Servizi di E-mail

- Primo e-mail: nel 1971 su Arpanet
- Primo e-mail presidenziale: Clinton 2/3/93
- applicazioni per e-mail: mailers
  - Eudora, Outlook…(windows)
  - elm, pine…(linux, unix)
  - funzioni incorporate nei browser:
    - Netscape
    - Explorer...

Struttura di un messaggio e-mail

- Message header
- From *i.csci.unt.edu Sat Sep 18 21:25:48 1999
- Received: from Mercury.unix.acs.cc.unt.edu (mercury.acs.unt.edu [129.120.220.1])
- by CS.UniBO.IT (8.9.0/8.9.0) with ESMTP id VAA25584;
- Sat, 18 Sep 1999 21:25:46 +0200 (MET DST)
- Date: Sat, 18 Sep 1999 14:25:35 -0500 (CDT)
- From: *@silo.csci.unt.edu>
- To: bononi@cs.unibo.it
- Subject: URGENT
- Message-ID: <Pine.BSF.4.05.9909181425140.4760-100000@gab525i.csci.unt.edu>
- MIME-Version: 1.0
- Content-Type: TEXT/PLAIN; charset=US-ASCII
- Status: OR
- Message body
- Dear Luciano …..

Indirizzo di e-mail

- Nomeutente@dominio
  - es bononi@cs.unibo.it
    - bononi = login name
    - cs.unibo.it = indirizzo IP del mail-server
- Alias: nomi per insiemi di utenti
- nick-name: pseudonimo
- mailing list: forum per condivisione e-mail

Mailbox: Inbox e Received

- Inbox contiene i messaggi non ancora letti
- il mailer di solito presenta automaticamente il contenuto di Inbox.
- Alcuni programmi richiedono l'apertura esplicita di Inbox per vedere se ci sono nuovi messaggi
- Received: può contenere i messaggi letti se non diversamente specificato

Mailbox: Inbox (2)

- Presentazione contenuto inbox:
  - 1 Feb 19 Sajel K. Ds (253) Jpdc decision

– N2 Feb 19 Mark Whiery (236) Momuc99
– O3 Jan 31 Tom Jacob (65) Thanks!!!

From: mittente del messaggio
Subject: titolo del messaggio (argomento o parola chiave)

- uscendo dal mailer: salvare o non salvare?
- Mailbox (folder) secondari

Spedire un e-mail

- Comando (pulsante) send (s)
  – **TO**: e-mail address del destinatario
  – **From**: automatico
  – **Subject**: parola chiave o argomento
  – **CC**: altri destinatari dello stesso messaggio
  – **composizione testo messaggio**
    - limitare a 65-70 char/linea
    - non eccedere nella lunghezza
    - attenzione all'ironia...

Rispondere a un e-mail

- Selezionare l'e-mail originale
- comando o pulsante REPLY (r)
  – To: automatico
  – From: automatico
  – Subject: Re: (subject precedente)
  – CC: altri nuovi destinatari
  – eventuale testo originale + nuovo testo

Re-inviare un e-mail

- Selezionare l'e-mail originale
- comando o pulsante Forward (f)
  – To: nuovo destinatario
  – From: automatico
  – Subject: Fw: (subject precedente)
  – CC: altri nuovi destinatari
  – eventuale testo originale + nuovo testo

E-mail netiquette

- non URLARE...
- non avviare flames, spamming, bombing
- rendere l'ironia esplicita (emoticons) :-) ;-)
- inserire sempre il subject

- non scrivere messaggi troppo lunghi
- attenzione alle confidenze (forward)
- curare la grammatica e la sintassi

E-mail: non solo testo

- Mail attachment: formati bin --> ascii
  - bin -> **uuencode** -> ascii -> **uudecode** -> bin
  - MIME: Multipurpose Internet Mail Extensions
- comando: message, Attach document
  - immagini, suoni, video, documenti Word, Excel, e non ultimi…i VIRUS!!!
- Ricezione e interpretazione automatica

Abuso dell'e-mail

- Spamming: mandare e-mail a chiunque
- Bombing: sabotare la inbox di qualcuno
- Infection: spedire virus

- Reazioni:
  - avvisare i gestori del servizio
  - immettere filtri (procmail, ecc.)

