

Mensajería en Internet (E-Mail)

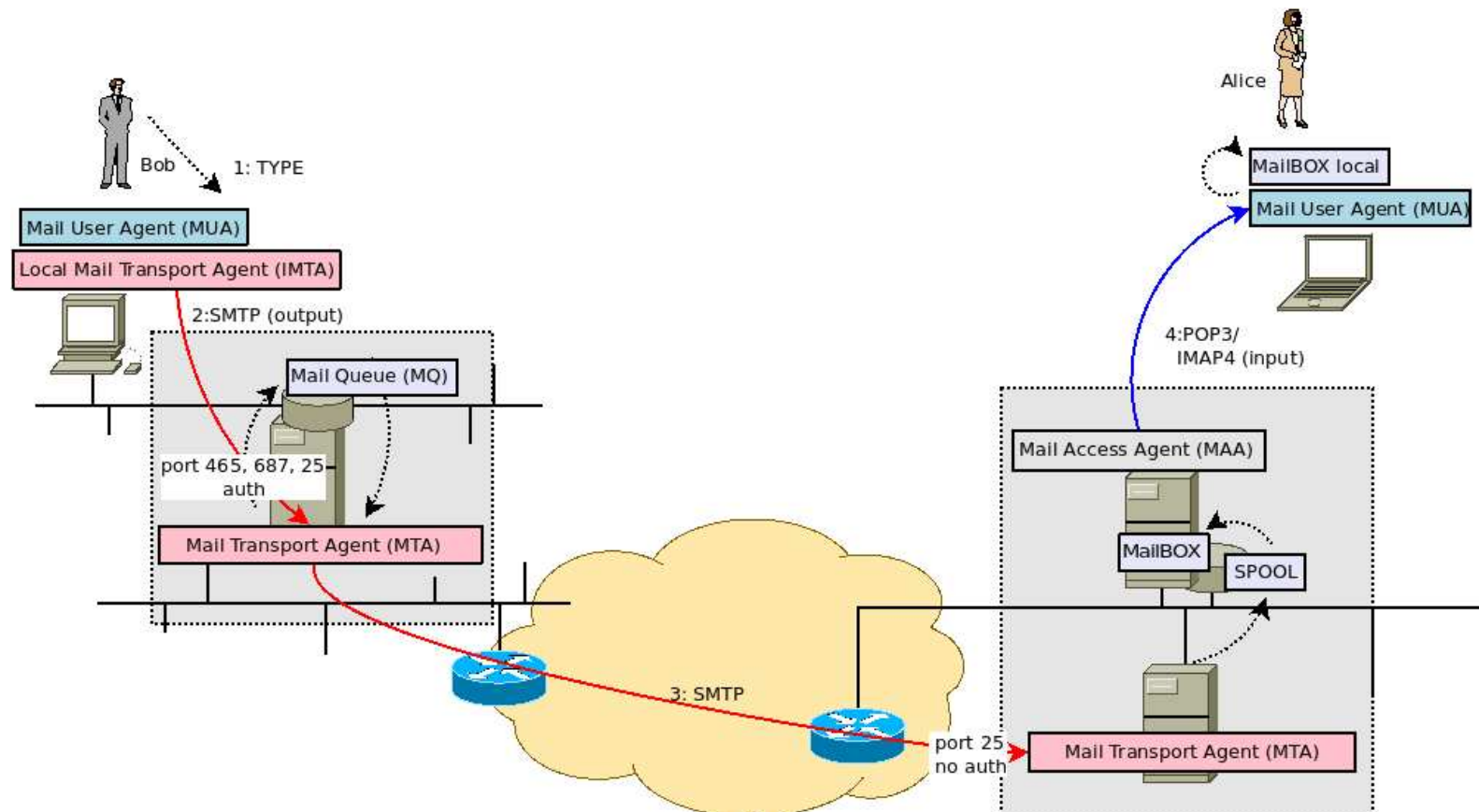
Redes y Comunicaciones



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 E-mail: MACH2!MACH1!USER.
- En 1972: Se escoge el símbolo “@” para denotar “en”, “at”.
- Casilla de E-mail: 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) o LDA (Local Delivery Agent).
 - MAA (Mail Access Agent).
 - Otros: MRA (Mail Retrieval Agent), MSA (Mail Submission Agent).
- Componentes Secundarias:
 - Servidor de Autenticación externo.
 - Web Mail (Front-End WWW).
 - Servidor de Anti-Virus, Anti-SPAM, Servidores de Listas, ...

Arquitectura Simplificada

- MTA = Servidor de correo saliente: integra MSA, MTA
- MAA = Servidor de correo entrante: integra MAA, MDA/LDA
- MUA = Cliente: integra MRA, MTA(local)

Arquitectura (MUA - Mail User Agent)

- Cliente.
- Interfaz con usuario.
- Lector/Editor/Emisor local de correos (e-mails).
- Posee integrado un local MTA para comunicarse con el Servidor de Mail Saliente, MTA que hace relay.
- El MTA que hace relay para el usuario pre-procesa el e-mail recibido desde el MUA con el agente MSA (Mail Submission Agent).
- Agrega la mayoría de los campos del header: Message-ID, To:, From:, Date:, Subject ...
- Posee integrado un MRA para comunicarse con el Servidor de Mail Entrante, MAA (Mail Access Agent).

- Utilizan protocolos SMTP o ESMTP, POP o IMAP, habla con MTA y con MAA propio.
- Ejemplos: Eudora, MS Outlook, Mozilla Thunderbird, elm, pine, mutt.
- Web-mailers: Horde/IMP, Squirrel, GMAIL, Yahoo, Hotmail.

Arquitectura (MSA - Mail Submission Agent)

- Servidor.
