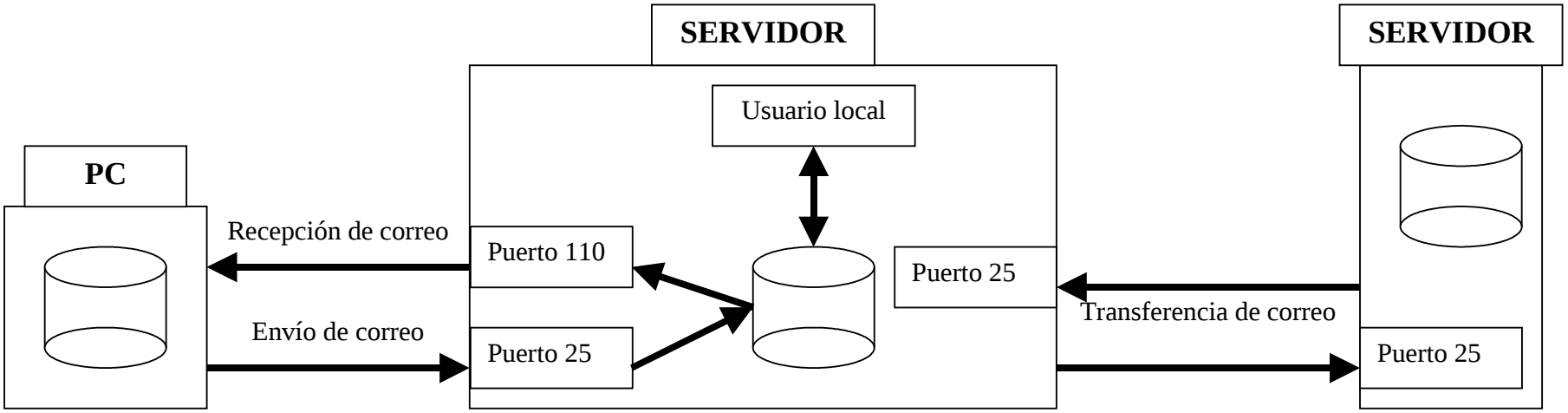
Introducción (I)

- Los primeros sistemas de correo electrónico eran protocolos de transferencia de ficheros.
  - La primera línea del fichero contenía el destino.
- En 1982, ARPANET definió el correo electrónico.
  - RFC821: Protocolo de transmisión.
  - RFC822: Formato de los mensajes.
- El correo electrónico consistía en dos subsistemas:
  - Agente de transferencia de mensaje, que mueve el correo entre el origen y el destino.
  - Agente de usuario, que permite leer y crear el correo electrónico.

Introducción (II)

- En la actualidad existen tres subsistemas:
  - Agente de transferencia.
  - Agente de usuario.
  - Protocolos de entrega final.



Configuración del servidor de SMTP (I)

- El servidor de Simple Mail Transfer Protocol transfiere el correo del ordenador origen al destino.
- Es un protocolo cliente/servidor:
  - Formato ASCII.
  - Utiliza el puerto 25 TCP del servidor.
- Los comandos de SMTP:
  - Se definieron en el RFC821.
  - Se modificaron en el RFC1425.
- El formato de los mensajes:
  - Se definió en el RFC822.
  - Se extendieron en el RFC1521: Multipurpose Internet Mail Protocol (MIME).

Configuración del servidor de SMTP (II)

- El servidor de SMTP es /usr/sbin/sendmail.
- Sus ficheros de configuración se encuentran en /etc/mail.
- Existen dos tipos de ficheros de configuración:
  - .cf
    - Contienen las instrucciones básicas de funcionamiento.
    - Se crean a partir de ficheros de extensión .mc.
    - El comando para crearlos es:

```
/usr/bin/m4 /etc/mail/fichero.mc > /etc/mail/fichero.cf
```

  - .db
    - Contienen permisos de acceso, etc.
    - Se crean a partir de ficheros sin extensión.
    - El comando para crearlos es:

```
/usr/sbin/makemap hash /etc/mail/fichero </etc/mail/fichero
```

Configuración de los ficheros .mc (I)

- Existen dos ficheros con extensión .mc:
  - submit.mc
  - sendmail.mc
- Su existencia obedece al doble trabajo de sendmail:
  - Como Mail Submission Agent, encargado de recibir el correo de los usuarios y procesarlos para su envio.
  - Como Mail Transport Agent, encargado de tranportar el correo entre ordenadores.
- Para funcionar como MSA necesita que los usuarios tengan acceso a ciertos directorios del sistema o activar el bit de GID.