Usenet (Newsgroups)

- BBS mondiale: >14000 forum (no profit)
- Online Services (profit): AOL, MSN
- Spazi e gruppi di discussione in rete:
  - open messages
  - moderati, non moderati, tecnici, culturali, ricreativi
- News reader (client) e News Server
  - articoli sottomessi e ricevuti in un unico archivio globale (follow-up e reply)
- Sottoscrivere (subscribe) un newsgroup…
- FAQ: frequently asked questions

Usenet (Newsgroups)

  - Es.
    - soc.colture.pakistan.history
    - soc.sexuality.spanking
    - talk.philosophy.metaphysics
    - unibo.cs.students
    - rec.travel.usa-canada

- italia.bologna.spettacolo
- it.fan.nutella
- it.cultura.filosofia
- it.comp.appl.macromedia

Napster e affini (filesharing)

– Creato nel 1999 da Shawn Fanning (19 anni) sta rivoluzionando il mercato musicale (filesharing)
– Applicazione che crea un unico file system condiviso su rete per condividere file MP3
– download di files mp3 direttamente dagli hard disk degli utenti collegati in rete
– Napster servers gestiscono le liste, che variano ora per ora a seconda degli utenti ON (ora si paga!)
– Macster (per mac) e Gnapster (open source code)
– RIAA vs Napster per copyright-infrangment sw, ma
  - gli MP3 non sono sul server e Napster è gratis
  - Napster è simile a tape recorder o masterizzatore (legali)

Napster e MP3

– MPEG audio layer 3, livello di compressione file audio (perceptual audio and psychoacoustic compression <--> Golden ears)
– frequency resolution 18 volte quella di layer 2
– CD stereo (bit rate 1411.2 Kb/s diviso fattore 12)
– MP3: 112-128 Kb/s senza perdere di qualità
– Rende possibile scaricare musica in tempo reale da Internet, e anche da casa (ISDN)
– il padre è Leonardo Chiariglione (CSELT Torino)
– in rete ci sono tutte le notizie: cercatele!

GNU e gnutella

– GNU: *GNU's not UNIX:* produzione di SW non proprietario (FSF free sw foundation)
– tutti possono scaricare modificare e re-distribuire GNU sw, purchè non limitino ulteriore distribuzione
– idea nata nel 1983 al MIT (Richard Stallman)
– Linux deve molto a GNU (ma sono cose diverse)
– GNUtella: rete peer-to-peer per condivisione sw (piratato e non)
– è un applicazione: non ha un server, non ha un responsabile… con chi se la prendono?
– Altri: Newtella, OpenNapster, FreeNet, ecc.

FTP: file transfer protocol

- Veicolo per trasferire file tra host diversi
- protocollo ftp-client/ftp-server
- upload: da host locale a host remoto (put)
- download: da host remoto a host locale (get)
- FTP server: mantiene una FTP directory
- FTP anonimo e FTP con registrazione
- es. ftp://www.cs.unibo.it/technicalreport/
  - viene mostrato il filesystem pubblico dell'host remoto

FTP: file transfer protocol (2)

- Text (ascii) and Binary files
- file utilities:
  - compressione/espansione
  - archivi: packing/extracting di insiemi di files
- freeware (shareware) files: gratis (temporaneo)
- ...solita attenzione ai Virus…
- per terminare: quit

Telnet

- Protocollo per controllo dell'accesso remoto
- login su host remoto: terminale client/server
  - telnet <indirizzo IP del terminale remoto>
  - login: nome di login
  - passwd:
- oppure mediante il browser:
  - telnet:// <URL del telnet gateway>
- settaggio del terminale virtuale

Altri servizi

- BBS (Bulletin Board System)
- MUD: multi-user domain (dungeon)
  - adventures, giochi di ruolo, mondi virtuali
  - arte e gioco (vedi URL)
- Internet Relay Chat: (IRC)
- per uscire: exit o ctrl-]

