



Curs 5

E-mail

Gestiunea serviciilor de rețea (GSR)
3 noiembrie 2016

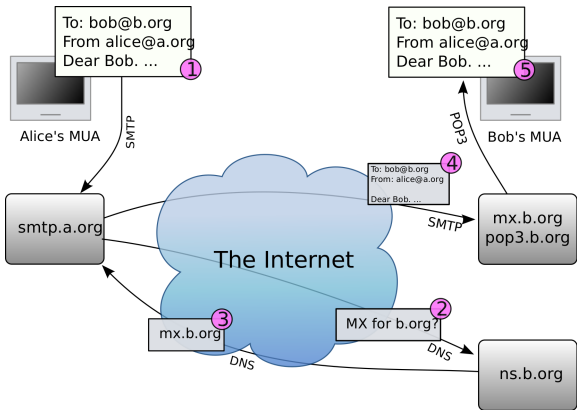
Departamentul de Calculatoare, Comunitatea RLUG

SMTP/ESMTP

POP3 / IMAP4

Implementari specifice: Postfix (MTA) si Dovecot

- ▶ Protocol client/server pentru trimiterea de mesaje de tip e-mail peste rețea
- ▶ Plain-text (comenzile se dau în mod text, câte una pe linie)
- ▶ A fost definit de Jon Postel în 1982 în RFC821
- ▶ Extins în 1995 prin RFC1869 și a devenit ESMTP, ultima revizie fiind făcută în RFC5321 în 2008
- ▶ Porturi folosite:
 - ▶ 25/TCP — SMTP/ESMTP
 - ▶ 465/TCP — SMTPS (SMTP Secure)
 - ▶ 587/TCP — Mail Submission



- ▶ Livrarea între MTA-uri se face printr-un mecanism asincron de tip "store-and-forward"

```
S: 220 smtp.example.com ESMTP Postfix
C: EHLO relay.example.org
S: 250 Hello relay.example.org, I am glad to meet you
S: 250-SIZE 157286400
S: 250-8BITMIME
S: 250-STARTTLS
S: 250-ENHANCEDSTATUSCODES
S: 250-PIPELINING
C: MAIL FROM:<bob@example.org>
S: 250 OK
C: RCPT TO:<alice@example.com>
S: 250 OK
C: RCPT TO:<theboss@example.com>
S: 250 OK
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: "Homer Simpson" <homer@example.org>
C: To: "Marge Simpson" <marge@example.org>
C: Cc: bart@simpson.com
C: Date: Tue, 15 January 2008 16:02:43 -0500
C: Subject: Test message
C:
C: Hello Marge.
C: This is a test message with 5 header fields and 4 lines in the message body.
C: Your husband,
C: Homer
C: .
S: 250 OK: queued as 12345
C: QUIT
S: 221 Bye
```

- ▶ "Internet Message Format" - RFC822/2822/5322
- ▶ Headers + body: ASCII only, linii de 78-998 caractere
 - ▶ Atașamentele binare sunt transmise codat folosind base64
- ▶ MIME (Multipurpose Internet Mail Extensions) definit în RFC 2045-2049
 - ▶ Atașamente non text (imagini, video, documente)
 - ▶ Corpul mesajelor format din mai multe părți (text/plain, application/octet-stream etc.)

- ▶ Codurile de stare sunt împărțite în clase:
 - ▶ 2XX: Status / Succes
 - ▶ 3XX: Informaționale
 - ▶ 4XX: Erori temporare (persistente)
 - ▶ 5XX: Erori permanente
- ▶ O listă a codurilor de status se regăsește în RFC3463

- ▶ MUA — Mail User Agent
- ▶ MTA — Mail Transport Agent
- ▶ MDA — Mail Delivery Agent

- ▶ Se folosește la securizarea transportului între două MTA
- ▶ Folosește certificate digitale X.509
- ▶ Verificarea capabilității STARTTLS a unui MTA
 - S: 220 mx.google.com ESMTP a127si11581079wme.65 -
gsmtip
 - C: EHLO me
 - S: ...
 - S: 250-STARTTLS
 - S: ...

