

Herramientas de diagnóstico de Red

A TRAVÉS DE LA RED

Linux posee las herramientas adecuadas para buscar y encontrar en la red errores y abrir el camino a los paquetes de datos.

POR HEIKE JURZIK

Obtener ayuda puede salir muy caro si la conexión a Internet falla inesperadamente o cuando no se puede tener acceso a los ordenadores de la red local. Varias herramientas de la línea de comandos pueden ayudar a investigar conflictos en la red. *ping* y *trace route* comprueban la disponibilidad de otros ordenadores; puede contactarse con los servidores con *host* y *dig*; *netstat* ayuda a descubrir qué está ocurriendo en el sistema.

¿Quién Soy Yo?

La herramienta *ifconfig* permite comprobar la propia interfaz de red del ordenador personal. Esta práctica utilidad no sólo presenta información de la configuración actual, sino que también ayuda a configurar la interfaz. Para presentar las configuraciones actuales se ejecuta */sbin/ifconfig* sin ningún parámetro. Como el programa reside en */sbin*, que habitualmente no se encuentra en *\$PATH* del usuario, será necesario especificar la ruta completa.

El Listado 1 muestra el comando y la salida para cada interfaz secciones separadas. En este ejemplo el ordenador posee una tarjeta de

red (*eth0*) con una dirección IP de (*inet addr*) *10.195.34.14*. Pueden verse los detalles de la dirección de emisión del programa (*Bcast*), y la máscara de red (*Mask*). La etiqueta *UP* muestra el número de paquetes recibidos, y *TX* el número de paquetes transmitidos.

Adicionalmente, se encuentra configurada la interfaz loopback (*lo*), que es la que da acceso interno a los usuarios a la máquina a través de la dirección IP *127.0.0.1* y el nombre de *localhost*. La tercera interfaz de esta lista es una conexión DSL, *ppp0*; el ordenador tiene una dirección en Internet de *11.22.33.44*.

¿Quiénes son los demás?

Gracias a una práctica invención llamada *Domain Name Service*, nadie está obligado a recordar las complejas direcciones IP. En su lugar pueden usarse nombres de dominios para contactar con los ordenadores. *dig* o *host*

en la línea de comandos permiten comprobar si la configuración DNS está funcionando adecuadamente. Ambas herramientas esperan bien un nombre de dominio o bien una dirección IP como argumento, y la resolución del nombre funciona en ambas direcciones.

El Listado 2 es un ejemplo de una petición *dig*. Además de *QUESTION SECTION*, *dig* también presenta una *ANSWER SECTION*. La dirección IP para el nombre de dominio pasó a *dig* seguido de *A*. Para resolverlo en la dirección opuesta, es decir, desde una dirección IP a un nombre de dominio, es necesario especificar la opción *-x*.

```

ubuntu@ubuntu: ~
File Edit View Terminal Tabs Help
ubuntu@ubuntu:~$ ping -c 8 www.google.de
PING www.l.google.com (66.249.93.104) 56(84) bytes of data:
64 bytes from 66.249.93.104: icmp_seq=1 ttl=233 time=145 ms
64 bytes from 66.249.93.104: icmp_seq=2 ttl=233 time=145 ms
64 bytes from 66.249.93.104: icmp_seq=3 ttl=233 time=145 ms
64 bytes from 66.249.93.104: icmp_seq=4 ttl=233 time=145 ms
64 bytes from 66.249.93.104: icmp_seq=5 ttl=233 time=144 ms
64 bytes from 66.249.93.104: icmp_seq=6 ttl=233 time=145 ms
64 bytes from 66.249.93.104: icmp_seq=7 ttl=233 time=145 ms
64 bytes from 66.249.93.104: icmp_seq=8 ttl=233 time=144 ms

--- www.l.google.com ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 6998ms
rtt min/avg/max/mdev = 144.830/145.291/145.997/0.478 ms
ubuntu@ubuntu:~$

```

Figura 1: Ping permite comprobar si la máquina está accesible.

