RESUMEN DE PARCIALES REDES -CAPA APLICACION				
Característica	**HTTP 1.0**	**HTTP 1.1**	**HTTP 2.0**	**HTTP 3.0**
Métodos Soportados	GET (en URL, no espera datos en body), POST, HEAD, PUT, DELETE, LINK, UNLINK	Incluye TRACE, HEAD, CONNECT	No cambia la semántica, mantiene los mismos métodos	Mantiene los métodos del HTTP 2.0
Multiplexación / Host Virtuales	Soporte básico, varios servicios en un mismo host	Mejorado con múltiples conexiones simultáneas para cada recurso	Uso de una sola conexión, con multiplexación a través de streams escritos en binario, con prioridades	Usa una sola conexión, basado en QUIC, mejor multiplexación
Conexión	TCP	TCP	Conexión persistente por defecto, sobre TCP (con o sin TLS)	QUIC (basado en UDP)
Semántica y Sintaxis	Sintaxis textual	Sintaxis textual	Sintaxis binaria (frames divididos en mensajes con diferentes prioridades y tipos: #data, #header, #push-promise)	Sintaxis binaria, igual que HTTP 2.0
Mejoras en rendimiento	Uso de caché web	Pipelining, conexiones persistentes, múltiples conexiones simultáneas	Multiplexación, compresión de headers, priorización de solicitudes, resolución de Head of Line (HOL) blocking	Mayor rendimiento y menor latencia gracias a QUIC
División en streams	No	No	Sí, cada conexión se divide en streams con diferentes prioridades	Igual que HTTP 2.0
Caché Web	Cacheo de recursos	Cacheo mejorado con If-Modified-Since & If-None-Match en solicitudes	Sigue mejorando con técnicas de compresión de headers, priorización y reutilización de conexiones persistentes	Igual que HTTP 2.0
Frames y mensajes	No	No	Los streams se dividen en mensajes que a su vez se dividen en frames (#data, #header, #push-promise)	Igual que HTTP 2.0
Soporte de TLS	No obligatorio	No obligatorio	Comúnmente implementado con TLS aunque no es un requisito	Incluye TLS integrado en QUIC

FTP

a. En el FTP pasivo, la conexión de datos la inicia el cliente desde el port <1023.
b. En el FTP activo, la conexión de datos la inicia el servidor desde el port 20.
c. Un archivo descargado se obtiene a través del canal de DATOS.
d. FTP utiliza un canal de datos y un canal de control (2 conexiones)
e. Los clientes FTP requieren NO interfaz gráfica
f. Corre sobre TCP
g. NO Es soportado por los navegadores utilizando la URI ftp://
h. Es un protocolo antiguo, en desuso
i. NO CONEXIONES PERSISTENTES, mantiene estado (si esta autenticado).
j. No es necesario autenticarse para su uso, puede ser incognito.

TLS SSL caracteristicas

a. Implementa autenticación del servidor.
b. HTTP,POP3,imap usan TLS para asegurar las comunicaciones.
c. Provee cifrado para garantizar confidencialidad de los datos.
d. Como parte del handshake el servidor da su certificado que contiene su clave PUBLICA.
e. Los mensajes se cifran con la clave de sesion,la cual es un secreto compartido entre cliente y servidor (ambos la conocen).

DNS

Iterativa: Al realizar una consulta como DNS local a un ROOTSERVER/TLD/AUTORITATIVO, por no tener cacheada la respuesta .
Recursiva: Cuándo se consulta al servidor DNS local y a un open DNS como 8.8.8.8.
SOA- nos da el servidor PRIMARIO (nos muestra NOMBRE y NRO SERIE).

EMAIL POP3/IMAP SMTP/DNS

3. SMTP/DNS. Si el usuario ada@a.com envía un e-mall a bob@b.org, el MTA de "a" deberá consultar.
   a- MX b- A y/o AAAA
5. Comandos EMAIL y las relaciones a los HEADER: MUA local - commandos:
   b. FROM - MAIL FROM. e. TO - RCPT TO. C.HELO b.QUIT D.DATA

8. EMAIL partes involucradas desde SALIDA a RECEPCION:
   MUA: Enviar correos electrónicos a través de una interfaz con el usuario.
   MSA: Procesa el mail del mua y lo deja en el MTA.
   MTA: Transportar los correos electrónicos entre diferentes servidores de correo electrónico.
   MDA/LDA: Entregar los correos electrónicos al buzón del destinatario.
   MAA (usa POP3/IMAP): AUTENTICA AL MUA, le permite el acceso al buzón de correo electrónico.

9. POP e IMAP.
   a. POP3 e IMAP permiten correr de forma segura utilizando SSL/TLS
   b. POP3 E IMAP NECESITA autenticación.
   C. El protocolo POP3 solo permite acceder a la carpeta INBOX del mailbox.
   d. IMAP permite gestionar carpetas del lado del servidor
   e. LIST, USER Y PASS son comandos del protocolo POP3
   a-POP3 descarga obligatoriamente los mensajes del servidor al dispositivo del usuario.
   b- IMAP permite el acceso a los mensajes desde múltiples dispositivos y la manipulación de mensajes en el servidor (en carpetas).
   c- POP3/IMAP protocolos requieren autenticación ASCII 7 bits en 8 NVT.

9. ¿cuáles son los posibles protocolos utilizados por el MUA y el MTA respectivamente? Marque todas las opciones correctas:
   MUA: POP3, MTA: SMTP :: MUA: IMAP, MTA: SMTP
5. E-MAIL. Indicar características verdaderas de protocolo SMTP
   a. Usa conexiones persistentes.
   b. NO requiere autenticación.
   c. Usa como protocolo de transporte TCP.
   d. Usa por default el puerto 25.
   e- Se utiliza para la comunicación entre MTAS.
   f- comando del protocolo: mail from, rcpt to, quit,helo, data
   g- ESMTP: extiende SMTP y puede usar 8bits MIME y TLS.

OTROS

1. Arquitectura cliente-servidor en términos de distribución de tareas y responsabilidades?
   a. PEER to PEER: La arquitectura distribuye las tareas de manera equitativa entre clientes y servidores.
   b. MAINFRAIM: Los servidores realizan todas las tareas, y los clientes solo solicitan información (DUMB CLIENT).
   c. cliente-servidor: Los servidores gestionan recursos y servicios, mientras que los clientes solicitan y utilizan esos recursos.

5. ¿Cuál es el propósito de la delegación de autoridad en una red? Selecciona todas las respuestas correctas.
   a-Facilitar la administración DISTRIBUIDA de la red.
   b- Reducir la carga de trabajo en servidores centrales.
   c- Permitir que los servidores locales tomen decisiones autónomas.
   NOTA- NO MEJORA LA SEGURIDAD EN LA RED.