing based on message settings and recipient information. Supports Notes Encryption via Public Key and S/MIME via X.509 Public Cert in Person doc
  - Stores Mail in mail.box (either Local or on Server)

Demo Notes Mailer

- Notes 1.1 Mail Database in Notes 7.0.2 Client with some extra computed for display fields



Lotus software

Lotusphere 2007

Mail-Router

- Servertask for Transferring (Routing) and Delivering Mail
- Mail-Router picks up each message from mail.box, analyzes the routing path (aka dispatching) and either
  - a.) Forwards the message to another server (via Notes or SMTP) to another mail.box
    - Store and forward principle – "recipients" field is updated accordingly
    - Delivery and Transfer Queues are used
      - Check via "tell router status"
  - b.) Locally Delivers the message to an user, mail-in DB
    - Copies the note to local mail-file
    - Sets "DeliveredDate" and adds it to the "Inbox" folder
    - Add some other details like populates BCC field, ...
    - Removes Recipient field
  - c.) Or stores mail in foreign Domain databases or sends it to servers outside the own domain
  - When all recipients have been processed mail is purged from mail.box

Mail-Routing Details

- Notes Mail-Routing works via store and forward from server to server
- Each server re-calculates the routing path again
  - Inside a Domain all servers should have the same information
  - Server to Server connection work via Notes Named Networks (NNN) or Connection Documents
- Internally a routing table is used based on connections and Domains, NNN, Relay Host information in the Domino Directory
  - Basically this comes from Graph Theory: It's a Weighted, Directed Graph
    - Connections have direction and costs
- Each Person Document contains information about
  - Home-Mail-Server, Mail-File-Name, Message Format (MIME, Richtext, ...)
    - Message Format Preferences (should be set to "Keep in Senders Format")
  - Public Key and X.509 Public Cert for Encryption (mostly used by the Client)

Notes Domain

- All Servers and Users inside a Domain should use the same Domino Directory with the same information about
  - Persons, Groups, Servers, Connections and Domains
- You only need the user name to address a mail inside a Domain
  - Notes Mailer does a lookup to check if the user exists
- Each User has a person document specifying
  - Home-Mail-Server, Mail-file Location
  - Certificates
  - Message Preference
- ($Users) view is used internally to find users
- Server to Server routing needs connections documents
  - Servers in the same Notes Named Network (NNN) route messages at once
- Addressing outside the own Domain uses connection documents

Mail-Routing Destination Queues

- Mail-Router builds queues for transferring and delivering messages
  - Per destination server (Notes or SMTP) there is a transfer queue if messages are pending
  - Router checks mail.box and build message lists
    - And after processing messages updates "recipients" field and finally purges message from mail.box
  - Therefore you cannot modify any message once it has been saved in the mail.box!
  - Anti-Virus Vendors use Extension-Managers to "hook" into the message update before the router sees the message and sets it to "HOLD/DEAD"
  - "tell router status" shows the current queue status

```
tell router status
 Msgs State     Via   Destination
    1 Done      SMTP  GMAIL.COM (Push)
Transfer Threads: Max = 5; Total = 5; Inactive = 0; Max Concurrent = 2
Delivery Threads: Max = 5; Total = 2; Inactive = 0
```

What is SMTP-Mail?

- SMTP-Mail is mostly ASCII Text
- Compontents
  - Envelope (RFC 821)
  - Header (RFC 822)
  - Body (Plain-Text or MIME Text)
- SMTP = SIMPLE MAIL TRANSFER PROTOCOL (August 1982)

SMTP Message Envelope

- RFC 821 SIMPLE MAIL TRANSFER PROTOCOL
  - Describes Information needed for mail delivery
    - mainly Sender, Recipient
- Basic Commands:
  - Helo, ehlo 'Host' to initiate a SMTP session
  - Mail from: <user@domain.com> specifies sender
  - Rcpt to: <user@domain.com> specifies recipients (stored in "recipients" field)
  - Data starts RFC822 data part of the message
  - Quit closes transmission channel
- Used by the Message Transfer Agent (MTA) for Mail delivery
  - This is not part of the e-mail itself
    - This means you cannot see the "rcpt to" in the delivered message.
    - the "from" in RFC822 header (see next slides) might be totally different
    - Tip: use notes.ini SMTPMaxForRecipients=n to specify the number of "Rcpt to" entries that you want to see in the "Received" header
      - Be aware that you will also see BCC recipients

Example Envelope Data (RFC821)

- notes.ini SmtpDebugIO=3
  - Written to console log or debug_outfile

```
S:  220 NashCom ESMTP Service ready at Thu, 4 Jan 2007 12:59:08 +0100<CRLF>
R:  EHLO ug-out-1314.google.com
S:  250-notes.nashcom.de Hello tom.google.com ([66.249.92.168]), pleased to meet you<CRLF>
S:  250-SIZE<CRLF>
S:  250 8BITMIME<CRLF>
R:  MAIL FROM:<daniel.nashed@gmail.com>
S:  250 daniel.nashed@gmail.com... Sender OK<CRLF>
R:  RCPT TO:<nsh@nashcom.de>
S:  250 nsh@nashcom.de... Recipient OK<CRLF>
R:  DATA
... this part is not logged but you will see details of RFC822 header&body on next slides ...
S:  250 Message accepted for delivery<CRLF>
```

SMTP Mail Header

- RFC 822 STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES
  - Describes header information of a mail
  - Sender, SendTo, CopyTo, BlindCopyTo, …
  - Subject
- Not used for Mail Delivery
  - But is part of the message data and rendered into Notes items
  - Part of the message that starts after the "data" command
- There are required fields, optional fields and specific extensions (X-… fields)

Body of a SMTP Message / MIME

- Body of a SMTP message contains the actual information
  - Very Similar Concept to Notes Mail Body
- The format can be simple text but is most likely a "MIME" encoding
  - MIME = Multipurpose Internet Mail Extensions
- MIME can have multiple formats with different kind of encoding
  - Content-Type: e.g. text/plain, text/html, text/calendar, …
  - Attachments can be inline or referenced, …
  - Encodings: e.g. BASE64, Quoted Printable
- There are a many relevant RFCs for MIME
  - Most important RFC1521
    MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies
  - RFC 1522 describes encoding of headers (e. g. Subject)
  - MIME supports multiple character sets and Unicode

Example Mail Header (RFC822)

- SMTPSaveImportErrors=2
  - Creates a Temp file (name is logged)

```
Message-ID: <2fbf67...2cf@mail.gmail.com>
Date: Thu, 4 Jan 2007 12:14:08 +0100
From: "Daniel Nashed" <daniel.nashed@gmail.com>
To: nsh@nashcom.de
Subject: Ping
Message-ID: <2fbf67870701040314157b360caude5aa58fdb3642cf@mail.gmail.com>
Date: Thu, 4 Jan 2007 12:14:08 +0100
From: "Daniel Nashed" <daniel.nashed@gmail.com>
To: nsh@nashcom.de
Subject: Ping
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="----=_Part_3922_19055467.1167909248240"
------=_Part_3922_19055467.1167909248240
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: 7bit
Content-Disposition: inline
Test Body
------=_Part_3922_19055467.1167909248240
Content-Type: text/html; charset=ISO-8859-1
Content-Transfer-Encoding: 7bit
Content-Disposition: inline
Test Body<br>
------=_Part_3922_19055467.1167909248240--
```

