Práctica 4 RyC

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

En ambos casos se usa SMTP.

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

IMAP y POP3.
POP3 es un protocolo más simple que consta de 3 fases: Autorización, transacción, y actualización. En cada fase se ejecutan ciertos comandos, el primera se ejecuta por ejemplo user <nombreusuario> y pass <contraseña>.
En la transacción el usuario recupera los mensajes y los puede marcar para borrar, y el servidor responderá con +OK e información, -ERR si hubo un error con el comando.
En la fase de actualización se hace cuando se ejecute el comando quit y se hace todo lo de borrado.
Además se puede configurar para “descargar y borrar” (es decir descargar todo en la terminal local y borrar del server, comandos list, retr y dele) o “descargar y guardar”.

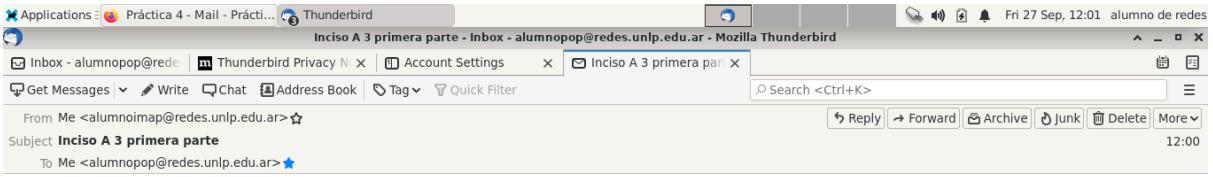
IMAP es un protocolo más complejo, ya que permite el manejo de carpetas, los mensajes se ponen en el buzón del recipiente que luego los puede mover entre carpetas, eliminar, crear nuevas carpetas o borrarlas, etc. Además permite buscar y obtener partes de los mensajes en vez de descargarlos entero.
Guarda información entre sesiones como el nombre de las carpetas y que mensajes tienen.

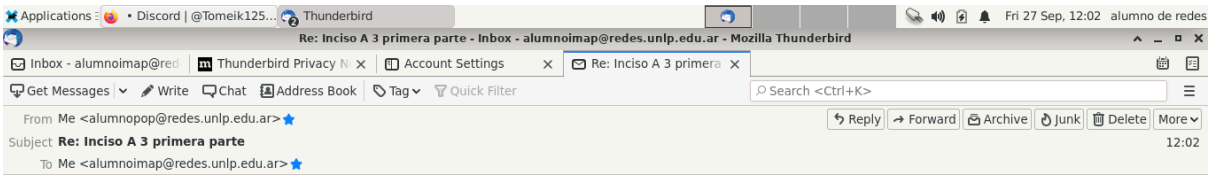
3. Utilizando la VM y teniendo en cuenta los siguientes datos, abra el cliente de correo (Thunderbird) y configurar dos cuentas de correo. Una de las cuentas utilizará POP para solicitar al servidor los mails recibidos para la misma mientras que la otra utilizará IMAP.

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
• 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.



