Teoría 2025

Enero

Pregunta 1.

(a) Diferencias entre control de flujo y control de congestión. Mecanismos TCP usados para implementarlos (TCP)

- **Control de flujo:**
  - **Concepto:** Se encarga de evitar que el emisor abrume al receptor con más datos de los que éste puede procesar o almacenar.
  - **Mecanismo:**
    - **Ventana de recepción:** Cada receptor informa, en los ACK, cuántos bytes está dispuesto a recibir (campo "ventana").
    - El emisor limita la cantidad de datos "en vuelo" a la menor de la ventana de recepción anunciada y la ventana de congestión.
  - **Enfoque:** Se centra en la capacidad del receptor (fin a fin).
- **Control de congestión:**
  - **Concepto:** Previene que el emisor inunde la red (routers y enlaces) con demasiados datos, lo que causaría pérdida de paquetes y retrasos.
  - **Mecanismo en TCP:**
    - **Ventana de congestión (CWND):** El emisor ajusta dinámicamente esta ventana en función de la retroalimentación que le proporciona la red (por ejemplo, a través de la pérdida de paquetes o retrasos en los ACK).
    - Algoritmos como el **"inicio lento" (slow start)** y la **"prevención de congestión" (congestion avoidance)**, que modifican la CWND en función de los ACK recibidos y de la detección de pérdidas (timeouts o duplicados).
- **(b) Definición y diferencias entre inicio lento y prevención de congestión (TCP)**
- **Inicio lento (Slow Start):**
  - **Definición:** Es la fase inicial de la conexión TCP en la que la ventana de congestión se incrementa de forma exponencial (en cada RTT, se duplica el tamaño de la ventana) hasta alcanzar un umbral preestablecido, denominado **ssthresh**.
  - **Objetivo:** Rápida "sondeo" de la capacidad de la red al principio, sin sobrecargarla.
- **Prevención de congestión (Congestion Avoidance):**
  - **Definición:** Una vez que la ventana de congestión alcanza el umbral (ssthresh), el crecimiento pasa de exponencial a lineal. En cada RTT, la ventana se incrementa en aproximadamente 1 MSS (Maximum Segment Size).
  - **Objetivo:** Evitar incrementos bruscos que puedan saturar la red y provocar pérdidas.
  - **Diferencia clave:**
    - *Inicio lento* utiliza un crecimiento exponencial para explorar la red rápidamente.

- *Prevención de congestión* utiliza un crecimiento más moderado (lineal) para mantener la estabilidad y evitar congestión.

Pregunta 2.

Definición del proceso y agentes implicados en el envío de correo (Protocolos de correo)

El envío de correo electrónico involucra varios pasos y entidades (o agentes) que participan en el proceso:

1. **Agente de Usuario (MUA):**
   - Es el programa que utiliza el usuario para componer y leer el correo (por ejemplo, Outlook, Thunderbird).
   - **Proceso:** El usuario redacta el mensaje y lo envía a través del MUA.
2. **Agente de Transferencia de Correo (MTA):**
   - Se encarga de recibir el mensaje del MUA y de reenviarlo a través de la red hasta llegar al servidor del destinatario.
   - Utiliza el protocolo **SMTP (Simple Mail Transfer Protocol)** para enviar mensajes entre servidores de correo.
3. **Agente de Acceso a Correo (MDA):**
   - En algunos casos se incluye un agente de entrega (Mail Delivery Agent, MDA) que almacena el correo en el buzón del destinatario.
4. **Agente de Recuperación de Correo (MUA en el receptor o protocolos de acceso):**
   - El destinatario utiliza su cliente de correo para acceder al buzón.
   - Se utilizan protocolos como **POP3** o **IMAP** para recuperar o consultar los mensajes.

Proceso resumido:

- El MUA del remitente envía el mensaje mediante SMTP al MTA de salida.
- Este MTA reenvía el mensaje (posiblemente a través de varios MTA) hasta el servidor de correo del dominio del destinatario.
- El servidor almacena el mensaje y el MUA del destinatario, mediante POP3 o IMAP, lo descarga o lo consulta.

Pregunta 3.

Definición y diferencias de la resolución iterativa y recursiva (DNS)

- **Resolución recursiva:**
  - **Definición:** El cliente (o resolver local) envía una consulta DNS a un servidor recursivo, que se encarga de buscar la respuesta completa.
  - **Proceso:** El servidor recursivo consulta a otros servidores (servidores raíz, TLD, etc.) de manera secuencial hasta obtener la respuesta, la almacena en caché y se la devuelve al cliente.

- **Ventajas:** Simplifica la tarea del cliente (recibe la respuesta final sin gestionar múltiples pasos).
- **Desventaja:** Mayor carga para el servidor recursivo.

- **Resolución iterativa:**

  - **Definición:** El cliente consulta a un servidor DNS, que devuelve la mejor respuesta que tiene (generalmente la dirección de otro servidor que tiene información más específica).
  - **Proceso:** El cliente debe realizar sucesivas consultas a distintos servidores (por ejemplo, al servidor raíz, luego al TLD, etc.) hasta obtener la respuesta final.
  - **Ventajas:** Distribuye la carga entre varios servidores y puede ser más rápido en algunos escenarios si la caché está bien poblada.
  - **Desventaja:** El cliente debe gestionar múltiples pasos.

Teoría 2025: Febrero

En el examen de febrero 2025 **no se han facilitado los enunciados específicos** (se indican "?"). Por tanto, en este apartado se reconoce que no contamos con las preguntas detalladas. (Si en el examen se proporcionan en el momento, el alumno deberá estructurar la respuesta siguiendo la misma metodología: definición, explicación detallada, ejemplos y, en su caso, diagrama o tablas necesarias).

Teoría 2024

Enero

Pregunta 1.

Definición de congestión de red y dónde se origina (TCP)

- **Congestión de red:**
  - Es el fenómeno que ocurre cuando la demanda de recursos (ancho de banda, capacidad de procesamiento en routers, buffers) excede la capacidad disponible en la red.
  - **Origen:** Se produce principalmente en los routers, cuando los buffers se saturan por la llegada de demasiados paquetes en un corto periodo, lo que puede provocar la pérdida de paquetes y retrasos.
  - **Impacto en TCP:** TCP detecta la congestión (por ejemplo, mediante la pérdida de ACKs) y reduce su tasa de envío mediante algoritmos de control de congestión.

Pregunta 2.

Explicación de mensajes tras resolución DNS y autoridades de zonas DNS (DNS)

- **Proceso de resolución DNS (general):**

  1. **Consulta inicial:** Un cliente (por ejemplo, un navegador) envía una consulta al resolver local para obtener la dirección IP correspondiente a un nombre de dominio.
  2. **Consulta al servidor recursivo:** Si el resolver local no tiene la respuesta en su caché, envía la consulta a un servidor DNS recursivo.

3. **Consultas a servidores raíz y TLD:** El servidor recursivo interroga a los servidores raíz, que responden con la dirección del servidor responsable del dominio de nivel superior (TLD).
4. **Consulta a la autoridad de la zona:** Finalmente, el servidor recursivo consulta al servidor autorizado (la "autoridad de zona") para el dominio en cuestión y obtiene la respuesta definitiva (por ejemplo, un registro A para www.ejemplo.com).

- **Autoridad de zonas DNS:**
    - Un servidor con autoridad es aquel que contiene la copia oficial (la "zona") de un dominio determinado.
    - **Delegación:** La autoridad de una zona puede delegarse a otros servidores (servidores secundarios) para mejorar la disponibilidad y distribuir la carga.

