1 O servizo de correo electrónico

O servizo de correo electrónico, tamén chamado e-mail, é un dos máis usados en Internet. Permite o envío de mensaxes entre usuarios en modo *asíncrono*. O destinatario dun correo electrónico pode non estar conectado na rede cando o correo fose enviado, e recibilo máis tarde cando se conecte á rede e solicite recibilo.

Buzón

O correo electrónico substituíu en gran medida ao correo tradicional, (servizo postal para envío de cartas, correo certificado e outros tipos de envíos). Especialmente nas comunicacións de empresa emprégase o correo electrónico moitísimo máis que o tradicional xa que, entre outras cousas, reduce notablemente os custos e axiliza as comunicacións. Incluso o correo electrónico pode substituír ao envío de correo certificado, xa que permite o acuse de recibo que certifica a recepción dun correo por un usuario.

O servizo de correo electrónico xa se comezou a usar nos anos 60 do século pasado. Moito antes de que se desenvolvese Internet xa existían unha gran cantidade de usuarios de correo electrónico. Nas súas orixes, o correo electrónico só permitía enviar mensaxes de texto codificados en ASCII. Desde que, nos anos 90, se comezaran a desenvolver os tipos MIME, o correo electrónico permite achegar nas mensaxes arquivos de diversos tipos.

O correo electrónico, baséase en procedementos operativos moito máis complicados que os dos servidores web. Para a maioría dos usuarios, o funcionamento é transparente, o cal significa que non é necesario entender como funciona o correo electrónico para poder utilizalo.

1.1 Sumario

1.2 Elementos do servizo de correo electrónico

Seguro que utilizas diariamente o correo electrónico, e serías capaz de describir o que son ou a función que teñen os elementos básicos do servizo de correo electrónico. De todos os xeitos imos citar cales se poden considerar elementos básicos do servizo de correo electrónico e a describilos:

- **Mensaxe**: é a información que transmite o servizo de correo electrónico. As mensaxes son máis coñecidos como correos ou correos electrónicos. As mensaxes permiten achegar arquivos de diversos tipos.
- **Cliente**: é un programa de usuario que permite editar as mensaxes, envialos cara a un servidor que se encargue de que cheguen ao destinatario, ou de descargar os recibidos dende unha caixa de correo de usuario.
- **Servidor**: é un software que se encarga de recibir correos dun cliente ou doutro servidor funcionando como cliente e de envialos cara a outro servidor ou transferilos cara ao usuario destino. Máis adiante veremos que hai dous tipos de servidores: de transferencia ou de intercambio e de descarga ou de entrega. Os servidores serían o mesmo que son no funcionamento do correo tradicional os carteiros, que se encargan de recoller o correo, seleccionalo, dirixilo cara ao seu destino e deixalo nas caixas de correo dos domicilios dos destinatarios.
- **Contas de correo**: son as identificacións para os remitentes do correo electrónico e os destinatarios. Un usuario pode ter moitas contas de correo. Cada conta de correo está rexistrada nun servidor de correo. Cada conta de correo ten asociado unha caixa de correo de usuario. As contas de correo teñen o formato:

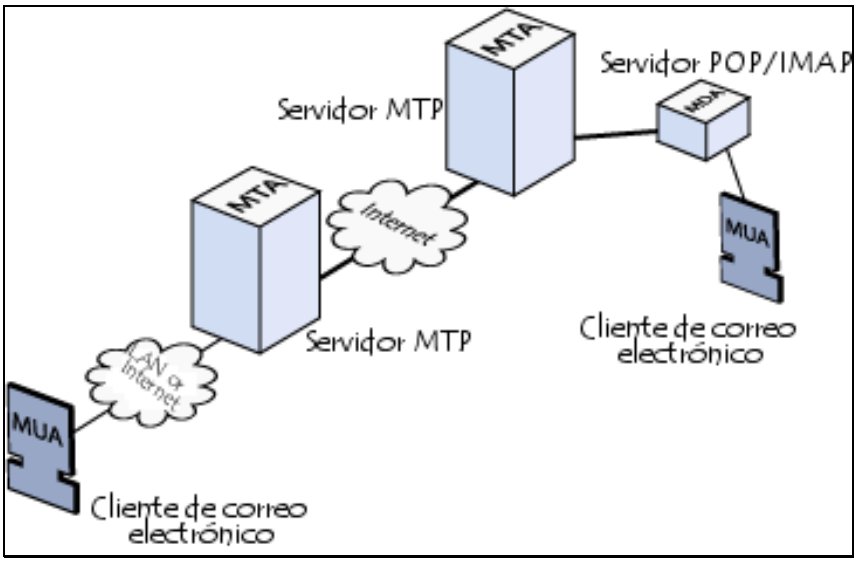
  nome@dominio, como por exemplo *luis@aula1.com*, sendo o nome escollido polo usuario, e o dominio ao que pertence o equipo que ten rexistrada a conta do usuario. Cando se vai a enviar un correo electrónico, consúltase no DNS o nome do dominio para buscar servidores de correo de ese dominio (rexistros MX da zona).