Domino Itemizer

- Notes MIME Messages are stored in Notes Items – similar to Notes Mail
  - When the mail is send to or received from another SMTP Server the message needs to be "converted" from a "item based" message into a flat text stream and vise versa
  - Inbound conversion done by the "Itemizer" which knows which item to handle in which way
    - There are standard items like "from", "SendTo", "PostedData" and additional fields
    - By default only those fields are converted for outgoing messages
  - You can define field lists for excluding/including in the config document
    - !Caution: Those lists are limited to 255 bytes!!!, Conversion works (and looks) different than for standard fields
  - Tip: If you want all items in outgoing messages set the field $SMTPKeepNotesItems=1 in the mail-document
    - This converts items to full "X-" Tag items that can be converted back on other side
    - Also used by Notes for Calendar Documents
    - But Calendar Messages also use "Content-Type: text/calendar" and VCALENDAR for outgoing messages

No more Winmail.dat in Domino 7.0.2

- Microsoft has it's own “standard” for richtext fields
- TNEF support has been build into Domino 7.0.2
  - But it is disabled by default
- Enabled by notes.ini: TNEFEnableConversion=1 (default = 0)

- Additional Settings
  - notes.ini: TNEFKeepAttachment=1 (default = 0)
    - Keeps original attachment
  - notes.ini: TNEFAttachRTF=1 (default = 0)
    - Attach RTF as attachment named "message_body.rtf"

  - Brand new code you might want to consider to enable SmtpSaveImportErrors=3 ;-)
    - See next slides

TNEF Troubleshooting notes.ini Settings

- TNEFDebug=1 (default = 0)
  - Enable Debugging / Trace Messages
- TNEFConverter_Log_Level=n (default = 20)
  - 10: minimal -- errors only
  - 20: normal -- errors and terse info
  - 30: informational -- errors, terse info, and some additional info
  - 40: verbose -- provides all information
- TNEFBreakSMIME=1 (default = 0)
  - 0: do not process TNEF objects in S/MIME signed messages
  - 1: process TNEF objects in S/MIME mail, invalidating signature if necessary

Debugging Incoming SMTP Messages

- Generates temp file with full message content before itemization
  - Message as received by SMTP channel --> Useful for troubleshooting
  - Temp file name is writen to log.nsf
- SmtpSaveImportErrors=1
  - Save if error occurs during message itemization
- SmtpSaveImportErrors=2
  - Always save
- SmtpSaveImportErrors=3
  - Only save temporary before message conversion and delete after successful conversion. Useful for rare occurring server crashes
  - Extra Tip!
    - SMTPSaveFileFrom=string in combination with SmtpSaveImportErrors=3 keeps log files after conversion if string partially matches with RFC822 "from"
    - Undocumented but very useful to trace issues with certain users or domains in production!

More SMTP Debugging (notes.ini)

- SmtpSaveOutboundToFile=1
  - Similar to inbound logging all messages are saved to temporary files
- SMTPClientDebug=1
  - Logs RFC821 conversation for outgoing messages
  - Does write to log misc events instead of debug_outfile!
- SMTPDebugIO=1
  - Logs transferred bytes
- SMTPDebugIO=2
  - Not implemented
- SMTPDebugIO=3
  - Logs all RFC822 headers
- SMTPDebugIO=4
  - Use this very carefully! Logs also RFC822 data / body!!!

More Debug Parameters (notes.ini)

- SMTPDebug
  - 1 – Basic logging like Errors and some IOCP information
  - 2 – Logs Information about SMTP protocol state, processing and state change
  - 3 – looks the same as 2 (traced in D7.0.2)
- DebugRouter
  - 1 - shows whether messages are ready to be routed and add/delete of recipient from routing queues, etc.
  - 2 – routing path information, least cost path calculation, routing table, ...
  - 3 – combination of both because the two other settings are bit flags

Log Mail-Routing – Config Document!

- Log_MailRouting has been replaced by config document setting!
  - 10 (MINIMAL)
    - Mandatory status messages and fatal error messages for example, startup and shutdown, mail database compaction, etc.
    - Successful deliveries and transfers are not recorded
  - 20 (NORMAL)
    - Also logs all warning messages indicating conditions that do not cause processing to stop
  - 30 (INFORMATIONAL)
    - Also logs: Intermediate storage, MAIL.BOX access, Message handling (including thread information), Message conversion, Transport status
  - 40 (VERBOSE) – Only for Debugging!!!
    - Successful transfers and deliveries
    - Message queues and full document information for Mail.Box
    - The full hierarchical names of senders and recipients
    - The UNID of each message and creation, usage, idling, and shutdown of routing threads

Notes vs. Internet Mail

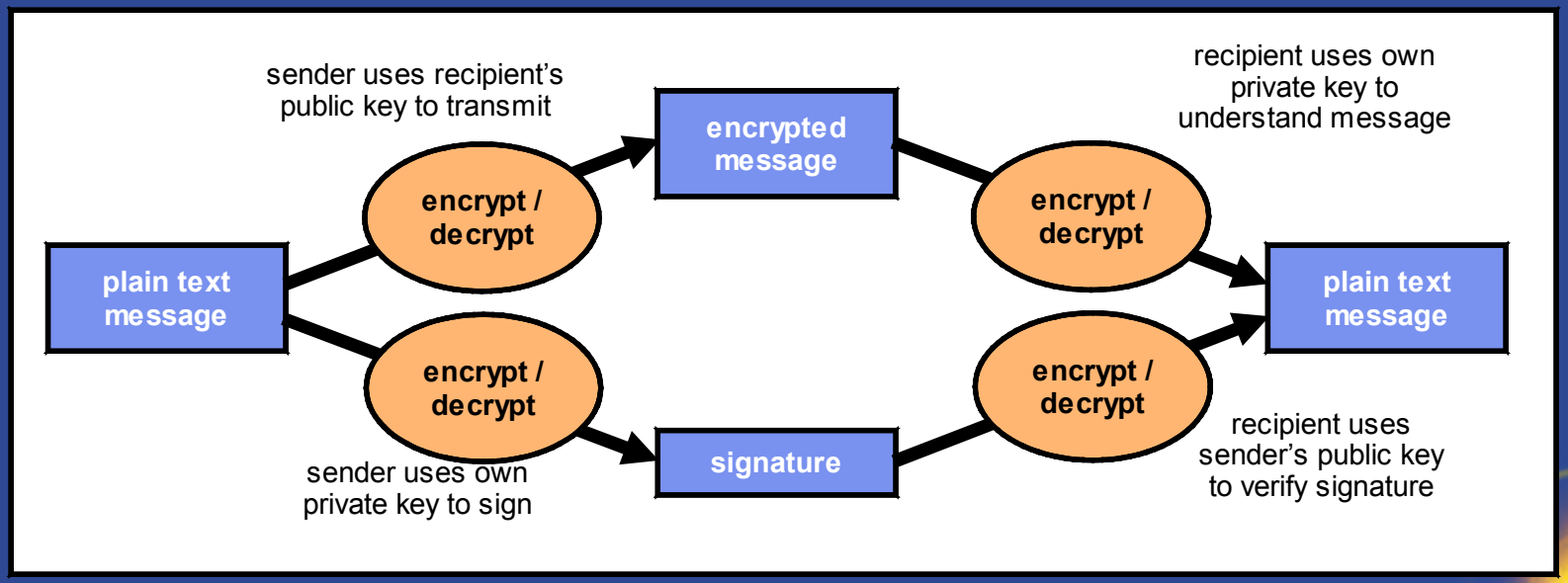
- Notes Mail uses CD-Record formated Body items
  Internet Mail uses MIME Body formated items
  - Totally different format
- Notes Items use Standard Text fields
  Internet Mail uses RFC822Text fields
  - Quite similar but different formating
- Header fields are mapped
  - e. g. RFC822 Subject, To, ... are mapped to the corresponding Notes items
- INETForm field sets the "from" for Internet messages
  - Specified in location document and added to each outgoing message
- Address Format is different:
  - Notes: Daniel Nashed/NashCom/DE@NashCom
  - Internet: "Daniel Nashed" <nsh@nashcom.de>

