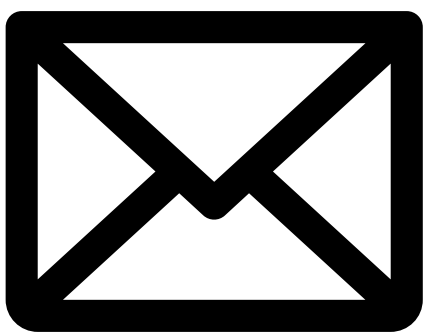

Mailservers

RFC 724

12 May 1977

“Proposed Official Standard for the Format of ARPA Network Messages”

> Messages are expected to consist of lines of text.

Message -> information in rigid format, followed by main part of message

'main part': text, format not specified

```
From: NOREPLY@example.com
To: recipient@example.com
Subject: ehlo

Hello World!
```

SMTP

September 1980: first drafts for Mail Transfer Protocol

By november 1981: RFC for Simple Mail Transfer Protocol

```
$> telnet httpforever.com 80
Trying 2604:a880:4:1d0::1f1:2000...
Connected to httpforever.com.
Escape character is '^]'.
GET /                                          <- HTTP GET
<!DOCTYPE HTML>
<html>
  <head>
    <title>HTTP Forever</title>
    [...]
</html>
```

```
$> telnet smtp.google.com 25
Trying 74.125.143.26...
Connected to smtp.google.com.
Escape character is '^]'.
220 mx.google.com ESMTP a640c23a62f3a-ae6e7e8c3d8si992696466b.58 - gsmtp
EHLO hifrombornhack.dk                                  <- EHLO command
250-mx.google.com at your service, [95.171.163.95]      <- response
250-SIZE 157286400
250-8BITMIME
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-CHUNKING
250 SMTPUTF8                                            <- until here
^]
telnet> quit
Connection closed.
```

```
$> openssl s_client -quiet -starttls smtp -connect 127.0.0.1:587
Connecting to 127.0.0.1
Can't use SSL_get_servername
depth=2 C=US, O=Internet Security Research Group, CN=ISRG Root X1
verify return:1
depth=1 C=US, O=Let's Encrypt, CN=E6
verify return:1
depth=0 CN=jappie.dev
verify return:1
250 CHUNKING
EHLO jappie.dev
250-PIPELINING
250-SIZE 10240000
250-ETRN
250-AUTH PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
```

```
AUTH PLAIN [...]                    // echo -ne "\0username\0password" | base64
235 2.7.0 Authentication successful
MAIL FROM: NOREPLY@jappie.dev       // path 'back' to the sender, later used w/ SPF
250 2.1.0 Ok
RCPT TO: j@jappie.dev               // destination SMTP server
250 2.1.5 Ok
DATA                                // IMF, RFC5322
354 End data with <CR><LF>.<CR><LF>
From: NOREPLY@jappie.dev
To: j@jappie.dev
Subject: EHLO

EHLO from Bornhack!

.                                   // <CRLF>.<CRLF>
250 2.0.0 Ok: queued as C986349BC8
QUIT
221 2.0.0 Bye
```

- MTA -> message transfer agent
  - port 25
- MSA -> message submission agent
  - port 587 (or 465) (and historically maybe 25)
- MDA -> message delivery agent
  - POP: 110, with TLS: 995
  - IMAP: 143, with TLS: 993

MTA

- Postfix, Exim, etc.
- Usually functions as MSA too
- Port 25, 587 & 465
- Used when sending & receiving mail
- Milters: mail filters, i.e. DKIM signing, spam filtering (e.g. rspamd), etc.

MDA

- Stores user's mail
- Dovecot, Courier, Cyrus, etc.
- Queried for new mail when you open your mailbox
  - IMAP (143), IMAPS (993), POP3 (110), POP3S (995)
- LMTP, maildrop, etc. to receive mail from MTA
- Sieve scripts: sorting mail into folders & applying tags
  - https://thsmi.github.io/sieve-demo/libSieve/SieveGui.html

```
require ["variables", "fileinto", "regex", "envelope", "subaddress", "mailbox", "enotify"];

if envelope :detail :matches "to" "*" {
  set :lower "subaddress" "''${1}";
  if envelope :user :matches "to" "*" {
    set "name" "''${1}";
  }
  if envelope :domain :matches "to" "*" {
    set "domain" "''${1}";
  }
  if mailboxexists "INBOX.''${subaddress}" {
      fileinto "INBOX.''${subaddress}";
      stop;
  } else {
      fileinto :create "INBOX.''${subaddress}";
      notify :message "Folder INBOX.''${subaddress} was just created" "mailto:''${name}@''${domain}";
      stop;
  }
}

keep;
```

MUA

- The email client on your device
- Uses IMAP (or POP3) to query MDA for mail
- Uses SMTP to submit mail to MSA (MTA)

DNS

- MX -> specifies mail server
- DKIM -> mail signing
  - `v=DKIM1; h=sha512:sha256; k=rsa; p=MIG[...]AQAB;`
- SPF -> list of mail servers that are allowed to send
  - `MAIL FROM:`
  - `v=spf1 mx -all`
- DMARC -> what to do with mail after checking SPF & DKIM
  - quarantine, reject, deliver
  - how to check `From:` field in `Data`
  - `v=DMARC1; p=quarantine; adkim=s; aspf=s; fo=1; pct=100; rf=afrf; ri=86400; rua=mailto:postmaster@jappie.dev; ruf=jasper@jappie.dev; sp=reject;`

My setup:

- Postfix
- Dovecot
  - Pigeonhole for Sieve support
  - Handles authentication via SASL
- NixOS!

- outlook, google, local ISP, etc.
- 5 months -> no spam
- lucky IP? (mxtoolbox.com/blacklists.aspx)

So, should you?

EOM

My NixOS config: https://app.radicle.xyz/nodes/git.jappie.dev/rad:z4HEZGDPknT12W4fuXc6wM3HtYTf2/tree/hosts/Flugel/services/mail.nix