

COMANDOS DE RED EN LINUX

Los comandos de red más usados son:

ifconfig

route

ping

traceroute

netstat

nslookup

host

arp

En linux, la mayoría de estos comandos se usan en modo administrador. Si ejecutamos la orden `sudo su`, solo tendremos que escribir la contraseña de administrador una vez.

COMANDOS DE RED EN LINUX

ifconfig → Da información sobre todas las tarjetas de red y ayuda a configurarlas, pero **esa configuración solo dura hasta que el ordenador se reinicia o se apaga**, para mantenerla de forma permanente hay que usar el configurador gráfico de xwindows (kde, gnome, etc) o editar a mano el archivo **/etc/network/interfaces**.

Si cometemos un error al modificar /etc/network/interfaces nada nos lo va a indicar, así que, hay que hacerlo con mucho cuidado

COMANDOS DE RED EN LINUX

Para pedir información de una tarjeta de red, como eth0, ejecutamos **ifconfig eth0**

```
# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:13:72:CC:EB:00
          inet addr:10.14.106.0  Bcast:10.14.107.255  Mask:255.255.252.0
          inet6 addr: fe80::213:72ff:fecc:eb00/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6853429 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2055296 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13573539098 (3.3 GiB)  TX bytes:401474390 (382.8 MiB)
          Interrupt:169
```

#

Type of
Media

IP
Address

Metrics on Transmission
and Reception of Data

MAC

Netmask

COMANDOS DE RED EN LINUX

Vamos a configurar la tarjeta de red **eth0** con estos datos:

ip → 192.168.1.100

Puerta de enlace → 192.168.1.1

Máscara de subred → 255.255.255.0

ifconfig **eth0** 192.168.1.100 **netmask** 255.255.255.0

MUY IMPORTANTE: En linux, la puerta de enlace se configura mediante el comando **route**

COMANDOS DE RED EN LINUX

Podemos activar la tarjeta de red, por ejemplo, eth0:

```
ifconfig eth0 up
```

Podemos desactivarla:

```
ifconfig eth0 down
```

Podemos ponerla en modo promiscuo (el modo favorito para hacer una auditoría y el de los delincuentes informáticos)

```
ifconfig eth0 – promisc
```

En este modo la tarjeta recibe todos los paquetes que circulan por la red, tanto lo que van dirigidos a ella como los que no.

COMANDOS DE RED EN LINUX

route → Sirve para ver, añadir o modificar las tablas de enrutado de nuestro sistema linux, pero **esa configuración solo dura hasta que el ordenador se reinicia o se apaga**, para mantenerla de forma permanente hay que usar el configurador gráfico de xwindows (kde, gnome, etc) o editar a mano el archivo **/etc/rc.local** aunque este archivo, esta cayendo en deshuso y desapareciendo en algunos sistemas como Ubuntu versión 18

192.168.1.10 → 1100 0000.1010 1000.0000 0001.0000 1010

255.255.255.0 → 1111 1111.1111 1111.1111 1111.0000 0000

Solo cojo los primeros 24 bits en binario, que es lo que indica la máscara con tantos unos. **Si los contamos, hay 24 números uno**

En linux se escribe abreviadamente: **192.168.1.10/24**

COMANDOS DE RED EN LINUX

Cuando queremos conectarnos a nuestro router para poder navegar, debemos modificar la tabla de enrutado, añadiendo la ruta hacia la puerta de enlace:

ip fija del ordenador **192.168.2.100/24**

Puerta de enlace del router: **192.168.1.1**

Tarjeta de red: **eth0** (**eth0= ethernet 0**)

add → opción para añadir una nueva ruta

-net → opción para indicar que vamos a cambiar una red

gw → ip de la puerta de enlace del router (**gw=gateway**)

dev → dispositivo (device). Se refiere a que tarjeta de red vamos a usar, porque podemos tener más de una tarjeta de red, o wifi.

route **add -net 192.168.2.0/24 gw 192.168.1.1 dev eth0**

COMANDOS DE RED EN LINUX

ping → Sirve para enviar paquetes de tipo **icmp** a la ip o a la web que queramos, y medir el tiempo que tardan en regresar. Usamos ping para comprobar si hay conexión entre nuestro ordenador y el que le digamos y cual es la calidad de esa conexión.

