



## Introducción a Herramientas de Red

# Linux en Red

Las máquinas conectadas a la red ofrecen enormes beneficios, pero añaden responsabilidades. Desde el momento en que conectamos nuestra máquina a la red debemos no solo conocer todo acerca de nuestra máquina, si no también sobre la forma en que ésta se comunica con el mundo exterior.

Las herramientas estándar de Linux nos pueden ayudar. **POR NICO LUMMA**

Un ordenador sin conexión al mundo exterior parece un paso atrás. Si bien las distribuciones de Linux de hoy en día soportan normalmente la instalación de componentes de red, los administradores han de asumir su parte de responsabilidad y, en algunos casos, su formación puede no haber cubierto técnicas de redes. En estos casos lo lógico es obtener el mayor conocimiento posible sobre lo que necesita un ordenador para conectarse a una red.

Una red puede no responder o una máquina aislada (por ejemplo un servidor Web) puede no estar accesible. Los principales distribuidores de Linux disponen de herramientas que controlan estas situaciones.

## Fundamentos de redes

El componente básico de Internet y de numerosos sistemas de red local es el TCP/IP. Es una combinación del Protocolo de Control de Transmisiones y el Protocolo de Internet, especificando como se comunican e intercambian datos los ordenadores en una red.

### GLOSARIO

**DNS:** los servidores DNS contienen bases de datos que se pueden usar para emparejar direcciones IP con nombres de Internet (y viceversa). Buscan en sus bases de datos para responder consultas enviadas por buscadores y aplicaciones de Internet desconocidas por sus usuarios. Un usuario que escribe *www.google.com* está realmente formulando una consulta cuya respuesta es la dirección IP 216.239.39.99. Es con esta dirección con el que el buscador abrirá realmente la conexión.

Como un navegador Web no necesita saber si la información se transmite mediante componentes inalámbricos o mediante líneas FDDI, ni las líneas FDDI necesitan saber si los bytes que transporta corresponden a ficheros HTML, MP3s o vídeos, los expertos en redes utilizan un modelo basado en capas para describir las redes de ordenadores. Al margen de que cada capa se apoya en la capa subyacente, las capas son independientes entre sí.

La capa aplicación, como su propio nombre indica, define como las aplicaciones como buscadores o programas de correo hablan con servidores Web o de correo. El medio por el cual ocurre esto depende de cada aplicación. Por ejemplo, el Protocolo de Transferencia de Hipertexto, HTTP, es usado para Webs, mientras que el Protocolo de Transferencia de Ficheros, FTP, es usado habitualmente para la descarga de ficheros.

La capa de transporte está por debajo de la capa de aplicaciones. Esta capa establece las conexiones entre ordenadores, permitiéndoles el intercambio de datos. TCP proporciona un canal de garantía (para protocolos de aplicaciones como HTTP, SSH, POP o SMTP), asegurando que los bloques de información que fallen son retransmitidos. El Protocolo Datagram (UDP) es otro protocolo importante a este nivel que puede transmitir bloques de información, pero con pérdidas de paquetes. Este protocolo es

el usado, por ejemplo, por los canales de Real Audio. En la siguiente capa es donde las cosas empiezan a ponerse interesantes. Aquí es donde los paquetes de información (independientemente de su contenido) son puestos en un cable e intentan buscar la mejor ruta a su destino. Cada bloque contiene la dirección de su remitente y de su receptor. Cuando se sirve una página, los paquetes de información pueden utilizar rutas distintas. Tras aceptar los paquetes, el receptor debe asegurarse de que los paquetes se pueden reorganizar en el orden correcto. Al margen del propio Protocolo de Internet, la capa de red contiene otros protocolos como el Protocolo de Control de Mensajes de Internet, ICMP, para el control de mensajes (por ejemplo, de error), el Protocolo de determinación de Direcciones, ARP, que confronta direcciones IP con direcciones de hardware (MAC) y, su homólogo, el Protocolo de Inversión de Direcciones Determinadas (RARP).

