

Enrotamento básico con Linux

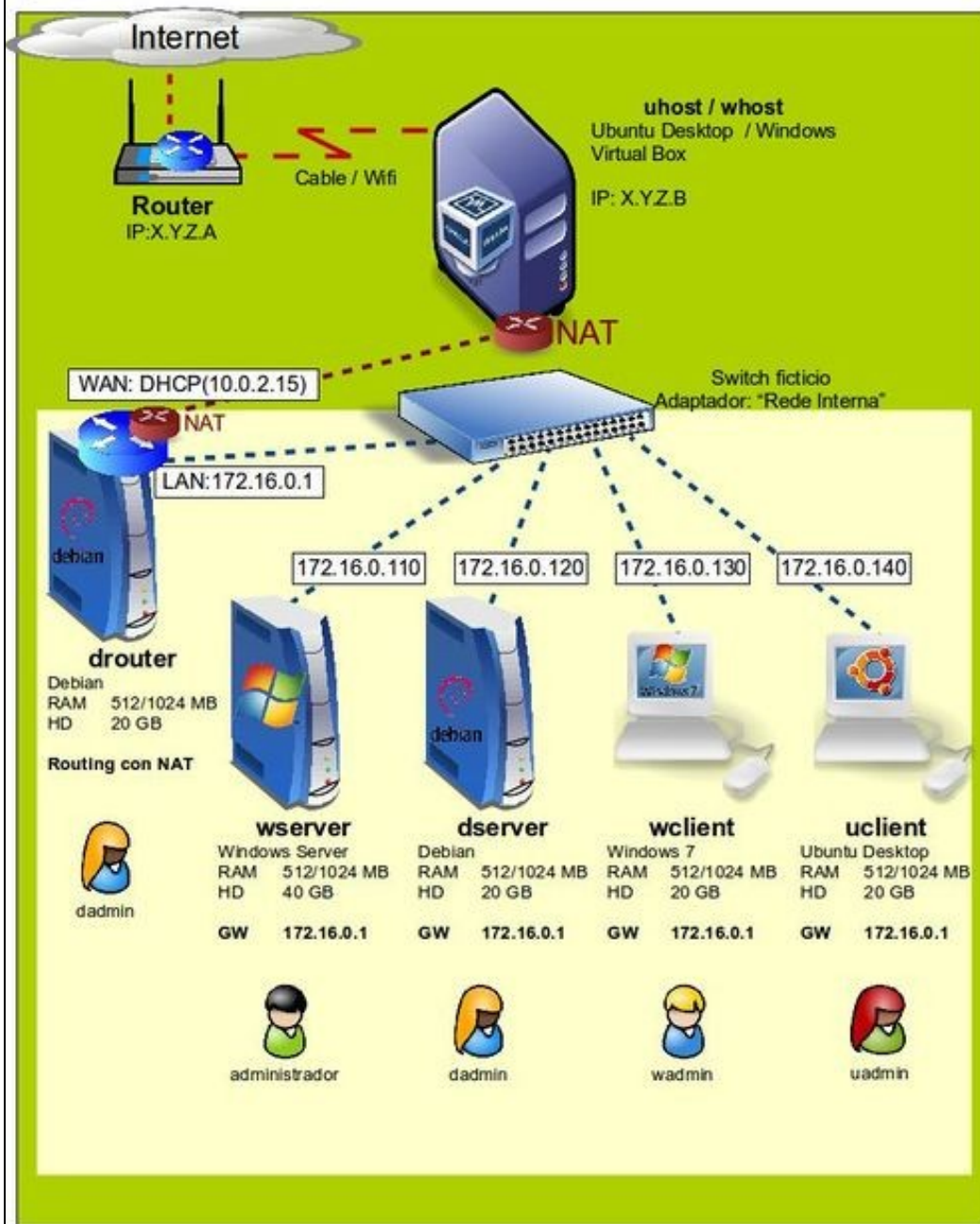
Sumario

- 1 Introducción
- 2 Preparativos da MV drouter
- 3 Preparativos S.O. drouter
- 4 Configuración do servizo de routing sobre NAT
- 5 Configurar a porta de enlace dun cliente da LAN
 - ◆ 5.1 Probas de conectividade

Introdución

- Imos crear un escenario que faga uso dun router, implantado cunha MV, que permite dar saída a internet ás demais MVs e ademais así cada MV só precisa ter un adaptador, conectado a unha rede interna.
- Preténdese instalar e configurar un router en Debian, de xeito que este faga de pasarela para os equipos da rede interna (*wserver*, *dserver*, *wclient*, *uclient*, etc).

