Índice hora 5

Objetivos

- Revisar el servicio de correo electrónico o email
- Presentar el protocolo de envió de email extremo a extremo, STMP
- Funcionalidades añadidas al servicio: multiparte, mime, autenticación
- Presentar los protocolos de acceso a buzones, POP e IMAP
- Indicar la arquitectura de un servicio de webmail
- Esbozar los problemas de seguridad del servicio de correo electrónico

5 Correo electrónico/SMTP,POP3,IMAP

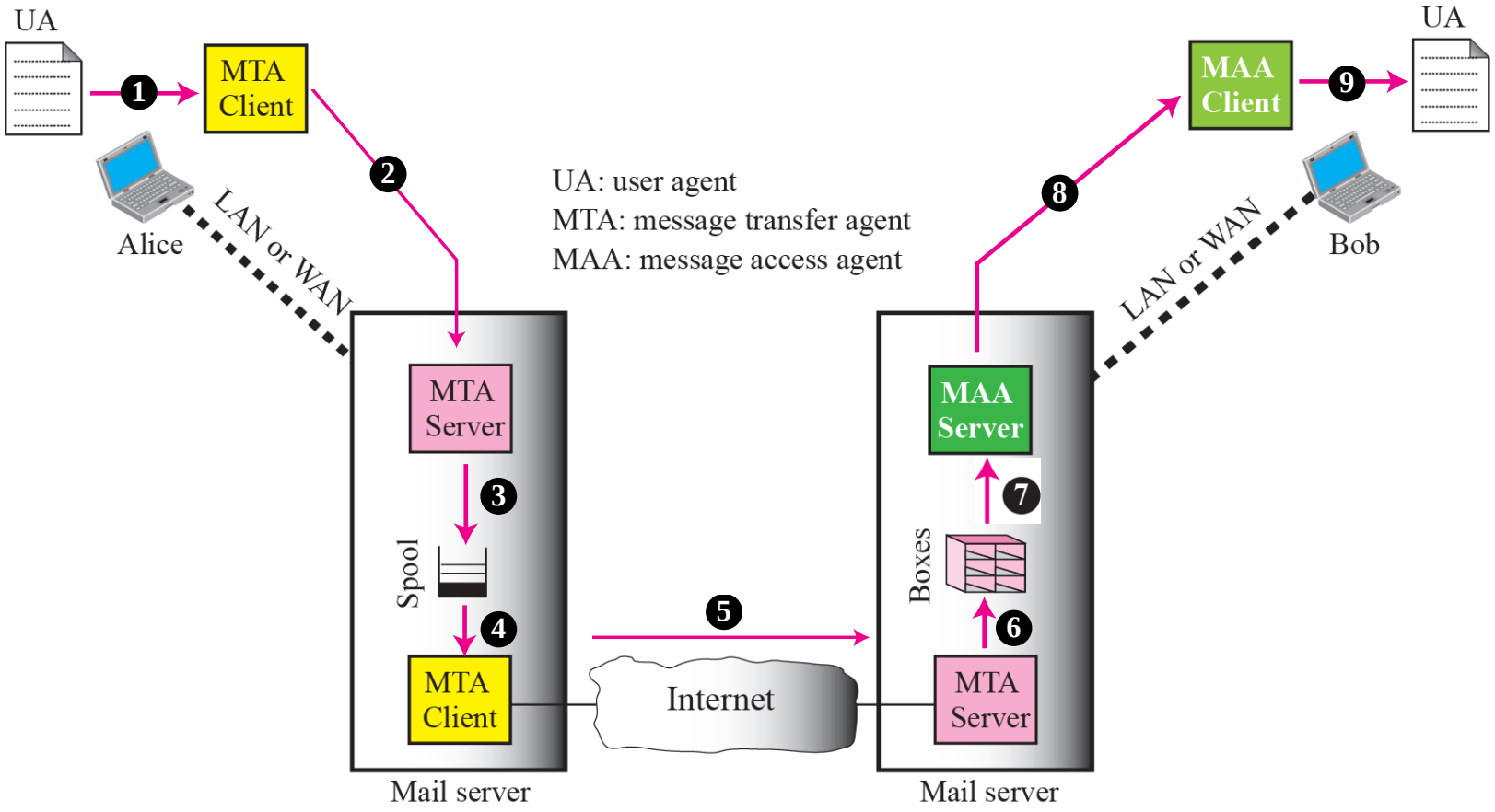
- Servicio de envío y recepción de correos electrónicos
  - A diferencia de otras aplicaciones no requiere que los extremos que se comunican estén conectados simultáneamente
  - Los servidores del servicio se encargan de almacenar los mensajes hasta que el destinatario los reclama
- Componentes del servicio de correo electrónico
  - Agentes de usuario
    - Lector de correo
    - Permite enviar y recibir mensajes de correo electrónico
    - Hace funciones de cliente
  - Servidores de correo
    - Buzones: almacenan los mensajes del usuario
    - Cola de mensajes salientes
    - Hace también funciones de cliente para conectarse a otros servidores
  - Protocolos
    - SMTP (Simple Mail Transfer Protocol)
    - POP3 (Post Office Protocol v3)
    - IMAP4 (Internet Message Access Protocol)

Dirección de correo electrónico

- Necesario un servidor de correo por nombre de dominio
- Un dominio tendrá asociado un registro MX indicando la dirección IP del servidor de correo del dominio.

