Arquitectura de Redes, Modelo OSI y Capa de Transporte (TCP/UDP)

Sección 1: Mapeo de Capas, Equipos, PDUs y Protocolos

1.1 Matriz de Integración OSI

Completa la siguiente tabla indicando el nombre de la capa, la PDU correspondiente, los equipos o hardware asociados y al menos tres protocolos o estándares representativos de ese nivel.

N° Capa	Nombre de la Capa	PDU	Equipos / Dispositivos Principales	Protocolos / Estándares Representativos
7	Aplicación	APDU	Gateway de aplicación, Firewall de Capa 7 (WAF)	HTTP/HTTPS, DNS, SSH, SMTP
6	Presentación	PPDU		
5	Sesión	SPDU		
4	Transporte	Segmento (TCP) / Datagrama (UDP)		
3	Red	Paquete		
2	Enlace de Datos	Trama (Frame)		
1	Física	Bits		

1.2 Preguntas de Análisis Técnico
Hub vs. Switch (Nivel 1 vs. Nivel 2):

Explica detalladamente por qué un Hub pertenece a la Capa 1 y un Switch gestionable opera primordialmente en la Capa 2. En tu respuesta debes comparar:

- Manejo de dominios de colisión y dominios de difusión (*broadcast*).
- Uso de la tabla CAM (Content Addressable Memory) / MAC y método de reenvío de tramas.

1.2 Switches de Capa 3 (*Multilayer Switches*) vs. Routers Tradicionales:

Ambos dispositivos procesan paquetes a nivel de Capa 3:

- ¿Cuál es la diferencia fundamental en la arquitectura de hardware entre el enrutamiento realizado por un Switch L3 (ASIC/TCAM) y un Router convencional?
- ¿En qué escenario de red corporativa elegirías cada uno?

1.3 El dilema de la Capa 2.5:

Protocolos como **ARP (Address Resolution Protocol)** y **MPLS (Multiprotocol Label Switching)** suelen catalogarse informalmente como de "Capa 2.5". Justifica técnicamente por qué ARP no encaja de forma pura ni en la Capa 2 ni en la Capa 3 del modelo OSI.

Sección 2: Capa de Transporte — TCP, UDP y Gestión de Puertos

2.1 Clasificación y Análisis de Puertos
Los puertos lógicos van del 0 al 65535 y se dividen en tres rangos estandarizados por la IANA (Internet Assigned Numbers Authority):

- **Puertos bien conocidos (*Well-known ports*):** 0 a 1023
- **Puertos registrados (*Registered ports*):** 1024 a 49151
- **Puertos dinámicos / privados / efímeros (*Ephemeral ports*):** 49152 a 65535

Responde:

- Identifica el número de puerto por defecto y el protocolo de transporte (TCP, UDP o ambos) para los siguientes servicios:
  - **DNS (Consultas estándar de clientes vs. Transferencia de zona):**
  - **DHCP (Cliente y Servidor):**

- **NTP (Sincronización horaria):**
- **SNMP (Monitoreo):**
- **LDAPS (Directorio seguro):**
- **BGP (Enrutamiento externo):**

Sección 3: Casos de Estudio y Diagnóstico de Tráfico

Caso 1: Desglose de Encapsulación en una Petición Web Segura
Un usuario dentro de la red privada 192.168.10.50/24 abre su navegador y accede a https://servidorseguro.edu.co (IP: 200.89.45.10).

Describe el estado de la PDU en cada una de las siguientes capas antes de salir de la tarjeta de red (NIC) del cliente:

```
[ Capa 7 - Aplicación ]  --> Protocolo utilizado: _____________
[ Capa 4 - Transporte ]  --> Protocolo: TCP | Puerto Origen: ______ | Puerto Destino: ______
[ Capa 3 - Red ]         -->   IP Origen: _____________ | IP Destino: _____________
[ Capa 2 - Enlace ]      -->  MAC Origen: _____________ | MAC Destino:_____________
[ Capa 1 - Física ]      -->   Representación en el medio de transmisión: _____________
```