La capa inferior del modelo OSI es la capa Física. A este nivel estamos intere-

```
Linux:~ # ip addr
1: lo: <LOOPBACK,UP> mtu 16436 qdisc noqueue
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
      inet6 ::1/128 scope host
2: eth0: <BROADCAST,MULTICAST,NOLOOPBACK,UP> mtu 1500 qdisc pfifo_fast q
   link/ether 00:0a:c6:42:07:c4 brd ff:ff:ff:ff:ff:ff
   inet 192.168.1.245/24 brd 192.168.1.255 scope global eth0
      inet6 fe80::20a:c6ff:fe42:7c4/64 scope link
3: sit0: <NONE> mtu 1400 qdisc noop
   link/sit 0.0.0.0 brd 0.0.0.0
Linux:~ #
```

Figura 1: Los numerosos datos de obtenidos por "ip addr" incluyen información crítica de la dirección IP actual e "inet" indica la máscara de red.

```
linux:~ #
linux:~ #
linux:~ # ip route
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.245
default via 192.168.1.1 dev eth0
linux:~ #
```

Figura 2: "ip route" proporciona información IP más clara.

```
linux:~ # ping -c 5 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data:
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.216 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.218 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.232 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.216 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=0.216 ms

--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 0.216/0.219/0.232/0.017 ms
linux:~ #
```

Figura 3: La máquina receptora, 192.168.1.1, respondió a los 5 pings enviados.

sados en la transmisión de bits y la estandarización de de la negociación de protocolos con interfaces eléctricas, mecánicas y de señalización. Esto incluye los estándares RS-232 y X.21.

Los componentes de red son identificados mediante su dirección IP. TCP puede retransmitir paquetes asegurando que el receptor dispone del conjunto completo de paquetes. El protocolo de aplicaciones en el nivel superior depende de este servicio. Sin un conocimiento básico de estas capas, muchas de las herramientas de red no tendrían mucho sentido.

## Comprobación del estado

Antes de comenzar a analizar el tráfico de red es importante comprobar que nuestro ordenador esté utilizando la red adecuadamente.

Dicho de forma sencilla, cada máquina necesita una dirección IP única para ser capaz de comunicarse con otras máquinas en la red. La dirección de la puerta de enlace permite que los paquetes de datos destinados al exterior abandonen la red local.

El comando *ip* proporciona detalles de la configuración actual. Los sistemas

antiguos puede que solo tengan los comandos *ipconfig* y *route*, que proporcionan la misma información, pero en un formato distinto. Es posible que si el sistema no puede localizar estos comandos sea por que estén instalados en */sbin*, que no es una ruta habitual de búsqueda. Si éste es el caso, simplemente debemos añadir la ruta completa (por ejemplo, */sbin/ip*).

La opción *addr* indica al comando *ip* que debe mostrar los detalles de nuestro adaptador de red. Si queremos indicar el número de adaptador debemos incluir la línea *eth0* para la primera tarjeta de red, *eth1* para la segunda y así sucesivamente. Esto mostrará nuestra dirección IP (192.168.1.245 en la Figura 1), la máscara de red (/24), la dirección de difusión (192.168.1.255) y el nombre del interfaz de la red, *eth0*. Los datos obtenidos con el comando *ip route* son más sencillos de leer (ver Figura 2). La primera línea muestra la red (la dirección de la red en nuestro ejemplo es 192.168.1.1), la máscara de la red /24, el interfaz de la red y finalmente el origen de los datos (*src* significa origen), o sea, la dirección IP (192.168.1.245). La segunda línea muestra la puerta de

enlace por defecto 192.168.1.1. Si aquí no aparece información crítica como la dirección IP o la puerta de enlace puede explicar que nuestro ordenador no se comporte en la red como debiese. Si éste es el caso, debemos ejecutar la herramienta de configuración de nuestro distribución (por ejemplo YaST for Suse) y comprobar nuestra configuración.

