

Lo strato Applicativo

EMAIL-SMTP

Reti di Calcolatori
AA. 2023-2024

Docente: Federica Paganelli
Dipartimento di Informatica
federica.paganelli@unipi.it

Posta elettronica

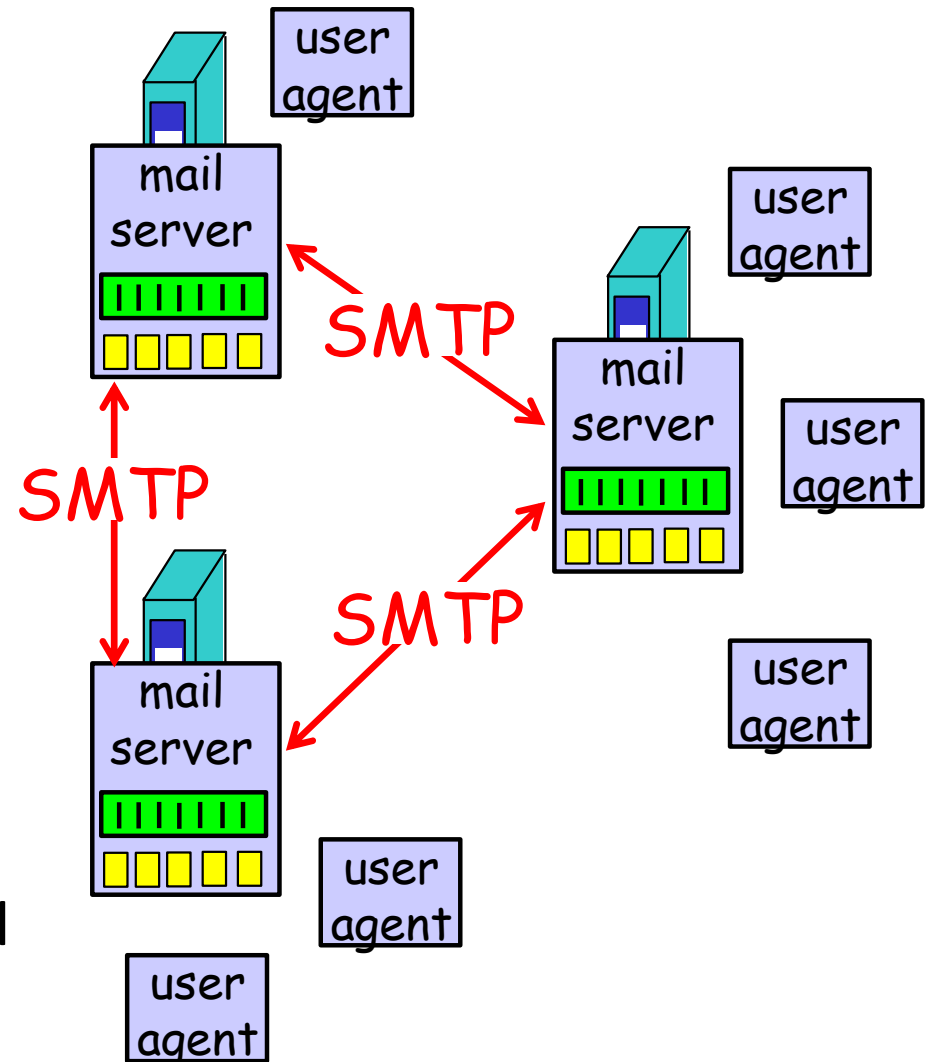
- Uno dei primi servizi applicativi di Internet (1982)
- Trasferimento di un messaggio tra uno user mittente e uno user destinatario
 - il destinatario potrebbe non essere in quel momento disponibile ad accettare messaggi di posta:
 - utente impegnato
 - computer spento
- Il servizio di posta elettronica si basa su componenti intermediari per trasferire i messaggi
 - Disaccoppiando lato mittente e destinatario
 - Analogia con posta tradizionale

Posta elettronica

 Coda msg
in uscita

■ user mailbox

- User agent
 - per la composizione, editing, lettura di messaggi di posta
 - es.: Eudora, Outlook, Thunderbird
- Mail server
 - i messaggi in entrata ed uscita vengono archiviati sul server
 - le mailbox (CASSETTE di POSTA) contengono messaggi in ingresso (che devono ancora essere letti) diretti all'utente
 - una coda di messaggi in uscita (che devono essere inviati)
- Protocollo SMTP: dialogo tra mail server
 - **“client”**: mail server che invia
 - **“server”**: mail server che riceve



Indirizzi email

- Un destinatario è identificato da un indirizzo email nella forma:

