

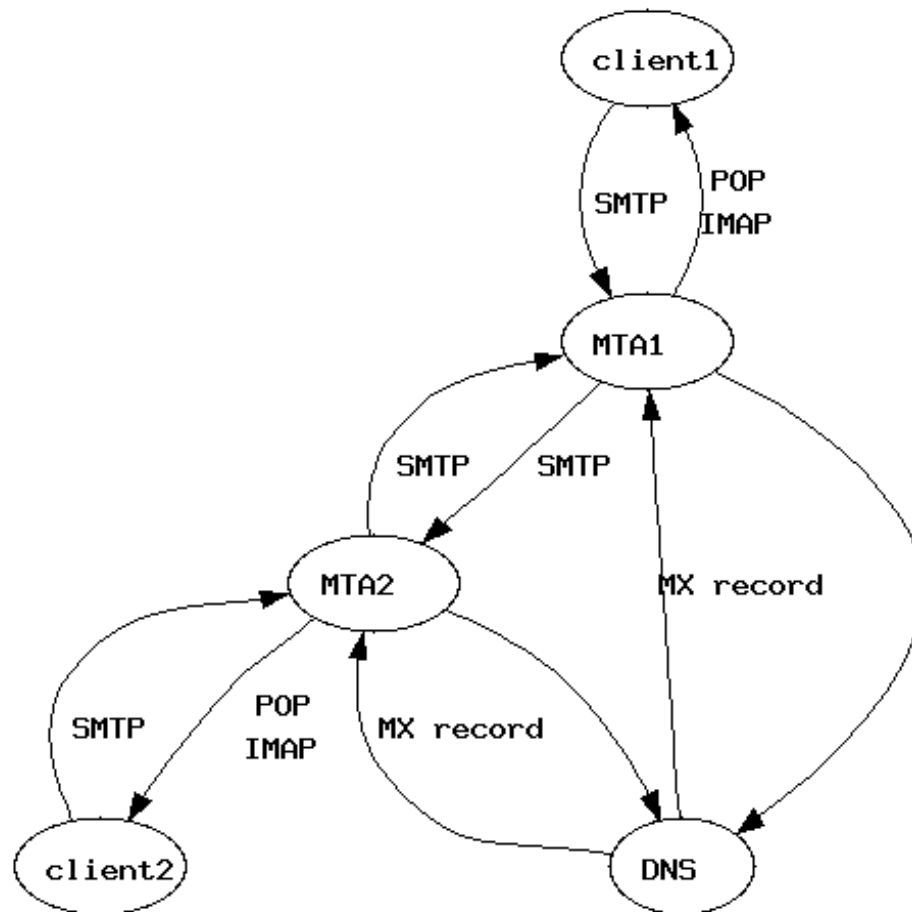
# Mail

AAU  
15 marts 2006

Karsten Thygesen  
CTO, Partner, Netic A/S  
karthy@netic.dk

- 1971: Ray Tomlinson invented SENDMSG and READMAIL for Arpanet. Used the [user@host](#) addressing.
- 1977: RFC733 unions various email formats
- 1982: RFC822 revised version of RFC733
- 1982: Relaying done with UUCP
- 1984: Eric Allman invented sendmail
- 1993: AOL connected their mail to the Internet
- 2000: Spam becomes a threat to email

- Open Standards makes the Internet tick
- System Administration is all about knowing the fundamental protocols
- Study Standards, then products!



```
; <<>> DiG 9.3.0 <<>> karthy.net mx
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61523
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;karthy.net.          IN  MX

;; ANSWER SECTION:
karthy.net.          42658 IN  MX 20 mail-relay.tele2adsl.dk.
karthy.net.          42658 IN  MX 10 mail.karthy.net.

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Apr 19 13:31:06 2005
;; MSG SIZE rcvd: 83
```

