Universidad de Costa Rica

Facultad de Ingeniería

Escuela de Ciencias de la Computación e Informática

Redes de Comunicación

CI-0121

Profesor: Mag. José Antonio Brenes Carranza

I Proyecto de Investigación

Servicios de red: Correo electrónico (SMTP, IMAP, POP3)

Elaborado por:

Derrick Allen Smith	B20208
José Alberto Chaves	B72142
Juan Garro Nuñez	B83249
Ronald Leon Morales	B33733
Sergio Ortega Carpio	B65162

Septiembre 2020

Introducción

Como bien se sabe, las redes de comunicación de datos están compuestas por diferentes protocolos y servicios. Por otro lado, es bien sabido que estos protocolos y servicios están divididos según la necesidad que se tenga y por supuesto por una división a nivel de capas de un modelo llamado OSI, el cual posee siete de estas capas anteriormente mencionadas.

Este proyecto de investigación tiene como objetivo explorar algunos de los principales servicios de red para correo electrónico. A lo largo de este documento se detallan las principales características de los protocolos SMTP, IMAP y POP3 iniciando con un breve vistazo a la historia de los mensajes de correo.

Se trabaja una especie de eje transversal donde se menciona de manera breve como estos protocolos se complementan con algunos otros protocolos que residen en capas superiores e inferiores. Además, se mencionan aspectos relevantes a la arquitectura involucrada en la transmisión de mensajes de correo electrónico, aspectos de seguridad relacionados a cada unos de los protocolos mencionados, ejemplos de sesiones, entre otras cosas.

Historia

La historia del correo electrónico que conocemos hoy en día se divide en dos etapas, en primer lugar la correspondencia utilizando cartas físicas junto con el suceso del correo pre-internet. La segunda parte será post-internet junto con lo que conocemos el día de hoy como correo electrónico o email.

Evidentemente se contaba con anterioridad el sistema de entrega de correos o correspondencias, este sistema puede constar de siglos, incluso tiempo después de que en la humanidad haya descubierto y formalizado un método estructurado para comunicarse de forma escrita. Con el paso del tiempo este sistema se mejoró gracias a los medios de transportes que se utilizaban, todo esto sucedía mientras no se estaba cerca de la época pre-internet, esta época la vamos a definir a conveniencia como la época en la que se estaba sumamente cerca de descubrirse el internet y con esta herramienta las muchas utilidades que conlleva.

Según Scheerder el primer sistema de correo se implementó en las instalaciones de MIT con el Sistema de Tiempo Compartido en el año 1965 (Jeroen Scheerder & C. P. J. Koymans, 2007). Este sistema de tiempo compartido era una estructura en la que podían interactuar múltiples usuarios y tenían la opción de compartir en una única ocasión información.

Después en 1971 aparece Ray Tomlinson quien envía oficialmente el primer mensaje de correo donde el medio en el que se compartió fue ARPANET - esta fué una red que se implementó en Estados Unidos por el Departamento de Defensa (DoD) para comunicarse entre diversos estados, es el predecesor del internet - y fué utilizado FTP como protocolo de envío, con esto ya se terminaría la etapa pre-internet.

En la etapa post-internet aparece en primer lugar el UUCP, este es un sistema creado en 1978 en los Bell Labs, este era un sistema en Unix que permitía enviar información de un servicio Unix a otro Unix, entre ellos correos y noticias.

Antes de que apareciera el protocolo UUCP, se había creado el DECnet, este protocolo fue implementado por la empresa Digital Equipment Corporation (DEC) el cual permitía comunicarse entre diferentes dispositivos sin importar la marca para poder hacer el almacenamiento y envío de correos.

A principios de la década de los 80s aparece el BITNET (Because It's Time Network por sus siglas en inglés), protocolo creado por IBM que permitía el almacenamiento y envío de mensajes electrónicos.

Arquitectura

Para iniciar, se debe notar que el servicio SMTP y DNS que son muy utilizados para correo electrónico pertenecen a la capa 7 o capa de Aplicación.

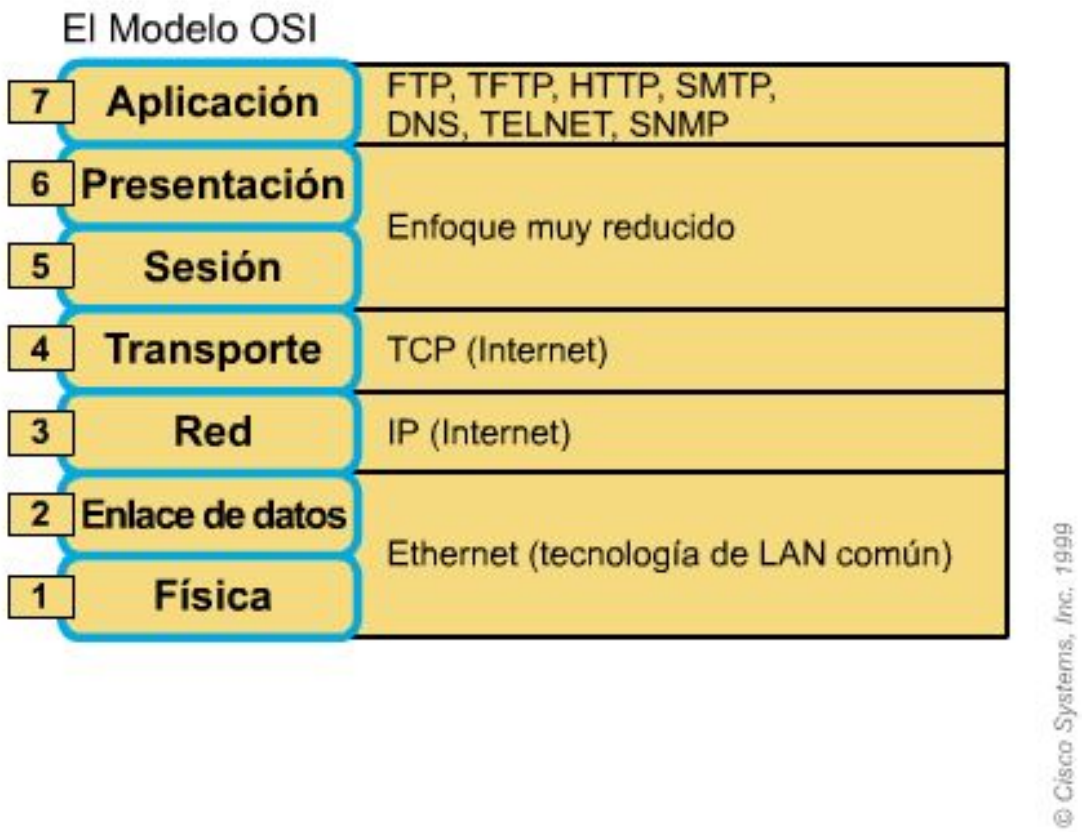

Figura 1. Cuadro del modelo OSI

Para explicar la estructura involucrada en la transmisión del correo electrónico, se puede observar distintos tipos de agentes involucrados en la transmisión de los mensajes:

- Mail User Agent (MUA): interfaz para leer y escribir los mensajes. Aquí se utiliza el protocolo IMAP o POP.
- Mail Transfer Agent (MTA o servidores de correo): encargado del transporte de los mensajes. Aquí se utiliza el protocolo SMTP.
- Mail Delivery Agent (MDA): Recibe información de servidores MTA para asegurarse de entregarlos al cliente que lo debe recibir.
- Mail Submission Agent (MSA): Recibe información de los MUA para asegurarse que son enviados al destinatario.

Actualmente, el correo electrónico es un método para enviar, almacenar y recuperar mensajes electrónicos a través de una red. Los mensajes de correo electrónico se guardan en bases de datos en servidores de correo. Para ejecutar el correo

electrónico en cualquier dispositivo se requieren varios servicios y aplicaciones como se muestra en la figura de abajo.

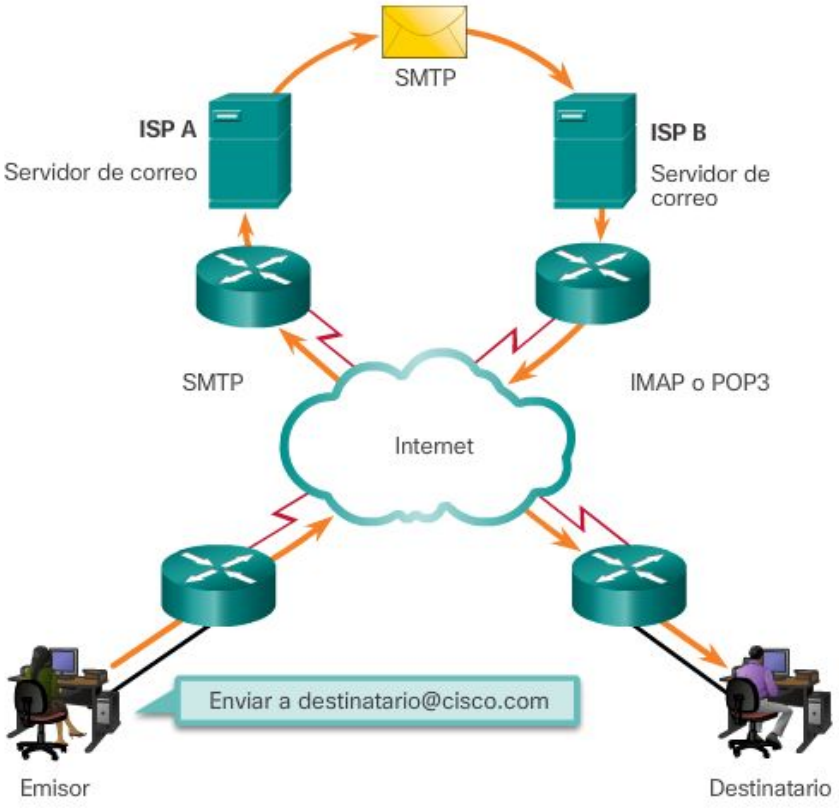

Figura 2. Ejemplo de intercambio de mensajes de correo electrónico.

El agente de usuario o clientes de correo (MUA) se comunica con servidores de correo (MTA) para enviar y recibir mensajes de correo electrónico. Los servidores de correo utilizan el protocolo SMTP para comunicarse con otros servidores de correo para transportar mensajes desde un dominio a otro, posteriormente en el documento se menciona cómo es que los MTA resuelven esos dominios y básicamente es consultandole al DNS.

Los clientes de correo dependen del servidor de correo para el transporte de los mensajes. Los MTA son los encargados de la transmisión de los mensajes de un servidor de correo a otro, los encargados de la administración y como esos mensajes son entregados al destinatario es responsabilidad de las configuraciones que se hagan en nuestro cliente por medio de POP3 o IMAP.

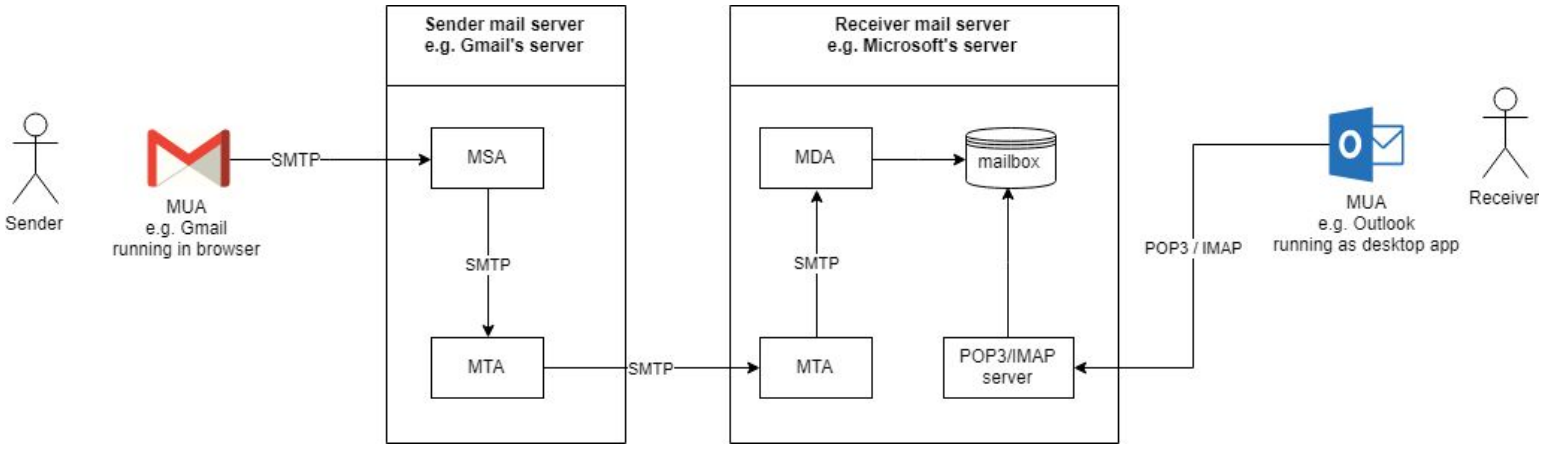

Figura 3. Diagrama de uso del proceso de intercambio de correo electrónico.

