

Indirizzi email

Simbolo @ → si dice "at" non chiocciola. Il suo utilizzo serve ad indicare a quale dominio appartiene l'utente.

Gli indirizzi email seguono un formato definito in RFC2822 e poi successivamente in RFC3696:

local_username@domain

- **MAX 64 caratteri nella parte di username**, che dovrebbe essere case sensitive, ma alcuni mail server, per garantire maggiori compatibilità, lo escludono;
- **MAX 255 caratteri nella parte di domain**, essa NON è case sensitive.

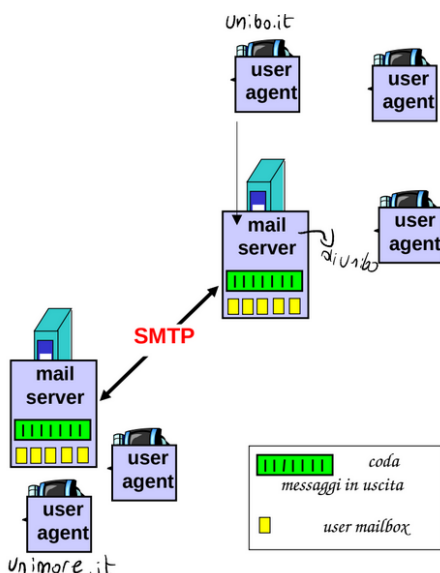
Protocolli e agenti software utilizzati per la gestione della posta elettronica non prevedono meccanismi di autenticazione per gli indirizzi di posta elettronica del mittente, in quanto questo campo non può essere considerato come un'informazione affidabile data la facilità nel generare una mail con un mittente arbitrario.

Gestione posta elettronica

La posta elettronica è un sistema che si compone di vari elementi, **fondamentali** e **aggiuntivi**:

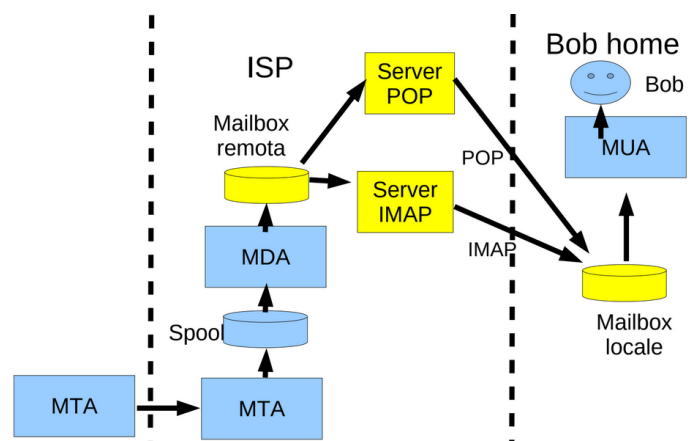
- **Mail Transfer Agent (MTA)**: mail server per la gestione e trasferimento della posta;
- **SMTP**: Simple Mail Transfer Protocol, protocollo per il trasferimento della posta;
- **DNS**: resource record MX;
- **Mail User Agent(MUA)**: applicativo client per la gestione della posta lato utente(tipo Thunderbird)
- **Mail Delivery Agent(MDA)**;
- **Mail Submission Agent(MSA)**

Esempio: scambio di mail tra unimore.it e unibo.it



1. x@unibo.it vuole mandare una mail a y@unimore.it;
2. x scriverà la mail tramite il suo user agent, una volta finita cliccherà su invia;
3. La mail arriverà nel mail server di UniBO, il quale comunicherà con il mail server di UniMORE con SMTP;
4. La mail, ora nel mail server di UniMORE, arriverà a y dopo essere stato trovato.

