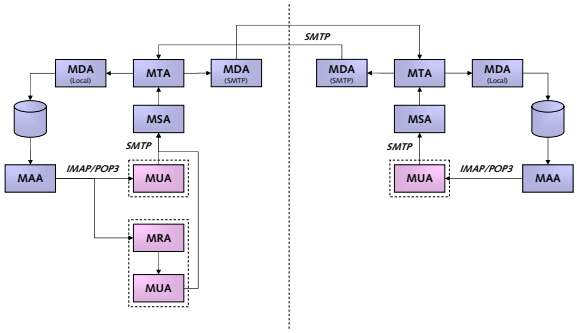
Electronic Mail

PRINCIPLES – DNS – ARCHITECTURES – SPAM

David Byers

davby@ida.liu.se
IDA/ADIT/IISLAB

Mail system components



MUA

Mail User Agent

- Reads and writes e-mail
- Writes e-mail to MTA using SMTP (usually)
- Reads e-mail delivered by MDA or retrieved by MRA

Examples

- Mozilla Thunderbird
- Outlook Express

MRA

Mail Retrieval Agent

- Retrieves e-mail from MAA
- Makes mail available to MUA

Examples

- Fetchmail
- Integrated in Thunderbird etc.

MAA

Mail Access Agent

- Authenticates MUA/user
- Reads e-mail from mailbox
- Makes e-mail available to MUA

Examples

- Courier IMAPD

MSA

Mail Submission Agent

- Accepts mail from MUA
- Prepares and delivers to MTA

Examples

- Postfix postdrop+pickup
- sendmail-msa

MTA

Mail Transfer Agent

- Routes incoming mail
- Determines which MDA to send mail to
- May alter mail being routed

Examples

- Postfix cleanup + qmgr + + trivial-rewrite
- Sendmail

MDA

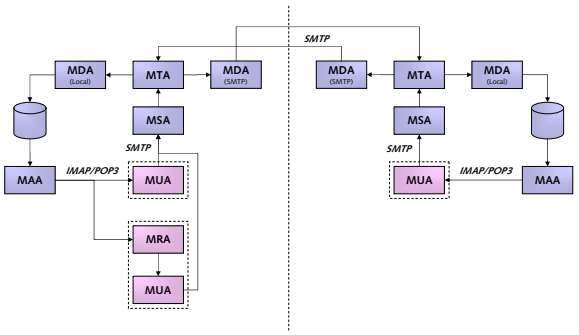
Mail Delivery Agent

- Accepts mail from MTA
- Delivers mail to local mailbox
- Delivers mail to other MTA

Examples

- Postfix local, smtp, pipe
- mail.local (local delivery)
- procmail (local delivery)

Mail system components



Path of a message

1. New message written

- Mail is written in MUA
- Mail is submitted to MSA

2. Reception of message at MSA

- MSA authenticates user
- MSA checks that user is authorized to submit mail
- MSA may rewrite headers
- MSA submits message to MTA
- MSA reports success to MUA

3. Reception of message at MTA

- MTA checks that sender and recipient are valid and permitted
- MTA checks that contents are valid and permitted
- MTA may run content filters
- MTA may rewrite headers
- MTA determines which MDA to submit mail to (SMTP, local etc)
- MTA submits mail to MDA
- If unsuccessful, MTA queues mail for later delivery

Path of a message

4. Reception of message at MDA

- MDA sends message to remote MTA using SMTP (example)

5. Rcpt of message at remote MTA

- Same as step 3
- Message submitted to MDA

6. Reception of message at MDA

- MDA may check filters/rules
- MDA delivers message to appropriate local mail store