- RFC 821 - Simple Mail Transfer Protocol
  - Obsoleted by RFC2821 - Simple Mail Transfer Protocol
  - How MTA's exchange messages
- RFC 822 - Standard for the format of ARPA Internet text messages
  - obsoleted by RFC2822 - Internet Message Format
  - What a message looks like

RFC821  
Simple Mail Transfer Protocol

```
karthy@karthyws$ telnet mail.netic.dk 25
Connected to mail.netic.dk.
Escape character is '^]'.
220 netic.dk ESMTP
ehlo karthyws.netic.dk
250-netic.dk
250-STARTTLS
250-PIPELINING
250-8BITMIME
250 AUTH LOGIN PLAIN CRAM-MD5
mail from:<karthy@netic.dk>
250 ok
rcpt to:<karthy@karthy.net>
250 ok
data
354 go ahead
From: Karsten Thygesen <karthy@netic.dk>

Here is a mail...
.
250 ok 1113913050 qpp 15175
quit
221 netic.dk
Connection closed by foreign host.
```

Sending  
Receiving



```
karthy@karthyws$ telnet mail.netic.dk 25
Connected to mail.netic.dk.
Escape character is '^]'.
220 netic.dk ESMTP
ehlo karthyws.netic.dk
250-netic.dk
250-STARTTLS
250-PIPELINING
250-8BITMIME
250 AUTH LOGIN PLAIN CRAM-MD5
mail from:<karthy@netic.dk>
250 ok
rcpt to:<karthy@karthy.net>
250 ok
data
354 go ahead
From: Karsten Thygesen <karthy@netic.dk>
```

Here is a mail...

```
.
250 ok 1113913050 qp 15175
quit
221 netic.dk
Connection closed by foreign host.
```

Only codes matters  
Text is for humans  
All defined in RFC821

220 <domain> Service Ready  
221 <domain> Service closing  
transmission channel  
250 Requested mail action ok,  
completed  
354 Start mail input; end with  
<CRLF>.<CRLF>

First digit:  
1-3: success  
4: temp. negative  
5: failure

- Use EHLO instead of HELO
- Server will answer with list of extensions
- If the server gives a failure, the client must revert to HELO
- Defined in RFC1651 (EHLO), RFC1652 (8BITMIME), RFC1653 (SIZE)

# RFC822

## Email Headers

```
X-Gmail-Received: 78a3a1844aa57e94f797d0dcc2eab0667426acea
Delivered-To: karthy@gmail.com
Received: by 10.39.2.25 with SMTP id e25cs10291rni;
      Wed, 20 Apr 2005 00:50:40 -0700 (PDT)
Received: by 10.38.125.1 with SMTP id x1mr725496rnc;
      Wed, 20 Apr 2005 00:50:40 -0700 (PDT)
Return-Path: <hosthist@dk-hostmaster.dk>
Received: from netic.dk (goto.netic.dk [192.38.202.205])
      by mx.gmail.com with ESMTP id 71si1598305rnc.2005.04.20.00.50.38;
      Wed, 20 Apr 2005 00:50:40 -0700 (PDT)
Received-SPF: fail (gmail.com: domain of hosthist@dk-hostmaster.dk does not
designate 192.38.202.205 as permitted sender)
Received: (qmail 338 invoked by uid 1099); 20 Apr 2005 07:50:38 -0000
Received: from 83.72.2.91 by goto (envelope-from <hosthist@dk-
hostmaster.dk>, uid 89) with qmail-scanner-1.23
      (clamscan: 0.80. spamassassin: 3.0.2.
      Clear:RC:1(83.72.2.91):.
      Processed in 0.023527 secs); 20 Apr 2005 07:50:38 -0000
Received: from 83.72.2.91.ip.tele2adsl.dk (HELO karthy.net) (83.72.2.91)
      by netic.dk with (DHE-RSA-AES256-SHA encrypted) SMTP; 20 Apr 2005
07:50:38 -0000
```

```
Received: (qmail 30220 invoked by uid 1000); 20 Apr 2005 09:49:52 +0200
Delivered-To: karthy@karthy.net
Received: (qmail 30212 invoked from network); 20 Apr 2005 09:49:51 +0200
Received: from fitch5.uni2.net (130.227.212.5)
  by 192.168.0.2 with SMTP; 20 Apr 2005 09:49:51 +0200
Received: from tornado.dk-hostmaster.dk (tornado.dk-hostmaster.dk
 [193.163.102.19])
  by fitch5.uni2.net (Postfix) with ESMTP id 1ACBFD1743
  for <karthy@karthy.net>; Wed, 20 Apr 2005 09:50:36 +0200 (CEST)
Received: by tornado.dk-hostmaster.dk (Postfix, from userid 5001)
  id B8EBFC10; Wed, 20 Apr 2005 09:50:05 +0200 (CEST)
To: karthy@karthy.net
Subject: Onlinebetaling gennemført
From: DK Hostmaster A/S <info@dk-hostmaster.dk>
Mime-Version: 1.0
Content-type: text/plain; charset=iso-8859-1
Message-Id: <20050420075005.B8EBFC10@tornado.dk-hostmaster.dk>
Date: Wed, 20 Apr 2005 09:50:05 +0200 (CEST)
```