Configuración de los ficheros .mc (II)

Palabra	Descripción
dnl	Comienzo de comentario. Todo lo que siga en la línea se considera un comentario y no será tenido en cuenta.
divert(n)	Las líneas que siguen deben ser ignoradas en la salida (n=-1) o incluidas en la salida (n>=0). De forma general para incluir las líneas n será 0, aunque puede tomar valores hasta 9 para indicar su inclusión según ciertas condiciones y/o orden.
include	Incluye el contenido del fichero indicado.
sinclude	Incluye el contenido del fichero indicado.
define	Permite definir el valor de una macro de configuración con el valor indicado.
VERSIONID	Incluye como información el mensaje escrito.
OSTYPE	Define el sistema operativo sobre el que ejecuta sendmail.
MAILER	Tipos de correo que son aceptados.
DOMAIN	Define los ordenadores que aceptarán cada tipo de correo.
FEATURE	Especifica opciones particulares de configuración de sendmail.

El fichero submit.mc (I)

- Configura el que los usuarios puedan enviar correo. Sus líneas son:

```
VERSIONID(`linux setup')dnl
```

Incluir esta información sobre la versión en el fichero de salida.

```
define(`confCF_VERSION', `Submit')
```

Define el valor de la macro confCF_VERSION que se añade a la identificación de la versión de configuración

```
define(`__OSTYPE__',`')
```

Añadida por exigencia del programa m4.

```
define(`_USE_DECNET_SYNTAX_', `1')
```

Utilizar sintaxis DECnet.

El fichero submit.mc (II)

```
define(`confTIME_ZONE', `USE_TZ')
```

Zona horaria a utilizar:

- USE_SYSTEM: Obtenerla del sistema.
- USE_TZ: Obtenerla de la variable de ambiente TZ.
- Valor fijo: Utilizar esa zona horaria.

```
define(`confDONT_INIT_GROUPS', `True')
```

No llamar a la función initgroups:

- Los usuarios solo pertenecen a su grupo principal.

```
define(`confPID_FILE', `/var/run/sm-client.pid')
```

Localización del identificador del proceso.

```
FEATURE(`use_ct_file')
```

Leer el fichero /etc/mail/trusted-users.

```
FEATURE(`msp',`[127.0.0.1]')
```

Ordenador (o dirección IP) como el que se envía el correo local.

El fichero sendmail.mc (I)

```
VERSIONID(`setup for linux')dnl
```

Incluir esta información sobre la versión en el fichero de salida.

```
OSTYPE(`linux’)
```

Es obligatorio. Especifica el sistema operativo sobre el que se ejecuta el demonio. Permite configurar:

- Caminos de ficheros.
- Opciones de funcionamiento.
- Etc.

El fichero sendmail.mc (II)

```
dnl define(`SMART_HOST',`smtp.your.provider')
```

Define el ordenador a través del cual se envía el correo electrónico saliente. Si el SMART_HOST se especifica como:

- nombre: Se utiliza registro MX.
- [nombre]: Se utiliza registro A.

```
define(`confDEF_USER_ID`,``8:12’’)
```

Define el usuario y grupo como el que se ejecuta el servidor.

```
define(`confTO_CONNECT’,`1m’)
```

Define el tiempo máximo de espera en la conexión.

