

Resumen Redes y Comunicaciones

Basado en preguntas viejas

DNS.....	1
SMTP/DNS.....	5
HTTP.....	7
EMAIL.....	10
FTP.....	12
CAPA DE APLICACION.....	13

Las respuestas correctas están resaltadas en rosa (gracias Mile 🙏).

DNS

Indique en qué casos la **consulta** se hace forma **iterativa**

- Cuando se consulta por un registro SOA
- Cuando se consulta al servidor de DNS local que tenemos configurado en nuestra red
- Al realizar una consulta como DNS local al root server
- Cuando el DNS tiene que resolver una consulta que no tiene cacheada la respuesta
- Al consultar a un open DNS como 8.8.8.8

Justificación:

Cuando no tengo la respuesta el DNS local la busca iterativamente entre los servidores DNS, cada consulta a los servidores externos sería iterativa.

El SOA es un registro que guarda información de la configuración de un dominio, no importa para saber si es iterativa o no.

Indique en qué casos la **consulta** se hace forma **recursiva**

- Cuando se consulta por un registro SOA
- Cuando se consulta al servidor de DNS local que tenemos configurado en nuestra red
- Al realizar una consulta como DNS local al root server
- Cuando el DNS tiene que resolver una consulta que no tiene cacheada la respuesta
- Al consultar a un open DNS como 8.8.8.8

Dada la siguiente respuesta DNS indicar las afirmaciones correctas

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47728
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;, udp: 1232
;; QUESTION SECTION:
;chatgptonline.io.          IN      NS

;; ANSWER SECTION:
chatgptonline.io.          86400   IN      NS      novalee.ns.cloudflare.com.
chatgptonline.io.          86400   IN      NS      paul.ns.cloudflare.com.

;; Query time: 20 msec
;; SERVER: 108.162.193.135#53(108.162.193.135)
;; WHEN: lun abr 10 10:39:12 -03 2023
;; MSG SIZE rcvd: 103
```

- El servidor que respondió es autoritativo.
- La consulta se realizó de forma recursiva.
- El servidor acepta consultas recursivas.
- El servidor de DNS consultado es 108.162.193.135.
- El servidor de DNS consultado es 8.8.8.8
- Se consultó por un registro CNAME.
- Se consultó por un registro A.

Justificación:

AA -> Es autoritativo.

RD -> La consulta se hizo de forma recursiva.

RA -> El Servidor acepta consultas recursivas (no lo tiene).

En parte final donde dice SERVER podemos ver el server, y el registro pedido fue NS (QUERY SECTION)

¿Cuál es el propósito de la delegación de autoridad en una red? Selecciona todas las respuestas correctas.

- Facilitar la administración centralizada de la red.
- Reducir la carga de trabajo en servidores centrales.
- Permitir que los servidores locales tomen decisiones autónomas.
- Mejorar la seguridad de la red.

Justificación:

Delegar baja la descentralización y mejora la distribución e independencia.

Marque todas las opciones correctas

- Las consultas recursivas y las iterativas son dos términos que se utilizan indistintamente en DNS.
- Las consultas recursivas de DNS pueden ser utilizadas para obtener información de cualquier dominio en Internet, incluso si el servidor DNS que recibe la consulta no es el servidor autoritativo para ese dominio.
- Las consultas recursivas de DNS sólo pueden ser utilizadas para obtener información de los dominios que están configurados en el servidor DNS que recibe la consulta.

Indique con una R(recursiva) o con I(iterativa) en cada opción, cómo se debería hacer la consulta

- Cuando se consulta a un servidor de un TLD [I]
- Cuando se consulta al servidor de DNS local resolver que tenemos configurado en nuestra red [R]
- Al realizar una consulta como DNS local/resolver a un root server [I]
- Cuando el DNS local debe resolver una consulta que no tiene cacheada la respuesta [I]
- Al consultar a un open DNS como por ejemplo 1.1.1.1 [R]
- Cuando el servidor de mail debe determinar a qué servidor enviar el e-mail [R]

Justificación:

Cuando consultamos a un servidor local es recursivo, un open DNS actúa como servidor local.

Dada la siguiente respuesta DNS indicar cuales son verdaderas

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24766
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
/amazon.                                IN      NS

;; ANSWER SECTION:
amazon.      21600  IN      NS      dnsb.nic.amazon.
amazon.      21600  IN      NS      dnsc.nic.amazon.
amazon.      21600  IN      NS      dns1.nic.amazon.
amazon.      21600  IN      NS      dns2.nic.amazon.
amazon.      21600  IN      NS      dns3.nic.amazon.
amazon.      21600  IN      NS      dnsc.nic.amazon.
amazon.      21600  IN      NS      dnsc.nic.amazon.
amazon.      21600  IN      NS      dns4.nic.amazon.

;; Query time: 92 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Wed Apr 17 16:34:52 -03 2024
;; MSG SIZE rcvd: 191
```