Pregunta 3.

Justificar propiedades de seguridad en un mensaje (ciberseguridad)

Para garantizar la seguridad de un mensaje, se deben cubrir varios aspectos:

- **Confidencialidad:** Se asegura mediante el cifrado de los datos (por ejemplo, usando AES en cifrado simétrico o RSA en cifrado asimétrico) de forma que solo el receptor autorizado pueda leer el contenido.
- **Integridad:** Se verifica que el mensaje no ha sido alterado durante la transmisión. Esto se consigue usando funciones hash (MD5, SHA-256) y códigos de autenticación de mensajes (HMAC), de modo que el receptor pueda comparar el hash recibido con el recalculado.
- **Autenticación:** Se garantiza que el remitente es quien dice ser, normalmente mediante firmas digitales o protocolos de reto-respuesta que utilizan criptografía asimétrica.
- **No repudio:** Se procura que el emisor no pueda negar la autoría del mensaje. Esto se logra si se utiliza la firma digital (en la que el mensaje o su resumen se cifra con la clave privada del emisor), ya que, al poder ser verificado con la clave pública correspondiente, queda vinculada de forma única al emisor.

En conjunto, un mensaje seguro suele incluir cifrado para confidencialidad, un hash o HMAC para integridad, y una firma digital (junto con certificados) para autenticación y no repudio.

Febrero

Pregunta 1.

Diferencias entre protocolos HTTP y IMAP (Protocolos de correo)

- **HTTP:**
    - Es un protocolo de transferencia de hipertexto utilizado principalmente para la comunicación entre navegadores y servidores web.
    - Es **stateless** (sin estado), aunque HTTP/1.1 puede mantener conexiones persistentes para transmitir múltiples objetos en una sola conexión.
    - Opera sobre TCP, utiliza métodos como GET, POST, HEAD, etc.
    - Se usa en la web para descargar documentos, imágenes, vídeos, etc.

- **IMAP (Internet Message Access Protocol):**
    - Es un protocolo utilizado para acceder y gestionar correos electrónicos directamente en el servidor.
    - Permite la organización en carpetas y la sincronización entre múltiples dispositivos.
    - Es **stateful** en el sentido de que mantiene el estado (por ejemplo, qué mensajes han sido leídos) en el servidor.
    - Opera sobre TCP y normalmente utiliza el puerto 143 (o 993 para IMAP sobre SSL).
- **Diferencias clave:**
    - **Finalidad:** HTTP se centra en la transferencia de documentos web, mientras que IMAP se especializa en el acceso y gestión de correo.
    - **Estado:** HTTP es sin estado (aunque con persistencia de conexión), mientras que IMAP mantiene estado sobre el servidor.
    - **Interacción:** HTTP se basa en solicitudes-respuestas simples para cada recurso; IMAP permite interacciones más complejas (búsqueda, organización, marcación de mensajes).

Pregunta 2.

Definición de control de errores TCP, parámetro fundamental (timeout) y adaptación en conexión (TCP)

- **Control de errores en TCP:**
    - TCP utiliza mecanismos de confirmación (ACKs) y retransmisión para garantizar la entrega fiable de los datos.
    - Cada segmento enviado se asocia a un temporizador; si no se recibe el ACK correspondiente antes de que expire el timeout, el segmento se retransmite.
- **Parámetro fundamental: Timeout**
    - **Timeout:** Es el tiempo que espera el emisor por un ACK antes de retransmitir el segmento.
    - Se calcula de forma dinámica basándose en una estimación del RTT (Round Trip Time) usando fórmulas de promedio móvil (por ejemplo, el algoritmo de Karn), y se ajusta en función de las variaciones observadas.
    - Si un segmento expira, TCP reduce la ventana de congestión (en Tahoe, se reinicia a 1 MSS) y duplica el timeout para evitar retransmisiones repetidas innecesarias.
- **Adaptación en conexión:**
    - La combinación de control de errores, control de flujo y control de congestión permite que TCP se adapte a las condiciones de la red, incrementando o reduciendo la tasa de transmisión según la calidad del enlace.

Pregunta 3.

Procedimiento autenticación en un intercambio de mensajes y definiciones varias (ciberseguridad)

Para autenticar un intercambio de mensajes entre dos entidades (por ejemplo, A y B) se sigue un procedimiento que normalmente involucra:

- **Intercambio de certificados digitales:**
  - Cada entidad posee un certificado digital emitido por una Autoridad Certificadora (AC) que vincula su identidad a su clave pública.
- **Proceso de autenticación (por ejemplo, usando firma digital):**
  1. **Generación del resumen:** La entidad emisora calcula el hash (usando MD5, SHA-256, etc.) del mensaje.
  2. **Firma digital:** El resumen se cifra con la clave privada del emisor (KPRI) para crear la firma digital.
  3. **Envío:** Se envía el mensaje junto con la firma digital y, habitualmente, el certificado digital.
  4. **Verificación:** El receptor utiliza la clave pública contenida en el certificado para descifrar la firma y obtener el resumen original. Luego, calcula el hash del mensaje recibido y lo compara con el resumen descifrado.
- **Definiciones clave:**
  - **Certificado digital:** Es un documento electrónico que asocia la identidad de una entidad con su clave pública, firmado por una AC de confianza.
  - **Firma digital:** Proporciona autenticación (garantiza que el mensaje fue enviado por quien afirma enviarlo) e integridad (cualquier alteración en el mensaje invalidaría la firma).
- **Posibles protocolos y mecanismos:**
  - Se pueden usar protocolos basados en TLS, o sistemas de correo seguro (PGP, S/MIME) que incorporan estas técnicas.

Teoría 2023

Enero

Pregunta 1.

Definición de NAT y procedimiento en un caso (NAT)

- **Definición de NAT (Network Address Translation):**
  - Es un mecanismo mediante el cual un router modifica las direcciones IP de origen o destino en los paquetes que atraviesan una red.
  - Se utiliza habitualmente para permitir que dispositivos con direcciones privadas (no ruteables en Internet) se comuniquen utilizando una o varias direcciones públicas.
- **Procedimiento en un caso típico (por ejemplo, salida a Internet):**
  1. **Cliente interno:** Un host con IP privada (p. ej., 10.0.0.3) envía un paquete al exterior (destino en Internet).
  2. **Router NAT:** Al recibir el paquete, el router NAT consulta su tabla de traducciones; como es la primera vez, asigna una dirección IP pública (por ejemplo, 24.1.70.210) y, para evitar ambigüedad en los puertos, modifica el puerto de origen (por ejemplo, de 1049 a otro valor disponible).
  3. **Envío a Internet:** El paquete modificado sale con la dirección pública de origen y, cuando la respuesta regresa, el router NAT utiliza su tabla para reescribir el paquete con la IP y puerto originales del host interno.
- **Aspectos importantes:**

- NAT traduce tanto direcciones como números de puerto (PAT – Port Address Translation).
- Garantiza que múltiples hosts internos puedan compartir una única dirección pública.

Pregunta 2.

Definición de cifrado asimétrico (Ciberseguridad)

- **Cifrado asimétrico:**
  - Utiliza un par de claves: una clave pública (que puede distribuirse abiertamente) y una clave privada (que se mantiene en secreto).
  - **Proceso:**
    - Para cifrar, se utiliza la clave pública del receptor; sólo quien posee la clave privada correspondiente puede descifrar el mensaje.
    - Para firmar digitalmente, el remitente cifra un resumen (hash) del mensaje con su propia clave privada; cualquier receptor puede verificar la firma usando la clave pública del remitente.
  - **Ventajas:** Facilita el intercambio seguro de información sin necesidad de compartir una clave secreta previamente.