El fichero sendmail.mc (III)

```
define(`confTRY_NULL_MX_LIST’,true)
```

Indica que es el mejor MX para recibir el correo con este destino.

```
define(`confDONT_PROBE_INTERFACES’,true)
```

No insertar nombre o direcciones equivalentes.

```
define(`PROCMAIL_MAILER_PATH',`/usr/bin/procmail')
```

Localización del programa procmail.

```
define(`ALIAS_FILE', `/etc/aliases')
```

Localización del fichero de alias.

```
define(`STATUS_FILE', `/var/log/mail/statistics')
```

Localización del fichero con el estado del programa.

El fichero sendmail.mc (IV)

```
define(`UUCP_MAILER_MAX', `2000000')
```

Tamaño máximo del correo enviado mediante UUCP.

```
define(`confUSERDB_SPEC', `/etc/mail/userdb.db')
```

Base de datos de usuarios autorizados a enviar correo.

- Si no existe todos los usuarios pueden enviar correo.

```
define(`confPRIVACY_FLAGS',
  `authwarnings,novrfy,noexpn,restrictqrun')
```

Banderas de privacidad:

- novrfy: No permitir verificar usuarios.
- noexpn: No expandir alias.
- restrictqrun: Permitir solo a root procesar la cola de mensajes.
- Por defecto solo esta activada authwarnings.

El fichero sendmail.mc (V)

```
define(`confAUTH_OPTIONS', `A')
```

Los usuarios pueden enviar correo sin autenticarse.

- Si se desea que los usuarios se autentiquen debe comentarse la línea anterior y descomentar:

```
define(`confAUTH_OPTIONS', `A p')
```

Los mecanismos de autenticación, se especifican como:

```
dnl TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
dnl define(`confAUTH_MECHANISMS', `EXTERNAL GSSAPI DIGEST-MD5 CRAM-
   MD5 LOGIN PLAIN')dnl
```

Si se utiliza usuario/contraseña debe ir sobre SSL, indicando los certificados con:

```
dnl define(`confCACERT_PATH',`/etc/pki/tls/certs')
dnl define(`confCACERT',`/etc/pki/tls/certs/ca-bundle.crt')
dnl define(`confSERVER_CERT',`/etc/pki/tls/certs/sendmail.pem')
dnl define(`confSERVER_KEY',`/etc/pki/tls/certs/sendmail.pem')
```

El fichero sendmail.mc (VI)

```
dnl define(`confTO_QUEUEWARN', `4h')
```

Tiempo de espera antes de enviar un aviso al remitente.

```
dnl define(`confTO_QUEUERETURN', `5d')
```

Tiempo máximo de intento de envío de un correo.

```
dnl define(`confQUEUE_LA', `12')
dnl define(`confREFUSE_LA', `18')
```

Promedio de carga del procesador a partir del cual son rechazados los mensajes para su envío (confQUEUE_LA) o para su recepción (confREFUSE_LA).

```
define(`confTO_IDENT', `0')
```

Tiempo de espera antes de aceptar una conexión.

```
dnl FEATURE(delay_checks)
```

No comprobar el cliente que se conecta o ejecuta un comando de correo.

El fichero sendmail.mc (VII)

```
FEATURE(`smrsh',`/usr/sbin/smrsh')
```

Shell que usará sendmail cuando necesite alguna.

```
FEATURE(`mailertable',`hash -o /etc/mail/mailertable.db')
```

Tabla que sobreescribe rutas para dominios particulares.

```
FEATURE(`virtusertable',`hash -o /etc/mail/virtusertable.db')
```

Forma del alias de dominios virtuales para el servidor de correo.

```
FEATURE(redirect)
```

Rechazar el correo enviado a usuarios cuya cuenta ha sido trasladada con el código 551.

```
FEATURE(always_add_domain)
```

Incluir el dominio del ordenador local en el correo recibido desde el mismo.

El fichero sendmail.mc (VIII)

```
FEATURE(use_cw_file)
```

Leer el fichero /etc/mail/local-host-names para seleccionar otros nombres del ordenador.

```
FEATURE(use_ct_file)
```

Leer el fichero /etc/mail/trusted-user (opción idéntica a la de submit.mc).

```
dnl define(`confMAX_DAEMON_CHILDREN', 12)
```

Número máximo de hijos que puede lanzar para atender las peticiones.

```
dnl define(`confCONNECTION_RATE_THROTTLE', 3)dnl
```

Número máximo de conexiones por segundo que son aceptadas.