- Agente habitualmente integrado en el MTA.
- Recibe el mensaje del MUA y lo pre-procesa antes de pasarlo al MTA para que haga el transporte.
- Agrega campos que pueden faltar, formato del header: Message-ID, To:, From:, Date: ...
- Termina de dar formato al header del e-mail.
- Utiliza protocolo SMTP, ESMTP.
- Habitualmente usaba el port 25, se recomienda usar 587(submission), RFC-6409, ex:RFC-4409.
- Ejemplos: componentes de Postfix (postdrop, pickup), Sendmail-MSA.

Arquitectura (MTA - Mail Transport Agent)

- Cliente y Servidor.
- Toma el e-mail desde el MSA o directamente desde el MUA (MSA integrado).
- Se encarga de enviar el mensaje de e-mail al servidor donde está la casilla de mensaje destino, comunicación de MTA a MTA.
- Almacena temporalmente el correo saliente.
- Se encarga de recibir y almacenar temporalmente los mensajes para las casillas que sirve desde el MTA remoto.
- Utiliza protocolo SMTP o ESMTP, entre servidores MTA.
- Ejemplos: Postfix, Sendmail, MS Exchange, Exim, Qmail.

Arquitectura (MDA/LDA Mail Delivery Agent)

- Servicio interno o Servidor.
- Se encarga de tomar los e-mails recibidos por el MTA (acepta mensajes del MTA) y llevarlos al mailbox del usuario local.
- Se lo llama también LDA (Local Delivery Agent).
- Habitualmente define el formato del mailbox.
- Servicio de MDA puede hacer delivery remoto, cumple rol de MAA.
- Se integra con los protocolos POP y/o IMAP dejando los recursos disponibles al MAA o directamente al usuario.
- Ejemplos: procmail, postfix local, Sendmail, courier, cyrus-IMAP, dovecot, sieve, fetchmail(mas un MRA), getmail(más un MRA).