Listado 1: Salida ifconfig

```

01 $ /sbin/ifconfig          10   carrier:0
02 eth0      Link encap:Ethernet  11           (...)
   HWaddr 00:30:48:70:4B:40
03          inet                12 lo        Link encap:Local
   addr:10.195.34.14           Loopback
   Bcast:10.195.34.255        13          inet addr:127.0.0.1
   Mask:255.255.255.0        Mask:255.0.0.0
04          Mask:255.255.255.0  14           (...)
05          UP BROADCAST RUNNING  15 ppp0      Link
   MULTICAST MTU:1500 Metric:1  encap:Point-Point Protocol
06          (...)                16          inet addr:11.22.33.44
07          RX packets:1162180567  P-t-P:11.22.33.55
   errors:0 dropped:449        Mask:255.255.255.0
   overruns:0
08          frame:0              17           (...)
09          TX packets:2046191782
   errors:0 dropped:0 overruns:0
    
```

La herramienta *host* no necesita un parámetro para especificar la dirección a resolver, aunque tampoco ofrece tanta información como *dig*. Acepta IPs y nombres de dominios sin protestar. Hay un ejemplo en el Listado 3: algunos nombres de dominio comparten a menudo la misma dirección IP, cuando un servidor web hospeda diferentes páginas, por ejemplo. Al mismo tiempo, un nombre de dominio puede resolver a múltiples direcciones IP: raramente usa sitios webs como Google o eBay, por razones de rendimiento usa múltiples servidores.

¿Bien Conectado?

Si tu ordenador no se encuentra conectado directamente a Internet, sino que se usa un router, puede ejecutarse el comando *route* para obtener la tabla routing. Es preciso introducir de nuevo la ruta completa para este comando. Las salidas de las direcciones IP en lugar de nombres de hosts configura adicionalmente el parámetro *-n*.

La salida desde este comando es una tabla con el destino como primera columna (*Destination*). La última columna contiene la interfaz a través del cual se enviarán y recibirán los paquetes. En nuestro ejemplo (Listado 4), todos los paquetes enviados a las direcciones IP que comienzan con *10.195.34* usan la interfaz de red *eth0*. La conexión a Internet se muestra en la segunda línea; si la dirección destino no comienza con *10.195.34*, el paquete será enviado primero a *10.195.34.5* (el router) que se ocupará de remitirlo a su destino.

Ping-Pong

El comando *ping* permite comprobar si una máquina se encuentra activo. El programa espera una dirección IP o un nombre de host como entrada, y mide la respuesta del destino. Para comprobar si está funcionando la conexión a Internet puede hacerse ping a una

máquina fuera de la propia red, tal como *ping -c 8 www.google.com*.

El programa envía paquetes ICMP al ordenador especificado, el cual, habitualmente, responderá con paquetes ICMP. Si no se especifica ningún parámetro adicional, la prueba continuará hasta que deje de hacerse ping pulsando el atajo de teclado [Ctrl] + [C]. La opción *-c número* permite restringir el número de paquetes a intercambiar. Después de completarse el intercambio de paquetes, ping presenta estadísticas con los tiempos de viaje, que adicionalmente dirán el número de paquetes que se han perdido (Figura 1).

ping es una muy buena manera de aislar algunos errores de comandos:

- Si se arranca el programa y no ocurre nada pero se ve un mensaje de error tal como *ping: unknown host www.google.de* poco tiempo después probablemente sea por que hay un problema DNS. En este caso hay que intentar hacer ping a una dirección IP para comprobar las configuraciones de red.
- Si todo es un poco lento y *ping* no proporciona ninguna salida primero, aunque luego muestra la salida normal, el primer servidor de nombres puede que no se encuentre disponible o bien podría tener algún otro pro-

Listado 2: Ejemplo de dig

```

01 ]$ dig www.linux-magazine.es  15 ;; AUTHORITY SECTION:
02                               16 linux-magazine.es.      82832
03 ; <<>> DiG 9.3.1 <<>>        IN      NS
   www.linux-magazine.es        ns2.m-online.net.
04 ;; global options: printcmd  17 linux-magazine.es.      82832
05 ;; Got answer:                IN      NS
06 ;; ->>HEADER<<- opcode: QUERY, ns1.m-online.net.
   status: NOERROR, id: 29166  18
07 ;; flags: qr rd ra; QUERY: 1,  19 ;; ADDITIONAL SECTION:
   ANSWER: 1, AUTHORITY: 2,    20 ns1.m-online.net.      68887
   ADDITIONAL: 2              IN      A      212.18.0.8
08                               21 ns2.m-online.net.      68884
09 ;; QUESTION SECTION:         IN      A      212.18.3.8
10 ;www.linux-magazine.es.      22
   IN      A                               23 ;; Query time: 2409 msec
11                               24 ;; SERVER:
12 ;; ANSWER SECTION:           194.25.0.69#53(194.25.0.69)
13 www.linux-magazine.es.      85779  25 ;; WHEN: Mon Jan 1 21:18:31
   IN      A      212.227.96.14  2007
14                               26 ;; MSG SIZE rcvd: 135
    
```