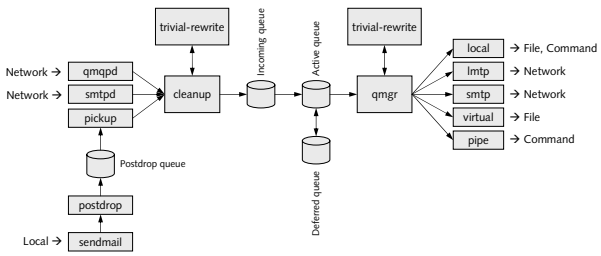
7. MAA detects new message

- MAA signals MUA
- MUA retrieves message

8. Message read

- MUA presents message to user

Postfix architecture



SMTP

Simple Mail Transfer Protocol

- Default: TCP port 25
- RFC 2821
- ESMTP – Extensions

- Text-based protocol
- No encryption
- No authentication

Example

```
%telnet mail.ida.liu.se 25
Trying 130.236.177.25...
Connected to mail.ida.liu.se.
Escape character is '^]'.
220 mail.ida.liu.se ESMTP Sendmail 8.13.3/8.13.3; Mon, 29 Aug 2005
    13:34:42 +0200 (CEST)
EHLO lap-65.ida.liu.se
250-mail.ida.liu.se Hello gedrix.ida.liu.se [130.236.176.11],
    pleased to meet you
MAIL FROM:<davby@ida.liu.se>
250 2.1.0 <davby@ida.liu.se>... Sender ok
RCPT TO:<info@samizdat.se>
250 2.1.5 <info@samizdat.se>... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
From: David Byers <davby@ida.liu.se>
To: Samizdat Info <info@samizdat.se>
Date: Mon, 29 Aug 2005 13:38:00 +0100
Subject: Testing SMTP

Body text.
.
250 2.0.0 j7TBYgXf001051 Message accepted for delivery
QUIT
221 2.0.0 portofix.ida.liu.se closing connection
```

The role of DNS

Problem: which server to contact for a mail address?
Solution: look up MX record in DNS

Example:

example.com MX 10 mail1.example.com.
example.com MX 10 mail2.example.com.
example.com MX 20 mx.nodomain.edu.

Structure of a message

Envelope

- From SMTP dialog

Header

- Message metadata
- Specified in RFC 2822

Body

- Sequence of ASCII characters
- Separated from body by CRLF

Syntax

message::= headers CRLF body
headers ::= header headers | ε
header ::= name ":" value CRLF

```
Return-Path: andjo@ida.liu.se
Delivery-Date: Fri May 14 08:38:34 2004
Received: from diag7.ida.liu.se (diag7.ida.liu.se [130.236.177.217])
      by portofix.ida.liu.se (8.12.11/8.12.11) with ESMTP id i423760;
      Fri, 14 May 2004 08:38:31 +0200 (MEST)
Received: (from andjo@localhost)
      by diag7.ida.liu.se (8.12.10+Sun/8.12.10/Submit) id i401197;
      Fri, 14 May 2004 08:38:31 +0200 (CEST)
Date: Fri, 14 May 2004 08:38:31 +0200
From: Andreas Johansson <andjo@ida.liu.se>
To: David Byers <davby@ida.liu.se>
Cc: pjn@ida.liu.se
Subject: Re: =?ISO-8859-1?Q?N=E4tverksproblem?=
Message-Id: <20040514083831.495c66a2.andjo@ida.liu.se>
In-Reply-To: <41r7togybd.fsf@obel19.ida.liu.se>
References: <41r7togybd.fsf@obel19.ida.liu.se>
Organization: =?ISO-8859-1?Q?Link=F6pings?= universitet
X-Mailer: Sylpheed version 0.9.6 (GTK+ 1.2.10; sparc-sun-solaris2.9)
Mime-Version: 1.0
Content-Type: text/plain; charset=ISO-8859-1
X-Virus-Scanned: clamd / ClamAV 0.70, clamav-milter 0.70j
X-Spam-Flag: NO
X-Scanned-By: milter-spamc/0.15.245 ( [130.236.177.25]); pass
```

