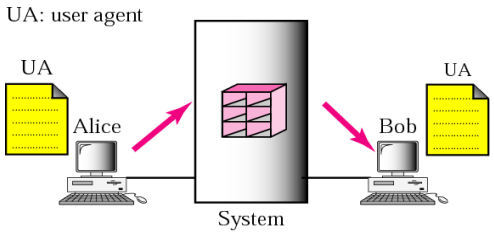
Protocoale de nivel aplicaţie:

SMTP, POP, IMAP

Arhitectura SMTP

4 scenarii în schimbul de e-mail; al 4-lea e cel mai comun.

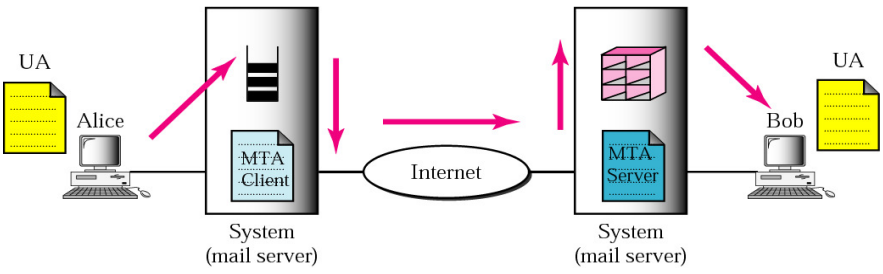
Scenariul 1



2 UA necesari cînd expeditorul/destinatarul sînt pe acelaşi sistem

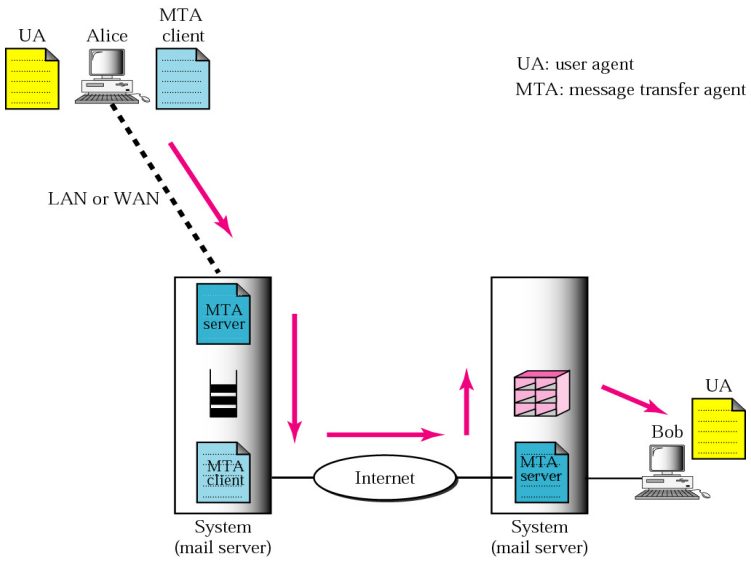
Scenariul 2

UA: user agent
MTA: message transfer agent



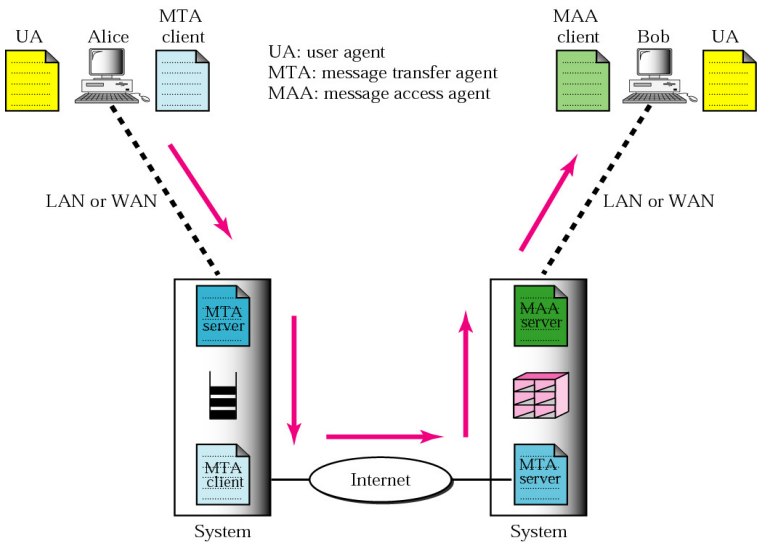
Cînd E şi D sînt pe sisteme diferite, sînt necesare 2 UA şi 2 MTA