- Some mailers check to see that the domain name in the HELO matches the reverse DNS entry

HELO

DNS

```
Received: from netic.dk (goto.netic.dk [192.38.202.205])  
by mx.gmail.com with ESMTTP id 71si1598305rnc.2005.04.20.00.50.38;  
Wed, 20 Apr 2005 00:50:40 -0700 (PDT)
```

- RFC1123 – Requirements for Internet Hosts – claims that mailers **MUST** accept the mail even if the HELO does not match DNS

- The Message-ID is optional but always used
- Crucial to detect mail loops
- No specified format, but must be unique
- Added by the handling (sending) server

- RFC1561, RFC1562 and *many* more
- MIME encapsulates arbitrary binary material so that it can be transferred over the Internet
- MIME labels identifies content types, so useragents can do clever stuff
- Uses BASE64 encoding



From: Karsten Thygesen <karthy@netic.dk>  
User-Agent: Mozilla Thunderbird 1.0.2 (X11/20050403)  
X-Accept-Language: en-us, en  
MIME-Version: 1.0  
To: karthy@gmail.com  
Subject: Attachment for class  
Content-Type: multipart/mixed;  
boundary="-----080300030102000500020108"

This is a multi-part message in MIME format.

-----080300030102000500020108  
Content-Type: text/plain; charset=ISO-8859-1; format=flowed  
Content-Transfer-Encoding: 7bit

Here is my vinum config file

-----080300030102000500020108  
Content-Type: text/plain;  
name="vinum.conf"  
Content-Transfer-Encoding: 7bit  
Content-Disposition: inline;  
filename="vinum.conf"

drive a device /dev/ad0s2g  
drive b device /dev/ad1s1e

-----080300030102000500020108--

- Encodes 8bit ISO-8859-1 text to 7bit
- Nickname: Quoted Unreadable :)
- ALL headers MUST be 7bit!

Subject: =?ISO-8859-1?Q?=F81\_og\_bl=E5\_tuborg\_til\_l=E6reren?='

- Offline (POP)
  - Mail is fetched by client and deleted from server
- Online (IMAP old model)
  - Mail is stored on server and client connects while reading mail
- Disconnected (IMAP as of today)
  - Mail is synchronized between server and (multiple) clients.
  - Can be read both online and offline

- POP and IMAP protocols are ONLY for reading mail
- Clients sends mail using SMTP
- Client must be configured with both a POP/IMAP server and a SMTP server

```
telnet mail.netic.dk pop3  
Trying 192.38.202.205...  
Connected to mail.netic.dk.  
Escape character is '^['.
```

```
+OK Hello there.
```

```
user what@about.dk
```

```
+OK Password required.
```

```
pass Brian
```