- El servidor que respondió es autoritativo.
- La consulta se realizó de forma recursiva.
- El servidor acepta consultas recursivas.
- El servidor de DNS soporta consultas recursivas
- El servidor de DNS consultado es 8.8.8.8
- Se consultó por un registro NS.
- Se consultó por un registro A
- El dominio es un TLD.
- dnsb.nic. amazon es el servidor primario del dominio amazon
- dnsb.nic.amazon es un servidor primario del dominio amazon

Justificación:

RA, RD la falta de AA nos indican las 4 primeras, podemos ver el server 8.8.8.8 en el campo SERVER y NS en la QUERY SECTION, para saber cual es el servidor primario de un dominó consultamos por el SOA

Indique qué registros de DNS se pueden consultar para averiguar el servidor primario

- MX
- NS
- SOA
- TXT
- A

Qué información se encuentra en el mismo registro SOA

- La IP del mismo
- El nombre del servidor
- Un numero de serie
- El puerto de capa de transporte en el cual espera las peticiones

SMTP/DNS

Si el usuario ada@a.com envía un email a bob@b.org, el MTA de "a", qué registros de DNS deberá consultar el MTA local para contactar al MTA destino.

- NS
- SOA
- MX
- CNAME
- USER
- PTR
- A y/o AAAA
- SRV

Justificacion:

MX contiene el nombre canónico del servidor de correo con el cual luego podemos consultar por la IP (registro A/AAAA).

¿Cuáles de las siguientes consultas DNS debe realizar un MTA al enviar un correo electrónico del dominio usuario@dominiouno.com al dominio usuario@doniniodos.com?

- Consultar el registro MX del dominio dominiodos.com para encontrar el servidor de correo entrante (SMTP) del dominio receptor.
- Consultar el registro NS del dominio dominiodos.com para obtener el nombre del servidor de correo entrante.
- Consultar el registro TXT del dominio dominiodos.com para obtener información adicional sobre las políticas de recepción de correo y las claves de cifrado.
- Consultar el registro A y/o AAAA para obtener la dirección IP del servidor de correo del dominio dominiodos.com.
- Consultar el registro SOA del dominio dominiodos.com para obtener información sobre la autoridad del dominio y la administración de DNS.

- Consultar el registro CNAME del dominio dominiouno.com para obtener la dirección IP del servidor de correo saliente.

Si el usuario uno@domain.com envía un e-mail a dos@otrodomain.org, el local DNS/resolver del MTA de "uno", ¿qué servidores de DNS deberá consultar si no tiene cacheada la respuesta y necesita resolverla (indicar todos los servidores por los que deber' pasar)?

- Servidores del TLD com
- Servidores raíces
- Servidores del TLD org
- Servidores del dominio domain.com
- Servidores del dominio otrodomain.org
- Servidores del cc-TLD del país donde se encuentra el servidor MX del dominio domain.com
- Servidores del cc-TLD del país donde se encuentra el servidor MX del dominio otrodomain.org

Justificación:

La ruta es buscando desde la raíz pasando por todos los servidores DNS de la jerarquía (en este caso solo .org) y llegar al servidor del dominio.