Scenariul 3



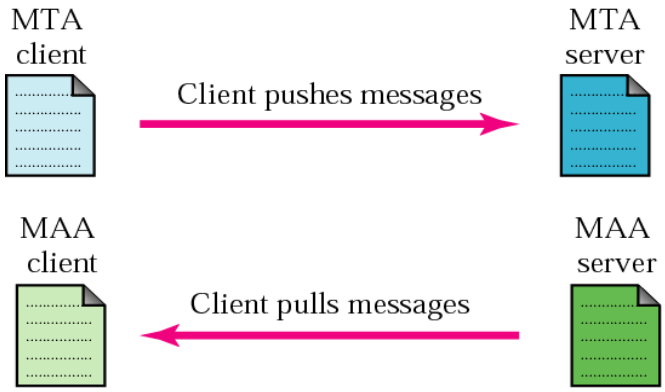
Cînd E e conectat la mail server prin LAN/WAN, sînt necesare 2 UA şi 2 MTA

Scenariul 4

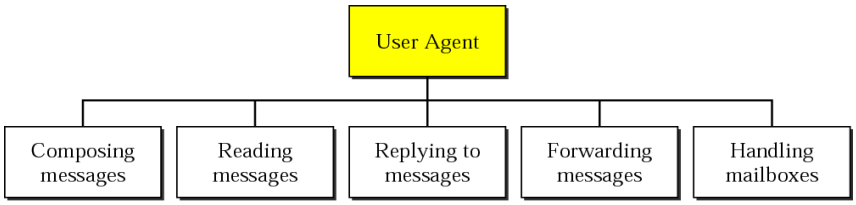


cînd atît E cît şi D sînt conectaţi prin intermediul LAN/WAN, sînt necesari 2 UA, 2 MTA, 2 MAA

MTA vs MAA: Push vs. pull



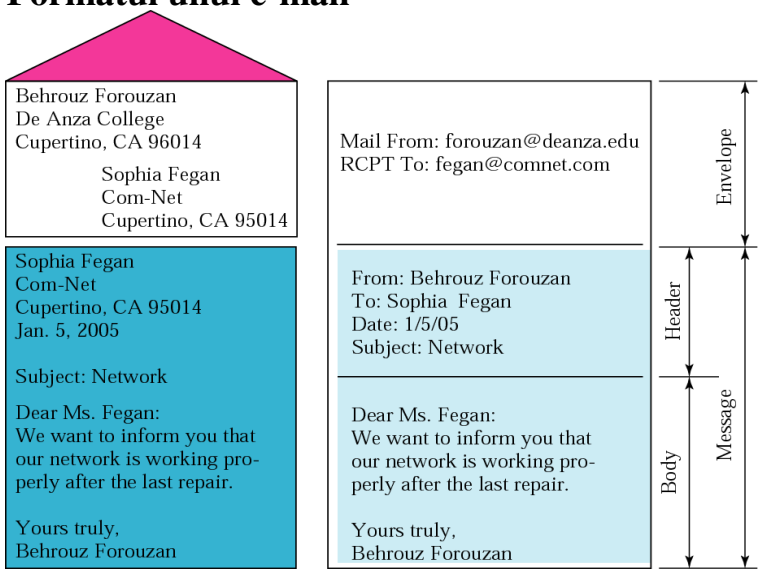
UA: roluri



***UA* asigură serviciul de expediere/recepţie a mesajului**

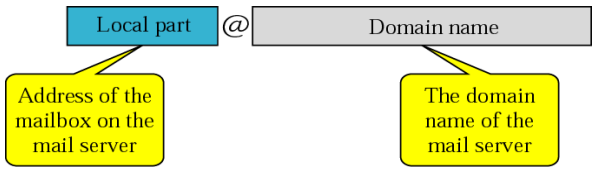
UA command-line (CLI): mail, elm, pine, alpine, mutt, ... (pe UNIX)
UA grafice: MS Outlook, Eudora, Netscape Mail, Thunderbird, ...

Formatul unui e-mail



Poştă clasică: plic+conţinut e-mail

Adresa de e-mail; Mail Exchanger



Q: Cine este "serverul" corespunzător unui domeniu ?
A: *mail exchanger*-ul (MX)

#NAME	TTL	IN	TYPE	ADR	
example.com.		IN	A	69.9.64.11	
www1.example.com.		IN	A	69.9.64.12	
server1.example.com.		IN	A	69.9.64.15	
example.com.	14400	IN	MX	0	example.com.
example.com.	14400	IN	MX	30	server1.example.com.