Sicurezza e privacy

- Crittografia: messaggi pubblici, ma non decifrabili senza la chiave
- Chiavi sicure: es. fattorizzazione di n. primi
  - es. PGP: pretty good privacy, semplice, efficace
  - encryption/decryption
  - **chiave pubblica (pubblicata)**: usata per criptare i messaggi diretti al suo proprietario
  - chiave privata (key security): usata per decriptare da parte del proprietario

Sicurezza e privacy

- RSA: fattorizzazione di numeri primi
- meccanismo di crittografia a chiave pubblica
- de-facto standard per Internet:
  - Internet explorer, Netscape navigator

Sicurezza e privacy

- DES: Data Encryption Standard
- meccanismo di crittografia a:
  - **chiave simmetrica**
  - una sola chiave condivisa per criptare/decriptare
  - Problema: condivisione sicura della chiave

Sicurezza e privacy

- Autenticazione delle parti e digital signature
- PKI: Public Key Infrastructure
- CA: Certification authority
- certificati digitali
  - rilasciati su richiesta del sender da CA
  - contengono chiave pubblica del sender e sono criptati dal CA.
- commercio elettronico
- pagamenti con carte di credito

Sicurezza e privacy

- Digital Signature: es. MD5
- hash function: funzione non invertibile
- cripta (testo -> hash -> valore numerico)
- permette di testare se il msg ha avuto modifiche -> garantisce ciò che si firma

Sicurezza e privacy

- Meccanismi di protezione per il sistema
- Firewall: per tagliare accessi su intranet
  - sniffing : annusare i pacchetti, ovvero leggere l'intestazione e agire di conseguenza
- Limitare i diritti utente
  - password, livelli di sicurezza
- Log file: accessi, aree dati protette

Protocolli sicuri

- SSL (***S**ecure **S**ockets **L**ayer)*, protocollo sviluppato da Netscape per trasferimento sicuro su Internet. SSL usa una chiave privata. Sia Netscape communicator che Internet Explorer supportano SSL, e molti siti web usano SSL per info confidenziali. Convenzione: le pagine web che usano SSL definiscono il protocollo *https:* invece di *http*:.

Protocolli sicuri

- Altro protocollo per trasmettere dati sicuri sul WWW: secure HTTP (S-HTTP). Mentre SSL crea una connessione sicura tra client e server, sulla quale posso trasmettere molti dati tutti sicuri, S-HTTP è progettato per trasmettere messaggi individuali in forma sicura. SSL e S-HTTP, possono essere visti come protocolli complementari.

Protocolli sicuri

- Le versioni sicure di Telnet e FTP
- Sono applicazioni scaricabili in rete:
  - esiste il sorgente in rete
  - attenzione a chi le fornisce!!!
- es. putty, ssl per Windows (telnet)
- es. pscp, scp per Windows (ftp)
- SSH: secure Shell: versione sicura di rlogin
  - è tutto criptato con RSA da passwd in poi.

Internet Service Provider

- Oggi molti sono gratuiti:
  - e-mail + spazio webpage + navigazione 24/7
  - banda non garantita

  - tariffa telefonica locale (...numero verde?)
- POP: Post office protocol (server) o IMAP
  - scarico e-mail senza connessione continua
- SMTP: Simple mail transfer protocol
  - invio e-mail da mail client a mail server
- Modem/ISDN per la connessione
  - 56Kb/s oppure 128 Kb/s

Internet Service Provider (2)

- Accedo specificando
  - numero telefonico del (pool di) modem
  - userid e password
- ottengo
  - indirizzo IP temporaneo per ricevere dati
  - indirizzo IP del DNS e default Gateway
- navigo…poi chiudo la connessione.

Motori di ricerca

- Altavista, Yahoo, infoseek, Excite, Lycos, google, raging,
- Virgilio, it.lycos ...
- Ricerca: parole chiave
- caratteri jolly: prefissi, postfissi, oper. logici
  - + parola necessaria, - parola da omettere
  - * qualsiasi testo
  - AND, OR

Motori di ricerca

- Es.
  - tutorial +HTML -fee edu*
- Elenco dei riferimenti (link) ordinati
- migliori riferimenti mostrati per primi
- raffinamento/generalizzazione della ricerca

Motori di ricerca

- Mirror site
- Guide in linea
- argomenti e attualità
- librerie virtuali
- ricerca persone su web

- yellow pages