**Capa de Aplicación - Correo electrónico Redes y comunicaciones - 2022**

**Práctica 4**

**Capa de Aplicación - Correo electrónico**

**Correo electrónico**

**3 4 5 6 7 8 9 10 11 12**

**1. ¿Qué protocolos se utilizan para el envío de mails entre el cliente y su servidor de correo? ¿Y entre**

**servidores de correo?**

Con el fin de enviar un correo a un destinatario, un usuario debe hacer uso de un agente de usuario para correo electrónico, que le permita enviar su correo hacia su servidor de correo. Esta transferencia de información se puede lograr haciendo uso de SMTP.

● SMTP: Es un protocolo de comunicaciones basado en texto. Opera en los servicios de correo electrónico. Limitaciones en cuanto a la recepción de mensajes en el servidor de destino (cola de mensajes recibidos), por las que se asocia con otros protocolos, como el POP o IMAP, otorgando a **SMTP** la tarea específica de **enviar correo**, y recibirlos empleando los otros protocolos antes mencionados (POP O IMAP).

● HTTP: Cuando el usuario utiliza un navegador web para el envío de correos, el protocolo que se utiliza para la comunicación es HTTP. Sin embargo, no debe considerárselo como protocolo para correo electrónico, ya que solo es el protocolo usado para llegar hasta el servidor de correo. Luego, la aplicación a la cual nos conectamos va a utilizar protocolos SMTP para enviar mails, y POP3 o IMAP para recibir mails.

Podemos afirmar que si usamos un cliente de correo, no se va a utilizar HTTP.

● ESMTP: la versión segura de SMTP.

El protocolo que siempre se utiliza para la comunicación entre los servidores de correo es SMTP o ESMTP.

**2. ¿Qué protocolos se utilizan para la recepción de mails? Enumere y explique características y diferencias entre las alternativas posibles.**

Para leer los correos se debe utilizar un agente de usuario el cual se comunicará con el servidor de correo a través de algunos de los siguientes protocolos:

● POP3: (Post Office Protocol -- Version 3) es un protocolo de acceso de correo simple. Su funcionalidad es bastante limitada. Comienza cuando el agente de usuario abre una conexión TCP hacia el servidor de correo en el puerto 110. Con la conexión TCP establecida, POP3 avanza a lo largo de 3 fases: autorización, transacción y actualización:

Autorización: El agente de usuario envía un username y una contraseña para autenticar al usuario.

Transacción: El agente de usuario recibe mensajes y el usuario puede marcar correos para borrado.

Actualización: Luego de que el usuario utiliza el comando quit, el cual finaliza la sesión POP3; en este momento el servidor de mail elimina los correos marcados.

Este protocolo descarga los mails en la PC, donde quedan almacenados. Una vez hecho esto, los correos sólo serán accesibles desde la PC donde se bajaron, ya que al bajarse se eliminan del servidor. (configuración descarga-borrado. También existe la configuración descarga-almacenamiento, la cual deja los mails en el servidor.)

Útil si se usa siempre la misma PC. Se puede acceder a los correos ya descargados si no hay internet.

● IMAP: Protocolo de acceso de correo. Mas características y complejidad que POP3. Asocia cada mensaje con una carpeta; cuando un mensaje arriba al servidor es asociado con la carpeta INBOX del receptor, quien puede mover, leer o eliminar el mensaje.

Tiene comandos que le permiten al usuario obtener solamente obtener el header del mensaje o una parte de un mensaje MIME. Esto es útil cuando la conexión tiene poco ancho de banda. IMAP no descarga los mensajes a tu ordenador: tanto los mensajes como las carpetas se mantienen en el servidor, lo que es ventajoso si se usan diferentes dispositivos. Por esto, hay que tener en cuenta que eventualmente podría llenarse el espacio límite concedido.

También brinda más seguridad si se usa una PC compartida, ya que no almacena información en la máquina local.

El inconveniente de este protocolo es que siempre hemos de disponer de conexión a internet.