Si el usuario uno@dom.com envía un email a dos@otrodom.org que servidor y registro de DNS deberá consulta el servidor SMTP local de correo saliente de la cuenta uno@dom.com

- Algun servidor del TLD org
- Algun servidor raíz
- Algun servidor local/servidor que tenga configurado

Justificación:

El servidor de correo saliente es cliente del servidor DNS, entonces como cliente el simplemente consulta al servidor local que luego resuelve la solicitud.

Siguiendo la anterior, consultará por los registros:

- MX
- A y/o AAAA
- SOA
- NS

HTTP

HTTP. Indicar afirmaciones verdaderas para el http/2 y http/3

- http/2 Usa conexiones persistentes por default.
- http/3 no usa conexiones TCP ya que trabaja sobre UDP.
- http/2 mayormente se Implementa sobre TLS, es decir funciona cifrado, aunque no es requisito del RFC.
- Ambos dividen la conexión en streams y pueden mandar parte de datos con diferentes prioridades.
- http/2 usa como protocolo de transporte TCP.
- Tanto http/2 como http/3 mejoran el rendimiento de HTTP sin cambiar semántica.

Observando las siguientes salidas, indique las opciones verdaderas

> GET /drive/search?q=redes HTTP/1.1

> Host: drive.google.com

>User-Agent: cur1/7.68.0

>Accept: */*

>

< HTTP/1.1 301 Moved Permanently

< Content-Type: application/binary

- El requerimiento tiene parámetros en la URL
- El user-agent puede procesar cualquier tipo de contenido
- El código 301 y 302 son códigos que indican redirecciones.
- La cabecera Host permite el uso de VirtualHost la cual es renombrada en http/2

Justificación:

Parametro q=redes, Accept */*, códigos 30x indican redirecciones (304 es not modified).

¿Cómo mejora la velocidad de carga de las páginas web el protocolo HTTP? Marque todas las opciones correctas

- HTTP utiliza caché web

- En HTTP/2 solamente a través de la caché web y recursos en caché. En HTTP/1.1, se logra debido a multiplexación, compresión de cabeceras y priorización de solicitudes
- En HTTP/2, introduce la multiplexación, compresión de cabeceras y priorización de solicitudes
- En HTTP/1.1, se acelera la velocidad de carga al minimizar el uso de caché web y cargar todos los recursos directamente desde el servidor. HTTP/2.0 mejora la velocidad al utilizar múltiples conexiones simultáneas para cada recurso

Justificación:

HTTP/2 introduce lo que dice ahí, pero no minimiza el uso de la caché (bajaría la velocidad de carga).

HTTP. Observando la siguiente salida. Marque todas las opciones correctas

›GET /recurso HTTP/1.1

›Host: www.ejemplo.com

›User-Agent: MiNavegador/1.0

›Accept: application/json

›HTTP/1.1 401 Unauthorized

›Date: Thu, 24 Aug 2023 15:30:00 GMT

›Server: Apache

›Www-Authenticate: Basic realm="Acceso Restringido"

›Content-Type: text/html; charset=UTF-8

La consulta fue exitosa y se obtuvo la información solicitada.

- La consulta tuvo un error de sintaxis en la URL.
- El recurso solicitado no se encontró en el servidor.
- El servidor requiere autenticación y el cliente no proporciona las credenciales adecuadas.
- La consulta fue bloqueada debido a una sobrecarga en el servidor.

¿Cuál es el método en HTTP que permite obtener el documento requerido y no espera recibir datos en body? Marque todas las opciones correctas

- POST
- GET
- PUT
- DELETE

Indicar qué características mejoran el rendimiento de HTTP (implementadas en diferentes versiones):

- Pipelining
- Conexiones persistentes
- Compresión de headers
- Uso de SSL
- Binary Framing
- Implementación de cookies

Justificación:

SSL e implementación de cookies no tiene que ver con el rendimiento.

