



MANAGING EMAIL

Intelligent front-end hosts for SMTP

By [Ron Herardian](#)

This article is the second in a three-part series covering Domino and Internet email. Last month I explained capacity planning issues for Internet email. This month's article describes front-end solutions that allow centralization of SMTP services and that ease migration to Domino from cc:Mail.

Internet email is not what it used to be. Medium and large sized companies today have to deal with multiple DNS domains, multiple languages (character sets), multiple Internet address formats, migration issues, spam, and directory synchronization issues. Managing Internet email can be complex and companies are often at a loss for ways to deal with these things. The answer, however, is much less complex than the problem: install an intelligent front-end host to process and route inbound Internet email. The power and architectural simplicity of this solution will become apparent as we look at the different problems that are all solved by this solution.

An intelligent front-end solution for SMTP means that inbound SMTP email is received by a mail host that forwards mail to various MTAs or gateways. Typically this means receiving email from the Internet and forwarding it to other systems through a private WAN. The simplest implementation of this kind would use Berkeley sendmail and a simple alias file. A more sophisticated version would do the following:

- Handle email for multiple DNS domains and address formats;
- Handle mail spanning multiple languages and character sets;
- Handle email migration issues;
- Provide industrial-strength anti-spam capabilities;
- Synchronize directory information with Domino and possibly other systems.

The same host may also serve as an outbound SMTP relay but this is standard functionality in sendmail so we won't spend any time looking at outbound Internet email. There may be one or many points at which mail exits an organization's WAN.

In last month's article I wrote about the rapid growth of Internet email and the challenges that it presents for administrators. Rapid growth in Internet email increases the administrative burden and creates pressure to centralize SMTP services. Centralization of SMTP services means that mail hosts must be able to handle multiple Internet domains and languages.

Multiple DNS domains: The Internet perspective

Nearly every company has to deal with multiple DNS domains. The reason why this is important is that companies want to standardize their Internet address format or limit the number of address formats. First we'll want to deal with the mechanics of this from the Internet point of view and then from the Domino point of view. It is important to note that the SMTP and DNS technologies allow mail for a given domain to be routed only to one primary point for that domain. In general, Internet mail is not routed based on the user ID (an exception is source routing).

From the Internet point of view multiple Internet domains mean multiple MX (mail exchanger) records in the

company's DNS database. In most implementations of bind, the DNS daemon, the "database" is a set of related structured text files containing IP address and host name information so that machines can find each other by name based on which Internet domain they are in (or find names by looking up addresses). In the database, various record types are defined for machine addresses, mail exchangers, and other things. The MX records are in the domain database file typically named after the Internet domain name (e.g., GSSNET.DOM). In the file are records in the following format:

```
@ IN MX 10 mail1.gssnet.com
@ IN MX 20 mail2.gssnet.com
```

Handling email for multiple DNS domains usually means pointing MX records for more than one domain name to a single host. This host must be able to forward or deliver mail to users whose SMTP addresses contain the various domains handled by the company's mail hosts. One way to see what mail exchangers are configured in a DNS is to use the nslookup program, a command line utility available on most UNIX systems:

```
nslookup -type=MX gssnet.com
```

The output should look something like this:

```
gssnet.com preference = 10, mail exchanger = mail1.gssnet.com
gssnet.com preference = 20, mail exchanger = mail2.gssnet.com
gssnet.com nameserver = ns1.gssnet.com
gssnet.com nameserver = ns2.gssnet.com
mail1.gssnet.com internet address = 206.184.139.12
mail2.gssnet.com internet address = 206.184.139.13
ns1.gssnet.com internet address = 209.24.149.41
ns2.gssnet.com internet address = 209.157.102.11
```

```
nslookup -type=MX gssnet.com
```

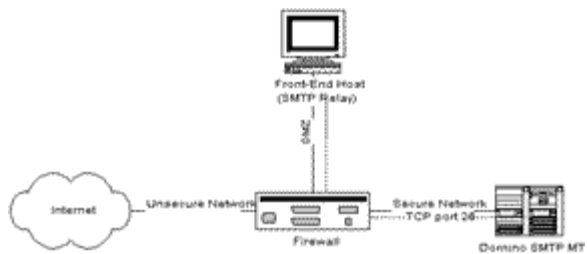
```
messagingcentral.com preference = 10, mail exchanger = mail1.gssnet.com
messagingcentral.com preference = 20, mail exchanger = mail2.gssnet.com
messagingcentral.com nameserver = ns1.gssnet.com
messagingcentral.com nameserver = ns2.gssnet.com
mail1.gssnet.com internet address = 206.184.139.12
mail2.gssnet.com internet address = 206.184.139.13
ns1.gssnet.com internet address = 209.24.149.41
ns2.gssnet.com internet address = 209.157.102.11
```

In this example Internet mail for both the gssnet.com and messagingcentral.com domains is sent to mail1.gssnet.com. Causing mail for multiple domains to be routed to a particular host is a straightforward matter. It's only a question of editing the right text files and adding or modifying the right MX record entries.