- **Caixa de correo**: é un espazo de almacenamento dun servidor onde este garda as mensaxes destinadas a usuarios para que estes os poidan obter. Cada usuario ten asignada unha caixa de correo de usuario. É igual que a caixa de correo do noso domicilio onde o carteiro deixa as cartas dirixidas a nós.
- **Contas de correo redirixidas**: son contas ás que se asocia unha caixa de correo pertencente a outra conta doutro dominio. Por exemplo, luis@aula2.com pode ser redirixida a luis@aula1.com e entón os correos enviados a luis@aula2.com almacenaranse na caixa de correo de luis@aula1.com.
- **Alcume (Alias)**: son contas ás que se asocia unha caixa de correo doutra conta do mesmo dominio. Por exemplo, profesri@aula1.com pode ser redirixida a luis@aula1.com e entón os correos enviados a profesri@aula1.com almacenaranse na caixa de correo de luis@aula1.com.

1.3 Axentes de correo

Nos RFC que describen o funcionamento do servizo de correo electrónico fálase dos axentes de correo. Un axente de correo é un software que se encarga de realizar algunha operación coas mensaxes de correo. Na transmisión do correo electrónico fundamentalmente interveñen tres axentes:

- **MTA (Correo Electrónico Transfer Agent)**: é un software que se encarga de recibir o correo ou reenvialo a outro axente MTA, ou de deixalo almacenado nunha caixa de correo de usuario. Un MTA pode recibir o correo dende outros axentes MTA ou dende un axente MUA. Un axente MTA debe ter asociado un rexistro MX nunha zona dun dominio para que se poida coñecer a que equipo se ten que enviar o correo destinado a contas dese dominio. Os axentes MTA usan o protocolo SMTP cando transfiren ou reciben correo.
- **MDA (Correo Electrónico Delivery Agent)**: é un software que se comunica cos MUA para entregarlles o correo almacenado nas caixas de correo dos usuarios que estean a utilizar os MUA. Un MDA accede ás caixas de correo dos usuarios e entrega os correos aos MUA utilizando o protocolo POP3 ou o protocolo IMAP.
- **MUA (Correo Electrónico User Agent)**: é un software de usuario onde un usuario pode enviar e recibir correos. Nunha MUA un usuario pode iniciar sesión cunha ou con varias das súas contas. Para cada conta o usuario ten configurado cual vai a ser o MTA que se encarga da transferencia dos correos que vaia enviar e cal vai ser o MDA que se encarga de entregarlle o correo almacenado na caixa de correo de usuario.



1.3.1 Como funciona o correo electrónico?

O correo electrónico xira arredor do uso das caixas de correo de correo electrónico. Cando se envía un correo electrónico, a mensaxe encamíñase de servidor a servidor ata chegar ao servidor de correo electrónico do receptor. Máis precisamente, a mensaxe envíase ao MTA que ten a tarefa de transportalos cara ao MTA do destinatario. En Internet, os MTA comunícanse entre si usando o protocolo SMTP, e polo tanto chámallos servidores SMTP (ou ás veces servidores de correo saínte).

Logo o MTA do destinatario entrega o correo electrónico ao servidor do correo entrante (chamado MDA, do inglés Correo Electrónico Delivery Agent -Axente de Entrega de Correo), o cal almacena o correo electrónico, mentres espera que o usuario o acepte. Existen dous protocolos principais utilizados para recuperar un correo electrónico dun MDA:

POP3 (Post Office Protocol - Protocolo de Oficina de Correo), o máis antigo dos dous, que se usa para recuperar o correo electrónico e, nalgúns casos, deixar unha copia no servidor.

IMAP (Internet Message Access Protocol -Protocolo de Acceso a Mensaxes de Internet), o cal úsase para coordinar o estado dos correos electrónicos (lido, eliminado, movido) a través de múltiples clientes de correo electrónico. Con IMAP, gárdase unha copia de cada mensaxe no servidor, de maneira que esta tarefa de sincronización se poida completar.

Por esta razón, os servidores de correo entrante chámanse servidores POPS ou servidores IMAP, segundo o protocolo usado.

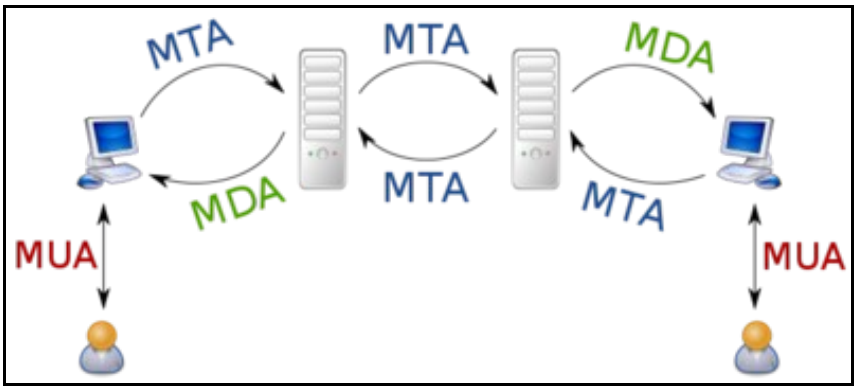
Usando unha analoxía do mundo real, os MTA actúan como a oficina de correo (a área de clasificación e de transmisión, que se encarga do transporte da mensaxe), mentres que os MDA actúan como casas de correo, que almacenan mensaxes (tanto como lles permita o seu volume), ata que os destinatarios accedan á súa casa. Ésto significa que non é necesario que os destinatarios estean conectados para poder enviarlles un correo electrónico.

Para evitar que calquera, lea os correos electrónicos doutros usuarios, o MDA está protexido por un nome de usuario chamado rexistro e un contrasinal.

