

Mensajería en Internet (E-Mail)

Andres Barbieri

Marzo 2016

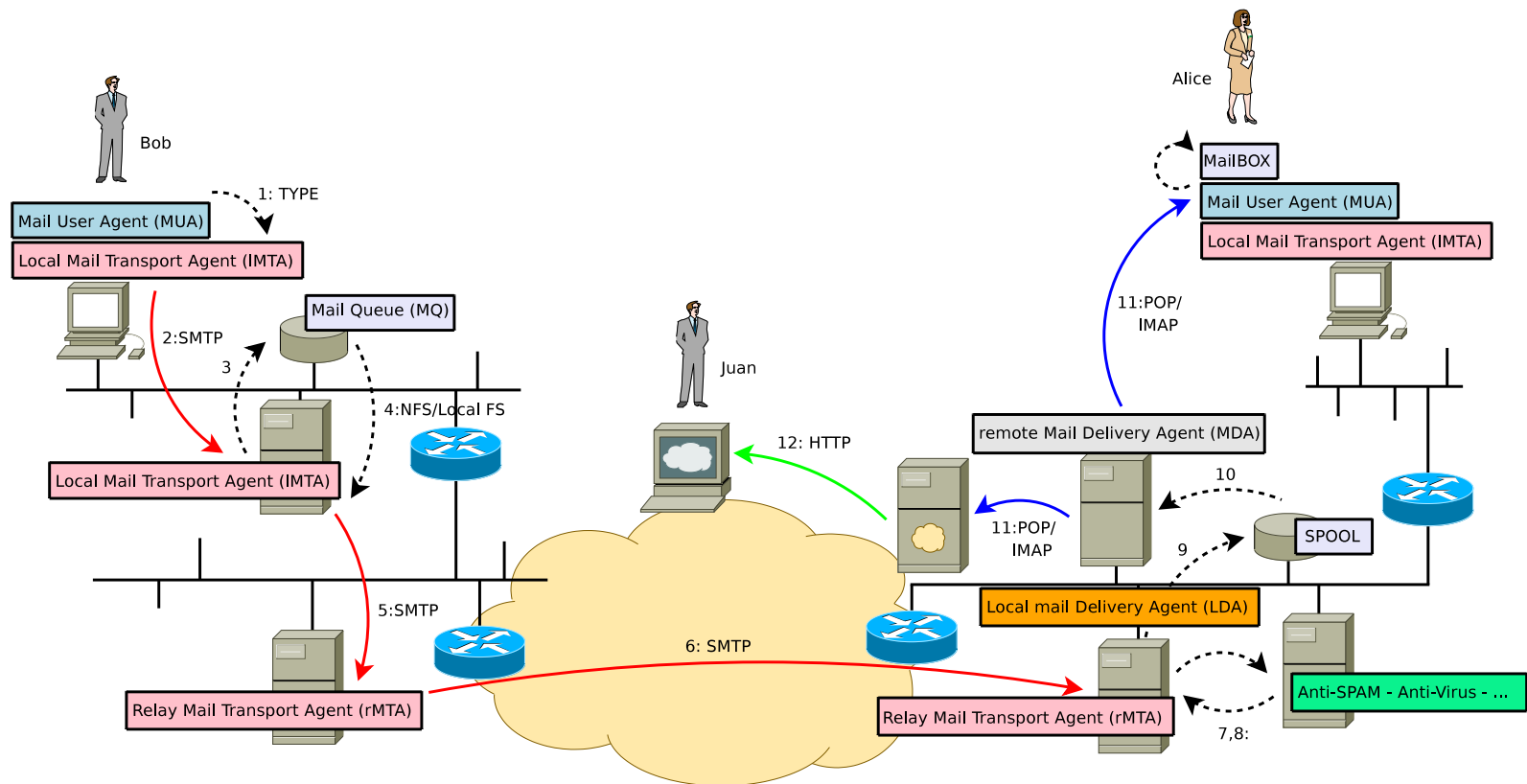


0-0

Introducción

- Uno de los primeros servicios de Internet.
- Creado por Ray Tomlinson en 1971.
- Primeros protocolos de transporte UUCP (Unix-to-Unix Copy).
- Conexiones vía módems.
- Formato de Email: MACH2!MACH1!USER.
- En 1972: Se escoge el símbolo “@” para denotar “en”, “at”.
- Casilla de Email: USER@FQDN-DOMAIN o USER@FQDN-SERVER.
- En 1982: surge SMTP.
- En 1988: Gusano Morris, primer Virus, usaba el Sendmail.