Interoperability MIME / Notes Mail

- Domino 5 first introduced MIME messages
  - Older code (clients and servers) do not understand MIME
- Opening a note without preserve MIME Flags converts items to Richtext (CD-Records) and standard text items – you will loose fidelity
  - C-API: Open Flags: OPEN_RAW_RFC822_TEXT | OPEN_RAW_MIME_PART
  - Script: Session.ConvertMIME = False before opening documents
  - For person documents set "Keep in senders format"
- If e.g. agents or the mail-router convert a message it will be logged
  - e.g. "Begin MIME to CD Conversion (Process: ..., Database: m.nsf, Note: xyz)"
  - You can turn this off via notes.ini "converter_log_level=10" but you should better understand why this happens first (e.g. notes.ini debug_threadid=1 and tracing)
  - You should avoid any kind of conversion for performance and message fidelity

Public-Private Key Technology

- To securely send information to a known entity
  - Encrypt with user's public key, user decrypts with its private key
- To sign information and to authenticate
  - Encode a hash based on the signed content with your private key, other party verifies with your public key
- The same algorithm both encrypts and decrypts



Mail Encryption

- Symmetric Session Key is generated
  - Message is encrypted with this key
  - Symmetric key is encrypted with public key of recipient(s) and the sender
- Encryption works quite similar for Notes Encryption and S/MIME
- Notes Mail encrypts all items with the Seal Flag set into "$SealData" Items
  - Usually Body and File-Attachments
  - Stores symmetric encryption key into "$Seal" item and encrypts it with recipients public key
  - Decryption does restore "$SealData" into normal fields when document is opened in client
  - $Signature contains signature
- S/MIME Encrypts message body into MIME Blob "smime.p7m" attachment
  - Decryption does convert MIME Blob into MIME items
  - "smime.p7s" contains the signature – also for encrypted messages – included in MIME Blob
- You need Notes and Internet Cross Certificates (for S/MIME) to verify signatures and encrypting messages!

S/MIME Support in Domino

- S/MIME needs a X.509 Cert added to the Notes.ID
  - Either self singed via Notes Certificate and Domino CA issued via admin client
  - Or have a 3rd party cert imported manually into the Notes.ID
    - C-API call "PKCS12_ImportFileToIDFile" that can help do this on client side
  - Cert is stored in the Notes.ID and can be used to sign and encrypt
- Public Cert is stored in Person Document
  - Either local directory or server based
  - Local LDAP Directories are not supported but server based (via Directory Assistance) work fine
- If Encrypt Option is enabled Internet Messages are automatically encrypted with S/MIME when Internet recipient is addressed
  - Take care if Notes Certificate is present in person doc and preference is not "MIME" mail is encrypted with Notes Public key instead!
- Messages are automatically split into a Notes and Mime Message and encrypted and signed accordingly

MIME Programmability Support

- Since Domino 6 new Lotus Script Classes for MIME Header & Body
  - NotesMIMEHeader, NotesMIMEEntity
    - See session slides ” BP309 A MIME is a Terrible Thing to Waste—Automating MIME-Encoded Email” for details
- Since Domino 6.x C-API SMTP Extension-Manager support
  - You can hook into the SMTP Dialog on Server side!
- Since Domino 7.0.2 C-API Calls
  - Most functions are wrappers calling the native routines in core Domino
    - MIMEConvert..., MIMEEntity..., Conversion Options, ... MIMEStream...,
    - MIMEHeaderNameToItemName, MIMEItemNameToHeaderName
    - Looking into those calls gives you a deeper understanding how the server/ client creates/converts messages (Itemizer, etc)

