Aquí tienes unos apuntes estructurados, con puntos clave y resúmenes concisos, para que puedas memorizar rápidamente los conceptos esenciales de TCP y de los protocolos de los 5 temas, así como algunos aspectos de seguridad. He agrupado la información siguiendo el estilo de las preguntas que revisamos, para que no quede ningún concepto difuso.

Apuntes de Repaso para Exámenes de Teoría

I. TCP (Transmisión de Control Protocol)

1. Establecimiento de Conexión (Three-Way Handshake)

- **Paso 1: SYN**
  - **Cliente:** Envía un segmento con flag SYN y su número de secuencia inicial ($ISN_{(}C_{)}$).
- **Paso 2: SYN+ACK**
  - **Servidor:** Responde con un segmento que tiene SYN y ACK; incluye su propio $ISN_{(}S_{)}$ y confirma el $ISN_{(}C_{)}$ (ACK = $ISN_{(}C_{)}$ + 1).
- **Paso 3: ACK**
  - **Cliente:** Envía un segmento ACK confirmando el $ISN_{(}S_{)}$ (ACK = $ISN_{(}S_{)}$ + 1).
- **Objetivo:** Sincronizar ambos contadores de secuencia para establecer el canal de comunicación.

2. Control de Flujo vs. Control de Congestión

- **Control de Flujo:**
  - **Objetivo:** Evitar que el emisor envíe más datos de los que el receptor puede procesar.
  - **Mecanismo:** El receptor anuncia su ventana de recepción (valor en los ACK), y el emisor no excede ese límite.
- **Control de Congestión:**
  - **Objetivo:** Evitar saturar la red (routers, enlaces) con demasiados datos.
  - **Mecanismo:** Se utiliza la ventana de congestión (CWND) que el emisor ajusta en función de la retroalimentación de la red (pérdida, retrasos).
  - **Algoritmos:**
    - **Inicio Lento (Slow Start):**
      - Comienza con CWND pequeña (1 o 2 MSS) y crece de forma exponencial (se duplica por cada RTT) hasta llegar al umbral (ssthresh).
    - **Prevención de Congestión (Congestion Avoidance):**
      - Una vez superado ssthresh, el crecimiento de CWND es lineal (aproximadamente +1 MSS por RTT).
  - **Recuperación:** Si se detecta pérdida (timeout o triple duplicate ACK) se reduce ssthresh y se reinicia (o se activa fast recovery en TCP Reno).

3. Control de Errores y Timeout en TCP

- **ACK Acumulativos:**
  - Cada ACK confirma todos los bytes recibidos hasta cierto número; permite detectar pérdidas y reordenar segmentos.

- **Estimación del RTT y Timeout:**
  - Se mide el tiempo entre el envío de un segmento y la recepción de su ACK.
  - Fórmula típica: [RTT_{estimado} = \alpha \times RTT_{previo} + (1-\alpha) \times RTT_{medido}] y se calcula una desviación para ajustar: [Timeout = RTT_{estimado} + 4 \times \text{Desviación}]
  - **Algoritmo de Karn:** No se actualiza el RTT con ACKs de segmentos retransmitidos y se duplica el timeout en caso de retransmisión.
- **Impacto:** Un timeout demasiado corto provoca retransmisiones innecesarias; uno muy largo retrasa la recuperación.

4. TCP vs. UDP

- **TCP:**
  - Orientado a conexión (three-way handshake).
  - Garantiza la entrega ordenada, confiable y sin errores.
  - Control de flujo y congestión.
  - Se usa en aplicaciones donde la fiabilidad es vital (web, correo, transferencia de archivos).
- **UDP:**
  - No orientado a conexión; cada datagrama se envía de forma independiente.
  - No garantiza entrega ni orden.
  - Menor sobrecarga y latencia.
  - Ideal para aplicaciones en tiempo real (streaming, videojuegos, DNS).

5. Números de Secuencia y Ventana (Bandwith-Delay Product)

- **Números de Secuencia:**
  - Cada byte tiene un número; se usan para reordenar y detectar pérdidas.
  - Inician en un ISN (pseudoaleatorio) durante el handshake.
- **Ventana de Congestión (CWND):**
  - La cantidad máxima de datos “en vuelo”.
  - Debe ser mayor o igual al producto de la velocidad por el RTT (BDP): [BDP = \text{Velocidad de transmisión} \times \text{RTT}]
  - Permite evitar “interrupciones” en el envío.

II. Protocolos de Capa de Red y Aplicación

1. Protocolo IP, ARP e ICMP

- **Encaminamiento IP:**
  - Cada router usa su tabla de rutas (destino, máscara, next hop, interfaz) para determinar el mejor camino (longest prefix matching).
- **ARP:**
  - Mapea direcciones IP a direcciones MAC en la LAN.
  - Si no existe entrada, se envía una solicitud ARP (broadcast) y se obtiene la dirección física.
- **ICMP:**
  - Envía mensajes de error y diagnóstico (por ejemplo, “Time Exceeded” y “Destination Unreachable”).

    - Se usa en herramientas como ping y traceroute.

2. Protocolos de Aplicación: HTTP, SMTP, DNS

- **HTTP:**
    - Protocolo para transferir páginas web.
    - Opera sobre TCP y es stateless (cada solicitud es independiente).
    - Utiliza métodos como GET, POST, HEAD.
- **SMTP:**
    - Protocolo para envío de correo electrónico entre servidores.
    - Opera sobre TCP y establece una sesión stateful (comienza con HELO, MAIL FROM, RCPT TO, DATA, etc.).
- **DNS:**
    - Traduce nombres de dominio a direcciones IP.
    - Normalmente usa UDP en el puerto 53; puede usar TCP para transferencias de zona.
    - Es stateless: cada consulta es independiente.
- **Comparación:**
    - HTTP y SMTP usan TCP para garantizar la fiabilidad; DNS se diseña para rapidez y bajo overhead.