Caso 2: Diagnóstico de Socket y Estado de Conexiones (netstat **/** ss**)**
Un administrador de sistemas ejecuta el comando ss -tuln en un servidor Linux de producción y obtiene la siguiente salida:

```
Netid   State      Recv-Q   Send-Q   Local Address:Port         Peer Address:Port
tcp     LISTEN     0        128          0.0.0.0:22                 0.0.0.0:*
tcp     LISTEN     0        511          127.0.0.1:3306             0.0.0.0:*
tcp     LISTEN     0        100          0.0.0.0:80                 0.0.0.0:*
tcp     LISTEN     0        100          0.0.0.0:443                0.0.0.0:*
udp     UNCONN     0        0            0.0.0.0:123                0.0.0.0:*
udp     UNCONN     0        0            192.168.1.10:161           0.0.0.0:*
```

En Linux ejecutar en la consola

ss -tuln

ó

netstat -tuln

Desglose de los parámetros:

- *-t (TCP): Muestra únicamente los sockets TCP.*
- *-u (UDP): Muestra únicamente los sockets UDP.*
- *-l (Listening): Filtra para mostrar solo los puertos que están en estado de escucha (listening).*
- *-n (Numeric): Muestra las direcciones IP y los números de puerto en formato numérico (evita la resolución DNS y nombres de servicios, mostrando 22 en lugar de ssh, o 3306 en lugar de mysql).*

En Windows ejecutar en powershell

netstat -ano

ó

netstat -an | findstr /i "listening udp"

Parámetros en Windows:
- *-a: Muestra todas las conexiones activas y puertos en escucha.*
- *-n: Muestra direcciones IP y puertos en formato numérico (evita resolver nombres).*
- *-o: Muestra el PID (identificador de proceso) del programa dueño de cada puerto.*

Preguntas de Diagnóstico:
1. ¿A qué servicios corresponden los puertos 22, 3306, 80, 443, 123 y 161?
2. Un desarrollador intenta conectarse a la base de datos MySQL (3306) desde su equipo de escritorio (192.168.1.25) y recibe un error de "Conexión rechazada". Observando la columna Local Address:Port, explica la causa exacta del fallo.
3. ¿Qué implicación de seguridad tiene que el servicio SSH (0.0.0.0:22) esté escuchando en 0.0.0.0 frente a una interfaz de red específica?

Caso 3: Ataques DoS a Nivel de Transporte y Capa de Enlace

Nmap en Linux

- Escaneo estándar (Los 1,000 puertos más comunes):Analiza los puertos más utilizados mediante un saludo parcial (SYN Scan), el cual es rápido y efectivo.
    - *nmap -sS 192.168.1.50*
- Escaneo rápido (Top 100 puertos):Ideal si tienes poco tiempo y solo quieres buscar los servicios más obvios (HTTP, SSH, FTP, etc.).

- *nmap -F 192.168.1.50*

- Escaneo de todos los puertos (Los 65,535 puertos completos):Por defecto, Nmap no escanea todo el rango. Si un administrador escondió un servicio en un puerto inusual (ej. el puerto 54321), necesitas este comando:
  - *nmap -p- 192.168.1.50*

- Escanear ciertos puertos
  - *nmap -p 80,443,3306 192.168.1.50*

Nmap en Windows

Descargar del sitio oficial:

https://nmap.org/download#windows

Desde powershell entramos a su carpeta :

cd 'C:\Program Files (x86)\Nmap\'

Y ejecutamos cada instrucción:

.\nmap.exe -sS 192.168.1.1

Preguntas

- Explica en qué consiste un ataque de inundación **TCP SYN Flood**:
  - ¿Qué fases del *3-way handshake* (SYN, SYN-ACK, ACK) se ven involucradas?
  - ¿Qué recurso del sistema operativo se agota en la víctima (tabla de conexiones / backlog queue)?
  - Menciona un mecanismo de mitigación estándar (ej. *SYN Cookies*).

- Explica la diferencia entre un ataque de **ARP Spoofing/Poisoning** (Capa 2) y un escaneo de puertos **TCP FIN** (Capa 4): ¿Qué capa del modelo OSI vulnera cada técnica y cuál es el objetivo del atacante en cada caso?