

## Paquete de comandos de red net-tools

Durante muchos años se utilizaron estos comandos para auditar y configurar la red en Linux. Actualmente se consideran obsoletos y se recomienda el cambio a comandos más modernos. Ya no suelen venir por defecto en las nuevas distribuciones pero se pueden instalar con el paquete `net-tools`

### **ifconfig**

Administrar las interfaces de red.

### **netstat**

Muestra las conexiones de red, tablas de encaminamiento y estadísticas de tráfico.

### **route**

Administra las tablas de enrutamiento IP

### **tracpath / tracpath6**

Muestra el camino recorrido hasta llegar al destino indicado

### **traceroute / traceroute6**

Parecido a **tracpath** pero con más opciones. Puede requerir permisos de root

### **ping / ping6**

Envía un paquete ICMP para comprobar que el destino responde. En Linux no termina hasta que pulsemos CONTROL+C. A no ser que se use la opción **-c** que indica el número de paquetes a enviar.

Comandos obsoletos	Comandos equivalentes
arp	ip n (ip neighbor)
ifconfig	ip a (ip addr), ip link, ip -s (ip -stats)
netstat	ss, ip route (for netstat -r), ip -s link (for netstat -i), ip maddr (for netstat -g)
route	ip r (ip route)

## iproute2 (ip)

Reemplaza los comandos ifconfig, route, y arp. Además aporta otras muchas funciones. Sintaxis

**ip** [ OPCIONES ] **OBJETO** [ COMANDO [ ARGUMENTOS ] ]

## Objetos

- ▶ **link:** Para configurar los objetos físicos o lógicos de la red
- ▶ **address:** Manejo de direcciones asociadas a los diferentes dispositivos.
- ▶ **neighbour:** Administrar los enlaces de vecindad (ARP).
- ▶ **rule:** Ver las políticas de enrutado y cambiarlas.
- ▶ **route:** Ver las tablas de enrutado y cambiar las reglas de las tablas.
- ▶ **tunnel:** Administrar los túneles IP
- ▶ **maddr:** Ver las direcciones multienlace, sus propiedades y cambiarlas.
- ▶ **mroute:** Establecer, cambiar o borrar el enrutado multienlace.
- ▶ **monitor:** Monitorizar continuamente el estado de los dispositivos, direcciones y rutas

## Iproute2 (ip)

- ▶ **Des/activar interfaz:** `ip link set enp0s3 up/down`
- ▶ **Des/activar arp:** `ip link set dev enp0s3 arp on/off`
- ▶ **Ver Direcciones IP:** `ip addr show / ip -c a`
- ▶ **Añadir dirección IP:** `ip addr add 192.168.1.4/24 dev enp0s3`
- ▶ **Borrar dirección IP:** `ip addr del 192.168.1.4/24 dev enp0s3`
- ▶ **Ver tabla enrutamiento:** `ip route show`
- ▶ **Añadir ruta:** `ip route add 10.10.50.0/24 via 192.168.1.1 dev enp0s3`
- ▶ **Borrar ruta:** `ip route del 10.10.50.0/24`
- ▶ **Puerta de enlace:** `ip route add default via 192.168.1.1`

## Socket Statistics (ss)

Obtiene información sobre los sockets (internos y de red). Sin parámetros lista todas las conexiones actuales. Sintaxis

```
ss [options] [FILTER]
```

## Opciones

- ▶ **-t** Sólo conexiones TCP, **-u** las UDP
- ▶ **-l** Socket a la escucha
- ▶ **-p** Muestra el nombre y PID del proceso asociado a cada conexión
- ▶ **-s** Estadísticas resumidas
- ▶ **-n** No resolver los nombres, mostrar las IP's

## Filtros

`FILTRO := [state ESTADO-TCP] [exclude ESTADO-TCP] [EXPRESIÓN]`

Con **state** los sockets deben estar en: `ESTABLISHED`, `LISTENING`, `CLOSED`, `CONNECTED`, `TIME-WAIT`, etc..