Arquitectura



Arquitectura (Cont'd)

- Componentes Principales:
 - MUA (Mail User Agent).
 - MTA (Mail Transport Agent).
 - MDA (Mail Delivery Agent).
- Componentes Secundarias:
 - Servidor de Autenticación.
 - Web Mail (Front-End WWW).
 - Servidor de Anti-Virus, Anti-SPAM, ...
 - Servidores de Listas.

Arquitectura (MUA)

- Cliente.
- Lector/Emisor Local de Correo.
- Escritura, edición, lectura de mensajes de correos (Mails).
- Ejemplos: Eudora, MS Outlook, Mozilla Thunderbird, elm, pine, mutt.
- Web-mailers: Horde/IMP, Squirrel, GMAIL, Yahoo, Hotmail.
- Interfaz con el usuario.
- Poseen un LMTA para comunicarse con el Servidor de Mail Saliente.
- Utilizan protocolos SMTP, POP, IMAP, habla con MTA y con MDA.

Arquitectura (MTA)

- Cliente y Servidor.
- Se encarga de enviar el mensaje de mail al servidor donde está almacenada la casilla de mensaje destino.
- Almacena temporalmente el correo saliente.
- Se encarga de recibir y almacenar temporalmente los mensajes para las casillas que sirve.
- Ejemplos: Postfix, Sendmail, MS Exchange, Exim, Qmail.
- Utiliza protocolo SMTP, entre servidores MTA.

Arquitectura (MDA)

- Cliente y Servidor.
- Se encarga de tomar los mensajes recibidos por el MTA y llevarlos al usuario.
- Existen MDA locales (LDA) y remotos (rMDA).
- Ejemplos de LDA: procmail, maildrop, Deliver, Sendmail.
- Ejemplos de rMDA: Cyrus IMAPd, Courier IMAPd, WU (University of Washington) IMAPd, Dovecot.
- Utilizan protocolos POP y/o IMAP.

Protocolo SMTP

- Simple Mail Transport Protocol.
- Protocolo Cliente/Servidor.
- Utiliza fromato ASCII 7 bits en 8 NVT.
- Usa TCP puerto servidor: 25.
- Los LMTA de los MUA hablan SMTP con su servidor SMTP saliente.
- Los servidores SMTP hablan entre sí este protocolo.
- RFC-821 (SMTP), extendida por RFC-1869 (ESMTP) y Redefinida por RFC-2821.

Protocolo SMTP (Ejemplo)

```
? telnet 172.20.1.5 25
```

```
...
```

```
220 brasilia.cities.org SMTP Sendmail 8.12.8/8.12.8 ...
```

```
HELO server.other.test
```

```
250 brasilia.cities.test Hello server... pleased to meet you
```

```
MAIL FROM: <bob@other.test>
```

```
250 2.1.0 bob@other.test... Sender ok
```

```
RCPT TO: <alice@cities.org>
```

```
250 2.1.5 alice@cities.org ... Recipient ok
```

```
DATA
```

```
354 Enter mail, end with "." on a line by itself
```

```
Esto es una prueba
```

```
.
```

```
250 2.0.0 k5HF1B0d005647 Message accepted for delivery
```

```
QUIT
```

```
221 2.0.0 brasilia.cities.org closing connection
```

Protocolo SMTP (Cont'd)

- Requiere finalizar con CRLF.CRLF.
- Usa conexiones persistentes.
- Trabaja de forma Interactiva (Requerimiento/Respuesta) o Pipeline.
- Puede o no requerir Autenticación.
- Puede o no trabajar de forma segura: SSL/TLS.