## Ping-Pong

*ping* es una herramienta de análisis de redes muy simple y tremendamente práctica. Transmite un paquete de datos ICMP desde nuestro ordenador a un objetivo, mostrando el tiempo que la respuesta tarda en llegar devuelta a nuestro ordenador (suponiendo que el receptor responda). La parte final nos muestra el número de paquetes ping transmitidos (cinco en la Figura 3), cuantas respuestas obtuvimos (cinco de nuevo) y cuanto tardo el proceso (4002 milisegundos). Si algún paquete se pierde es mostrado en la sección *packet loss*. Si el receptor no se puede alcanzar no ocurre nada durante un rato, puesto que ping espera respuestas. *ping nombrehost* lanza un ping hacia el receptor hasta que presionamos [Ctrl-c]. En su

```
linux:~ # traceroute linux-magazine.com
traceroute to linux-magazine.com (62.245.157.219), 30 hops max, 40 byte packets
 1 10.13.128.1  9.389 ms  8.458 ms  7.684 ms
 2  oldh-t2can1-a-ge-wan52-124.inet.ntli.com (88.5.164.97)  14.933 ms  12.084 ms  7.035 ms
 3  mant-t2core-a-ge-wan64.inet.ntli.com (213.104.242.53)  12.293 ms  9.756 ms  10.149 ms
 4  man-bb-a-so-230-0.inet.ntli.com (62.253.184.57)  14.359 ms  8.733 ms  7.959 ms
 5  lee-bb-b-so-700-0.inet.ntli.com (62.253.185.194)  14.047 ms  9.968 ms  9.999 ms
 6  lee-bb-a-ae0-0.inet.ntli.com (62.253.187.185)  13.009 ms  8.624 ms  9.302 ms
 7  pop-bb-b-so-100-0.inet.ntli.com (62.253.185.238)  20.918 ms  23.011 ms  14.915 ms
 8  tele-ic-1-so-000-0.inet.ntli.com (62.253.185.82)  28.653 ms  39.346 ms  29.861 ms
 9  LINX.LON-1-eth110.uk.lanbdanet.net (195.66.224.99)  17.072 ms  24.408 ms  26.059 ms
10  F-2-pos310.de.lanbdanet.net (217.71.96.93)  35.853 ms  39.630 ms  34.914 ms
11  S-3-atn030-733.de.lanbdanet.net (217.71.105.6)  49.997 ms  37.457 ms  39.965 ms
12  M-4-atn010-732.de.lanbdanet.net (217.71.105.122)  47.006 ms  41.662 ms  53.231 ms
13  MNet-M.de.lanbdanet.net (217.71.100.46)  52.950 ms  40.073 ms  38.612 ms
14  ntn-gu.m-online.net (212.18.3.132)  54.255 ms  59.496 ms  51.367 ms
15  raphael.ntn-gmbh.de (62.245.157.254)  48.469 ms  62.375 ms  42.630 ms
16  * * * * *
17  * * * * *
18  * * * * *
19  * * * * *
20  * * * * *
21  * * * * *
22  * * * * *
23  * * * * *
24  * * * * *
25  * * * * *
26  * * * * *
27  * * * * *
```