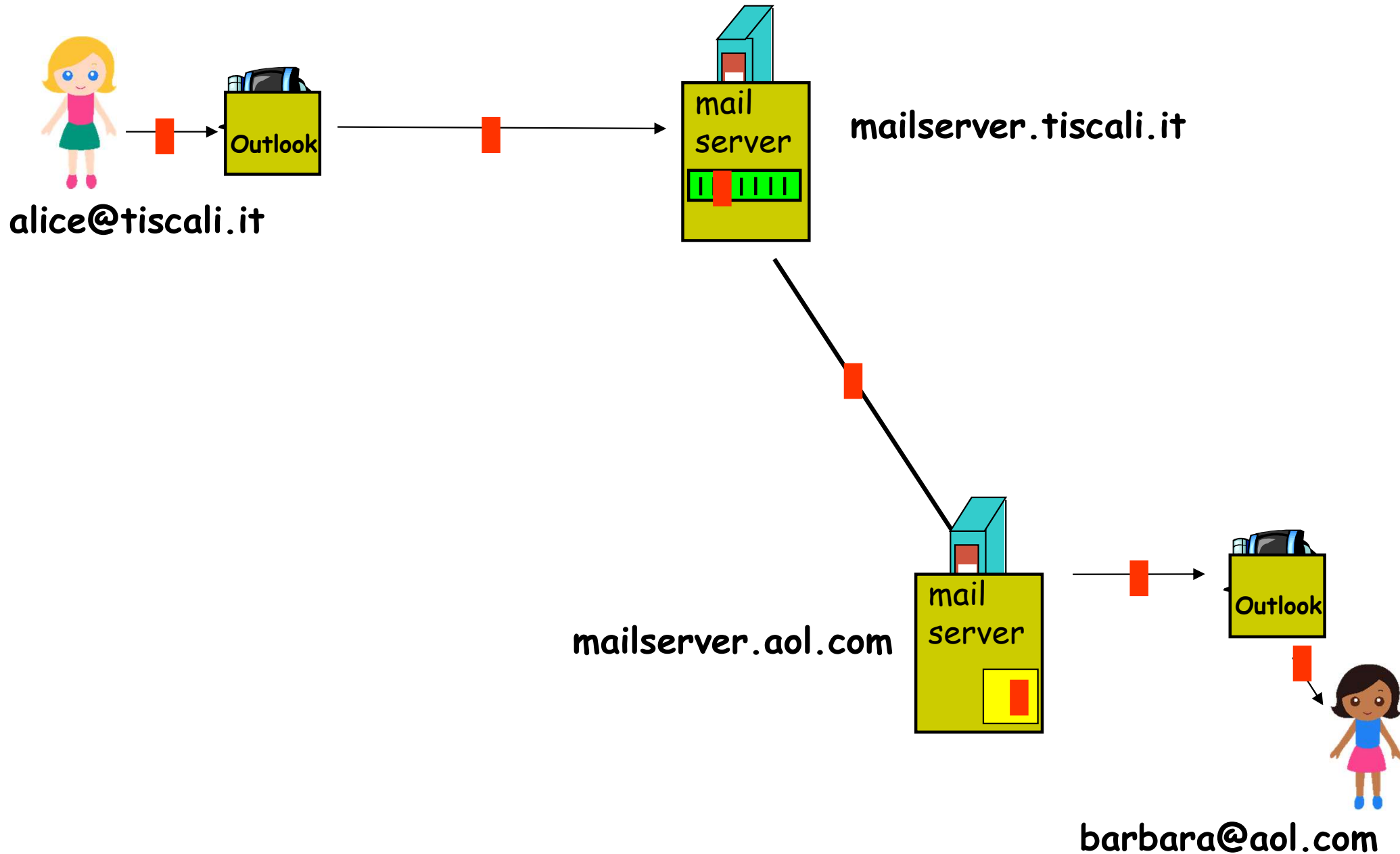
local-part @ **domain-name**

- **domain-name** : specifica un mail server. Determina il nome di dominio di una destinazione a cui la mail dovrebbe essere recapitata.

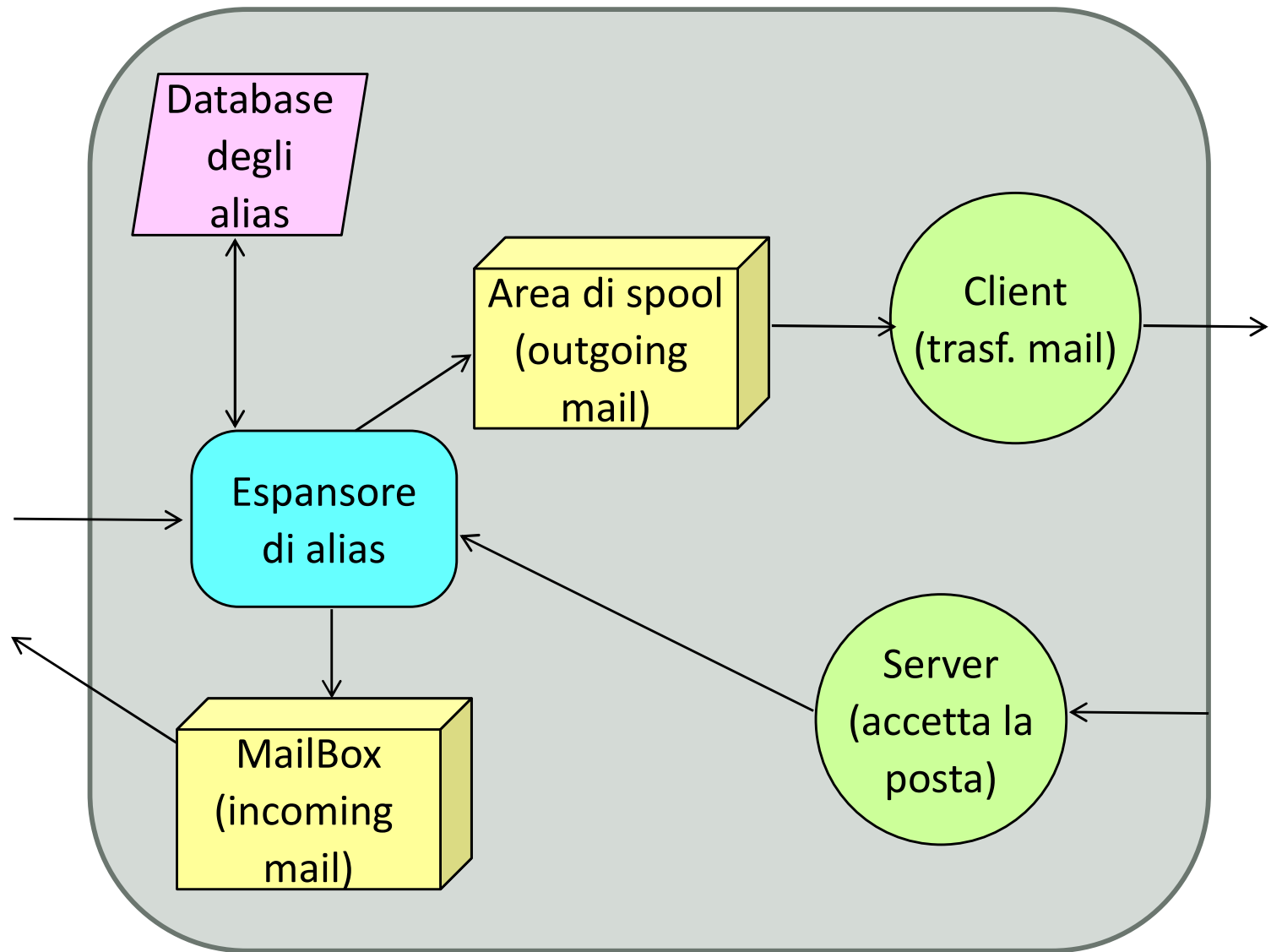
local part : specifica la cassetta di posta nel mail server. Spesso è identica al nome di login o al nome completo dell'utente



La storia di un messaggio



Server postale (con gestione alias)