El fichero sendmail.mc (IX)

```
FEATURE(local_procmail,``,`procmail -t -Y -a $h -d $u')
```

Formato de llamada a procmail en el reenvío de un correo.

```
FEATURE(`access_db',`hash -T<TMPF> -o /etc/mail/access.db')
```

Habilita la base de datos que limita los ordenadores que pueden enviar correo a través de este servidor.

```
FEATURE(`blacklist_recipients')
```

Habilita la “lista negra” para bloquear correos de ciertos usuarios u ordenadores.

```
EXPOSED_USER(`root')
```

Usuarios que deben ser mostrados en lugar de otros nombres que puedan tener.

El fichero sendmail.mc (X)

```
DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')
```

- Escuchar solo en el interfaz de loopback (dirección 127.0.0.1).
  - Debe comentarse si se desea utilizar el ordenador para enviar correo de otros ordenadores.
  - Pueden especificarse varias líneas para permitir que el servicio permanezca a la escucha en varias direcciones IP del ordenador.

```
FEATURE(`accept_unresolvable_domains')
```

Permite aceptar el correo de dominios no resolubles por un DNS.

```
dnl FEATURE(`relay_based_on_MX')
```

Permitir el reenvio de correo basado en registros MX.

El fichero sendmail.mc (XI)

```
MAILER(smtp)
```

Especifica los servidores de correo utilizados en el sistema.

```
dnl # Introduccion del ClamAV como antivirus
INPUT_MAIL_FILTER(`clmilter',`S=local:/var/run/clamav/
   clamav-milter.sock,F=, T=S:4m;R:4m')
define(`confINPUT_MAIL_FILTERS',`clmilter')
```

Introduce un antivirus para el chequeo del correo.

Configuración de los ficheros .db (I)

- Los ficheros de bases de datos son:
  - access: Ordenadores autorizados a enviar correo a través de este.
  - domaintable: Otros dominios por los que puede ser conocido el ordenador (generalmente vacio).
  - local-host-name: Todos los nombre de nuestro ordenador. No se convierte a base de datos (.db).
  - mailertable: Sobreescribe la ruta para algunos dominios particulares.
  - trusted-users: Usuarios que pueden enviar correo en nombre de otros.
  - virtusertable: Alias para los dominios virtuales.

Configuración de los ficheros .db (II)

- Ejemplo de fichero access:

```
Connect:localhost.localdomain    RELAY
Connect:localhost                RELAY
Connect:127.0.0.1                RELAY
Connect:147.156.222              RELAY
Connect:147.156.223              RELAY
Connect:irobot.uv.es             RELAY
ClientRate:127.0.0.1             0
ClientRate:147.156.1.90          0
ClientRate:147.156.0.253         0
ClientRate:147.156.222.65        0
ClientRate:                      21
```

Configuración de los ficheros .db (III)

- Ejemplo de fichero local-host-names:

```
# local-host-names - include all aliases for your
# machine here.
localhost
localhost.localdomain
glup
robotica
irtic
glup.uv.es
robotica.uv.es
irtic.uv.es
glup.irobot.uv.es
robotica.irobot.uv.es
irtic.irobot.uv.es
```

Configuración de los ficheros .db (IV)

- Ejemplo de fichero mailertable:

```
uv.es           esmtp:[post.uv.es]
valencia.edu    esmtp:[post.uv.es]
alumni.uv.es    esmtp:[post.uv.es]
.uv.es          esmtp:[%1.uv.es]
```

Configuración de los ficheros .db (V)

- Ejemplo de fichero virtusertable:

```
root@robotica.uv.es          quique
quique@robotica.uv.es        ebonet@amparo.uv.es
@correo.cdlibre.org          barto
```

Configuración de los ficheros .db (VI)

- Ejemplo de fichero trusted-users:

```
# trusted-users - users that can send mail as others
# without a warning apache, mailman, majordomo, uucp,
# are good candidates
apache
```

