Practica 4 EMAIL

Ejercicio 1✅

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

Protocolo SMTP (Simple Mail Transfer Protocol): Es el protocolo estándar para el *envío* de correos electrónicos, es un protocolo de transferencia de correo, principal protocolo de la capa de aplicación para el correo electrónico. Se utiliza para enviar correos desde el cliente al servidor saliente y también se usa entre servidores de correo para el reenvió de mail.

Post Office Protocol (POP3): Descarga los correos al cliente y, por defecto, los elimina del servidor.

Internet Message Access Protocol (IMAP): Además de recibir correos mantiene los mensajes en el servidor y permite sincronización entre varios dispositivos

Ejercicio 2 ✅

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

Post Office Protocol (POP3):
Descarga los correos al cliente y, por defecto, los elimina del servidor.

Características:

- Diseñado para **descargar** los correos desde el servidor al cliente y **eliminarlos del servidor** por defecto.
- Ideal si usás un **solo dispositivo p**ara gestionar el correo.
- Es **simple** y consume pocos recursos.
- No permite organizar los correos en carpetas en el servidor.

Puertos:

- **110** → Sin cifrado.
- **995** → Con cifrado SSL/TLS.

Desventajas:

- Si descargas los correos en un dispositivo, **no los vas a ver en otro** (a menos que configures que no se eliminen del servidor).
- **No mantiene sincronización** entre dispositivos.

Internet Message Access Protocol (IMAP): Además de recibir correos mantiene los mensajes en el servidor y permite sincronización entre varios dispositivos

Características:

- Diseñado para que los correos **permanezcan en el servidor**.
- Ideal si usás **varios dispositivos** (ejemplo: celular, notebook, webmail).
- Permite organizar los correos en **carpetas** en el servidor.

- Sincroniza el estado de los correos (leído, respondido, borrado, etc.).

Puertos:

- **143** → Sin cifrado.
- **993** → Con cifrado SSL/TLS.

Ventajas:

- Todo queda centralizado en el servidor.
- La sincronización es en tiempo real.
- Perfecto para entornos colaborativos o empresariales

Ejercicio 3 ✅

Ejercicio 4 ✅

Ejercicio 5 ✅

Ejercicio 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. Asegúrese que tiene mails en el inbox y en la carpeta recientemente creada en cada una de las cuentas.
b. Cierre la sesión de la máquina virtual del usuario redes e ingrese nuevamente identificándose 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.
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?

b. i. POP: Todos los correos que anteriormente estaban marcados como NO VISTOS ahora no lo estan
IMAP: Los correos figuran como estaban en el otro usuarios, figuran como VISTOS
ii. POP no me muestra la carpeta que cree mientras que IMAP si

c. Si solamente se van enviar, recibir y a ver correos desde un solo sitio y usuario POP resulta ser una opcion buena, pero si se necesita acceder a la cuenta desde multiples lugares, crear carpetas, organizar los correos, ademas de enviar y recibir, la opcion mas fuerte es IMAP. Tener en cuenta que IMAP consume mas recursos del servidor ya que no borra los correos y se sincroniza permanentemente con los cambios realizados

Ejercicio 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

Destinatarios multiples del mismo dominio (MUA-MSA y MTA-MTA): Se puede enviar mas de un correo (o un solo correo a multiples destinatarios) durante la misma conexion TCP, tanto en MUA-MSA como MTA-MTA
Destinatarios múltiples de diferentes dominios (MUA-MSA y MTA-MTA): El MUA puede enviar el correo a múltiples dominios en una única conexión TCP con su MSA pero el MMA o los MTA involucrados deben abrir conexiones, TCP con su MSA pero el MSA o los MTA involucrados deben abrir conexiones TCP separadas para cada uno de los dominios
Resumen:
mismo dominio → Optimizar conexión TCP
diferentes dominio → requiere múltiples conexiones para asegurar la entrega

Destinatarios múltiples del mismo dominio

Entre MUA y MSA / Entre MTA y MTA:

- Sí, es posible enviar varios destinatarios o incluso varios mensajes durante una misma conexión TCP.
- SMTP permite reutilizar la conexión para múltiples comandos `RCPT TO`, siempre que los destinatarios pertenezcan al mismo dominio.
- Esto es eficiente y evita el costo de abrir nuevas conexiones.

Ventaja: Optimiza la conexión TCP y reduce latencia.

Destinatarios múltiples de distintos dominios

Entre MUA y MSA:

- El cliente (MUA) puede enviar un mensaje con varios destinatarios (de distintos dominios) en una sola conexión TCP al servidor de salida (MSA).
- Es el MSA el que se encarga de separar el mensaje por dominios y repartirlos.

Entre MTA y MTA:

- El MSA/MTA debe abrir una conexión TCP separada por cada dominio de destino.
- Cada servidor de correo (MTA) es responsable solo de su propio dominio, por lo tanto, SMTP requiere establecer una sesión diferente con cada uno.

Implicancia: Requiere múltiples conexiones TCP → más recursos.

Ejercicio 8 ✅

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

Sí, es posible.