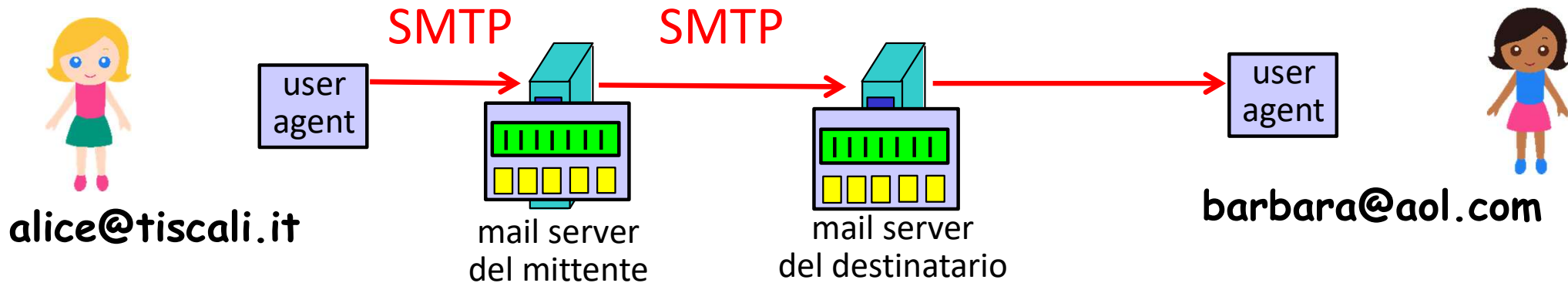
Server postale (schema di principio)

- I server di posta adottano una tecnica, denominata *spooling*:
 - L'utente invia un messaggio, il sistema ne pone una copia in memoria (*spool* – o area di accodamento della posta), insieme con id mittente, id destinatario, id macchina di destinazione e tempo di deposito.
 - Il sistema avvia il trasferimento alla macchina remota. Il sistema (client) stabilisce una connessione TCP con la macchina destinazione
 - Se la connessione viene aperta, inizia il trasferimento del messaggio.
 - Se il trasferimento va a buon fine il client cancella la copia locale della mail
 - Se il trasferimento non va a buon fine, il processo di trasferimento scandisce periodicamente l'area di spooling, e tenta il trasferimento dei messaggi non consegnati. Oltre un certo intervallo di tempo (definito dall'amministratore del server) se il messaggio non è stato consegnato, viene inviata una notifica all'utente mittente.

Server postale (Gestione alias)

- L'alias è una **cassetta postale virtuale** che serve a ridistribuire i messaggi verso uno o più indirizzi di posta elettronica personali.
- **molti-uno**: il sistema di alias permette ad un singolo utente di avere identificatori di mail multipli, assegnando un set di identificatori ad una singola persona -> Un utente – più indirizzi postali (es. mansioni)
- **uno-molti**: il sistema permette di associare un gruppo di destinatari ad un singolo identificatore -> Un indirizzo postale – più utenti destinatari (es. mailing list)
- Meccanismo di espansione degli ALIAS postali: conversione di identificatori di indirizzi postali in uno o più indirizzi postali nuovi
 - Se l'alias database specifica che all'indirizzo x deve essere assegnato il nuovo indirizzo y, l'espansione dell'alias riscriverà l'indirizzo di destinazione; si provvederà poi a determinare se y specifichi un indirizzo locale o remoto e lo posizionerà nell'area di spool relativa.

Protocollo di trasferimento della posta



- Servizio di trasferimento posta:
 - Intermediari, no consegna diretta
- **SMTP** [RFC 2821]: distribuisce/archivia nel mail server del destinatario
 - **Protocollo di tipo «push»**

Simple Mail Transfer Protocol

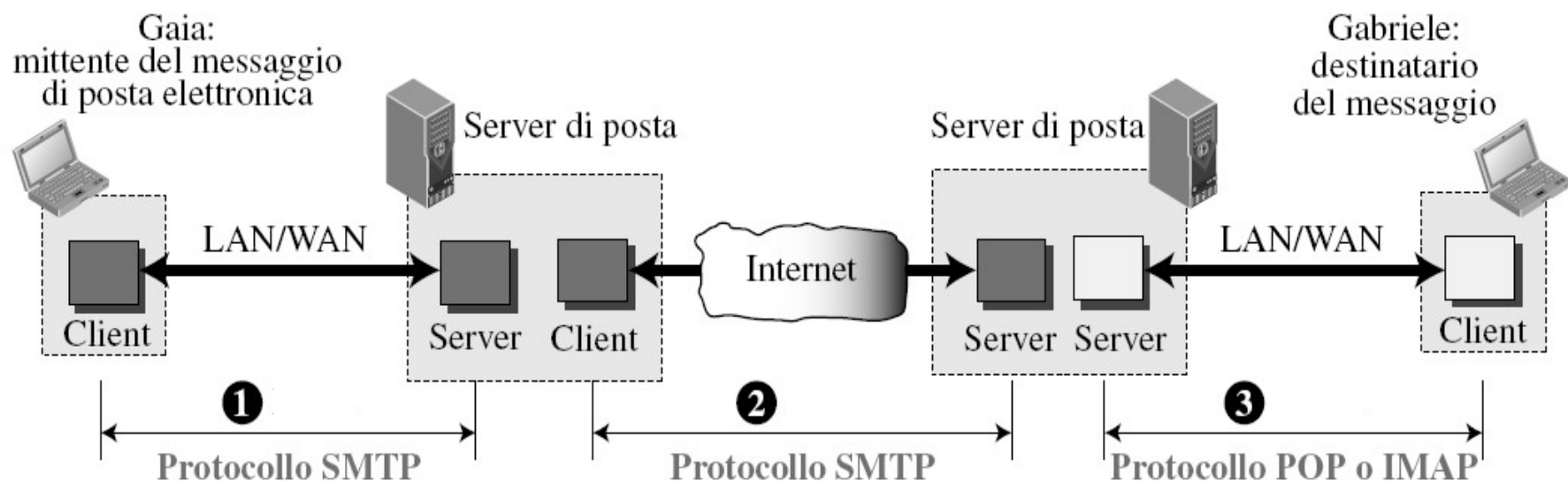
- RFC 821, 2821, 5321
- L'obiettivo di SMTP è il **trasferimento affidabile e efficiente** di mail
- SMTP è indipendente dal sistema di trasmissione usato e richiede solo il trasferimento di stream di byte ordinato e affidabile (l'RFC discute SMTP su TCP)
- Una caratteristica di SMTP è la capacità di trasportare mail attraverso più reti. Un messaggio di mail può passare attraverso server intermedi nel percorso da mittente a destinatario finale

SMTP Model

Quando un client SMTP vuole trasferire un messaggio, stabilisce un **canale di trasmissione bidirezionale con un server SMTP**. La responsabilità di un client è di trasferire la mail a un server SMTP, o comunicare un eventuale insuccesso (**scambio formale di responsabilità**).

