Transparencias del Curso de Correo Electronico - Postfix

Grupo de usuarios de linux

Univ. Carlos III de Madrid

1 de diciembre de 2002

Contenido de la charla

- Historia y Evolucion del Correo-e
- Protocolos involucrados
- Postfix vs Sendmail
- Configuración e intalación de Postfix
- Todo lo que demos . . .

Nuestro amigo el Correo Electronico (correo-e)

- Crecimiento en los ultimos años
- De *luxury* a *necessity*
- Del entorno Corporativo al hogar (ISP's)

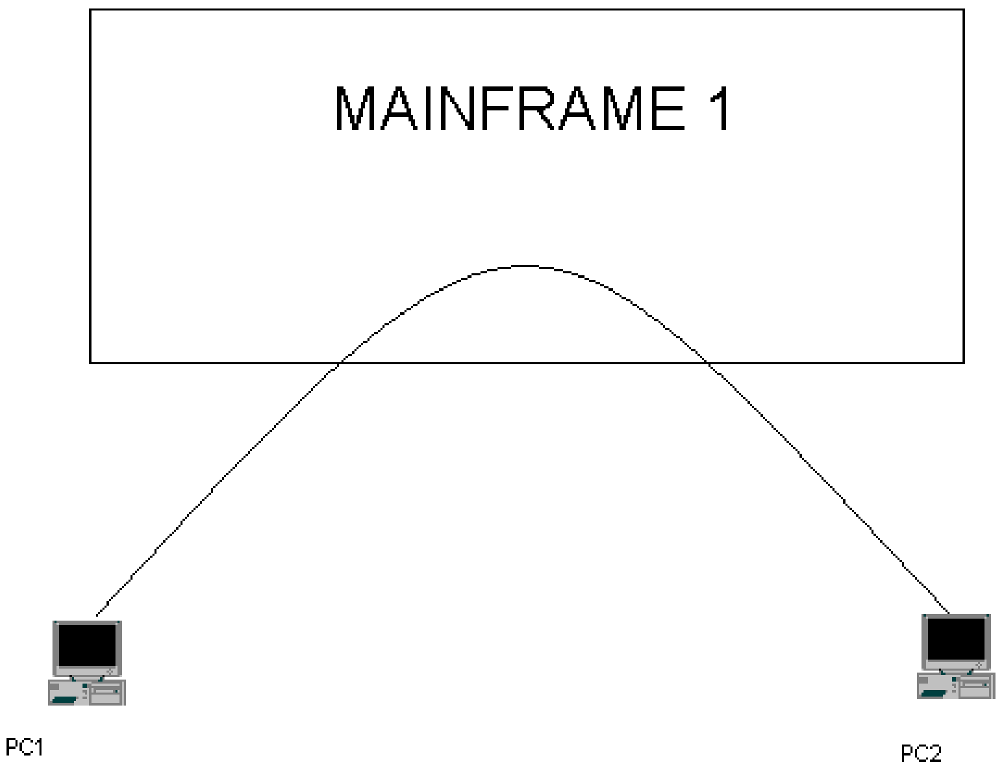
Comienzos del correo-e

Mainframe messages

- Mensajes entre usuarios
- Requeria que el usuario estuviera conectado
- Querian más funcionalidades