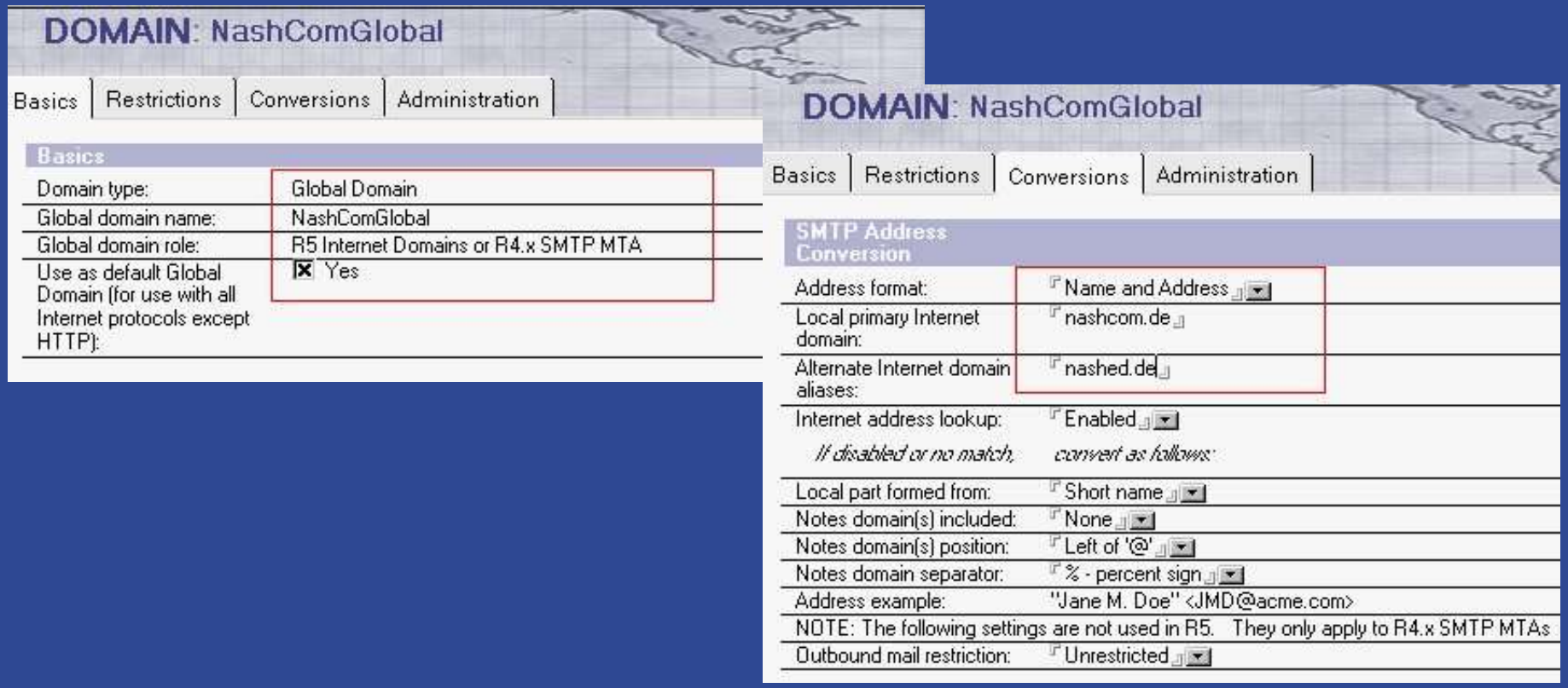
SMTP Mail Configuration

- Server-Document
  - SMTP Listener, Ports, ...
- "Global Domain" Document
  - Domains, Domain Aliases and Conversions
- Configuration Document
  - Enabling SMTP for a Server, Inbound/Outbound Restrictions (Relay), Relay-Hosts, Smart-Host, MIME Settings
- SMTP Connection Documents and Foreign SMTP Domain
  - Used to specify gateway servers
- Notes.ini
  - Special settings and Debugging

Global Domain Document (GDD)

- Defines local Domains and Aliases
  - Mail to all other Domains from external are treated as a Relay attempt!
  - You should have a GDD for each separate set of Domains with the corresponding Domain Aliases
- All SMTP Servers use all GDDs
  - You should have a default global Domain
  - "Use as default Global Domain (for use with all Internet protocols except HTTP)"
- For different sets of Domains use different GDDs
  - (e.g. acme.com, acme.de are aliases, nashcom.de is a complete different Domain)
- Defines Address Conversion for all mail where INETFrom is not filled
  - Usually INETFrom is filled by client
  - You can remove the INETFrom via "Notes items to be removed from headers:" MIME / Advanced / Advanced Outbound Message Options
  - Specify Enable "Lookup Internet address for all Notes addresses when Internet address is not defined in document" in Config Doc: MIME / Conversion Options / Outbound

Example Global Domain Document (GDD)

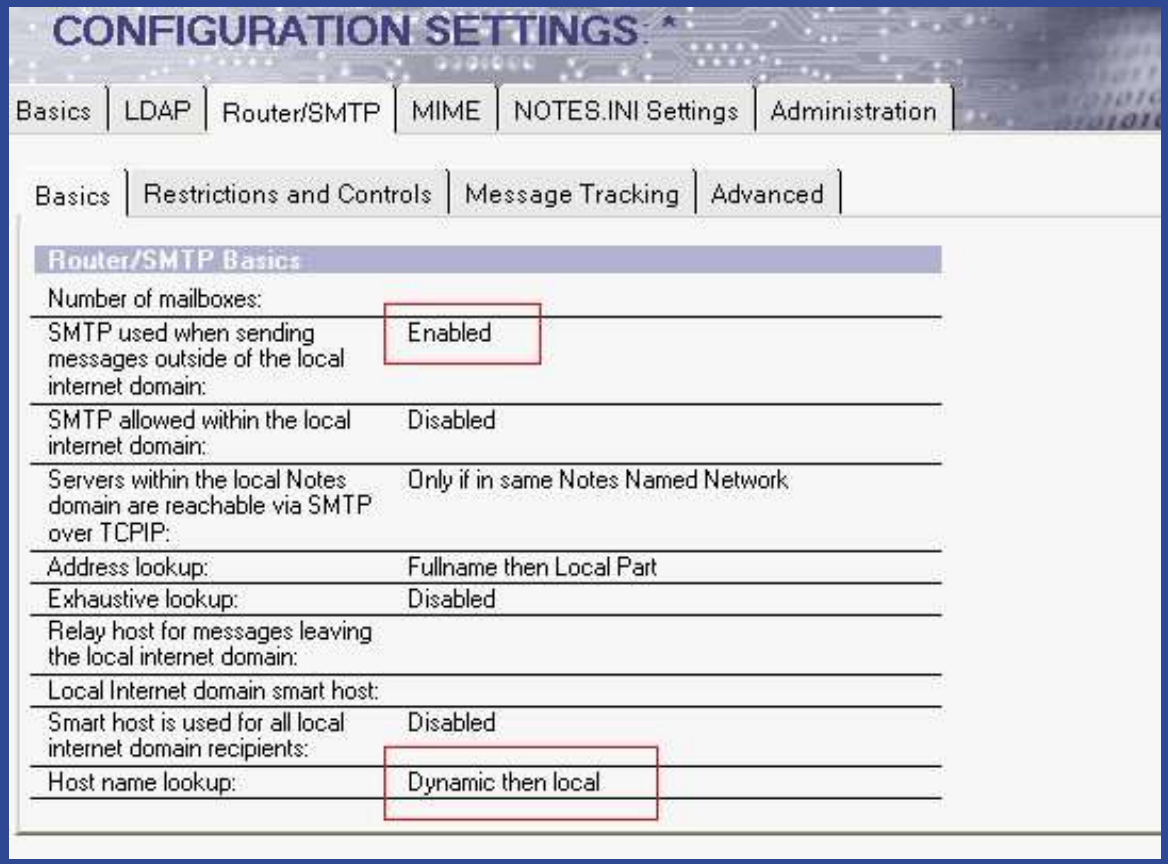


Configuration Document

- Router/SMTP – Basic
  - SMTP used when sending messages outside of the local internet domain: Enabled
  - Address lookup: "Fullname then Local Part" -> "Fullname only"
  - Relay host for messages leaving the local internet domain:
    - Depends on your messaging topology
  - Local Internet domain smart host:
    - If some users use a different mail system

- Router/SMTP – Restrictions and Controls – SMTP Inbound Controls
  - Deny messages to be sent to the following external internet domains: *
  - Deny messages from the following internet hosts to be sent to external internet domains: *
    - Ensures server does not relay
  - **Verify that local domain recipients exist in the Domino Directory:** Enabled
    - Ensures that messages are rejected if the recipient is not found in Domino Directory
    - Take care about bounces if Domino is not the first server in your messaging loop