Firewalls

Of course there are other considerations, for example sending mail through a firewall. Typically, the front-end host will be placed on a DMZ connected to a firewall but not on the outside of the firewall, as shown in Figure A.

FIGURE A



Here's a diagram of a simplified DMZ Configuration for SMTP Relay Host.

Of course, the diagram in Figure A is simplified, but it gets at the main issue which is securing internal SMTP services to make them inaccessible to any host other than the SMTP relay or front-end host.

There are so-called email firewall products on the market that provide virus scanning, content checking, anti-spam capabilities and other features but this article isn't directly concerned with email security at this level.

Multiple DNS domains: The Domino perspective

From the Domino perspective any domain and any SMTP address can be supported for inbound email and for user-from addresses (when users send email outbound). It's the SMTP addresses that are the main issue. The main thing to remember is that the SMTP address used must match the "Internet/short name" field in the corresponding person document in the Domino NAB (e.g., Super.Human@anyname.com, is valid for user Ron Herardian when this address appears in Ron Herardian's Internet "Internet/short name" field). An agent can be used to automatically populate the "Internet/short name" field based on which Domino OU the user belongs to.

When writing agents of this kind, keep in mind that addresses must be unique thus checking for duplicates is important. For example in applying an address scheme such as 'First_Last' it would be easy to forget that in Domino "First Last/Sales/GSS" and "First Last/Exec/GSS" are unique whereas the two common names are identical.

The default address format for SMTP from fields includes Domino NAB information but this results in unnatural (but functional) SMTP addresses such as First_Last/CAM/Lotus@lotus.com. The problem becomes more apparent when things are longer (e.g., LongFirst_LongLast/LongOU1/LongOU2/LongOU3/ROOT@longhost.longdomanname.com, which to most users would be incomprehensible).

Multiple languages and character sets

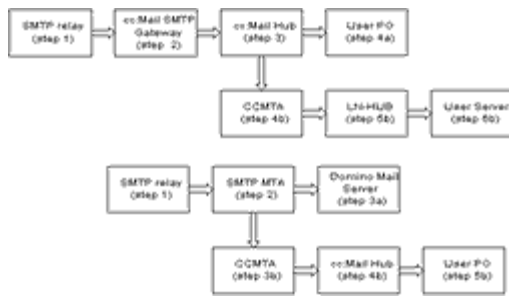
In currently deployed versions (prior to R5) the Domino SMTP MTA could handle only one character set per MTA. Messages piped through the wrong MTA would appear garbled or special characters would be lost. In theory, MIME encoding of Internet message bodies would avoid using the wrong character set but the real world is not very theoretical. In practice, we might find a Pan European version of Windows 95 configured for Lithuania running an international English version of Lotus Notes; so what's the correct character set for Internet messages? You see the problem.

In Domino R5, the issue is not completely solved but the SMTP MTA gains the ability to forward mail to the appropriate MTA. The intelligent front-end solution solves this problem by routing inbound mail directly to the appropriate MTA or gateway.

Email migration issues

When migrating from cc:Mail to Domino, use of both the SMTP MTA and CCMTA are necessary. Unfortunately, routing cc:Mail messages to and from the Internet via the cc:Mail and SMTP MTAs has been a less than perfect solution in the past, significantly because of cc:Mail MTA issues. Usually, companies try to consolidate SMTP services on one side or the other during migration, as shown in Figure B.

FIGURE B



This diagram shows consolidation of SMTP Services on cc:Mail and on Domino.

In theory consolidation of SMTP services on Domino is the cleanest configuration, however, in both configurations the MTAs are dependent on each other.