Los paquetes **icmp** son como una hormiga exploradora que va buscando el ordenador de destino y cuando lo encuentra, regresa al ordenador del que partió, a casa, estableciendo que ruta deben seguir los paquetes de datos para llegar a el.

COMANDOS DE RED EN LINUX

Perder muchos paquetes significa que hay problemas de conexión física, por un cable en mal estado, mal tiempo, etc.

Que los paquetes tarden mucho en llegar, indica saturación de la red, o del servidor, etc.

ejemplo: ping -c 5 www.google.com

Con -c 5 (c de count) solo mandamos 5 paquetes icmp

```
chris@ubuntu-GT70: ~  
chris@ubuntu-GT70:~$ ping -c 5 google.com  
PING google.com (173.194.33.0) 56(84) bytes of data.  
64 bytes from sea09s01-in-f0.1e100.net (173.194.33.0): icmp_seq=1 ttl=58 time=17.9 ms  
64 bytes from sea09s01-in-f0.1e100.net (173.194.33.0): icmp_seq=2 ttl=58 time=42.1 ms  
64 bytes from sea09s01-in-f0.1e100.net (173.194.33.0): icmp_seq=3 ttl=58 time=16.0 ms  
64 bytes from sea09s01-in-f0.1e100.net (173.194.33.0): icmp_seq=4 ttl=58 time=27.0 ms  
64 bytes from sea09s01-in-f0.1e100.net (173.194.33.0): icmp_seq=5 ttl=58 time=10.9 ms  
  
--- google.com ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4005ms  
rtt min/avg/max/mdev = 10.909/22.817/42.149/10.991 ms  
chris@ubuntu-GT70:~$
```

COMANDOS DE RED EN LINUX

traceroute → muestra por que servidores y ordenadores pasan los paquetes de datos con el ordenador de destino que yo le indique, mediante su ip o web

Ejemplo: **traceroute** www.google.es

```
bob@ubuntu-comp:/home$ traceroute www.google.com
traceroute to www.google.com (173.194.116.145), 30 hops max, 60 byte packets
 1 speedtouch.lan (192.168.1.1) 12.669 ms 11.902 ms 11.053 ms
 2 78.134.144.1-dsl.net.metronet.hr (78.134.144.1) 13.987 ms 15.648 ms 17.37
1 ms
 3 10.50.0.73 (10.50.0.73) 22.473 ms 23.213 ms 26.523 ms
 4 10.50.0.74 (10.50.0.74) 29.124 ms 30.102 ms 34.318 ms
 5 213.147.96.110 (213.147.96.110) 35.266 ms 38.136 ms 39.979 ms
 6 212.162.29.1 (212.162.29.1) 41.924 ms 36.542 ms 38.233 ms
 7 ae-2-3.bar1.Ljubljana1.Level3.net (4.69.151.233) 36.919 ms 13.695 ms 15.1
55 ms
 8 * * *
 9 * * *
10 ae-3-80.edge3.Frankfurt1.Level3.net (4.69.154.135) 81.414 ms ae-4-90.edge3.
Frankfurt1.Level3.net (4.69.154.199) 39.745 ms ae-1-60.edge3.Frankfurt1.Level3.
net (4.69.154.7) 42.889 ms
11 4.68.70.186 (4.68.70.186) 45.590 ms 48.088 ms 50.605 ms
12 209.85.240.64 (209.85.240.64) 65.602 ms 55.049 ms 57.458 ms
13 66.249.94.69 (66.249.94.69) 60.435 ms 23.370 ms 23.618 ms
14 173.194.116.145 (173.194.116.145) 24.013 ms 23.452 ms 23.585 ms
```

COMANDOS DE RED EN LINUX

netstat → sirve para comprobar el estado general de la red. Si tenemos muchas conexiones a la vez, más de 30 en un ordenador doméstico, es posible que hallan pirateado el ordenador, a distancia.