No security – cleartext password!

```
+OK logged in.
```

```
list
```

```
+OK POP3 clients that break here, they violate STD53.
```

```
1 2231
```

Message 1 occupies 2231 bytes

```
.
```

```
list 1
```

```
+OK 1 2231
```

```
stat
```

```
+OK 1 2231
```

Total mailboxsize is 1 mail and 2231 bytes

```
quit
```

```
+OK Bye-bye.
```

```
Connection closed by foreign host.
```

- Invented when security was no big deal
- APOP later added – challenge response
- POP over SSL/TLS
- Kerberos authentication (limited)
- Cleartext still most common authentication method!!

- Interactive Message Access Protocol
- Online, Offline, Disconnected mode
- Folders
- Better authentication (Kerberos and more!)
- Full MIME support (partial fetch)
- Multiple Servers
- Serverside sort
- Serverside search
- Access Control Lists (ACL)
- IMAP still not deployed by many ISPs due to storage, load and complexity

\* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE  
THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA  
IDLE ACL ACL2=UNION STARTTLS] Courier-IMAP ready. Copyright  
1998-2004 Double Precision, Inc. See COPYING for distribution information.

a login what@about.dk Brian

a OK LOGIN Ok.

a select inbox

\* FLAGS (\Draft \Answered \Flagged \Deleted \Seen \Recent)

\* OK [PERMANENTFLAGS (\* \Draft \Answered \Flagged \Deleted \Seen)]

Limited

\* 1 EXISTS

\* 1 RECENT

\* OK [UIDVALIDITY 1113998983] Ok

\* OK [MYRIGHTS "acdilrsw"] ACL

a OK [READ-WRITE] Ok





### c fetch 1 full

```
* 1 FETCH (FLAGS () INTERNALDATE "20-Apr-2005 13:46:45 +0200" RFC822.SIZE
2231 ENVELOPE ("Wed, 20 Apr 2005 13:46:37 +0200" "test" (("Karsten Thygesen" NIL
"karthy" "gmail.com"))) (("Karsten Thygesen" NIL "karthy" "gmail.com"))) ((NIL NIL
"karthy" "karthy.net"))) ((NIL NIL "what" "about.dk"))) NIL NIL NIL
"<35b813da05042004465dcfcde6@mail.gmail.com>") BODY (("text" "plain" ("charset"
"iso-8859-1") NIL
NIL "quoted-printable" 33 3)("text" "html" ("charset" "iso-8859-1") NIL NIL "quoted-
printable" 45 3) "alternative"))
c OK FETCH completed.
```

### d fetch 1 body

```
* 1 FETCH (BODY (("text" "plain" ("charset" "iso-8859-1") NIL NIL "quoted-printable" 33
3)("text" "html" ("charset" "iso-8859-1") NIL NIL "quoted-printable" 45
3) "alternative"))
d OK FETCH completed.
```

- Open relays abused by spammers
- Relay for your own users only
  - Based on IP segments (local nets)
  - Based on relay-after-pop
  - Based on ASMTTP – authenticated SMTP(RFC2554)
- ORDB.org lists open relays
- Many ISP blocks port 25!
- SPF will potentially limit relaying

- Defined in RFC2554
- Recommended for all ISP to implement (RFC3013 Nov 2000)

```
S: 220 smtp.example.com ESMTP server ready
C: EHLO jgm.example.com
S: 250-smtp.example.com
S: 250 AUTH CRAM-MD5 DIGEST-MD5
C: AUTH CRAM-MD5
S: 334
PENCeUxFREJoU0NnbmhNWitOMjNGNndAZWx3b29kLmlubm9zb2Z0ImNvbT4=
C: ZnJlZCA5ZTk1YWVlMDljNDBhZjJiODRhMGM5YjNiYmFlNzg2ZQ==
S: 235 Authentication successful.
```

- Currently 75% of all mail is spam
- Only longterm effective weapon is prohibition by law!