Example: Configuration Document



MIME Settings in Config Doc

- There are many MIME settings in the configuration document
  - You should keep international MIME settings default!
    - They work for most cases and are only needed if no charset information is present in the mail
  - You can specify many different conversion options mostly needed when mail is converted from Notes to MIME on server or other special cases
- Some recommendations:
  - MIME/Conversion Options / Basic
  - Return receipt mapping: Use Return-Receipt-To
    - Better understood by user than DSN (Delivery Status Notification)
  - MIME/Conversion Options / Inbound
    - Use character set auto-detection if message has no character set information: Yes
    - Only option that really makes sense for International MIME
  - MIME/Conversion Options / Inbound
    - Lookup Internet address for all Notes addresses when Internet address is not defined in document: Enabled --> for emails without "INETFrom"

Inbound Internet Recipients Resolving

- Scenario:
  - Inbound mail to john@acme.com
  - Person-Doc: ineternet address: john@acme.com
  - Config-Doc: Internet Domain: acme.com, Alias: acme.de
  - Config-Doc: Address lookup - "Fullname only"
- What the server does in detail:
  - 1. Direct lookup in ($Users) if name including INET Domain is found
  - 2. Checks if Domain "acme.de" is alias of any Primary Domain and do a lookup with the "local part" and the replaced corresponding Global Domain (john@acme.com)
- Some side-notes
  - The lookup is always done with the primary Domain specified in the GDD
  - The result needs to be unique
  - If you specify "Fullname then Local Part" the server will also truncate the INET Domain and try to search for the local part only
  - In this case the result might be the same if only one "john" is listed in in Domino Directory – But this might not be what you want in general!

Recommendations for the Person Document

- Alias email addresses should be configured in the "fullname" field
  - First entry of "fullname" field always has to be the Notes canonical user name!!!
    - An user is always authenticated with this name.
- Have the primary Internet address with the primary Domain specified in the "Internet address:" field
  - This field is also synced by the Dynamic Client Config into the Location Document
    - Notes Client uses this field to populate the "INETFrom"
    - And used for lookup if the "INETFrom" is not present
- Set "Format preference for incoming mail:" Keep in senders' format
  - Ensures messages stay in the original format and no conversion is done

What is a (Open) Relay?

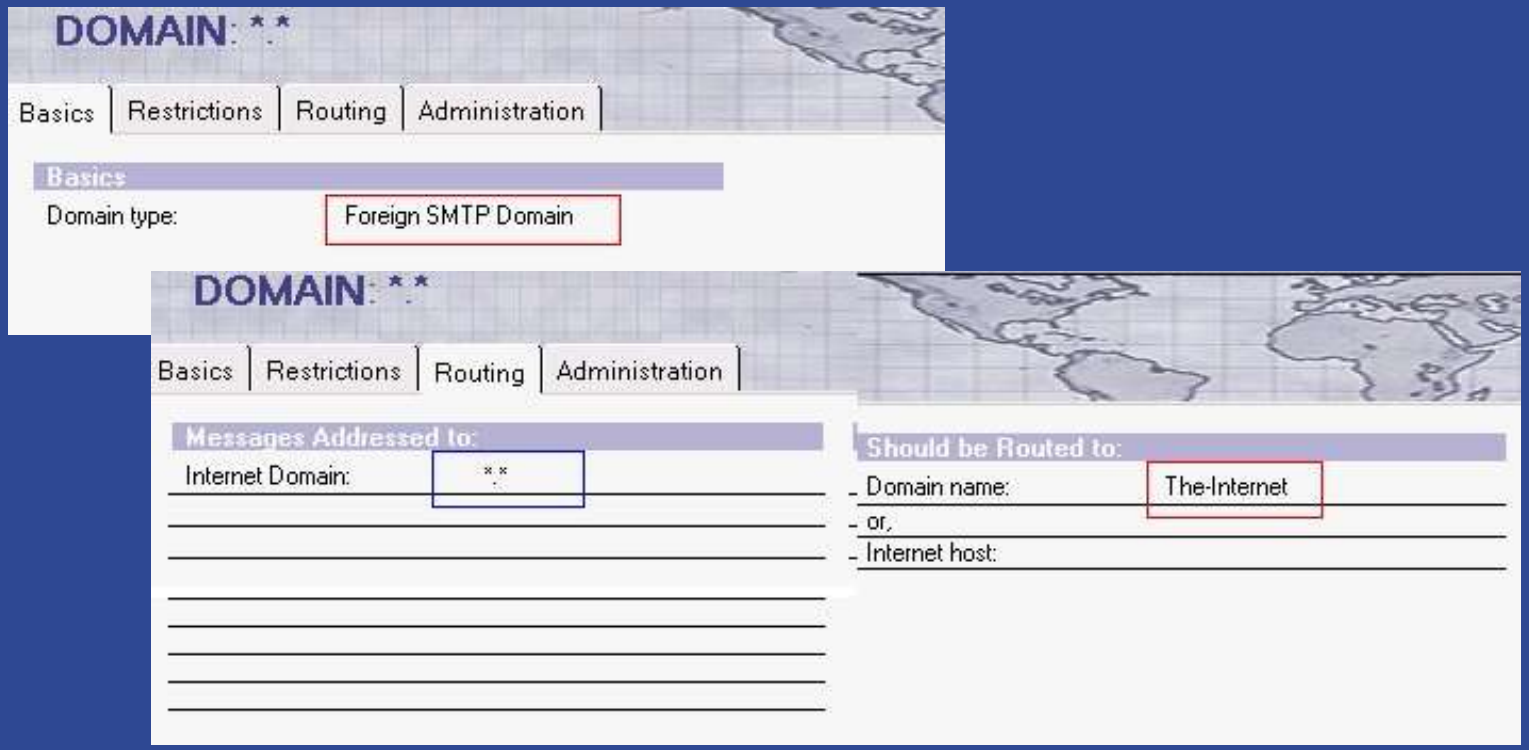
- Mail send from an External Server to your server intended for another "external" server
  - Recipients not matching your Domain and Domain Aliases in your GDDs
- Relay could be intended, providing a Relay for your own users
  - You could allow local addresses or authenticated users to relay thru your server
    - Specified in Configuration Document (SMTP Inbound Controls)
    - Take care to always specify IP Addresses in brackets e.g. [192.168.96.*]
- But most likely relaying is used by SPAMMERS!
  - And you have to take care that your relay is not open for everyone
  - Else you might be listed as a SPAMMER very soon!
  - Listed on a Open-Relay List or even worse listed as a SPAMMER

Planning a SMTP Topology

- Should all servers directly send and receive Internet Mail?
  - Probably not
  - Usually you have gateway hosts sending and receiving Internet Mail
    - Those servers have the SMTP Listener (Server Doc) and "SMTP used when sending messages outside of the local internet domain: Enabled" (Config Doc)
  - Inbound Mail is automatically forwarded to the right server
    - Person Document lists home mail server
  - For Outbound Mail you need to configure a Foreign SMTP Domain and a SMTP Connection Document
    - This document points from the gateway server(s) to the Virtual Internet Domain
    - You can have multiple connection documents for fail-over configurations