Escenario 4.B: Routing con Debian



- Este equipo, como router, terá 2 interfaces:
 - ♦ **Interface LAN:** para poder comunicarse cos equipos da LAN e viceversa. A IP desta interface será a porta de enlace que deberá configurar todo cliente da LAN.
 - ♦ **Interface WAN:** co que este equipo se vai comunicar co exterior. Ademais cando se configure o servizo de routing vaise configurar NAT nesta interface, para que calquera solicitude de conexión co exterior que parta dos equipos da LAN sexa transformada cara o exterior como se fora este equipo (drouter) que a fixera. Ao recibir a resposta do exterior vaise encargar de enviarlle ao equipo da LAN que iniciou a conexión.



PODES CONSULTAR...

Para revisar e afondar no coñecemento sobre NAT pódese consultar:

- NAT da parte III do presente curso.
- Antes de comezar a implantar o escenario, obsérvase que só se vai configurar **drouter** e **uclient**, os demais equipos enténdese que o usuario sería quen de configuralos, pero irase facendo pouco a pouco cando se precisen.

Preparativos da MV drouter

- Antes de configurar o servizo de routing vaise configurar a MV que o implantará:
 - ♦ Clonar a MV Debian, que teña xa o servizo de ssh e o Webmin instalado.
 - ◊ Nome MV: **drouter**.
 - ♦ Facer unha instantánea.

• Red

Adaptador 1 Adaptador 2 Adaptador 3 Adaptador 4

☒ Habilitar adaptador de red

Conectado a: NAT

Nombre:

Avanzadas

Tipo de adaptador: Intel PRO/1000 MT Desktop (82540EM)

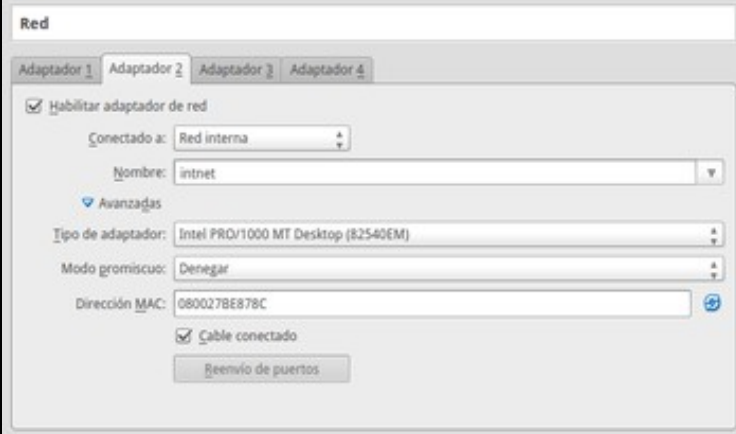
Modo promiscuo: Denegar

Dirección MAC: 080027A778D7

☒ Cable conectado

Reenvío de puertos

Configurar o adaptador 1 por NAT, e asegurarse de que o enderezo MAC non é o mesmo que o da MV da que se clonou.

- 

Configurar o adaptador 2 por **Rede Interna**, e asegurarse de que o enderezo MAC non é o mesmo que o da MV da que se clonou.

Preparativos S.O. drouter

- Antes de instalar o servizo de routing, configuraranse as interfaces de rede.

- Preparación de máquina drouter

```
root@dserver:/home/dadmin# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 08:00:27:a7:78:d7
          inet addr:192.168.1.120  Bcast:192.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::a00:27ff:fea7:78d7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:190 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1100 (1.0 KiB)  TX bytes:53309 (52.0 KiB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:be:87:8c
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:211 errors:0 dropped:0 overruns:0 frame:0
          TX packets:211 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:31696 (30.9 KiB)  TX bytes:31696 (30.9 KiB)
```

Agora no sistema aparecerán dúas interfaces de rede, co nome *eth0* e *eth1*. Podemos velas co comando **ifconfig -a**, e nos fixaremos nas súas direccións MAC para saber cal é a interface conectada en modo interna e cal é a NAT. Neste caso, *eth0* é a interface en modo NAT e *eth1* está en rede interna.

```
GNU nano 2.2.6  Ficheiro: /etc/network/interfaces  Modificado

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp

auto eth1
iface eth1 inet static
    address 172.16.0.1
    netmask 255.255.0.0
```