- ▶ Protocolul ESMTP permite autentificarea expeditorilor
 - ▶ La conectarea clientului, severul îi prezintă acestuia metodele de autentificare suportate

S: 250-AUTH LOGIN PLAIN XOAUTH2
PLAIN-CLIENTTOKEN OAUTHBEARER XOAUTH

- ▶ Cea mai folosită metodă este AUTH PLAIN
 - ▶ Transmitere utilizator/parolă:
base64(username\0username\0password)

C: AUTH PLAIN dGVzdAB0ZXN0AHRlc3RwYXNz
S: 235 Authentication successful

Demo ESMTP și STARTTLS

SMTP/ESMTP

POP3 / IMAP4

Implementari specifice: Postfix (MTA) si Dovecot

- ▶ ... Post Office Protocol versiunea 3
- ▶ Protocol plain text, port 110/TCP în clar, 995/TCP securizat TLS
- ▶ Utilizat pentru citirea mesajelor de pe un server și descărcarea lor local

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

- ▶ ... Internet Message Access Protocol versiunea 4 (rev1)
- ▶ Protocol plain text, port 143/TCP în clar, 993/TCP securizat TLS
- ▶ Utilizat pentru citirea mesajelor de pe un server (fără a fi descărcate local)
- ▶ Are noțiunea de folders

```
S: * OK Dovecot ready.
C: a1 LOGIN MyUsername MyPassword
S: a1 OK Logged in.
C: a2 LIST "" "*"
S: * LIST (\ HasNoChildren) "." "INBOX"
S: a2 OK List completed.
C: a3 EXAMINE INBOX
S: * FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
S: * OK [PERMANENTFLAGS ()] Read-only mailbox.
S: * 1 EXISTS
S: * 1 RECENT
S: * OK [UNSEEN 1] First unseen.
S: * OK [UIDVALIDITY 1257842737] UIDs valid
S: * OK [UIDNEXT 2] Predicted next UID
S: a3 OK [READ-ONLY] Select completed.
C: a4 FETCH 1 BODY[]
S: * 1 FETCH (BODY[] 405
S: Return-Path: sender@example.com
S: Received: from client.example.com ([192.0.2.1])
S:         by mx1.example.com with ESMTP
S:         ...
S: From: sender@example.com
S: Subject: Test message
S: To: recipient@example.com
S: ...
S: a4 OK Fetch completed.
C: a5 LOGOUT
S: * BYE Logging out
S: a5 OK Logout completed.
```


- ▶ Acceptă sau nu mesaje ca server de (E)SMTP
- ▶ Decide unde să le trimită (rutarea mesajelor)
 - ▶ Livrare către alte servere (E)SMTP (ca și client)
 - ▶ Livrare locală (via un MDA sau direct în Mailbox)
 - ▶ Drop (generează un DSN (Delivery Status Notification))
- ▶ Are logică de retry (exponential backoff)

- ▶ ... Mail Delivery Agent
- ▶ Se ocupă de livrarea mesajelor SMTP intr-o structură potrivită pentru citirea de către utilizatori
- ▶ Poate fi parte a MTA-ului final sau un program separat (ex: procmail)

- ▶ Mailbox cunoscut și sub numele de mbox
- ▶ Maildir
- ▶ cyrus-imap

- ▶ E-mailul face ușoară și ieftină comunicarea unidirecțională ⇒ devine rentabil abuzul
- ▶ Imposibilă categorisirea obiectivă, ca atare au apărut diverse mecanisme de combatere:
 - ▶ Mecanisme de autentificare a expeditorului (rDNS, SPF, DKIM, DMARC etc.)
 - ▶ Mecanisme de verificare a reputației expeditorului (RBL)
 - ▶ Analizoare de SPAM

- ▶ Datorită funcționalității multi-hop a SMTP, un server poate fi exploatat pentru a livra e-mailurile unui terț răuvoitor
- ▶ Open Relay

SMTP/ESMTP

POP3 / IMAP4

Implementari specifice: Postfix (MTA) si Dovecot

- ▶ MTA scris de Wietse Zweitze Venema și contributori
- ▶ Foarte versatil, modular și performant
- ▶ Arhitectura sa este bazată pe filosofia Unix "do one thing and do it well"
- ▶ Directorul de configurare: `/etc/postfix`
 - ▶ `main.cf` — fișierul de configurare a opțiunilor
 - ▶ formatul este de forma: `cheie = valoare`
 - ▶ `master.cf` — fișierul de configurare pentru suita de daemoni ce compun postfix
- ▶ Se poate integra cu MySQL, PostgreSQL, (Open)LDAP, `cyrus-imap` etc.

Demo

- ▶ Dovecot este un server de POP3(S) și IMAP(S)
- ▶ Se poate integra cu MySQL, PostgreSQL sau (Open)LDAP pentru autentificarea utilizatorilor
- ▶ Directorul de configurare: /etc/dovecot
 - ▶ `dovecot.conf` — fișierul principal de configurare
 - ▶ `conf.d/imap.conf` — fișier de configurare pentru un serviciu (ex: IMAP)

Demo