Things the MTA does

Header rewriting

- Addition of received header
- Addition of Message-ID
- Address rewriting

Example rewriting

- Removal of host name
- Addition of domain name
- davby → david.byers

Mail routing

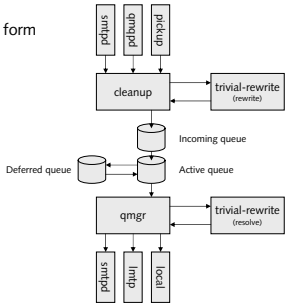
- Find server for recipient address
- Queue mail for submission
- Re-submit failed messages
- Send delivery status notifications

SMTP example

- Find MX records for address
- Try records in ascending order
- Try A record for address

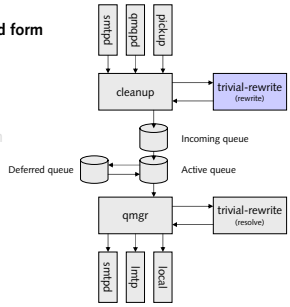
Postfix address rewriting

- Rewrite addresses to standard form
- Canonical address mapping
- Address masquerading
- Automatic BCC recipients
- Virtual aliasing
- Resolve address to destination
- Mail transport switch
- Relocated users table
- Generic mapping table
- Local alias database
- Local per-user .forward files
- Local catch-all address



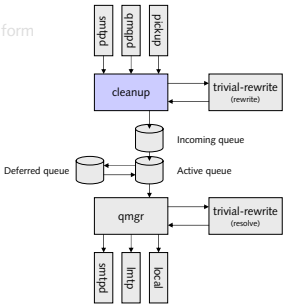
Postfix address rewriting

- **Rewrite addresses to standard form**
- Canonical address mapping
- Address masquerading
- Automatic BCC recipients
- Virtual aliasing
- Resolve address to destination
- Mail transport switch
- Relocated users table
- Generic mapping table
- Local alias database
- Local per-user .forward files
- Local catch-all address



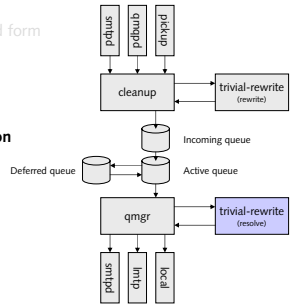
Postfix address rewriting

- Rewrite addresses to standard form
- **Canonical address mapping**
- **Address masquerading**
- **Automatic BCC recipients**
- **Virtual aliasing**
- Resolve address to destination
- Mail transport switch
- Relocated users table
- Generic mapping table
- Local alias database
- Local per-user .forward files
- Local catch-all address



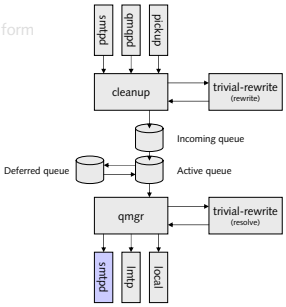
Postfix address rewriting

- Rewrite addresses to standard form
- Canonical address mapping
- Address masquerading
- Automatic BCC recipients
- Virtual aliasing
- **Resolve address to destination**
- **Mail transport switch**
- **Relocated users table**
- Generic mapping table
- Local alias database
- Local per-user .forward files
- Local catch-all address



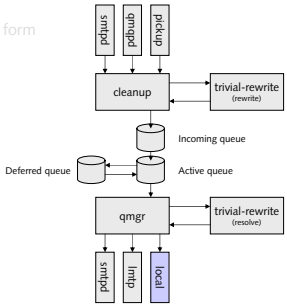
Postfix address rewriting

- Rewrite addresses to standard form
- Canonical address mapping
- Address masquerading
- Automatic BCC recipients
- Virtual aliasing
- Resolve address to destination
- Mail transport switch
- Relocated users table
- **Generic mapping table**
- Local alias database
- Local per-user .forward files
- Local catch-all address