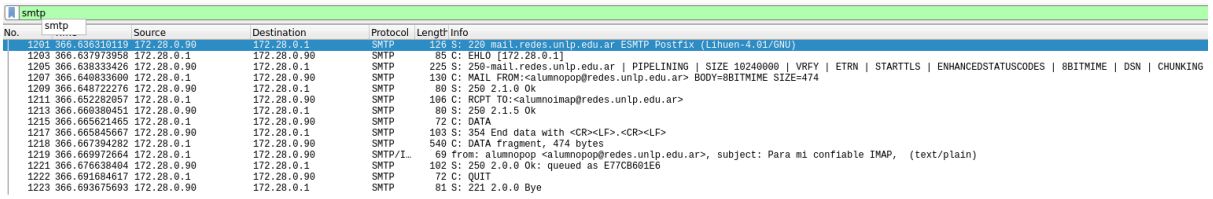


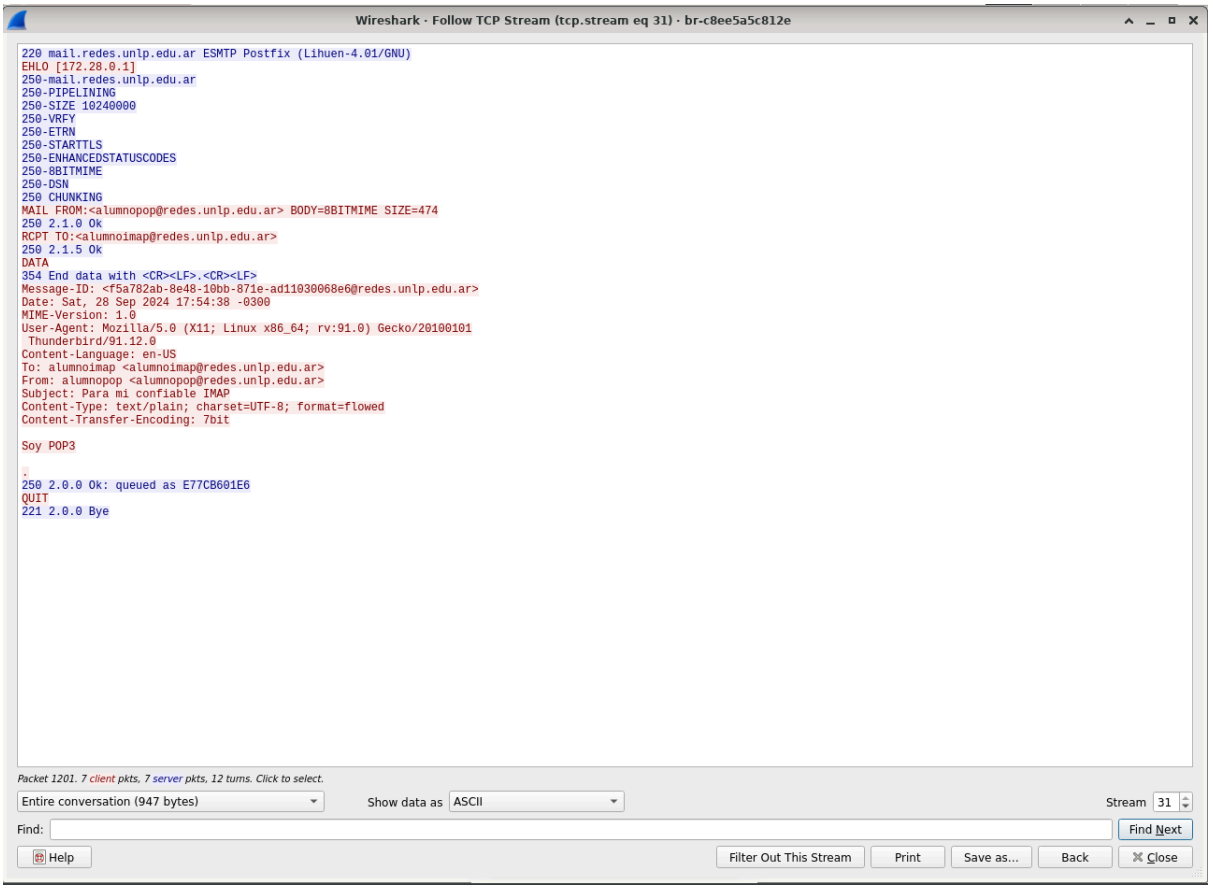

```
On 9/27/24 12:00, alumnoimap wrote:
Respuesta desde POP
```

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

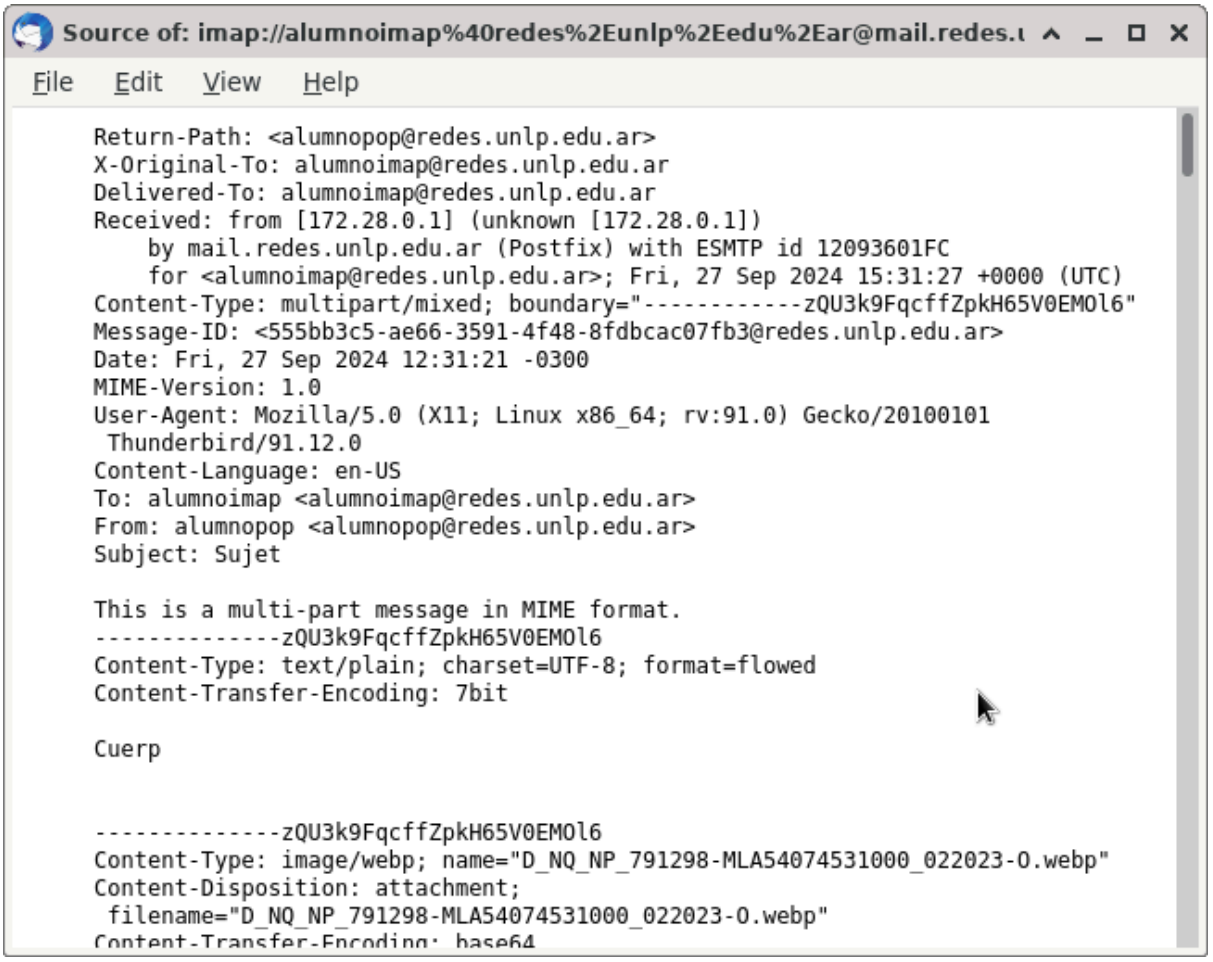
ii. Utilice el filtro SMTP para observar los paquetes del protocolo SMTP en la captura generada y analice el intercambio de dicho protocolo entre el cliente y el servidor para observar los distintos comandos utilizados y su correspondiente respuesta. Ayuda: filtre por protocolo SMTP y sobre alguna de las líneas del intercambio haga click derecho y seleccione Follow TCP Stream.