Pregunta 3.

Explicación Tt, Tp, Tamaño Cw en el emisor para evitar interrupciones (TCP)

- **Tt (Tiempo de transmisión):**
  - Es el tiempo necesario para "poner" en el medio todos los bits de un segmento. Se calcula como
    $$ T_t = \frac{\text{Tamaño del segmento (bits)}}{\text{Velocidad de transmisión (bps)}} $$
- **Tp (Tiempo de propagación):**
  - Es el tiempo que tarda un bit en viajar desde el emisor hasta el receptor a través del medio. Se calcula como
    $$ T_p = \frac{\text{Distancia}}{\text{Velocidad de propagación}} $$
- **Tamaño de la ventana de congestión (CW):**
  - Es la cantidad de datos (en bytes o segmentos) que el emisor puede tener "en vuelo" antes de recibir un ACK.
  - Para evitar interrupciones (es decir, momentos en que el emisor se quede sin datos para enviar mientras espera ACKs), la cantidad de datos en vuelo (CW) debe ser al menos igual al **Bandwidth-Delay Product (BDP)**, que es:
    $$ \text{BDP} = \text{Velocidad de transmisión} \times \text{RTT} $$
  - Donde el RTT incluye 2·Tp y el tiempo de transmisión de los segmentos.
- **Objetivo:**
  - Que el tiempo de ida y vuelta (RTT) sea menor o igual al tiempo que tarda en transmitir la cantidad de datos definida por CW. Así, el emisor puede enviar continuamente sin esperar por ACKs.

Febrero

Pregunta 1.

Definición y uso de las máscaras de red (Máscaras)

- **Definición:**
    - Una máscara de red es un patrón de bits que, junto con una dirección IP, se utiliza para determinar qué parte de la dirección corresponde al identificador de la red y qué parte al identificador del host.
- **Uso:**
    - Permite dividir una red IP en subredes más pequeñas (subnetting) y asignar direcciones de forma eficiente.
    - Ayuda a agrupar dispositivos en redes lógicas y facilita el encaminamiento, ya que los routers pueden usar el prefijo de la dirección para decidir la ruta.
- **Ejemplo:**
    - La dirección IP 192.168.1.100 con máscara 255.255.255.0 (o /24) significa que los primeros 24 bits identifican la red y los últimos 8 bits identifican el host.
    - Con una máscara /27, la red tendría 32 direcciones, de las cuales 30 pueden asignarse a hosts (ya que se reservan la dirección de red y la de difusión).

Pregunta 2.

Procedimiento y mensajes de una firma digital usando BB (Big Brother) (Ciberseguridad)

- **Procedimiento de firma digital con doble cifrado "con Big Brother":**
    1. **Preparación y claves:**
        - Cada entidad (por ejemplo, A y B) dispone de su par de claves (clave pública y clave privada).
        - Existe una entidad de confianza (BB) que comparte claves secretas con cada parte ($K_(A–BB_)$ y $K_(B–BB_)$).
    2. **Proceso de firma:**
        - **Autenticación y no repudio:**
            - A cifra un resumen (hash) del mensaje (T) con su clave privada ($KPRI_(A_)$) para generar la firma digital.
        - **Incorporación de BB:**
            - A envía a BB (o a B, si BB interviene de forma transparente) el mensaje firmado, y BB verifica la autenticidad utilizando la clave secreta compartida.
            - BB puede incluir una marca o sello adicional (por ejemplo, cifrado con $K_(A–BB_)$) que respalde la identidad de A.
    3. **Mensajes intercambiados:**
        - A → B: (\text{Firma} = KPRI_A(\text{Hash}(T))) y el mensaje (T), junto con su certificado (opcionalmente).
        - BB (si interviene) añade su sello para garantizar la integridad de la relación.

4. **Verificación:**
    - B usa el certificado de A (emitido por una AC de confianza) para obtener la clave pública de A y verifica la firma.
    - La intervención de BB añade un nivel de confianza extra al validar la correspondencia entre la identidad y la clave.

- **Requisitos:**
    - Que la entidad BB sea de confianza (por ejemplo, mediante un certificado digital de una AC).
    - Que se incluya un hash del mensaje para asegurar la integridad.
    - Las claves deben cumplir los estándares de longitud y seguridad (por ejemplo, RSA de 2048 bits o superior).

Pregunta 3.

Explicación de envío de correo y agentes implicados (Protocolos de correo)

- **Proceso completo en el envío de correo:**

1. **Agente de Usuario (MUA):**
    - El usuario redacta el mensaje en su cliente de correo (MUA).
    - El MUA envía el mensaje al servidor de correo saliente.
2. **Agente de Transferencia de Correo (MTA):**
    - El MTA del remitente recibe el mensaje y, mediante SMTP, lo reenvía a otros servidores (otros MTA) hasta alcanzar el MTA del dominio del destinatario.
3. **Resolución DNS:**
    - Durante este proceso, el MTA remitente realiza una consulta DNS para obtener el registro MX del dominio del destinatario.
4. **Almacenamiento y entrega:**
    - El MTA del destinatario almacena el correo en el buzón asociado.
    - Cuando el destinatario consulta su correo (usando POP3 o IMAP), su cliente (MUA) se conecta al servidor y descarga o consulta el mensaje.
5. **Agentes involucrados:**
    - **MUA:** Programa de correo en el ordenador del usuario.
    - **MTA:** Servidor de correo que transfiere el mensaje entre dominios.
    - **MDA (Mail Delivery Agent):** A veces se distingue, responsable de entregar el mensaje al buzón.
    - **Servidor DNS:** Resuelve los nombres de dominio (por ejemplo, el registro MX) para facilitar la entrega.

- **Resumen:** El envío de correo implica la interacción entre el MUA del remitente, el MTA remitente, el MTA del destinatario y el MUA del destinatario; junto con consultas DNS para resolver nombres de dominio y obtener registros MX.

Teoría 2022

Enero

Pregunta 1.

Definición de encaminamiento dinámico y protocolos del mismo (Routing)

- **Encaminamiento dinámico:**
    - Es el proceso por el cual los routers intercambian información de sus tablas de rutas de forma automática para determinar el mejor camino hacia un destino.
    - A diferencia del encaminamiento estático (configurado manualmente), los protocolos dinámicos permiten que la red se adapte a cambios (como fallos o congestión).
- **Protocolos de encaminamiento:**
    - **RIP (Routing Information Protocol):**
        - Utiliza el algoritmo vector-distancia y la métrica del número de saltos.
        - Envía actualizaciones periódicas (cada 30 segundos).
    - **OSPF (Open Shortest Path First):**
        - Basado en el estado de enlace y el algoritmo de Dijkstra para calcular la ruta de menor costo (usualmente el inverso de la velocidad del enlace).
        - Permite dividir la red en áreas para mejorar la escalabilidad y tiene una convergencia más rápida que RIP.

Pregunta 2.

Explicar cómo se determina el time-out en TCP (TCP)

- **Determinación del time-out en TCP:**
    - Se estima el **Round Trip Time (RTT)** midiendo el tiempo desde que se envía un segmento hasta que se recibe el ACK correspondiente.
    - Se calcula un **RTT estimado** mediante un promedio ponderado (usando un factor alfa) de los RTT medidos.
    - Se calcula además una **desviación** para reflejar la variabilidad del RTT.
    - Finalmente, el **time-out** se establece como: [\text{Time-out} = \text{RTT estimado} + 4 \times (\text{Desviación})]
    - Además, si se produce un time-out, el algoritmo de Karn indica que el time-out no se actualice con ACKs ambiguos, y se suele duplicar el valor para evitar retransmisiones innecesarias.