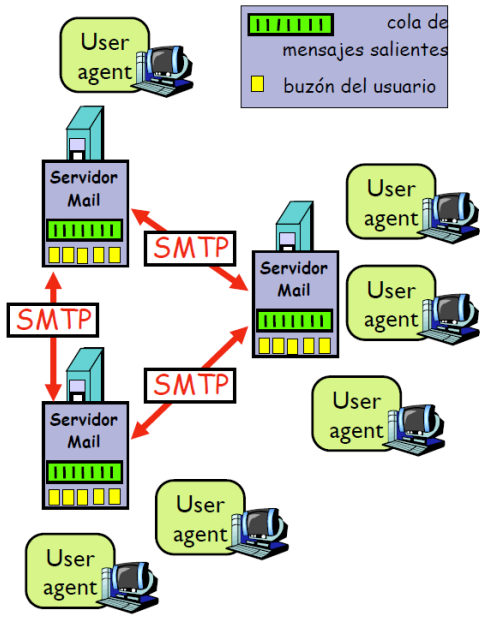
```
#nslookup
Servidor predeterminado:  prunus.unavarra.es
Address:  130.206.159.2

> set type=MX
> google.com
Servidor:  prunus.unavarra.es
Address:  130.206.159.2

Respuesta no autoritativa:
google.com      MX preference = 20, mail exchanger = alt1.aspmx.l.google.com
google.com      MX preference = 30, mail exchanger = alt2.aspmx.l.google.com
google.com      MX preference = 40, mail exchanger = alt3.aspmx.l.google.com
google.com      MX preference = 50, mail exchanger = alt4.aspmx.l.google.com
google.com      MX preference = 10, mail exchanger = aspmx.l.google.com

google.com      nameserver = ns2.google.com
google.com      nameserver = ns3.google.com
google.com      nameserver = ns4.google.com
google.com      nameserver = ns1.google.com
aspmx.l.google.com      internet address = 173.194.67.26
alt1.aspmx.l.google.com internet address = 173.194.70.26
alt2.aspmx.l.google.com internet address = 173.194.69.26
alt3.aspmx.l.google.com internet address = 173.194.71.26
alt4.aspmx.l.google.com internet address = 74.125.127.26
ns1.google.com  internet address = 216.239.32.10
ns2.google.com  internet address = 216.239.34.10
ns3.google.com  internet address = 216.239.36.10
ns4.google.com  internet address = 216.239.38.10
```

MTA/MAA


UA
MTA Client
1
2
Alice
LAN or WAN
UA: user agent
MTA: message transfer agent
MAA: message access agent
MTA Server
3
Spool
4
MTA Client
Mail server
5
Internet
MAA Server
7
Boxes
6
MTA Server
Mail server
8
MAA Client
9
UA
LAN or WAN
Bob

5.1 SMTP

- RFC 2821
- Utiliza TCP para transferir confiablemente mensajes de correo desde el cliente al servidor, utiliza el puerto 25
- Protocolo texto: mensajes están codificados en ASCII de 7 bits
- Permite la transferencia de correos electrónicos directa:
  - Entre un agente de usuario y un servidor de correo
  - Entre dos servidores de correo
- La transferencia tiene tres fases
  - Handshaking (saludo)
  - Transferencia del los mensajes
  - Cierre
- Interacción comando/respuesta
  - comandos: texto ASCII
  - respuesta: códigos de estado y frase



SMTP, Ejemplo

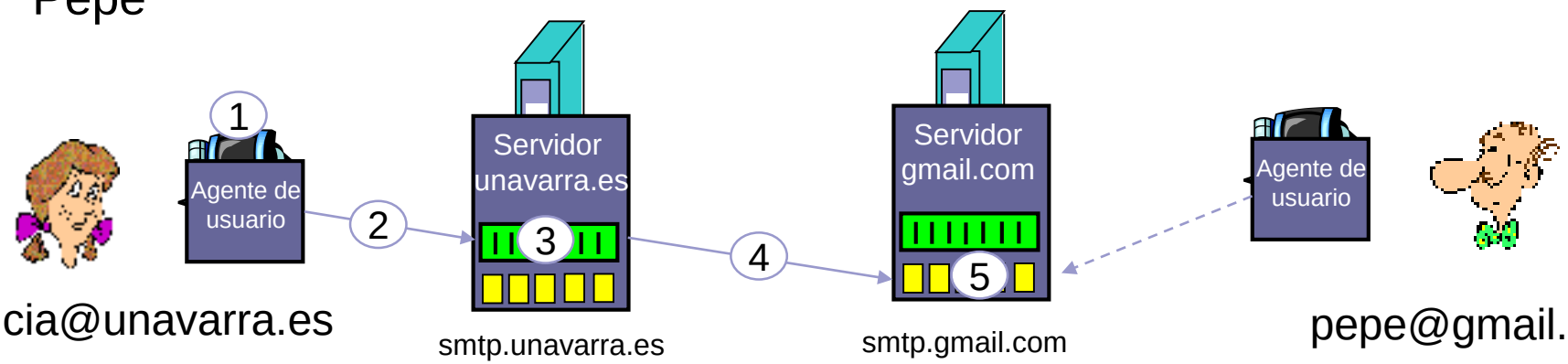
1) Alicia con su email alicia@unavarra.es utiliza su agente de usuario para elaborar un mensaje para pepe@gmail.com

