

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 | <code>sudo ip link set eth0 up</code> | 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)

Errores comunes en la Capa 3 (Red)

| Error | Descripción | Cómo detectarlo | Solución |
|---|---|---|---|
| ❌ Ruta estática mal configurada o ausente | No hay una ruta para llegar a la red destino (192.168.1.0/24) en el router o PC | <code>ip route</code> o <code>tracert</code> se detiene en la puerta de enlace | Agregar ruta con <code>ip route add</code> |
| ⚠️ Máscara de subred incorrecta | El equipo cree que el destino está en otra red o en la suya erróneamente | <code>ip a</code> muestra máscara incorrecta, o <code>ping</code> se comporta erráticamente | Configurar correctamente la máscara de red (ej. /24) |
| 🔗 Puerta de enlace mal definida | La puerta de enlace apunta a un dispositivo incorrecto o inexistente | <code>ip route</code> muestra gateway equivocado | Corregir con <code>ip route change default via <IP_correcta></code> |
| 📶 Fallo de NAT o ACL en el router | El router bloquea tráfico hacia la red destino | Tráfico llega a la puerta de enlace pero no sale | Revisar configuración del router/firewall |
| 🚫 IP duplicada | Dos dispositivos con la misma IP pueden causar conflicto de enrutamiento | Tráfico se pierde o respuestas inesperadas | Verificar con <code>arp -a</code> o <code>nmap -sn</code> en la red |
| 🟡 Fallo en el router intermedio | El router está encendido pero con fallas de configuración o servicios | <code>ping</code> llega al router pero no más allá | Reiniciar servicios o revisar logs del router |

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

👉 Otras soluciones posibles para restaurar el servicio web

| Situación | Solución alternativa | Justificación técnica |
|---|---|---|
| El servicio está corriendo pero responde en otro puerto (por ejemplo, 8080) | Acceder desde el navegador a <code>http://192.168.1.100:8080</code> o cambiar la configuración en <code>/etc/apache2/ports.conf</code> para que escuche en el puerto 80 | Apache puede estar configurado en otro puerto distinto al predeterminado |
| El servicio web está caído por errores de configuración | Ejecutar <code>sudo apache2ctl configtest</code> para verificar errores y luego reiniciar con <code>sudo systemctl restart apache2</code> | Un error de sintaxis en la configuración impide que el servicio se inicie |

| Situación | Solución alternativa | Justificación técnica |
|--|---|---|
| SELinux está bloqueando la conexión (en distribuciones como CentOS/RHEL) | Ejecutar <code>sudo setenforce 0</code> para desactivarlo temporalmente o configurar el contexto correcto con <code>semanage</code> | SELinux puede impedir que Apache use ciertos puertos o archivos |
| El firewall del servidor bloquea todas las conexiones excepto SSH | Verificar con <code>sudo ufw status</code> o <code>iptables -L</code> , y permitir tráfico HTTP | A veces el firewall está en modo restrictivo por defecto |
| El servicio está activo pero atado a localhost (127.0.0.1) | Cambiar la directiva <code>Listen</code> <code>127.0.0.1:80</code> por <code>Listen 0.0.0.0:80</code> en la config de Apache | Esto permite que se pueda acceder desde otras máquinas y no solo localmente |
| El servicio está bloqueado por un WAF (Web Application Firewall) | Revisar y configurar correctamente las reglas del WAF para permitir el tráfico legítimo hacia el puerto 80 | El WAF puede bloquear solicitudes válidas por motivos de seguridad |



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.