A recuperación do correo lógrase a través dun programa de software chamado MUA (Correo Electrónico User Agent - Axente Usuario de Correo).

Cando o MUA é un programa instalado no sistema do usuario, chámase cliente de correo electrónico (tales como Mozilla Thunderbird, Microsoft Outlook, Eudora Mail, Incredimail ou Lotus Notes).

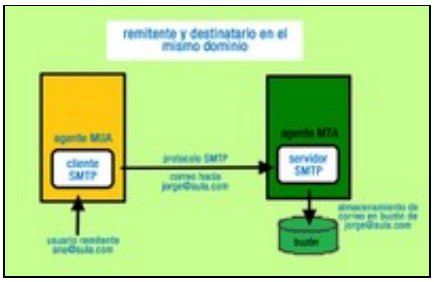
Cando se usa unha interface de web para interactuar co servidor de correo entrante, adóitase chamar webmail.



1.4 Proceso de envío dun correo

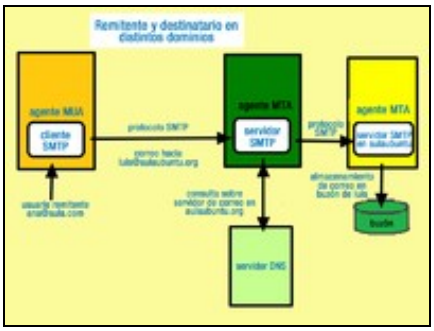
Anteriormente vimos os axentes de correo. Agora imos ver como interveñen estes axentes no envío dun correo dende un remitente cara a un destinatario. Imos ver dous casos distintos, aínda que se poderían ter outros.

As contas de usuario remitente e de destinatario pertencen ao mesmo dominio



Un usuario *ana@aula.com* utiliza un MUA para editar un correo destinado á conta de usuario *lois@aula.com* pertencente ao mesmo dominio. Cando Ana envía o correo, o MUA actúa como cliente SMTP para enviar o correo ao MTA que actúa como servidor SMTP no dominio *aula.com*. Dado que o destinatario pertence ao dominio do MTA, este comproba que ese destinatario ten conta de usuario no dominio. Se é así, deposita o correo na caixa de correo de usuario.

As contas de usuario remitente e de destinatario pertencen a distintos dominio



Un usuario *ana@aula.com* utiliza un MUA para editar un correo destinado á conta de usuario *lois@aulaubuntu.com* pertencente a outro dominio. Cando Ana envía o correo, o MUA actúa como cliente SMTP para enviar o correo ao MTA que actúa como servidor SMTP no dominio aula.com. Dado que o destinatario non pertence ao dominio do MTA, este envía unha consulta ao servidor DNS para descubrir a que MTA debe enviar o correo para que chegue ao seu destinatario. Consulta os rexistros MX do dominio *aulaubuntu.com* para obter o nome do servidor SMTP ao que debe enviar o correo e despois consulta cal é a IP dese servidor. O MTA de *aula.com* actuando como cliente SMTP envía o correo ao MTA de *aulaubuntu.com* actuando como servidor SMTP. O MTA de *aulaubuntu.com* comproba que o destinatario *lois@aulaubuntu.com* ten conta de usuario no dominio. Se é así, deposita o correo na caixa de correo de usuario.