Indicar que encabezados HTTP en el requerimiento se pueden usar para mejorar el caching

- If-modified-since
- E-tag
- If-none-match
- Last-modified
- Set-cookie

Cual es el método en HTTP/2 que permite obtener solo los encabezados del documento requerido

- PUT
- HEAD
- POST
- GET
- Ninguno de los anteriores es un método HTTP/2

Marque las opciones correctas para HTTP/2

- HTTP/2 resuelve HOL
- Como HTTP/1.1 y anteriores, HTTP/2 es un protocolo textual
- Cada stream necesita utilizar una nueva conexión TCP
- La mayoría de las implementaciones utilizan TLS/SSL, aunque el estándar no lo requiere
- El metodo TRACE y HEAD no estan soportados en HTTP/2
- Las streams pueden ser priorizados

EMAIL

E-MAIL. El header de un e-mail "To:" lo agrega

- MUA local.
- MTA Remoto.
- MTA local.

Justificación:

El MUA local agrega al email los campos del header, message-id, to, from, date, subject, sino lo agrega el MSA antes de dárselo al MTA.

Con que comando está relacionado el header "To"

- RCPT FROM.
- MAIL FROM.
- HELO.
- MAIL TO.
- RCPT TO.

Justificación:

Mail to, y rcpt from no existen, los otros están relacionados con otras cosas.

POP e IMAP. Indicar cuál de las siguientes afirmaciones es correcta

- POP3 e IMAP permiten correr de forma segura utilizando SSU/TLS
- POP3 permite acceso al mailbox sin autenticación
- El protocolo POP3 solo permite acceder a la carpeta INBOX del mailbox.
- IMAP permite gestionar carpetas del lado del servidor
- LIST, USER y PASS son comandos del protocolo POP3

¿Cuál es el rol principal del MTA (Mail Transport Agent) ? Marque todas las opciones correctas

- Entregar los correos electrónicos al buzón del destinatario.
- Permitir el acceso del usuario al buzón de correo electrónico.
- Transportar los correos electrónicos entre diferentes servidores de correo electrónico.
- Enviar correos electrónicos a través de una interfaz con el usuario.

Justificación:

Entregar los correos electrónicos al buzón del destinatario -> El MDA (mail delivery agent)

Permitir el acceso del usuario al buzón de correo electrónico -> MAA (mail access agent)

Enviar correos electrónicos a través de una interfaz con el usuario -> MUA (mail user agent)

En la arquitectura del correo electrónico, ¿cuales son los posibles protocolos utilizados por el MUA (Agente de Usuario de Correo) y el MTA (Agente de Transferencia de Correo) respectivamente?

- MUA: SMTP, MTA: IMAP
- MUA: POP3, MTA: SMTP
- MUA: HTTP, MTA: FTP
- MUA: IMAP, MTA: SMTP
- MUA: TCP, MTA: UDP

Justificación: El agente de transferencia solo puede usar SMTP/ESMTP, el MUA podría usar todos los protocolos de mail.

En relación a los protocolos de acceso al correo electrónico, indique cuáles de las siguientes afirmaciones son verdaderas.

- POP3 es un protocolo más eficiente que IMAP, ya que descarga los mensajes del servidor al dispositivo del usuario.
- IMAP es un protocolo más flexible que POP3, ya que permite el acceso a los mensajes desde múltiples dispositivos y la manipulación de mensajes en el servidor.
- POP3 permite la manipulación de mensajes en el servidor.
- Ambos protocolos requieren autenticación, pero IMAP utiliza el formato ASCII 7 bits en 8 NVT, mientras que POP3 utiliza el formato ASCII 8 bits
- Ambos protocolos utilizan el puerto TCP 143
- IMAP no es adecuado para la organización de mensajes en carpetas
- POP puede correr sobre SSL/TLS POP3S (995)
- IMAP permite la ejecución segura sobre SSL/TLS.