Un client SMTP determina l'indirizzo di un host appropriato che ospita un server SMTP risolvendo il nome della destinazione in un indirizzo del mail server destinazione

- risoluzione di nome in indirizzo IP del mail server destinatario attraverso il DNS.





.. non ho ricevuto il tuo messaggio

Possibili problemi:

- connessione con mailserver del mittente (server inesistente o irraggiungibile)
 - connessione con mailserver destinatario (server inesistente o irraggiungibile)
 - inserimento in mailbox destinatario (user unknown, mailbox full)
- ... ma in tutti questi i casi **il mittente riceve una notifica!**

Destinatario può non ricevere (senza che mittente sia avvisato) solo se qualcuno (intruso, filtro antispam) rimuove messaggio



SMTP - protocollo

- In pratica: uso il protocollo TCP (**porta 25**) per consegnare in modo affidabile messaggi dal client al server
- Tre fasi durante il trasferimento via SMTP:
 - handshaking (“stretta di mano”)
 - trasferimento del messaggio
 - chiusura della connessione
- Interazione comando/risposta (command/response)
 - comandi: testo ASCII
 - risposta: codice di stato e descrizione (facoltativa)
- Messaggi (header e body): testo con caratteri ASCII a 7-bit

```
S: MAIL FROM:<Smith@Alpha.ARPA>
R: 250 OK

S: RCPT TO:<Jones@Beta.ARPA>
R: 250 OK

S: RCPT TO:<Green@Beta.ARPA>
R: 550 No such user here

S: RCPT TO:<Brown@Beta.ARPA>
R: 250 OK

S: DATA
R: 354 Start mail input;
end with <CRLF>.<CRLF>
S: Blah blah blah...
S: ...etc. etc. etc.
S: <CRLF>.<CRLF>
R: 250 OK
```

SMTP - protocollo

Handshaking

Il client stabilisce la connessione e attende che il server invii

220 READY FOR MAIL (Disponibilità a ricevere posta)

Il client risponde con il comando **HELO**

Il server risponde identificandosi

A questo punto il client può trasmettere i messaggi

```
S: 220 Beta.GOV Simple Mail Transfer Service ready
```

```
C: HELO Alfa.EDU
```

```
S: 250 Beta.GOV
```

Comandi SMTP

- Alcuni comandi:
 - HELO <client identifier>
 - MAIL FROM:<reverse-path> <CRLF>
 - RCPT TO:<forward-path> <CRLF>
 - DATA
 - QUIT
- N.B. <CRLF>.<CRLF> per determinare la fine di un messaggio

Formato messaggi mail

SMTP: protocollo per lo scambio dei messaggi

RFC 2822: standard per il formato testo:

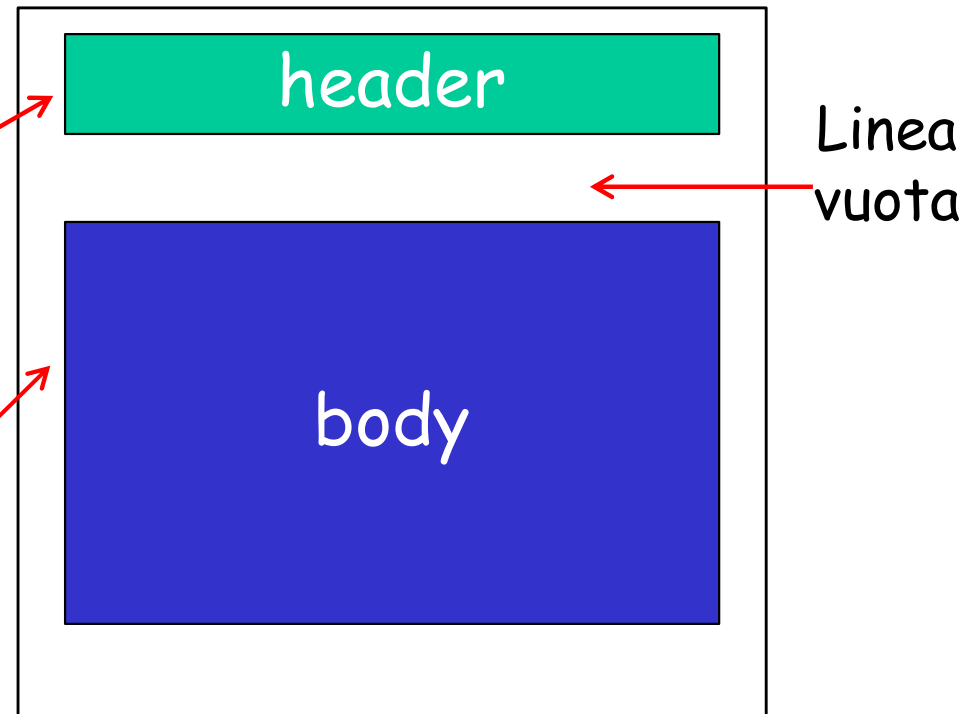
- **linee intestazione**, es.,

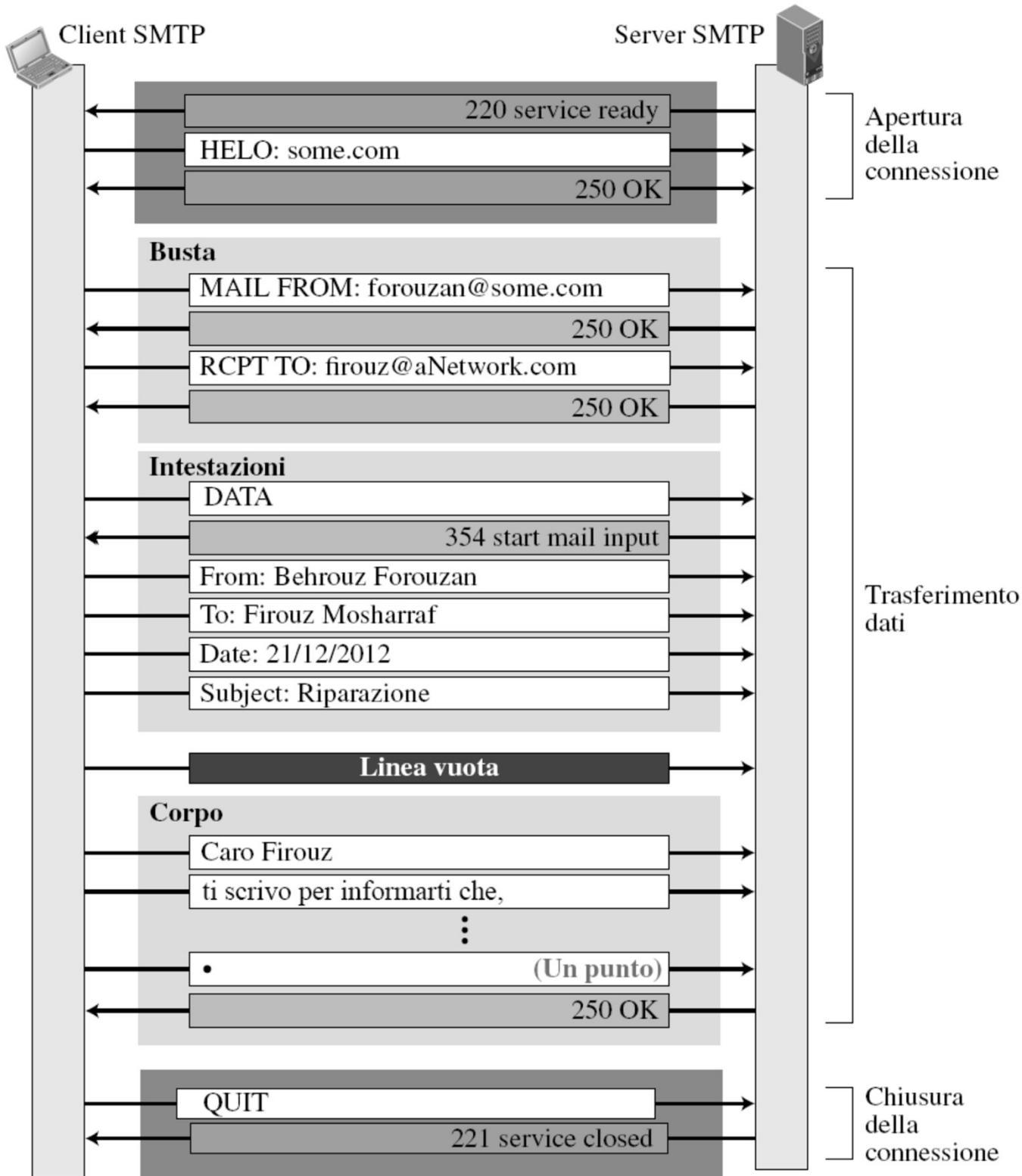
- To:
- From:
- Subject:

sono diversi dai comandi SMTP !

- **body**

- il “messaggio”, solamente caratteri ASCII a 7 bit





Esempio di interazione SMTP

Format dei messaggi: estensioni multimediali

RFC 822 permette di inviare solo messaggi di testo in ASCII

- **Problema:** come permettere agli utenti di Internet di inviare/ricevere messaggi
 - in lingue con accenti (come l'italiano), in alfabeti non latini (come russo o ebraico), in lingue senza alfabeto (come il cinese)
 - contenenti audio o video

MIME

- idea di base: continuare a usare il formato del messaggio specificato in RFC 822 ma aggiungendo una struttura al message body e definendo regole di codifica (encoding) per il trasferimento di testo non-ASCII.
- **Perché questa scelta?**
- **Questo ha permesso di inviare messaggi MIME usando protocolli e mail server esistenti (necessario invece cambiare gli User Agents)**

Format dei messaggi: estensioni multimediali

MIME: Multipurpose Internet Mail Extension (MIME), RFC 2045, 2046 è un Internet Standard che estende il formato di e-mail per supportare:

- * testo in set di caratteri diversi da US-ASCII;
- * allegati in formato non testuale;
- * corpo del messaggio con più parti (multi-part)
- * header in set di caratteri non-ASCII

MIME (RFC 2045) definisce un insieme di **metodi per rappresentare dati binari in formato ASCII**

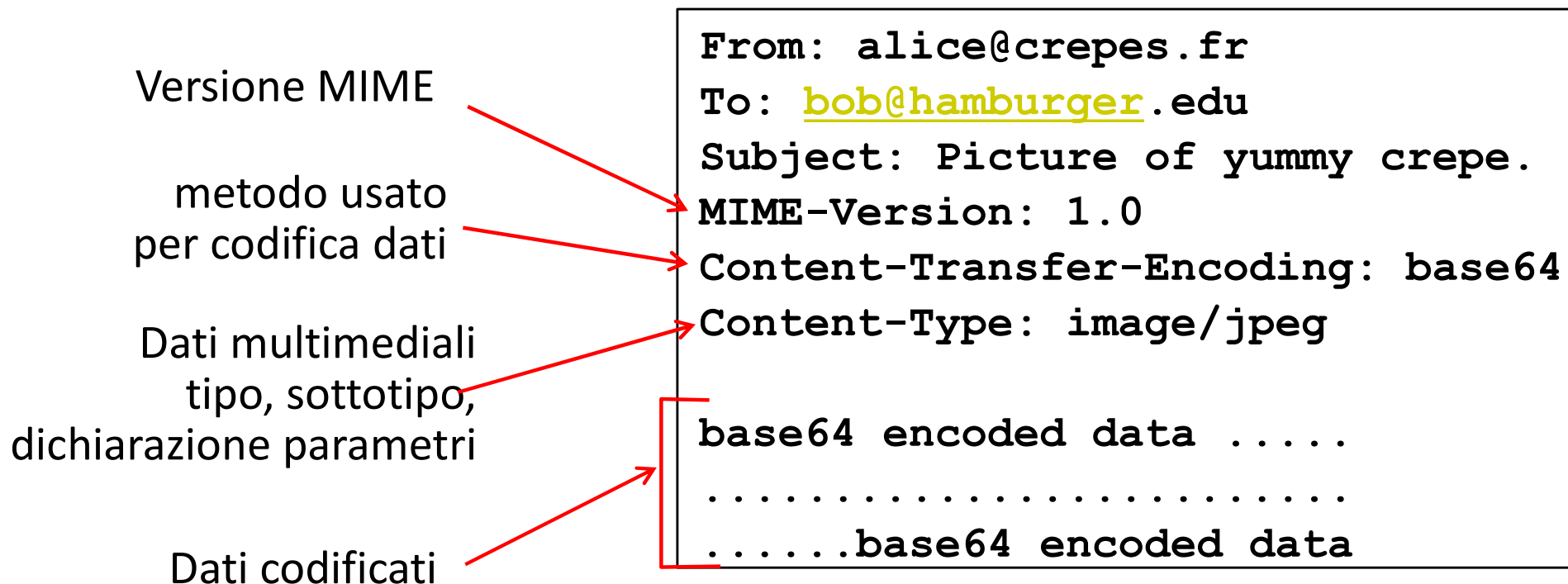
linee di intestazione aggiuntive per dichiarare il tipo di contenuti MIME