Wireshark · Follow TCP Stream (tcp.stream eq 31) · br-c8ee5a5c812e
220 mail.redes.unlp.edu.ar ESMTP Postfix (Lihuen-4.01/GNU)
EHLO [172.28.0.1]
250-mail.redes.unlp.edu.ar
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250 CHUNKING
MAIL FROM:<alumnopop@redes.unlp.edu.ar> BODY=8BITMIME SIZE=474
250 2.1.0 Ok
RCPT TO:<alumnoimap@redes.unlp.edu.ar>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Message-ID: <f5a782ab-8e48-10bb-871e-ad11030068e6@redes.unlp.edu.ar>
Date: Sat, 28 Sep 2024 17:54:38 -0300
MIME-Version: 1.0
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
Thunderbird/91.12.0
Content-Language: en-US
To: alumnoimap <alumnoimap@redes.unlp.edu.ar>
From: alumnopop <alumnopop@redes.unlp.edu.ar>
Subject: Para mi confiable IMAP
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 7bit
Soy POP3
.
250 2.0.0 Ok: queued as E77CB601E6
QUIT
221 2.0.0 Bye
Packet 1201. 7 client pkts, 7 server pkts, 12 turns. Click to select.
Entire conversation (947 bytes)
Show data as ASCII
Stream 31
Find:
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close

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 las fuentes del correo recibido para entender cómo se utiliza el header “Content-Type: multipart/mixed“ para poder realizar el envío de distintos archivos adjuntos.



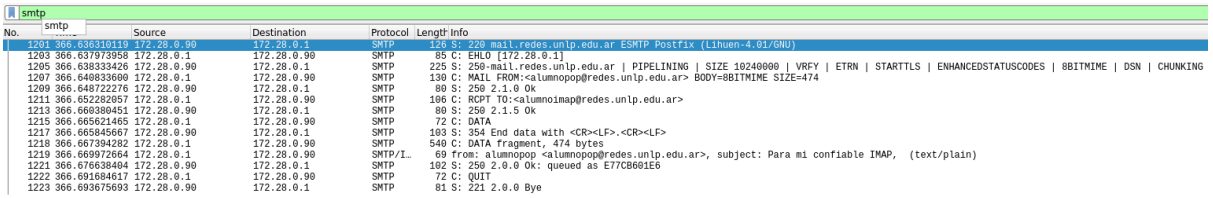
Content-type: multipart/mixed; indica que el mensaje tiene muchas partes y diferentes tipos, boundary=”...” es el que separa cada parte. Cada parte tendrá su tipo y su codificación, en este caso la imagen viene en base64 y el texto en ascii 7 bits.

ii. Extraiga la imagen adjunta del mismo modo que lo hace el cliente de correo a partir de las fuentes del mensaje.

Se intentó, copiamos el código base64 a un txt y lo intentamos transformar pero decía que era un input invalido.

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.



(Misma imagen que el punto anterior porque hace lo mismo)

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.