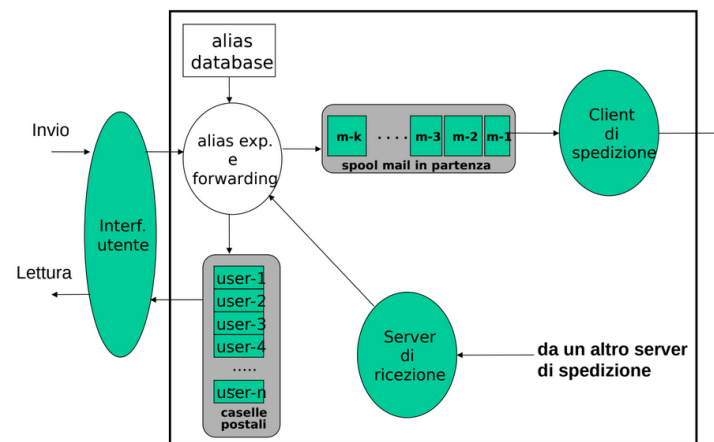
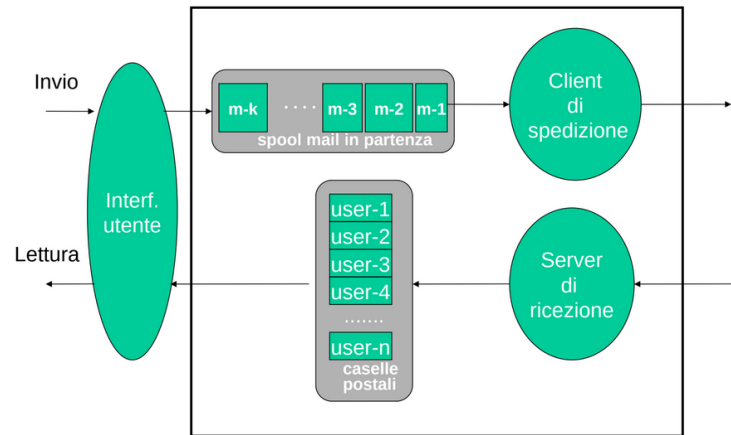
Ora, il passaggio non è così diretto, soprattutto in casi in cui si fa utilizzo di mail server remoti (POP o IMAP). In questo caso, si fa uso del delivery agent e tra esso e l'utente c'è uno strato di software, in cui la mailbox viene resa fruibile mediante appositi server, che verranno poi usati per copiare i contenuti nella mailbox locale.



Mail Server(o MTA)

Funzionamento:

- I messaggi in arrivo vengono memorizzati nelle user mailbox;
- I messaggi in uscita vengono mantenuti temporaneamente in una coda, in cui vi rimarranno per un tempo prefissato in caso il server di destinazione non sia raggiungibile;
- L' MTA funge dunque da client e da server;
- La destinazione è una macchina il cui nome è caratterizzato come "mail-exchange object"... Il nome della mailbox, normalmente ad un username, ma può anche essere un alias (si fa uso dunque di un alias database per la risoluzione del nome);
- Una mail può anche arrivare da elementi interni all'organizzazione, non richiedendo dunque una connessione all'esterno.



Mail transfer agent

È il processo principale che trasferisce messaggi da un computer all'altro. Ha un funzionamento trasparente, in quanto l' user vedrà solo il MUA.

Può ricevere messaggi da:

- Un altro MTA;
- Da un MUA;
- Un MSA che, a sua volta ha ricevuto posta da un MUA.

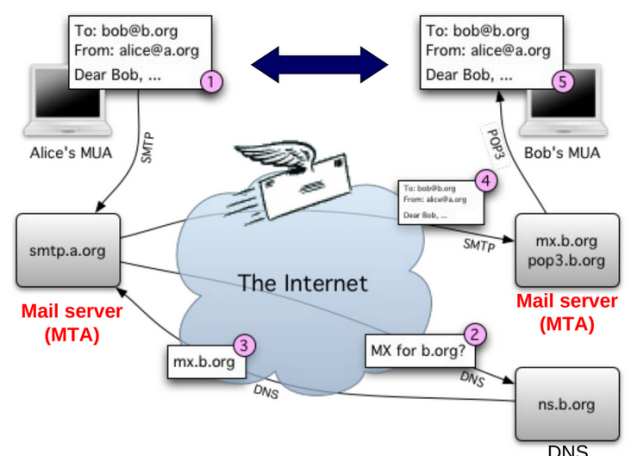
Ha due modalità di trasferimento:

Diretto → dall'MTA sending server all'MTA receiving server;

Relay → dall'MTA sending server a un server intermedio.

Interazione con il DNS

L'esempio fatto prima, nella connessione tra unibo.it e unimore.it, era molto semplice e lasciava molte cose indietro. Chiaramente un mail server non conosce a priori il mail server che gestisce il dominio di posta del destinatario, dovrà dunque interagire con il DNS. Esso gestisce infatti un tipo di resource record di tipo MX che specifica come deve essere inoltrato un messaggio, nello specifico un elenco di mail server che possono ricevere l'email per quel dominio con relativa priorità.