Entorno inicial

Figura 1: MainFrame1

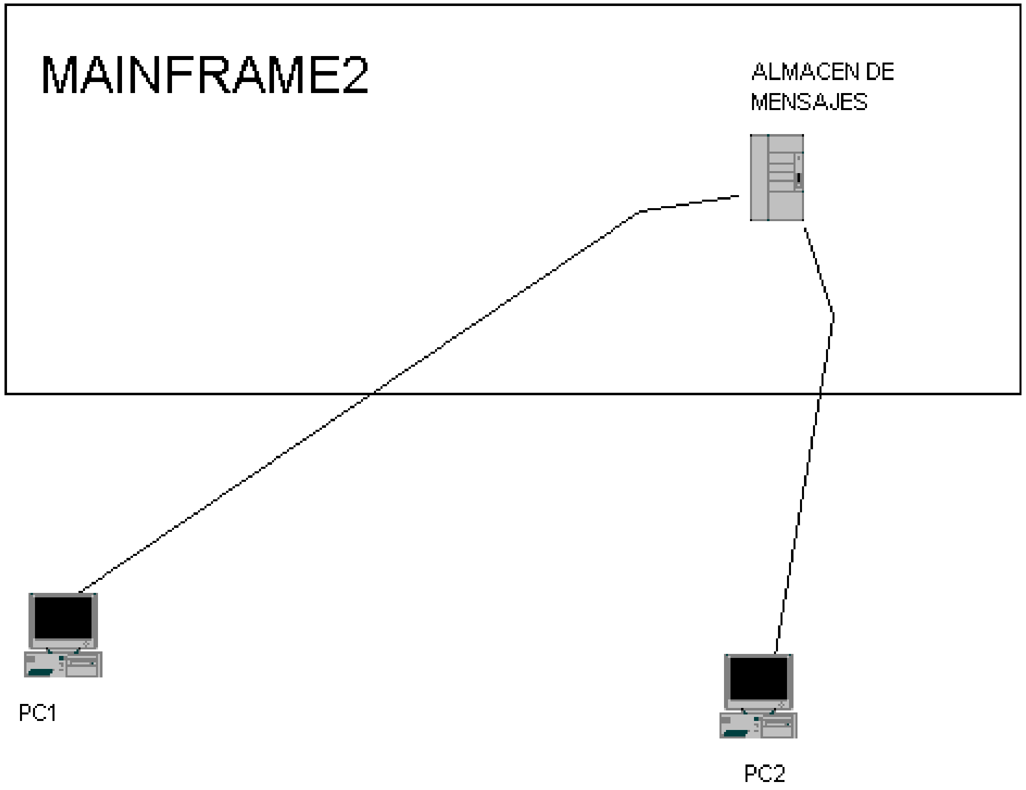


Mainframe con Almacenamiento

- El mensaje se almacenaba y posteriormente se mostraba al usuario
- No era necesaria la conexion del usuario para el envio del mensaje
- Requeria un software mas complejo
- Se penso en una comunicacion entre MainFrames...
- `$ mail manolito`