Pregunta 3.

Definición de certificado digital (Ciberseguridad)

- **Certificado digital:**
    - Es un documento electrónico que vincula de forma fehaciente la identidad de una entidad (persona, empresa, dispositivo) con su clave pública.
    - **Contenidos:**
        - Identidad del titular (nombre, organización, etc.).
        - Clave pública del titular.
        - Datos de validez (fechas de emisión y expiración).
        - Información de la Autoridad de Certificación (AC) que lo emitió, incluida su firma digital.

- **Función:**
  - Permite a terceros confiar en que la clave pública corresponde a la entidad indicada, siendo fundamental para la autenticación, el cifrado y el no repudio en comunicaciones seguras.

Febrero

Pregunta 1.

Envío de correo electrónico y agentes implicados (Protocolos de correo)

- **Proceso de envío de correo:**
  1. **MUA del remitente:** Redacta y envía el correo.
  2. **MTA remitente:** Recibe el mensaje y lo envía a través de SMTP al MTA del dominio del destinatario.
     - Durante este proceso se realizan consultas DNS para resolver el registro MX del destinatario.
  3. **MTA destinatario:** Recibe el mensaje y lo almacena en el buzón del destinatario (MDA).
  4. **MUA del destinatario:** Se conecta al servidor (usando POP3 o IMAP) para descargar o consultar el mensaje.
- **Agentes implicados:**
  - Cliente de correo (MUA), Servidor de correo (MTA/MDA) y Servidores DNS para resolución de nombres.

Pregunta 2.

Explicación de los números de secuencia en la capa de transporte (TCP)

- **Números de secuencia en TCP:**
  - Cada byte de datos en una conexión TCP se asigna un número de secuencia.
  - El campo de **número de secuencia** en la cabecera TCP indica el número del primer byte en el segmento.
  - Los números de secuencia permiten:
    - **Reensamblar** los segmentos en el orden correcto.
    - **Detectar pérdidas:** Si hay un "hueco" en la secuencia, el receptor sabe que faltan datos.
  - Se inicializan en la fase de establecimiento de conexión mediante el ISN (Initial Sequence Number), que se selecciona de forma pseudoaleatoria y se incrementa con el número de bytes enviados.

Pregunta 3.

Explicación del doble cifrado y qué servicios proporciona (ciberseguridad)

- **Doble cifrado (ejemplo de firma digital "doble cifrado"):**
  - **Paso 1:** El remitente (A) cifra el mensaje (T) con su clave privada (KPRI(_A)); esto genera una firma digital que garantiza la **autenticidad** y **no repudio**, ya que solo A posee la clave privada.
  - **Paso 2:** Para garantizar la **confidencialidad**, A cifra el mensaje (T) (o una clave secreta que se usará para cifrar (T)) con la clave pública del receptor (KPUB(_B)).

- **Servicios que proporciona:**
  - **Autenticación:** El receptor puede verificar que el mensaje proviene realmente de A, usando la clave pública de A.
  - **Integridad:** Si el receptor recalcula el hash del mensaje y lo compara con el firmado, se asegura de que el contenido no ha sido alterado.
  - **Confidencialidad:** Al cifrar con la clave pública del receptor, solo B (que posee la clave privada correspondiente) puede descifrar el mensaje.
  - **No repudio:** Una vez que el mensaje está firmado digitalmente, A no puede negar haberlo enviado, siempre que se garantice la asociación fehaciente mediante certificados digitales.

Teoría 2022

Enero

Pregunta 1.

Definición de encaminamiento dinámico y protocolos del mismo (Routing)

(Ver respuesta en Teoría 2022: Enero en Teoría 2022, ya explicado anteriormente)

- El encaminamiento dinámico implica que los routers intercambian información para actualizar automáticamente sus tablas de rutas.
- Protocolos típicos: RIP (vector-distancia) y OSPF (estado de enlace).

Pregunta 2.

Explicar cómo se determina el time-out en TCP (TCP)

(Ver respuesta en Teoría 2022: Febrero, Pregunta 2 en Teoría 2022)

- Se calcula a partir del RTT estimado y la desviación, según la fórmula:
  [\text{Timeout} = \text{RTT estimado} + 4 \times (\text{Desviación})]
- Se utiliza el algoritmo de Karn para evitar ambigüedades en retransmisiones.

Pregunta 3.

Definición de certificado digital (Ciberseguridad)

(Ver respuesta en Teoría 2022: Enero, Pregunta 3 en Teoría 2022)

- Un certificado digital asocia una identidad con una clave pública y es firmado por una AC de confianza; garantiza autenticidad y sirve para la verificación de firmas digitales.

Febrero

Pregunta 1.

Envío de correo electrónico y agentes implicados (Protocolos de correo)

(Ver respuesta en Teoría 2022: Febrero, Pregunta 1)

- Se repite el proceso: MUA remitente → MTA remitente (SMTP) → MTA destinatario → MUA destinatario (POP3/IMAP).
- Se realizan consultas DNS para resolución MX.

Pregunta 2.

Explicación de los números de secuencia en la capa de transporte (TCP)

(Ver respuesta en Teoría 2023: Febrero, Pregunta 2)

- Cada byte se numera; el número de secuencia facilita el reordenamiento y la detección de pérdidas. Se inicializa con un ISN y se incrementa según el tamaño de los datos enviados.

Pregunta 3.

Explicación del doble cifrado y qué servicios proporciona (ciberseguridad)

(Ver respuesta en Teoría 2023: Febrero, Pregunta 3)

- Mediante doble cifrado se garantiza confidencialidad (cifrado con la clave pública del receptor) y autenticación/no repudio (firma digital mediante la clave privada del emisor).
- Se añade integridad mediante un hash (por ejemplo, MD5 o SHA-256).

Teoría 2018

Enero

Pregunta 1.

Diferencias entre control de congestión y control de flujo (TCP)

- **Control de flujo:**
    - Se centra en evitar que el receptor se vea abrumado con datos; utiliza la ventana de recepción anunciada en los ACK.
- **Control de congestión:**
    - Se ocupa de evitar la saturación de la red (routers y enlaces) mediante la limitación de la cantidad de datos “en vuelo” (ventana de congestión).
    - Utiliza mecanismos de inicio lento y algoritmos de prevención/recuperación ante congestión.

Pregunta 2.

Explicar los niveles del modelo OSI (Modelo OSI)

- **Modelo OSI de 7 capas:**
    1. **Física:** Transmisión de bits a través de medios físicos.
    2. **Enlace de datos:** Encapsulación en tramas, detección y corrección de errores a nivel local.

3. **Red:** Encaminamiento y direccionamiento (por ejemplo, IP).
4. **Transporte:** Comunicación end-to-end, segmentación, control de errores y flujo (TCP/UDP).
5. **Sesión:** Establecimiento, gestión y terminación de sesiones de comunicación.
6. **Presentación:** Formateo y traducción de datos (codificación, cifrado).
7. **Aplicación:** Servicios de red para las aplicaciones (HTTP, FTP, SMTP, etc.).

Pregunta 3.

Enviar mensaje de A a B usando DNS (DNS)

- **Procedimiento resumido:**
  1. El host A que desea enviar un mensaje consulta a un servidor DNS (resolver) para obtener la dirección IP del host B.
  2. Se envía una consulta DNS; si es iterativa, el resolver va preguntando a los servidores raíz, TLD y finalmente al servidor autoritativo de B.
  3. Una vez resuelta la IP, A utiliza esa dirección para enviar el mensaje.
  4. Se puede incluir un diagrama en el que se muestre la cadena: A → Resolver → Servidor raíz → Servidor TLD → Servidor autoritativo → Resolver → A.