Debemos configurar a interface NAT de forma automática por DHCP e a que está en rede interna coa dirección 172.16.0.1. Podemos facelo de calquera das formas xa vistas no curso, na imaxe móstrase como facelo utilizando o ficheiro de configuración das interfaces en Debian.

```
root@dserver:/home/dadmin# service networking restart
root@dserver:/home/dadmin# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a7:78:d7
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea7:78d7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:17 errors:0 dropped:0 overruns:0 frame:0
          TX packets:325 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2488 (2.4 KiB)  TX bytes:93243 (91.0 KiB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:be:87:8c
          inet addr:172.16.0.1  Bcast:172.16.255.255  Mask:255.255.0.0
          inet6 addr: fe80::a00:27ff:febe:878c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:53 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:24449 (23.8 KiB)
```

Tras gardar os cambios no ficheiro, reiniciamos o servizo de rede para aplicar a nova configuración. Comprobamos co comando **ifconfig** que as interfaces están configuradas cos novos datos.

```
root@dserver:/home/dadmin# ping -c 2 www.google.es
PING www.google.es (64.233.166.94) 56(84) bytes of data:
64 bytes from wm-in-f94.1e100.net (64.233.166.94): icmp_seq=1 ttl=63 time=47.9 ms
64 bytes from wm-in-f94.1e100.net (64.233.166.94): icmp_seq=2 ttl=63 time=39.3 ms

--- www.google.es ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 100ms
rtt min/avg/max/mdev = 39.361/43.647/47.933/4.286 ms
root@dserver:/home/dadmin#
```

Comprobamos con *ping* que a máquina ten conexión con *www.google.es*.

Configuración do servizo de routing sobre NAT

- En Linux, o protocolo NAT configúrase como unha regra dentro do servizo do Firewall. Para poder configurar este servizo de forma sinxela, instalaremos a aplicación **shorewall**. Webmin inclúe un módulo que nos permitirá configurar de forma gráfica todo o comportamento do Firewall e do procolo NAT.

- Instalación do servizo de routing con NAT



Utilizamos o módulo de **Paquetes de software** da categoría **Sistema** do Webmin para instalar o paquete **shorewall**.



Unha vez instalado o paquete, utilizamos a opción de **Refrescar módulos** para que se mova o módulo de xestión de shorewall á categoría que lle corresponde.



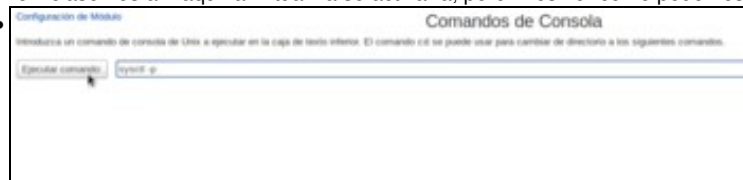
En primeiro lugar imos activar o servizo de enrutamento. Dentro da categoría de **Rede** imos ao apartado de **Configuración de rede** e picamos sobre **Enrutamento e portas de enlace**.



Activamos a opción de **Actuar como router** e gardamos os cambios.



Na páxina principal do módulo de configuración da rede, picamos no botón de **Aplicar configuración** para activar os cambios realizados. Pero neste caso (debido a un *bug* do webmin) con isto non conseguimos realmente activar xa o servizo de routeo na máquina. Se reiniciásemos a máquina virtual xa se activaría, pero imos ver como podemos activar o cambio sen ter que reiniciar.



No propio webmin, imos á ferramenta de **Comandos de consola** (dentro do apartado de **Outros**) e introducimos o comando: **sysctl -p**. Picamos no botón de Executar comando para executar este comando no sistema.



Vemos o resultado do comando, que xa activa o enrutamento.



Zonas de Red

Las zonas, vistas en esta página, representan diferentes redes, accedidas desde la consola, no obstante, estas entidades no tienen ningún efecto sobre el catálogo de dispositivos, simplemente definen nombres y descripciones de zonas. Ninguna no es la verdadera categoría de red.

[Cargar una nueva zona de red](#)

Presione este botón para editar manualmente la forma de cómo se ven las zonas de la consola, desde donde guardamos las entradas de zona.

[Ayuda en Formato Manualmente](#)

[Volver a la lista de zonas](#)

[illegible][illegible]

Interfaces de Red

En esta página, puedes crear, editar y configurar una o más interfaces de red del sistema que quieres que WinBox gestione, asociables con la zona de la que están conectados. La mayoría de interfaces de red no se gestionan.