Algunas de las marcas más reconocidas para la implementación de servidores de correo electrónico son ***Exchange Email*** de la compañía Microsoft y ***Postfix*** muy popular en el mundo del código libre o abierto.

Protocolos de correo electrónico

Según la Escuela de Sistemas Informáticos, en 1980 Suzanne Sluizer y Jon Postel realizaron trabajos con un protocolo que posteriormente se denominaría SMTP ("Simple Mail Transfer Protocol"). El protocolo SMTP fue desarrollado pensando en que los sistemas siempre iban a intercambiar mensajes por medio de grandes computadores utilizando tiempo compartido y multi usuarios conectados de forma permanente a internet. Sin embargo, con la aparición de las computadoras portátiles y de escritorio que tienen una conectividad ocasional, se hizo necesaria una solución para que el correo llegara a estos equipos.
Para solventar esta limitación, en 1984 surge POP. Este protocolo, en su especificación inicial, solo permite funciones básicas como recuperar todos los mensajes, mantenerlos en el servidor y borrarlos, lo cual mejoró sus funcionalidades hasta llegar a POP3.

El correo electrónico admite tres protocolos diferentes para su funcionamiento: el protocolo simple de transferencia de correo (SMTP), el protocolo de oficina de correos (POP), y el protocolo de acceso de mensaje de Internet (IMAP). El proceso de capa de aplicación que envía correo utiliza SMTP. Sin embargo, un cliente recupera el correo electrónico mediante uno de dos protocolos de capa de aplicación: POP o IMAP.

A continuación se detallan los protocolos previamente mencionados.

SMTP

Este protocolo se considera parte o una extensión del protocolo TCP/IP, básicamente pretende estandarizar la comunicación que existe entre los diferentes MTAs emisores y receptores y es el protocolo utilizado en la actualidad. Permite la transferencia de mensajes de correo de un servidor a otro.

Su propósito principal es enviar, recibir y retransmitir correos entre los emisores y receptores, además de reportar si hubieron errores. El RFC 5321, el cual es una norma para los protocolos de correos electrónicos, definió utilizar el puerto 25 del protocolo TCP, como el puerto estándar de SMTP, pero en la actualidad han surgido algunas complicaciones relacionadas el uso de ese puerto, por lo que también se han definido el uso de otros puertos para SMTP, como el 465 y el 587.

SMTP es únicamente utilizado para la transmisión de mensajes, limitado a solamente caracteres ASCII sin color, fuente, imágenes, gráficos, etc. Actualmente es muy probable que los mensajes contengan otros archivos adjuntos o inclusive como parte del *body* del correo, para esto se crearon lo que se conocen como *workarounds* o extensiones para poder cubrir estas limitaciones. Estos *workarounds* están definidos en el Multipurpose Internet Mail Extensions (MIME). El MIME se divide en 3 partes:

- Parte 1: Format of Internet Message Bodies
- Parte 2: Media Types
- Parte 3: Message Header Extensions for Non-ASCII Text

Las partes mencionadas en conjunto forman el MIME, que redefine el formato de los mensajes para permitir entre otras muchas cosas:

- Mensajes con otra codificación diferente de US-ASCII.
- Imágenes
- Audio
- Video
- Información en otros tipos de datos para ser interpretada por aplicaciones.

Formato del mensaje de correo
Email File Format (EML)

El formato EML está compuesto de 2 partes:

1. Header: Información sobre el encabezado del mensaje. Incluye:
    a. La dirección del “Sender”, es decir, el que envía.
    b. Las direcciones de los que reciben. “Recipient”.
    c. El título o “Subject” del mensaje.
    d. Estampilla de fecha y tiempo del mensaje
    e. Ejemplo:

        From: sender@email.com

        To: recipient@email.com

        Date: Thu, 8 Mar 2018 10:43:37 +0100

        Subject: bmw eml light

2. Body: Contiene la información primaria del mensaje, para el protocolo SMTP se permite únicamente texto, pero posteriormente con las extensiones que se crearon, ahora se puede también transmitir otro tipo de datos diferentes de texto, lo que ahora se envía por medio de *attachments* o archivos adjuntos.

Al crear una conexión con otro servidor SMTP, esta es unidireccional, por lo que, el receptor debe esperar a que se termine de enviar el correo para poder establecer otra conexión y emitir otro correo. El protocolo utiliza comandos de texto enviados al servidor para comunicarse con el cliente. Durante la comunicación, el cliente envía una serie de comandos y el servidor le responde. Al abrir sesión con el protocolo SMTP, el primer comando que se envía es el HELO. A continuación se muestra un ejemplo de una comunicación entre el servidor de correo y el cliente para que este pueda leer el contenido del mensaje.