Arquitectura (MAA - Mail Access Agent)

- Servidor.
- Integrado o separado del MDA.
- Autentica al MUA/usuario y lee los e-mails del mailbox local dejados por el MDA/LDA.
- Transpara los e-mails hacia el MUA o los hace accesibles a este.
- Se integra con el MDA. Implementa los protocolos POP y/o IMAP dejando acceder a los recursos y dialogando con el MUA.
- Ejemplos de MDA/LDA: courier, cyrus-IMAP, dovecot, sieve.

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

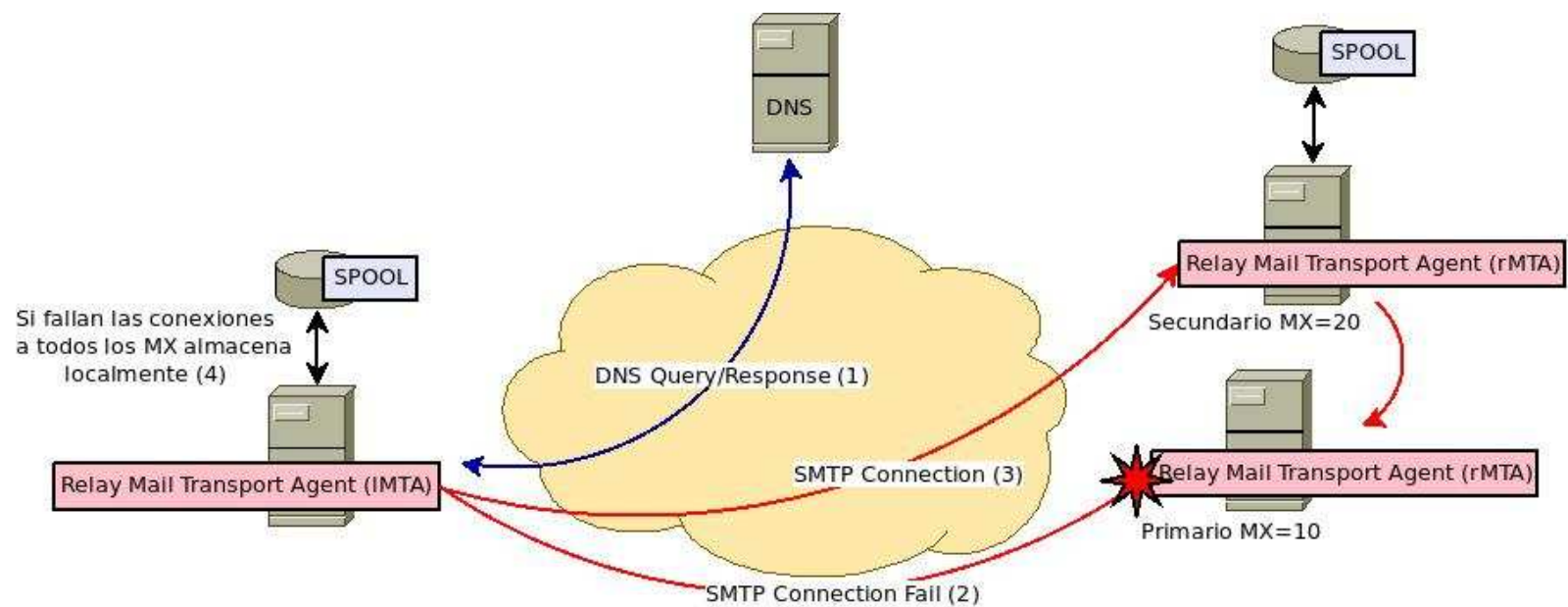
250-ETRN

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
```

```
.
```

POP (Ejemplo) (Cont.)

TOP 1 100

+OK Top of message follows

Return-Path: <juan@...>

...

TOP 2 100

+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
```