2) El agente de usuario de Alicia envía el mensaje a su servidor de correo unavarra.es. El mensaje es colocado en la cola de mensajes

3) El lado cliente de SMTP abre una conexión TCP con el servidor de correo de Pepe

4) El lado cliente de SMTP envía el mensaje de Alicia sobre la conexión TCP

5) El servidor de correo de Pepe coloca el mensaje en el buzón de Pepe



SMTP, Ejemplo paso 4

```
C: cliente smtp.unavarra.es
S: servidor smtp.gmail.com
```

```
S: 220 gmail.com
C: HELO unavarra.es
S: 250  Hello unavarra.es, pleased to meet you
C: MAIL FROM: <alicia@unavarra.es>
S: 250 alicia@unavarra.es... Sender ok
C: RCPT TO: <pepe@gmail.com>
S: 250 pepe@gmail.com ... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: ¿Te gusta la salsa de tomate?
C:   ¿y los pepinillos?
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 gmail.com closing connection
```

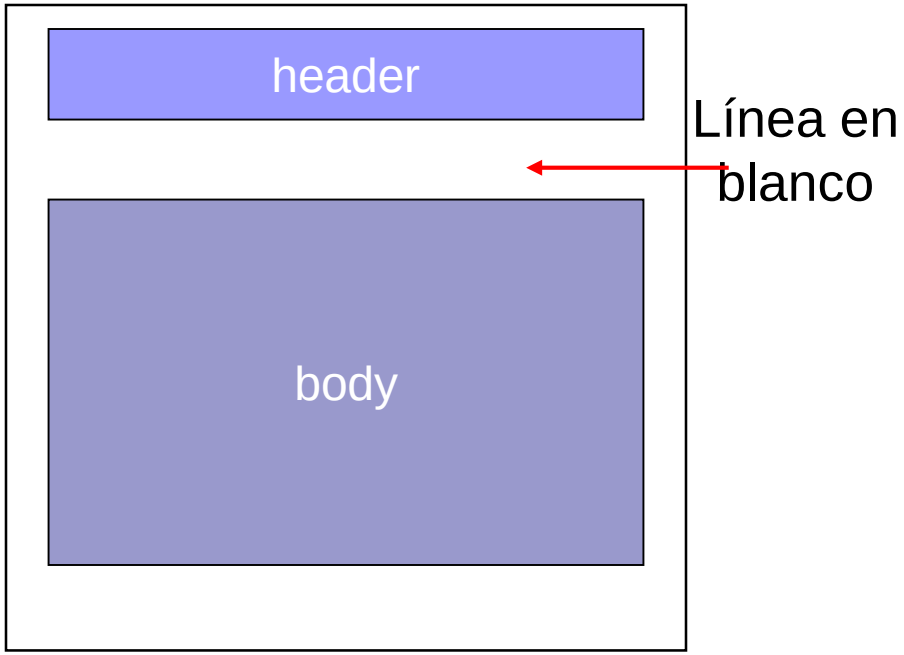
Pruebe a hacer un:
#nc servidordecorreo 25