Listado 3: Nombre de Dominio con Múltiples IPs

```

$ host www.google.com
www.google.com is an alias for www.l.google.com.
www.l.google.com has address 66.102.9.104
www.l.google.com has address 66.102.9.147
    
```

```

ubuntu@ubuntu:~$ traceroute www.example.com
traceroute to www.example.com (192.0.34.166), 30 hops max, 40 byte packets
 1 192.168.41.254 (192.168.41.254)  0.548 ms  0.398 ms  0.160 ms
 2  * * *
 3 217.0.72.74 (217.0.72.74) 19.393 ms 19.073 ms 19.149 ms
 4 nyc-e5.NYC.US.net.DTAG.DE (62.154.14.53) 109.975 ms 109.670 ms 110.166 ms
 5 65.59.192.5 (65.59.192.5) 109.464 ms 110.222 ms so-1-3-0.gar1.NewYork1.Level3.net (4.68.111.69) 109.995 ms
 6 ae-1-53.bbr1.NewYork1.Level3.net (4.68.97.129) 110.574 ms ae-1-51.bbr1.NewYork1.Level3.net (4.68.97.1) 110.632 ms so-1-3-0.gar1.NewYork1.Level3.net (4.68.97.65) 110.068 ms
 7 so-3-0-0.mpl.Tustin1.Level3.net (209.247.8.118) 195.367 ms 194.211 ms 194.273 ms
 8 so-9-0.hsal.Tustin1.Level3.net (4.68.114.6) 191.238 ms so-8-0.hsal.Tustin1.Level3.net (4.68.114.2) 191.396 ms so-9-0.hsal.Tustin1.Level3.net (4.68.114.6) 192.613 ms
 9 ln-cit-gsr-Level3.ln.net (67.30.130.67) 189.476 ms 189.625 ms 189.388 ms
10 130.152.181.162 (130.152.181.162) 191.325 ms 190.972 ms 191.130 ms
11 207.151.118.18 (207.151.118.18) 194.602 ms 252.323 ms 271.229 ms
12 * * *
13 * * *
14 * * *
    
```

Figura 2: La herramienta traceroute muestra las estaciones intermedias en ruta desde tu ordenador a la estación destino.

```

ubuntu@ubuntu:~$ mtr www.example.com
My traceroute  [v0.69]
ubuntu (0.0.0.0)(tos=0x0 psize=64 bitpattern=0x00)  Fri Jul 28 11:47:02 2006
Resolver: Received error response 2. (server failure)er of fields  quit
Packets
Host      Loss%  Snt  Last  Avg  Best  Wrst StDev
1. 192.168.41.254
2. ???
3. 217.0.72.74
4. nyc-e5.NYC.US.net.DTAG.DE 12.9%  31  20.8  20.6  19.6  24.5  1.2
5. so-1-3-0.gar1.NewYork1.Level3.net 0.0%  31  110.3  111.3  109.5  134.1  4.4
6. ae-1-53.bbr1.NewYork1.Level3.net 0.0%  31  123.6  113.4  109.8  181.5  12.8
7. so-3-0-0.mpl.Tustin1.Level3.net 0.0%  31  197.2  197.2  193.6  217.9  6.9
8. so-8-0.hsal.Tustin1.Level3.net 0.0%  31  193.2  192.0  191.0  193.3  0.6
9. ln-cit-gsr-Level3.ln.net 0.0%  31  189.8  190.0  189.0  191.2  0.6
10. 130.152.181.162 0.0%  31  192.5  195.1  191.3  277.8  15.6
11. 207.151.118.18 0.0%  31  203.6  207.4  193.3  295.9  22.7
12. cs-1-b14k-e-1-1.icann.org 0.0%  30  194.8  202.3  192.9  288.2  18.6
13. www.example.com 0.0%  30  197.1  202.3  191.8  278.4  19.9
    
```

Figura 3: mtr combina la funcionalidad de las utilidades ping y traceroute.

blema. En este caso, el segundo servidor de nombres de la configuración entra en funcionamiento después de una corta demora.