● HTTP: Cuando el usuario utiliza su navegador web como agente de usuario para la recepción de correos, éste utilizará el protocolo HTTP para comunicarse con su servidor de correo. Sin embargo, el servidor de correo debe usar los protocolos antes mencionados.

|  |  |  |
| --- | --- | --- |
|  | **POP** | **IMAP** |
| **Almacenamiento de correos** | Temporal en un servidor (por default), permanente en los clientes | Servidor externo principalmente |
| **Mantenimiento de sincronía entre clientes** | Difícil | Fácil |
| **Estabilidad** | Baja | Alta |
| **Organización, en el servidor** | Único buzón de entrada para todos los correos | Se pueden crear subcarpetas |
| **Organización, en los clientes** | Se pueden crear subcarpetas | Se pueden crear subcarpetas |

**3. Utilizando la VM y teniendo en cuenta los siguientes datos, abra el cliente de correo (thunderbird) y**

**configure dos cuentas de correo. Una de las cuentas utilizará POP para solicitar al servidor los mails**

**recibidos para la misma mientras que la otra utilizará IMAP.**

**Al crear cada una de las cuentas, seleccionar Manual config y luego de configurar las mismas según lo**

**indicado, ignorar advertencias por uso de conexión sin cifrado.**

**Datos para POP**

**Cuenta de correo: alumnopop@redes.unlp.edu.ar**

**Nombre de usuario: alumnopop**

**Contraseña: alumnopoppass**

**Puerto: 110**

**Datos para IMAP**

**Cuenta de correo: alumnoimap@redes.unlp.edu.ar**

**Nombre de usuario: alumnoimap**

**Contraseña: alumnoimappass**

**Puerto: 143**

**Datos comunes para ambas cuentas**

**Servidor de correo entrante (POP/IMAP):**

**• Nombre: mail.redes.unlp.edu.ar**

**• SSL: None**

**• Autenticación: Normal password**

**Servidor de correo saliente (SMTP):**

**• Nombre: mail.redes.unlp.edu.ar**

**Página 1 de 7Capa de Aplicación - Correo electrónico Redes y comunicaciones - 2022**

**• Puerto: 25**

**• SSL: None**

**• Autenticación: Normal password**

**a. Verificar el correcto funcionamiento enviando un email desde el cliente de una cuenta a la otra y**

**luego desde la otra responder el mail hacia la primera.**

**b. Análisis del protocolo SMTP**

**i. Utilizando Wireshark, capture el tráfico de red contra el servidor de correo mientras desde la**

**cuenta alumnopop@redes.unlp.edu.ar envía un correo a alumnoimap@redes.unlp.edu.ar**

**ii. Utilice el filtro SMTP para observar los paquetes del protocolo SMTP en la captura generada y**

**analice el intercambio de dicho protocolo entre el cliente y el servidor para observar los distintos**

**comandos utilizados y su correspondiente respuesta. Ayuda: filtre por protocolo SMTP y sobre**

**alguna de las líneas del intercambio haga click derecho y seleccione Follow TCP Stream. . .**

**c. Usando el cliente de correo, thunderbird del usuario alumnopop@redes.unlp.edu.ar envíe un correo**

**electrónico alumnoimap@redes.unlp.edu.ar el cual debe tener: un asunto, datos en el body y una**

**imagen adjunta.**

**i. Verifique los fuentes del correo recibido para entender como se utiliza el header “Content-Type:**

**multipart/mixed“ para poder realizar el envío de distintos archivos adjuntos.**

**ii. Extraiga la imagen adjunta del mismo modo que lo hace el cliente de correo a partir de los**

**fuentes del mensaje.**

**4. Análisis del protocolo POP**

**a. Utilizando Wireshark, capture el tráfico de red contra el servidor de correo mientras desde la cuenta**

**alumnoimap@redes.unlp.edu.ar le envía una correo a alumnopop@redes.unlp.edu.ar y mientras**

**alumnopop@redes.unlp.edu.ar recepciona dicho correo.**

**b. Utilice el filtro POP para observar los paquetes del protocolo POP en la captura generada y analice**

**el intercambio de dicho protocolo entre el cliente y el servidor para observar los distintos comandos**

**utilizados y su correspondiente respuesta.**

**5. Análisis del protocolo IMAP**

**a. Utilizando Wireshark, capture el tráfico de red contra el servidor de correo mientras desde la cuenta**

**alumnopop@redes.unlp.edu.ar le envía una correo a alumnoimap@redes.unlp.edu.ar y mientras**

**alumnoimap@redes.unlp.edu.ar recepciona dicho correo.**

**b. Utilice el filtro IMAP para observar los paquetes del protocolo IMAP en la captura generada y analice**

**el intercambio de dicho protocolo entre el cliente y el servidor para observar los distintos comandos**

**utilizados y su correspondiente respuesta.**

**Página 2 de 7Capa de Aplicación - Correo electrónico Redes y comunicaciones - 2022**

**6. IMAP vs POP**

**a. Marque como leídos todos los correos que tenga en el buzón de entrada de alumnopop y de alumnoimap. Luego, cree una carpeta llamada POP en la cuenta de alumnopop y una llamada IMAP en**