### Jeremy Jaynes Gets 9 Years for Spamming

Spammer Jeremy Jaynes, who operated using the alias 'Gaven Stubberfield' and was listed by Spamhaus as the 8th most prolific spammer in the world, has been convicted of spamming using deceptive routing information to hide the source. A Virginia court recommended Jaynes spend **nine years** in prison for sending hundreds of thousands of unsolicited bulk emails.

- DNS checks (can we return a mail?)
- Realtime Blocking Lists (RBL)
  - Blocks known open relays, known spammers
- Signature matching (Razor)
  - Compares hash of content to database of know spam
- Heuristics (Spamassassin)
  - Scoring based on pattern matching
- Neural networks (DSPAM, Many)
- SPF – Sender Policy Framework

- No single method finds all spam
- Scoring over multiple methods necessary
- Spammers gets more clever – so does the tools.
- The problem with false positives
  - How to migrate backward in the toolchain?
- The danish law prohibits deletion of spam!
  - Tagging, folders, web interfaces

How many ways can you spell Viagra?

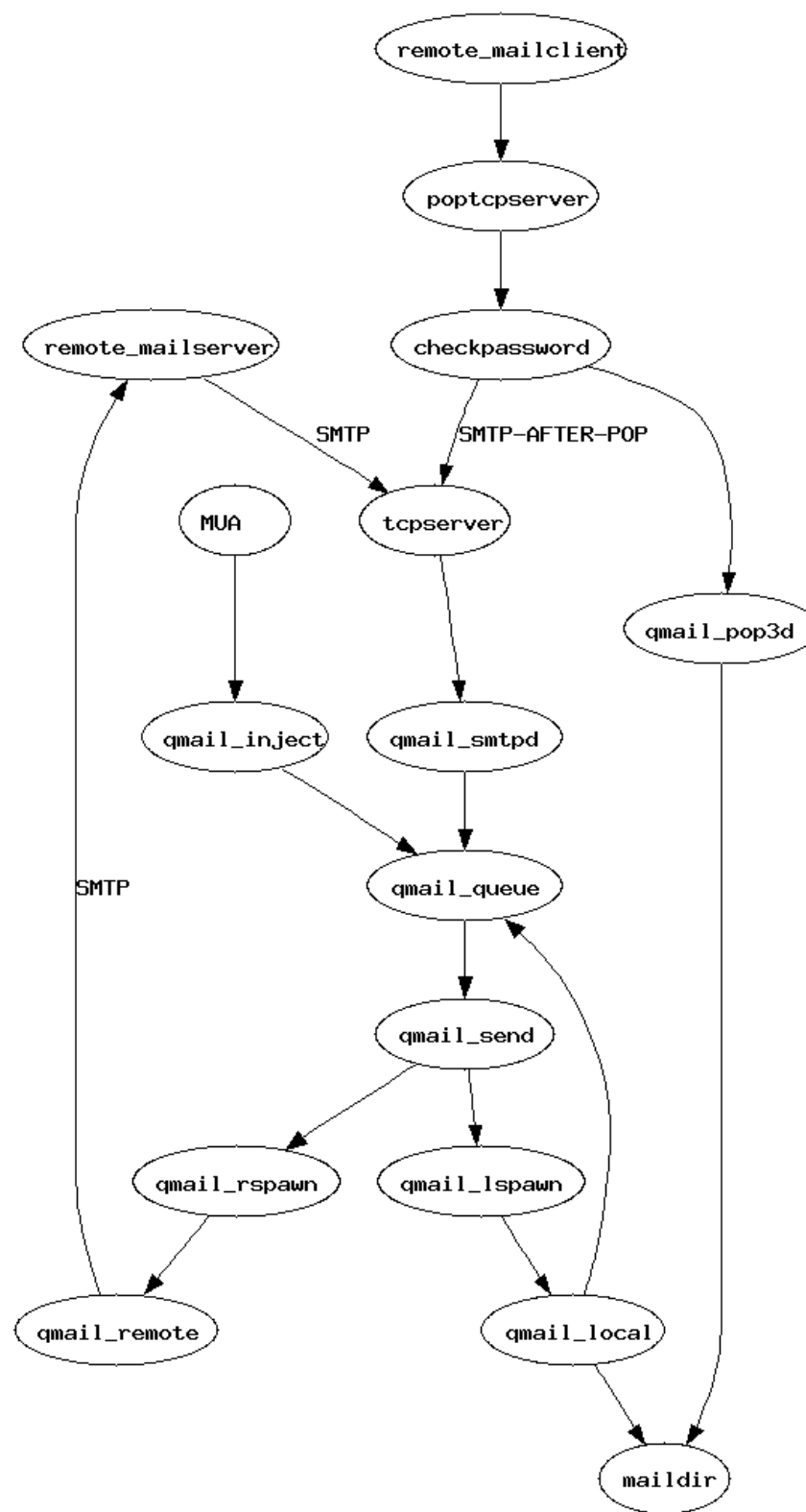
- SPF allows the owner of an Internet domain to use special DNS records to specify which machines are authorized to transmit e-mail for that domain
- example.org. IN TXT "v=spf1 a mx -all"
- Supported by Amazon, AOL, EBay, Google, GMX, Hotmail, W3C and Netic :-)
- Nov 2005: 1.700.000 domains publish SPF records
- RFC early 2006