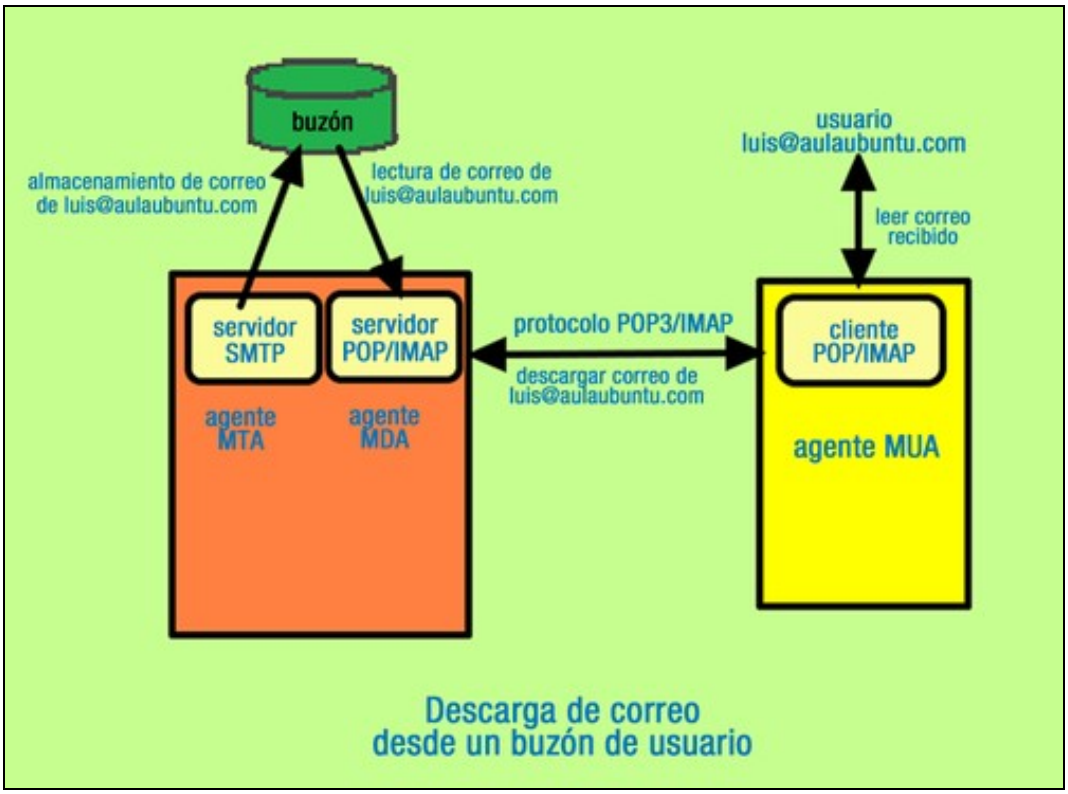
1.5 Proceso de descarga dun correo

Anteriormente vimos como chega un correo a través dun ou varios MTA a unha caixa de correo do usuario destinatario e queda alí almacenado. Para que o usuario destinatario poida ler o correo recibido tería que acceder a consultar a súa caixa de correo.

Hai dous protocolos que son utilizados para que un MUA poida obter o correo almacenado nas caixas de correo de usuario e entregárllelo aos seus destinatarios:

- **POP3**.
- **IMAP**.

O proceso de descarga de correo desenvólvese da seguinte forma:



Un usuario *lois@aulaubuntu.com* inicia unha sesión no MUA do seu equipo.

- O MUA actúa como cliente POP3 e/ou IMAP e contacta co MDA ou servidor POP3/IMAP que teña configurado usando o protocolo correspondente.
- O MUA solicita descargar o correo de *lois@aulaubuntu.com*.
- O MDA do dominio *aulaubuntu.com* le a caixa de correo do usuario *lois@aulaubuntu.com*, obtén as mensaxes almacenadas e entrégallos ao MUA.
- O MUA mostra as mensaxes recibidas ao usuario.

1.6 Estrutura das mensaxes de correo electrónico

O documento RFC 5322 establece cal debe ser a estrutura das mensaxes de correo electrónico. Unha mensaxe está dividida en dúas partes:

- **Cabeceiras ou heads**: conteñen varios campos coa información necesaria para que se poida transmitir correctamente a mensaxe.
- **Corpo ou body**: é o texto da mensaxe.

As cabeceiras conteñen varias liñas de cabeceira, cada unhas das cales dan unha información relativa á mensaxe de correo. Na imaxe de abaixo móstranse algunhas cabeceiras que se mostran ou editan ao crear unha mensaxe co cliente de correo Thunderbird. As cabeceiras que se utilizan con máis frecuencia nas mensaxes son as seguintes:

- **From**: identifica o remitente do correo, a conta de correo do usuario remitente.
- **To**: especifica quen é o destinatario do correo, a conta de correo do usuario destinatario.
- **CC**: indica un conxunto de destinatarios dunha copia da mensaxe que se envía ao destinatario especificado en To. Todos os destinatarios poderán ver, ao recibir un correo con varios destinatarios, as direccións das contas de correo dos outros destinatarios.
- **CCO** ou **BCC**: igual que a anterior, pero neste caso os destinatarios non poden ver as direccións de correo dos outros destinatarios.
- **Subject: é o asunto da mensaxe. É un texto curto que describe o contido da mensaxe.**
- **Date**: indica a data e hora en que se enviou dende o ordenador do remitente a mensaxe. Detrás da hora indícase cantas horas está desfasado o sistema horario do remitente respecto do horario GMT.

- **Reply-To**: especifica a dirección de correo electrónico na que o remitente indica ao destinatario que quere recibir a resposta á mensaxe enviada.

1.7 Clientes de correo electrónico

Un cliente de correo electrónico é un programa de usuario permite que que os usuarios editen e envíen mensaxes de correo e/ou obteñan o correo recibido lendo as caixas de correo do usuario. Existen varios clientes de correo electrónico. A maioría poden actuar como clientes SMTP, POP3 e IMAP, aínda que algúns clientes só poden actuar como clientes dun só protocolo. Hai clientes en modo texto aínda que o máis normal é que os usuarios utilicen clientes gráficos.

Clientes en modo texto:

- **mail**: é un cliente para Linux que só pode traballar con SMTP, polo tanto, non pode descargar correo. Ao executarse, iníciase unha interface de comandos correo electrónico.
- **pine**: É un cliente para Linux moi doado de usar. Permite enviar e descargar correo. Ao executalo iníciase unha interface de ventá con menús pero de tipo texto (non se pode usar o rato).
- **mutt**: É un cliente para Linux moi potente. Permite enviar e descargar correo. Ao executalo iníciase unha interface de ventá con menús pero de tipo texto (non se pode usar o rato).
- **fetchmail**: É un cliente para Linux que só permite ler mensaxes de correo recibidas en caixas de correo.

Clientes en modo gráfico:

- **Mozilla Thunderbird**: Multiplataforma. Pódese instalar en sistemas Windows, Linux, Mac, ...
- **Microsoft Outlook**: So para Windows.
- **Evolution**: Multiplataforma. Pódese instalar en sistemas Windows, Linux, Mac, ...

1.8 Protocolo de transferencia de mensaxes SMTP

Mediante o protocolo **SMTP** (Simple Mail Transfer Protocol) prodúcese o transporte das mensaxes de correo electrónico dende o ordenador do remitente ata que se deposita na caixa de correo do usuario destinatario.

