

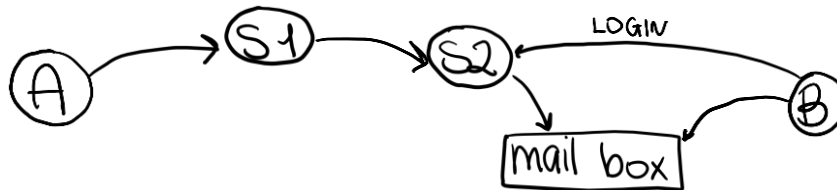
ALTRO PROTOCOLLO APPLICATIVO : **SMTP** (SIMPLE MAIL TRANSFER PROTOCOL)

UTILIZZA IL PROTOCOLLO TCP SULLA PORTA 25

UNO DEI PIÙ VECCHI USATI IN RETE (PRIMA VERSIONE 1981, RFC 788, ORA RFC 5321)

ASINCRONO : FUNZIONA COME SERVIZIO POSTALE, IL MESSAGGIO VIENE RECAPITATO

INDIPENDENTEMENTE DALLA "PRONTEZZA" DEL DESTINATARIO, RIMANE PRONTA FINCHÉ NON VIENE LETTA.



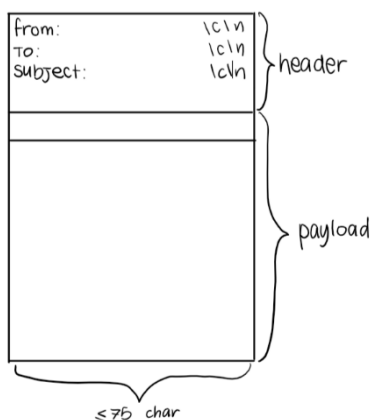
PER REALIZZARLO CI SONO SERVER INTERMEDI (DI POSTA ELETTRONICA), IL MESSAGGIO VIENE INVIATO AL SERVER, CHE LO MANDA A SUA VOLTA AD UN ALTRO SERVER

QUALITÀ SERVIZIO : BEST EFFORT, SERVER FA DEL SUO MEGLIO NEL RECAPITARE IL MESSAGGIO SENZA DARE GARANZIE, NON PUÒ SAPERE SE E QUANDO CLIENT SARÀ DISPONIBILE A RICEVERLO

DESTINAZIONE DEI MESSAGGI : **CASELLA POSTALE**, FILE DI TESTO DELL'UTENTE DESTINATARIO, NEL QUALE VIENE SCRITTO IL CONTENUTO DEL MESSAGGIO RICEVUTO; IL FILE CONTIENE INOLTRE TUTTI I VECCHI MESSAGGI. È COMPITO POI DEL DESTINATARIO DI ACCEDERE ALLA MAILBOX, UN TEMPO CON IL LOGIN AL SERVER, ORA CON ALTRI PROTOCOLLI

A POTREBBE CONNETTERSI DIRETTAMENTE AL SERVER DI POSTA DI B, **NON C'È NECESSITÀ DI HOP** IN SMTP, MA SONO UTILI

LA TRASMISSIONE AVVIENE CON CODIFICA ASCII A 7 BIT (NON BYTE DA 8 BIT); C'È UN LINGUAGGIO, QUINDI IL CLIENT PUÒ MANDARE COMANDI, CODIFICATI CON 9 LETTERE MINUSCOLE, IL SERVER RISPONDE CON NUMERI CODIFICATI IN ASCII



I MESSAGGI SONO DIVISI IN DUE PARTI: INTESTAZIONE E CORPO.

NELL'INTESTAZIONE, LE PAROLE CHIAVE Danno INFORMAZIONI (FROM, TO, SUBJECT, DATE, ECC.)

PER DIVIDERE L'HEADER DAL PAYLOAD, C'È UNA RIGA VUOTA

(\c\n\c\n, DUE TERMINATORI DI FILA); LE RIGHE DEVONO TERMINARE CON \c\n (\c\n = <cr><lf>)

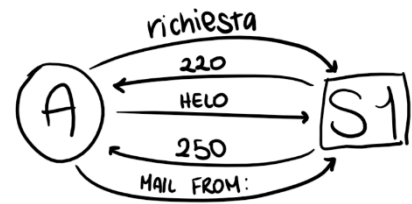
OGNI RIGA PUÒ ESSERE LUNGA MASSIMO 75 CARATTERI, MENTRE I

MESSAGGI POSSONO AVERE UNA LUNGHEZZA VARIABILE; IL MESSAGGIO

TERMINA CON .\c\n IN UNA RIGA (= <cr><lf>.<cr><lf>). PER INVIARLO C'È UNA SEQUENZA DI ESCAPE.

vengono codificati allo stesso modo per tutto il "viaggio". Client apre la connessione TCP con il server su porta 25, prima di mandare comandi aspetta conferma con numero 220 + una parte testuale con indirizzo del server (esempio. <SMTP.DIBRIS.UNIGE.IT><CR><LF>)

Il primo comando che il client può dare è "HELO", con l'indirizzo del client (DIBRIS.UNIGE.IT). Il server risponde con 250. Il comando successivo potrebbe essere "MAIL FROM:" con l'indirizzo del mittente (quindi indirizzo del client + user) (esempio. GIULIA@DIBRIS.UNIGE.IT). Il server risponde di nuovo



con 250 (che significa OK), poi "RCPT TO:" + indirizzo destinatario. Client risponde con 250 e poi con il comando "DATA" -> il messaggio da inviare. Risposta 354 -> "OKAY, MI ASPETTO IL MESSAGGIO". Ricevuto il messaggio, il server risponde con 250, poi client usa "QUIT" e il server risponde 221 (arrivederci).

Quindi a questo punto il server prova a instaurare una connessione con l'altro server; se fallisce, arriva notifica al mittente

Solo il proprietario di mailbox può accedervi, deve autenticarsi.

Subito l'autenticazione non era richiesta al mittente, ma questo crea problemi di sicurezza: uno può connettersi a server e mandare enorme quantità di messaggi (SPAM); ora i server non accettano connessioni da client sconosciuti. Ogni client ha uno o più di un server di posta elettronica dedicati a lui, che accettano connessioni solo da client che ne hanno diritto -> comunicazione server-server filtrata con white e black list

L'autenticazione può avvenire o ad apertura di connessione o in protocollo SMTP, usando la versione estesa del protocollo -> ESMTP, con comandi estesi (esempio. "HELO" ha versione "EHLO", che dà la possibilità di cifrare i dati)