SMTP

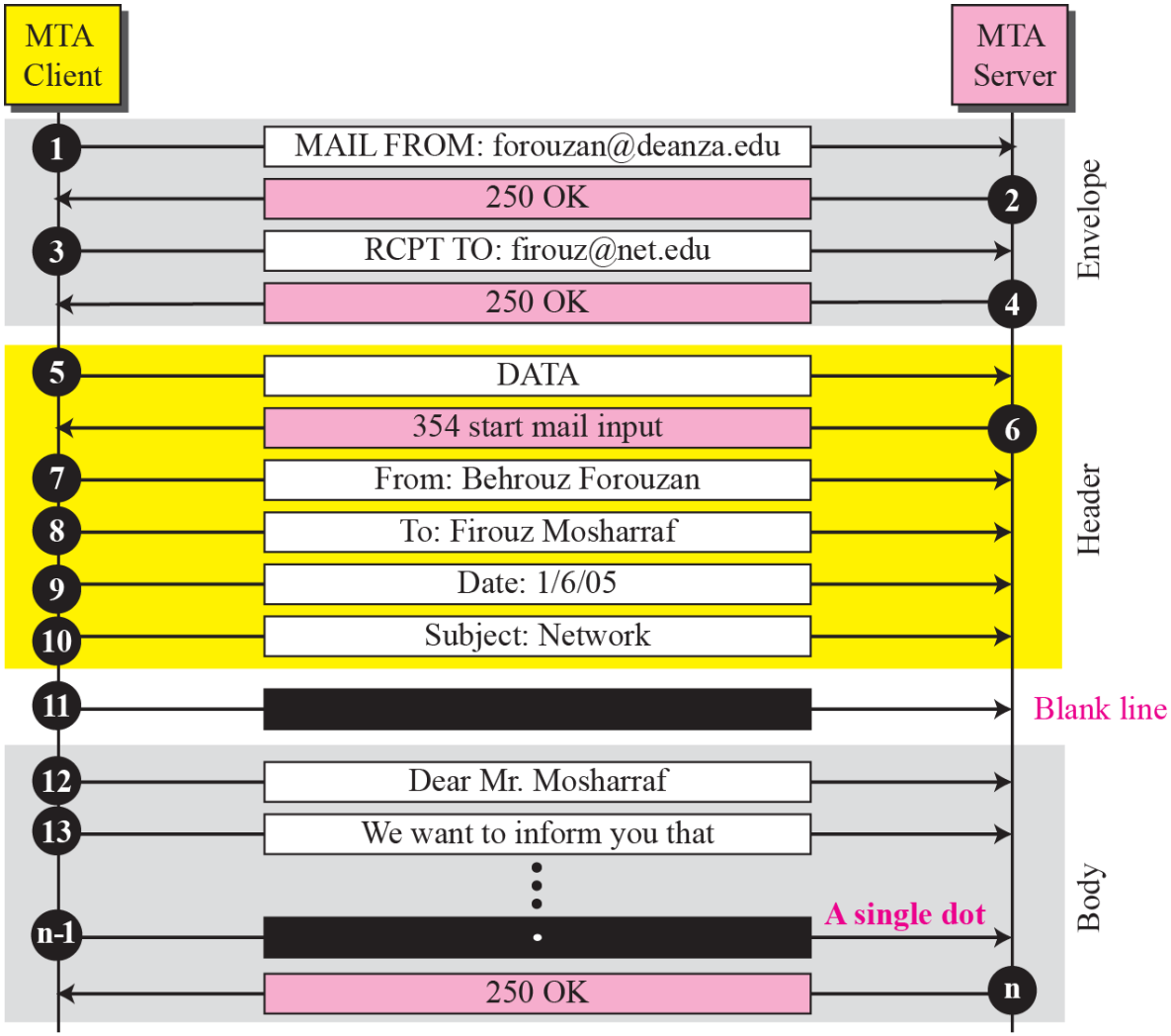
- Comandos
  - HELO
  - MAIL FROM
  - RCPT TO
  - DATA: utiliza CRLF.CRLF (“\r\n.\r\n”) para indicar donde está el final del mensaje enviado con DATA
  - QUIT
- SMTP es un protocolo de tipo PUSH (el cliente manda datos al servidor) frente a un protocolo HTTP que es de tipo PULL (el servidor manda datos al cliente)

SMTP

- El formato del mensaje en DATA se especifica en RFC822
  - Líneas de cabecera
    - To:
    - From:
    - Subject:
    - ¡Son diferentes a los comandos SMTP!
  - Cuerpo (body)
    - Es el contenido del correo electrónico