1. L'MTA mittente cerca di stabilire una connessione SMTP/TCP con il server a priorità più alta nel resource record del DNS e continua fin quando non c'è un server dell'elenco che risponde;
2. Il messaggio viene inoltrato al primo server che risponde;
3. Si parla di un generico Mail Exchange Server poiché esso potrebbe essere sia un server di destinazione o un relay.

La presenza di MTA multipli serve per garantire il funzionamento in casi di alto traffico e per differenziare i due principali casi d'uso:

- SMTP server, il quale gestisce il trasferimento dei messaggi inviati dall'interno del dominio, interagisce con i client di posta e gestisce code piccole;
- MX server, il quale gestisce la ricezione dei messaggi provenienti dall'esterno, gestisce code molto lunghe e richiede dunque molta potenza computazionale.

Altri agenti per mail server

In alcuni casi il mail server fa anche utilizzo di Mail Submission Agent e Mail Delivery Agent oltre che del solito MTA. Questa organizzazione multi-livello è ormai lo standard nei mail server delle organizzazioni più complesse, soprattutto a causa di varie necessità:

- Logging;
- Spam detection;
- Virus detection;
- Controllo dell'autorizzazione a insiemi di mittenti/destinatari

Il **Mail Delivery Agent** effettua operazioni di filtro e di ordinamento, ad esempio l'inserimento in cartelle in base a keyword, soggetto, mittente e testo (ad esempio lo smistamento in SPAM di mail che arrivano da indirizzi sospetti) e anche invio di auto-reply sulla base di eventi stabiliti dall'utente.

Il **Mail Submission Agent** è il processo che riceve un messaggio da un Mail User Agent e contatta un Mail Transmission Agent per inviarlo, anche se molti MTA agiscono da MSA, contando che queste due funzioni sono sempre state storicamente integrate. **Ma perché dunque separarle?** Interagendo direttamente con un MUA può correggere o segnalare all'utente mittente alcuni errori evidenti. L'MSA può fare utilizzo di diverse politiche di filtro e antispam per l'accettazione dei messaggi e richiedere l'autenticazione al posto del MTA

SMTP

- Protocollo di comunicazione tra MTA;
- Paradigma client/server del tipo MTA del mittente/MTA del destinatario e sono in esecuzione su ogni mail server;
- Usa TCP per il trasferimento affidabile di messaggi tra client e server.
- Uso della porta 25;
- Dialogo tramite "frasi" in formato testuale human-readable;
- Interazione comando/risposta (comandi in formato ASCII-7 bit, risposta: codice + commento);

Trasferimento

3 fasi:

- Handshaking;
- Trasferimento;
- Chiusura.

Si usa TCP per creare connessioni persistenti e per trasferire più messaggi in una sola volta tra gli stessi interlocutori.

Formato del messaggio SMTP

Due parti:

- Header con campi codificati;
- Body, testo in ascii.

- Linee di header, es.:

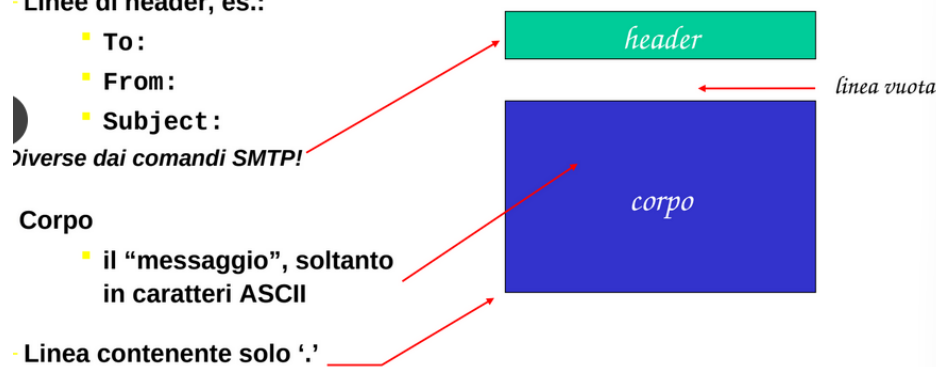
- To:
- From:
- Subject:

Diverse dai comandi SMTP!

Corpo

- il "messaggio", soltanto in caratteri ASCII

- Linea contenente solo '.'



