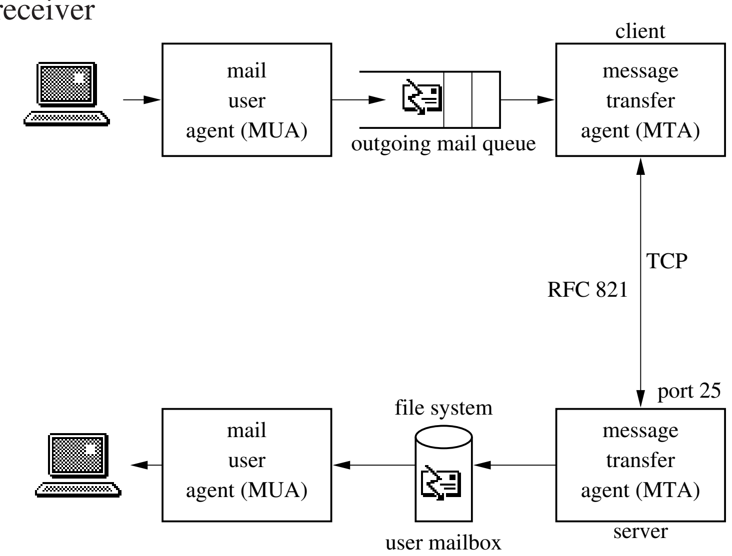
Electronic Mail: SMTP

Electronic mail

Asynchronous exchange of data – sender does not know when (if) data reaches receiver



Email by example

You can do this via telnet to port 25 (server says) :

```
220 ceres.fokus.gmd.de PP Here - Pleased to meet you
HELO lupus.fokus.gmd.de
250 ceres.fokus.gmd.de:  lupus.fokus.gmd.de looks good to me
MAIL From:  Bill Clinton <clinton@whitehouse.gov>
250 OK
RCPT To:  hgs@fokus.gmd.de
250 Recipient OK.
DATA
354 Enter Mail, end by a line with only '.'
To:  hgs
From:  Bill Clinton <clinton@whitehouse.gov>
Subject:  Your new job
Date:  Wed, 24 Jan 96 11:49:58 EST


Welcome to your new job as chief of staff.
.
250 Submitted, queued (msg.01721-0)
```

GMD fokus

```
QUIT
221-ceres.fokus.gmd.de says goodbye to lupus.fokus.gmd.de
221 at Wed Jan 24 19:40:05.
```

- MTA retries until success (usually 4-5 days)
- may be several hops (relay agents), e.g., one for whole company relays to department

GMD fokus

The mail as received

```
Return-path: <clinton@whitehouse.gov>
Delivery-date: Wed, 24 Jan 1996 19:40:00 +0100
Received: from lupus.fokus.gmd.de by ceres.fokus.gmd.de
  with SMTP (PP-ICR1v5); Wed, 24 Jan 1996 19:39:23 +0100
To: schulzrinne@fokus.gmd.de
From: Bill Clinton <clinton@whitehouse.gov>
Subject: Your new job
Message-Id: <199601241649.LAA06306@ceres.fokus.gmd.de>
Date: Wed, 24 Jan 96 11:49:58 EST

Welcome to your new job as chief of staff.
```

Don't try this at home!

GMD fokus

SMTP Commands: RFC 821

Similar to FTP: client issues commands and server replies with number/text.

HELO *client-host* introduce client host

MAIL FROM *origin* mail originator

RCPT TO *destination* mail destination (may be repeated)

DATA data follows until single dot

EXPN *name* expand aliases

NOOP do nothing, but return 250

VRFY *name* verify addresses

RSET reset state

QUIT done

Order is important!

GMD fokus

Email addresses: RFC 822

- `doe@host.domain`
- `John Doe <doe@host.domain>`
- `doe@host.domain (John Doe)`
- `group: user1, user2;`
- not: `user1, user2`

The components of a message

envelope: used by MTA for delivery

Headers: used by MUA for display (RFC 822), followed by blank line

Body: lines of text (< 1000 NVT bytes each)

Content = headers + body

Common mail headers

NVT ASCII, may be continued across lines

To: destination

From: "logical" source of mail

Sender: "physical" source of mail (secretary)

Message-Id: MTA identifies outgoing message (for replies)

Date: Wed, 24 Jan 1996 17:51:14 +0100

Subject: what the mail is about

In-reply-to: message id

Trace path of message:

```
Received: from ns.gte.com by ceres.fokus.gmd.de
   with SMTP (PP-ICR1v5); Wed, 24 Jan 1996 17:31:07 +0100
```


DNS MX records

- Use `company.com` rather than `host.company.com`
- Several mail hosts for reliability or load sharing

```
host -a -v -t mx sun.com
Query done, 3 answers, authoritative status: no error
sun.com     86400 IN MX 10 mercury.Sun.COM
sun.com     86400 IN MX 20 venus.Sun.COM
sun.com     86400 IN MX 30 Sun.COM
Additional information:
mercury.Sun.COM 86400 IN A 192.9.25.1
venus.Sun.COM   86400 IN A 192.9.25.5
Sun.COM         86400 IN A 192.9.9.1
```

Extended SMTP

- use `EHLO` instead of `HELO`
- SIZE command: provide size ahead of time ($\leftrightarrow$ failing after 10 MB)
- 8-bit transport ➠ shorter messages
- negotiate capabilities

MIME

- transport binary data as lines of NVT
- structured mail with several body parts (attachments)
- multipart mixed, parallel, digest, alternative
- Internet media types: text, image, audio, video, application, …
- uses local definition (mailcap file) to render
- also allows external definitions (ftp)

MIME example

```
Mime-Version: 1.0
Content-Type: multipart/mixed;
              boundary="PART-BOUNDARY=.19512211143.ZM4824.esp10"

--PART-BOUNDARY=.19512211143.ZM4824.esp10
Content-Type: text/plain; charset=us-ascii

--PART-BOUNDARY=.19512211143.ZM4824.esp10
Content-Description: JPEG Image
Content-Type: image/jpeg ; name="sclaus.jpg"
Content-Transfer-Encoding: base64
```


/9j/4AAQSkZJRgABAQAAAQABAAD/2wBDAAgGBgcGBQgHBwcJCQgKDBQNDAsLDBkSEw8UHRof
Hh0aHBwgJC4nICIsIxwcKDcpLDAxNDQ0Hyc5PTgyPC4zNDL/2wBDAQkJCQwLDBgNDRgyIRwh

Email security: PGP

- no authentication (see example), no privacy
- shared secret (symmetric): same key, different for each pair ➠ doesn’t scale
- public key cryptography (asymmetric): use private key to encrypt, public key to decrypt
- anybody can generate public/private key pair
- web of trust: is the key signed by person I trust?