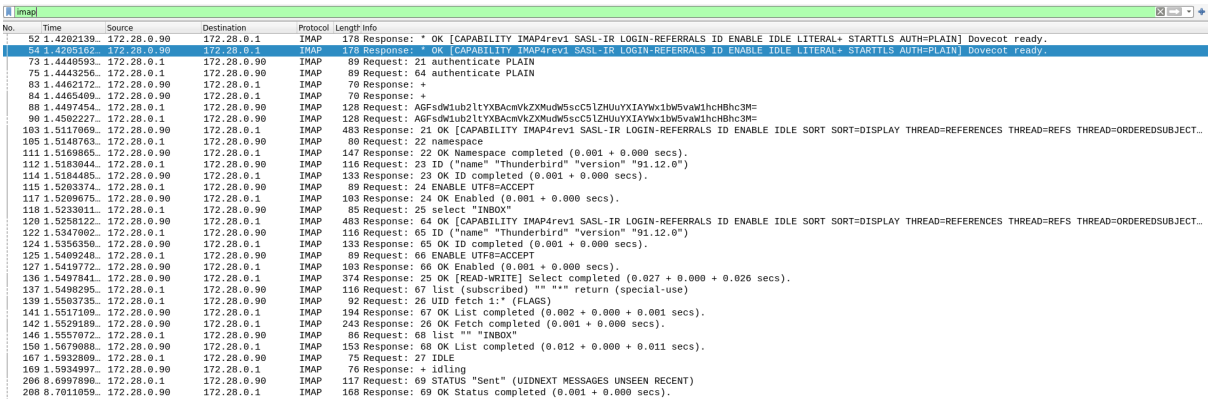
pop

No.	Time	Source	Destination	Protocol	Length	Info
56	1.4225281…	172.28.0.90	172.28.0.1	POP	86	S: +OK Dovecot ready.
58	1.4330347…	172.28.0.1	172.28.0.90	POP	72	C: AUTH
60	1.4342492…	172.28.0.90	172.28.0.1	POP	81	S: +OK
71	1.4440092…	172.28.0.1	172.28.0.90	POP	72	C: CAPA
77	1.4447779…	172.28.0.90	172.28.0.1	POP	155	S: +OK
97	1.4561372…	172.28.0.1	172.28.0.90	POP	78	C: AUTH PLAIN
99	1.4575965…	172.28.0.90	172.28.0.1	POP/…	70	+
101	1.4577479…	172.28.0.1	172.28.0.90	POP	100	C: AGFsdW1ub3BvcABhbHVtbm9wb3BwYXNz
107	1.5150423…	172.28.0.90	172.28.0.1	POP	82	S: +OK Logged in.
109	1.5151423…	172.28.0.1	172.28.0.90	POP	72	C: STAT
128	1.5422114…	172.28.0.90	172.28.0.1	POP	77	S: +OK 1 776
130	1.5479277…	172.28.0.1	172.28.0.90	POP	72	C: LIST
132	1.5481986…	172.28.0.90	172.28.0.1	POP	93	S: +OK 1 messages:
133	1.5493655…	172.28.0.1	172.28.0.90	POP	72	C: UIDL
135	1.5495276…	172.28.0.90	172.28.0.1	POP	94	S: +OK
143	1.5540490…	172.28.0.1	172.28.0.90	POP	72	C: QUIT
145	1.5549558…	172.28.0.90	172.28.0.1	POP	84	S: +OK Logging out.
15…	618.35919…	172.28.0.90	172.28.0.1	POP	86	S: +OK Dovecot ready.
15…	618.35953…	172.28.0.1	172.28.0.90	POP	72	C: CAPA
15…	618.36034…	172.28.0.90	172.28.0.1	POP	155	S: +OK
15…	618.36341…	172.28.0.1	172.28.0.90	POP	78	C: AUTH PLAIN
15…	618.36442…	172.28.0.90	172.28.0.1	POP/…	70	+
15…	618.36890…	172.28.0.1	172.28.0.90	POP	100	C: AGFsdW1ub3BvcABhbHVtbm9wb3BwYXNz
15…	618.37494…	172.28.0.90	172.28.0.1	POP	82	S: +OK Logged in.
15…	618.37608…	172.28.0.1	172.28.0.90	POP	72	C: STAT
15…	618.37623…	172.28.0.90	172.28.0.1	POP	77	S: +OK 1 776
15…	618.37754…	172.28.0.1	172.28.0.90	POP	72	C: LIST
15…	618.37774…	172.28.0.90	172.28.0.1	POP	93	S: +OK 1 messages:
15…	618.37866…	172.28.0.1	172.28.0.90	POP	72	C: UIDL
15…	618.37891…	172.28.0.90	172.28.0.1	POP	94	S: +OK
16…	618.38678…	172.28.0.1	172.28.0.90	POP	72	C: QUIT
16…	618.38728…	172.28.0.90	172.28.0.1	POP	84	S: +OK Logging out.

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 un 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.