Demonstraţie practică: aflarea MX-ului folosind *nslookup* cu *set type=MX*

Adresa de e-mail; Mail Exchanger

Demonstraţie practică: aflarea MX-ului folosind *nslookup* cu *set type=MX*

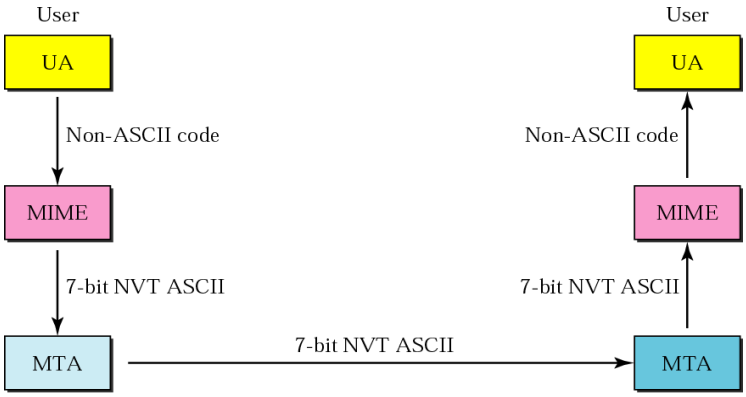
```
root@matrix:~# nslookup
> yahoo.com
Server:         141.85.43.10
Address:        141.85.43.10#53

Non-authoritative answer:
Name:   yahoo.com
Address: 206.190.36.45
Name:   yahoo.com
Address: 98.138.253.109
Name:   yahoo.com
Address: 98.139.183.24
```

Adresa de e-mail; Mail Exchanger

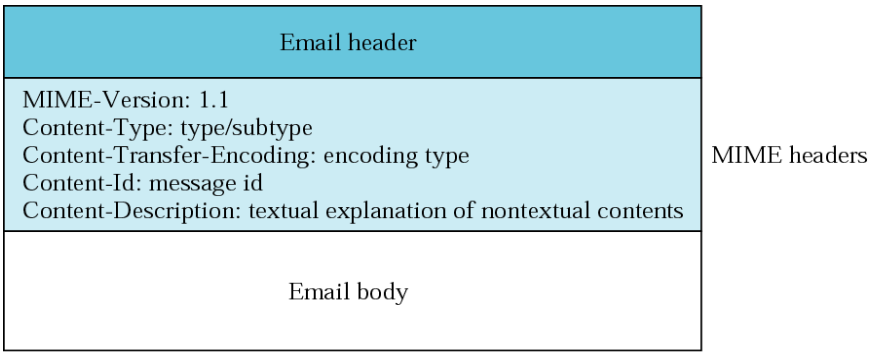
Demonstraţie practică: aflarea MX-ului folosind *nslookup* cu *set type=MX*

```
> set type=MX
> yahoo.com
Server:         141.85.43.10
Address:        141.85.43.10#53

Non-authoritative answer:
yahoo.com       mail exchanger = 1 mta7.am0.yahoodns.net.
yahoo.com       mail exchanger = 1 mta5.am0.yahoodns.net.
yahoo.com       mail exchanger = 1 mta6.am0.yahoodns.net.

Authoritative answers can be found from:
yahoo.com       nameserver = ns6.yahoo.com.
yahoo.com       nameserver = ns1.yahoo.com.
yahoo.com       nameserver = ns5.yahoo.com.
yahoo.com       nameserver = ns4.yahoo.com.
yahoo.com       nameserver = ns2.yahoo.com.
yahoo.com       nameserver = ns3.yahoo.com.
ns1.yahoo.com   internet address = 68.180.131.16
ns2.yahoo.com   internet address = 68.142.255.16
ns3.yahoo.com   internet address = 203.84.221.53
ns3.yahoo.com   has AAAA address 2406:8600:b8:fe03::1003
ns4.yahoo.com   internet address = 98.138.11.157
ns5.yahoo.com   internet address = 119.160.247.124
ns6.yahoo.com   internet address = 121.101.144.139
ns6.yahoo.com   has AAAA address 2406:2000:108:4::1006
```

MIME



Header MIME



Tipuri şi subtipuri de date în MIME

Type	*Subtype*	*Description*
Text	Plain	Unformatted
	HTML	HTML format (see Chapter 22)
Multipart	Mixed	Body contains ordered parts of different data types
	Parallel	Same as above, but no order
	Digest	Similar to Mixed, but the default is message/RFC822
	Alternative	Parts are different versions of the same message

Tipuri şi subtipuri de date în MIME (cont.)

Type	*Subtype*	*Description*
Message	RFC822	Body is an encapsulated message
	Partial	Body is a fragment of a bigger message
	External-Body	Body is a reference to another message
Image	JPEG	Image is in JPEG format
	GIF	Image is in GIF format
Video	MPEG	Video is in MPEG format
Audio	Basic	Single channel encoding of voice at 8 KHz
Application	PostScript	Adobe PostScript
	Octet-stream	General binary data (eight-bit bytes)

Tipuri de Content-transfer-encoding

Type	*Description*
7bit	NVT ASCII characters and short lines
8bit	Non-ASCII characters and short lines
Binary	Non-ASCII characters with unlimited-length lines
Base64	6-bit blocks of data are encoded into 8-bit ASCII characters
Quoted-printable	Non-ASCII characters are encoded as an equal sign followed by an ASCII code