- Easy (relative) and fairly reliable to catch
- Must keep signature database current
- Danish law allows deletion
- Potential very dangerous
  - Full or partial destruction of systems
  - Service Interruptions
  - Privacy disclosures
  - Global Internet Shutdown

One firm estimates that the projected damage from the two Code Red viruses has risen to more than US\$2 billion -- and is mounting at the rate of \$200 million per day. (aug 2001)

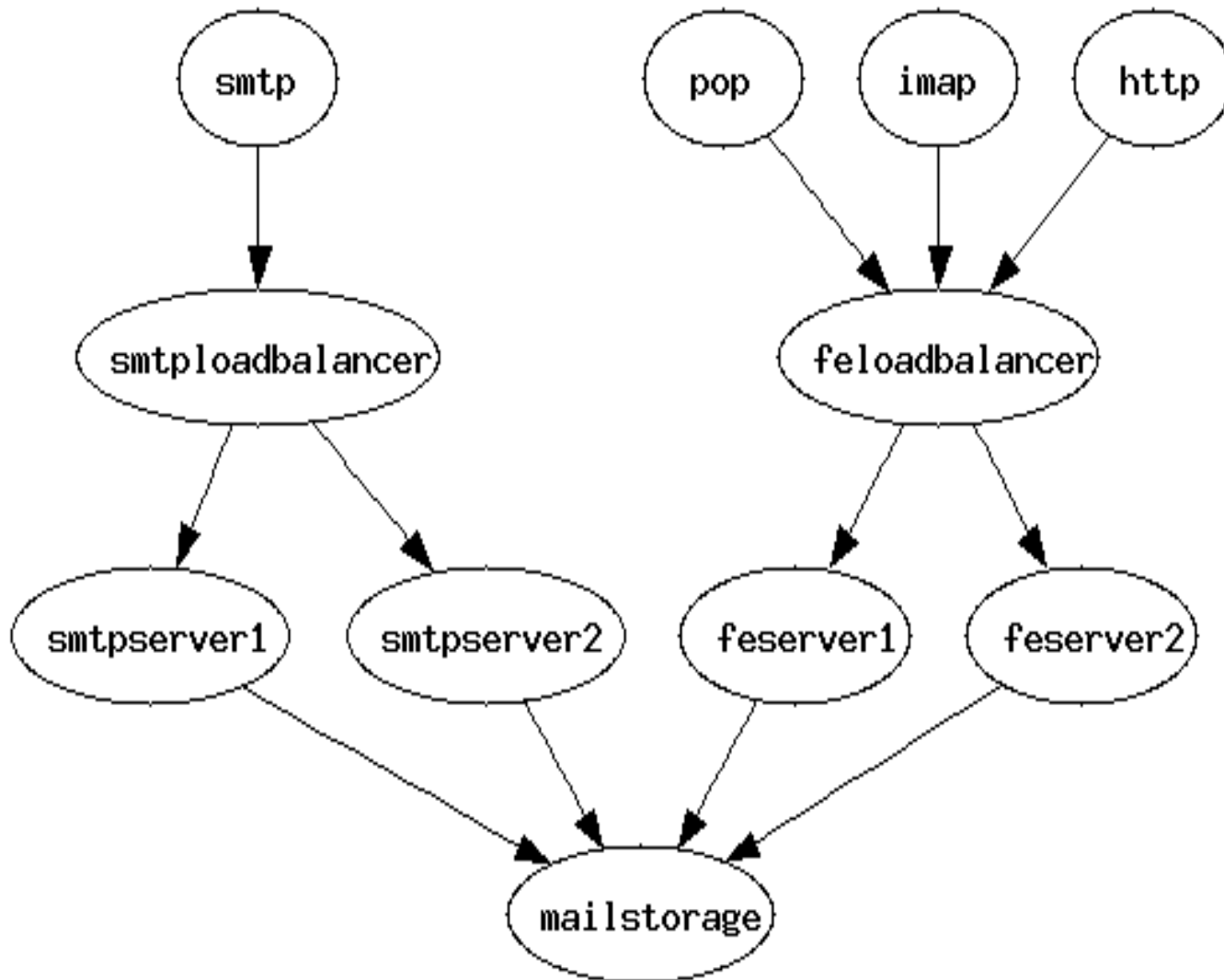






- Do log rotation based on size – not time!
- Spam and Virus requires daily maintenance
- “suspected” False Positive spam is a problem
- Expect user to go crazy
  - Plan for zillions of mail/day
  - Expect users to mail a copy of their harddisk
  - Do effective monitoring
    - full partitions
    - Queue size
    - Mail flow (both too much and too little)
    - Enforce quotas
- Adhere to standard! Do not blackhole mail!

- Most basic mail software is pretty secure (latest qmail is from 1998 – bounty since 1997)
- Webmail (particularly PHP based) have many problems
- Do security segmentation (users and vservers)
- Plan for DOS