(Esta pregunta suele incluir el dibujo de la cadena de resolución, que se espera se dibuje en el examen.)

Febrero

Pregunta 1.

Definir y diferencias protocolos POP3 e IMAP (Protocolos de correo)

- **POP3 (Post Office Protocol 3):**
  - Descarga el correo del servidor a un solo cliente (generalmente eliminando el mensaje del servidor).
  - Es adecuado para usuarios que usan un único dispositivo y no necesitan sincronización.
- **IMAP (Internet Message Access Protocol):**
  - Permite la gestión de mensajes directamente en el servidor, manteniendo el estado (leído/no leído, carpetas).
  - Es ideal para usuarios que acceden a su correo desde múltiples dispositivos.
- **Diferencias clave:**
  - **POP3:** Menor uso de almacenamiento en el servidor; limitado en funcionalidad.
  - **IMAP:** Ofrece mayor flexibilidad, sincronización y organización de mensajes.

Pregunta 2.

Conexión con servidor usando DNS y ARP (DNS)

- **Proceso cuando un host quiere conectarse a un servidor:**

1. **Resolución DNS:**
    - El host envía una consulta DNS para resolver el nombre del servidor (por ejemplo, www.servidor.com).
    - El resolver recursivo o iterativo obtiene la dirección IP (por ejemplo, 150.214.204.25).
2. **Resolución ARP:**
    - Si el host se encuentra en la misma LAN que el servidor o el router de salida, se utiliza ARP para determinar la dirección MAC asociada a la IP destino.
    - El host envía una solicitud ARP y recibe una respuesta con la dirección MAC correspondiente.
3. **Conexión:**
    - Con la dirección IP y la MAC obtenidas, el host puede establecer la conexión (por ejemplo, mediante TCP) para enviar y recibir datos.

(Se recomienda ilustrar el proceso con un diagrama simple: Host → DNS Query → Respuesta DNS → ARP Request → ARP Reply → Conexión TCP.)

Pregunta 1.

¿Cuáles son las diferencias entre cifrado simétrico y cifrado asimétrico? Explique sus características, ventajas y casos de uso.

Respuesta:

- **Cifrado Simétrico:**
    - **Características:**
        - Utiliza una única clave para el cifrado y el descifrado (K = K').
        - Es generalmente más rápido y requiere menos recursos computacionales.
    - **Ventajas:**
        - Eficiente para cifrar grandes volúmenes de datos.
        - Bajo consumo computacional.
    - **Desventajas:**
        - El intercambio seguro de la clave es un problema, ya que ambas partes deben conocerla de forma secreta.
    - **Casos de uso:**
        - Cifrado de datos en tiempo real (por ejemplo, AES para proteger la información en disco o comunicaciones internas).
        - Utilizado en combinación con cifrado asimétrico en protocolos híbridos (por ejemplo, TLS: el cifrado asimétrico se usa para intercambiar una clave simétrica).
- **Cifrado Asimétrico:**
    - **Características:**
        - Utiliza un par de claves: una pública (K_pub) y una privada (K_priv).
        - La clave pública se distribuye libremente; la privada se mantiene en secreto.
    - **Ventajas:**
        - Facilita el intercambio seguro de claves, ya que no es necesario compartir la clave privada.

        - Permite la firma digital, ya que el remitente puede firmar con su clave privada y cualquier receptor verifica con la clave pública.
    - **Desventajas:**
        - Es más lento y requiere mayor capacidad computacional.
        - Generalmente se usa para cifrar volúmenes pequeños de datos (como claves o resúmenes).
    - **Casos de uso:**
        - Intercambio de claves (por ejemplo, en el establecimiento de sesiones seguras).
        - Autenticación y firma digital (por ejemplo, RSA para firmar certificados y mensajes).

Pregunta 2.

Explique el proceso de firma digital. ¿Qué servicios de seguridad proporciona y cuáles son los elementos que debe contener un certificado digital?

Respuesta:

- **Proceso de Firma Digital:**

    1. **Generación del Resumen:**
        - El emisor calcula un hash (resumen criptográfico) del mensaje usando una función hash segura (por ejemplo, SHA-256).
    2. **Firma:**
        - El emisor cifra el resumen con su clave privada, generando la firma digital.
    3. **Envío:**
        - Se envía el mensaje junto con la firma digital. En muchas implementaciones, se adjunta también el certificado digital del emisor.
    4. **Verificación:**
        - El receptor utiliza la clave pública (obtenida del certificado digital) para descifrar la firma y recuperar el resumen.
        - Calcula el hash del mensaje recibido y lo compara con el resumen obtenido de la firma. Si coinciden, la integridad y la autenticidad están garantizadas.

- **Servicios de Seguridad Proporcionados:**

    - **Autenticación:** Garantiza que el mensaje fue firmado por el poseedor de la clave privada (la identidad del emisor).
    - **Integridad:** Cualquier alteración en el mensaje hará que los hash no coincidan.
    - **No repudio:** El emisor no podrá negar haber enviado el mensaje, ya que solo él posee su clave privada.

- **Elementos que debe contener un Certificado Digital:**

    - **Identidad del titular:** Nombre, organización y otros datos identificativos.
    - **Clave pública del titular:** La que se utilizará para verificar las firmas.
    - **Datos de validez:** Fechas de emisión y expiración.
    - **Información de la Autoridad de Certificación (AC):** Nombre de la AC y la firma digital de la misma, que garantiza la veracidad de la asociación entre identidad y clave pública.
    - **Número de serie y otros identificadores:** Para identificar de manera única el certificado.

Pregunta 3.

Describa el proceso de intercambio Diffie-Hellman. ¿Cómo permite establecer una clave secreta en un canal no seguro? Mencione sus vulnerabilidades y cómo se pueden mitigar.

Respuesta:

- **Proceso de Intercambio Diffie-Hellman:**

    1. **Parámetros Públicos:**
        - Se eligen dos números públicos: un primo grande (n) y una base (g) (generador).
    2. **Elección de Valores Privados:**
        - Cada parte (A y B) elige un número secreto (a) y (b) respectivamente.
    3. **Cálculo de Valores Intermedios:**
        - A calcula (A = g^a \mod n) y B calcula (B = g^b \mod n).
        - Estos valores (A) y (B) se intercambian entre A y B.
    4. **Cálculo de la Clave Secreta:**
        - A calcula (K = B^a \mod n) y B calcula (K = A^b \mod n).
        - Ambos obtienen la misma clave secreta (K = g^{ab} \mod n).

- **Establecimiento de la Clave en un Canal No Seguro:**

    - Aunque los valores intermedios (A) y (B) se transmiten de forma pública, el valor (a) o (b) no se revelan, de modo que un atacante no puede calcular (K) sin resolver el problema del logaritmo discreto, considerado computacionalmente difícil.

- **Vulnerabilidades:**

    - **Ataque "Man-in-the-Middle":**
        - Un atacante puede interceptar y modificar los valores (A) y (B), estableciendo claves separadas con cada parte sin que estas se den cuenta.

- **Mitigaciones:**

    - **Autenticación Previa:**
        - Utilizar certificados digitales o un mecanismo de autenticación mutua para garantizar que las partes con las que se intercambian los valores son las legítimas.
    - **Integración en Protocolos Seguros:**
        - Emplear Diffie-Hellman como parte de un protocolo seguro (por ejemplo, TLS), donde la autenticación del servidor (y opcionalmente del cliente) impide ataques de intermediarios.