Con la opción **-at** vemos todas las conexiones (**a=all**) de tipo tcp (**t=tcp**)

```
rjujare@LinuxAndUbuntu:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:ipp           *:*                     LISTEN
tcp        0      0 LinuxAndUbuntu:domain  *:*                     LISTEN
tcp        0      0 192.168.182.128:53146   ec2-54-200-92-89.:https ESTABLISHED
tcp        0      0 192.168.182.128:53144   ec2-54-200-92-89.:https ESTABLISHED
tcp        0      0 192.168.182.128:53148   ec2-54-200-92-89.:https ESTABLISHED
tcp        0      0 192.168.182.128:58120   ec2-52-42-156-143:https TIME_WAIT
```

COMANDOS DE RED EN LINUX

nslookup → Sirve para comprobar si un dns funciona. Dispone de opciones para especificar si queremos comprobar zonas inversas, ftp, e-mail,etc

Con la opción **-type=a** (**a**= zona directa) comprobamos todas las zonas directas del dominio google.com para un servidor.

```
File Edit View Search Terminal Help
student@Comp9:~$ nslookup -type=a google.com
Server:          127.0.0.53
Address:         127.0.0.53#53

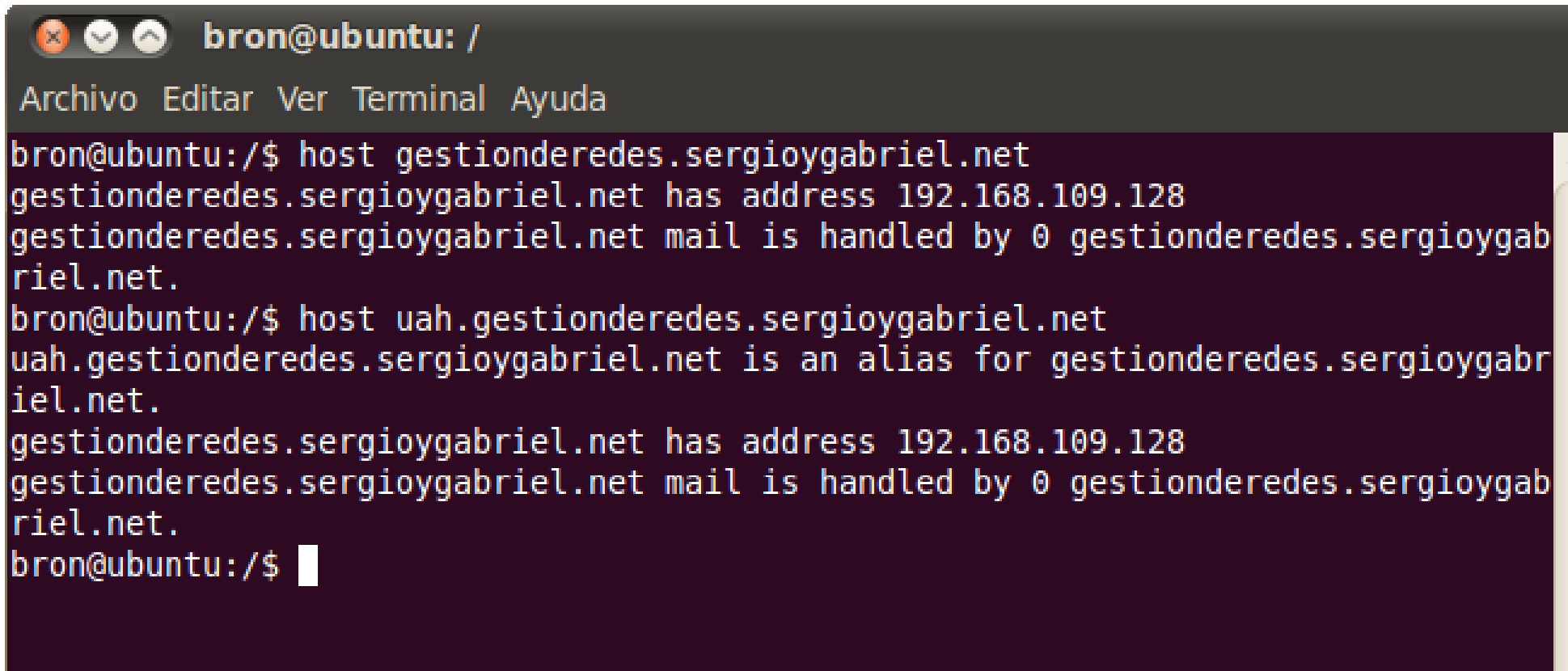
Non-authoritative answer:
Name:   google.com
Address: 172.217.166.174

student@Comp9:~$
```