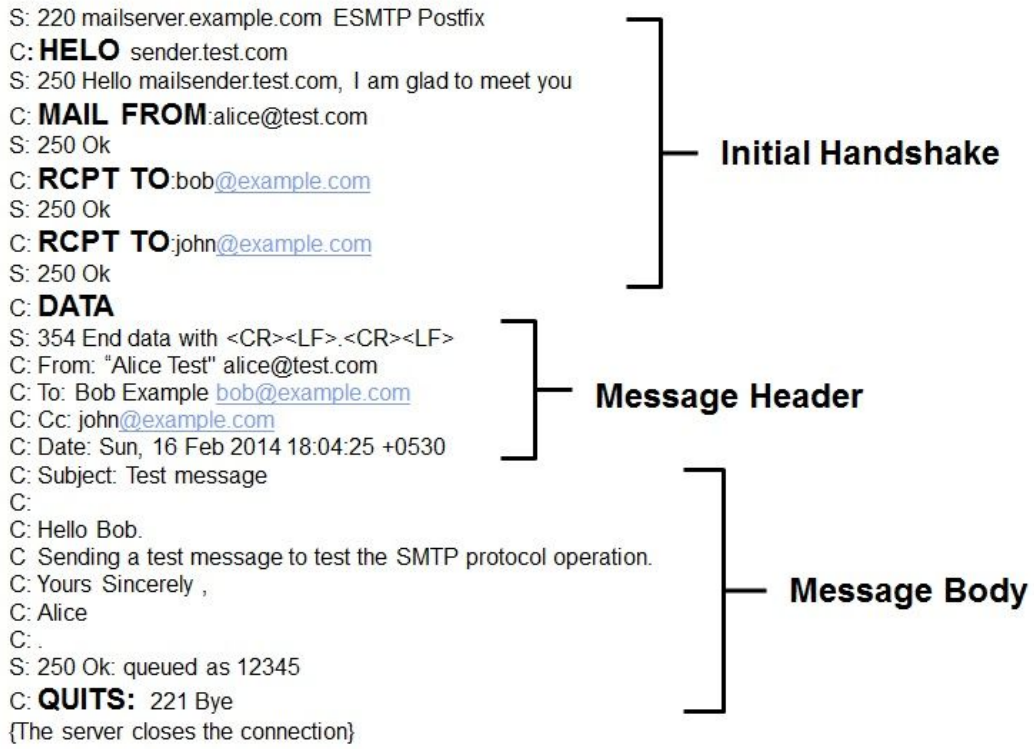

Figura 4. Ejemplo de una sesión SMTP.

En la anterior figura se pueden notar los siguientes códigos de respuesta por parte del servidor de correo S y el cliente C:

- 220: El servidor está listo. Es sólo un mensaje de saludo.
- 250 OK: Indica que el servidor logró transmitir el mensaje exitosamente.
- 354: Indica que el servidor ya recibió el “From” y el “To” y se encuentra a la espera del *Body.*
- 221: Indica que todo el mensaje ha sido transmitido y cierra el canal de transmisión.

Seguridad en el protocolo SMTP

Por su naturaleza, el protocolo SMTP es inseguro, ya que cuando se creó no se tomó en cuenta la seguridad y ahora existe la posibilidad de comunicarse directamente con los servidores que transmiten y reciben los mensajes, creando mensajes falsos que se hagan pasar por otro mensaje, a este ataque se le llama Man-in-the-middle.

En el medio de comunicación de los mensajes entre los clientes y servidores SMTP, no es posible tener certeza de que estos sean auténticos. Por lo que su seguridad se basa en firmas digitales contenidas en los cuerpos de los mensajes. Un ejemplo de estas firmas digitales es el S/MIME.

Anteriormente, en la sección del protocolo SMTP, se mencionó lo que es un MIME (Multipurpose Internet Mail Extensions), por lo que se va a definir lo que es un S/MIME (Secure Multipurpose Internet Mail Extensions).

El S/MIME es un estándar de criptografía que provee los siguientes servicios de seguridad para la mensajería electrónica: confidencialidad de los datos, autenticación, integridad del mensaje y no-repudio del origen. Los mensajes S/MIME se encuentran encapsulados por un cuerpo con datos MIME y el cifrado de datos.

El cifrado de los mensajes de mensajería electrónica mantiene la privacidad del mensaje, tanto como de su integridad. Por lo que solo el usuario al que se le envía el mensaje, puede leer el mensaje, además de que como dicho mensaje es encriptado, impide que se pueda descifrar por medio de algún ataque que pueda ocurrir durante el transporte.

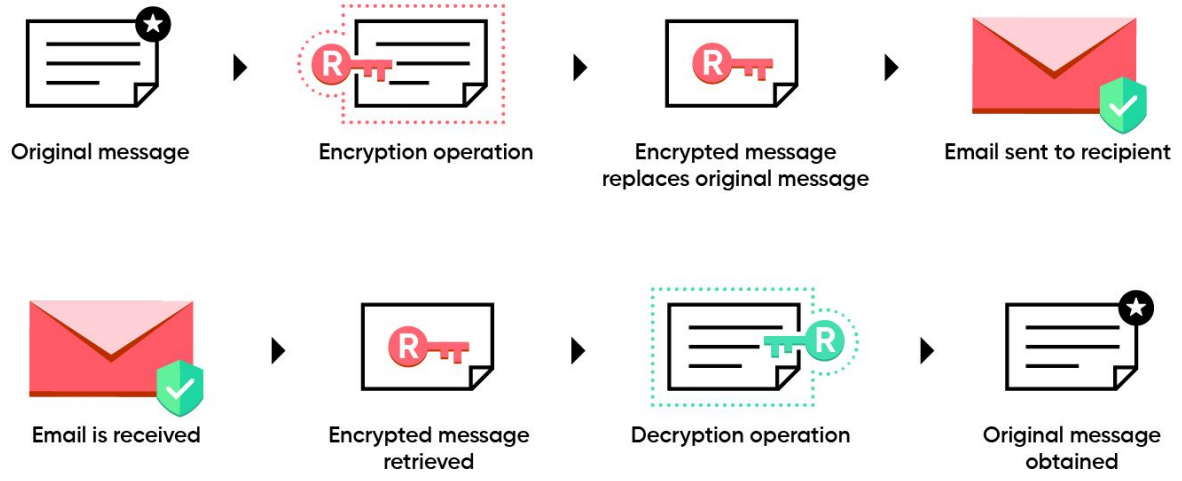

Figura 5 y 6. Proceso de encriptado y descifrado.
Fuente: www.zoho.com/es-xl/mail/help/s-mime.html

Dado que el protocolo SMTP posee ciertas vulnerabilidades, se han implementado a lo largo del tiempo ciertos métodos para minimizar los riesgos para dicho protocolo, se mencionan a continuación algunos de los métodos de seguridad que se agregan a SMTP y posteriormente un grupo de recomendaciones para implementar este protocolo de forma segura, ya sea a nivel de una corporación o bien para uso personal.