O protocolo SMTP establece conexións cliente servidor, nas que o cliente solicita o envío dunha mensaxe de correo ao servidor, e este encárgase de transportalo cara a outro servidor ou ben de almacenalo en caixas de correo de usuario.

O servidor SMTP comunícase cos clientes no porto TCP 25. Os clientes poden usar calquera porto maior que 1024.

SMTP é un protocolo inseguro porqué transmite a información en texto plano e non require autenticación. Agora é bastante normal que SMTP traballe sobre conexións seguras nas que se cifra a información. Non requirir autenticación pode ocasionar graves problemas xa que calquera usuario podería solicitar o envío de correos a través dun servidor SMTP.

O protocolo SMTP defínese no RFC 2821. Desenvolvéronse varias melloras no funcionamento do protocolo que foron recollidas en varios RFC, por exemplo para mellorar a seguridade no envío de correos. O protocolo establece un conxunto de comandos que os clientes poden enviar aos servidores e os formatos das posibles respostas aos comandos.

1.8.1 Comandos SMTP

Tras establecer unha conexión TCP cliente/servidor no porto 25, o cliente pode comezar a enviar comandos SMTP ao servidor. Os comandos SMTP máis importantes son:

- **`HELO nombre_máquina`**: envíao o cliente para identificarse. Aínda que é válido calquera valor en nombre_máquina, deberíase escribir o nome real.

- **`MAIL FROM:dirección`**: para identificar o remitente do correo. En dirección hai que escribir a dirección de correo electrónico do remitente.
- **`RCPT TO:dirección`**: para identificar o destinatario do correo. En dirección hai que escribir a dirección de correo electrónico do destinatario. Pódese enviar varias veces seguidas este comando cando se quere enviar un correo a varios destinatarios.
- **`DATA`**: para indicar que se vai comezar a enviar a mensaxe. Este ten que rematar cunha liña que teña só un punto e pulsando despois ENTER.
- **`SUBJECT:asunto`**: permite especificar o asunto da mensaxe. É obrigatorio que este comando se envíe a continuación de DATA, que despois se envíe unha liña en branco e despois o contido ou corpo da mensaxe.
- **`QUIT`**: pecha a conexión cliente servidor.