SMTP, diagrama de mensajes



(*) Versión simplificada
Los mensajes correctos son los de la slide 8

5.1.1 Enrutado de mensajes

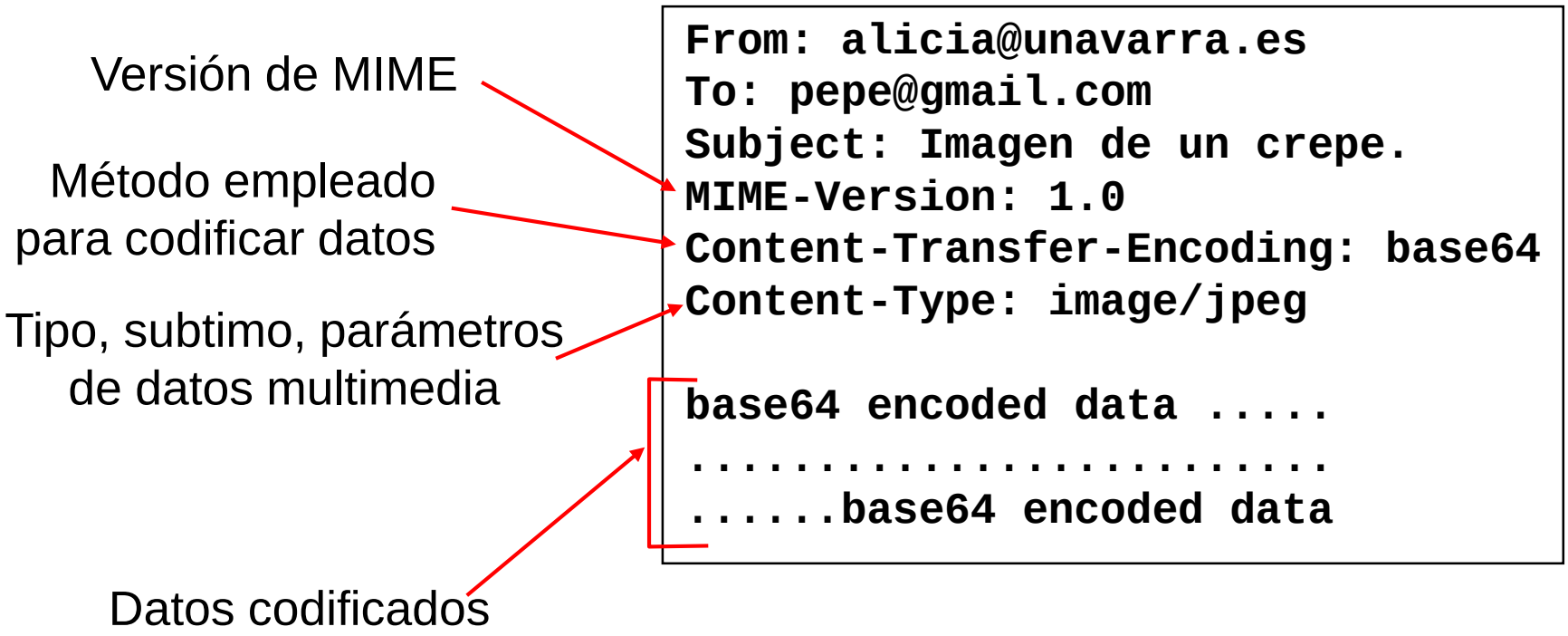
- Una máquina de usuario puede
  - Contactar con el servidor de correo de su dominio para entregarle el correo y este servidor se encargue de enviarlo al servidor destino. La forma habitual.
    - Para evitar que cualquier usuario de Internet pueda hacer uso de un servidor de correo que no es de su dominio, SMTP incorpora amplicaciones para autenticar al usuario por dirección IP o usuario/contraseña (RFC4954).
  - Contactar directamente con el servidor del dominio del correo electrónico destino.
    - Normalmente no habilitado por problemas de seguridad (SPAM)
    - Autenticación entre servidores
- Un servidor que tenga que enviar un correo puede no contactar directamente con el servidor del dominio destino y en su lugar pasarlo a un servidor intermedio llamado **relay**
  - Principalmente razones relacionadas con la seguridad

Enrutado de mensajes

- Si el servidor del dominio destino no está alcanzable en un momento determinado, el servidor de correo previo guardará el mensaje (típicamente 24-48h, reintentando varias veces) y en caso de no poder entregarlo retorna un mensaje de error al origen
- Si el email llega al servidor del dominio destino y resulta que el buzón indicado en el email no existe, devuelve otro email indicando el error al origen

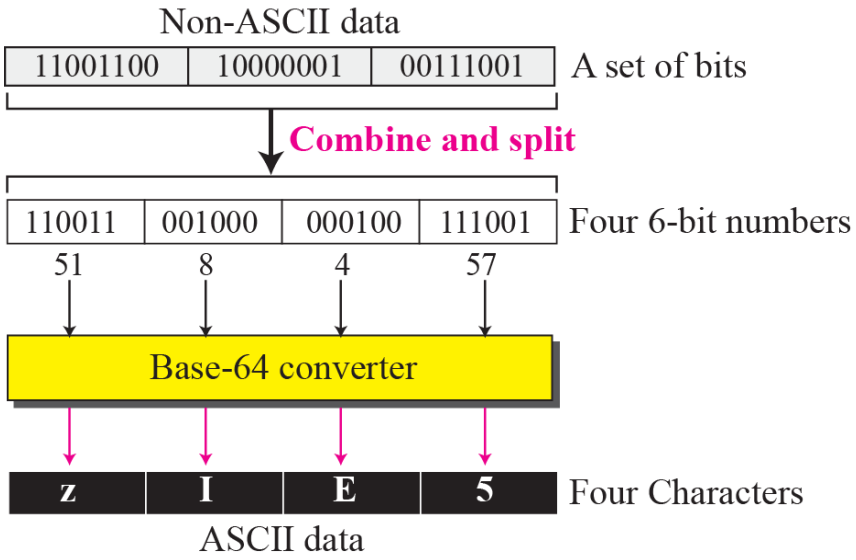
5.1.2 MIME

- MIME: Multimedia Internet Mail Extension, RFC 2045, 2056
- Líneas adicionales en el header del mensaje para el tipo MIME
  - Content-Type: tipo/subtipo; parámetros
- La codificación permite el envío de datos no ASCII