Postfix address rewriting

- Rewrite addresses to standard form
- Canonical address mapping
- Address masquerading
- Automatic BCC recipients
- Virtual aliasing
- Resolve address to destination
- Mail transport switch
- Relocated users table
- Generic mapping table
- **Local alias database**
- **Local per-user .forward files**
- **Local catch-all address**



Things the MTA does

Content filtering
- Scan for virus content
- Check validity of attachments
- Check size of messages
- Check for spam

Common spam checks
- Keyword/feature filters
- IP address blacklists
- Greylisting

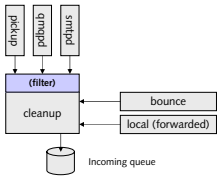
Authorization
- Check submitting host IP
- Check from address
- Check recipient address
- Check contents

Typically permitted
- Mail from local systems
- Mail to local recipients
- Mail from trusted hosts to any recipient

Postfix content filters

Three flavors
- **Built-in content inspection**
- After queue content filter
- Before queue content filter

Built-in content inspection
- "Body checks", "Header checks"
- Regexp checks on message
- For stopping **specific** problems



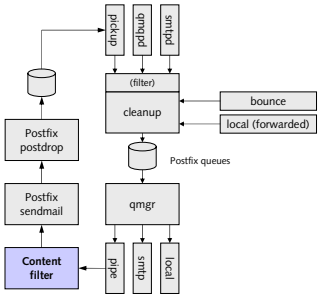
Postfix content filters

Three flavors

- Built-in content inspection
- **After queue content filter**
- Before queue content filter

After queue content filter

- After mail has been accepted
- Heavy-duty filtering
- Need to avoid spurious DSNs



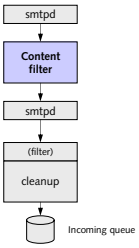
Postfix content filters

Three flavors

- Built-in content inspection
- After queue content filter
- **Before queue content filter**

Before queue content filter

- Before mail is accepted
- Heavy-duty filtering
- Only for low-volume sites



Spam protection

- Relay restrictions
- Greylisting
- DNS-based blocklists

SMTP Restrictions

Denying relay

```
220 solzhenitsyn.samizdat.se ESMTP Postfix
HELO gedrix.ida.liu.se
250 solzhenitsyn.samizdat.se
MAIL FROM:<davby@ida.liu.se>
250 Ok
RCPT TO:<byers@lysator.liu.se>
554 <byers@lysator.liu.se>: Relay access denied
```

Greylisting in action

```
220 portofix.ida.liu.se ESMTP Sendmail 8.13.3/8.13.3
HELO metzengerstein.visit.se
250 portofix.ida.liu.se Hello metzengerstein.visit.se [212.214.112.221]
MAIL FROM:<info@samizdat.se>
250 2.1.0 <info@samizdat.se>... Sender ok
RCPT TO:<davby@ida.liu.se>
451 4.7.1 Greylisting in action, please come back in 00:10:00
```

DNS-based blocklists

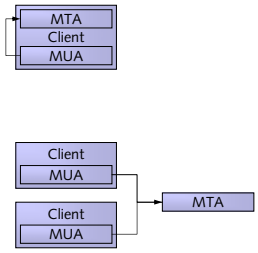
Blocklists work like in-addr.arpa lookup

```
%host -t TXT 1.185.167.195.l1.spews.dnsbl.sorbs.net
1.185.167.195.l1.spews.dnsbl.sorbs.net  TXT
    "! [1] XPD Limited, see http://spews.org/ask.cgi?S3007"

%host -t TXT 1.185.167.195.dnsbl.sorbs.net
1.185.167.195.dnsbl.sorbs.net   TXT    "Spam Received See:
           http://www.sorbs.net/lookup.shtml?195.167.185.1"
```