Figura 4: "traceroute" muestra la ruta hasta "linux-magazine.com".

```
linux:~ # mtr Matt's traceroute [u0.52]
Thu Mar  4 17:08:14 2004
Keys: D - Display mode  R - Restart statistics  Q - Quit
          Packets
Hostname  %Loss  Rcv  Snt  Last  Best  Avg  Worst
 1. 10.13.128.1  0%  3  3  7  7  8  8
 2. oldh-t2can1-a-ge-wan52-124.i  0%  3  3  7  7  7  8
 3. mant-t2core-a-ge-wan64.inet.  0%  3  3  7  7  16  33
 4. man-bb-a-so-230-0.inet.ntli.c  0%  3  3  7  7  8  9
 5. lee-bb-b-so-700-0.inet.ntli.c  0%  3  3  9  9  11  13
 6. lee-bb-a-ae0-0.inet.ntli.com  0%  3  3  8  8  8  9
 7. pop-bb-b-so-100-0.inet.ntli.c  0%  3  3  15  14  14  15
 8. tele-ic-1-so-000-0.inet.ntli.  0%  3  3  63  37  53  63
 9. LINX.LON-1-eth110.uk.lanbdan  0%  3  3  14  14  15  16
10. F-2-pos310.de.lanbdanet.net  0%  3  3  34  34  34  35
11. S-3-atn030-733.de.lanbdanet.  0%  3  3  38  38  41  46
12. M-4-atn010-732.de.lanbdanet.  0%  2  2  43  43  43  43
13. MNet-M.de.lanbdanet.net  0%  2  2  39  38  39  39
14. ntn-gu.m-online.net  0%  2  2  42  42  43  43
15. raphael.ntn-gmbh.de  0%  2  2  44  43  43  44
16. www.linux-magazine.com  0%  2  2  295  56  175  295
```

Figura 5: "mtr" combina los resultados de "traceroute" y de "ping".

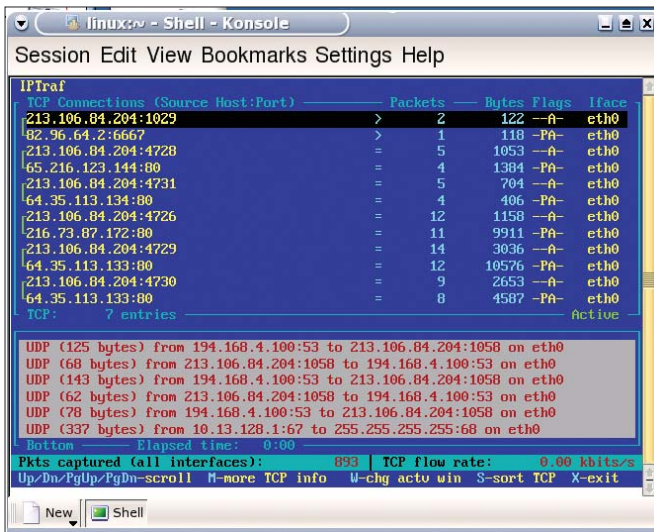


Figura 7: ¿Cuántos paquetes van y vienen desde qué dirección?

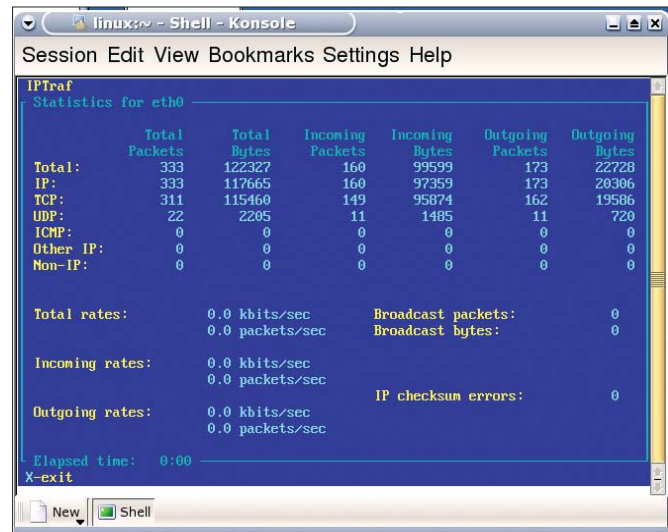


Figura 8: "iptraf" proporciona estadísticas de red detalladas.

lugar podemos especificar `ping -c 10 nombredelhost` para transmitir solo 10 pings.