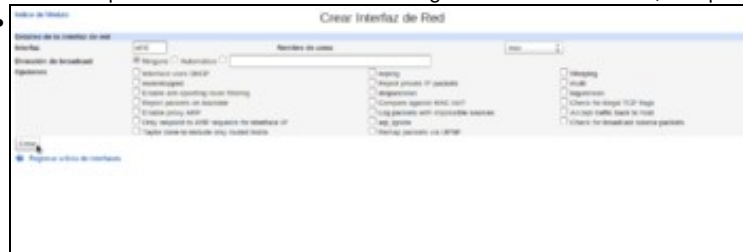
Ver de las diferentes categorías interfaces de red.

[Agregar una nueva interfaz de red](#)

[Ayuda de la Interfaz Manualmente...](#)

Regístrate y más de WinBox

Veremos que non hai definida no firewall ningunha interface de rede, así que agregamos unha.



Para crear unha interface de rede no firewall, debemos introducir o nome dunha das interfaces de rede do equipo (que será do tipo *eth0*, *eth1*, *wlan0*, etc.) e seleccionar á zona de rede coa que está conectada esta interface. Por exemplo, no noso caso a interface *eth0* está conectada á zona *wan*. Creamos a interface...



e da mesma maneira engadiríamos a interface *eth1*, neste caso conectada á zona *lan*. Como *router* só ten dúas interfaces de rede, xa están todas definidas e regresamos á lista de táboas.



Para rematar, temos que definir as políticas por defecto do firewall, que son os criterios básicos que o firewall utiliza para decidir se acepta ou rexeita as conexións. Estas políticas poden ser refinadas de forma máis específica mediante *reglas*, en función das máquinas de orixe ou de destino das conexións ou o protocolo que se utilicen na mesma, pero neste curso non imos afondar máis na xestión do firewall.



Vemos que non hai ningunha política definida, así que imos crear unha nova.



Basicamente, para definir unha política deberemos indicar a zona de orixe e de destino dos paquetes aos que se aplicará a política, e a decisión a aplicar que fundamentalmente pode ser **Aceptar** (*ACCEPT*) ou **Borrar** (*DROP*). Para simplificar todo o posible a configuración do firewall, imos crear unha política que acepte todas as conexións, veñan da zona que veñan e vaian á zona que vaian. Isto non sería unha configuración desexable nun caso real, xa que facilitaría ataques externos á nosa rede, pero como se dixo non se pretende afondar na xestión do firewall.



Vemos na imaxe a política creada. Regresamos a lista de táboas, para iniciar xa o servizo do firewall.



Coa configuración establecida xa podemos iniciar o cortafuegos, picando sobre o botón.



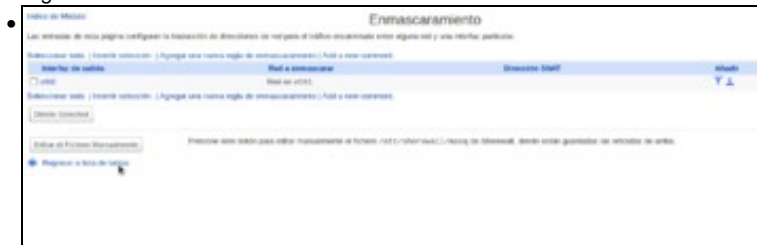
Saberemos que o servizo está iniciado porque os botóns da parte inferior da páxina cambian, para mostrar opcións que só están dispoñibles cando o firewall está en execución. Quédanos por ver como utilizar este módulo para configurar o protocolo NAT. Picaremos na opción de **Enmascaramento**. Dáselle este nome ao protocolo NAT porque o que fai é *enmascarar* as direccións dunha rede privada a través da dirección IP pública do router.



Veremos que non hai ningunha regra de enmascaramento creada, así que engadimos unha nova.



O importante é seleccionar a interface de saída, que é a que ten a dirección IP pública es está conectada á rede WAN (que neste caso é **eth0**) e marcar como rede a enmascarar a que está conectada á interface que ten a dirección IP privada (neste caso **eth1**). Creamos a regra.