Conţinut non-text în e-mail

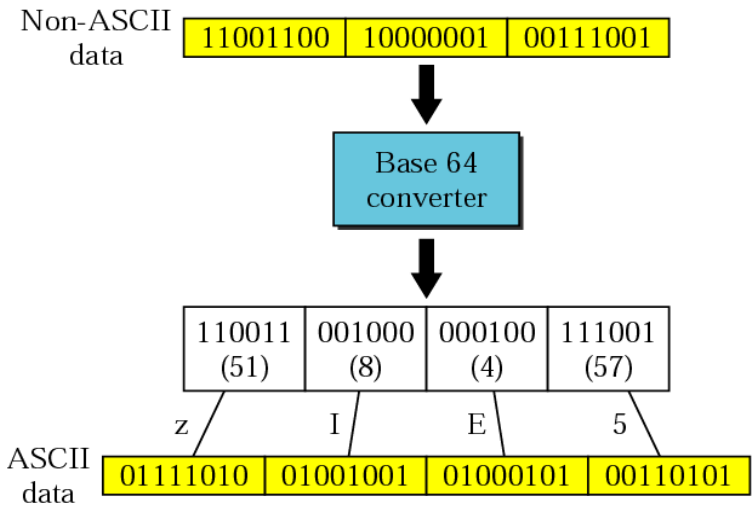
- Textul simplu poate fi transmis (ASCII, original 7 biţi)
- Ceea ce nu e text simplu (coduri 0..255 = conţinut binar: imagini, documente word, etc) se converteşte în ASCII

  – original: uuencode
  – ulterior: MIME, utilizează BASE64 encoding (RFC 2045)
    - schemă de conversie binar -> text
    - caractere permise A-Z, a-z,0-9, +,/
    - schema:
    - 3 octeţi de date (24 biţi)
      – se extrag 4 grupe de 6 biţi
      – fiecare valoare este folosită ca index în:

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/

      – se obţin 4 caractere ASCII

Base64



Index Base64

Value	*Code*	*Value*	*Code*	*Value*	*Code*	*Value*	*Code*	*Value*	*Code*	*Value*	*Code*
0	**A**	11	**L**	22	**W**	33	**h**	44	**s**	55	**3**
1	**B**	12	**M**	23	**X**	34	**i**	45	**t**	56	**4**
2	**C**	13	**N**	24	**Y**	35	**j**	46	**u**	57	**5**
3	**D**	14	**O**	25	**Z**	36	**k**	47	**v**	58	**6**
4	**E**	15	**P**	26	**a**	37	**l**	48	**w**	59	**7**
5	**F**	16	**Q**	27	**b**	38	**m**	49	**x**	60	**8**
6	**G**	17	**R**	28	**c**	39	**n**	50	**y**	61	**9**
7	**H**	18	**S**	29	**d**	40	**o**	51	**z**	62	+
8	**I**	19	**T**	30	**e**	41	**p**	52	**0**	63	/
9	**J**	20	**U**	31	**f**	42	**q**	53	**1**		
10	**K**	21	**V**	32	**g**	43	**r**	54	**2**		

exemplu codare BASE64

text original:

Man is distinguished, not only by his reason, but by this singular passion from other animals, which is a lust of the mind, that by a perseverance of delight in the continued and indefatigable generation of knowledge, exceeds the short vehemence of any carnal pleasure.

BASE64:

TWFuIGlzIGRpc3Rpbmd1aXNoZWQsIG5vdCBvbmx5IGJ5IGhpcyByZWFzb24sIGJ1dCBieSB0
aGlzIHNpbmd1bGFyIHBhc3Npb24gZnJvbSBvdGhlciBhbmltYWxzLCB3aGljaCBpcyBhIGx1
c3Qgb2YgdGhlIG1pbmQsIHRoYXQgYnkgYSBwZXJzZXZlcmFuY2Ugb2YgZGVsaWdodCBpbiB0
aGUgY29udGludWVkIGFuZCBpbmRlZmF0aWdhYmxlIGdlbmVyYXRpb24gb2Yga25vd2xlZGdl
LCBleGNlZWRzIHRoZSBzaG9ydCB2ZWhlbWVuY2Ugb2YgYW55IGNhcm5hbCBwbGVhc3VyZS4=

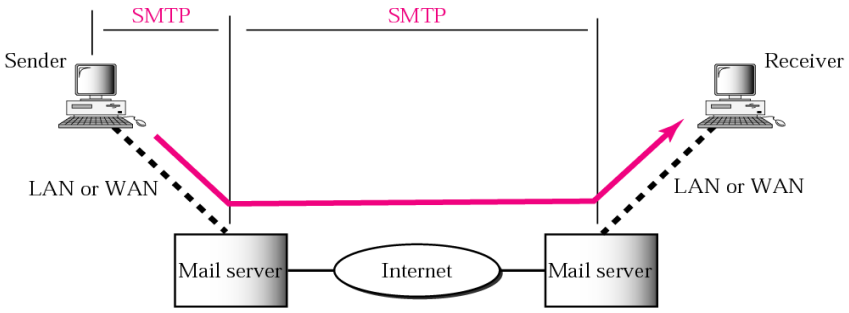
MESSAGE TRANSFER AGENT (MTA): SMTP

MTA implementează protocolul SMTP care realizează transferul propriu-zis de e-mailuri.

