Email Architecture

with sendmail and postfix

dr. C. P. J. Koymans

Informatics Institute

Universiteit van Amsterdam

November 27, 2007

Organisation

- Say O is an example organisation
  - A is an autonomous suborganisation
  - M is a managed suborganisation
    - a is an autonomous part of M
    - m is a managed part of M

Structure of the organisation

- O
  - A
  - M
    - a
    - m

DNS mirrors the structure

- Where are the cuts?
- O.org.
  - A.O.org.
  - M.O.org.
    - a.M.O.org.
    - m.M.O.org.

Email mirrors the structure

- mail.. . . are mail relays and servers
  - mail.O.org.
    - mail.A.O.org.
    - mail.M.O.org.
    - mail.a.M.O.org.
    - mail.m.M.O.org.

MX records (1)

O.org.	MX	0	mail.O.org.
A.O.org.	MX	0	mail.A.O.org.
		10	mail.O.org.
M.O.org.	MX	0	mail.M.O.org.
		10	mail.O.org.

MX records (2)

a.M.O.org.	MX	0	mail.a.M.O.org.
		5	mail.M.O.org.
		10	mail.O.org.
m.M.O.org.	MX	0	mail.m.M.O.org.
		5	mail.M.O.org.
		10	mail.O.org.

Email addresses

- Employee “The Boss” working in department “a”
  - boss@a.M.O.org
  - The.Boss@M.O.org
  - emp0@O.org

Email forwarding

- emp0@O.org is forwarded to
  - The.Boss@M.O.org, which is in turn forwarded to
    - boss@a.M.O.org
- Forwarding can be
  - user based (.forward)
  - system based (alias file or database)

SMTP flow (inbound) (1)

- Directly to mailhost in MX record
  - emp0@O.org enters at top
  - boss@a.M.O.org enters at leaf

SMTP flow (inbound) (2)

- Always to mail.O.org.
  - Requires “split” DNS
    - Different outside MX record for a.M.O.org., pointing to mail.O.org.
  - Alternatively block port 25 from the outside

SMTP flow (outbound)

- Directly to outside world
  - No “corporate” policy
  - Needs smart hosts decentrally
- Flowing up the tree step by step
- Directly to the top of the tree
  - Last two items use the “smart host” option

Mail access

- Only leaf mail servers supply mail access
- Intermediate servers are relay only
- In case you want to deliver higher in the tree
    - Create an extra child for mail delivery
    - Separate SMTP relay from local delivery and IMAP access

sendmail configuration (Ubuntu 7.10)

- Debian specific (based on sendmail 8.14.1)
- Has an extensive init script to control sendmail execution
- Uses a separate sendmail.conf file to source inside init script
- Uses a helper program (sendmailconfig) to generate the main configuration file sendmail.mc

sendmail configuration directory (Ubuntu 7.10)

- /etc/mail as configuration directory
    - sendmail.mc, which is used to generate
        - sendmail.cf
        - using the m4 macro processor
    - local-host-names
    - aliases
    - access
    - . . .

m4 macros (Ubuntu 7.10)

- Inside /usr/share/sendmail/cf
    - m4 source files m4/*
        - cf.m4, cfhead.m4, proto.m4
    - debian/*, domain/*, feature/*, . . .
    - hack/*, mailer/*, ostype/*, . . .

sendmail.mc

- OSTYPE(debian)
- DOMAIN(debian-mta)
- DAEMON_OPTIONS(. . .)
- FEATURE(. . .)
    - no_default_msa
    - access_db
    - . . .
- MAILER
    - local
    - smtp

debian.m4

- define(conf. . .)
- Lots of configuration parameters, to name a few
  - confSMTP_LOGIN_MSG
  - confCW_FILE
  - confDEF_USER_ID

debian-mta.m4

- Many more conf. . . options
  - confMAX_HOP
  - confDONT_BLAME_SENDMAIL
  - All kinds of TimeOut(TO)-timers
    - confTO_MAIL
    - confTO_QUIT
    - . . .

sendmail.cf macros

- Macros
  - C<class> ($=<class>)
  - F<class_in_file>
    - Fw/etc/mail/local-host-names
  - D<name> ($<name>)

sendmail.cf hostnames

- sendmail -bt -d0.4
  - Debugging local hostname(s)
  - $j=$w.$m
- What is inside $=w class?
  - Many “hostnames”, also numeric

sendmail.cf map lookup

- K<mapname> <type> <detail>
  - mailertable hash -o /etc/mail/mailertable.db
  - generics hash -o /etc/mail/genericstable.db
  - virtuser hash -o /etc/mail/virtusertable.db

sendmail.cf options

- AliasFile
- ForwardPath
- DaemonPortOptions (UseMSP)
- Timeout
- *LA (Queue, Refuse, Delay)
- SmtpGreetingMessage
- …