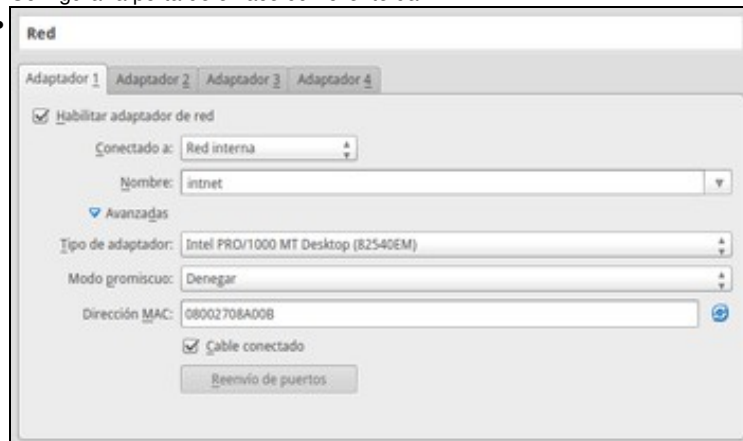
Podemos ver a regra creada, que enmascara a rede conectada a *eth1* sobre a interface *eth0*. Con isto xa estamos proporcionando a información necesaria para facer NAT. Regresamos á lista de táboas...



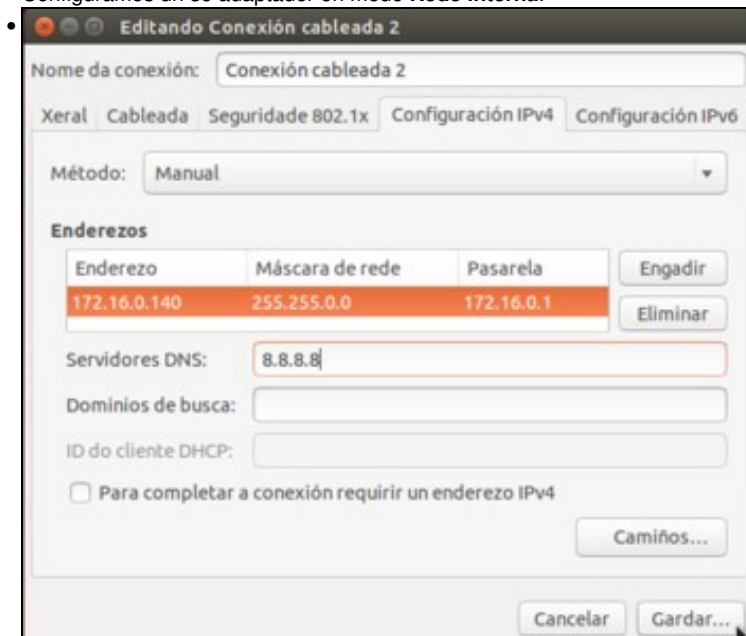
e tan só temos que aplicar a configuración.

Configurar a porta de enlace dun cliente da LAN

- Para mostrar a configuración da porta de enlace nun cliente da LAN vaise escoller a MV **uclient**; nos demais equipos a filosofía sería a mesma.
- Configurar a porta de enlace dun cliente da LAN



Configuramos un só adaptador en modo **Rede interna**.



Configuramos a IP segundo o escenario: 172.16.0.140/16, porta de enlace 172.16.0.1 (*drouter*, pola interface LAN).

```
uadmin@uclient:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:08:a0:0b
          inet addr:172.16.0.140  Bcast:172.16.255.255  Mask:255.255.0.0
          inet6 addr: fe80::a00:27ff:fe08:a00b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1095 errors:0 dropped:0 overruns:0 frame:0
          TX packets:616 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1012586 (1.0 MB)  TX bytes:67813 (67.8 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:474 errors:0 dropped:0 overruns:0 frame:0
          TX packets:474 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:55040 (55.0 KB)  TX bytes:55040 (55.0 KB)
```

Con **ifconfig** comprobamos que a configuración establecida está activada. De non estalo, desconectamos a tarxeta de rede e conectámola de novo.

Probas de conectividade

- Para comprobar que todo está correcto pódense facer pings entre os distintos equipos do escenario.
- Neste caso vanse amosar exemplos de conectividade realizados dende **uclient** e que en moitos casos teñen que atravesar **drouter**.