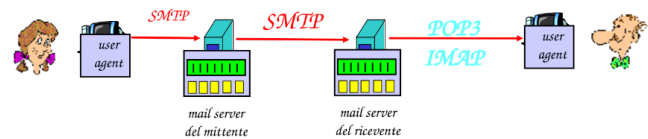
Perché non HTTP?

HTTP è un protocollo pull (client prende dal server), SMTP è un protocollo push (client da al server)

Mail User Agent

Applicazione utente della posta, comprende:

- User Interface;
- Strumenti per scrivere e inviare mail;
- Strumenti per leggere mail;
- Strumenti per la gestione di allegati;
- Strumenti di gestione posta inviata e ricevuta;



- SMTP: consegna/memorizzazione al mail server del destinatario
- Protocollo di accesso alla posta
 - POP: Post Office Protocol [RFC 1939]
 - autorizzazione (user agent ↔ mail server) e download
 - IMAP: Internet Mail Access Protocol [RFC 1730]
 - più caratteristiche (maggiore complessità)
 - possibilità di manipolazione dei messaggi memorizzati sul server

• HTTP: accesso alla posta tramite Webmail, non utilizzo un "vero" MUA, ma un browser che si collega a un applicativo web dinamico che mi consente di scrivere e inviare messaggi, e di accedere alla mia mailbox (completamente remota)

POP3

Fasi:

- **Instaurazione connessione** TCP con un mail server sulla porta 110;
- **Autorizzazione** MUA invia al mail server la propria mail e password per il login;
- **Transazione** in cui il MUA recupera i messaggi e indica alcuni messaggi per poterli cancellare;
- **Aggiornamento**, avviene dopo il quit del client, in cui vengono cancellati dalla mailbox i messaggi indicati dall'utente.

IMAP

- Più funzionalità e complessità rispetto a POP3
- Permette all'utente di modificare la propria mailbox come se fosse locale e di ottenere solo alcune parti del messaggio (come ad esempio solo alcuni allegati);

Fasi:

- **Instaurazione della connessione** TCP con il mail server (MSA o MTA a seconda del sistema);
- **Autorizzazione** MUA invia al mail server mail e password per il login;
- **Transazione** che comprende comandi client, dati e risultati dal server.

MIME

SMTP tratta correttamente solo caratteri ASCII a 7 bit, ma come faccio a trasferire altri caratteri o dati in binario? Lo standard de facto attuale è MIME (Multipurpose Internet Mail Extension).

Si interpone tra UI e mailer, automatizzando la procedura di conversione che viene effettuata dai client e dai server quando si spediscono mail in formato SMTP/MIME, introducendo un ulteriore livello di incapsulamento: viene esteso l'header dei messaggi con 5 campi specifici del MIME, ovvero:

- **MIME-version** che deve valere 1.0 per indicare la conformità alle specifiche delle RFC;
- **Content-type** che descrive i dati nel body;
- **Content-Transfer-Encoding** trasformazione usata per il body, in modo da renderlo trasmissibile con ASCII a 7 bit;
- **Content-ID** che serve per identificare le entità del MIME in contesti multipli
- **Content-Description** descrizione testuale human-readable dell'oggetto codificato

Message type

- message/rfc822 → definisce ricorsivamente il contenuto come un altro messaggio completo;
- message/partial → usato per gestire frammentazione di un messaggio, ha campi di:
 - ID: valore comune a tutti i frammenti;
 - Number: numero d'ordine della sequenza;
 - Totale: numero di parti;
- message/external-body → usato per accedere a documenti esterni;
- FTP + param;
- TFTP + param;
- Anon-FTP → FTP anonimo;
- local-file → segue un path-name locale sul ricevitore;
- AFS → accessibile tramite Andrew File System;
- mail-server → body accessibile inviando una mail a un dato sito

Lo standard MIME è nato per essere espandibile, le sue definizioni includono metodi per definire altri tipi di contenuti e per questa sua flessibilità viene utilizzato anche da altri protocolli non di posta.

Limiti della posta elettronica

- Non ci sono garanzie di confidenzialità, integrità, consegna, autenticazione e non ripudio;
- SPAM;

Come si può migliorare la sicurezza?

- Estensioni di SMTP (autenticazione utenti, cifratura dati, conferma di ricezione)
- Supporto per la crittografia nei messaggi di posta (firma digitale e cifratura dei messaggi, in modo che non siano leggibili anche se archiviati).