En primer lugar tenemos los sistemas más básicos de seguridad que se pueden implementar, serían el SSL - Secure Socket Layer por sus siglas en inglés - y el TLS - Transport Layer Security por sus siglas en inglés - estos son métodos de encapsulamiento o aislamiento del medio por medio de certificados, estos contienen un thumbprint on una especie de huella única con la que se puede verificar que el receptor y el agente de transferencia de correo (MTA) se conocen y que es seguro el vínculo que se hizo entre ellos dos.

Originalmente el puerto 25 no soportaba SSL ni TLS, por lo que por un tiempo se utilizó el puerto 465 para conexiones seguras por medio de SSL. Eventualmente, para SMTP se desarrolló el comando 'STARTTLS' que permite el uso de SSL y TLS en los puertos donde solo se aceptaban conexiones inseguras, haciendo los puertos 25 y 587 compatibles con conexiones SSL y TLS. Actualmente el puerto 465 es obsoleto, pero aún se mantiene para garantizar compatibilidad con programas viejos que no soportan 'STARTTLS'.

Por otro lado se encuentran los métodos de que permiten la encriptación de la información, tenemos el PEM - Privacy-Enhanced Mail por sus siglas en inglés - este utiliza un certificado de autorización (CA), luego está PGP - Pretty Good Privacy por sus siglas en inglés - y GPG - GNU Privacy Guard por sus siglas en inglés - estos protocolos trabajan mediante el par de llaves, una privada y la otra pública, junto con el certificado de autorización CA y la autorización de validación. Por último se encuentra el MIME y S/MIME que se mencionó anteriormente.

Dado que existen diferentes opciones para implementar la seguridad a nivel de protocolo de envío de correos, acá se proporciona una lista con algunas de las recomendaciones a tomar en cuenta a la hora de implementar este servicio:

- Implementar el protocolo en el puerto seguro, para POP3 sería el puerto 995, para el IMAP seguro está el puerto 993 y para SMTP seguro está el puerto 587, estos puertos cuentan con un sistema de encriptación que permitirá un nivel avanzado de seguridad respecto a los puertos convencionales que no lo poseen del todo.
- Se recomienda también implementar el servicio de Reverse DNS Lookup o Búsqueda Inversa de DNS, este servicio tiene como tarea

principal revisar si el DNS que se está recibiendo está asociado a una dirección IP específica, de esta forma se pueden evitar ataques de spam que vayan a ocasionar una denegación de servicio o DoS a nivel del servidor.

- Con el sistema de lista de bloqueo en tiempo real de spam - SURBL por sus siglas en inglés - se pueden evitar ataques suplantación de identidad junto con correos que tengan virus o archivos que pueden afectar el sistema.

IMAP

El Protocolo de Acceso a Mensajes en Internet o IMAP por sus siglas en inglés (Internet Message Access Protocol), permite a un cliente acceder y manipular mensajes de correo electrónico alojados en un servidor.

La conexión consiste básicamente en establecer interacciones iniciales entre cliente - servidor. Dichas interacciones iniciales consisten en comandos del cliente para extraer datos del servidor en su respuesta a los comandos.

Permite la manipulación de buzones de correo o "***mailboxes*"** que son folders remotos de una manera que parezca local. Además, permite a clientes re-sincronizar con el servidor aún cuando se encuentran fuera de línea.

Algunas de las operaciones que permite el protocolo:

- Creación, borrado y renombrado de los buzones de correo.
- Revisión por nuevos mensajes.
- Eliminación de mensajes.

Este protocolo no hace referencia al posteo de mensajes en lo absoluto, esta función es realizada por un protocolo de transferencia de mensajes como SMTP (Simple Message Transfer Protocol).

El protocolo IMAP tiene su definición en el RFC 1730 y su última versión de IMAP es la cuarta (IMAP4), tanto IMAP como POP3 interactúan en la descarga u obteniendo correos electrónicos.

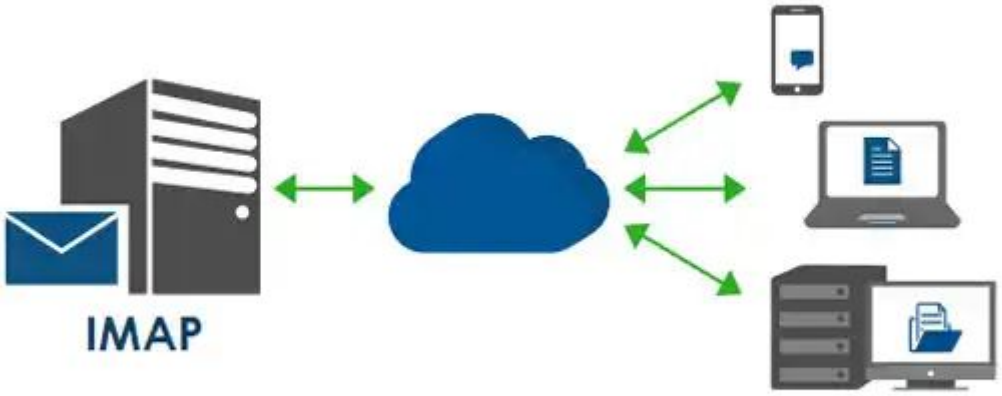

Figura 7. Ejemplo del protocolo IMAP

Fuente: https://www.tecnologia-informatica.com/protocolos-pop-smtp-imap/

Seguridad en el protocolo IMAP

Uno de los problemas más grandes que tiene el protocolo de IMAP es que transmite información totalmente confidencial, y por ende crítica, en texto plano, nos referimos a credenciales. Y al igual que SMTP, cuando estos protocolos se crearon, lastimosamente no se pensó en el componente de seguridad del protocolo, por ende el protocolo en sí carece de seguridad y para que este lo tenga se debe de implementar mediante especies de parches que disminuyan esta condición.

Actualmente la última versión de IMAP hasta el momento, IMAP4 cuenta con un sistema llamado CRAM - Challenge-Response Authentication Mechanism, que implementa un poco de seguridad a nivel de protocolo, ya que se asegura que el cliente note una especie de prueba que recibe y este debe de responder esta prueba al retornar la información, totalmente encriptada, que se le solicite en esa prueba mediante un algoritmo hash.