Formato del Mensaje

- El concepto de Envelope fue definido en RFC-821.
- Definido el Cuerpo y el Encabezado en RFC-822, Redefinido RFC-2822.
 - Envelope (Envoltorio), el usuario no lo ve, usado por MTAs, MAIL FROM:, RCPT TO:
 - Header (Encabezado), meta información del mail: Subject:, From:, To:, Return-Path: X-Mailer:, X-....:
 - Body (Cuerpo), separado por línea en blanco del header: Contenido del e-mail.

Formato del Mensaje Extendido

- Extensiones para enviar datos binarios.
- MIME (Multipurpose Internet Mail Extensions): Definido en RFC-1521 y RFC-1522. Redefinidas en RFC-2045 y RFC-2046.
- Con tags especiales indica el tipo al sistema destino.
- Luego codifica el mensaje binario en formato que no viole US-ASCII (NVT).
- Algunos Ejemplos: uunecode, base64, quotes-strings, etc.

Formato del Mensaje (Ejemplo)

```
From: bob@other.test
To: alice@cities.org
Subject: Test Mail MIME
Date: Thu, 11 Aug 2005 20:20:56 -0300 (ART)
MIME-Version: 1.0
Content-Transfer-Encoding: base64
Content-Type: image/jpeg

base64 encoded image .....
.....
.....base64 encoded image
```

Mensajes Multipart (Ejemplo)

```
From: bob@other.test
To: alice@cities.org
Subject: Test Mail MIME Multipart
Date: Thu, 11 Aug 2005 20:20:56 -0300 (ART)
MIME-version: 1.0
Content-type: multipart/mixed; boundary="DDDDIIIVVVIIISSSOOORRR"
```

This is a message with multiple parts in MIME format.

--DDDDIIIVVVIIISSSOOORRR

Content-type: text/plain

Mensaje en Texto

--DDDDIIIVVVIIISSSOOORRR

Content-type: application/octet-stream

Content-transfer-encoding: base64

base64 encoded stream

.....

.....base64 encoded stream

--DDDDIIIVVVIIISSSOOORRR--

Protocolo ESMTP (SMTP Extendido)

220 brasilia.cities.org ESMTP Sendmail 8.12.8/8.12.8 ...

EHL0 server.other.test

250 brasilia.cities.test Hello server..., pleased ...

