

Apunts sobre el correu electrònic

Vocabulari i software:

***MTA (Mail Transfer Agent):** Software servidor que s'encarrega d'enviar els correus a altres servidors MTA (o bé rebre'ls d'altres servidors MTA). Fan servir el protocol SMTP. Exemples de software servidor MTA són:

Postfix (<http://www.postfix.org>)

Exim (<http://www.exim.org>)

Sendmail (<http://www.sendmail.org>)

CourierMTA (<http://www.courier-mta.org>)

Una altra tasca que avui dia també integren tots els programes anteriors és la de **MDA (Mail Delivery Agent)** - antigament ho feien programes separats-, la qual consisteix bàsicament en recollir tots els missatges rebuts pel servidor MTA final (provinents d'altres servidors MTA) i col·locar-los a la bústia personal de l'usuari de destí. Altres tasques d'un software MDA és el filtratge, l'ordenació o la resposta automàtica de correus (quan el destinatari està de vacances, per exemple).

***Servidor POP:** Software que permet als usuaris registrats accedir a la seva bústia personal on trobarà els missatges allà presents (prèviament col·locats allí per algun software MDA). Fan servir el protocol POP3. Opcionalment podrà descarregar aquests missatges al seu ordinador local. Un servidor POP és senzill d'operar i no necessita massa potència...normalment vénen empaquetats juntament amb els servidors IMAP (veure següent paràgraf).

***Servidor IMAP:** Software que permet als usuaris registrats accedir a la seva bústia personal on trobarà els missatges allà presents (prèviament col·locats allí per algun software MDA). Fan servir el protocol IMAP4. A diferència dels servidors POP, però, no es poden descarregar els missatges a l'ordinador local de l'usuari. Una altra de les diferències entre el protocol POP i IMAP és que el primer no permet reorganitzar la bústia en diferents nivells de subcarpetes i/o etiquetes però el segon sí. Un servidor IMAP requereix força RAM i molt d'espai d'emmagatzematge. Exemples de software servidor POP/IMAP són:

Dovecot (<http://www.dovecot.org>)

CourierIMAP (<http://www.courier-mta.org/imap>)

CyrusIMAP (<http://cyrusimap.web.cmu.edu>)

UW Imap Toolkit (<http://www.washington.edu/imap>)

***MUA (Mail User Agent) :** Software que utilitza l'usuari per escriure i enviar nous missatges (fent servir per això un determinat servidor MTA que el MUA ha de tenir configurat) i també per visualitzar els missatges que hi hagi a la seva bústia personal (havent-se de connectar el MUA, per fer això, amb un determinat servidor IMAP/POP que tingui configurat). Exemples de software MUA:

Thunderbird (<http://www.mozilla.org>)

Evolution (<http://projects.gnome.org/evolution>)

Mutt (<http://www.mutt.org>) -Per consola-

Alpine (<http://www.washington.edu/alpine>) -Per consola també-

A més d'un servidor MTA-MDA, un servidor POP/IMAP i un client MUA, que seria el mínim necessari per implementar un sistema complet d'enviament i rebuda de correus, es pot afegir a més altre software addicional:

***Eliminadors d'spam i/o detectors de virus als missatges** (s'instal·len en els servidors MTA-MDA):

SpamAssassin (<http://spamassassin.apache.org>) -AntiSpam-

Assp (<http://assp.sourceforge.net>) -AntiSpam-

MailScanner (<http://www.mailscanner.info>) -AntiSpam i AntiVirus-

Amavis-new (<http://www.ijs.si/software/amavisd>) -AntiVirus-

ClamAV (<http://www.clamav.net>) -AntiVirus-

***Gestors de llistes de correu** (s'instal·len en els servidors MTA-MDA):

Majordomo (<http://www.greatcircle.com/majordomo>)

MailMan (<http://www.list.org>)

***Clients WebMail:** Software MUA que funciona sobre un servidor web, de manera que l'usuari no ha de tenir instal·lat localment cap MUA sinó que amb un navegador pot accedir, com si fos una pàgina web més, a la seva bústia per llegir els missatges rebuts i enviar-ne d'altres. Generalment aquest tipus de software està escrit amb un llenguatge d'script de

servidor com PHP o similar. Exemples de software WebMail són:

SquirrelMail (<http://www.squirrelmail.org>)

Horde IMP (<http://www.horde.org/imp>)

Ilohamail (<http://ilohamail.org>)

Sqwebmail (<http://www.courier-mta.org/sqwebmail>)

RoundCube (<http://roundcube.net>)

Rainloop (<http://www.rainloop.net>)

Webmail-Lite (<https://afterlogic.org/webmail-lite>)

***Suites completes integrades** (inclouen servidor MTA-MDA, servidor IMAP/POP, client WebMail, etc):

Mail-in-a-box (<https://mailinabox.email>)

Les següents suites a més contenen agendes i calendaris, capacitats de missatgeria instantània, etc, de manera que són més aviat una "suite de col.laboració".