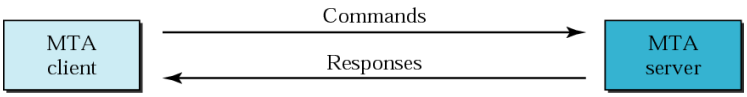
Cuprins:

- ***Comenzi/răspunsuri***
- ***Faze ale transferului de mail***

domeniul de lucru al SMTP



Comenzi/răspunsuri



Formatul comenzilor:

Keyword:argument(s)

Keywords

Keyword	*Argument(s)*
HELO	Sender's host name
MAIL FROM	Sender of the message
RCPT TO	Intended recipient of the message
DATA	Body of the mail
QUIT	
RSET	
VRFY	Name of recipient to be verified
NOOP	
TURN	
EXPN	Mailing list to be expanded
HELP	Command name
SEND FROM	Intended recipient of the message
SMOL FROM	Intended recipient of the message
SMAL FROM	Intended recipient of the message

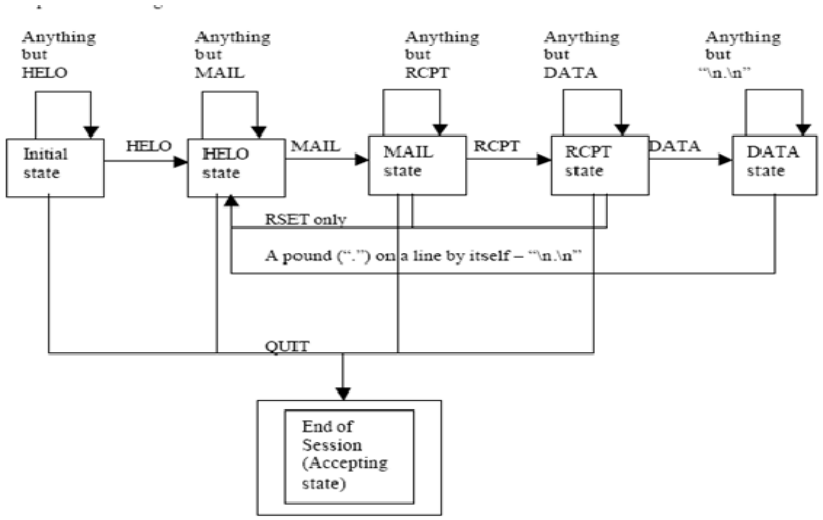
Răspunsuri

Code	*Description*
Positive Completion Reply	
211	System status or help reply
214	Help message
220	Service ready
221	Service closing transmission channel
250	Request command completed
251	User not local; the message will be forwarded
Positive Intermediate Reply	
354	Start mail input
Transient Negative Completion Reply	
421	Service not available
450	Mailbox not available
451	Command aborted: local error
452	Command aborted; insufficient storage

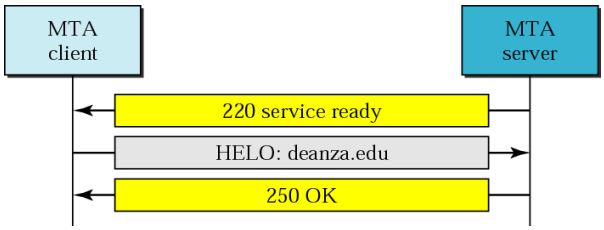
Răspunsuri

Permanent Negative Completion Reply	
500	Syntax error; unrecognized command
501	Syntax error in parameters or arguments
502	Command not implemented
503	Bad sequence of commands
504	Command temporarily not implemented
550	Command is not executed; mailbox unavailable
551	User not local
552	Requested action aborted; exceeded storage location
553	Requested action not taken; mailbox name not allowed
554	Transaction failed