Foreign SMTP Domain

- Defines a connection for Internet Addresses
  - Usually *.* but you can have multiple connections pointing to different target Domains or Relay Hosts
- All recipients matching this schema will be send thru this connection

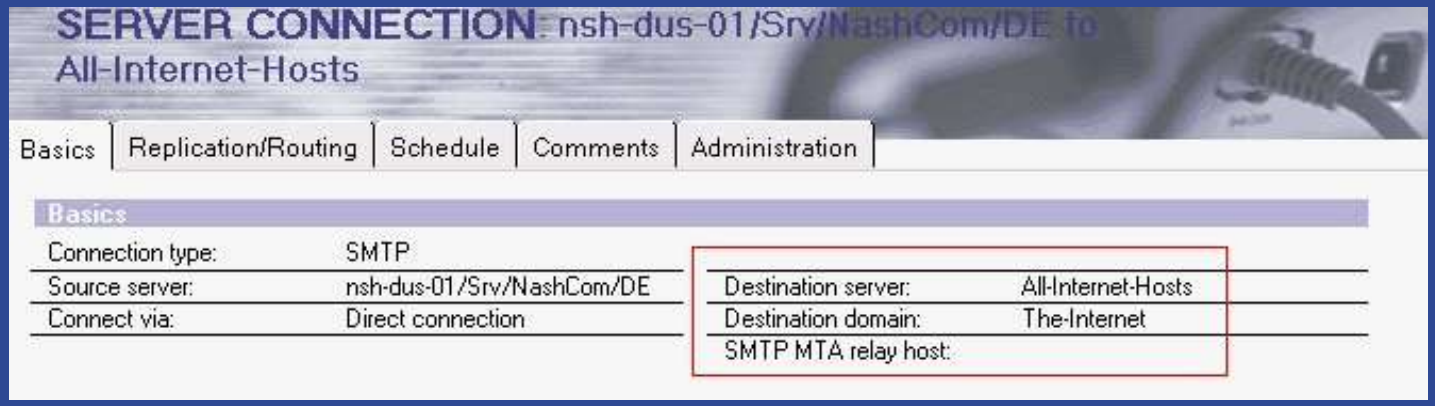


Lotus software

Lotusphere 2007

Foreigen SMTP Connection Document

- Used to define the Server or Servers sending SMTP messages
  - The connection is from the server to the Virtual Internet Domain Name
  - You can have multiple Servers pointing to the same virtual Domain for fail-over
  - The connection type has to be "SMTP"



Relay-Host Scenarios

- Depending on your configuration Domino Servers might not directly sending and receiving messages from/to the Internet.
  - Specialized/Hardened SMTP Server (Sendmail, Postfix Iron Port, etc...) in the DMZ. External provider filtering mail (Virus-Scanning, SPAM)

- Domino Server can use a Relay-Host
  - For outgoing messages – relay all mail to a non-Domino server over SMTP
  - For incoming messages – receive all messages from a non-Domino server over SMTP
  - Relay-Hosts can be specified in the Configuration Doc or in a SMTP Connection Doc
    - You can specify either an IP address or better a DNS name pointing to multiple MX Records
    - For high availability you can use a load-balancer
    - Or a virtual host with multiple MX records (see details on next slides)

What are MX Records and how are they used?

- MX = Mail Exchange Records are used to specify which host is responsible for accepting inbound SMTP messages for an INET-Domain
  - Depending on your scenario MX records either point to
    - a.) Domino
    - b.) Another host in your firewall
    - c.) Or an external provider
  - You can have multiple MX Records with different or same "preferences"
    - Same preferences are used for "load-balancing",
      different preferences are used for "fail-over" (lowest preference is used first).
  - You should have at least 2 MX Records for your Domain pointing to servers in different networks/data centers – Don't use a backup MX record at your ISPs location!!!
- First server accepting the mail should do Anti-Relay & Recipient checking!!
  - You have the full information including the connecting host
  - Depending on the legal requirements you might be able reject potential SPAM messages before it has been accepted by any of your servers
    - Send a permanent (5xx status-code) or temporary (4xx status code) error

Example: Checking MX Records for a Domain

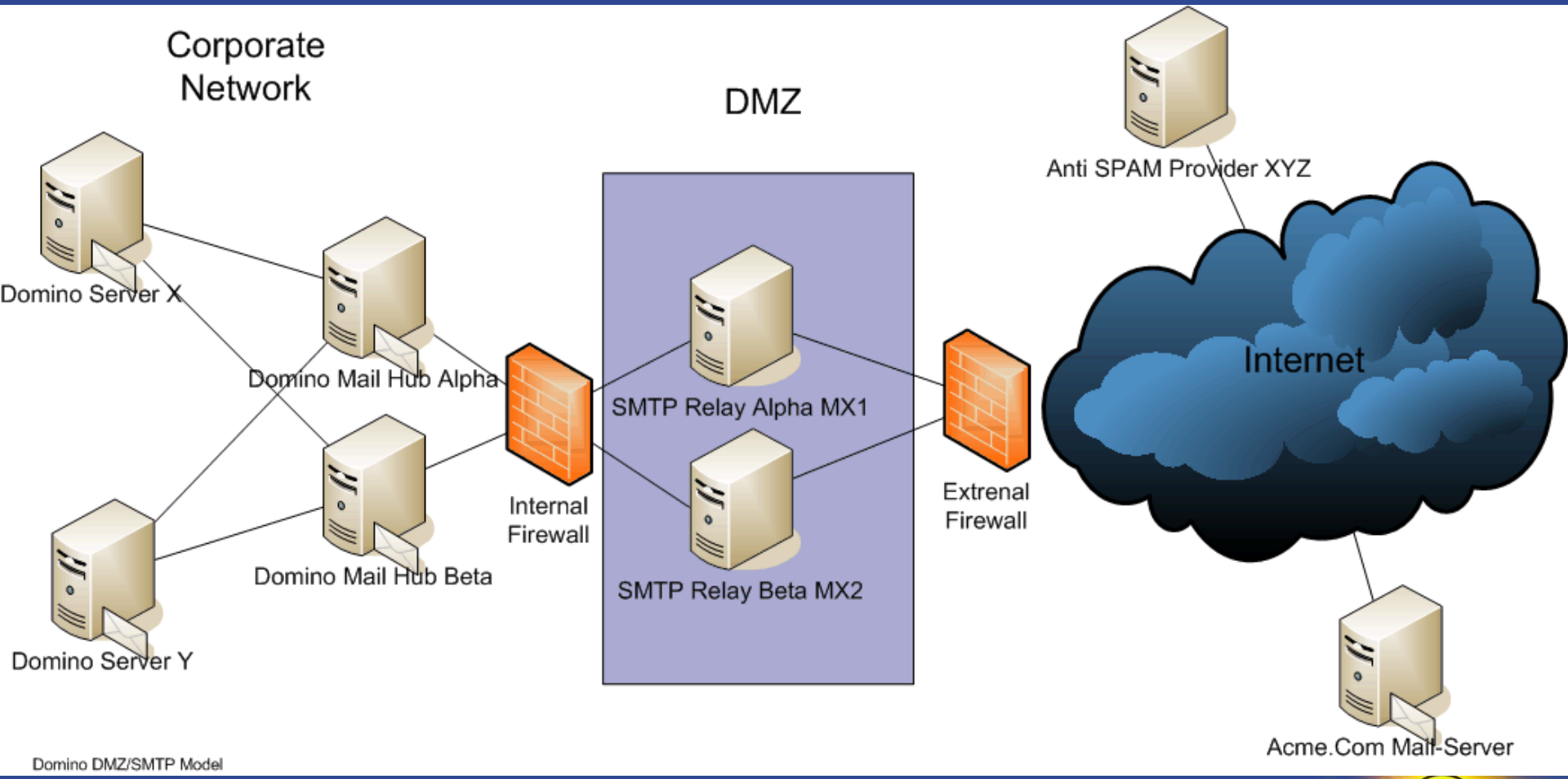
- Can be checked via nslookup
- SPAMMERs usually don't care about preferences and assume that low-priority MX records (with higher preference- value) are less optimal configured
  - That's why you don't want to use a backup MX at your ISP
  - If your server does not respond messages are queued at the sending SMTP MTA
    - That's what SMTP MTAs designed for

```
nslookup
> set query=mx
> iris.com
Server:  nsh-dmz-01.dus.nashcom.de
Address:  192.168.96.20

Non-authoritative answer:
iris.com        preference = 10, mail exchanger = capricorn.iris.com
iris.com        preference = 20, mail exchanger = arista.iris.com
iris.com        preference = 40, mail exchanger = elektra.iris.com
iris.com        preference = 30, mail exchanger = epic.iris.com
> quit
```