Justificación:

Ambos usan ASCII de 7 bits, POP usa puerto 110, y IMAP 143, ambos pueden usar SSL/TLS, más flexible es IMAP, pero no sabemos si eficiente.

Indicar características verdaderas de protocolo SMTP

- Usa conexiones persistentes.

- Siempre requiere autenticación.
- Usa como protocolo de transporte UDP.
- Usa por default el puerto 143 o el 110.
- Se utiliza para la comunicación entre MTAs.
- "MAIL FROM" es un comando del protocolo.

Justificación:

Puerto -> 25,487

Indicar qué ventajas tiene IMAP4 sobre POP3

- Permite autenticación.
- Permite enviar correos cifrados.
- Manejo de carpetas.
- POP3 requiere copiar los mensajes completos al MUA, IMAP es más flexible, permite manipular mensajes en el servidor.
- POP3 solo sirve con SMTP y no con ESMTP.

Indicar qué afirmación son verdaderas con respecto a servicios de correo

- POP3 no permite autenticación
- IMAP4 básico no envía al servidor los correos cifrados
- IMAP4 permite manejo de carpetas a diferencia de POP3
- ESMTP es un protocolo que extiende SMTP y permite funcionalidades extra como 8BitMime o TLS.

FTP

Marque las opciones correctas sobre FTP

- En el FTP pasivo, la conexión de datos la inicia el servidor desde el port 20
- En el FTP activo, la conexión de datos la inicia el servidor desde el port 20
- Un archivo descargado se obtiene a través del canal de control
- FTP utiliza un canal de datos y un canal de control

Justificación:

El archivo se pasa por el canal de datos. Uno a la vez y se cierra la conexión.

Indicar características verdaderas de FTP

- Usa 2 conexiones, una para control y otra para datos
- Los clientes FTP requieren interfaz gráfica
- Corre sobre UDP
- Es soportado por los navegadores utilizando la URI ftp://
- En el modo activo el que abre la conexión de datos es el cliente

Indicar las afirmaciones verdaderas de FTP

- Usa 2 conexiones, una para control y otra para datos
- Es un protocolo antiguo y casi en desuso
- Corre sobre UDP
- En el modo pasivo el que abre la conexión de datos es el cliente
- En el modo activo el que abre la conexión de datos es el cliente

CAPA DE APLICACION

¿Qué caracteriza a la arquitectura cliente-servidor en términos de distribución de tareas y responsabilidades?

- La arquitectura cliente-servidor distribuye todas las tareas de manera equitativa entre clientes y servidores.
- Los servidores realizan todas las tareas, y los clientes solo solicitan información.
- Los servidores gestionan recursos y servicios, mientras que los clientes solicitan y utilizan esos recursos.
- Los clientes realizan todas las tareas de procesamiento y cálculo, y los servidores almacenan datos.

SSL. Indicar características verdaderas de TLS

- Implementa autenticación del servidor.
- Sólo HTTP y POP3 usan TLS para asegurar las comunicaciones.
- Provee cifrado para garantizar confidencialidad de los datos.
- Como parte del handshake el servidor envía su certificado que contiene su clave privada.
- Los mensajes se cifran con la clave pública del servidor.
- La clave de sesión es un secreto compartido entre cliente y servidor (ambos la conocen).

Justificación:

El handshake involucra enviar un certificado que contiene la clave pública, que el cliente cree una clave de sesión, que se la pase al server, y que el server la desencrpte con su clave privada, para luego encriptar o desencrptar todos los mensajes con la de sesión.

Extra:

FTP: 20 (Control), 21 (Datos)

SMTP: 25/587

DNS: 53

HTTP: 80

POP3: 110

IMAP: 143

HTTPS: 443

Procesos Servidores: 0 al 1023