Tamén podemos enviar correos establecendo unha conexión mediante *telnet* ao porto 25

```
telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 servidor.probas.lan ESMTP Postfix (Debian/GNU)

HELO root
250 servidor.probas.lan
MAIL FROM: root
250 2.1.0 Ok
RCPT TO: anton
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
SUBJECT: Saber que tal vas...
Hola Antón, qué tal vai todo por ahí?
Unha aperta.
.
250 2.0.0 Ok: queued as 9F1EB2E530
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

1.8.2 Códigos de resposta

O servidor SMTP envía respostas ao cliente para indicarlle como foi procesado un comando. Nas respostas SMTP o servidor envía un código numérico de 3 díxitos co que indica como foi procesado o comando ao que corresponde a resposta. O primeiro dos díxitos indica se o comando foi ou non procesou con éxito. Os outros dous díxitos dan maior detalle do contido da resposta.

Códigos de respostas SMTP

Código	Descrición
2xy	A acción realizouse con éxito. Pode enviarse outro comando.
3xy	estase a esperar que o cliente envíe información adicional necesaria para poder completar a acción.
4xy	indícase que se produciu un erro temporal e que podería enviarse o comando novamente para posiblemente procesarse con éxito.
5xy	indícase que se produciu un erro permanente, seguirase producindo aínda que se siga enviando o comando.

1.9 Protocolos e servizos de descarga de correo

Anteriormente vimos que os servidores SMTP se encargan de transportar as mensaxes de correo dende o ordenador cliente SMTP do remitente ata a caixa de correo do usuario destinatario. Nesta caixa de correo quedan almacenadas as mensaxes como arquivos. Un usuario podería consultar as mensaxes recibidas accedendo á súa caixa de correo (unha carpeta no disco do servidor onde o usuario ten a conta de correo) e editando os arquivos, pero evidentemente isto non é realizable na práctica cando o usuario non ten acceso ao ordenador servidor.

Ademais do protocolo SMTP de transferencia de mensaxes de correo electrónico, existen dous protocolos (POP3 e IMAP) para a descarga de correo polos usuarios receptores dende as súas caixas de correo de usuario. Estes protocolos son

Para ámbolos dous protocolos, un cliente do protocolo establece unha conexión autenticada cun servidor e unha vez establecida a conexión permite que o usuario, dende o cliente, poida acceder ao correo da súa caixa de correo, solicitar a súa entrega e xestionalo.

Cando un usuario iniciou un programa cliente de correo e solicita acceder ao correo recibido nunha das súas contas, o programa cliente pídelle un contrasinal que será a correspondente á conta de correo que estea a usar. O cliente de correo enviará a dirección de correo da conta e o contrasinal ao servidor que validará estes para iniciar a conexión cliente-servidor.

1.9.1 Características e funcionamento de POP

O protocolo POP (post Office Protocol, traducido como Protocolo de Oficina de Correo) é un protocolo cliente/servidor para a entrega ou descarga de correo dende as caixas de correo de usuario nos servidores aos programas clientes de usuario.

Actualmente úsase POP3 (versión 3 do protocolo). As normas de funcionamento do protocolo pop3 desenvólvense no RFC 1939. O protocolo POP3 escoita os clientes no porto TCP 110.

É necesario que un usuario teña unha conta de correo nun servidor para que o usuario poida ter unha caixa de correo de correo e, polo tanto, para que poida acceder a esa caixa de correo. Ademais, para usar POP3 como protocolo de descarga, será necesario que o cliente de correo poida usar o protocolo POP3, que o servidor de descarga sexa un servidor POP3 e que o cliente envíe ao servidor a dirección de conta e o contrasinal correcto.

> O protocolo POP3 é un protocolo inseguro xa que, aínda que utiliza autenticación, todo o intercambio de información se realiza en texto plano (sen cifrar) incluídos a dirección de correo e o contrasinal. O protocolo POP3S mellora a seguridade encriptar ou cifrando mediante SSL a información transmitida. O protocolo POP3S usa o porto 995.

Unha conexión cliente/servidor POP3 desenvólvese da seguinte forma:

- *Conexión*: o cliente solicita establecer unha conexión de transporte co porto TCP 110.
- *Fase de autorización*: tras establecerse a conexión TCP, o cliente autentícase ante o servidor enviando a dirección de correo e o contrasinal do usuario mediante os comandos POP3 USER e PASS.
- *Fase de transacción*: dende o cliente xa se poden enviar comandos ao servidor para xestionar o correo e listalo, descargalo, eliminalo, etc.
- *Fase de actualización*: Iníciase cando o cliente solicita pechar a conexión POP3 enviando o comando QUIT. É nesta fase cando o servidor elimina realmente mensaxes que foran marcadas para ser borrados.

Nunha conexión POP3 o cliente envía comandos e o servidor devolve respostas. Os comandos de POP3 descríbense no RFC 1989.

1.9.2 Características e funcionamiento de IMAP

Ao igual que POP3, o protocolo IMAP (Internet Message Access Protocol) é un protocolo para a descarga de correos dende as caixas de correo de usuario aos clientes do servizo. Actualmente trabállase coa versión 4 deste protocolo (IMAP4) desenvolvida no RFC 3501.

Un servidor IMAP establece as conexións cos clientes no porto TCP 143 e se se usa o protocolo IMAP seguro para transmitir a información cifrada, utiliza o porto TCP 993.

O funcionamento de IMAP presenta varias diferenzas con respecto a POP3:

- *Mantemento de conexións*: con POP3 mantense a conexión mentres se descarga o correo. Con IMAP mantense a conexión mentres o cliente está activo. Trabállase en liña e, polo tanto, o usuario pode ver ao momento cada novo correo recibido.
- *Acceso a partes das mensaxes*: IMAP permite obter parte das mensaxes ou algúns dos obxectos MIME incluídos sen ter que descargar todo o correo.
- *Soporte para acceso simultáneo a varias caixas de correo*: IMAP permite que un usuario poida acceder a varias caixas de correo simultáneamente e mesmo mover mensaxes dunha caixa de correo a outro.
- *Respaldo para buscas*: IMAP permite que o usuario poida realizar buscas de mensaxes que cumpran determinados criterios.
- *Acceso simultáneo a unha caixa de correo*: IMAP permite que se estea a acceder a unha mesma caixa de correo dende varios clientes. Isto é adecuado cando unha caixa de correo corresponde a unha conta de usuario utilizada por varias persoas.