Architectures

Client-side outgoing mail



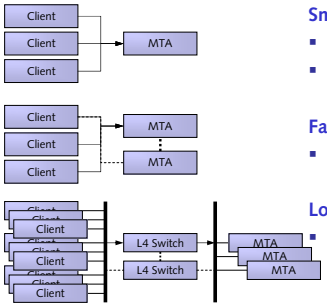
Client has an MTA

- Client MTA queues mail

Client has no MTA

- If central MTA is down, no mail can be sent

Outgoing mail



Smarthost

- All mail through one MTA
- Central configuration

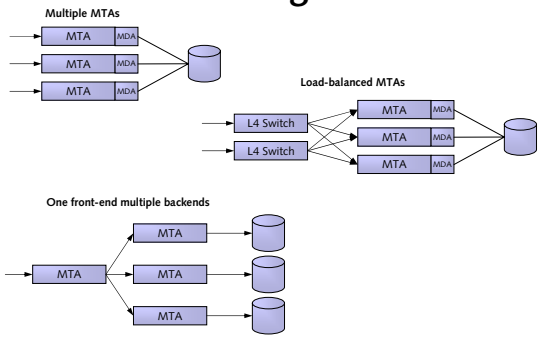
Failover

- Better reliability

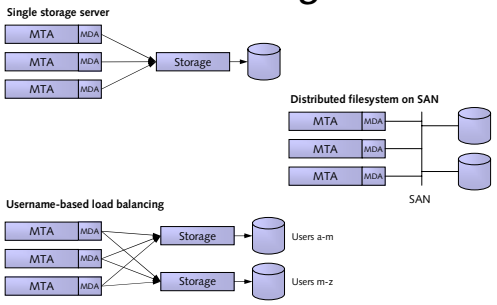
Load balancing

- Better reliability
- Better performance

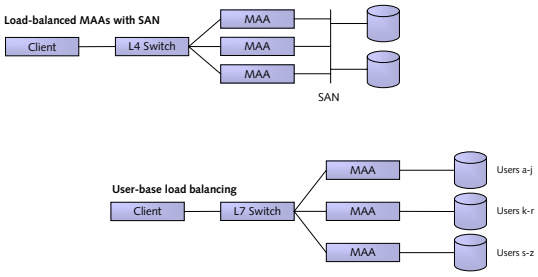
Incoming mail



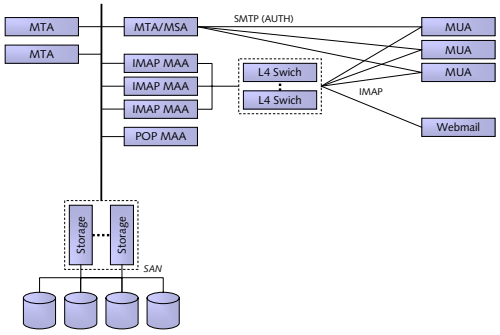
Mail storage



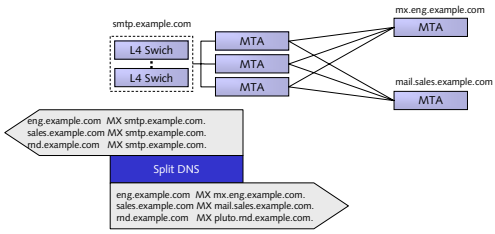
Reading mail



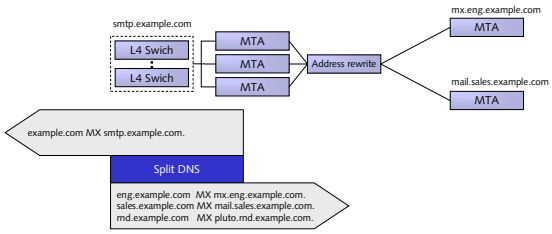
Centralized example



Corporate example (I)



Corporate example (II)



Summary

E-mail components
- MTA, MDA, MUA etc

Postfix architecture
- Address rewriting
- Content filtering

Spam protection
- Relaying, greylisting

Mail system architectures