imap

No.	Time	Source	Destination	Protocol	Length	Info
52	1.4202139…	172.28.0.90	172.28.0.1	IMAP	178	Response: * OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITERAL+ STARTTLS AUTH=PLAIN] Dovecot ready.
54	1.4205162…	172.28.0.90	172.28.0.1	IMAP	178	Response: * OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITERAL+ STARTTLS AUTH=PLAIN] Dovecot ready.
73	1.4440593…	172.28.0.1	172.28.0.90	IMAP	89	Request: 21 authenticate PLAIN
75	1.4443256…	172.28.0.1	172.28.0.90	IMAP	89	Request: 64 authenticate PLAIN
83	1.4462172…	172.28.0.90	172.28.0.1	IMAP	70	Response: +
84	1.4465409…	172.28.0.90	172.28.0.1	IMAP	70	Response: +
88	1.4497454…	172.28.0.1	172.28.0.90	IMAP	128	Request: AGFsdW1ub2ltYXBAcmVkZXMudW5scC5lZHUuYXIAYWx1bW5vaW1hcHBhc3M=
90	1.4502227…	172.28.0.1	172.28.0.90	IMAP	128	Request: AGFsdW1ub2ltYXBAcmVkZXMudW5scC5lZHUuYXIAYWx1bW5vaW1hcHBhc3M=
103	1.5117069…	172.28.0.90	172.28.0.1	IMAP	483	Response: 21 OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE SORT SORT=DISPLAY THREAD=REFERENCES THREAD=REFS THREAD=ORDEREDSUBJECT…
105	1.5148763…	172.28.0.1	172.28.0.90	IMAP	80	Request: 22 namespace
111	1.5169865…	172.28.0.90	172.28.0.1	IMAP	147	Response: 22 OK Namespace completed (0.001 + 0.000 secs).
112	1.5183044…	172.28.0.1	172.28.0.90	IMAP	116	Request: 23 ID ("name" "Thunderbird" "version" "91.12.0")
114	1.5184485…	172.28.0.90	172.28.0.1	IMAP	133	Response: 23 OK ID completed (0.001 + 0.000 secs).
115	1.5203374…	172.28.0.1	172.28.0.90	IMAP	89	Request: 24 ENABLE UTF8=ACCEPT
117	1.5209675…	172.28.0.90	172.28.0.1	IMAP	103	Response: 24 OK Enabled (0.001 + 0.000 secs).
118	1.5233011…	172.28.0.1	172.28.0.90	IMAP	85	Request: 25 select "INBOX"
120	1.5258122…	172.28.0.90	172.28.0.1	IMAP	483	Response: 64 OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE SORT SORT=DISPLAY THREAD=REFERENCES THREAD=REFS THREAD=ORDEREDSUBJECT…
122	1.5347002…	172.28.0.1	172.28.0.90	IMAP	116	Request: 65 ID ("name" "Thunderbird" "version" "91.12.0")
124	1.5356350…	172.28.0.90	172.28.0.1	IMAP	133	Response: 65 OK ID completed (0.001 + 0.000 secs).
125	1.5409248…	172.28.0.1	172.28.0.90	IMAP	89	Request: 66 ENABLE UTF8=ACCEPT
127	1.5419772…	172.28.0.90	172.28.0.1	IMAP	103	Response: 66 OK Enabled (0.001 + 0.000 secs).
136	1.5497841…	172.28.0.90	172.28.0.1	IMAP	374	Response: 25 OK [READ-WRITE] Select completed (0.027 + 0.000 + 0.026 secs).
137	1.5498295…	172.28.0.1	172.28.0.90	IMAP	116	Request: 67 list (subscribed) "" "*" return (special-use)
139	1.5503735…	172.28.0.1	172.28.0.90	IMAP	92	Request: 26 UID fetch 1:* (FLAGS)
141	1.5517109…	172.28.0.90	172.28.0.1	IMAP	194	Response: 67 OK List completed (0.002 + 0.000 + 0.001 secs).
142	1.5529189…	172.28.0.90	172.28.0.1	IMAP	243	Response: 26 OK Fetch completed (0.001 + 0.000 secs).
146	1.5557072…	172.28.0.1	172.28.0.90	IMAP	86	Request: 68 list "" "INBOX"
150	1.5679088…	172.28.0.90	172.28.0.1	IMAP	153	Response: 68 OK List completed (0.012 + 0.000 + 0.011 secs).
167	1.5932809…	172.28.0.1	172.28.0.90	IMAP	75	Request: 27 IDLE
169	1.5934997…	172.28.0.90	172.28.0.1	IMAP	76	Response: + idling
206	8.6997890…	172.28.0.1	172.28.0.90	IMAP	117	Request: 69 STATUS "Sent" (UIDNEXT MESSAGES UNSEEN RECENT)
208	8.7011059…	172.28.0.90	172.28.0.1	IMAP	168	Response: 69 OK Status completed (0.001 + 0.000 secs).

imap

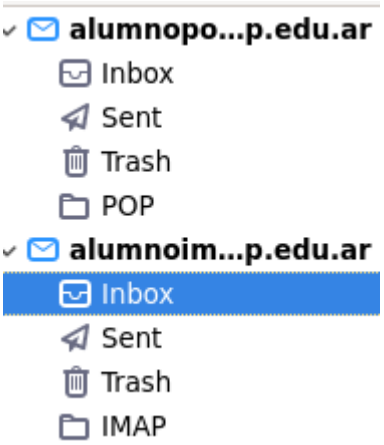
No.	Time	Source	Destination	Protocol	Length	Info
218	47.662199…	172.28.0.1	172.28.0.90	IMAP	72	Request: DONE
220	47.663437…	172.28.0.90	172.28.0.1	IMAP	121	Response: 27 OK Idle completed (46.071 + 46.069 + 46.070 secs).
222	47.672444…	172.28.0.1	172.28.0.90	IMAP	75	Request: 28 noop
224	47.673291…	172.28.0.90	172.28.0.1	IMAP	110	Response: 28 OK NOOP completed (0.001 + 0.000 secs).
226	47.675394…	172.28.0.1	172.28.0.90	IMAP	92	Request: 29 UID fetch 7:* (FLAGS)
228	47.676360…	172.28.0.90	172.28.0.1	IMAP	144	Response: 29 OK Fetch completed (0.001 + 0.000 secs).
230	47.693911…	172.28.0.1	172.28.0.90	IMAP	75	Request: 30 IDLE
232	47.694396…	172.28.0.90	172.28.0.1	IMAP	76	Response: + idling
360	167.93819…	172.28.0.90	172.28.0.1	IMAP	83	Response: * OK Still here
362	167.93971…	172.28.0.1	172.28.0.90	IMAP	72	Request: DONE
364	167.93997…	172.28.0.90	172.28.0.1	IMAP	124	Response: 30 OK Idle completed (120.246 + 120.245 + 120.245 secs).
365	167.94070…	172.28.0.1	172.28.0.90	IMAP	75	Request: 31 noop
367	167.94104…	172.28.0.90	172.28.0.1	IMAP	110	Response: 31 OK NOOP completed (0.001 + 0.000 secs).
368	167.94128…	172.28.0.1	172.28.0.90	IMAP	92	Request: 32 UID fetch 7:* (FLAGS)
370	167.94161…	172.28.0.90	172.28.0.1	IMAP	144	Response: 32 OK Fetch completed (0.001 + 0.000 secs).
371	167.96847…	172.28.0.1	172.28.0.90	IMAP	75	Request: 33 IDLE
373	167.96882…	172.28.0.90	172.28.0.1	IMAP	76	Response: + idling
958	287.07120…	172.28.0.90	172.28.0.1	IMAP	83	Response: * OK Still here
960	287.07610…	172.28.0.1	172.28.0.90	IMAP	72	Request: DONE
962	287.07635…	172.28.0.90	172.28.0.1	IMAP	124	Response: 33 OK Idle completed (119.108 + 119.107 + 119.107 secs).
964	287.08205…	172.28.0.1	172.28.0.90	IMAP	75	Request: 34 noop
966	287.08338…	172.28.0.90	172.28.0.1	IMAP	118	Response: 34 OK NOOP completed (0.002 + 0.000 + 0.001 secs).
968	287.08510…	172.28.0.1	172.28.0.90	IMAP	92	Request: 35 UID fetch 7:* (FLAGS)
970	287.08614…	172.28.0.90	172.28.0.1	IMAP	144	Response: 35 OK Fetch completed (0.001 + 0.000 secs).
972	287.12370…	172.28.0.1	172.28.0.90	IMAP	75	Request: 36 IDLE
974	287.12408…	172.28.0.90	172.28.0.1	IMAP	76	Response: + idling
12…	367.21380…	172.28.0.90	172.28.0.1	IMAP	90	Response: * 5 EXISTS
12…	367.21447…	172.28.0.1	172.28.0.90	IMAP	72	Request: DONE
12…	367.21470…	172.28.0.90	172.28.0.1	IMAP	121	Response: 36 OK Idle completed (80.091 + 80.079 + 80.090 secs).
12…	367.21496…	172.28.0.1	172.28.0.90	IMAP	75	Request: 37 noop
12…	367.21511…	172.28.0.90	172.28.0.1	IMAP	110	Response: 37 OK NOOP completed (0.001 + 0.000 secs).
12…	367.21522…	172.28.0.1	172.28.0.90	IMAP	92	Request: 38 UID fetch 7:* (FLAGS)

