🤖**Diagnóstico de Fallas de Conectividad - Modelo OSI**

😺Escenario 1: Falla en Capa 1 - Problema físico (10 puntos)

Situación: El equipo `pc-01` conectado al switch `sw-lab1` no responde a ningún intento de conexión. Fue recientemente configurado con IP estática. Otros equipos en la misma VLAN funcionan correctamente.

1. Capturas de comandos utilizados

```
ip link show
sudo ethtool eth0
sudo tcpdump -i eth0
ifconfig eth0
```

2. Diagnóstico detallado

- Revisar luces LED del switch:
- Encendidas/parpadeando: conexión activa.
- Apagadas: posible problema físico.
- Verificar el cable UTP y conectores RJ-45:
- Probar con un tester de red o cambiando el cable.
- Revisar el crimpado.
- El `ip link show` y `ethtool` pueden indicar que la interfaz está inactiva o no detecta el cable.
- `tcpdump` no muestra tráfico, lo que refuerza un fallo físico.

3. Soluciones propuestas y justificación técnica

Causa	Solución	Justificación técnica
Cable dañado o mal crimpado	Cambiar el cable, revisar con tester.	Sin continuidad no se establece enlace físico.
Interfaz de red desactivada	`sudo ip link set eth0 up`	Activa la interfaz manualmente si está desactivada.
Puerto del switch deshabilitado	Revisar configuración del switch.	Si el puerto está apagado, no habrá conexión.
Tarjeta de red defectuosa	Reinstalar/cambiar la NIC.	El hardware podría estar dañado y no establecer enlace.

😺Escenario 2: Falla en Capa 3 - Problema de enrutamiento (15 puntos)

Situación: El servidor `dns-utu.lab` con IP `192.168.1.53` no puede ser alcanzado desde `pc-estudiante`, aunque hay ping exitoso a la puerta de enlace (`192.168.1.1`).

1. Capturas de comandos utilizados

```
ping 192.168.1.53
traceroute 192.168.1.53
ip route
```

2. Diagnóstico detallado

- `ping` a la puerta de enlace funciona, descartando problema físico o de capa 2.
- `traceroute` indica que el tráfico no llega más allá del router.
- `ip route` muestra que no hay ruta específica a la subred del servidor.

3. Solución propuesta y justificación técnica

```
sudo ip route add 192.168.1.0/24 via 192.168.1.1
```

- Esto añade una ruta explícita para alcanzar el servidor.
- También verificar configuración IP local:

```
ip a
ip r
```

Justificación técnica: La falta de una ruta correcta impide el reenvío del paquete hacia la red de destino. Al agregar una ruta, se soluciona el fallo de conectividad a nivel de capa 3.

Salida de ejemplo:

```
$ ip route
default via 192.168.1.1 dev eth0
# Faltaba la ruta específica a 192.168.1.0/24
```

😺Escenario 3: Falla en Capa 4 - Servicio inaccesible (15 puntos)

Situación: Desde `pc-docente` se intenta acceder al servidor web `192.168.1.100` pero el navegador indica “Conexión rechazada”. El ping responde correctamente.

1. Capturas de comandos utilizados

```
nmap 192.168.1.100 -p 80
sudo tcpdump -i eth0 port 80
sudo systemctl status apache2
```

2. Diagnóstico detallado

- `nmap` indica que el puerto 80 está cerrado o filtrado.
- `tcpdump` muestra intentos de conexión saliendo, pero no hay respuesta.
- El estado del servicio `apache2` muestra que está inactivo.

3. Solución propuesta y justificación técnica

```
sudo systemctl start apache2
sudo ufw allow 80/tcp
```

- Se activa el servicio web (Apache) y se abre el puerto en el firewall.

Justificación técnica: Aunque la red funciona, si el servicio web no está en ejecución o el firewall bloquea el puerto, el navegador no podrá conectarse.

🧠Comentario reflexivo final

- **Capa 1**: La inspección física fue fundamental. Observar los LED del switch, probar el cable con un tester y usar `ethtool` permitió identificar rápidamente la ausencia de enlace físico.
- **Capa 3**: Utilizar `traceroute` mostró que los paquetes no pasaban la puerta de enlace, y `ip route` confirmó la falta de ruta adecuada.
- **Capa 4**: `nmap` y `tcpdump` ayudaron a verificar que el puerto 80 no estaba disponible, y `systemctl` reveló que Apache no estaba corriendo.

🔍La estrategia más efectiva fue comenzar con pruebas desde lo más básico (capa física) e ir subiendo en el modelo OSI. Utilizar herramientas específicas como `ping`, `traceroute`, `nmap`, `tcpdump`, `ip route` y `systemctl` permitió un diagnóstico estructurado y preciso.

Este informe presenta un enfoque completo para el diagnóstico de red basado en el modelo OSI, utilizando herramientas prácticas, capturas reales y justificación técnica en cada paso.