**la cuenta de alumnoimap.**

**Asegurese que tiene mails en el inbox y en la carpeta recientemente creada en cada una de las**

**cuentas.**

**b. Cierre la sesión iniciada e ingrese nuevamente identificandose como usuario root y password packer,**

**ejecute el cliente de correos.**

**De esta forma, iniciará el cliente de correo con el perfil del superusuario (diferente del usuario con**

**el que ya configuró las cuentas antes mencionadas).**

**Luego configure las cuentas POP e IMAP de los usuarios alumnopop y alumnoimap como se describió anteriormente pero desde el cliente de correos ejecutado con el usuario root.**

**Luego responda:**

**i. ¿Qué correos ve en el buzón de entrada de ambas cuentas? ¿Están marcados como leídos o**

**como no leídos? ¿Por qué?**

**ii. ¿Qué pasó con las carpetas POP e IMAP que creó en el paso anterior?**

**c. En base a lo observado. ¿Qué protocolo le parece mejor? ¿POP o IMAP? ¿Por qué? ¿Qué protocolo**

**considera que utiliza más recursos del servidor? ¿Por qué?**

**7. ¿En algún caso es posible enviar más de un correo durante una misma conexión tcp?**

**Considere:**

**Destinatarios múltiples del mismo dominio entre MUA-MSA y entre MTA-MTA**

**Destinatarios múltiples de diferentes dominios entre MUA-MSA y entre MTA-MTA**

**8. Indique sí es posible que el MSA escuche en un puerto TCP diferente a los convencionales y qué**

**implicancias tendría.**

**9. Indique sí es posible que el MTA escuche en un puerto TCP diferente a los convencionales y qué implicancias tendría.**

**10. Ejercicio integrador HTTP, DNS y MAIL**

**Suponga que registró bajo su propiedad el dominio redes2022.com.ar y dispone de 4 servidores:**

* **Un servidor DNS instalado configurado como primario de la zona redes2022.com.ar. (hostname: ns1 / ip: 203.0.113.65).**
* **Un servidor DNS instalado configurado como secundario de la zona redes2022.com.ar. (hostname: ns2 / ip: 203.0.113.66).**
* **Un servidor de correo electrónico (hostname: mail / ip: 203.0.113.111). Permitirá a los usuarios enviar y recibir correos a cualquier dominio de Internet.**
* **Un servidor WEB para el acceso a un webmail (hostname: correo / ip: 203.0.113.8). Permitirá a los usuarios gestionar vía web sus correos electrónicos a través de la URL https://webmail.redes2022.com.ar**

**a. ¿Qué información debería informar al momento del registro para hacer visible a Internet el dominio**

**registrado?**

Necesita informar, al servidor con autoridad sobre com.ar.:

i)Que ns1.redes2022.com.ar y ns2.redes2022.com.ar son servidores DNS para el dominio redes2022.com.ar (registros NS)

ii)Que ns1.redes2022.com.ar es el servidor primario para el dominio redes2022.com.ar (registro SOA)

iii)Que las IPv4 de ns1.redes2022.com.ar y ns2.redes2022.com.ar son 203.0.113.65 y 203.0.113.66 respectivamente (registros A)

**b. ¿Qué registros sería necesario configurar en el servidor de nombres? Indique toda la información**

**necesaria del archivo de zona. Puede utilizar la siguiente tabla de referencia (evalúe la necesidad de**

**usar cada caso los siguientes campos): Nombre del registro, Tipo de registro, Prioridad, TTL, Valor**

**del registro.**

redes2022.com.ar. 86400 IN SOA ns1.redes2022.com.ar. email\.admin.redes2022.com.ar. 2022091700 604800 86400 2419200 86400

redes2022.com.ar. 86400 IN NS ns1.redes2022.com.ar.

redes2022.com.ar. 86400 IN NS ns2.redes2022.com.ar.