...

Mucho más, IMAP son una banda de cosas.

6. IMAP vs POP

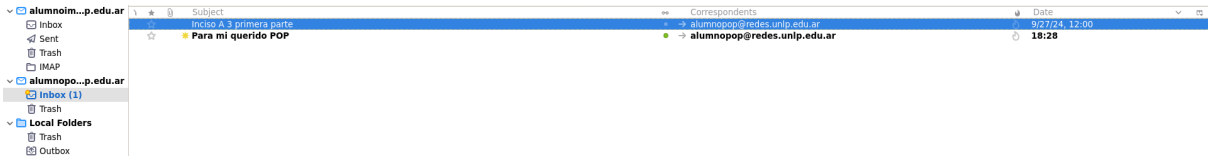
a. Marque como leídos todos los correos que tenga en el buzón de entrada de alumnopop y de alumnoimap. Luego, cree una carpeta llamada POP en la cuenta de alumnopop y una llamada IMAP en la cuenta de alumnoimap. Asegúrese que tiene mails en el inbox y en la carpeta recientemente creada en cada una de 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?



Lo que estaba en la carpeta de POP se desmarcó como leído y se puso en la inbox, y no está más la carpeta POP, IMAP se mantuvo igual.

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?

Mejor IMAP, pero requiere más recursos para mantener el tema de las carpetas.

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

Si es posible, en la teoría se indica que una conexión SMTP posee conexión persistentes para enviar varios mails seguidos de ser necesario.

Considere:

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

Sí, es posible. Si todos los destinatarios pertenecen al mismo dominio, el MUA puede enviar un único mensaje al MSA en una sola conexión TCP. El MSA luego se encargará de procesar y entregar el correo a los múltiples destinatarios internos o enviarlo a su respectivo destino.

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

También es posible. Los MTAs pueden optimizar la transferencia de correos utilizando una sola conexión TCP para enviar múltiples mensajes a diferentes destinatarios que pertenezcan al mismo dominio. Esto reduce la sobrecarga de establecer nuevas conexiones para cada correo.

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

Si, pero además el MUA también debería enviar los correos por ese puerto asi el MSA los interviene y los procesa.

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

Sí, es posible que un MTA escuche en un puerto diferente al 25, pero hay varias implicancias:

- **Compatibilidad**: El puerto 25 es el estándar para la comunicación entre MTAs, por lo que usar un puerto diferente podría romper la interoperabilidad con otros servidores de correo si estos no están configurados para usar el puerto alternativo.

- **Seguridad**: Al igual que en el caso del MSA, usar un puerto no estándar podría evitar algunos tipos de ataques automatizados, pero también podría requerir configuraciones personalizadas y más complejas para garantizar que todos los MTAs se comuniquen correctamente.
- **Configuración adicional**: Si el MTA usa un puerto no estándar, todos los MTAs que intenten enviarle correos tendrían que estar configurados para usar ese puerto, lo que puede complicar la configuración de red y la entrega de correos.

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.

● Un servidor de correo electrónico (hostname: mail - IP: 203.0.113.111).

● 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?

- Servidores de nombres (NS): Se debe informar la dirección IP y el hostname de los servidores DNS primario y secundario:
    - Primario: ns1.redes2024.com.ar con IP 203.0.113.65.
    - Secundario: ns2.redes2024.com.ar con la IP que se le asigne al servidor.12
- Registro A para el servidor web: Para que la URL https://webmail.redes2024.com.ar funcione correctamente, se debe crear un registro A que asocie el hostname "webmail" con la IP 203.0.113.8.3

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.