## Rutas

Si bien `ping` simplemente nos informa de la respuesta de nuestro objetivo, `traceroute` (normalmente: `/usr/sbin/traceroute`) nos indica la ruta que los paquetes de datos han seguida hasta la máquina de destino (ver Figura 4). Los asteriscos (\*\*\*) indican un error en la ruta o que un cortafuegos no ha permitido el paso a este tipo de paquetes IP. Por cierto, podemos especificar la opción `-n` con el fin de no mostrar el nombre de equipo. `mtr hostdestino` (normalmente: `/usr/sbin/mtr`) nos proporciona una imagen clara (ver Figura 5) de por dónde pasan nuestros paquetes mientras no presionamos [q]. La herramienta descubre que ocurre con los paquetes de datos en cada cambio en la ruta. Por tanto, `mtr` puede ser considerado como una combinación de `ping` y `traceroute`.

```
mtr -c 10 -report
<I>hostdestino<I>
```

Indica a `mtr` que deje de transmitir tras 10 pings y luego informe de sus hallazgos.

La columna HOST indica exactamente donde está el paquete de datos; LOSS indica el porcentaje de paquetes perdidos; RCVD y SENT informan del número de paquetes que fueron recibidos y enviados; y las columnas BEST, AVG y WORST indican cuanto tiempo tardaron los paquetes.

## Para mayor precisión...

... prueba `tcpdump`, la herramienta de análisis de redes más versátil que existe. La mayoría de las distribuciones nos proporcionarán un paquete listo para usar. Si no es el caso, podemos descargar uno desde [1] (sin olvidar el archivo `libpcap` requerido) y compilar la herramienta nosotros mismo. Necesitamos privilegios de administrador para utilizar esta herramienta puesto que habilita el modo promiscuo de nuestra tarjeta de red permitiéndole leer cualquier bloque de datos que aparezca en nuestra red local. Esto puede permitir a un usuario leer las contraseñas de otras personas.

`tcpdump` nos va a mostrar cualquier paquete de datos que nuestra tarjeta de red vea.

```
11:56:27.833598 192.168.1.245
. ssh > 192.168.1.20.39258: P
1392512:1392720(208) ack 1201
win 9120 <nop,nop,timestamp
2599771999 1711932971> (DF)
[ tos 0x10 ]
```

Podemos ver que `192.168.1.245` ha enviado un paquete de datos `ssh` a la máquina `192.168.1.20`. Escribe...

```
tcpdump -i eth0 port 80
```

... y nos mostrará los datos del puerto 80, que es el que la mayoría de los buscadores Web usan. Por otro lado, `tcpdump nombredelhost` nos mostrará el tráfico de red del host destino.

## ¿Quién va?

Tiene sentido la instalación de herramientas especializadas que nos eviten perdernos. `iptraf` es un ejemplo. Nos dice exactamente que está ocurriendo con nuestra tarjeta de red, que protocolos está utilizando actualmente y con qué máquinas se está comunicando. Escribiendo [q] [Intro] se cierra esta herramienta.

El menú principal (Figura 6) contiene un monitor de tráfico IP (ver Figura 7) que nos muestra el tráfico de entrada y salida, permitiendo encontrar los puntos donde las transiciones ocurren.

Por otro lado, el interfaz de estadísticas detallado (ver Figura 8) no nos muestra que máquinas están intercambiando datos, pero analiza los flujos de tráfico por protocolos. Esto nos proporciona información muy valiosa sobre el rendimiento e indica cuellos de botella. Por ejemplo, si hay más salidas que entradas, podemos suponer que alguien está descargando algo desde nuestra máquina.

Por supuesto que podríamos decir mucho más acerca de `iptraf` y las otras herramientas mencionadas en este artículo. Pero si deseas enriquecer tus conocimientos en esta área no hay alternativa a los conocimientos básicos de redes. ■

## RECURSOS

[1] `tcpdump`: <http://www.tcpdump.org/>