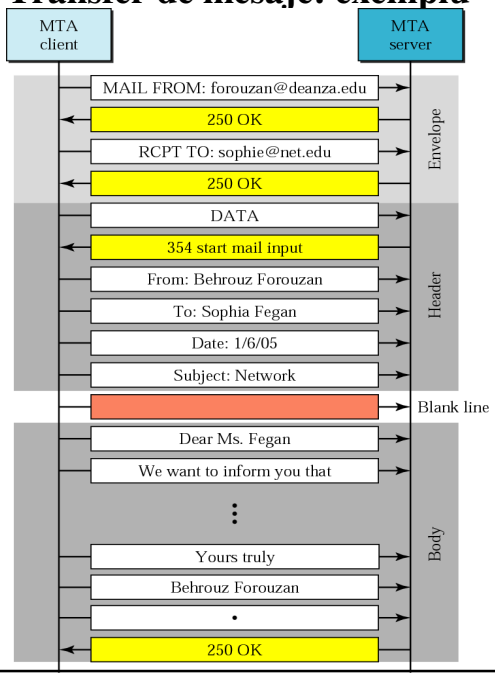
Diagrama de stare SMTP



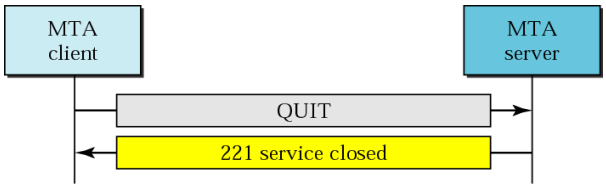
Faza 1: Stabilirea conexiunii



Faza 2: Transfer de mesaje: exemplu



Faza 3: Încheierea conexiunii



Demonstraţie practică !

MTA server: *postfix* (linux)
MTA client: *telnet* (comenzi manuale) pe portul 25
Schimb manual de mesaje

UA local: *alpine* (linux)

Demonstraţie folosind *telnet*

MTA server: *postfix* (linux)
MTA client: *telnet* (comenzi manuale) pe portul 25

```
telroot@matrix:~# telnet localhost 25
Trying ::1...
Connected to localhost.
Escape character is '^]'.
220 matrix ESMTP Postfix (Ubuntu)
mail from: ms@elcom.pub.ro
250 2.1.0 Ok
rcpt to: asi1@matrix.elcom.pub.ro
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
From: Studentu Cutare
Subject: test

mail de test
.
250 2.0.0 Ok: queued as DF94192146
quit
221 2.0.0 Bye
Connection closed by foreign host.
root@matrix:~#
```

MESSAGE ACCESS AGENT (MAA): POP şi IMAP

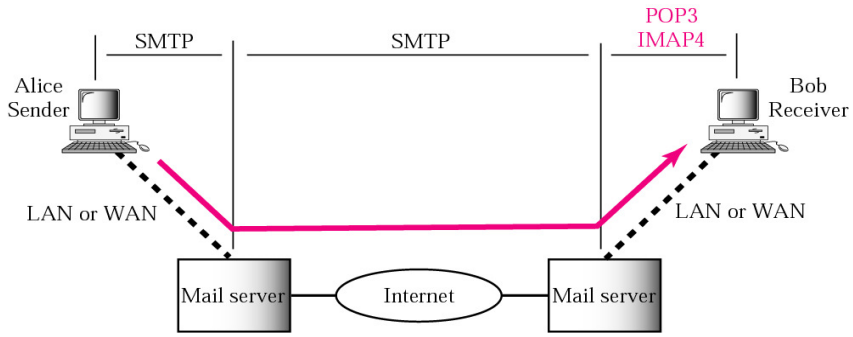
Etapa finală (opţională) în lanţul parcurs de e-mail: folosirea unui MAA pentru extragerea (pull) mesajului de pe server

OBS: în exemplul precendent (local), nu se foloseşte un MAA căci UA rulează chiar pe server.

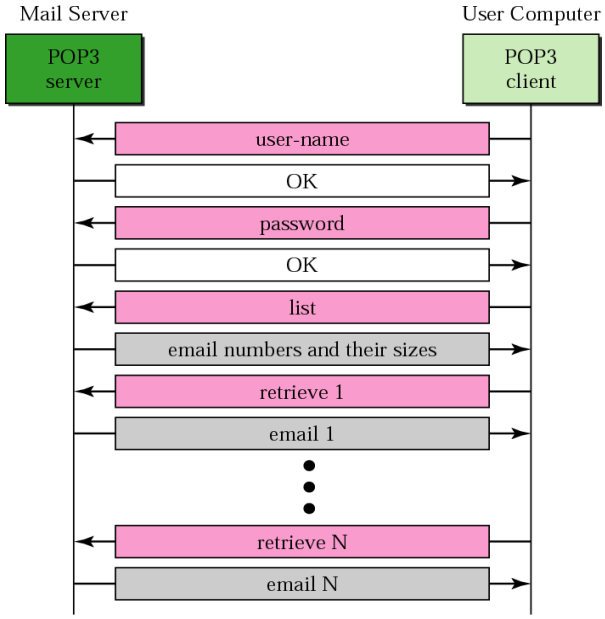
Protocoale pentru MAA:

POP3 (Post Office Protocol v. 3)
IMAP4 (Internet Mail Access Protocol v. 4)

POP3, IMAP4



POP3



Protocol POP3 (tcp: port 110)

faza de autorizare

- comenzi client:
  - **user:** declare username
  - **pass:** password
- răspunsuri server
  - **+OK**
  - **-ERR**

faza de tranzacţie, client:

- **list:** list message numbers
- **retr:** retrieve message by number
- **dele:** delete
- **quit**

Exemplu de secvenţă de comenzi Client-Server

```
S: +OK POP3 server ready
C: user bob
S: +OK
C: pass hungry
S: +OK user conectat cu succes
```

```
C: list
S: 1 498
S: 2 912
S: .
C: retr 1
S: <message 1 contents>
S: .
C: dele 1
C: retr 2
S: <message 1 contents>
S: .
C: dele 2
C: quit
S: +OK Deconectare server POP3
```

Lungime(bytes)

POP3: Comenzi

Command	Description
QUIT	Initiates session termination
STAT	Requests a “drop listing” indicating number of messages and size of the mail store
LIST [msg]	Requests a “scan listing” for specified or all message(s) indicating message number and size of the message
RETR msg	Retrieves specified message
DELE msg	Marks specified message as deleted
NOOP	No operation
RSET	Resets initial state by unmarking deleted messages
TOP msg n	Retrieves specified message’s headers and top n lines of body
UIDL [msg]	Requests a “unique-id listing” for specified or all message(s) indicating message number and unique ID of the message
USER name	Specifies username for USER/PASS authentication
PASS password	Specifies password for USER/PASS authentication
APOP name digest	Specifies MD5-based authentication credentials

POP3: Faza de autorizare

- Începe după transmisia mesajului de 1 linie:

```
+OK POP3 server ready
```

- Autentificare client - variante:
  - USER/PASS – Plaintext authentication
  - APOP – MD5 digest “encryption”
  - AUTH – Alternate authentication mechanism *(RFC 1734)*
- Dacă autentificare eşuează, se poate repeta sau clientul trimite un mesaj QUIT
- Succesul autentificării: începutul fazei de tranzacţie

Autentificare 1: USER/PASS

- Plaintext authentication (username şi password)
- Simplu, nesigur (parola în clar)

```
+OK POP3 server ready
USER cfugDemo@evoch.com
+OK cfugDemo@evoch.com
PASS cfugDemo123
+OK 0 messages 0 octets
```

```
+OK POP3 server ready
USER cfugDemo@evoch.com
+OK cfugDemo@evoch.com
PASS hack
-ERR Unknown user or incorrect password
```

Autentificare 2: APOP

- username şi MD5 hashed password
- Serverul indică suportul pentru APOP trimiţând un timestamp în mesajul de întîmpinare (⇨); clientul şi serverul cunosc amîndoi parola *mypass*
- Clientul va aplica MD5 pe şirul `<2004........>mypass`

  şi va obţine hashul `786b5c12203b391c9a903b515ce65a12`
- Serverul va compara cu hash-ul generat local

```
S: +OK POP3 server ready  Wed, 18 Aug 2004 15:05:27 -0400
⇨ <20040818150527@email02.mywebmailserver.com>
C: APOP cfugDemo@evoch.com 786b5c12203b391c9a903b515ce65a12
S: +OK 1 messages 458 octets
```

Autentificare 3: AUTH

- Specificat în RFC 1734, “POP3 AUTHentication Command,” permite autentificarea IMAP4 în POP3
- Mecanism de autentificare sigur

```
+OK POP3 server ready
AUTH KERBEROS_V4
+ AmFYig==
BAcAQU5EUkVXLkNNVS5FRFUAOCAsho84kLN3/IJmrMG+25a4DT
+nZImJjnTNHJUtxAA+o0KPKfHEcAFs9a3CL5Oebe/ydHJUwYFd
WwuQ1MWiy6IesKvjL5rL9WjXUb9MwT9bpObYLGOKi1Qh
+ or//EoAADZI=
DiAF5A4gA+oOIALuBkAAmw==
+OK Kerberos V4 authentication successful
```

POP3: Faza de tranzacţie

- Serverul asignează un număr de mesaj pt. fiecare mesaj; numărul este constant tot timpul sesiunii
- comenzi/răspunsuri
- Comanda QUIT de la client termină această fază (serverul intră în starea UPDATE în care îşi actualizează folderul de mesaje)

Comanda STAT

- “Drop listing” ca răspuns de la server: codul OK, numărul de mesaje, dimensiunea folderului de mesaje

```
STAT
+OK 2 2068
```

Comanda LIST

- Comanda cere o listă cuprinzînd numărul şi dimensiunea mesajelor (specificate/toate)

```
LIST
+OK 2 messages 2068 octets
1 1015
2 1053
.
```

```
LIST 2
+OK 2 1053
```

