109.1 Fundamentos de protocolos de Internet - Ejercicios

Nota: Estos ejercicios se centran en visualizar la configuración de red actual de tu sistema. Los resultados exactos (direcciones IP, nombres de interfaces) dependerán de tu configuración de red específica en la VM.

Ejercicio 9.1.1: Identificando Interfaces de Red y Direcciones IP/MAC

- **Objetivo:** Usar comandos modernos y antiguos para ver la configuración de tus interfaces de red.
- **Requisitos:** Acceso a la línea de comandos.
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Muestra la configuración con la herramienta moderna (`ip`):** Ejecuta `ip addr show`.
        - Identifica tus interfaces de red (ej: `lo`, `eth0`, `enpXsY`).
        - Para cada interfaz, busca la línea `link/ether` (es la dirección MAC) y las líneas `inet` (dirección IPv4) e `inet6` (dirección IPv6).
        - Busca la dirección de loopback (`127.0.0.1` para IPv4, `::1` para IPv6) en la interfaz `lo`.
    3. **Muestra la configuración con la herramienta antigua (`ifconfig`) (si está instalada):** Ejecuta `ifconfig`.
        - Si el comando no se encuentra, puedes intentar instalar el paquete `net-tools`: `sudo apt update && sudo apt install net-tools` (Debian/Ubuntu) o `sudo dnf check-update && sudo dnf install net-tools` (Red Hat/Fedora).
        - Observa la salida. La dirección MAC se muestra como `ether` o `HWaddr`. La dirección IP se muestra después de `inet` o `inet addr`. La máscara de subred se muestra como `netmask`.
        - Compara la salida con `ip addr show`.

Ejercicio 9.1.2: Viendo la Tabla de Enrutamiento y la Puerta de Enlace Predeterminada

- **Objetivo:** Determinar cómo tu sistema envía tráfico a otras redes y cuál es su puerta de enlace a Internet.
- **Requisitos:** Acceso a la línea de comandos. Tu VM debe estar conectada a una red con acceso a un router.
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Muestra la tabla de enrutamiento con `ip`:** Ejecuta `ip route show`.
        - Busca la línea que empieza con `default`. Esta línea define la ruta predeterminada (el "último recurso" para el tráfico que no conoce otra ruta específica).

    - La dirección IP después de `via` es la dirección de tu puerta de enlace predeterminada.
    - La interfaz después de `dev` es la interfaz de red por la que se envía el tráfico a la puerta de enlace.
3. **Muestra la tabla de enrutamiento con `netstat` (si está instalada):** Ejecuta `netstat -r`. La salida es similar a `ip route show`. Busca la línea con `default` o `0.0.0.0` en la columna `Destination`.

Ejercicio 9.1.3: Identificando Conexiones de Red y Puertos Abiertos

- **Objetivo:** Ver qué procesos tienen conexiones de red activas o están a la espera de conexiones (puertos a la escucha).
- **Requisitos:** Acceso a la línea de comandos. Privilegios de superusuario (`sudo`) para ver nombres de procesos para todos los sockets.
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Muestra sockets a la escucha (TCP/UDP) y los procesos asociados con `ss`:** Ejecuta `sudo ss -tulnp`.
        - `t`: TCP, `u`: UDP, `l`: Listening (a la escucha), `n`: Numeric (muestra puertos/direcciones numéricos), `p`: Processes (muestra el proceso propietario).
        - Busca puertos conocidos (ej: 22 para SSH, 80/443 si tienes un servidor web, 631 si CUPS escucha en red).
        - La columna `Local Address:Port` muestra la dirección IP local y el puerto. `*:22` significa que el servicio escucha en todas las interfaces en el puerto 22. `127.0.0.1:631` significa que solo escucha en la interfaz de loopback.
    3. **Muestra todas las conexiones y sockets a la escucha (TCP/UDP) con `ss`:** Ejecuta `sudo ss -antup`.
        - `a`: All (todos los estados - listening, established, closed, etc.).
        - Busca conexiones `ESTAB` (established) a otros hosts si tu sistema está activo.
    4. **Muestra sockets a la escucha (TCP/UDP) y procesos con `netstat` (si está instalada):** Ejecuta `sudo netstat -tulnp`. Compara la salida con `ss`.
    5. **Muestra todas las conexiones y sockets a la escucha (TCP/UDP) con `netstat` (si está instalada):** Ejecuta `sudo netstat -antup`. Compara con `ss`.
    6. **Nota:** `ss` generalmente arranca más rápido que `netstat` para listar muchas conexiones, ya que obtiene la información directamente del kernel.