• Probas de conectividade

```
uadmin@uclient:~$ ping -c 1 172.16.0.1
PING 172.16.0.1 (172.16.0.1) 56(84) bytes of data.
64 bytes from 172.16.0.1: icmp_seq=1 ttl=64 time=0.703 ms

--- 172.16.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/ndev = 0.703/0.703/0.703/0.000 ms
uadmin@uclient:~$ ping -c 1 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=61 time=1.42 ms

--- 10.0.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/ndev = 1.424/1.424/1.424/0.000 ms
uadmin@uclient:~$ ping -c 1 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=61 time=2.91 ms

--- 10.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/ndev = 2.912/2.912/2.912/0.000 ms
uadmin@uclient:~$ ping -c 1 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=61 time=17.1 ms

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/ndev = 17.190/17.190/17.190/0.000 ms
uadmin@uclient:~$ ping -c 1 www.google.es
PING www.google.es (64.233.167.94) 56(84) bytes of data.
64 bytes from wl-in-f94.1e100.net (64.233.167.94): icmp_seq=1 ttl=61 time=49.5 ms

--- www.google.es ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/ndev = 49.577/49.577/49.577/0.000 ms
```

A imaxe amos o resultado de facer ping a *drouter*, á dirección IP do host, á dirección IP do router físico que da a saída a Internet, a unha dirección IP en Internet (8.8.8.8) e a un servidor de Internet polo seu nome (*www.google.es*), obtendo resposta en todos os casos. A opción **-c 1** indica que faga un só faga unha solicitude de eco.

```
uadmin@uclient:~$ sudo apt-get install traceroute
[sudo] password for uadmin:
Lendo as listas de paquetes... Feito
Construindo a árbore de dependencias
Lendo a información do estado... Feito
Os seguintes paquetes NOVOS hanse instalar:
  traceroute
0 anovados, 1 instalados, Vanse retirar 0 e deixar 73 sen anovar.
Ten que recibir 45,0 kB de arquivos.
Despois desta operación ocuparanse 176 kB de disco adicionais.
AVISO: Non se poden autenticar os seguintes paquetes!
  traceroute
Instalar estes paquetes sen verificación? [s/N] s
```

Se queremos comprobar que os paquetes están pasando realmente por *drouter* podemos instalar o paquete **traceroute**, que mostra os routers polos que pasa un paquete para chegar a un destino determinado.

```
uadmin@uclient:~$ traceroute -n 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1 172.16.0.1  0.650 ms  0.649 ms  0.507 ms
 2 10.0.2.2  0.907 ms  0.905 ms  1.195 ms
 3 * * *
 4 87.235.0.10 11.673 ms 13.271 ms 13.089 ms
 5 172.29.56.110 12.957 ms 172.29.56.106 12.731 ms 12.378 ms
 6 172.29.56.109 12.262 ms 11.466 ms 11.744 ms
 7 * * *
 8 212.166.147.46 25.109 ms 17.468 ms 16.367 ms
 9 72.14.232.189 21.237 ms 72.14.234.233 21.094 ms 72.14.232.189 21.258 ms
10 216.239.48.221 22.747 ms 216.239.48.249 22.684 ms 216.239.48.87 22.454 ms
11 8.8.8.8 22.110 ms 18.254 ms 20.182 ms
uadmin@uclient:~$
```

Na imaxe vemos o resultado de executar **traceroute -n 8.8.8.8**, que mostra os routers intermedios (a opción **-n** é para que só mostre as direccións IP deses routers) ata chegar ao equipo coa dirección 8.8.8.8. Vemos marcado como pasa por *drouter* en primeiro lugar e logo polo router físico que da saída a Internet.

```
C:\Windows\system32\cmd.exe
C:\Users\uadmin>tracert -d 8.8.8.8

Traza a 8.8.8.8 sobre caminos de 30 saltos como máximo.

 1  <1 ms      <1 ms      <1 ms      172.16.0.1
 2  1 ms       <1 ms      <1 ms      10.0.2.2
 3  *          *          *          Tiempo de espera agotado para esta solicitud.
 4  6 ms       5 ms       4 ms       87.235.0.10
 5  6 ms       14 ms      5 ms       172.29.56.110
 6  *          6 ms       5 ms       172.29.56.109
 7  *          17 ms      16 ms      212.166.147.46
 8  17 ms      17 ms      16 ms      212.166.147.46
 9  28 ms      28 ms      21 ms      72.14.232.189
10  28 ms      28 ms      21 ms      216.239.48.133
11  17 ms      17 ms      17 ms      8.8.8.8

Traza completa.
C:\Users\uadmin>
```

Esta imaxe mostra o comando equivalente en *wclient*, que sería **tracert -d 8.8.8.8**. Como vemos, tamén se mostra como os paquetes pasan por *drouter* e polo router de saída a Internet.