Zimbra (<http://www.zimbra.com>)

Zarafa (<http://www.zarafa.com>)

Kolab (<https://kolab.org>)

Citadel (<http://www.citadel.org>)

Autenticació mitjançant SASL i xifratge mitjançant TLS:

Des de sempre als servidors POP o IMAP ha existit l'autenticació per poder accedir a la bústia personal particular de cada usuari loguejat. No obstant, per fer servir un servidor SMTP (és a dir, MTA) antigament no calia registrar-se: es podien enviar correus sense qualsevol tipus de control. Això, òbviament, va originar el problema de l'spam, així que avui dia tots els servidors SMTP comercials implementen un sistema d'accés on s'ha de tenir un compte d'usuari registrat per fer-lo servir com a remitent però si instal·lem un servidor SMTP propi, cal ser conscients de què no hi ha cap sistema d'accés implementat per defecte.

Avui dia la majoria de servidors SMTP (i també d'altres tipus com els IMAP, XMPP o LDAP) estan compilats amb una llibreria anomenada SASL ("Simple Authentication and Security Layer"), la qual permet posar d'acord diferents servidors SMTP per tal de consensuar el mecanisme d'autenticació que faran servir entre ells (i poder-se enviar, per tant, correus entre ells sense rebutjar-los). Si no es fa servir SASL, caldria especificar a mà el mètode d'autenticació a usar en cada servidor SMTP per on el missatge de correu hagués de passar. Cal tenir present, en aquest sentit, que per defecte, un servidor SMTP només accepta enviar correus a un altre servidor SMTP remot si aquests correus estan originats en clients de la seva pròpia xarxa però no pas si provenen d'altres servidors SMTP externs: és per això que un mecanisme d'autenticació ofert per SASL i acordat entre les parts de forma automàtica és vital. Mecanismes d'autenticació oferits per SASL molt comuns són PLAIN, LOGIN, DIGEST-MD5 o GSSAPI, entre d'altres (ho veurem més endavant).

D'altra banda, antigament tampoc s'usava cap mètode d'encryptació per enviar (i consultar) els correus, de manera que els missatges viatjaven per la xarxa totalment en obert. Avui dia es fa servir el protocol TLS per oferir els xifratge dels missatges. Com que aquest protocol se situa, dins la pila TCP/IP, entre la capa de transport i la capa d'aplicació, en aquest cas estarem parlant dels protocols SMTPS, POPS o IMAPS. La seva implantació però, és opcional, així que ens podem trobar servidors comercials (pocs) que no ofereixin l'encryptació de missatges.

El protocol TLS permet també realitzar autenticacions (i per tant, permet no haver s'usar SASL) però per diversos motius històrics avui dia els servidors SMTP usen una combinació de les dues tecnologies: SASL per autenticar i TLS per xifrar. En aquest cas, un cop autenticat l'usuari via SASL, per començar l'enviament de correus encryptats amb TLS cal que s'executi la comanda SMTP especial "STARTTLS", la qual indica el "pas" de comunicació no xifrada a comunicació xifrada.

Degut a totes aquestes variants (amb o sense autenticació, amb o sense xifratge), al llarg de la història els protocols SMTP, POP i IMAP han anat ampliant-se, de manera que avui dia a la pràctica ens podem trobar amb les següents casuístiques:

Servidor SMTP (sense autenticació o amb autenticació SASL només): escolta al port 25

Servidor SMTP (amb autenticació SASL + STARTTLS): escolta al port 587

Servidor SMTP (amb autenticació TLS i xifratge TLS) : escolta al port 465 . Actualment en desús