redes.unlp.edu.ar. 86400 IN MX 5 mail.redes2022.com.ar.

mail.redes2022.com.ar. 86400 IN A 203.0.113.111

webmail.redes2022.com.ar. 604800 IN A 203.0.113.8

ns1.redes2022.com.ar. 604800 IN A 203.0.113.65

ns2.redes2022.com.ar. 604800 IN A 203.0.113.66

redes2022.com.ar. 86400 IN SOA ns1.redes2022.com.ar. email\.admin.redes2022.com.ar. 2022091700 604800 86400 2419200 86400

**c. ¿Es necesario que el servidor de DNS acepte consultas recursivas? Justifique.**

No, porque al ser el que tiene autoridad sobre la zona, es capaz de devolver las IPs de los dominios solicitados. No es su responsabilidad poder resolver otros dominios externos (aunque podés configurarlo para que lo haga)

**d. ¿Qué servicios/protocolos de capa de aplicación configuraría en cada servidor?**

i) ns1: DNS

ii) ns2: DNS

iii) mail: SMTP, POP/IMAP

iv) correo: HTTP(S)

**e. Para cada servidor, ¿qué puertos considera necesarios dejar abiertos a Internet? A modo de referencia, para cada puerto indique: servidor, protocolo de transporte y número de puerto.**

|  |  |  |
| --- | --- | --- |
| **Servidor** | **Protocolo de transporte** | **Número de puerto** |
| ns1 | UDP | 53 |
| ns2 | UDP | 53 |
| mail | TCP | 25 |
| correo | TCP | 80 |

**Ver que al googlear dice que DNS usa udp y tcp**

**f. ¿Cómo cree que se conectaría el webmail del servidor web con el servidor de correo? ¿Qué protocolos usaría y para qué?**

El WebMail recibiría solicitudes HTTP, y para satisfacerlas se comunicaría con el servidor de correo, usando:

i) SMTP: Enviar emails a otros usuarios (Protocolo para transferencia simple de mails)

ii) IMAP: Almacenar y recibir emails, gestionar carpetas, etc

**g. ¿Cómo se podría hacer para que cualquier MTA reconozca como válidos los mails provienentes del**

**dominio redes2022.com.ar solamente a los que llegan de la dirección 203.0.113.111? ¿Afectaría**

**esto a los mails enviados desde el Webmail? Justifique.**

i) SPF, no tanto PTR

ii) No afectaría, porque el Webmail le envía los datos al servidor SMTP, y es éste quien emite realmente los emails (nop?)

**h. ¿Qué característica propia de SMTP, IMAP y POP hace que al adjuntar una imagen o un ejecutable**

**sea necesario aplicar un encoding (ej. base64)?**

La característica es que funcionan sobre ASCII de 7 bits. Como los bytes de los archivos pueden tomar cualquier valor (incluyendo caracteres no válidos), al codificarlos se restringe el conjunto de valores a caracteres ASCII válidos

**i. ¿Se podría enviar un mail a un usuario de modo que el receptor vea que el remitente es un usuario**

**distinto? En caso afirmativo, ¿Cómo? ¿Es una indicación de una estafa? Justifique**

i) Sería posible, modificando el valor del encabezado From:

ii) No necesariamente es una estafa, ya que puede usarse para enviar listas de mails

**j. ¿Se podría enviar un mail a un usuario de modo que el receptor vea que el destinatario es un usuario**

**distinto? En caso afirmativo, ¿Cómo? ¿Por qué no le llegaría al destinatario que el receptor vé? ¿Es**

**esto una indicación de una estafa? Justifique**

i) Sería posible, modificando el valor del encabezado To:

ii) No le llegaría porque una cosa es lo que se le indica al servidor SMTP mediante comandos (a éste le llegará realmente), y otra es lo escrito en los headers del mail

iii) Para mí no sería una estafa, aunque para un usuario sí que sería raro ver algo así. También depende del contenido del mensaje

**k. ¿Qué protocolo usará nuestro MUA para enviar un correo con remitente redes@info.unlp.edu.ar?**

**¿Con quién se conectará? ¿Qué información será necesaria y cómo la obtendría?**

i) Usará SMTP para todo lo relacionado a emails, y DNS para obtener direcciones IP

ii) La secuencia simplificada sería, asumiendo indirecciones:

1. El MUA obtiene del DNS la IP del MSA, y se comunica con éste para enviarle los datos del correo
2. El MSA obtiene del DNS la IP del rMTA fuente, y se comunica con éste para enviarle los datos del correo
3. El rMTA fuente extrae de la dirección de correo destino, el nombre del dominio destino
4. El rMTA fuente obtiene del DNS la IP del rMTA destino, y se comunica con éste para enviarle los datos del correo

**l. Dado que solo disponemos de un servidor de correo, ¿qué sucederá con los mails que intenten**

**ingresar durante un reinicio del servidor?**

l) El reinicio interrumpirá la comunicación SMTP (o no llega a iniciarse). Entonces, el servidor fuente detectará esto y guardará los datos del email en una cola interna, reintentando periódicamente enviar el correo. Si tras un tiempo, aún no pudo enviarlo, se rendirá e informará al usuario que el email no pudo ser entregado

**m. Suponga que contratamos un servidor de correo electrónico en la nube para integrarlo con nuestra**

**arquitectura de servicios.**

**i. ¿Cómo configuraría el DNS para que ambos servidores de correo se comporten de manera de**

**dar un servicio de correo tolerante a fallos?**

m) Habría que agregar, al archivo de zona:

redes.unlp.edu.ar. 86400 IN MX 10 nube.redes2022.com.ar.

nube.redes2022.com.ar. 86400 IN A 145.98.72.234 **🡪Que es esa A?**

**11. Utilizando la herramienta Swaks envíe un correo electrónico con las siguientes características:**

**Dirección destino: Dirección de correo de alumnoimap@redes.unlp.edu.ar**

**Dirección origen: redesycomunicaciones@redes.unlp.edu.ar**

**Asunto: SMTP-Práctica4**

**Archivo adjunto: PDF del enunciado de la práctica**

**Cuerpo del mensaje: Esto es una prueba del protocolo SMTP**

**a. Analice tanto la salida del comando swaks como los fuentes del mensaje recibido para responder**

**las siguientes preguntas:**

**i. ¿A qué corresponde la información enviada por el servidor destino como respuesta al comando**

**EHLO? Elija dos de las opciones del listado e investigue la funcionalidad de la misma.**

**ii. Indicar cuáles cabeceras fueron agregadas por la herramienta swaks.**

**iii. ¿Cuál es el message-id del correo enviado? ¿Quién asigna dicho valor?**

**iv. ¿Cuál es el software utilizado como servidor de correo electrónico?**

**v. Adjunte la salida del comando swaks y los fuentes del correo electrónico.**

**b. Descargue de la plataforma la captura de tráfico smtp.pcang y la salida del comando swaks smtp.swaks**

**para responder y justificar los siguientes ejercicios.**

**i. ¿Por qué el contenido del mail no puede ser leido en la captura de tráfico?**

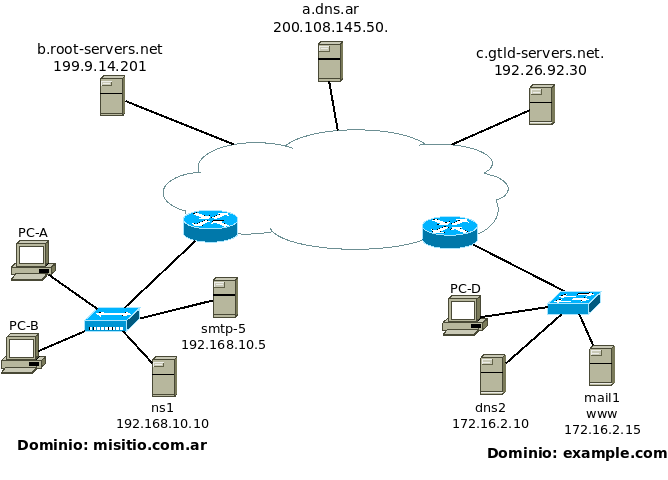
**c. Realice una consulta de DNS por registros TXT al dominio info.unlp.edu.ar y entre dichos registros**

**evalúe la información del registro SPF. ¿Por qué cree que aparecen muchos servidores autorizados?**

**d. Realice una consulta de DNS por registros TXT al dominio outlook.com y analice el registro correspondiente a SPF. ¿Cuáles son los bloques de red autorizados para enviar mails?. Investigue para**