Comanda RETR

- Cere transmiterea mesajului cu numărul respectiv

```
RETR 1
+OK 1015 octets
From: “John Doe" <john.doe@evoch.com>
To: <cfugDemo@evoch.com>
Subject: Test Message #1
Date: Wed, 18 Aug 2004 15:58:32 -0400
[... more headers ...]

12345
.
```

```
RETR 3
-ERR No such message
```

Comanda DELE

- marchează mesajul pentru ştergere
- ştergerea se face doar după QUIT (starea UPDATE)
- Folosind RSET se anulează ştergerea

```
DELE 1
+OK Message deleted
```

Comanda NOOP

- Folosit ca keep-alive

```
NOOP
+OK
```

Comanda RSET

- Resetează sesiunea, anulează efectele DELE

```
RSET
+OK
```

Comanda QUIT

- încheie sesiunea
- Serverul intră în UPDATE dacă comanda QUIT s-a dat în faza de tranzacţie, nu şi în faza de autorizare.

```
QUIT
+OK POP3 server closing connection
```

Comanda TOP

- Listează headerele şi primele 3 linii ale mesajelor

```
TOP 2 3
+OK 1053 octets
From: “John Doe" <john.doe@evoch.com>
To: <cfugDemo@evoch.com>
Subject: Test Message #1
Date: Wed, 18 Aug 2004 15:58:32 -0400
[... more headers ...]

1st line
2nd line
3rd line
.
```

Comanda UIDL

- solicită “unique-id listing” adică corespondenţa număr mesaje - ID unic de pe server
- comandă opţională

```
UIDL
+OK
1 20040818155839E5E3
2 20040818155912E640
.
```

```
UIDL 2
+OK 2 20040818155912E640
```

Demonstraţie folosind *telnet*

```
telnet: > telnet pop.example.com 110
telnet: Trying 192.0.2.2...
telnet: Connected to pop.example.com.
telnet: Escape character is '^]'.
server: +OK InterMail POP3 server ready.
client: USER MyUsername
server: +OK please send PASS command
client: PASS MyPassword
server: +OK MyUsername is welcome here
client: LIST
server: +OK 1 messages
server: 1 1801
server: .
client: RETR 1
server: +OK 1801 octets
server: Return-Path: sender@example.com
server: Received: from client.example.com ([192.0.2.1])
server:         by mx1.example.com with ESMTP
server:         id <20040120203404.CCCC18555.mx1.example.com@client.example.com>
server:         for <recipient@example.com>; Tue, 20 Jan 2004 22:34:24 +0200
server: From: sender@example.com
server: Subject: Test message
server: To: recipient@example.com
server: Message-Id: <20040120203404.CC18555.mx1.example.com@client.example.com>
server:
server: This is a test message.
server: .
client: DELE 1
server: +OK
client: quit
server: +OK MyUsername InterMail POP3 server signing off.
```

POP3: resurse

- rfc1939.txt – “Post Office Protocol - Version 3”
- rfc2384.txt – “POP URL Scheme”
- rfc2449.txt – “POP3 Extension Mechanism”
- rfc1734.txt – “POP3 AUTHentication command”
- rfc2195.txt – “IMAP/POP AUTHorize Extension for Simple Challenge/Response”
- rfc3206.txt – “The SYS and AUTH POP Response Codes”
- rfc2595.txt – “Using TLS with IMAP, POP3 and ACAP”
- rfc1321.txt – “MD5 Algorithm”
- rfc1521.txt – “MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies”
- rfc2045.txt - “Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies”

IMAP vs POP3

- Cu IMAP, mesajele stau pe server în foldere diferite, eventual create de utilizator; astfel, un utilizator îşi poate accesa mailul de pe orice calculator şi îşi poate vedea mailul sub aceeaşi formă şi organizare. Toate schimbările în mesaje/foldere se salvează pe server.
- În POP3 toate mesajele sînt ţinute pe server în folderul INBOX. Mailul din folder este transmis pe calculatorul local, unde poate fi aranjat în foldere locale. Pe fiecare calculator local al utilizatorului (dacă este cazul) acesta trebuie să-şi creeze foldere.
- Cu POP3 doar mesajele sînt pe server, cu IMAP sînt mesajele+folderele
- POP3 nu permite transferul parţial al mesajelor. Cu IMAP se pot transfera doar porţiuni de mesaje (de exemplu nu se transferă ataşamentele care nu ne interesează, se şterg direct pe server).

Bibliografie

- TCP/IP Protocol suite: *Electronic Mail: SMTP, POP, and IMAP*
- Behrouz Forouzan, *Cryptography and network security*, McGraw-Hill
- Mosh Teitelbaum , *ColdFusion Foundations: POP3*