Pregunta 4.

¿Qué es una función hash criptográfica? Explique sus propiedades esenciales y cómo se utiliza en HMAC para garantizar integridad y autenticidad.

Respuesta:

- **Función Hash Criptográfica:**

    - Es un algoritmo que toma como entrada un mensaje de longitud variable y produce una salida (hash) de longitud fija.

- **Propiedades Esenciales:**

    - **Determinística:** El mismo mensaje siempre produce el mismo hash.
    - **Eficiente:** El cálculo del hash es rápido.
    - **Unidireccional:** Es computacionalmente inviable obtener el mensaje original a partir del hash.
    - **Resistencia a colisiones:** Es difícil encontrar dos mensajes distintos que produzcan el mismo hash.
    - **Sensibilidad al cambio:** Un pequeño cambio en el mensaje produce un hash completamente distinto.

- **Uso en HMAC (Hash-based Message Authentication Code):**

    - **Objetivo:** Garantizar la integridad y la autenticidad de un mensaje usando una función hash combinada con una clave secreta.
    - **Procedimiento:**
        1. Se toma una clave secreta (K) y se la concatena de forma específica con el mensaje (M).
        2. Se aplica la función hash a esta combinación para obtener un código de autenticación (HMAC).
    - **Servicios Proporcionados:**
        - **Integridad:** Si el mensaje se modifica, el HMAC recalculado en el receptor no coincidirá con el HMAC enviado.
        - **Autenticación:** Sólo quienes poseen la clave secreta pueden generar un HMAC válido, garantizando que el mensaje proviene de la fuente legítima.

- **Ejemplo:**

    - Utilizar HMAC-SHA256, donde se calcula:
      [\text{HMAC}(K, M) = H\left((K \oplus \text{opad}) \parallel H((K \oplus \text{ipad}) \parallel M)\right)]
    - (\oplus) denota la operación XOR, y (\text{opad}) e (\text{ipad}) son constantes definidas por el estándar.

Pregunta 5.

Explique qué es un ataque "Man in the Middle" (MitM) y describa al menos dos técnicas o mecanismos que se emplean para prevenirlo en comunicaciones seguras.

Respuesta:

- **Definición del Ataque MitM:**

    - Un ataque "Man in the Middle" consiste en que un atacante intercepta, altera o inyecta mensajes entre dos partes que se comunican, sin que éstas lo detecten. El atacante se sitúa entre el emisor y el receptor, pudiendo leer o modificar la información en tránsito.

- **Técnicas para Prevenirlo:**

1. **Uso de TLS/SSL con Certificados Digitales:**
    - **Autenticación del Servidor:** Durante el handshake TLS, el servidor presenta un certificado digital emitido por una Autoridad de Certificación (CA). El cliente verifica la autenticidad del certificado (por ejemplo, comprobando la firma digital y la cadena de confianza), lo que garantiza que se está comunicando con el servidor legítimo.
    - **Intercambio Seguro de Claves:** Se utiliza un intercambio de claves (RSA o Diffie-Hellman autenticado) para establecer una clave de sesión secreta. Esto impide que un atacante, aun interceptando los mensajes, pueda descifrar la comunicación sin conocer la clave privada correspondiente.
2. **Autenticación Mutua (Mutual TLS):**
    - **Certificados para Ambos Extremos:** No sólo el servidor se autentica, sino que el cliente también presenta su certificado digital. Esto asegura que ambas partes son quienes dicen ser y dificulta la intervención de un intermediario.
    - **Verificación Bidireccional:** Cada parte verifica la identidad de la otra usando la clave pública contenida en el certificado, lo que reduce la posibilidad de que un atacante se haga pasar por cualquiera de los dos.

- **Conclusión:**
  Al implementar TLS/SSL con autenticación (idealmente mutua) y validar correctamente los certificados digitales, se reduce significativamente la posibilidad de un ataque MitM, ya que un atacante no podrá falsificar certificados válidos ni interceptar el intercambio de claves de forma que pueda descifrar la comunicación.

Pregunta 6.

¿Qué es una Infraestructura de Clave Pública (PKI) y cuál es el rol de una Autoridad de Certificación (CA) dentro de ella?

Respuesta:

- **Definición de PKI:**
    - La Infraestructura de Clave Pública (PKI) es un conjunto de hardware, software, políticas, procedimientos y roles necesarios para crear, gestionar, distribuir, utilizar, almacenar y revocar certificados digitales. Su objetivo es facilitar la utilización segura de la criptografía de clave pública en entornos de comunicación.
- **Rol de la Autoridad de Certificación (CA):**
    - **Emisión de Certificados:** La CA verifica la identidad de los solicitantes y, una vez confirmada, emite un certificado digital que vincula la identidad de una entidad (persona, servidor, etc.) con su clave pública.
    - **Firma Digital:** La CA firma digitalmente el certificado utilizando su propia clave privada, lo que garantiza la integridad y la autenticidad del certificado.
    - **Gestión y Revocación:** La CA mantiene y publica listas de revocación de certificados (CRL) para informar si algún certificado ya no es válido.

- **Confianza:** Al actuar como entidad de confianza, la CA permite que los usuarios y sistemas confíen en la relación entre una identidad y su clave pública, lo que es esencial para establecer comunicaciones seguras y para la verificación de firmas digitales.

- **Conclusión:**
  La PKI es el marco que permite el uso generalizado de criptografía asimétrica en redes, y la CA es el pilar de confianza dentro de esta infraestructura, garantizando que los certificados emitidos sean válidos y que la asociación entre identidad y clave pública sea confiable.

Pregunta 7.

Explique el funcionamiento de IPSec y compare brevemente los modos de operación "túnel" y "transporte". ¿En qué escenarios se utiliza cada modo?

Respuesta:

- **Funcionamiento de IPSec:**
  - IPSec es un conjunto de protocolos diseñado para asegurar las comunicaciones a nivel de red mediante la autenticación, integridad y, opcionalmente, la confidencialidad de los paquetes IP. Se utiliza para establecer conexiones seguras (por ejemplo, VPN) mediante el cifrado y autenticación de los datos.

- **Modos de Operación:**

  1. **Modo Túnel:**
     - **Descripción:** Se encapsula el paquete IP completo (cabecera y datos) dentro de un nuevo paquete IP. Se añade una nueva cabecera IP.
     - **Uso:** Es ideal para conectar redes completas a través de Internet (VPN entre sitios), ya que protege toda la información de origen y destino de la red interna.
  2. **Modo Transporte:**
     - **Descripción:** Solo se protege el payload (la carga útil) del paquete IP, dejando la cabecera original sin modificar.
     - **Uso:** Es utilizado en comunicaciones directas entre dos hosts, donde la protección del contenido es necesaria pero se desea preservar la cabecera original para el enrutamiento.

- **Escenarios de Uso:**
  - **Modo Túnel:** Conexiones VPN entre sucursales o entre un usuario remoto y la red corporativa, donde se requiere encapsular y proteger completamente el tráfico interno.
  - **Modo Transporte:** Comunicaciones seguras entre dos dispositivos finales (por ejemplo, en aplicaciones de comunicación punto a punto), donde solo se necesita cifrar los datos sin alterar la cabecera IP.

- **Conclusión:**
  IPSec ofrece flexibilidad al operar en dos modos que se adaptan a diferentes necesidades: el modo

túnel para proteger redes completas y el modo transporte para asegurar la comunicación entre hosts, garantizando la integridad, autenticación y, opcionalmente, la confidencialidad de la información.