Escenario Sin Conexion

Figura 2: MainFramex2

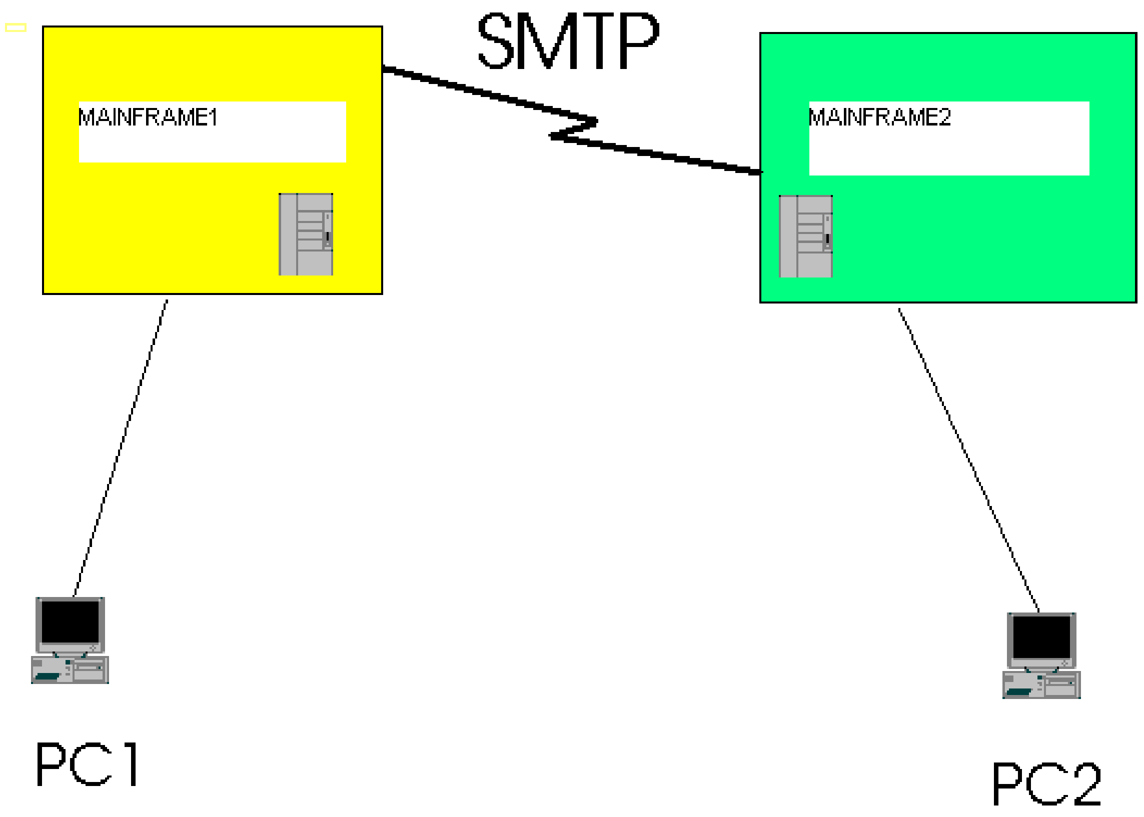


Escenario Multi-Mainframes

- Podias mandar mensajes entre MainFrames
- Necesidad de un identificador de Host
- `$ mail nina@otherHost`

Escenario Multi-Mainframes

Figura 3: MainFrame3



Soluciones UNIX ;)

Se exijian ya muchas cosas y se hizo un monstruo...

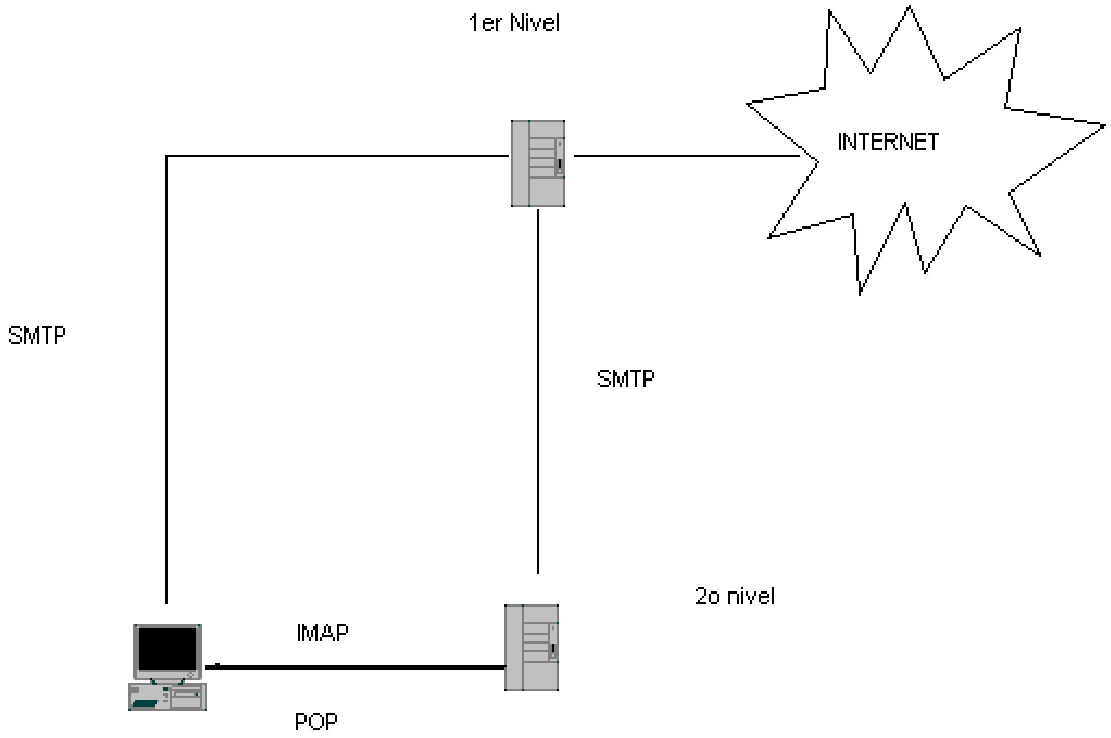
- Modularidad:
- Transporte - Entrega - Usuario
  - Mail User Agent
    MUA (PINE, Evolution, Mutt)
  - Mail Delivery Agent
    MDA (Maildrop, Sendmail)
  - Mail Transport Agent
    MTA (Postfix, Sendmail, Exim)

Vida Real: Modelo RACE

Red Academica Correo Electronico, RedIris

- Basado en Estafetas. Permite Control de Cabeceras, antivirus, anti-relay . . .