El MSA (Mail Submission Agent), que típicamente escucha en el puerto **587** (o **465** para SMTPS), **puede configurarse para escuchar en otro puerto**.

Implicancias:

- **Configuración manual necesaria:** El MUA (cliente de correo) debe estar correctamente configurado para usar ese puerto no convencional.
- **No estándar:** Algunos cortafuegos o servicios de red podrían **bloquear puertos no estándar**, lo que dificultaría la entrega del correo.
- **Puede usarse como técnica de evasión de filtros o restricciones**, por ejemplo, en redes donde los puertos de correo estándar están bloqueados.

Ejercicio 9 ✅

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

Sí, también es posible.

Un MTA (Mail Transfer Agent), que normalmente escucha en el puerto **25** para la recepción de correos entre servidores, puede ser configurado para usar otro puerto.

Implicancias:

- **Problemas con otros MTA:** Los servidores de correo de Internet **esperan que el MTA escuche en el puerto 25**. Si se usa otro puerto:
  - **Otros servidores no podrán entregar correos** a ese dominio a menos que estén explícitamente configurados para hacerlo, lo cual **no es práctico** ni estándar.
- **No recomendado para uso público**, ya que **rompe con la interoperabilidad** esperada en SMTP.

Ejercicio 10

Ejercicio integrador HTTP, DNS y MAIL
Suponga que registró bajo su propiedad el dominio
redes2024.com.ar y dispone de 4 servidores:
● Un servidor DNS instalado configurado como primario de la zona
redes2024.com.ar. (hostname: ns1 - IP: 203.0.113.65).
● Un servidor DNS instalado configurado como secundario de la zona
redes2024.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 envíar 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.redes2024.com.ar
a. ¿Qué información debería informar al momento del registro para hacer visible a Internet el dominio registrado?
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.
c. ¿Es necesario que el servidor de DNS acepte consultas recursivas? Justifique.
d. ¿Qué servicios/protocolos de capa de aplicación configuraría en cada servidor?

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.
f. ¿Cómo cree que se conectaría el webmail del servidor web con el servidor de correo? ¿Qué protocolos usaría y para qué?
g. ¿Cómo se podría hacer para que cualquier MTA reconozca como válidos los mails provenientes del dominio
redes2024.com.ar solamente a los que llegan de la dirección 203.0.113.111? ¿Afectaría esto a los mails enviados desde el Webmail? Justifique.
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)?
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
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 ve? ¿Es esto una indicación de una estafa? Justifique
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?
l. Dado que solo disponemos de un servidor de correo, ¿qué sucederá con los mails que intenten ingresar durante un reinicio del servidor?
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?

a. Se debe proporcionar al momento de hacer visible el dominio la informacion de los servidores de DNS autoritativos, deben ser configurados para ser autoritativos del dominio redes2024.com.ar

b.

Nombre del registro	Tipo de registro	Prioridad	TTL	Valor del registro
@ (redes2024.com.ar)	NS	-	3600	ns1.redes2024.com.ar.
@ (redes2024.com.ar)	NS	-	3600	ns2.redes2024.com.ar.
ns1.redes2024.com.ar	A	-	3600	203.0.113.65
ns2.redes2024.com.ar	A	-	3600	203.0.113.66
correo.redes2024.com.ar	A	-	3600	203.0.113.8
mail.redes2024.com.ar	A	-	3600	203.0.113.111
webmail.redes2024.com.ar	CNAME	-	3600	correo.redes2024.com.ar
@ (redes2024.com.ar)	MX	10	3600	mail.redes2024.com.ar.

c. No, no es necesario, el servidor DNS debe ser autoritativo para redes2024.com.ar, no resolver dominios para clientes, permitir recursión puede ser un riesgo de seguridad

d. NS1 y NS2 → DNS
Mail → Smtp, IMAP o POP
Correo → HTTPS

e.

Servidor	Protocolo	Transporte	Puerto
ns1, ns2	DNS	UDP/TCP	53
mail	SMTP	TCP	25
mail	IMAP	TCP	143 o mejor 993 (IMAPS)

mail	POP3	TCP	110 o mejor 995 (POP3S)
correo	HTTPS	TCP	443

f. Se conectarian mediante POP3 o IMAP que permiten consultar y gestionar correos mientras que para el envio de correos utilizaria SMTP

g. Se debe configurar SPF en el DNS, este registro especificara que solo solo los correos provenientes de esa IP son validos. No afectaria al webmail ya que tambien utiliza esa ip para el envio de correos

h. La carateristica es que todos los protocolos (SMTP, IMAP y POP) trabajan sobre texto ASCII de 7 bits, no se permiten datos binarios, por eso se usa un encoding para convertir binarios a texto valido.