Format dei messaggi: estensioni multimediali

MIME: Multipurpose Internet Mail Extension, RFC 2045, 2046

linee di intestazione aggiuntive per dichiarare il tipo di contenuti MIME



Format dei messaggi: estensioni multimediali

- Client e server SMTP si aspettano messaggi ASCII (caratteri ASCII che usano 7 degli 8 bit di un byte). I dati binari usano invece tutti gli 8 bit di un byte (es. immagini, eseguibili, set estesi di caratteri).
- MIME fornisce vari schemi di transfer encoding, tra cui:
 - ASCII encoding of binary data: base 64 encoding
 - Gruppi di 24 bit sono divisi in 4 unità da 6 bit e ciascuna unità viene inviata come un carattere ASCII
 - Quoted-printable encoding: per messaggi testuali con pochi caratteri non-ASCII, più efficiente
- **Oggigiorno i mail server possono negoziare l'invio di dati in 8 bit, se la negoziazione non ha successo si usano i caratteri 7bit-ASCII**

Tipi MIME

`Content-Type: type/subtype; parameters`

Specificano la natura dei dati nel corpo di un'entità MIME

Text

esempi di subtypes: `plain`,
`html`

Image

esempi di subtypes: `jpeg`, `gif`

Audio

esempi di subtypes: `basic` (8-bit
mu-law encoded), `32kadpcm` (32
kbps coding)

Video

esempi di subtypes: `mpeg`,

Application

altri dati che devono essere
processati da un'applicazione
prima di essere visualizzabili
esempi di subtypes: `msword`,
`octet-stream` (dati
arbitrari binari)

Tipo “Multipart”

From: alice@crepes.fr
To: bob@hamburger.edu
Subject: Picture of yummy crepe.
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary=98766789

--98766789

Content-Transfer-Encoding: quoted-printable
Content-Type: text/plain

Dear Bob,
Please find a picture of a crepe.

--98766789

Content-Transfer-Encoding: base64
Content-Type: image/jpeg

base64 encoded data

.....

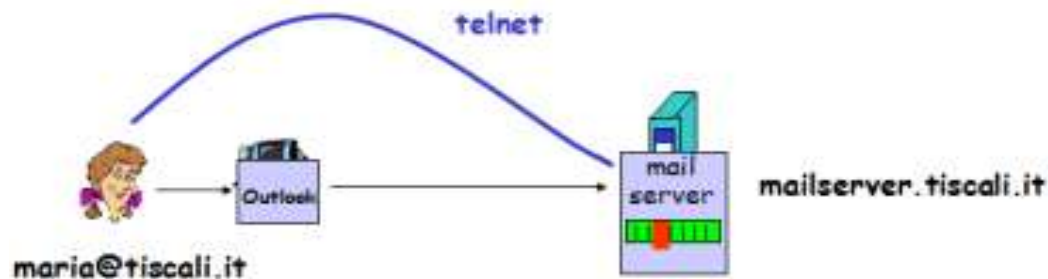
.....base64 encoded data

--98766789--

...

Protocolli email

- sperimentare SMTP con *telnet servername 25*



HTTP	SMTP
Pull	Push
Ogni oggetto incapsulato in un messaggio di risposta	Tutti gli oggetti di un msg inviati in un multipart message

Porta 25 (per semplicità e ragioni storiche, in realtà possono essere usate altre porte, es. 587)

Esempio

```
paganelli@lrst:~$ telnet out.example.it 25
Trying 150.217.6.201...
Connected to smtpbal.server.example.it.
220 smtpbal.server.maildomain.it ESMTP Postfix
```

