

SESIÓN 9 : Diagnóstico y resolución de problemas de red

1. ¿Qué es el diagnóstico de red?

Cuando una web no carga o una aplicación no funciona, la mayoría piensa:

"El servidor está caído"

Pero **la mayoría de fallos NO son del servidor.**

Pueden ser por:

- wifi desconectado
- cable suelto
- fallo de DNS
- firewall bloqueando puertos
- problema de ruta en Internet
- servicio que no está escuchando

Diagnosticar red es como seguir **una cadena paso a paso** para descubrir DÓNDE se rompe.

2. ¿Cómo funcionan las redes?

Las redes funcionan en capas:

1. **Capa física** : cables, router, wifi
2. **Capa de red** : direcciones IP
3. **Capa de transporte** : TCP / UDP (puertos)
4. **Capa de aplicación** : HTTP, FTP, correo...

Un fallo puede estar en cualquiera de estas capas.

3. Herramientas esenciales

PING: ¿El equipo responde?

Envía un "hola, ¿estás ahí?".

Ejemplo:

ping google.com

Sirve para:

- saber si hay conexión
- ver la latencia (tiempo)

TRACEROUTE / TRACERT: ¿Por dónde pasan mis paquetes?

Muestra la ruta completa desde tu PC hasta el destino.

Ejemplo:

tracert google.com (Windows)

traceroute google.com (Linux)

Sirve para:

- ver en qué punto "muere" la conexión
- identificar routers lentos

DIG / NSLOOKUP : ¿Funciona el DNS?

DNS = convierte nombres (google.com) en IPs.

Ejemplo:

nslookup google.com

Sirve para:

- comprobar que el dominio está bien configurado
- ver si un DNS está fallando

NETSTAT / SS: ¿Está tu servicio escuchando?

Lista puertos abiertos y conexiones activas.

Ejemplo en Linux:

```
ss -lntp
```

Sirve para:

- comprobar si un servidor web está escuchando en el puerto correcto
- detectar puertos bloqueados
- ver si una app no está arrancada

CURL / WGET : ¿La web o API responde?

Permiten enviar peticiones HTTP desde consola.

Ejemplo:

```
curl -I http://google.com
```

Sirve para:

- ver si la web está viva (código 200 OK)
- ver errores (404, 500)

Resumen

- **Ping**: ¿está vivo?
- **Traceroute**: ¿por dónde pasan los paquetes?
- **DNS**: ¿el nombre apunta a la IP correcta?
- **Netstat**: ¿el puerto está abierto?
- **Curl**: ¿el servicio funciona?

4. Metodología profesional de diagnóstico

Siempre seguir este orden. Nunca saltarse pasos.

1. ¿El host responde? Ping

- Si falla: problema físico / firewall / conexión / red caída.

2. ¿Por dónde se pierde? Traceroute

- Si un salto no responde: problema del proveedor, router o salto intermedio.

3. ¿El DNS funciona? Nslookup

- Si por IP funciona y por nombre NO: fallo DNS.

4. ¿El servicio está escuchando? ss o netstat

- Si no aparece: no está arrancado o está mal configurado.

5. ¿La aplicación responde? curl

- Si devuelve un error HTTP : problema de la aplicación.

5. Caso real

“La app que no abría el puerto”

Problema

- Una empresa hizo una app Node.js.
- En local funciona.
- En el servidor no carga desde Internet: “Connection refused”.

Diagnóstico paso a paso

1. Ping al servidor: responde

- No es un problema de conexión

2. Traceroute: ruta completa

- No hay cortes

3. Netstat: puerto 8080 NO está escuchando

4. Firewall UFW: puerto 8080 bloqueado

- Se abre con:

- sudo ufw allow 8080/tcp

5. Curl

- curl -I <http://servidor:8080>
 - HTTP/1.1 200 OK

Resultado

- No era un fallo del código
- NO era el servidor
- Era un **puerto bloqueado por el firewall**

6. Errores típicos

- Pensar que si ping funciona, la web también
- Olvidar mirar el firewall
- No comprobar si el servicio está escuchando
- Probar dominios sin comprobar DNS
- Culpar al servidor sin evidencia
- Saltarse pasos del diagnóstico

7. Ejemplos

Ejemplo 1: Fallo DNS

ping 142.250.184.142 : RESPONDE
 ping google.com : si NO RESPONDE

- El DNS falla

Ejemplo 2: Puerto cerrado

ss -tuln | grep 80 : vacío

- El servidor web NO está corriendo

Ejemplo 3: Problema de ruta

tracert servidor.com

Se queda colgado en el salto 6

- fallo del ISP, no del servidor

Ejemplo 4 — Problema de aplicación

```
curl -I http://localhost:8000
```

HTTP/1.1 500 Internal Server Error

- El servidor responde, pero la aplicación está rota

Test**1. ¿Qué comprueba ping?**

- A) El estado de los puertos
- B) La latencia y accesibilidad del host
- C) El registro DNS
- D) La velocidad de transferencia

2. Si un dominio no responde pero su IP sí, ¿qué está fallando?

- A) El servidor web
- B) La tarjeta de red
- C) El DNS
- D) El cable Ethernet

3. ¿Qué herramienta muestra la ruta completa de los paquetes?

- A) netstat
- B) traceroute / tracert
- C) dig
- D) ss

4. Si ss -tuln no muestra el puerto 80, ¿qué significa?

- A) El firewall lo está bloqueando
- B) No hay ningún proceso escuchando en el puerto 80
- C) La red está caída
- D) El puerto está en modo mantenimiento

5. ¿Qué comando se usa para comprobar si una API responde?

- A) ping
- B) nslookup
- C) curl
- D) ssh