i. Si, es posible alterar el campo from den un correo esto se llama Spoofing, es un truco comun en estafas del tipo Phishing

j. Si, usando campos como BCC el destinatario no ve que otro tambien lo recibio

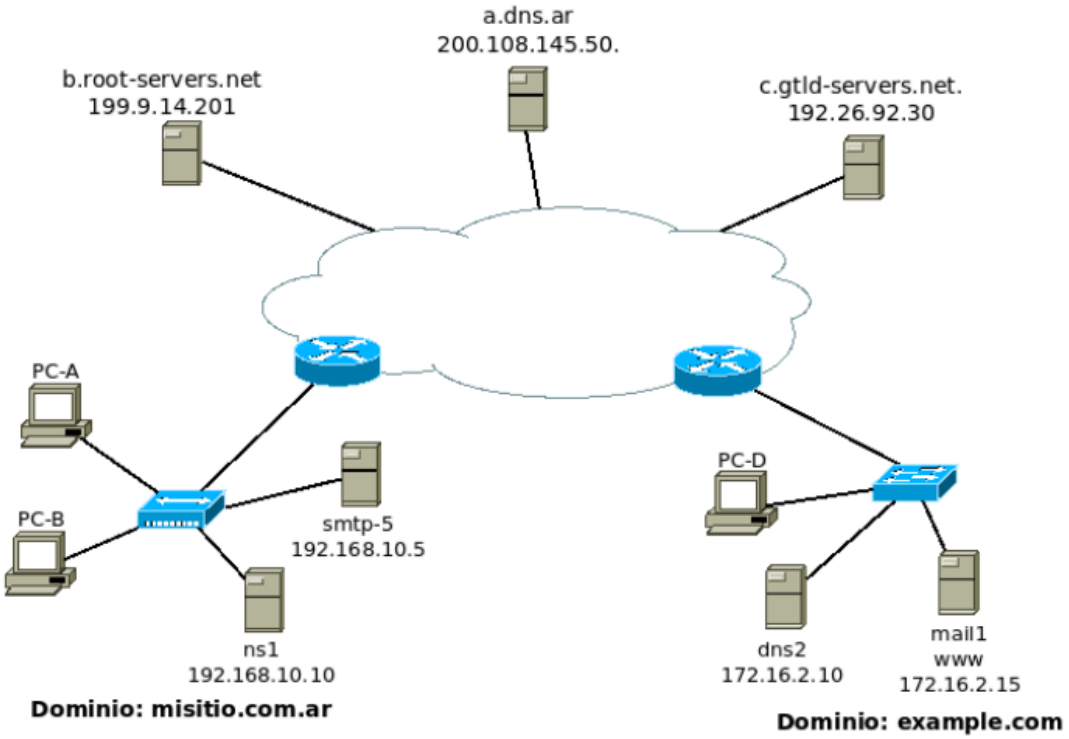
k.
   - El MUA (cliente de correo) usará **SMTP** (normalmente puerto 587 autenticado).
   - Se conectará al servidor **SMTP** del dominio `info.unlp.edu.ar`.
   - Obtendrá la dirección del servidor mediante una consulta **DNS tipo MX**.
   - Necesitará **usuario y contraseña** para autenticarse.

l. Los servidores de correo remoto intentaran reintentar la entra del correo varias veces, durante horas o dias, antes de descartar el correo

m. Se podria utilizar un sistema de master/slave (con prioridades) poner como servidor primario de mail al servidor en la nube y como secundario al nuestro, o sea tendríamos que agregar otro registro MX y a su vez otro registro A con la ip de este servidor en la nube

Ejercicio 11 ❌

Ejercicio 12



● El usuario juan@misitio.com.ar en PC-A desea enviar un mail al usuario alicia@example.com
● Cada organización tiene su 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?
b. Al enviar el mail, ¿por cuál registro de DNS consultará el MUA?
c. Una vez que el mail fue recibido por el servidor smtp-5, ¿por qué registro de DNS consultará?
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?

a. Es posible que suceda, pero se identificaría el servidor de mail y de http mediante los puertos que utiliza
b. Consultaria por el registro MX
c. Consultaria por el registro A de example.com
d. Si seria necsario ya que necesita resolver el nombre de una direccion IP, esto implica realizar una consutla de tipo A o AAAA al servidor DNS
e. .
f. F: El servidor DNS no analiza caberas SMTP ya que las consultas se basan en el nombre de dominio y los reg. DNS, no en el contenido del mail
   F: El protocolo SMTP opera en la capa de aplicación, los datos son encapsulados en el transporte TCP para la transmisión
   V: Cada protocolo agrega su propia cabecera con info especifica necesario para el funcionamiento
   F: Aunque todos operan en la capa de app. las cabeceras agregadas por cada protocolo no se

puede interpretar directamente entre protocolos distintos
F: No es necesario que los SO sean iguales solo que los interpretes utilicen tecnologías compatibles

g. Si, siempre que NS1 tenga la capacidad de resolver el nombre de dominio www.example.com, no es lo comun si no tiene la recursion habilitada

h. Deberia consulta al registro MX del dominio eample.com para determinar cual es el servidor de correo encargado de manejar correos electronicos

i. Envio de correo SMTP → 25 o 587 (TCP)
Recepcion de correo → IMAP (145 o 993) o POP (110 o 995) (TCP)