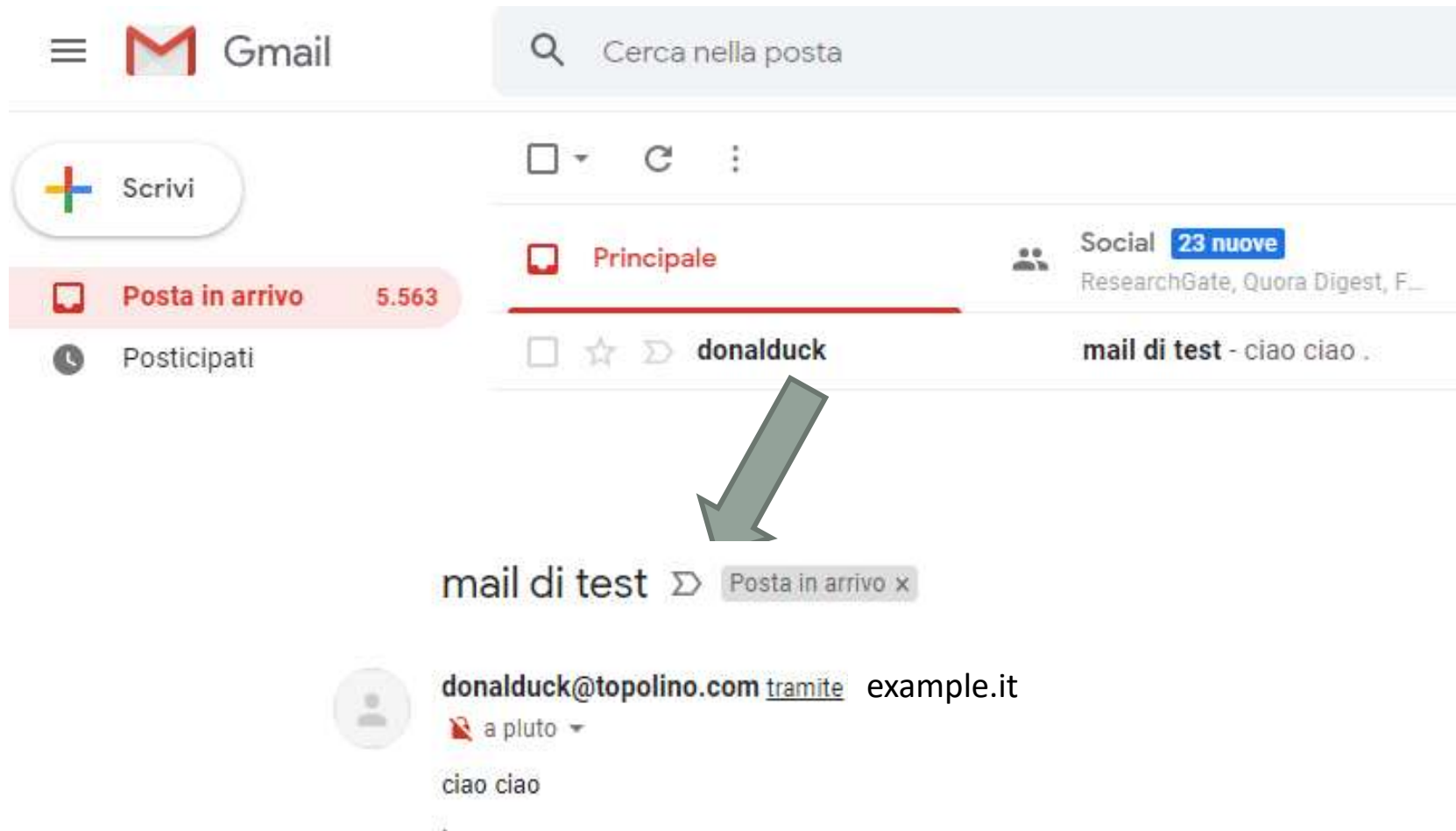
Username e password...

```
235 2.7.0 Authentication successful
MAIL FROM:<federica.paganelli@example.it>
250 2.1.0 Ok
RCPT TO:<federica.paganelli@gmail.com>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: donalduck@topolino.com
To: pluto@esempio.it
Subject: mail di test
```