Registros Necesarios en el Servidor de Nombres para redes2024.com.ar

Para que el dominio `redes2024.com.ar` y sus servicios funcionen correctamente, se necesitan configurar los siguientes registros en los servidores de nombres `ns1` y `ns2`:

Nombre del registro	Tipo de registro	Prioridad	TTL (segundo)	Valor del registro
redes2024.com.ar	SOA		86400	ns1.redes2024.com.ar. admin.redes2024.com.ar. 2023102601 7200 3600 604800 86400
redes2024.com.ar	NS		86400	ns1.redes2024.com.ar.
redes2024.com.ar	NS		86400	ns2.redes2024.com.ar.
ns1	A		86400	203.0.113.65
ns2	A		86400	203.0.113.xx
mail	A		86400	203.0.113.111
redes2024.com.ar	MX	10	86400	mail.redes2024.com.ar.
correo	A		86400	203.0.113.8
webmail	CNAME		86400	correo.redes2024.com.ar.

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

Mientras que un servidor DNS local/resolver recursivo es esencial para resolver nombres de dominio fuera de la zona redes2024.com.ar, los servidores DNS ns1 y ns2 pueden funcionar correctamente sin aceptar consultas recursivas. Su función principal es proporcionar información autoritativa para su zona, lo que pueden lograr respondiendo a consultas directas o proporcionando referencias a otros servidores DNS a través de consultas iterativas

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

- ns1 (Servidor DNS Primario):
  - Servicio: Sistema de Nombres de Dominio (DNS).
  - Protocolo: DNS.
- ns2 (Servidor DNS Secundario):
  - Servicio: Sistema de Nombres de Dominio (DNS).

    - Protocolo: DNS.
- mail (Servidor de Correo Electrónico):
    - Servicio: Correo Electrónico.
- Protocolos:
    - SMTP (Simple Mail Transfer Protocol): Para el envío de correos electrónicos desde los clientes de correo hacia el servidor y entre servidores de correo.
    - POP3 (Post Office Protocol versión 3) o IMAP (Internet Message Access Protocol): Para la recepción de correos electrónicos por parte de los clientes de correo desde el servidor.
- correo (Servidor WEB para Webmail):
    - Servicio: Webmail.
    - Protocolo: HTTPS (HTTP Seguro)

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.

DNS 53 , POP110, IMAP 143, SMTP 25 o 587, HTTPS 443.

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

El webmail sería el MUA, usaría SMTP para enviar y para extraer IMAP o POP.

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.

- SPF (Sender Policy Framework): SPF permite a los propietarios de dominios especificar en los registros DNS qué servidores están autorizados a enviar correos electrónicos en su nombre. Los MTA pueden verificar el registro SPF para determinar si la IP del remitente está autorizada.
- DKIM (DomainKeys Identified Mail): DKIM utiliza firmas digitales para verificar que los correos electrónicos no han sido modificados durante el tránsito
- DMARC (Domain-based Message Authentication, Reporting and Conformance): DMARC combina SPF y DKIM para proporcionar una capa adicional de protección contra el correo electrónico fraudulento y el phishing.

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)?

Que use ASCII de 7 bits.

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

Sí, es posible enviar un correo electrónico de modo que el receptor vea un remitente distinto al real. Esto se debe a que la información del remitente que se muestra en la interfaz de un cliente de correo electrónico se extrae del encabezado del mensaje, específicamente de las líneas From: y To:, que contienen meta información del correo.
¿Cómo se Puede Hacer?
Un usuario malintencionado podría modificar el encabezado del mensaje para falsificar la dirección del remitente. Esto se puede lograr a través de diversas técnicas, incluyendo:
Manipulación del Software de Correo: Algunos softwares de correo permiten modificar manualmente los campos del encabezado, incluyendo la dirección del remitente.
Scripts y Herramientas Especializadas: Existen scripts y herramientas disponibles que pueden automatizar el proceso de falsificación de correos electrónicos, permitiendo a los usuarios malintencionados enviar correos masivos con remitentes falsos.
¿Es una Indicación de Estafa?
En muchos casos, sí. La falsificación del remitente en un correo electrónico es una técnica comúnmente utilizada en estafas de phishing y otros tipos de ataques informáticos.

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

Sí, es posible enviar un correo electrónico de manera que el encabezado muestre un destinatario diferente al real. Esta manipulación se logra modificando la línea RCPT TO: del envoltorio del mensaje, la cual no es visible para el usuario final.
¿Cómo se Puede Hacer?
La modificación del envoltorio se realiza a nivel del servidor de correo (MTA) y generalmente requiere acceso privilegiado al sistema. Un usuario malintencionado con acceso al servidor de correo podría modificar el destinatario real del mensaje sin que esto se refleje en el encabezado visible para el usuario.
¿Por qué No le Llegaría al Destinatario que el Receptor Ve?
El destinatario real del correo electrónico se define en el envoltorio, utilizado por los MTA para la entrega del mensaje. El encabezado, incluyendo la línea To:, solo contiene meta información visible para el usuario pero no determina la ruta de entrega. El MTA emisor utiliza la información del envoltorio, específicamente la línea RCPT TO:, para determinar el servidor de correo del destinatario y entregar el mensaje al buzón correspondiente.
¿Es una Indicación de Estafa?
Potencialmente, sí. Si bien la manipulación del destinatario en el envoltorio no es visible para el usuario final, podría ser utilizada con fines maliciosos, como:

Interceptación de Información: Un atacante podría interceptar correos electrónicos dirigidos a un destinatario específico, modificando el envoltorio para que el mensaje sea entregado a su propio servidor.
Ataques de Suplantación: Al combinar la manipulación del destinatario en el envoltorio con la falsificación del remitente en el encabezado, un atacante podría enviar correos electrónicos que parezcan provenir de un usuario legítimo y dirigidos a otro usuario, ocultando su verdadera identidad y la del destinatario real.

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?