Multiple Messaging Scenarios

- This is just a generic example to demonstrate possible combinations



Domino DMZ/SMTP Model

Scenario1: Domino Server Only

- Domino Server located in the DMZ
- MX Records directly point to Domino Servers
  - Inbound messages directly hit the Domino Server
  - Anti Relay configuration REQUIRED for Domino!
  - Think about Anti-SPAM (e.g. Domino Black/Withe-Lists, 3rd party Domino Tools...)
- Outgoing mail is directly send to the Internet
  - Domino Server should have fast local DNS server!
- Connection between Corporate Network and Domino uses NRPC
- Firewall Rules needed
  - SMTP (port 25) Inbound and Outbound to Internet
  - DNS UDP and TCP (port 53) for local DNS servers! (at least two to avoid SPoF!)
  - NRPC (port 1352) Inbound/Outbound between Domino DMZ and Corporate Network
    - Domino needs a connection both ways
  - Depending on your needs Domino DMZ NRPC (port 1352) with Internet for Notes Mail
    - Ensure port encryption is enabled on Domino server

Scenario2: Domino Server with Relay Host in DMZ

- Domino Server located in corporate network
- Relay Host in DMZ – for example Sendmail or an appliance box
- MX Records directly point to Relay Host in DMZ
  - Inbound messages hit the relay host and are forwarded to the Domino Server
  - Anti Relay configuration REQUIRED for Relay Host
  - Anti-SPAM should be done on Relay host / Appliance
    - Depending on your configuration have e.g. LDAP lookups on Domino for checking recipients before mail is accepted
- Outgoing mail is send from Domino to the Relay Host
  - Connection between Corporate Network and Domino uses SMTP
- Firewall Rules needed
  - Domino SMTP (port 25) Inbound and Outbound between Relay Hosts/Appliance in DMZ
  - DNS UDP and TCP (port 53) for local DNS servers! (at least two to avoid SPoF!)
  - LDAP (port 389) Inbound to Domino Server from Relay Host
    - LDAP over SSL (port 636) would be overkill because of firewall

Scenario3: Domino Server with external Provider

- Domino Server(s) located in DMZ
- Inbound mail is send to the Messaging Provider
  - MX Records directly point to the provider
  - Provider relays messages to Domino in DMZ via SMTP
  - Domino forwards messages to internal network over NRPC
  - Provider might need LDAP Lookup to Domino in DMZ to check recipients
- Outgoing mail is send from Domino in DMZ to Provider
  - Connection between Corporate Network and Domino in DMZ uses NRPC
  - Connection between Domino in DMZ and Provider uses SMTP
- Firewall Rules needed
  - NRPC (port 1352) Inbound and Outbound between Domino Corporate Network and DMZ
  - SMTP (port 25) Inbound and Outbound between Domino DMZ and Provider
  - DNS UDP and TCP (port 53) for local DNS servers! (at least two to avoid SPoF!)
  - LDAP (port 389) Inbound from Provider to Domino DMZ
    - Depending on Security: LDAP over SSL (port 636) --> Causes Overhead!

Scenario4: Combinations

- Any sort of combination of the 3 Scenarios
  - e.g. Inbound via provider but outbound directly to Internet via Domino, ...
- But from Domino point of view this comes down to 4 options
  - Outbound
    - Outbound Mail is directly send by Domino
    - Outbound Mail uses any kind of relay host
  - Inbound
    - Inbound Mail hits relay server and is forwarded to Domino
    - Inbound Mail is directly delivered to a Domino server
- The next pages describe specific tuning for those 4 options
- You also have to ensure none of the components become a Single Point of Failure (SPoF)

Transfer and Delivery Tuning

- Config Doc - Router/SMTP - Restrictions and Controls -
  - Delivery Controls - Maximum delivery threads:
  - Transfer Controls - Maximum transfer threads:
  - Transfer Controls - Maximum concurrent transfer threads:

- Default is based on BufferPoolSize Formula
  - does not make sense in most cases
  - Maximum delivery threads = 3 + BufferPoolSizeMB / 32
  - Maximum transfer threads = 3 + BufferPoolSizeMB / 32
  - Total Maximum in default formula is 25 (means you reach the limit at 704MB)
  - Maximum concurrent transfer threads = Maximum transfer threads / 2

Concurrent Delivery of Large Messages to Large Group

- If large messages being to a large group of users.
  - When this message is sent out, all other mail backs up until this large message is delivered to all of its recipients.
  - This also causes a large memory consumption (BLK_OPENED_NOTE)
- You can limit the message delivery for this mail to one router thread since D6.x
  - SPR# JCHN4YCSKC – notes.ini RouterMaxConcurrentDeliverySize=n
  - Defines in Bytes the size limit for the message
  - This way only one delivery thread is "blocked" and there is only once instance of the message in memory!