ciao ciao

```
..
.
```

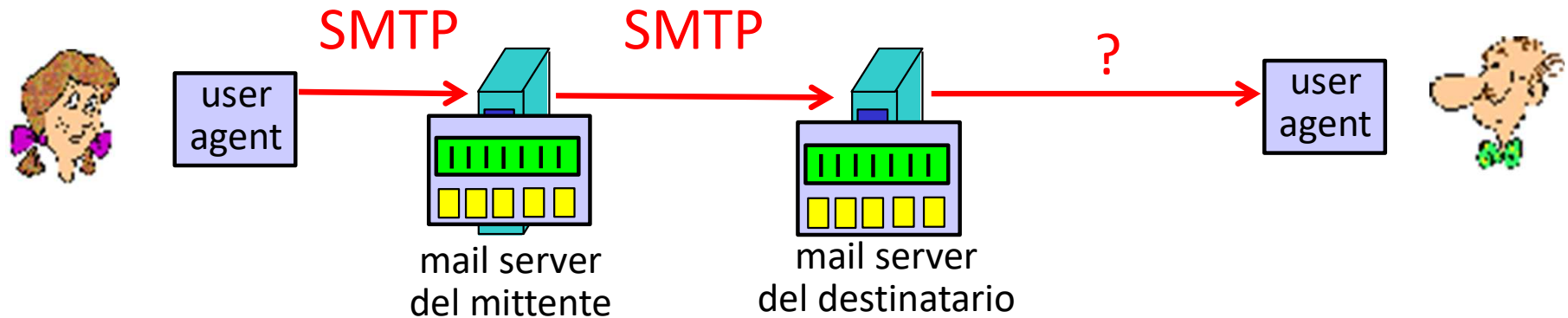
Esempio



Delivered-To: federica.paganelli@gmail.com
Received: by 2002:a05:6838:c0f2:0:0:0 with SMTP id l18csp793948nkb;
Sat, 3 Oct 2020 23:55:06 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJzEG1kr+8Z67lcn/yf3krp/oqmMUSQVJkguZbahzvqDye/M1QZdgBa5EDsFjGdzEc4gxp
X-Received: by 2002:a17:906:b7c1:: with SMTP id fy1mr9450027ejb.342.1601794506760;
Sat, 03 Oct 2020 23:55:06 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1601794506; cv=none;
d=google.com; s=arc-20160816;
b=fvmmquPGCafhTnzlnBpZx1npeUlgufotfHv5tA64ZnHr7/BkxZsAWQrvRxODCPIDl
284wkATesGQ69a2mwnl4a6aJi2ovOtWJK1kOD+XK980OZqcFsMuyoxcmawgv/yCrdSBw
hLeeQ0PUdOgaUBRXNcQx/ofXiO9O+UIX0Ym1nf+VVGpqqRP4b4UL4LQgrZeRwoo4vi7l
EeVJ0imlG8PX4zLtR7THoYdg4/EqPs0S2ECtU2muHtCULDlIjxCg4Fjr4UWx50+0ZDze
hTgd2OITkOCTUv9H7qeMCpYXm5jFC6uHtFY4v1NPBWMcTznHtspkDRvSXzKqVTNR8Op
Ehdg==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
h=date:message-id:subject:to:from;
bh=GWRkC1kbqyg52XVswqVXiF0gutvINyTKvTSkg41Txd4=;
b=i43lo5vZkTyv6pq0McJfAccKjxMF7/escGehteMRt9t/je6+kFVM1HE8koEesUquH
nARqATFwEzMoUJf9QHcaHiEvctQMmVACKTeVbmRUT6HJMJAAddyYtCGpAFFGQ7RYzsP9r
2MEONvuxR19Yfr8G455OiDcaOZ4EnCkD3KT1sk+IEBklzbJxQ/Wj9a1zQalNturpnwMH
h9PoCoUARux+q1XPYEhB5YWfxCjIIWk2+/xFCQc/DmwDTpsqFD9vdYo2CdRYOBZ8BABw
6yNxAE6QEWB4hfBKJyK3ktMKSIfJkxnoqqcwGqkBzEYgJ97dc11Zm8MFViVr1eTCg3f/
81rg==
ARC-Authentication-Results: i=1; mx.google.com;
spf=pass (google.com: domain of federica.paganelli@example.it designates 140.117.6.205 as permitted sender) smtp.mailfrom=federica.paganelli@example.it
Return-Path: <federica.paganelli@example.it>
Received: from av5.sf-csiasf.example.it (av5.sf-csiasf.example.it. [150.217.6.205])
by mx.google.com with ESMTP id jr10si4822322ejb.167.2020.10.03.23.55.06
for <federica.paganelli@gmail.com>;
Sat, 03 Oct 2020 23:55:06 -0700 (PDT)
Received-SPF: pass (google.com: domain of federica.paganelli@example.it designates 150.217.6.205 as permitted sender) client-ip=140.117.6.205
Authentication-Results: mx.google.com;
spf=pass (google.com: domain of federica.paganelli@example.it designates 150.217.6.205 as permitted sender) smtp.mailfrom=federica.paganelli@example.it
Received: from av5.sf.example.it (av5 [127.0.0.1]) by localhost (Postfix) with SMTP id 544861821F7 for <federica.paganelli@gmail.com>; Sun,
4 Oct 2020 08:55:06 +0200 (CEST)
Received: from lab.info.example.it (lab.info.example.it [150.217.8.90]) (Authenticated sender: *hidden*) by av5.sf.example.it (Postfix) with SMTP id DE83C1821F6 for <federica.paganelli@gmail.com>; Sun,
4 Oct 2020 08:54:00 +0200 (CEST)
From: donalduck@topolino.com
To: pluto@esempio.it
Subject: mail di test
Message-Id: <20201004065416.DE83C1821F6@av5.sf-csiasf.example.it>
Date: Sun,
4 Oct 2020 08:54:00 +0200 (CEST)

ciao ciao

Protocolli di accesso alla Mail



- Servizio di trasferimento posta:
 - Intermediari, no consegna diretta
- **SMTP** [RFC 2821]: distribuisce/archivia nel mail server del destinatario
 - protocollo di accesso alla Mail : recupero mail dal server del destinatario
 - **Protocollo di tipo «push»**
- Protocolli di accesso alla posta
 - **Protocolli di tipo «pull»**
 - POP: Post Office Protocol [RFC 1939]
 - IMAP: Internet Mail Access Protocol [RFC 1730]
 - HTTP

Accesso alla posta: POP3

- Lo user agent apre una connessione TCP (porta 110) verso il server di posta
- Fasi di: autorizzazione, transazione, aggiornamento

Accesso alla posta: POP3

- **Autorizzazione**
comandi del client:
 - `user`: specifica la username
 - `pass`: specifica la passwordil server risponde
 - OK
 - ERR
- **Fase di scambio**
comandi del client:
 - `list`: visualizza la lista dei messaggi
 - `retr`: preleva il messaggio per numero
 - `dele`: elimina il messaggio dal server
 - `quit`: chiude la sessione
- **Aggiornamento**
 - Dopo `quit` il server cancella i messaggi marcati per la rimozione

```
federica@federica:~$ telnet in.example.it
110
Trying 150.217.5.25...
Connected to in.example.it.
Escape character is '^]'.
+OK POP3 Ready mdap 00022982
user ...
+OK USER
pass [PASSWORD in CHIARO!!!]
+OK You are so in
list
+OK 318 messages:
1 319393
2 49513
3 8691
```

317 109229

318 990

.

retr 318

+OK 990 octets

Return-Path: <dino@stud.example.it>

Delivered-To: paganelli@imap2.sf-int.example.it

Received: from av3.sf.example.it (av3.sf-int.example.it [10.2.59.1])

by imap2.sf-int.example.it (Postfix) with ESMTP id 8C46F20303

for <paganelli@imap2.sf-int.example.it>; Sun, 24 Mar 2013 17:34:55 +0100 (CET)

Received: from av3.sf.example.it (localhost.localdomain [127.0.0.1])

by localhost (Postfix) with SMTP id 82DF7100024

for <paganelli@example.it>; Sun, 24 Mar 2013 17:34:55 +0100 (CET)

Received: from client (host20-197-dynamic.55-82-r.retail.telecomitalia.it [82.55.197.20])

by av3.sf.example.it (Postfix) with SMTP id 1688C100019

for <federica.paganelli@example.it>; Sun, 24 Mar 2013 17:34:35 +0100 (CET)

Message-Id: <20130324163446.1688C100019@av3.sf.example.it>

Date: Sun, 24 Mar 2013 17:34:35 +0100 (CET)

From: dino@stud.example.it

To: undisclosed-recipients;;

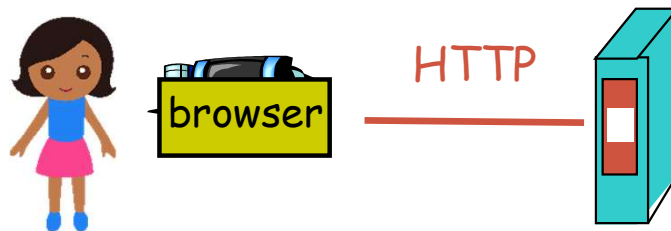
X-PMX-Version: 5.5.8.383112, Antispam-Engine: 2.7.2.376379, Antispam-Data: 2013.3.24.162719

ciao ciao ciao

.

Accesso alla posta

- IMAP
 - più feature (e più complesso) di POP3 (che non mantiene informazioni di stato tra sessioni – solo cancellazioni permesse)
 - manipolazione di messaggi memorizzati sul server (p.e. folder)
 - comandi per estrarre solo alcuni componenti dei messaggi (p.e. solo intestazioni se si sta usando una connessione lenta)
- HTTP: Hotmail , Yahoo! Mail, gmail, etc.





- SPAM
- messaggi “forged”
- messaggi letti da intrusi



- Differenze (di netiquette e "fisiche") tra:
 - To
 - Cc
 - Bcc