El problema que actualmente tiene IMAP4 con CRAM es que utiliza el método de encriptación MD5 y este no es un método recomendado para encriptar información y mucho menos transferir esta información con dicho sistema. Se ha comprobado que es un sistema sumamente débil y que en la actualidad es relativamente sencillo obtener la información transferida aún cuando está encriptada con MD5, incluso por eso es que se utiliza en diferentes escenarios medios de encriptación como SHA1 ó SHA256 en vez de MD5.

Webmail

Webmail es una manera de acceder a un cliente web desde el browser y tener la capacidad de consultar y manejar los mensajes de correo electrónico desde ahí. Actualmente es de los más usados por los usuarios en un mundo donde se cambia o se conecta desde múltiples dispositivos. El webmail utiliza el protocolo IMAP que permite almacenar los mensajes en el servidor para que justamente pueda ser accesado desde otros dispositivos remotos.

Ejemplos muy famosos, como Gmail, Outlook, Yahoo, ofrecen este tipo de servicios, donde los usuarios pueden crear cuentas online y administrarlas desde una interfaz web.

POP3

El Protocolo de Oficina de Correo versión 3 (Post Office Protocol 3 en inglés) define un conjunto de reglas de cómo un cliente puede recibir correos electrónicos de un servidor, siendo su misión la entrega final del correo al destinatario. Este protocolo es la última versión del protocolo POP, el cual comenzó a funcionar en 1980; las primeras dos versiones (POP1 y POP2) ya se encuentran obsoletas.

Este protocolo es uno de los más utilizados en los servidores de correo electrónico, siendo utilizado por Windows Mail, Gmail, Thunderbird y Outlook, así como por aplicaciones y servicios que se encargan de recoger los mensajes en el servidor email, funcionando de forma simultánea con SMTP.

A continuación, se mencionan algunas de sus características:

- Brinda posibilidad al usuario de descargar los correos electrónicos a sus ordenadores para leerlos sin tener una conexión a Internet o cuando la conexión es muy lenta.
- Cada vez que el usuario se conecta al servidor, los mensajes del correo electrónico son enviados desde el servidor hasta la computadora local.
- Una vez los mensajes han sido recibidos, la conexión con el servidor puede
- interrumpirse o cerrarse lo cual no afectará a la lectura de los mensajes.
- Brinda la posibilidad de mantener los correos en el servidor.

El cliente se comunica con el servidor, utilizando el protocolo TCP, en el puerto 110 (transporte inseguro con función SSL no habilitada) o 995 (transporte seguro con función SSL habilitada). Todos los mensajes transmitidos durante una sesión POP3 cumplen al estándar para el formato de Mensajes de Texto de Internet [RFC822].
Por otro lado, este protocolo tiene 3 fases de funcionamiento:

1. Autenticación: el cliente envía los comandos USER y PASS uno a continuación del otro, y se identifica como usuario autorizado; aquí es donde el cliente tiene que enviar los mensajes correspondientes de usuario y contraseña para identificarse.
2. Transacción: el cliente puede solicitar una lista de los correos electrónicos que estén almacenados en el servidor en la dirección asociada. Si el cliente decide retirar los correos, estos se descargan y automáticamente marca los mensajes para ser borrados en el servidor.
3. Actualización: tiene lugar cuando el cliente ha terminado la sesión y en ella se borran los mensajes marcados en la fase de transacción.

Los comandos en POP3 consisten en una palabra clave que no distingue entre mayúsculas y minúsculas, seguido de uno o más argumentos. Las palabras clave tienen tres o cuatro caracteres y cada argumento puede tener hasta 40, asimismo se usa el carácter del espacio para separarlos. A continuación se presentan los principales comandos usados por este protocolo:

Comando	**Descripción**
USER <usario>	Nombre de usuario
PASS <contraseña>	Contraseña
QUIT	Finalizar sesión
STAT	Número de mensajes y tamaño total.
LIST <n^{Q} de mensaje>	Número del mensaje y su tamaño. Si no se proporciona número de mensaje, lista todos.
RETR n^{Q} de mensaje	Descargar mensaje
DELE n^{Q} de mensaje	Borrar mensaje
TOP mensaje líneas	Muestra las primeras "líneas" líneas del mensaje número "mensaje". Incluye la cabecera.
NOOP	No-operación
RSET	Deshace los cambios hechos en la sección, incluido el borrado de mensajes.

Figura 8. Comandos para comunicaciones POP3.
Fuente: Universidad de Alcalá (2020)

A continuación, se presenta un ejemplo de una sesión de POP3:

```
S: <wait for connection on TCP port 110>
C: <open connection>
S:    +OK POP3 server ready <1896.697170952@dbc.mtview.ca.us>
C:    APOP mrose c4c9334bac560ecc979e58001b3e22fb
S:    +OK mrose's maildrop has 2 messages (320 octets)
C:    STAT
S:    +OK 2 320
C:    LIST
S:    +OK 2 messages (320 octets)
S:    1 120
S:    2 200
S:    .
C:    RETR 1
S:    +OK 120 octets
S:    <the POP3 server sends message 1>
S:    .
C:    DELE 1
S:    +OK message 1 deleted
C:    RETR 2
S:    +OK 200 octets
S:    <the POP3 server sends message 2>
S:    .
C:    DELE 2
S:    +OK message 2 deleted
C:    QUIT
S:    +OK dewey POP3 server signing off (maildrop empty)
C:  <close connection>
S:  <wait for next connection>
```

Fuente: RFC 1939

Para poder utilizar múltiples clientes POP3 para una misma cuenta de correo electrónico, existe la opción de generar y guardar una copia en el servidor de los correos que son descargados por un cliente, así permitiéndole a otro cliente descargar los mismos correos.

Seguridad en el protocolo POP3

A pesar de que el protocolo POP se encuentre en su más reciente versión, sigue sin tener un sistema de seguridad obligatorio que lo haga más seguro de utilizar. Similar a los protocolos anteriores, SMTP e IMAP, para el POP no se implementó una medida de seguridad que fuera requerida durante su proceso de poder obtener el tráfico de red.

Su integridad por la seguridad, está basada en el comando *opcional* APOP. Este comando maneja un identificador del correo electrónico y un resumen del mensaje (128 bits generados por el algoritmo MD5). Se dice que es opcional porque no forma parte del formato estándar RFC822.