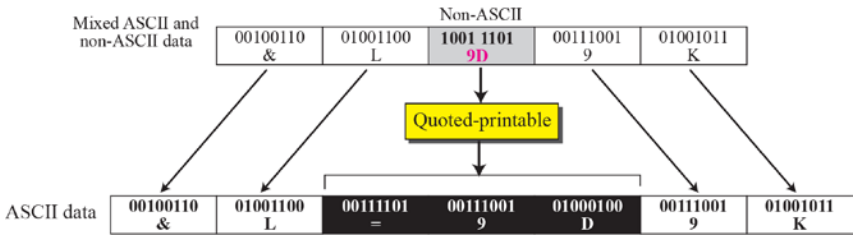


MIME codificaciones

- Base64



- Quoted printable



La codificación de cualquier dato binario en ASCII-7 hace que crezca el tamaño del mensaje (efecto de los adjuntos en el email)

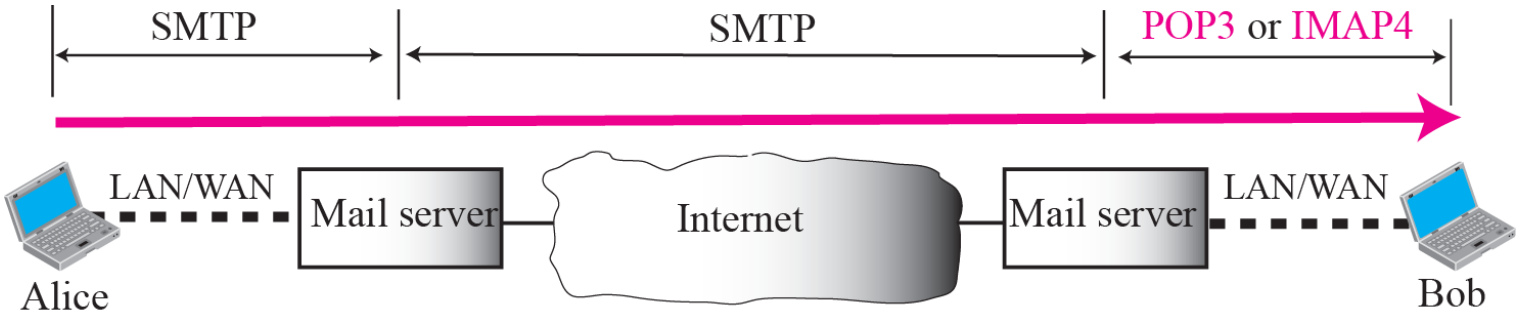
5.1.3 Multipart

- SMTP utiliza conexiones “persistentes”
  - Multiples objetos se pueden envíar en un mensaje “multiparte”
  - Multiples email se pueden enviar sobre la misma conexión TCP

```
From: alicia@unavarra.es
To: pepe@gmail.com
Subject: Imagen de un crepe.
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary=StartOfNextPart

--StartOfNextPart
Hola Beto, por favor encuentra la imagen de un crepe.
--StartOfNextPart
Content-Transfer-Encoding: base64
Content-Type: image/jpeg
base64 encoded data .....
.........................
......base64 encoded data
--StartOfNextPart
¿te gustaría tener la receta?
```

5.2 Protocolos de acceso al correo

- SMTP: entrega al servidor de correo del receptor
- Protocolo de acceso al correo: recupera los mensajes desde el servidor
  - POP: Post Office Protocol
    - autorización (agente <-->servidor) y descarga los mensajes
  - IMAP: Internet Mail Access Protocol
    - autorización (agente <-->servidor) y manipulación de los mensajes almacenados en el servidor
    - más funcionalidades y complejidad
  - HTTP - webmail: Gmail, Hotmail , Yahoo! Mail, etc.



5.2.1 POP

- RFC1939
- Sobre TCP en puerto 110
- Versión actual v3: POP3
- Protocolo
  - texto
  - sin estado: no guarda información de sesiones anteriores pero si mantiene estado de la misma conexión
  - del tipo petición/respuesta
- Permita la descarga de mensajes desde el servidor de correo que tiene el buzón del usuario al agente de usuario
  - Borrando los mensajes del servidor
  - Sin borrar los mensajes del servidor: permitirá descargas los correos en otro agente de usuario

POP

Fase de autorización

- Comandos del cliente:
  - **`user:`** nombre de usuario
  - **`pass:`** la clave
- Respuestas del servidor
  - **`+OK`**
  - **`-ERR`**