**qué se utiliza la directiva "~all"**

**12. Observar el gráfico a continuación y teniendo en cuenta lo siguiente, responder:**



**El usuario** [**juan@misitio.com.ar**](mailto:juan@misitio.com.ar) **en PC-A desea enviar un mail al usuario** [**alicia@example.com**](mailto:alicia@example.com)**. Cada organización tiene sus propios servidores de DNS y Mail**

**El servidor ns1 de misitio.com.ar no tiene la recursión habilitada**

**a. El servidor de mail, mail1, y de HTTP, www, de example.com tienen la misma IP, ¿es posible esto?**

**Si lo es, ¿cómo lo resolvería?**

Es posible, porque los servicios HTTP y SMTP usan distintos puertos para funcionar, aunque sean hosteados en una misma máquina física

**b. Al enviar el mail, ¿por qué registro de DNS consultará el MUA?**

Consultará por los registros MX del dominio misitio.com.ar., y luego, el registro A de smtp-5.misitio.com.ar. (si en la respuesta al MX no se incluyó su IP como información adicional)

**c. Una vez que el mail fue recibido por el servidor smtp-5, ¿por qué registro de DNS consultará?**

Consultará por los registros MX del dominio example.com., y luego, el registro A de mail1.example.com. (si en la respuesta al MX no se incluyó su IP como información adicional)

**d. Si en el punto anterior smtp-5 recibiese un listado de nombres de servidores de correo, ¿será necesario realizar una consulta de DNS adicional? Si es afirmativo, ¿por qué tipo de registro y de cuál servidor preguntaría?**

Si en la respuesta al MX no se incluyeron las IPs como información adicional, entonces se consultaría por el registro A de cada servidor SMTP en función de su prioridad (orden ascendente). Si el primero falla, se consulta al segundo, y así sucesivamente

**e. Indicar todo el proceso que deberá realizar el servidor ns1 de misitio.com.ar para obtener los servidores de mail de example.com**

**f. Teniendo en cuenta el proceso de encapsulación/desencapsulación y definición de protocolos, responder V o F y justificar:**

**Los datos de la cabecera de SMTP deben ser analizados por el servidor DNS para responder a la consulta de los registros MX**

Falso, porque el servidor SMTP es quien extrae el nombre de dominio a partir de los datos de la cabecera, y luego consulta al servidor DNS por los registros MX

**Al ser recibidos por el servidor smtp-5 los datos agregados por el protocolo SMTP serán analizados por cada una de las capas inferiores**

Falso, porque los datos agregados en la capa de aplicación (SMTP) son recibidos por otra instancia de esa misma capa

**Cada protocolo de la capa de aplicación agregará una cabecera con información propia de ese protocolo**

Verdadero, porque agrega los datos que necesita para poder funcionar

**Como son todos protocolos de la capa de aplicación, las cabeceras agregadas por el protocolo de DNS pueden ser analizadas y comprendidas por el protocolo SMTP o HTTP**

Falso, porque a pesar de pertenecer a la misma capa, se trata de protocolos diferentes entre sí

**Para que los clientes en misitio.com.ar puedan acceder el servidor HTTP** [**www.example.com**](http://www.example.com) **y mostrar correctamente su contenido deben tener el mismo sistema operativo.**

Falso, porque si todos los sistemas operativos (y navegadores usados, etc) implementan correctamente el protocolo HTTP, usar uno u otro será indistinto

**g. Un cliente web que desea acceder al servidor www.example.com y que no pertenece a ninguno**

**de estos dos dominios puede usar a ns1 de misitio.com.ar como servidor de DNS para resolver la**

**consulta.**

Falso, porque el servidor ns1 tiene la recursión deshabilitada

**h. Cuando Alicia quiera ver sus mails desde PC-D, ¿qué registro de DNS deberá consultarse?**

Consultará por los registros MX del dominio example.com., y luego, el registro A de mail1.example.com. (si en la respuesta al MX no se incluyó su IP como información adicional)

**i. Indicar todos los protocolos de mail involucrados, puerto y si usan TCP o UDP, en el envío y recepción de dicho mail**

|  |  |  |  |
| --- | --- | --- | --- |
| **Protocolo de emails** | **Protocolo de transporte** | **Número de puerto** | **Dirección de los datos** |
| SMTP | TCP | 25 | Envío/Recepción |
| IMAP | TCP | 143 | Envío/Recepción |
| POP | TCP | 110 | Recepción |