III. Seguridad en Redes

1. TLS y Certificados Digitales

- **Proceso TLS (Handshake):**
    1. **Client Hello:** El cliente envía versiones, suites y un valor aleatorio.
    2. **Server Hello:** El servidor elige la versión y suite, y envía su valor aleatorio.
    3. **Certificado:** El servidor envía su certificado digital para que el cliente verifique su identidad.
    4. **Intercambio de Claves:** El cliente cifra un pre-maestro con la clave pública del servidor; ambos derivan la clave de sesión.
    5. **Change Cipher Spec y Finished:** Se confirman los cambios al cifrado y se inicia la comunicación segura.
- **Rol de los Certificados y PKI:**
    - El certificado vincula la identidad con la clave pública y es firmado por una CA.
    - La PKI es el conjunto de herramientas y políticas que gestionan y verifican estos certificados.
    - Garantizan autenticación, integridad, confidencialidad y no repudio.

2. Cifrado: Simétrico vs. Asimétrico

- **Cifrado Simétrico:**
    - Usa la misma clave para cifrar y descifrar.
    - Es rápido y eficiente para grandes volúmenes de datos.
    - Problema: Intercambio seguro de la clave.
- **Cifrado Asimétrico:**
    - Usa un par de claves: pública y privada.
    - Facilita el intercambio seguro (solo se comparte la pública) y permite la firma digital.
    - Es más lento y se usa para intercambiar claves o para firmar mensajes.
- **Uso Híbrido:**

    - Muchos protocolos (como TLS) usan cifrado asimétrico para intercambiar una clave simétrica que luego se usa para cifrar la comunicación.

3. Firma Digital y Certificados

- **Firma Digital:**
    - Consiste en calcular un hash del mensaje y cifrarlo con la clave privada del emisor.
    - Permite autenticación, integridad y no repudio.
- **Certificado Digital:**
    - Documento electrónico que asocia la identidad de una entidad con su clave pública, firmado por una CA.
    - Contiene: Identidad del titular, clave pública, fechas de validez, información de la CA, número de serie.

4. Intercambio Diffie-Hellman

- **Proceso:**
    1. Se eligen parámetros públicos: un primo grande n y un generador g.
    2. Cada parte elige un secreto (a y b).
    3. Se intercambian $A = g^a \mod n$ y $B = g^b \mod n$.
    4. Cada parte calcula la clave secreta: $K = B^a \mod n = A^b \mod n$.
- **Vulnerabilidad:** Ataque Man-in-the-Middle.
- **Mitigación:** Autenticación previa (certificados) o integración en protocolos seguros (TLS).

5. Funciones Hash y HMAC

- **Función Hash:**
    - Toma un mensaje de longitud variable y produce un valor de longitud fija.
    - Propiedades: determinística, rápida, unidireccional, resistente a colisiones, sensibilidad al cambio.
- **HMAC:**
    - Combina una función hash con una clave secreta para generar un código que garantiza la integridad y autenticación.
    - Ejemplo: HMAC-SHA256.

6. Ataque Man in the Middle (MitM)

- **Definición:**
    - Un atacante intercepta y modifica la comunicación entre dos partes sin que estas lo sepan.
- **Prevención:**
    - Uso de TLS/SSL con verificación de certificados.
    - Autenticación mutua (certificados en ambos extremos).

7. IPSec: Modos de Operación

- **IPSec:**
    - Asegura la comunicación a nivel IP mediante autenticación, integridad y confidencialidad.
- **Modos:**
    - **Túnel:** Se encapsula el paquete completo; ideal para VPN entre sitios.
    - **Transporte:** Se cifra solo el payload; usado en comunicaciones punto a punto entre hosts.

IV. Otros Protocolos (Resumen General de los 5 Temas)

1. Capa Física y de Enlace

- **Funciones:** Transmisión de bits, delimitación de tramas, detección/corrección de errores a nivel de enlace.
- **Protocolos y estándares:** Ethernet, WiFi, Token Ring, etc.

2. Capa de Red

- **IP:** Direccionamiento y encaminamiento.
- **ARP:** Resolución de direcciones IP a MAC.
- **ICMP:** Mensajes de error y diagnóstico.
- **Enrutamiento Dinámico:** Protocolos como RIP, OSPF y BGP para la actualización automática de rutas.

3. Capa de Transporte

- **TCP:** Conexión, confiabilidad, control de flujo y congestión, numeración de bytes.
- **UDP:** Comunicación sin conexión, menor latencia, sin garantías de entrega.

4. Capa de Sesión, Presentación y Aplicación

- **Sesión y Presentación:** Manejo del diálogo, cifrado y codificación de datos.
- **Aplicación:** Protocolos como HTTP, FTP, SMTP, POP3, IMAP, DNS, etc.
    - **HTTP:** Transferencia de páginas web.
    - **SMTP/POP3/IMAP:** Envío y acceso a correo electrónico.
    - **DNS:** Resolución de nombres.

5. Seguridad

- **Cifrado (simétrico/asimétrico), firma digital, PKI, TLS, IPSec, HMAC, Diffie-Hellman.**
- **Objetivos:** Confidencialidad, integridad, autenticación y no repudio.