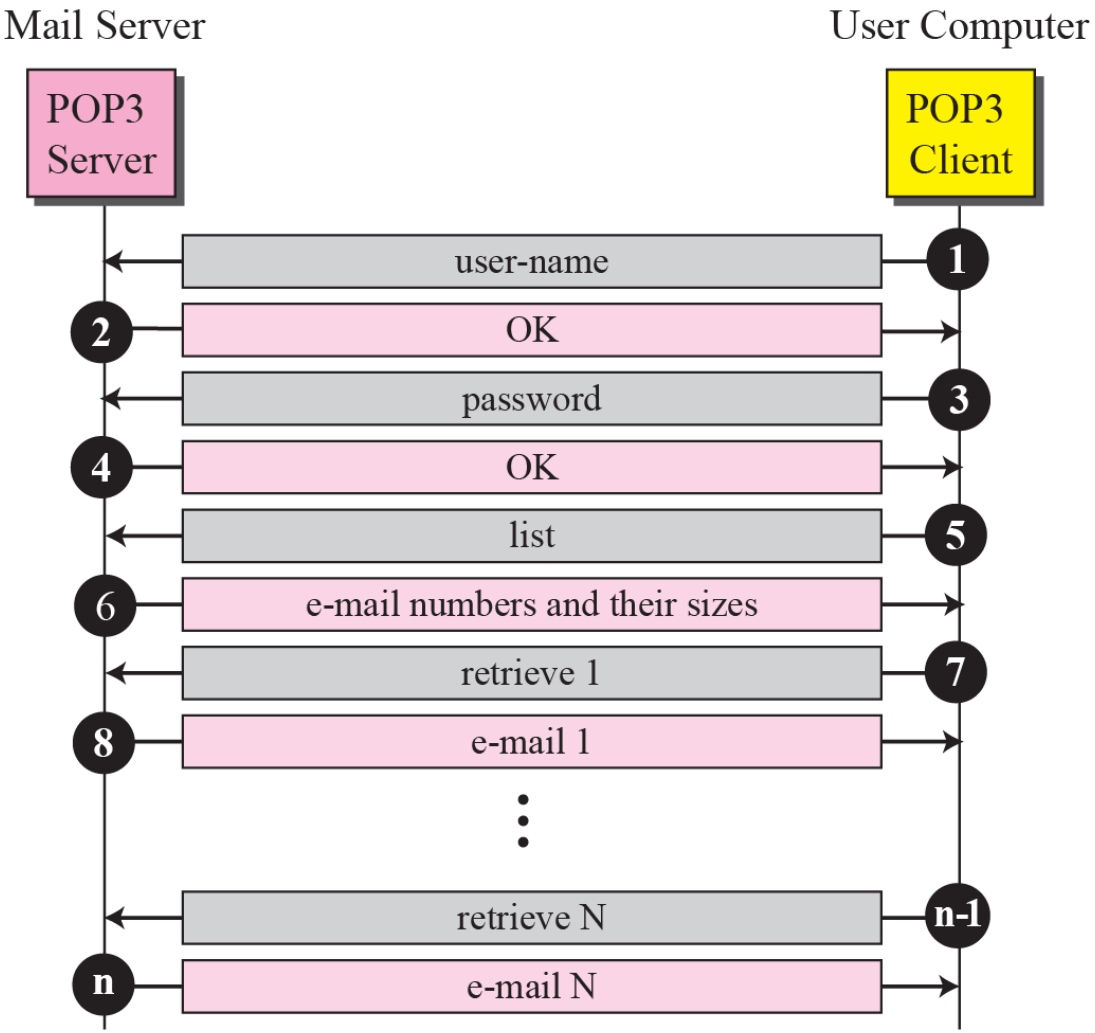
Fase de transacción, cliente:

- **`list:`** lista los números de los mensajes
- **`retr:`** recupera el mensaje por el número
- **`dele:`** borra el mensaje
- **`quit:`** termina la sesión

```
S: +OK POP3 server ready
C: user pepe
S: +OK
C: pass goloso
S: +OK user successfully logged on
```

```
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 POP3 server signing off
```

POP


Mail Server
User Computer
POP3 Server
POP3 Client
user-name
1
2
OK
password
3
4
OK
list
5
6
e-mail numbers and their sizes
retrieve 1
7
8
e-mail 1
retrieve N
n-1
n
e-mail N