Servidor POP (amb autenticació SASL només): escolta al port 110

Servidor POP (amb autenticació TLS i xifratge TLS) : escolta al port 995

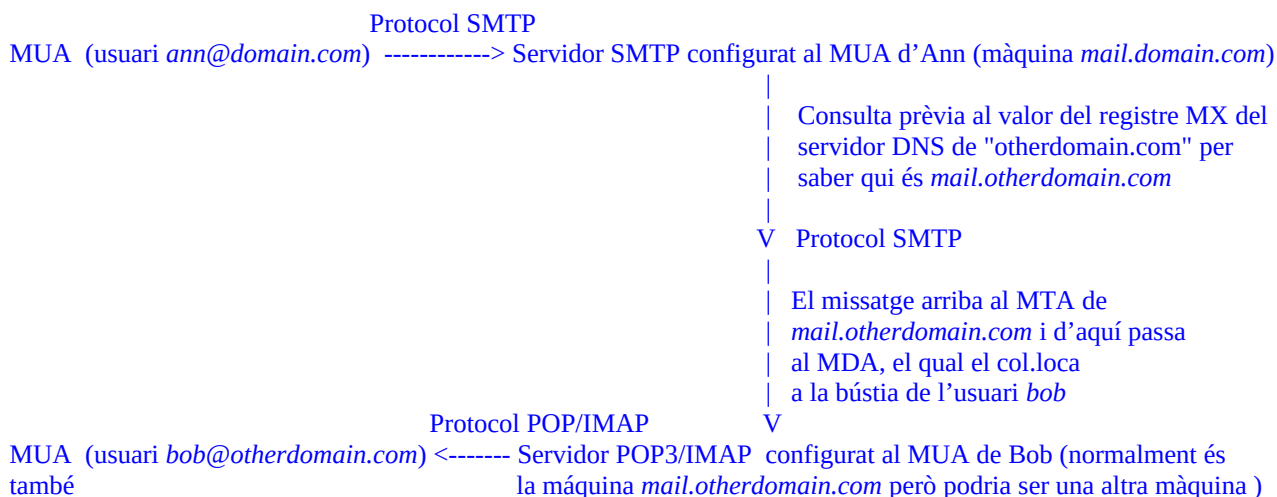
Servidor IMAP (amb autenticació SASL només) : escolta al port 143

Servidor IMAP (amb autenticació TLS i xifratge TLS) : escolta al port 993

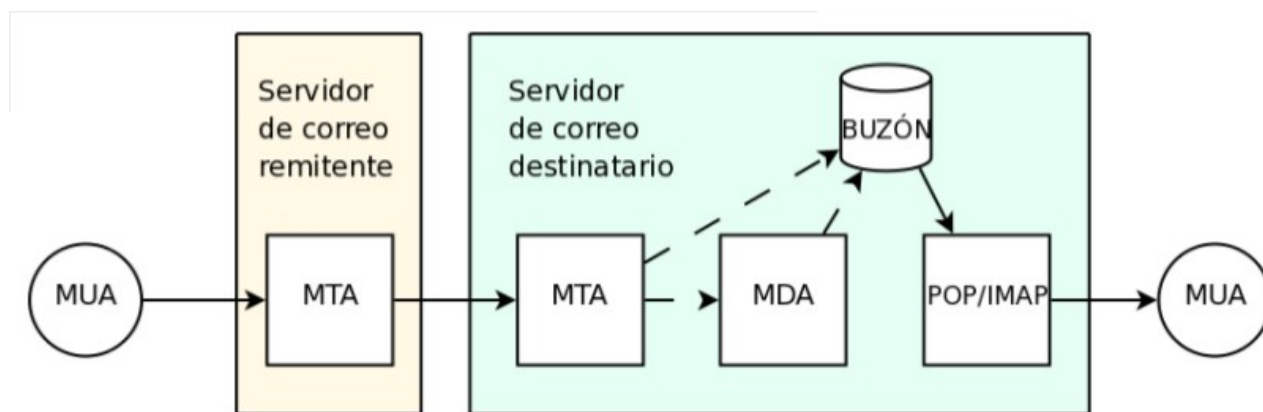
Esquema dels passos realitzats en l'enviament i rebuda d'un missatge de correu:

Básicamente, el envío de emails es un procedimiento donde se envía texto de una máquina a otra, añadiéndose al buzón de correo personal del destinatario. Este buzón, por cierto, actualmente puede estar en formato "mbox" o bien "Maildir" (la diferencia básica entre uno y otro es que el primero implica que todos los mensajes del buzón se encuentran dentro de un único fichero de texto mientras que el segundo implica que cada mensaje será guardado en un fichero de texto por separado).