  - Limit number of incoming connections both SMTP and POP/IMAP
  - Limit connection time
  - Do tar pitting on illegal users
  - Check for users existence during SMTP
- Be careful when handling virus!



- Qmail (vpopmail, netqmail etc)
- Exim
- Postfix
- Sendmail
- Iplanet
- Gmail, Hotmail, yahoo
- Oracle Collaboration Suite (unified mail)
- MS Exchange
- Lotus Notes
- Cc mail
- Suse

?

- <http://www.faqs.org/rfcs/> (RFCS)
- <http://www.spamhaus.org> - news on spam
- <https://spam.abuse.net> – clearinghouse, RBL
- <http://cr.yp.to> - qmail
-

- Browse the referred RFC's (especially RFC821, RFC822)
- Send a mail to your self or [what@about.dk](mailto:what@about.dk) (passwd: Brian) using only telnet
- Send a mail to your self using mail.netic.dk as mailservier. Relay problems?
- Read the same mail using only telnet
  - Using the POP3 protocol
  - Using the IMAP4 protocol
  - Read and understand the headers you see!



- Send a mail with a binary attachment (using your favorite email program) and study the raw mail (perhaps fetch it using telnet)
- Try authenticated SMTP to mail.netic.dk – perhaps port 1025 if port 25 is blocked