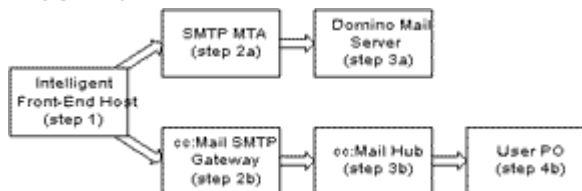
Since Domino is the migration direction, consolidation of SMTP services on Domino is intuitive. Going with this solution implies that the amount of mail passing through this relatively inefficient route will be systematically reduced and ultimately eliminated when migration is completed. The negative impact of any problems related to using multiple MTAs will be reduced and these problems will ultimately be eliminated when migration is complete because the cc:Mail MTA will no longer be needed. In any case, consolidation of SMTP gateway services on Domino is more efficient than consolidation of SMTP gateway services on cc:Mail.

Enter the intelligent front-end host

The best solution is to maintain independent SMTP services for cc:Mail and Domino during migration. The cc:Mail system can continue to use its existing gateway and Domino users use the SMTP MTA to send and receive mail from the Internet. At the same time routing Domino mail to and from the Internet via a cc:Mail-based SMTP gateway can be more problematic than going the other way. The only problem with using separate SMTP services for the two systems during migration is that inbound mail can only be routed to the SMTP gateway for cc:Mail or to the SMTP MTA. Enter the intelligent front-end host.

An SMTP host that can route mail based on the user ID (instead of just the domain) can send mail for Domino users to the MTA and mail for cc:Mail users to the cc:Mail SMTP gateway. This removes the dependency of the MTAs on one another so that Internet mail is autonomous for both systems. With an intelligent front-end host, inbound messages for cc:Mail users are routed directly to the cc:Mail SMTP gateway while inbound SMTP messages for Domino users are routed directly to Domino. Figure C shows a diagram of how that works.

FIGURE C



Here's a diagram of a Front-End Host Solution.

The intelligent front-end host is the most efficient alternative and it eliminates dependency of SMTP and cc:Mail MTA services. The intelligent front-end host also provides a logical load distribution (it does not impose the burden of Internet mail for cc:Mail users on Domino or vice versa). The core technology of the front-end host solution is essentially sendmail, which is known for its scalability and reliability. Using a sendmail (or derivative) as an SMTP relay for inbound mail improves both capacity and reliability is what I'd recommend for use with all SMTP gateways including the Domino SMTP MTA.

Directory synchronization

In order for the front-end host to route mail to an appropriate MTA or gateway, it must know which SMTP domains and user IDs go with which MTA or gateway. This means that some type of directory must be used. If a directory is used, it should be synchronized with the Domino NAB. We use Netscape Directory Server and Messaging Server to build front-end host solutions and synchronize the NAB one-way with the Netscape LDAP directory (using our GSS LDAP Synchronizer). Domino isn't used as the LDAP server because it doesn't support storage and retrieval of arbitrary data.

Although many versions of sendmail can be used as to front-end SMTP we prefer to use Netscape Messaging Server because of its LDAP-based routing and easy to configure SMTP routing tables. We also prefer Netscape because of its server plug-in capability and built-in powerful anti-spam capabilities: the front-end host is the correct place to eliminate spam, not at the MTA.

Summary

Several practical problems can be solved by implementing an intelligent front-end host for SMTP. This solution can help to address issues such as multiple Internet domains and SMTP address formats, multiple languages and character sets, coexistence and migration issues for cc:Mail and Domino, and spam. The core technology is LDAP-enabled SMTP and an LDAP directory can be synchronized with the NAB. For larger companies some type of front end host is necessary and increasingly medium-sized companies need this type of solution in order to support centralized processing and routing of Internet email for a number of different business units.

Glossary

DNS - domain name system
MX record - the IP address of a mail exchanger
Mail exchanger - an SMTP host that handles mail for a domain
bind - a program that provides DNS services
sendmail - the standard SMTP e-mail program for Internet mail
LDAP - Lightweight Directory Access Protocol
MTA - Message Transfer Agent
nslookup - a utility to look up network information in DNS

Product availability and resources

The GSS LDAP Synchronizer is available from the products section of <http://www.gssnet.com>.

Netscape Directory Server is available at <http://home.netscape.com/directory/v4.0/index.html>.

DominoPower Technical Editor Ron Herardian is CEO and Chief Technical Consultant at Global System Services (GSS). You can reach Ron via email at rherardi@gssnet.com, or via his web page at <http://www.gssnet.com>. GSS also sponsors Messaging Central (at <http://www.messagingcentral.com/>), a web-based resource devoted to electronic messaging integration, Internet messaging standards, and migration.

Copyright © 1998-2008, [ZATZ Publishing](#). All rights reserved worldwide.