Figura 4: RACE



Protocolos implicados

- Interactive Mail Access Protocol - IMAP
- Post Office Protocol - POP3
- Simple Mail Transfer Protocol - SMTP

SMTP

- Modelo sencillo y comprensible de comunicacion entre MTA's
- Luego veremos un ejemplo practico . . .

```
Connected to smtp.uc3m.es.
Escape character is '^]'.
220 smtp02.uc3m.es ESMTP Postfix
helo gul.uc3m.es
250 smtp02.uc3m.es
mail from: unodelgul@gul.uc3m.es
250 Ok
rcpt to: otrodelgul@gul.uc3m.es
250 Ok
data
354 End data with <CR><LF>.<CR><LF>
```

```
Probando boqueron...
.
250 Ok: queued as 538D799F30
quit
221 Bye
Connection closed by foreign host.
```

IMAP

- Las carpetas y mensajes se consultan y permanecen en el servidor
- Permite tener todo tu correo independientemente del ordenador en que lo leas
- Mayor trabajo para el administrador de Sistema (Quotas)

POP

- Los mensajes son descargados al ordenador
- El usuario es el responsable de sus correos
- Tambien supone trabajo para el administrador (Se descargan los mensajes y dicen q los han perdido -¿Tirar de Backup. . .)

Ejemplo IMAP

Contra un Courier-IMAP (correo.uc3m.es)

```
* OK Courier-IMAP ready. Copyright 1998-2002 Double Precision, Inc.
* login otrodelgul miclaveenclaroenunatransparencia
* OK LOGIN Ok.
* SELECT INBOX
* FLAGS (\Draft \Answered \Flagged \Deleted \Seen \Recent)
* OK [PERMANENTFLAGS (\Draft \Answered \Flagged \Deleted \Seen)] Lim
* 62 EXISTS
* 1 RECENT
* OK [UIDVALIDITY 1025596920] Ok
* OK [READ-WRITE] Ok
* 62 FETCH (FLAGS () INTERNALDATE "24-Nov-2002
23:46:25 +0100" RFC822.SIZE 739 ENVELOPE
("Sun, 24 Nov 2002 23:46:07 +0100 (CET)"
```

```
NIL (("unodelgul@gul.uc3m.es" NIL "unodelgul" "gul.uc3m.es"))
(("unodelgul@gul.uc3m.es" NIL "unodelgul" "gul.uc3m.es"))
(("unodelgul@gul.uc3m.es" NIL "unodelgul" "gul.uc3m.es"))
((NIL NIL "undisclosed-recipients" NIL)
(NIL NIL NIL NIL))
NIL NIL NIL "<20021124224607.538D799F30@smtp02.uc3m.es>"))
* OK FETCH completed.
* FETCH 62 RFC822.TEXT
* 62 FETCH (RFC822.TEXT {5}
Probando boqueron...
)
* OK FETCH completed.
```

Postfix vs Sendmail

- Sendmail es un monolitico dificil de mantener y con unos ficheros de configuracion complicados
- No es apto para administradores no experimentados
- Las aplicaciones para correo-e no se integran bien con Sendmail

Postfix vs Sendmail (2)

- Postfix es modular, cada módulo tiene una tarea
- El intercambio de informacion es mínimo entre los módulos (más seguridad)
- Ficheros de configuración en plano, cómodos para el administrador
- Tablas de acceso rápido en multiples formatos (hash, btree)
- Integracion con MySQL, LDAP...

