📁 LPIC-2 / 🌐 Examen 205 - Configuración de Red

205.3 Resolución de problemas de conectividad de red

Teoría

La resolución de problemas de red es una habilidad fundamental. Cuando un sistema o aplicación no puede comunicarse a través de la red, necesitas un enfoque estructurado para identificar la capa del problema y su causa raíz. Una metodología común se basa en el modelo de capas de red (TCP/IP o OSI), comenzando por las capas más bajas.

Metodología Sistemática para la Resolución de Problemas de Red:

1. **Capa 1 (Física):**
    - **Problema:** Cable desconectado, puerto de switch defectuoso, tarjeta de red deshabilitada.
    - **Diagnóstico:** Verificar el cable, las luces de enlace en la tarjeta de red y el switch, el estado de la interfaz en el sistema operativo (`ip link show` - buscar `UP,LOWER_UP`), revisar logs del sistema (`dmesg`, `journalctl`).
    - **Herramientas:** `ip link show`. Inspección visual. Logs.
2. **Capa 2 (Enlace de Datos):**
    - **Problema:** Problemas de comunicación en la red local (segmento Ethernet/Wi-Fi), dirección MAC incorrecta, problemas de ARP.
    - **Diagnóstico:** Verificar que la interfaz tiene la dirección MAC correcta (`ip link show`). Comprobar si puedes resolver la dirección MAC del gateway o de otros hosts locales dada su IP (`ip neigh show`, `arp -a`). Si la entrada ARP está incompleta o `FAILED`, puede haber un problema de Capa 2.
    - **Herramientas:** `ip link show`, `ip neigh show`, `arp`. `tcpdump` (para ver si llegan paquetes ARP request/reply).
3. **Capa 3 (Red/IP):**
    - **Problema:** Dirección IP/máscara de subred incorrecta, puerta de enlace incorrecta, problemas de enrutamiento, paquetes bloqueados por routers intermedios.
    - **Diagnóstico:** Verificar tu propia configuración IP (`ip addr show`). Verificar la tabla de enrutamiento y la puerta de enlace predeterminada (`ip route show`). Probar la alcanzabilidad a nivel IP (`ping` a IPs: localhost, gateway, host local, host remoto). Rastrear la ruta (`traceroute`, `mtr`) para ver dónde se detienen los paquetes o aumenta la latencia.
    - **Herramientas:** `ip addr show`, `ip route show`, `ping`, `traceroute`, `mtr`. `tcpdump` (para ver si los paquetes salen y si llegan respuestas ICMP).
4. **Capa 4 (Transporte/TCP/UDP):**

- **Problema:** El servicio de destino no está a la escucha, un firewall bloquea el puerto, el servicio está bloqueado por un firewall de red, problemas de conexión TCP/UDP.
- **Diagnóstico:** Verificar si el servicio en el host destino está escuchando en el puerto correcto (`ss -tulnp <puerto>`). Probar si el puerto es alcanzable desde tu host (`nc -zv <ip_destino> <puerto>`). Verificar firewalls locales en ambos extremos (`firewall-cmd`, `ufw`, `iptables -L`). Usar `tcpdump` para ver si se establece la conexión TCP (intercambio SYN, SYN/ACK, ACK) o si se recibe un paquete RST o un ICMP "Port Unreachable".
- **Herramientas:** `ss`, `netstat`, `nc`, `telnet`, comandos de firewall, `tcpdump`.

5. **Capa 7 (Aplicación):**
    - **Problema:** Problemas de resolución DNS, configuración incorrecta del servicio, problemas de protocolo de aplicación (HTTP, SSH, FTP), firewalls a nivel de aplicación, proxy issues.
    - **Diagnóstico:** Si el acceso por IP funciona pero por nombre falla, el problema es DNS (`host`, `dig`, `nslookup`, verificar `/etc/resolv.conf`, probar servidores DNS alternativos). Verificar el estado del servicio de aplicación en el host destino (`systemctl status`, `ps aux`). Revisar los logs del servicio de aplicación. Usar herramientas específicas del servicio (ej: cliente SSH con modo verbose `-v`). Usar `tcpdump` para ver el tráfico de la aplicación.
    - **Herramientas:** `host`, `dig`, `nslookup`, `cat /etc/resolv.conf`, `systemctl status`, `ps aux`, `journalctl`, logs específicos del servicio, `tcpdump`, clientes de aplicación con opciones de depuración.