El algoritmo MD5 realiza un proceso para encriptar datos recibidos y que esta sea la llave privada para poder autenticarse. Fue diseñado para aplicaciones de firma digital. Además, es la extensión del algoritmo MD4, el cual era más rápido, pero la parte de seguridad estaba en el límite, tanto que preferían que fuera más rápido y menos conservador. Por lo tanto, se diseñó el MD5 para aumentar la capacidad de seguridad, a pesar de que se disminuyera la velocidad del algoritmo.

Durante el proceso para la autenticación del protocolo POP3, comienza con un intercambio de usuario y la contraseña. El problema que tiene esta autenticación, es que, a pesar de ya tener seguridad de que lleva una contraseña, se realiza este proceso cada poco tiempo, para verificar si tiene algún mensaje nuevo. Por lo que el usuario y contraseña quedan expuestos en la red por más tiempo.

Con el comando APOP, se modifica el proceso de autenticación, por lo que ahora este lleva una marca de tiempo que debe ser distinta cada vez que se realiza una conexión con el servidor POP3. El cliente es el que produce la marca de tiempo, además de realizar el proceso del algoritmo MD5.

Relación con otros servicios de red

Servicio de DNS

En algunos casos cuando se quiere enviar un correo electrónico desde un dominio a otro distinto, el MTA o el servidor de correo debe primero hacer una consulta a su servidor DNS utilizando el protocolo DNS para poder resolver el dominio del destinatario, que generalmente representa un servidor de correo otorgado por el proveedor de internet, como se menciona anteriormente. Una vez que el servidor logra identificar por medio de DNS cual es la dirección a la que debe entregar los mensajes, hace conexión con dicho servidor para poder transferir el mensaje por medio de SMTP y posterior a eso ser consultado por el cliente por medio de alguno de los protocolos para correo electrónico previamente mencionados (POP e IMAP).

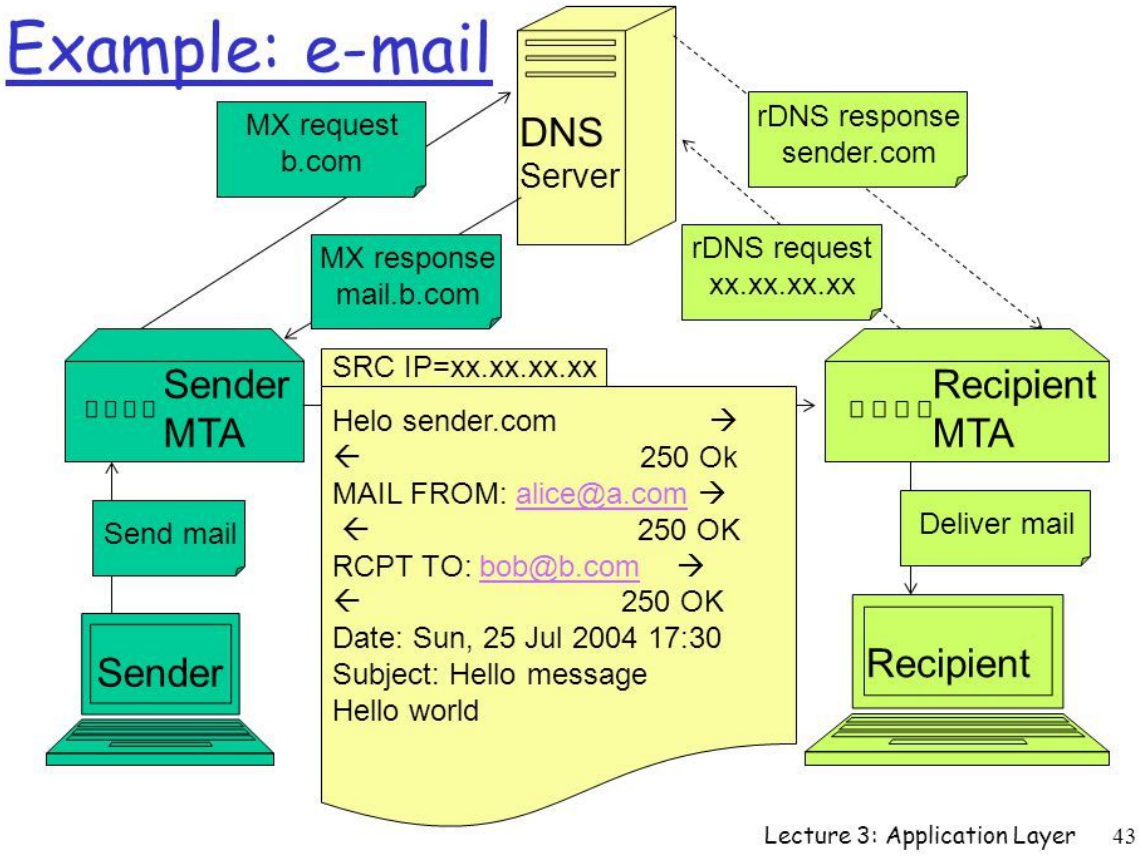

Figura 9. Ejemplo de consulta a servidor DNS desde MTA.

Servicio LDAP

Los servidores LDAP pueden almacenar información relacionada a las cuentas de usuario y los alias de correo electrónico. Los MTA y los Message Delivery Agents (MDA) pueden hacer consultas a ese servidor LDAP sobre información de las cuentas involucradas en un intercambio de mensajes de correo electrónico. Lo anterior trae una serie de ventajas principalmente dentro de la comunicación organizacional que es donde se utilizan este tipo de servidores LDAP.