250-ENHANCEDSTATUSCODES

250-PIPELINING

250-STARTTLS

250-AUTH

250-8BITMIME

250-SIZE

250-DSN

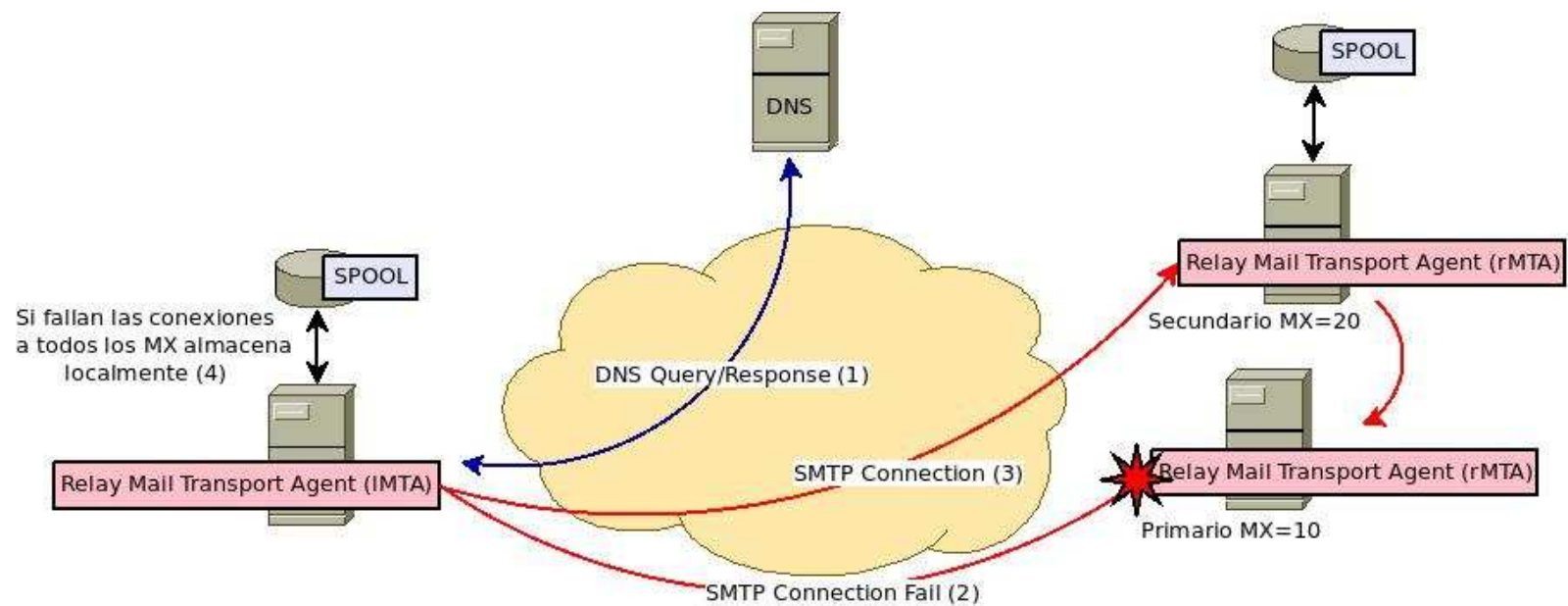
250-ETRN

250-VRFY

250-EXPN

250 HELP

SMTP y DNS



Protocolos Acceso a Correo

- POP: Post Office Protocol, RFC-1939: POPv3.
- IMAP: Internet Mail Access Protocol, RFC-1730: IMAPv4.
- Requieren Autenticación.
- Utiliza formato ASCII 7 bits en 8 NVT.
- Usan TCP puertos servidor: 110 y 143.
- Permiten correr de forma segura sobre SSL/TLS.
- IMAP más flexible permite uso de carpetas y manipulación de mensajes en el servidor.

POP (Ejemplo)

```
? telnet 127.0.0.1 110
```

```
...
```

```
+OK POP3 localhost.localdomain v2001.78rh server ready
```

```
user alice
```

```
+OK User name accepted, password please
```

```
pass 123456
```

```
+OK Mailbox open, 2 messages
```

```
NOEXIST
```

```
-ERR Unknown TRANSACTION state command
```

```
LIST
```

```
+OK Mailbox scan listing follows
```

```
1 620
```

```
2 622
```

```
.
```

```
TOP 1 1 100
```

```
+OK Top of message follows
```

Return-Path: <juan@...>

...

TOP 2 1 100

+OK Top of message follows

Return-Path: <root@...>

...

QUIT

+OK Sayonara

IMAP (Ejemplo)

```
? telnet 127.0.0.1 143
```

```
...
```

```
* OK brasilia.cities.org IMAP4rev1 v12.264 server ready
```

```
A0001 USER "alice" "123456"
```

```
* OK User alice authenticated
```

```
A0002 SELECT INBOX
```

```
* 1 EXISTS
```

```
* 1 RECENT ...
```

```
A0004 FETCH 1 BODY[HEADER]   ### Get first message header
```

```
...
```

```
A0005 FETCH 1 BODY[TEXT]     ### Get first message body
```

```
...
```

```
A0005 OK FETCH completed
```

```
A0006 LOGOUT
```

```
* BYE example.com IMAP4rev1 server terminating connection
```

```
A0006 OK LOGOUT completed
```

SPAM

- Open Relay.
- SPAMbots.
- Métodos para Contrarrestarlo.
 - RBL (Realtime Blackhole List) Blacklist.
 - Greylist, Whitelists.
 - Filtros de Contenido.
 - Reglas Dirigidas/Entrenadas por el usuario.

Fuentes de Información

- Kurose/Ross: Computer Networking (3rd Edition).
- TCP/IP Illustrated, Volume 1: The Protocols, W. Richard Stevens.
- RFCs: <http://www.isi.edu/in-notes/rfc821>, rfc822, ...
- Wikipedia: <http://www.wikipedia.org>.
- Slides de la Prof. Paula Venosa.
- Internet ...