- *Correo permanece no servidor*: IMAP permite que o correo permaneza ata que o usuario decida eliminalo. Con POP3, por defecto o correo elimínase do servidor cando foi descargado polo cliente.

1.10 Servidores de correo

Á hora de elixir un software servidor de correo electrónico hai varios servidores. Na elección terase en conta que sexa doadamente configurable e que teña moitas opcións de configuración, a xestión de contas de usuario e caixas de correo, o filtrado de correos, a seguridade que implementar etc. Tamén se debe ter en conta o sistema operativo sobre o que se vai instalar, o consumo de recursos, a rapidez de resposta, etc.

Agora imos realizar unha clasificación do software servidor en función de que corresponda a un servidor de transferencia de correo, de descarga de correo ou é á vez ambos os dous. Para cada servidor tes un enlace ao sitio oficial.

Servidores SMTP (Axentes MTA)

- Postfix: ten só distribución para Linux con licenza IBM Public License.
- Sendmail: ten só distribución para Linux con licenza GNU GPL.
- Exim:Exim4 e outro MTA desenrolado pola University of Cambridge paro usar en sistemas Unix/Linux conectados a Internet. Pode ser usado no canto de Sendmail, anco a configuración e un tanto diferente.
- Qmail: ten só distribución para Linux con licenza GNU GPL.

Servidores POP3/IMAP (Axentes MDA)

- Dovecot: ten só distribución para Linux con licenza MIT e LGPL.
- Cyrus IMAP server: ten só distribución para Linux con licenza BSD.

Servidores SMTP e POP3/IMAP

- Microsoft Exchange Server: é un servidor para sistema Windows de pagamento e con licenza propietaria. Ten unha versión de avaliación de 30 días.
- hMailServer: é un servidor para sistemas Windows gratuíto e de licenza GPL.
- Zymbra: É un servidor para sistemas Windows, Linux e MacOS. Ten distribucións de código aberto e de código pechado. Distribúese con licenza Zymbra Public License.

1.11 Integración de servidores en DNS

Para enviar unha mensaxe de correo e que chegue á caixa de correo do usuario destinatario, é necesario coñecer o servidor de correo encargado da caixa de correo de usuario e o seu enderezo IP. Será o servidor de correo do dominio ao que pertence a conta de correo do destinatario, o que deberá estar integrado na zona DNS.

Antes de enviar unha mensaxe a ana@aula.com dende unha conta de correo dun dominio diferente faise unha consulta ao servidor DNS responsable da zona aula.com. Neste servidor consúltase:

- Rexistro MX que indique o nome dun servidor MTA de correo para o dominio.
- Rexistro A que indique o enderezo IP do servidor de correo.

Obtido o enderezo IP do servidor, establecerase unha conexión SMTP co equipo que ten ese enderezo e enviaráselle a mensaxe de correo.

Para integrar un servidor MTA de correo nunha zona DNS hai que engadir na zona:

- Un rexistro MX que indique o nome do equipo servidor de correo.
- Un rexistro A que indique o enderezo IP do servidor de correo.
- Aínda que non é obrigatorio débese engadir un rexistro PTR na zona inversa para resolver o enderezo IP do servidor de correo. Isto é así porque algúns servidores de correo, ao recibilo dende outro servidor, verifican que o enderezo IP corresponde ao servidor remitente

mediante o rexistro PTR, (se non hai rexistro PTR ou é incoherente co rexistro A, a mensaxe de correo rexéitase).

1.12 Servidores open relay e servidores smart host

Dise que un servidor de transferencia de correo (MTA) é open relay cando permite reenviar a través del calquera correo recibido dende outro servidor MTA ou dende un MUA. Un servidor deste tipo pode ser usado para enviar indiscriminadamente a través del spam, virus, etc., debido a que non controlan o acceso dos remitentes.

Moitas veces estes servidores de correo poden estar configurados en modo open relay por descoido, por descoñecemento, por erro de configuración ou por modificación na súa configuración por un atacante, pero noutros moitos casos instálanse servidores en modo open relay para facilitar o envío de spam, de virus e doutros axentes maliciosos.

Por defecto, e por razóns históricas, antes non era necesario autenticar a propia identidade, para enviar un correo electrónico, o cal significa que era moi doado falsificar enderezos cando se enviaba un correo. Hai elaboradas listas negras de servidores de correo open relay sobre os que se detectaron usos maliciosos. As listas negras serven a outros servidores para detectar automaticamente o correo lixo ou spam.

Por esta razón, hoxe en día, case todos os provedores de servizo de Internet bloquean os seus servidores SMTP para que só os seus subscritores poidan usalos, ou máis precisamente só as máquinas cuxos enderezos IP pertenzan ao dominio do ISP. Ésto explica a razón pola cal os usuarios que viaxan, deben modificar a configuración do servidor de saída dos seus clientes de correo electrónico, para que lles permita enviar correos dende ISP distintos ao seu propio.

Cando o servidor de correo electrónico dunha organización está mal configurado e permite que terceiros, en calquera rede, envíen correos electrónicos, ésto denomínase relé aberto.

Xeralmente os relés abertos son usados polos spammers, xa que ao facelo, esconden a verdadeira orixe das súas mensaxes. Como resultado, moitos ISP manteñen unha lista negra actualizada de relés abertos, para evitar que os subscritores reciban mensaxes de tales servidores.

Se nun servidor open relay se establecen uns enderezos doutros servidores SMTP autorizados a reenviar correo a través do servidor e se lle denega o permiso para reenviar a calquera outro servidor, dise que o servidor é un smart host. Na autorización pódense dar enderezos IP e/ou nomes de servidores, enderezos de rede, rangos de enderezos ou nomes de dominios.

1.13 Servizo de correo electrónico vía web

Cando queremos ter un servidor de correo para o noso dominio podemos instalar o noso propio servidor ou contratar o servizo a un servidor de correo electrónico vía web.

Normalmente, as empresas de hosting adoitan proporcionar este servizo. O servizo contratado darase nunhas determinadas condicións, entre outras:

- Espazo total de disco dispoñible para as caixas de correo de usuarios.
- Máximo número de contas de usuario e tamaño máximo das caixas de correo de usuario.
- Sistemas de seguridade.
- Acceso a aplicacións polos clientes que accedan ao servizo.
- Tipo de asistencia.

Hai moitas empresas que ofrecen este servizo. Un dos máis coñecidos é Google Apps for Work, anque tamén Zoho ou Outlook tamén son moi usados.