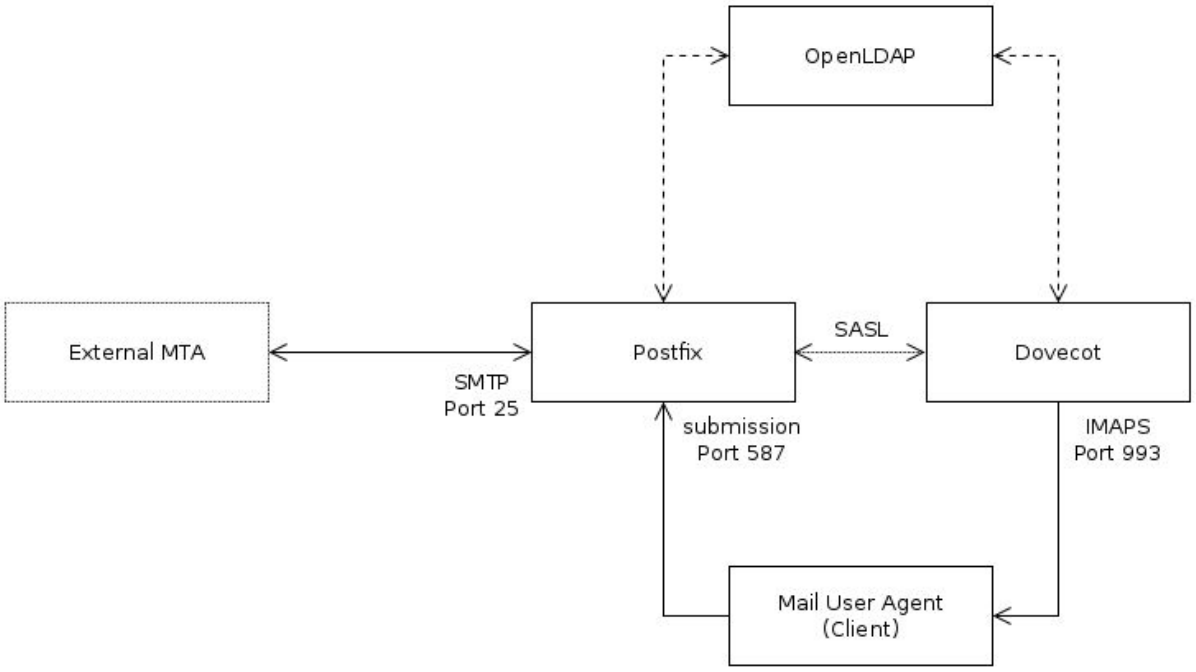

Figura 10. Interacción de MTA y MDA con LDAP.

Postfix es un MTA bastante popular de software libre, al igual que Dovecot, con la diferencia que Dovecot actúa como MDA para entregar los mensajes al cliente.

Referencias

1. Ahmet Efe, Gizem Kalkanci, Mehmet Donk, & Ziya Uysal. (2019, December). *A Hidden Hazard: Man-in-The-Middle Attack in Networks*. ResearchGate; unknown. https://www.researchgate.net/publication/336669198_A_Hidden_Hazard_Man-in-The-Middle_Attack_in_Networks
2. Al-Janabi, Sufyan & Ibrahim, Mohammed. (2006). *Secure E-Mail System Using S/MIME and IB-PKC*.
3. Archiveddocs. (2013, October 21). SMTP. Retrieved September 22, 2020, from Microsoft.com website: https://docs.microsoft.com/en-us/previous-versions/office/developer/exchange-server-2010/aa494182(v%3Dexchg.140)
4. *EL SISTEMA DE CORREO ELECTRÓNICO (SMTP Y POP3)*. (n.d.). Retrieved from http://www.falconmarbella.com/esigranada/dmdocuments/Punto_235_Correo_electronico.pdf
5. *Email Server Security Best Practices to Look Out For*. (2020, April 23). Att.Com. https://cybersecurity.att.com/blogs/security-essentials/basic-best-practices-for-configuring-email-servers
6. Falco Nordmann. (2020). *LDAP managed mail server with Postfix and Dovecot for multiple domains* | Vennedey.net. Retrieved September 22, 2020, from Vennedey.net website: https://www.vennedey.net/resources/2-LDAP-managed-mail-server-with-Postfix-and-Dovecot-for-multiple-domains
7. Jeroen Scheerder, & C. P. J. Koymans. (2007, January 27). Email. ResearchGate; unknown. https://www.researchgate.net/publication/281405832_Email
8. Kashif Iqbal. (2019, October 11). EML - EMail Message. Retrieved September 22, 2020, from Fileformat.com website: https://docs.fileformat.com/email/eml/
9. M. Tariq Banday. (2011, May 31). *Effectiveness and Limitations of E-Mail Security Protocols. ResearchGate; Academy and Industry Research Collaboration Center.* https://www.researchgate.net/publication/227859119_Effectiveness_and_Limitations_of_E-Mail_Security_Protocols

10. Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies. (2020). Retrieved September 23, 2020, from Ietf.org website: https://tools.ietf.org/html/rfc2045
11. Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types. (2020). Retrieved September 24, 2020, from Ietf.org website: https://tools.ietf.org/html/rfc2046
12. MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text. (2020). Retrieved September 24, 2020, from Ietf.org website: https://tools.ietf.org/html/rfc2047
13. *Network Working Group.* (n.d.). Retrieved September 24, 2020, from https://tools.ietf.org/pdf/rfc5321.pdf
14. *OSI Model and Network Protocols Objectives*. (n.d.). Retrieved from https://access.itxlearning.com/data/cmdata/NETPLUSN10004/Books/ec2_netplus004c04.pdf
15. Post Office Protocol - Version 3. (2020). Retrieved September 24, 2020, from Ietf.org website: https://tools.ietf.org/html/rfc1939
16. Read Gmail messages on other email clients using POP - Gmail Help. (2018). Retrieved September 24, 2020, from Google.com website: https://support.google.com/mail/answer/7104828
17. *S/MIME*. (2020). Retrieved from https://www.zoho.com/es-xl/mail/help/s-mime.html
18. *SMTP errors and reply codes - smtp mail server - professional SMTP service provider*. (2018, March 18). Retrieved September 24, 2020, from smtp mail server - professional SMTP service provider website: https://www.serversmtp.com/smtp-error/
19. Simple Mail Transfer Protocol. (2020). Retrieved September 22, 2020, from Ietf.org website: https://tools.ietf.org/html/rfc5321
20. Tracy, M., Jansen, W., Scarfone, K., & Butterfield, J. (n.d.). *Special Publication 800-45 Version 2 Guidelines on Electronic Mail Security Recommendations of the National Institute of Standards and Technology*. Retrieved September 24, 2020, from https://www.govinfo.gov/content/pkg/GOVPUB-C13-940e61a7e985d7e193fe34922ddfea33/pdf/GOVPUB-C13-940e61a7e985d7e193fe34922ddfea33.pdf