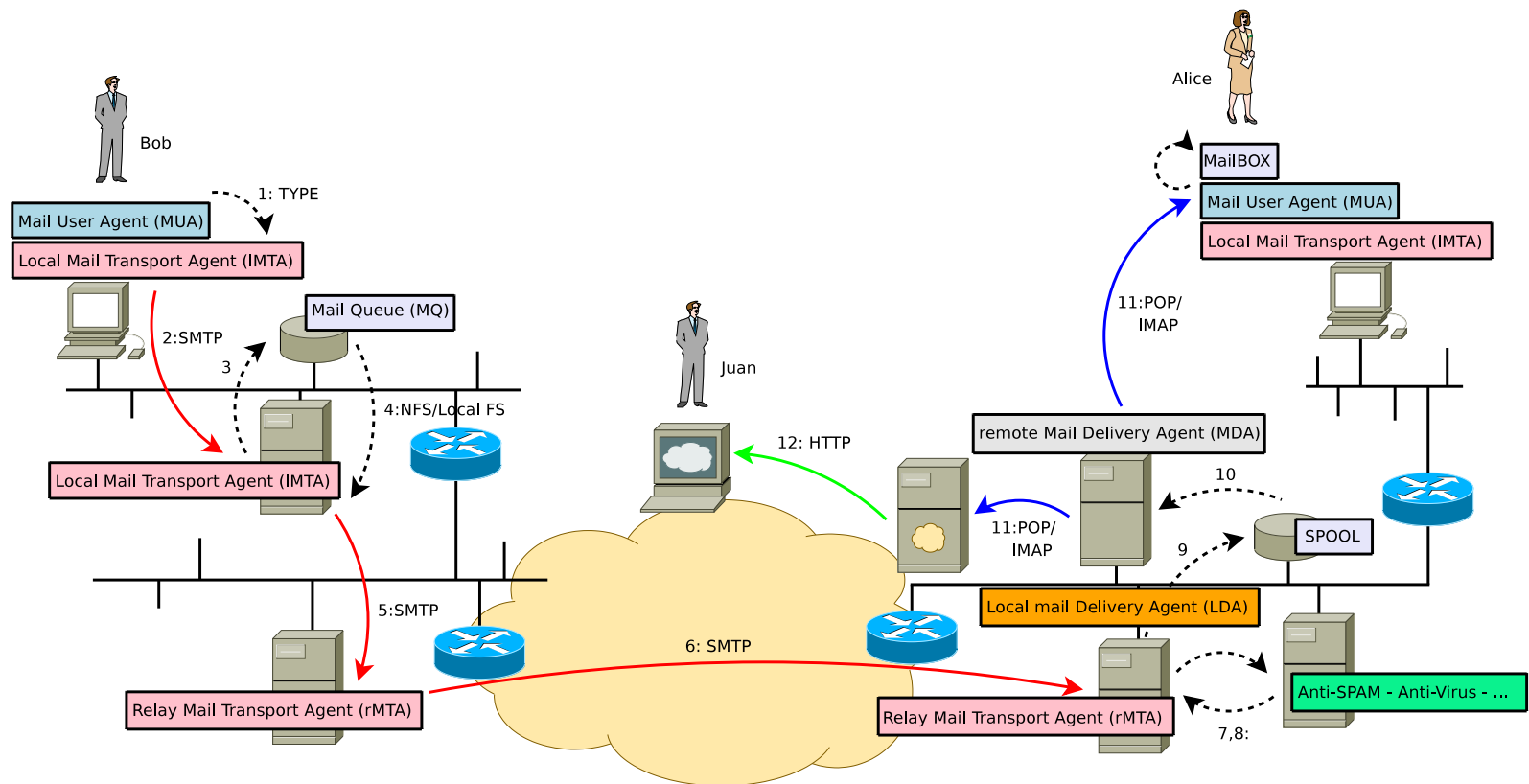
```
* BYE example.com IMAP4rev1 server terminating connection
```

```
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.

Arquitectura Extendida



Fuentes de Información

- Kurose/Ross: Computer Networking (6th 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>.
- Internet ...