Herramientas Clave y su Uso Avanzado (Revisión y Profundización):

- **`ping`:**
    - `ping -I <interfaz>`: Especifica la interfaz de origen para el ping. Útil en hosts con múltiples interfaces.
    - `ping -s <tamaño_paquete>`: Envía paquetes ICMP de un tamaño específico.
    - `ping -c <conteo>`: Envía solo un número limitado de paquetes.
    - `ping -W <timeout>`: Tiempo máximo de espera para una respuesta.
    - Interpretación: Pérdida de paquetes (`packet loss`) indica congestión o fallo en la ruta. Alta latencia (`rtt min/avg/max`) indica lentitud en la ruta o en el host de destino. Jitter (variación en la latencia) indica inestabilidad.
- **`traceroute` / `mtr`:**
    - Interpretación: Cada línea es un "salto" (normalmente un router). Los asteriscos (`*`) indican que no se recibió respuesta ICMP del salto (puede ser un firewall o un router que no responde a pings/traceroutes). Un aumento repentino de la latencia en un salto y en todos los subsiguientes indica un posible problema en ese salto o el enlace después de él. Pérdida de paquetes en un salto y en todos los subsiguientes (en `mtr`)

indica un problema en ese salto. Pérdida de paquetes solo en un salto intermedio pero no al final puede ser que ese router no priorice el tráfico ICMP.
    - `mtr --report <host>`: Modo reporte, útil para obtener estadísticas en un período.
- **`tcpdump`:** (Visto en 205.2) Filtrado por banderas TCP: `tcp[tcpflags] & (tcp-syn|tcp-ack) != 0` (captura SYN o ACK), `tcp[tcpflags] & tcp-fin != 0` (captura FIN), `tcp[tcpflags] & tcp-rst != 0` (captura RST). Permite ver si se inicia, establece, finaliza o reinicia una conexión.
- **`ss` / `netstat`:**
    - `ss -antup`: Muestra conexiones TCP/UDP en cualquier estado (LISTENING, ESTABLISHED, TIME-WAIT, CLOSE-WAIT) con direcciones numéricas, nombres de usuario/proceso.
    - Interpretación de estados TCP: `LISTEN` (servicio esperando conexiones), `ESTABLISHED` (conexión activa), `TIME-WAIT`, `CLOSE-WAIT` (estados durante el cierre de la conexión, pueden indicar problemas si hay muchos en un estado particular).
- **`ip` / `route`:**
    - `ip route get <ip_destino>`: Muestra la ruta específica que se usaría para alcanzar una IP de destino.
    - `ip route add <red/mascara> via <gateway> [dev <interfaz>]`: Añade una ruta temporal.
    - `ip route del <red/mascara>`: Elimina una ruta temporal.
- **`host` / `dig`:**
    - `dig +trace <hostname>`: Muestra la ruta de resolución DNS desde los servidores raíz.
    - `dig @<servidor_dns> <hostname>`: Consulta un servidor DNS específico.
    - `dig -x <ip>`: Consulta inversa (PTR).
- **Logs:**
    - `journalctl -f`: Seguir los logs del journal en tiempo real.
    - `journalctl -u <nombre_servicio>`: Logs de un servicio específico.
    - `journalctl -k`: Logs del kernel (`dmesg`).
    - Buscar en logs tradicionales como `/var/log/syslog`, `/var/log/messages`, `/var/log/auth.log` (Debian) o `/var/log/secure` (Red Hat) mensajes relacionados con red, firewall o fallos de servicio.

Diferencias Debian vs. Red Hat (Troubleshooting):

- **Logs:** Principalmente la ubicación y gestión de logs (Journald en systemd vs. archivos de texto tradicionales; rutas como `/var/log/syslog` vs. `/var/log/messages`/`secure`).

- **Servicios:** Nombres de servicios (ej: `apache2` vs. `httpd`, `networking.service` vs. `network.service`, `ufw` vs. `firewalld`) al usar `systemctl status <servicio>` o buscar en logs.
- Las herramientas de red de bajo nivel (`ping`, `ip`, `ss`, `tcpdump`, `host`, `dig`, `nc`, `traceroute`, `mtr`) son en su mayoría idénticas en sintaxis y funcionalidad.