COMANDOS DE RED EN LINUX

host → almacena la correspondencia entre una dirección ip y su dirección web, por ejemplo:

Es como un dns primitivo que guarda la correspondencia ip - web en el archivo `/etc/host`

A terminal window titled 'bron@ubuntu: /' with a menu bar containing 'Archivo', 'Editar', 'Ver', 'Terminal', and 'Ayuda'. The terminal shows the execution of the 'host' command twice. The first command is 'host gestionderedes.sergioygabriel.net', which returns the IP address 192.168.109.128 and states that mail is handled by 0 gestionderedes.sergioygabriel.net. The second command is 'host uah.gestionderedes.sergioygabriel.net', which returns that it is an alias for gestionderedes.sergioygabriel.net, followed by the same IP address and mail handling information. The prompt 'bron@ubuntu:/\$' is shown at the end of the output.

```
bron@ubuntu: /
Archivo  Editar  Ver  Terminal  Ayuda
bron@ubuntu:/$ host gestionderedes.sergioygabriel.net
gestionderedes.sergioygabriel.net has address 192.168.109.128
gestionderedes.sergioygabriel.net mail is handled by 0 gestionderedes.sergioygabriel.net.
bron@ubuntu:/$ host uah.gestionderedes.sergioygabriel.net
uah.gestionderedes.sergioygabriel.net is an alias for gestionderedes.sergioygabriel.net.
gestionderedes.sergioygabriel.net has address 192.168.109.128
gestionderedes.sergioygabriel.net mail is handled by 0 gestionderedes.sergioygabriel.net.
bron@ubuntu:/$
```

COMANDOS DE RED EN LINUX

Contenido de */etc/host*

```
solvetic@solvetic-Ubuntu: ~  
GNU nano 2.7.4 Archivo: /etc/hosts  
127.0.0.1    localhost  
127.0.1.1    solvetic-Ubuntu  
  
# The following lines are desirable for IPv6 capable hosts  
::1         ip6-localhost ip6-loopback  
fe00::0     ip6-localnet  
ff00::0     ip6-mcastprefix  
ff02::1     ip6-allnodes  
ff02::2     ip6-allrouters  
  
[ 9 líneas leídas ]  
^G Ver ayuda  ^O Guardar    ^W Buscar     ^K Cortar Tex ^J Justificar ^C Posición  
^X Salir      ^R Leer fich. ^_ Reemplazar  ^U Pegar txt  ^T Ortografía ^_ Ir a línea
```


COMANDOS DE RED EN LINUX

arp → sirve para gestionar la tabla arp, dicha tabla es muy importante pues establece la correspondencia entre la ip del ordenador y la dirección mac de la tarjeta de red.

La dirección mac de la tarjeta de red es única, no hay dos ordenadores en el mundo con la misma dirección.

Los hackers van a querer envenenar esta tabla para hacer ataques de tipo man in the middle

COMANDOS DE RED EN LINUX

Ejecutamos **arp -n** para ver la tabla arp

Con la opción **-n** le decimos que no use símbolos al mostrar los números, pues arp tiende por defecto a usar símbolos.

```
ubuntu@ubuntu:~$ arp -n
```

Address	HWtype	HWaddress	Flags	Mask	Iface
10.0.2.12	ether	08:00:27:f1:60:b7	C		enp0s3
10.0.2.3	ether	08:00:27:b8:e5:a2	C		enp0s8
10.0.2.13	ether	08:00:27:69:cb:49	C		enp0s8
10.0.2.7	ether	08:00:27:c2:69:6a	C		enp0s8
10.0.2.7	ether	08:00:27:c2:69:6a	C		enp0s3
10.0.2.1	ether	52:54:00:12:35:00	C		enp0s8
10.0.2.1	ether	52:54:00:12:35:00	C		enp0s3

```
ubuntu@ubuntu:~$
```