5.2.2 IMAP

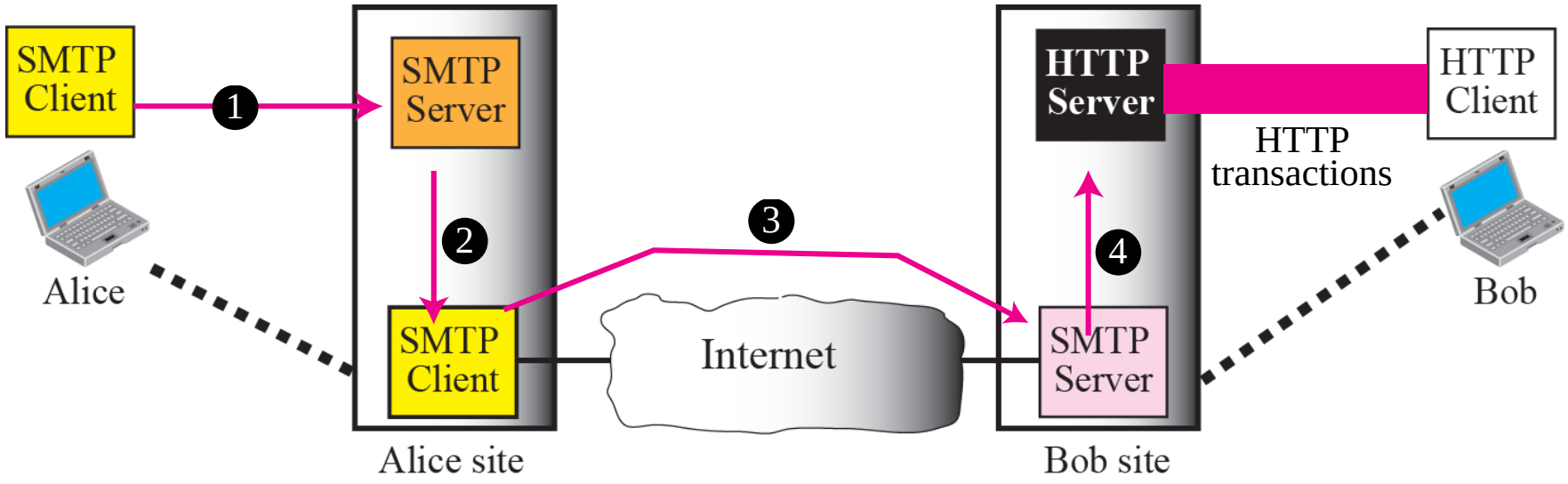
- RFC1730
- Sobre TCP en puerto 143
- Versión actual v4: IMAP4
- Protocolo
  - texto
  - con estado: guarda información de sesiones anteriores
  - del tipo petición/respuesta
- Mantiene todos los mensajes en el mismo lugar: el servidor
  - Permite al usuario organizar sus mensajes en carpetas sobre el propio buzón del servidor
    - Una búsqueda de mensajes se realiza en el propio servidor
  - Mantiene información de estado de sesiones anteriores:
    - Nombres de carpetas y “mapeo” entre la identificación de los mensajes y el nombre de las carpetas

IMAP

- No es necesario la descarga completa de todos los mensajes
  - Pueden descargarse sólo los títulos y remitente, y al seleccionar un correo proceder a la descarga del mensaje completo o partes (multipart) del mismo
- Modo conectado/no conectado
  - En modo no conectado el user agent puede hacer uso de la caché con información previamente descargada
- Permite compartir el mismo buzón entre varios usuarios
- Se hace necesario mantener una conexión abierta con el servidor para recibir notificaciones de llegada de nuevos correos

5.2.3 Webmail

- Pasos 1-3 como anteriormente (SMTP)
- Paso 4, pasarela a servidor web mediante una aplicación corriendo en el lado del servidor CGI que implementa el servicio webmail
  - El paso 4 se implementa habitualmente mediante
    - IMAP en recepción
    - SMTP en envío



5.3 Seguridad

- Todos los protocolos SMTP, POP3 e IMAP4 son inseguros por naturaleza.
- Se puede aportar seguridad:
  - A nivel de aplicación, mediante Pretty Good Privacy (PGP) and Secure MIME (SMIME)
  - Utilizando los servicios de Secure Sockets Layer (SSL) igual como ocurría en HTTP
    - Secure SMTP (SSMTP) - puerto 465
    - Secure IMAP (IMAP4-SSL) - puerto 585
    - IMAP4 over SSL (IMAPS) - puerto 993
    - Secure POP3 (SSL-POP) - puerto 995
  - A nivel de protección de correo indeseado, SPAM

Resumen

- Un agente de usuario deberá implementar
  - SMTP para enviar el correo
  - POP y/o IMAP para acceder a su buzón de correo
- Un servidor deberá implementar
  - SMTP para recibir y enviar correo
  - POP y/o IMAP para permitir el acceso de usuarios a sus buzones.
    - Si es un servidor de relay no necesita implementar este acceso
    - Pueden ser servidores diferentes los que provean SMTP y POP/IMAP
- SMTP, POP e IMAP son protocolos
  - texto
  - petición/respuesta sobre TCP
  - mantienen estado dentro la conexión TCP
  - IMAP además mantiene estado entre conexiones TCP
- La seguridad en el servicio de email es si cabe más crítica que en el resto de servicios al ser un servicio más expuesto

Referencias

- [Forouzan]
  - Capítulo 23, “Electronic Mail: SMTP, POP, IMAP and MIME”
- [Stevens]
  - Capítulo 28, “SMTP: Simple Mail Transfer Protocol”