El fichero de alias (I)

- El fichero de alias:
  - Se encuentra en /etc/aliases.
  - Contiene una relación entre distintos nombres que tienen los usuarios:
    - Enrique.Bonet con ebonet
  - Contiene una relación de nombres que hacen referencia a más de un usuario.
- Se convierte en el fichero /etc/aliases.db con el comando:

```
/usr/bin/newaliases
```

El fichero de alias (II)

- Ejemplo:

```
# Basic system aliases -- these MUST be present.
mailer-daemon: postmaster
postmaster:    root
# General redirections for pseudo accounts.
bin:        root
daemon:     root
adm:        root
lp:     root
...
# trap decode to catch security attacks
decode:     root
# Alias creados
# Alias del administrador de las paginas WEB.
webmaster: root
# Lista de administradores
administradores:   quique@glup.uv.es, susana@glup.uv.es
# Lista de alias de nombres de usuarios
Enrique.Bonet:     quique@glup.uv.es
Susana.Pons:       susana@glup.uv.es
```

El fichero de alias (III)

- El fichero de alias puede tener líneas que impliquen la ejecución de un comando.

```
lista1:       "|/usr/lib/mailman/mail/mailman post lista1"
lista1-admin:  "|/usr/lib/mailman/mail/mailman admin lista1"
...
```

Protocolos de entrega final (I)

- Permiten entregar el correo en el ordenador personal del usuario. Los más conocidos son:
  - POP3.
  - IMAP.
- Su servidor es el programa /usr/sbin/dovecot.
  - Utiliza programas del directorio /usr/libexec/dovecot:
    - imap.
    - imap-login.
    - pop3.
    - pop3-login.
- Su configuración se realiza en:
  - Fichero /etc/dovecot/dovecot.conf
  - Ficheros dentro del directorio /etc/dovecot/conf.d

Protocolos de entrega final (II)

- El fichero dovecot.conf contiene las líneas generales de configuración.

```
protocols = imap pop3
```

- Protocolos permitidos.

```
listen = *
```

- Interfaces en los que dovecot permanece a la escucha.

```
base_dir = /var/run/dovecot
```

- Directorio donde se guarda la información de ejecución.

```
instance_name = dovecot
```

- Nombre de la instancia. Se utiliza si se lanzan múltiples instancias.

Protocolos de entrega final (III)

- El fichero 10-auth.conf contiene los mecanismos de autenticación.

```
auth_mechanisms = plain
```

- Mecanismos de autenticación (plain, CRAM-MD5, DIGEST-MD5, ...).

```
disable_plaintext_auth = yes
```

- Utilizar siempre (valor no) o solo si es segura (valor yes). Se entiende como segura si es sobre SSL o la IP del cliente es local.

Protocolos de entrega final (IV)

- El fichero 10-mail.conf configura los buzones de correo.

```
mail_location = mbox:~/mail:INBOX=/var/mail/%u
```

- Localización de los buzones de correo del usuario si posee un buzón local (mbox) además del buzón de entrada de correo.

```
mail_access_groups = mail
```

- Grupos adicionales que puede utilizar dovecot para ejecutar su trabajo.

Protocolos de entrega final (V)

- El fichero 10-ssl.conf configura SSL en dovecot.

```
ssl = {no | yes | required}
```

- Indica si no se utiliza SSL, se utiliza para usuario/contraseña o se utiliza siempre, sea cual sea la autenticación elegida.

```
ssl_cert = </etc/pki/dovecot/certs/dovecot.pem
ssl_key = </etc/pki/dovecot/private/dovecot.pem
```

- Localización del certificado y la clave privada. Si la clave privada esta protegida por contraseña:

```
ssl_key_password = <fichero_clave
```

- Indica el fichero donde esta la clave.
  - Propietario root
  - Permisos 0600

Protocolos de entrega final (VI)

- Los ficheros 20-imap.conf y 20-pop3.conf contiene:
  - Limites de tamaño de los correos.
  - Etc.
- Sus valores por defecto son correctos en la mayoría de los casos.