sendmail.cf headers

- HReceived:
  - $?sfrom $s $.$?_($?s$|from $.$_)$.
  - by $j ($v/$Z)$?r with $r$. id $i
  - $?u for $u; $|;$.
  - $b

sendmail.cf rulesets

- S<name>=<number>
  - canonify=3 (always first)
  - parse=0 (resolves <mailer,host,user>)
  - check_relay (to disable open relaying)
  - check_mail (checks MAIL FROM:)
  - check_rcpt (checks RCPT TO:)

sendmail.cf rules

- LHS (Left Hand Side)
  - $*, $+, $-, $@ (token matching)
  - $=, $˜(class matching)
- RHS (Right Hand Side)
  - $1, $2, . . . , $:, $@ (substitution; control flow)
  - $>, $?$|$. (recursion; conditional)
  - $[. . . $], $(. . . $) (IP lookup; map lookup)

Sendmail ruleset testing

- sendmail -bt
  - =S<ruleset>, =M
  - $<m>, $=<c>
  - /parse <address>
  - /try <mailer> <address>
  - /map <map> <lookup>

sendmail.cf mailers

- M<mailer> <attributes>
  - local (maybe procmail as MDA)
  - prog, *file*, *include* (builtin)
  - smtp, esmtp, smtp8, relay, bsmtp, fido
  - procmail (as mail filter, called with “-m”)

Postfix

- (Mostly) compatible with sendmail
  - supplies /usr/{lib,sbin}/sendmail emulation
- Good performance
- Safe and secure
- Modular and flexible

General postfix features

- Support for multiple transports
- Easy virtual domain configuration
- Extensive UCE/SPAM control
- Rewriting through table lookups

Postfix modular setup

- One resident master process
  - compare to inetd super server
- Some semi-resident daemons
  - started via master.cf file
  - something like inetd.conf

Postfix queues

- maildrop (local incoming)
- incoming (after cleanup)
- active (being worked on)
    - deferred (temporary failure)
    - hold (needs human intervention)
    - corrupt (needs human inspection)

Postfix security

- Is not setuid root
- Uses chroot environment
- Is modular and not monolithic
- Filtering of outside information

Postfix daemons

- pickup (mail from maildrop via postdrop ("sendmail"))
- smtpd (remote mail from the Internet)
- cleanup (repairs incoming mail)
- qmgr (processes mail queues)
- local (local delivery)
- smtp (remote delivery)

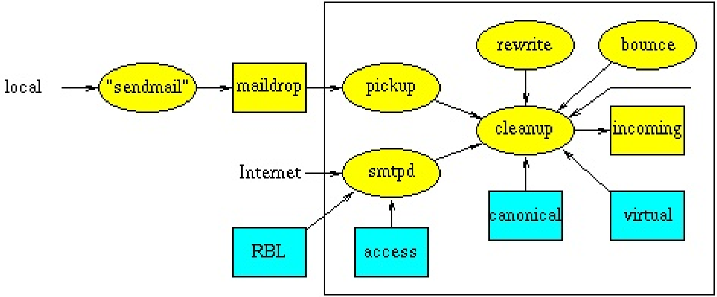
Postfix assistants

- (trivial-)rewrite
  - canonicalisation (compare “ruleset 3”)
  - resolving (compare “ruleset 0”)
- bounce
  - error mailer
  - defer messages

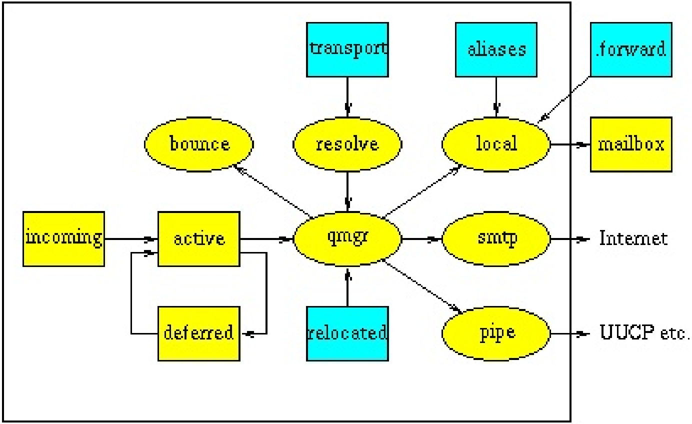
Postfix/Sendmail tables

Postfix	Sendmail
virtual	virtusertable
canonical	genericstable
transport	mailertable
access	access
relocated	- (aliases)

Postfix architecture inbound



Postfix architecture outbound



qmail

- Who looked at qmail and wants to explain?

Exim

- Who looked at Exim and wants to explain?