Pregunta 8.

Describa brevemente el proceso de establecimiento de una conexión TLS (SSL) y explique cómo este protocolo garantiza la confidencialidad, la integridad y la autenticación en una comunicación.

Respuesta:

- **Proceso de Handshake TLS:**

    1. **Inicio y Negociación:**
        - El cliente se conecta al servidor y envía un mensaje "Client Hello" que incluye las versiones de protocolo TLS compatibles, suites criptográficas y datos aleatorios.
        - El servidor responde con un "Server Hello", seleccionando la versión y la suite criptográfica, y enviando también un número aleatorio.
    2. **Autenticación del Servidor:**
        - El servidor envía su certificado digital (y, opcionalmente, certificados de la cadena de confianza) para que el cliente pueda verificar su identidad.
    3. **Intercambio de Claves:**
        - Se realiza un intercambio de claves (usualmente mediante RSA o Diffie-Hellman) en el que el cliente genera una clave secreta (pre-maestra) y la envía al servidor, cifrada con la clave pública del servidor. Ambos partes calculan la clave maestra a partir de la pre-maestra y los números aleatorios intercambiados.
    4. **Finalización del Handshake:**
        - Se envían mensajes de "Change Cipher Spec" y "Finished" desde ambas partes, indicando que a partir de ese momento se utilizará el cifrado y los algoritmos negociados para proteger la comunicación.

- **Garantías de Seguridad:**
    - **Confidencialidad:**
        - La clave de sesión derivada del intercambio de claves se utiliza para cifrar todos los datos transmitidos, impidiendo que terceros puedan leer la información.
    - **Integridad:**
        - Se utilizan códigos de autenticación de mensajes (MAC o HMAC) en cada registro de la comunicación, asegurando que los datos no sean modificados sin ser detectados.
    - **Autenticación:**
        - La verificación del certificado digital del servidor (y opcionalmente del cliente) permite confirmar la identidad de las partes, protegiendo contra ataques de suplantación.

- **Conclusión:**
  El protocolo TLS establece un canal seguro mediante un proceso de negociación y autenticación

(handshake), que permite a las partes intercambiar claves de forma segura y, a partir de entonces, garantizar la confidencialidad, integridad y autenticación de toda la comunicación.

A continuación te propongo una serie de preguntas sobre TCP y sobre los protocolos que abarcan los 5 temas (desde la capa de enlace hasta las aplicaciones y seguridad), siguiendo el estilo de los exámenes anteriores. Cada pregunta va acompañada de una respuesta detallada, que te ayudará a alcanzar la máxima calificación.

Pregunta 1. (TCP – Establecimiento de Conexión y Control de Ventana)

Enunciado:
Explique el proceso de establecimiento de una conexión TCP, detallando el three-way handshake. Además, describa cómo se ajusta la ventana de congestión durante el inicio lento (slow start) y la fase de prevención de congestión (congestion avoidance).

Respuesta:

- **Establecimiento de Conexión (Three-Way Handshake):**

  1. **SYN:** El cliente inicia la conexión enviando un segmento con el flag SYN activado y un número de secuencia inicial (ISN_C).
  2. **SYN+ACK:** El servidor responde con un segmento que tiene los flags SYN y ACK activos. En este segmento, el servidor asigna su propio ISN_S y confirma el ISN_C mediante el campo ACK (ACK = ISN_C + 1).
  3. **ACK:** El cliente finaliza el establecimiento enviando un segmento con el flag ACK, donde confirma el ISN_S (ACK = ISN_S + 1).
     Este intercambio sincroniza los contadores de secuencia y establece el canal de comunicación.

- **Control de Ventana y Ajuste de la Ventana de Congestión:**

  - **Inicio Lento (Slow Start):**

    - El emisor comienza con una ventana de congestión (CWND) pequeña (normalmente 1 o 2 MSS).
    - Por cada ACK recibido, la ventana se duplica de forma exponencial (CWND se incrementa en 1 MSS por cada segmento confirmado).
    - Este crecimiento rápido continúa hasta alcanzar un umbral (ssthresh) predefinido.

  - **Prevención de Congestión (Congestion Avoidance):**

    - Una vez que CWND alcanza o supera el ssthresh, el crecimiento se vuelve lineal: por cada ronda de envío (es decir, por cada RTT completo) se incrementa la CWND en 1 MSS (o de forma proporcional al número de ACK recibidos).
    - Si se detecta pérdida (por timeout o triple duplicate ACK), se reduce el ssthresh a la mitad de la CWND actual y se reinicia el proceso de slow start (en TCP Tahoe) o se utiliza una recuperación más sofisticada (por ejemplo, en TCP Reno).

Esta combinación de técnicas permite a TCP adaptarse dinámicamente a la capacidad de la red, evitando saturarla mientras se maximiza el uso de los recursos disponibles.

Pregunta 2. (TCP – Control de Errores y Timeout)

Enunciado:
Explique cómo TCP gestiona el control de errores. Incluya en su respuesta la función de los ACK acumulativos, el cálculo del timeout mediante la estimación del RTT, y el uso del algoritmo de Karn. ¿Cómo impacta este mecanismo en la retransmisión de datos?

Respuesta:

- **ACK Acumulativos:**
    - Cada segmento TCP lleva un número de secuencia que indica el primer byte de los datos enviados.
    - El receptor envía ACKs que confirman el recibo de todos los bytes hasta un cierto número (el "número de acuse"), lo que significa que todos los datos previos se han recibido correctamente.
    - Estos ACK son acumulativos; es decir, un solo ACK puede confirmar múltiples segmentos si llegan en orden.
- **Cálculo del Timeout:**
    - **Estimación del RTT:** TCP mide el tiempo que tarda un segmento en ser enviado y en recibir su ACK (Round-Trip Time o RTT).
    - **Algoritmo de Estimación:** Se utiliza una fórmula de media móvil: [RTT_{estimado} = \alpha \cdot RTT_{previo} + (1 - \alpha) \cdot RTT_{medido}] y se calcula la desviación del RTT para ajustar dinámicamente el tiempo de timeout: [Timeout = RTT_{estimado} + 4 \cdot \text{Desviación}]
    - **Algoritmo de Karn:** Cuando un segmento se retransmite, su RTT medido no se utiliza para actualizar la estimación, ya que el ACK recibido puede corresponder tanto al segmento original como a la retransmisión. Se duplica el timeout para evitar ambigüedades.
- **Impacto en la Retransmisión:**
    - Si un ACK no llega antes de que expire el timeout, TCP retransmite el segmento.
    - La adecuada estimación del timeout es crucial: un timeout demasiado corto causa retransmisiones innecesarias (reduciendo el rendimiento) y uno demasiado largo retrasa la recuperación ante pérdidas.

Con estos mecanismos, TCP garantiza la entrega confiable de datos ajustándose a las condiciones reales de la red.

Pregunta 3. (Comparación TCP vs UDP)

Enunciado:
Compare TCP y UDP en términos de sus características principales, control de errores, confiabilidad y aplicaciones típicas en las que se prefiere cada uno.

Respuesta:

- **TCP (Transmission Control Protocol):**

    - **Orientado a Conexión:** Se establece una conexión mediante el three-way handshake antes de la transferencia de datos.
    - **Confiabilidad:** Asegura la entrega ordenada y sin errores mediante el uso de ACKs, retransmisiones y números de secuencia.
    - **Control de Congestión y Flujo:** Adapta dinámicamente la tasa de envío para evitar saturar la red y para no sobrecargar al receptor.
    - **Aplicaciones Típicas:** Transferencia de ficheros, navegación web, correo electrónico, donde la confiabilidad es crucial.

