Announcements

- **Reading**
  - Today: 7.6 (up to 7.6.3)

- **Projects**
  - must submit project tar file by Wed May 14 at 9:00 AM
  - project demos will be Wed 5/14
    - must prepare a short/informal report that describes what has been implemented (and by whom)
  - project demo signups were taken
Transferring Messages

- **SMTP Agents** listen on TCP port 25
- **Protocol** consists of a series of 4 character commands
  - HELO: exchange identity
  - MAIL FROM: indicate origin of mail
  - RCPT TO: destination for mail
  - DATA: start of mail message (envelop and body)
  - QUIT: end of mail message

- **Email gateways**
  - Still many other mail systems out there
    - may use other formats
  - May want only a limited number of “public” mail servers
    - provides application level firewalls
    - hides interior topology of network
Pretty Good Privacy: PGP

- Developed by a single person
  - uses RSA, IDEA, and MD5
- Provides: privacy, compression, and digital signatures
- Has a collection of key servers for public key registration
- Uses three different key lengths (384, 512, and 1024 bits)

---

From: Computer Networks, 3rd Ed. by Andrew S. Tanenbaum, (c)1996 Prentice Hall.
Privacy Enhanced Email (PEM)

- Internet Standard
- Uses MD5 for hashing and DES for encryption
- Key Management:
  - collection of certificate authorities
  - authorities are certified by Policy Certificate Authorities
    • define policies to be followed by certificate authorities
  - PCAs are certified by Internet Policy Registration Authority
News

- **Large Collection of newsgroups**
  - currently a hierarchical namespace (used to be rather flat)
  - can be moderated: must be approved before being posted

- **Messages**
  - have a unique id
  - are associated with one or more newsgroups
  - contain a superset of RFC822 fields

- **Transport of news**
  - a site a list of one or more sites it gets is newsfeed from
    - a site periodically polls its newsfeeds for news
    - newsfeeds can also push new news out
  - **UUCP: Unix-to-Unix CoPy**
    - historical path using dialup modems
  - **NNTP: Net News Transfer Protocol (TCP port 119)**
NNTP

• Provides end-users with news (ala POP for email)
  – LIST and NEWSGROUPS commands
  – GROUP: list all articles in a group
  – NEWNEWS: all news since a specific time
  – ARTICLE: give me a specific article
    • note that this is done by id, not local number
  – POST: post a news article

• Supports moving news between servers
  – all commands from above plus..
  – IHAVE: supports flooding articles around the net

• Performance Problem
  – almost a gigabyte per day of news
  – protocol is stop and wait (limited for round-trip latency)
Naming in the World Wide Web

- **Uniform resource locator**
  - a single namespace for all objects on the Internet

- `<protocol>://<dns name>:<port>/<page reference>`
  - protocol: http, ftp, gopher, wais, file, news
  - port: optional - defaults to well known port for protocol
  - dns name: often an alias for a host name
    - also can be an IP address
    - use of www.* is a convention for naming an org’s web host but there is nothing special about this name
  - page reference: usually a file path name
    - servers can define default translations
      - default file suffix (e.g. .html)
      - default page for a directory: index.html
      - ~ to expand to a user’s home page