Postfix : The Big Picture

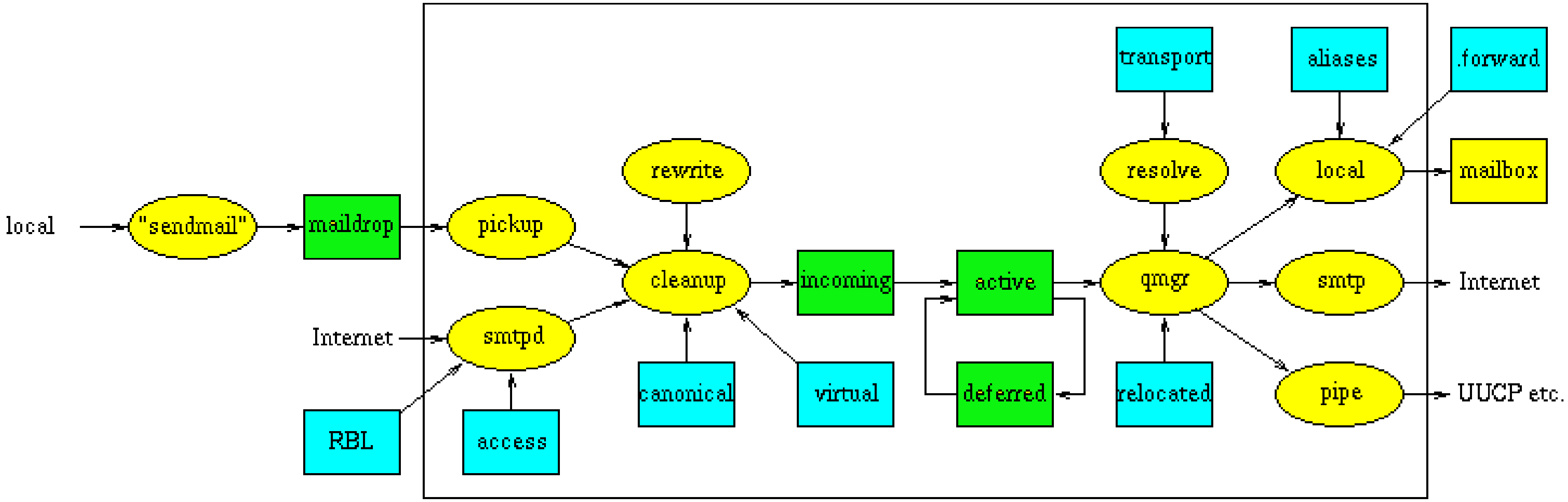


Figura 5: The Big Picture

Ficheros de configuracion

- main.cf
- *myhostname*
- *mydestination*
- *mynetworks*
- *smtpd_banner*
- master.cf

Postfix: Tablas

- tablas hash
- tablas btree
- tablas dbm
- regenerando las tablas *postmap*
  - postmap hash:/etc/postfix/tabla
- tablas regexp
- tablas pcre

Postfix: Transport

- Permite encaminar el correo al servidor de destino de forma explicita
- transport_maps = hash:/etc/postfix/transport
- Formato: patrón acción
- ejemplos:
  - `foo.org    :[gateway.foo.org]`
  - foo.org smtp:bar.org:2025
- directivas en el main.cf
  - default_transport
  - relayhost

Postfix: Aliases

- alias_maps = hash:/etc/aliases
- alias_database = hash:/etc/aliases
- regenerando los alias *newaliases*
- formato
  alias: direccion@prueba.es
  alias2: "—fichero_que_ejecuto"
  alias3: :include:/monton_de_direcciones

Controlando el Spam

- Filtrado de cabeceras

  `Header_checks`

- Restringir las conexiones

  `smtpd_client_restrictions`

- Restricciones en el HELO

  `smtpd_helo_restrictions`

- Restricciones al remitente

  `smtpd_sender_restrictions`

- Restricciones del destinatario

  `smtpd_recipient_restrictions`

- Mapas de listas negras

  `maps_rbl_domains`

Filtrado de cabeceras

- Header_checks
  - header_checks = regexp:/etc/postfix/header_checks
  - Un ejemplo

    `/^subject: .*coach.*/ REJECT`
  - Acciones
    - REJECT
    - REJECT text
    - IGNORE
    - WARN

Restringir las conexiones

- smtpd_client_restrictions
  - reject_unknown_client
  - permit_mynetworks
  - check_client_access maptype:mapname
  - reject_maps_rbl

Restricciones en el HELO (EHLO)

- smtpd_helo_required
- smtpd_helo_restrictions
    - reject_invalid_hostname
    - permit_naked_ip_address
    - reject_unknown_hostname
    - reject_non_fqdn_hostname
    - check_helo_access maptype:mapname

Restricciones en el emisor

- smtpd_sender_restrictions
  - reject_unknown_sender_domain
  - check_sender_access maptype:mapname
  - reject_non_fqdn_sender
  - reject_invalid_hostname
  - reject_unknown_hostname

Restricciones en el Destinatario

- smtpd_recipient_restrictions
    - check_relay_domains
    - check_sender_access maptype:mapname
    - reject_unauth_destination
    - reject_unknown_recipient_domain
    - reject_non_fqdn_recipient
    - permit_mx_backup

Mapas RBL

- Relay Black List (RBL)
- maps_rbl_domains = blackholes.mail-abuse.org

Se acabó :)