- **UDP (User Datagram Protocol):**

    - **No Orientado a Conexión:** No se establece conexión, cada datagrama se envía de forma independiente.
    - **Sin Confiabilidad Incorporada:** No se garantizan la entrega, el orden o la integridad de los datos; no hay retransmisión automática.
    - **Bajo Overhead y Latencia:** Menor retardo y menor sobrecarga en comparación con TCP.
    - **Aplicaciones Típicas:** Aplicaciones en tiempo real como videoconferencias, streaming, juegos en línea y DNS, donde la velocidad es más importante que la fiabilidad absoluta.

En resumen, TCP se utiliza cuando se requiere una comunicación fiable, mientras que UDP se prefiere en aplicaciones que toleran pérdidas de datos y donde la baja latencia es prioritaria.

Pregunta 4. (Capa de Red – IP, ARP, ICMP)

Enunciado:
Describa el proceso de encaminamiento en la capa de red de Internet. Explique el papel que desempeñan las tablas de encaminamiento, la función del protocolo ARP, y la importancia de ICMP en la red.

Respuesta:

- **Encaminamiento en la Capa de Red:**

    - Cada router mantiene una **tabla de encaminamiento** que contiene entradas con destinos, máscaras, el siguiente salto (next hop) y la interfaz por la que enviar el datagrama.
    - Para cada datagrama, el router realiza una **búsqueda de coincidencia de prefijo** (longest prefix matching) para determinar la ruta óptima.

- **Función del ARP (Address Resolution Protocol):**

    - ARP se utiliza para mapear direcciones IP (lógicas) a direcciones MAC (físicas) en redes locales.
    - Cuando un router o host necesita enviar un datagrama a una dirección IP dentro de la misma subred, consulta su tabla ARP para obtener la dirección MAC correspondiente. Si no la tiene, realiza una difusión ARP solicitando dicha dirección.

- **Importancia de ICMP (Internet Control Message Protocol):**

    - ICMP es un protocolo de señalización que se utiliza para enviar mensajes de error y diagnósticos.
    - Por ejemplo, envía mensajes de **"Time Exceeded"** cuando un datagrama supera su TTL, o de **"Destination Unreachable"** si no es posible alcanzar el destino.
    - Permite herramientas de diagnóstico como **ping** (echo request/reply) y **traceroute**.

Este conjunto de protocolos y mecanismos asegura que los datagramas se entreguen correctamente y que los errores se detecten y se comuniquen de vuelta al origen.

Pregunta 5. (Seguridad – TLS y Certificados Digitales)

Enunciado:
Explique el proceso de establecimiento de una conexión segura mediante TLS. ¿Cuál es el rol de los certificados digitales y de la Infraestructura de Clave Pública (PKI) en este proceso?

Respuesta:

- **Proceso de Handshake TLS:**
    1. **Client Hello:**
        - El cliente envía un mensaje "Client Hello" que incluye las versiones de TLS soportadas, suites criptográficas y un valor aleatorio.
    2. **Server Hello:**
        - El servidor responde con un "Server Hello" en el que selecciona la versión y suite a usar, y envía su valor aleatorio.
    3. **Certificado del Servidor:**
        - El servidor envía su certificado digital, que contiene su identidad y clave pública, firmado por una CA confiable.
    4. **Intercambio de Claves:**
        - El cliente verifica el certificado (comprobando la cadena de confianza y la firma) y, usando la clave pública del servidor, cifra un valor pre-maestro que se enviará al servidor.
        - Ambas partes generan una clave de sesión a partir del valor pre-maestro y los números aleatorios.
    5. **Change Cipher Spec y Finished:**
        - Se intercambian mensajes "Change Cipher Spec" para notificar el cambio a la comunicación cifrada, seguidos por mensajes "Finished" para confirmar que la negociación fue exitosa.

- **Rol de los Certificados Digitales y la PKI:**
    - **Certificados Digitales:**
        - Garantizan la autenticidad del servidor (y opcionalmente del cliente). Contienen la identidad de la entidad, su clave pública, y otros datos (por ejemplo, periodo de validez), y están firmados digitalmente por una CA.
    - **Infraestructura de Clave Pública (PKI):**
        - Es el conjunto de políticas, procedimientos y tecnologías que permiten la creación, gestión y verificación de certificados digitales.
        - Proporciona un mecanismo de confianza, ya que los usuarios confían en la CA para verificar que la asociación entre la identidad y la clave pública es correcta.

- **Garantías de Seguridad:**
    - **Confidencialidad:** Se establece una clave de sesión para cifrar el tráfico.
    - **Integridad:** Se utilizan MACs o HMACs para asegurar que los mensajes no se han alterado.
    - **Autenticación:** La verificación del certificado asegura que el servidor es quien dice ser.

De este modo, TLS permite establecer comunicaciones seguras a través de Internet, garantizando que los datos transmitidos sean confidenciales, íntegros y auténticos.

Pregunta 6. (Protocolos de Aplicación – HTTP, SMTP y DNS)

Enunciado:
Compare y contraste los protocolos HTTP, SMTP y DNS en cuanto a su función, la estructura de sus mensajes y la forma en que gestionan la comunicación (por ejemplo, si son orientados a conexión o no, si son stateful o stateless, etc.).

Respuesta:

- **HTTP (Hypertext Transfer Protocol):**
    - **Función:** Permite la transferencia de páginas web y otros recursos en la World Wide Web.
    - **Transporte:** Opera sobre TCP, lo que garantiza la entrega fiable y ordenada de los datos.
    - **Estado:** Es un protocolo *stateless*; cada solicitud es independiente, aunque se pueden usar mecanismos como cookies para mantener estado a nivel de aplicación.
    - **Estructura de Mensajes:** Se compone de un mensaje de solicitud (request) y de respuesta (response) con líneas de encabezado y, en el caso de las respuestas, el cuerpo del mensaje.
- **SMTP (Simple Mail Transfer Protocol):**
    - **Función:** Se utiliza para el envío de correo electrónico entre servidores y desde clientes hacia servidores.
    - **Transporte:** También opera sobre TCP, lo que permite la entrega ordenada y fiable de mensajes.
    - **Estado:** Es *stateful* en el sentido de que establece una sesión de conexión para el envío de un mensaje, que se cierra al finalizar la transmisión.
    - **Estructura de Mensajes:** Utiliza comandos y respuestas en texto ASCII (por ejemplo, HELO, MAIL FROM, RCPT TO, DATA) para gestionar el intercambio.
- **DNS (Domain Name System):**
    - **Función:** Traduce nombres de dominio legibles (por ejemplo, www.ejemplo.com) a direcciones IP numéricas.
    - **Transporte:** Predomina el uso de UDP en el puerto 53 para consultas rápidas, aunque se utiliza TCP para transferencias de zona o respuestas que exceden 512 bytes.
    - **Estado:** Es *stateless*; cada consulta es independiente y no se mantiene sesión alguna entre las solicitudes.
    - **Estructura de Mensajes:** Los mensajes DNS están compuestos por secciones de cabecera, preguntas, respuestas, autoridad y adicionales, y tienen un formato binario compacto.

En resumen, mientras que HTTP y SMTP operan sobre TCP y se benefician de la conexión orientada a sesión para garantizar la fiabilidad de la transferencia de datos, DNS se diseña para respuestas rápidas y generalmente sin conexión, lo que lo hace muy eficiente para la resolución de nombres.