General Best Practices

- notes.ini Disable_BCC_group_expansion=1
  - Expansion of BCC Groups can cause huge performance overhead TN #1089346
- notes.ini SMTPGreeting =Nash!Com ESMTP Service ready at %s
  - Hides Domino Version and allows own branding %s is placeholder for timedate
  - Example: 220 NashCom ESMTP Service ready at Fri, 5 Jan 2007 12:00:42 +0100
- notes.ini SMTPNoVersionInRcvdHdr=1
  - Removes Domino Version Information from Received Header

Relay Host Config Tuning

- Config Doc - Router/SMTP - Restrictions and Controls -
  - Transfer Controls - Initial transfer retry interval: Default 15 minutes!
  - TN #1089949: Interval used when server is not available on transfer.
    - First retry is 1x interval, second 2x interval, than every next retry after 3x interval!
      - This would be 45 minutes if the Relay server is not available for a while!
      - You should set this value to 1-3 minutes for a Relay Host Configuration
- notes.ini RouterAllowConcurrentXFERToALL=1
  - Causes concurrent transfer threads to be used for all types of connections inside and outside the local Domain
    - Without this setting some connection types only use one connection at once
  - DDT: Don't use this option if you have also slower connections (e.g. VPN)
- Disable DNS queries if server does not need to lookup names of connecting hosts
  - SMTPReverseLookups=0 when Domino thinks it's necessary
  - SMTPReverseLookups=1 never
  - SMTPReverseLookups=2 always

DNS Tuning/Troubleshooting

- By default only found domains are cached
  - If a Domain is not found the server by default retries up to 4 times if the DNS entry can be found.
    - Leads to message dispatch time of up to 16 seconds (including wait time per message)
      - Usually the case when you see the router status: Last Error: "Waiting for DNS"
      - "DNS requests time out" means usually that DNS server is not responding any more
      - check via "tell router status"
  - notes.ini MailDomainNoHitCacheTimeToLive=1800
    - Caches unsuccessful attempts for 30 Minutes
  - D7.0.2 notes.ini RouterDNSQueryRetryCount=2 (default 4)
    - Number of DNS query attempts. Each attempt doubles the wait time starting with 1 sec.
  - notes.ini Debug_TCP_Resolver=1 enables debugging for e.g. MX Record resolving

LDAP Configuration

- Create a user in the Domino directory
  - Needs fullname and HTTP password to be used as LDAP account
  - User does only need to be able to read the Domino directory
- For LDAP Lookup check the following settings in Server Document
  - Ensure LDAP port is enabled (389) else LDAP task will not start.
  - Ports / Internet Ports / Directory
  - Authentication Options
    - Name and Password: Yes
    - Anonymous: Based on your security needs
- Options can be specified separately for standard port and LDAP over SSL
  - In most cases unencrypted LDAP should be fine as long as the channel is trusted (e.g. within the firewall)
  - Encrypted LDAP needs SSL key-ring and Internet Cross Certificates on client side
  - SSL session can have impact on Domino server performance!

LDAP Troubleshooting

- Take care of "Enforce Server access settings" in LDAP Configuration
  - If LDAP user has no server access rights LDAP will not work
- Ensure that "Maximum Internet name and password" is set to reader or higher
- Ensure that LDAP user has at least reader access in names.nsf!
- Use ldapdebug=7 in case your LDAP connection does not work
  - Very verbose output for troubleshooting!
- Avoid complex LDAP queries for performance reasons
  - Best would be a simple query that works with the internal LDAP view

Anti SPAM Configuration

- This is not a Anti SPAM Best Practices Session
  - But I want to give you some general ideas
- Depending on your needs Domino 7 Anti-SPAM features might already help
  - You should be careful when using features like "DNS verify" because that might block not correctly configured customer servers!
  - You should have a correctly configured "IN-ARPA.ADDR" for all your external servers
    - Test if IP address of server resolves into right name via nslookup!
  - There are many resources out there how to configure DNS Black/White-Lists, etc...
  - Most settings are quite intuitive
  - Most is configured in config document
  - But there are a couple of caveats and tips
  - The first step is always to check your relay configuration to ensure your servers are not abused by SPAMMERs!
- But for larger installations it would make sense to look into a 3rd party tool or a SMTP Appliance (e.g. SpamAssassin on Linux, IronMail, ...)

Tagging or Blocking Messages

- Depending on your needs you might block or tag certain types of messages
  - Tagged messages can be

    a.) Routed into a different SPAM database with Server Mail Rules customized via "Extension Manager" Hooks

    b.) Moved to the SPAM folder in the mail-file with mail rules or better with a mail-pre-delivery agent (see example next page)

  - With Domino you can either block or tag messages for all configured RBL sites but not individual. Other solutions provide better flexibility and better success rates

  - Tip: You can specify groups allow/deny lists etc. in the configuration document for easier administration.
    - Those group can contain DNS names, IP addresses and IP ranges (e.g. [192.168.1.*]
  - Since Domino 7 you can also use DNS and private white-list

Pre-Delivery Agent for Anti-SPAM Processing

- Very low overhead because directly invoked by the mail-router in the context of the message
  - This is very easy to roll-out and to maintain if all your pre-delivery logic is stored in the mail-file design – the example below
  - Take care each Mail-Database can only one pre-delivery agent but that is usually OK

```
Sub Initialize
  Dim s As New NotesSession
  Dim doc As NotesDocument

  Print "Running SPAM check mail pre-delivery agent"
  s.ConvertMime = False
  Set doc = s.DocumentContext

  If (doc.X_Spam_Flag(0) = "YES") Then
     Print "We got SPAM"
     Call doc.PutInFolder( "($JunkMail)" )
     Call doc.RemoveFromFolder( "($Inbox)" )
  Else
     Print "not a SPAM message"
  End If
End Sub
```

- Basic Example without error checking!
- For DNS BlackList
  Check item $DNSBLSite
- For DNS WhiteList
  Check item $DNSWLSite

Links and Resources

- Anti SPAM
  - Developer Works Controlling spam: Advanced SMTP settings in Lotus Domino
    - http://www.ibm.com/developerworks/lotus/library/spam-smtp1/
    - http://www.ibm.com/developerworks/lotus/library/spam-smtp2/
  - http://spamassassin.apache.org/
- Lotus Knowledge Base
- Business Partner Forum if you are an IBM BP
- RFCs
  - http://www.faqs.org/rfcs/rfc821.html
  - http://www.faqs.org/rfcs/rfc822.html
  - http://www.faqs.org/rfcs/rfc1521.html

Question and Answers

- Related Sessions:
  - HND203 Mail Routing Mastery / Andrew Pollack
    - R1 SW Mockingbird - Monday 4:30pm – 6:15pm
    - R2 SW Mockingbird - Tuesday 08:00am – 9:45am
  - BP309 A MIME is a Terrible Thing to Waste—Automating MIME-Encoded Email
    - Erik Werfel, Mike Barlow
    - DL S. Hemisphere II - Tuesday 4:15pm - 5:15pm
- Questions?
  - Now or send an email after Lotusphere
  - nsh@nashcom.de
  - http://www.nashcom.de
- Please fill out your evaluations!

Lotus software

Nash!Com Communication Systems

Lotusphere 2007

© 2007 All Rights Reserved.