Con **exclude** se excluirán los que estén en el estado indicado.

**EXPRESIÓN** se puede construir con:

- ▶ Los operadores **and** (por defecto), **or** y **not**.
- ▶ (origen y/o destino) `{src|dst} [IP[/prefijo]][:puerto]`
- ▶ (puerto origen/destino) `{dport|sport} {eq|neq|gt|ge|lt|le} [IP]:puerto`

Ejemplos:

```
ss state established '(sport = :http or sport = :https)' src 192.188.1.0/24
```

```
ss sport neq :21 and sport neq :https or not dst 198.133.8.0/24
```



## **/etc/hostname**

Fichero en el que se guarda el nombre del host. Se puede editar el fichero o utilizar el comando `hostname nuevo_nombre`. Con `-s` se consulta el nombre y con `-f` el nombre más el dominio

## **/etc/hosts**

Fichero para asociar nombres a IP's. Cada línea contiene una IP seguido por uno o varios nombres que se asociarán a dicha IP.

## **hostnamectl**

Comando del ecosistema Systemd para modificar el nombre de host y otros valores.

Opciones: `status` ver el estado, `set-hostname NAME` modificar el nombre, etc.



## **/etc/resolv.conf**

Fichero en el que tradicionalmente se han configurados la IP de los servidores DNS para consultar la resolución de nombres (sobre todo en internet)

## **/etc/nsswitch.conf**

Con este fichero se puede especificar el orden en el que se buscará información en una serie de fuentes de datos.

Para la resolución de nombres a IP's se puede consultar un servidor DNS o usar el fichero /etc/hosts, la entrada que indica cuál se consultará antes es:

```
hosts:      files dns
```

## **/etc/network/interfaces**

Fichero de configuración de las tarjetas de red en Debian.

```
allow-hotplug enp0s3  
iface enp0s3 inet dhcp
```

```
auto enp0s3  
iface enp0s3 inet static  
address 192.168.0.5  
netmask 255.255.255.0  
gateway 192.168.0.1
```

## **/etc/sysconfig/network-script/ifcfg-nombre\_interfaz**

Fichero de configuración de las tarjetas de red en Red Hat.

```
TYPE=Ethernet           # Tipo de interfaz
DEVICE=enp0s3           # Nombre de la interfaz
NM_CONTROLLED="no"      # Ignorado por NetworkManager
ONBOOT=yes              # Inicia al arrancar el Sistema
BOOTPROTO=none          # Usar configuración estática (dhcp)
HWADDR=01:0A:03:1F:67:13 # Dirección MAC
IPADDR= 192.168.0.5      # Dirección IP
NETMASK= 255.255.255.0   # Máscara de red
NETWORK= 192.168.0.0     # Dirección de red
GATEWAY= 192.168.0.1     # Puerta de enlace
```

## Características de IPv6

- ▶ **Utiliza 128 bits:** Admite 340 sextillones de IP's distintas. 670 mil billones por cada milímetro cuadrado del planeta tierra. 😊💧
- ▶ **Notación Hexadecimal:** Está representado por ocho grupos de cuatro dígitos en Hexadecimal (representan valores del 0 al 15, siendo el 10 la letra A y el 15 la F)
  - ✓ Los grupos se separan por el signo de dos puntos ( : )
  - ✓ Si hay varios ceros seguidos se pueden quitar (pero solo una vez) `:0000:0000:` = `::`
  - ✓ Los ceros a la izquierda se pueden quitar `:0001:000F:` = `:1:F:`
- ▶ **Autoconfigurable:** Puede asignarse un valor basándose en la MAC
- ▶ **Sin máscara de red:** La parte de red siempre son los cuatro primeros grupos y el resto es la parte de host
- ▶ **Más seguro:** Incorpora opciones sobre seguridad. IPsec está integrado y permite autenticar y cifrar los paquetes