SMTP, se conecta con el MSA, necesita el registro MX y AAAA de remitente.

l. Dado que solo disponemos de un servidor de correo, ¿qué sucederá con los mails que intenten ingresar durante un reinicio del servidor?

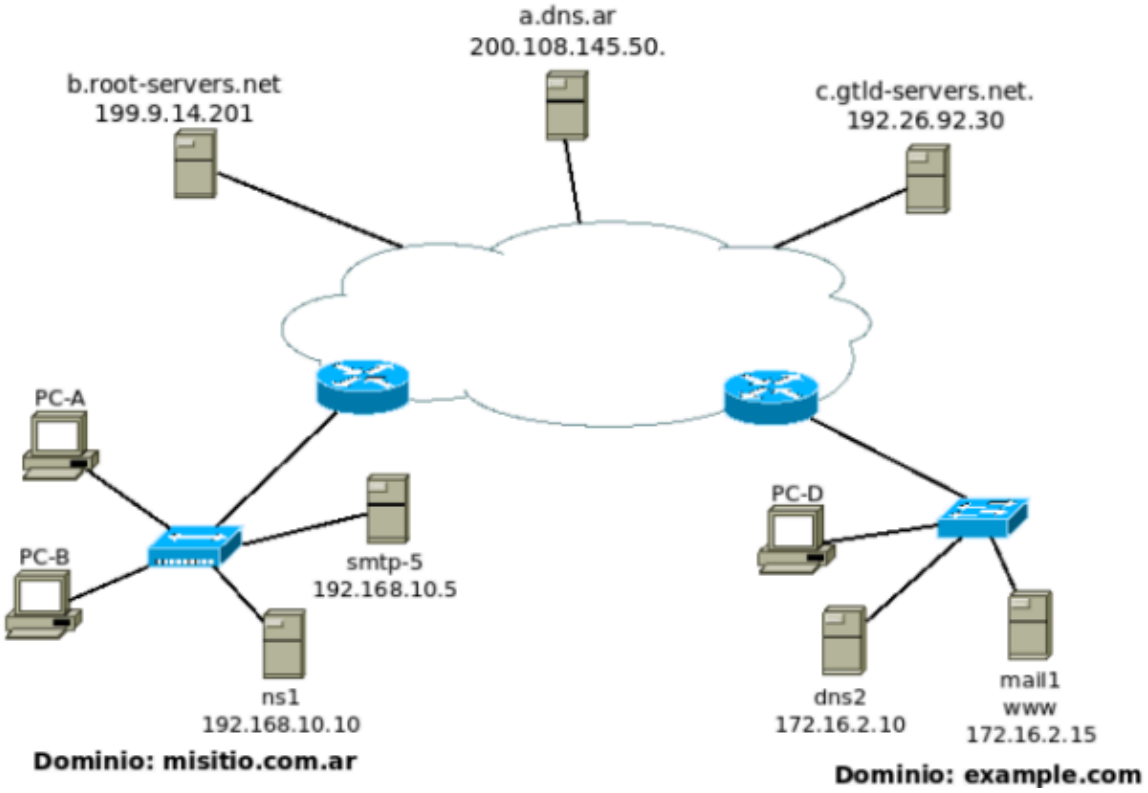
Se encolaran.

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?

1. Crear Registros MX para Ambos Servidores: Se debe crear un registro MX para cada servidor de correo, incluyendo el servidor propio y el servidor en la nube.
2. Asignar Prioridades a los Registros MX: Asignar una prioridad numérica a cada registro MX. El servidor con la prioridad más baja será el servidor principal, mientras que el servidor con la prioridad más alta actuará como respaldo en caso de fallo del servidor principal. Por ejemplo:
    a. mail.sudominio.com. MX 10 mail.nube.com. (prioridad 10 para el servidor en la nube)
    b. mail.sudominio.com. MX 20 mail.local.com. (prioridad 20 para el servidor propio)
3. Configurar los Servidores de Correo: Ambos servidores de correo deben estar configurados para aceptar correo para el dominio.

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



• 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?

Si, ya que están en la misma computadora. Para resolverlo ellos escucharan a puertos distintos.

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

A/AAAA..

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

MX.

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/AAAA.

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

Debe consultar por el root server mas temprano para los .com (c.gtld-servers.net)
Luego por el servidor autoritativo .com, que proporciona la IP del DNS que tiene example.com.
Por último consultará a los DNS autoritarios 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. Los datos de la cabecera de SMTP no deben ser analizados por el servidor DNS para responder a la consulta de 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. Al ser recibidos por el servidor smtp-5, los datos agregados por el protocolo SMTP no serán analizados por cada una de las capas inferiores.

● Cada protocolo de la capa de aplicación agrega una cabecera con información propia de ese protocolo

Verdadero. Cada protocolo de la capa de aplicación agrega una cabecera con información propia de ese protocolo.

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

Falso. Las cabeceras agregadas por el protocolo de DNS no pueden ser analizadas y comprendidas por el protocolo SMTP o HTTP.

● Para que los cliente en misitio.com.ar puedan acceder el servidor HTTP www.example.com y mostrar correctamente su contenido deben tener el mismo sistema operativo.

Falso. Para que los clientes en misitio.com.ar puedan acceder al servidor HTTP www.example.com y mostrar correctamente su contenido, no es necesario que tengan el mismo sistema operativo

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.

Debería poder asignarse cualquiera como servidor DNS para la consulta.

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

Ninguno accede desde PC-D mediante POP3 y IMAP.

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

SMTP, POP3, IMAP, 25, 110, 143