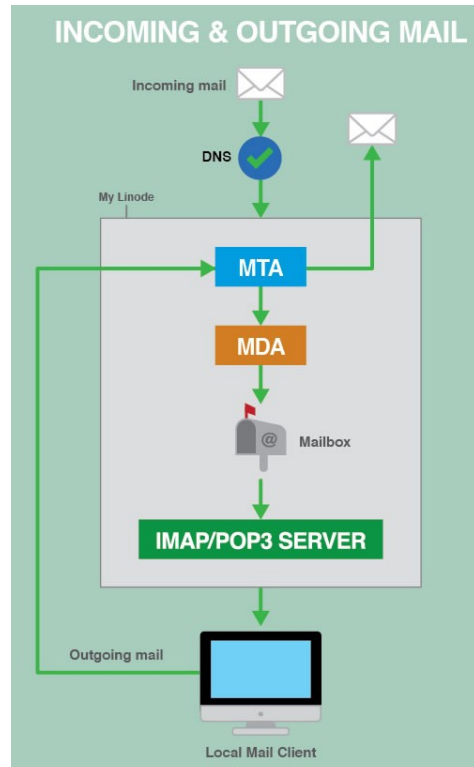
No obstante, este procedimiento es largo y complejo porque intervienen varios programas trabajando en cadena (incluyendo un servidor DNS, imprescindible para que un servidor SMTP sepa quien es el servidor SMTP siguiente!) para conseguir que el email llegue a su destino. Veamos en detalle cómo funciona el correo electrónico. Ann (*ann@domain.com*) quiere enviar un email a Bob (*bob@otherdomain.com*). Gráficamente:



O més bonic (encara que aquí no es mostra el pas intermig entre el quadrat groc i el verd, que és la consulta que ha de fer el servidor de correu groc a algun servidor DNS disponible per saber quin és el valor del registre MX associat al domini de destí -és a dir, la IP del servidor de correu verd-):



Un altre esquema similar és el següent:



Tal como se puede ver en los diagramas anteriores, el email llegará a su destino siguiendo estos pasos:

1.-Ann utiliza algún software cliente de correo (un MUA:como Outlook, Evolution, Thunderbird, Mutt ...) para crear el correo, y enviarlo al servidor SMTP que dicho MUA tenga configurado en primera instancia (en nuestro ejemplo, *mail.domain.com*). Este servidor SMTP normalmente primero comprobará que Ann pueda hacer uso de él comprobando que exista en él un usuario llamado "ann" (es decir, autenti  ndola); si es as  , el servidor SMTP recoge el correo de Ann y lo pone en la cola (en el caso de Postfix, por ejemplo, la cola es una simple carpeta: */var/spool/postfix*).

2.-El servidor SMTP de Ann, *mail.domain.com*, enviar   el correo al servidor SMTP correspondiente al dominio que se halla especificado como destinatario (es decir, si el destinatario es *b@otherdomain.com*, se buscar   el servidor SMTP correspondiente al dominio *otherdomain.com*, y se le enviar   el correo a   l). Este proceso puede no ser directo, y se puede enviar el correo a trav  s de varios SMTP hasta llegar al correcto.     mo sabe la m  quina *mail.domain.com* cu  l es el servidor SMTP de *otherdomain.com*? Pues realizando una consulta Dns del registro MX para ese dominio de destino!

3.-Una vez el correo ha llegado al servidor SMTP de destino,   ste lo puede enviar a alg  n agente intermediario MDA que lo haga pasar por alg  n escaneador de spam o alg  n antivirus. Finalmente, el correo se repartir   en el buz  n adecuado (del usuario bob, en este caso). Tal como hemos dicho, existen b  sicamente dos formatos de buz  n: Mbox y Maildir. Se recomienda emplear el segundo, ya que es m  s moderno y menos propenso a errores; en el formato Maildir un buz  n es en realidad una carpeta Maildir dentro de la carpeta Home del usuario en cuesti  n donde se almacenar  n los diferentes mensajes, cada uno en un fichero diferente (a diferencia del formato Mbox, que guarda todos los mensajes dentro de la carpeta */var/spool/mail/usuario* en un   nico fichero).

4.-El correo ya est   almacenado en el buz  n, pero para acceder a   l (esta vez comunic  ndose mediante el protocolo POP/IMAP contra el software servidor correspondiente, que no es el mismo que el software servidor SMTP), Bob tendr   que utilizar alg  n software cliente de correo (un MUA, otra vez). Evidentemente, para acceder al buz  n previamente se tendr   que autenticar como un usuario v  lido en el servidor POP/IMAP.En principio, los usuarios del servidor de correo son usuarios reales de la m  quina (aunque se puede configurar para que se extraigan de una base de datos tipo MySQL, o mejor, de un servidor LDAP, por ejemplo). Si accede mediante POP3, tendr   la posibilidad de descargar f  sicamente los mensajes desde su buz  n en el servidor a una carpeta local.