Tamén temos a posibilidade de instalar un cliente web de correo. O máis coñecido e Roundcube

1.14 Correo seguro

Os protocolos SMTP, POP3 e IMAP non son protocolos seguros xa que todos eles transmiten a información en texto plano e polo tanto, a información é susceptible de poder ser consultada e modificada doadamente por terceiros. A diferenza do protocolo SMTP que non autentica aos usuarios que envían correo, os protocolos POP3 e IMAP requiren autenticación dos clientes usando un nome de usuario e un contrasinal en texto plano.

Estes protocolos tampouco implementar ningún sistema para asegurar que os ordenadores clientes, os ordenadores servidores e os usuarios sexan os que aseguran ser nas mensaxes de correo ou nas mensaxes de conexión.

O correo seguro debe garantir:

- Confidencialidade: só o destinatario debe poder ler a mensaxe de correo.

- Integridade: débese evitar que o correo poida ser modificado por terceiros durante a transmisión e, se o é, debe poder detectarse a modificación.
- Autenticación: debe controlarse a identidade dos usuarios.

Hai varias vulnerabilidades sobre o correo electrónico producidas por unha deficiente seguridade:

- Suplantación da identidade para enviar ou recibir correo.
- Acceso a información sen autorización.
- Transmisión de correo spam.
- Transmisión de información para estafar receptores de correo, e outras moitas.

Sobre os protocolos SMTP pódense implementar extensións que permiten:

- Autenticar usuarios mediante varias técnicas como a autenticación SASL.
- Cifrado das mensaxes mediante encapsulamiento sobre protocolos SSL/TLS.

Na actualidade, os servidores de correo usan protocolos seguros en lugar dos protocolos SMTP, POP e IMAP. Basicamente trátase dunhas especificacións que melloran estes protocolos encapsular os sobre conexións SSL/TLS que garanten a confidencialidade, a autenticación e a integridade.

- **SMTPS**: garante a integridade das mensaxes transmitidas cara a servidores SMTPS e a confidencialidade, así como a autenticación dos servidores ante os clientes. Usan o portos TCP 465 e 587.
- **POP3S**: utiliza o porto TCP 995.
- **IMAPS**: utiliza o porto TCP 993.

1.15 Sinatura dixital

Cando recibes unha mensaxe de correo, na mensaxe figura o remitente. Pero iso non nos garante que realmente a mensaxe proceda dese remitente nin que a mensaxe sexa o mesmo que enviou o remitente. A mensaxe poderíase ter emitido dende algún servidor que o permitise suplantando a identidade do remitente, ou podería ter sido interceptado e modificado durante o seu envío e paso por servidores de correo intermedios.

A sinatura dixital utilízase para que o destinatario dunha mensaxe poida verificar que o remitente é quen di ser na mensaxe.

A sinatura dixital é especialmente útil no correo electrónico pero tamén pode ser utilizada na transmisión de datos noutros servizos de rede. Ao recibir unha mensaxe de correo asinado:

- Podemos asegurar a identidade do emisor.
- O remitente non pode repudiar a mensaxe, é dicir, non pode negar que o enviou.

A sinatura dixital dunha mensaxe consiste en obter un código de sinatura que se engade á mensaxe aplicando á mensaxe un algoritmo baseado nunha chave privada. O destinatario usará unha chave pública que terá recibido para verificar a autoría de todas as mensaxes asinadas procedentes dun determinado remitente.

Para que un usuario dispoña dunha chave privada e unha chave pública para asinar e cifrar mensaxes debe obter un certificado asinado por unha entidade autoridade de certificación como pode ser, por exemplo, Verisign. Este certificado garante a identidade do propietario e a relación entre a chave privada e a chave pública. Os destinarios das mensaxes asinadas obteñen a chave pública para verificar a sinatura dende as autoridades de certificación.

Cando un destinatario recibe dende un remitente unha primeira mensaxe asinada usando unha chave privada correspondente a un certificado autoasinado, o programa cliente alerta ao usuario de que non se pode garantir a autenticidade da sinatura e se se quere aceptar o certificado correspondente (implica solicitar a chave pública para verificar a autoría da sinatura). Para as seguintes mensaxes que nos envíe o mesmo remitente e que estean asinadas, o cliente non nos alerta e simplemente comproba a identidade do remitente usando a chave pública que recibiu coa primeira mensaxe.

Unha vez que dispoñemos dun certificado asinado e, polo tanto, dunha chave privada para asinar e dunha chave pública para que os destinatarios verifiquen a sinatura, podemos asinar calquera mensaxe usando os clientes de correo electrónico.

1.16 Cifrado de mensaxes

Se as mensaxes de correo electrónico se transmiten codificadas en texto plano e son interceptados por un terceiro, este poderá ler perfectamente a mensaxe. A interceptación pode realizarse de moitas e variadas formas no paso das mensaxes polos servidores de correo ou polo seu almacenamento nas caixas de correo.

O cifrado dunha mensaxe de correo evita que unha persoa que acceda á mensaxe poida interpretalo xa que estará codificado nun "código secreto" ou código cifrado.

Cando un cliente de correo envía unha mensaxe de correo cifrado:

- Antes de enviar, cifra a mensaxe aplicando un algoritmo de cifrado a partir dunha chave pública que debe ter para enviar correos cifrados ao destinatario.
- A mensaxe viaxa cifrado e é almacenada desa forma na caixa de correo do destinatario.
- O programa cliente destinatario descarga o correo cifrado e aplícalle un algoritmo de descrifrado a partir dunha chave privada que só el coñece. Tras isto xa pode mostrar a mensaxe para que o lea o usuario destinatario.

Se un terceiro intercepta un correo cifrado, accederá ao seu contido pero non poderá interpretalo xa que descoñecerá a chave privada para descifrar a mensaxe.

Se un usuario quere enviar un correo cifrado mediante un programa cliente, tívose que recibir antes unha chave pública do usuario destinatario dese correo, (non se pode enviar un correo cifrado a un destinatario sen ter a súa chave pública).

Se, por exemplo, Luis envía a Eva unha mensaxe de correo asinado, na firma inclúese a chave pública do certificado de Luis (para que Eva poida verificar a validez da firma). Esa chave pública poderá ser usada agora por Eva para enviarlle correos cifrados a Luis.

Só o destinatario real da mensaxe de correo poderá interceptalo porqué "coñece o código secreto" ou a chave para descifrar.