- Si no ve ninguna respuesta, el cortafuegos puede estar bloqueando los paquetes ICMP por el lado objetivo.
- *packet loss* no significa automáticamente que se tenga un problema, el objetivo del router podría estar ocupado.

La Ruta Adecuada

Aunque ping nos dice si se puede llegar hasta un servidor, sin embargo no ofrece información acerca de la ruta que siguen los paquetes a través de la red. Para encontrarla se necesita la herramienta *traceroute*. De nuevo habrá que pasar la dirección IP o el nombre de host a la herramienta (Figura 2).

Al igual que ping, *traceroute* envía paquetes traza a través de la red. Los paquetes tienen un tipo de “fecha de caducidad” (TTL=Time to Live, o Tiempo de vida). Cuando un paquete alcanza un host, éste envía un mensaje de error a la máquina fuente y rechaza el paquete. Si el paquete es válido, decrementa el TTL y envía el paquete a la siguiente estación en ruta.

Los mensajes de error rastrean la ruta. *traceroute* incrementa el TTL en cada etapa para permitir que los paquetes viajen a una estación más. Un paquete con un TTL de 2 alcanzará la segunda dirección intermedia. TTL 3 alcanzará la tercera, y así sucesivamente. *traceroute* repite esta transmisión tres veces para cada máquina, y espera tres segundos para que cada máquina individualmente responda.

traceroute puede tomar diferentes rutas. Si se envía a la misma máquina dos veces y se ven diferentes direcciones intermedias, no hay que preocuparse. Si se ven asteriscos

como en la Figura 2, probablemente se alcanzará un cortafuego en ruta, aunque los paquetes simplemente pueden desaparecer.

traceroute usa por defecto paquetes UDP, aunque especificando la opción *-l* podrán usarse paquetes ICMP. Si la salida contiene una cadena de asteriscos inusualmente larga, puede suponerse que la herramienta ha caído a merced de todos esos cortafuegos. En este caso, debería probarse con *tcptraceroute*, un programa que transmite paquetes TCP configurados para usar el puerto 80, el puerto al que escuchan la mayoría de los servidores web. Si se sabe que el destino no ejecuta un servicio web, hay que especificar el puerto. Para contactar con una máquina a través del puerto 22 (SSH), se escribe lo siguiente:

```
$ tcptraceroute target 22
```

Otras Herramientas

mtr es una ingeniosa combinación de ping y traceroute. Es preciso especificar la máquina destino cuando se arranca. La salida resul-

tante muestra la ruta tomada por los paquetes, presentándose las estaciones individuales y continuando con ping hasta que se abandone cuando se pulse [Q]. Como alternativa, puede especificarse un número determinado de paquetes; por ejemplo, *mtr -c 12 targets* abandona mtr después de enviar una docena de paquetes al destino.

netstat es otro programa que permite descubrir errores en la configuración de red. Sin ningún parámetro, vuelve al estado de sockets abiertas.

El parámetro *-e* ofrece información adicional sobre el UID, *-p* suministra información sobre el PID y el nombre del programa que abrió el socket. *-a* muestra todos los servicios, bien servicios activos o sockets de servidores escuchando conexiones. Si solamente se está interesado en conexiones TCP, puede especificarse adicionalmente la opción *-t*. El ejemplo en el Listado 5 muestra la ejecución de los servicios FTP y SMTP. Un usuario ha abierto una conexión FTP a la máquina y otro está navegando por la web.

Listado 4: Tabla de Enrutado

```

01 $ /sbin/route -n
02 Kernel IP routing table
03 Destination Gateway Genmask Flags Metric Ref Use Iface
05 10.195.34.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
06 0.0.0.0 10.195.34.5 0.0.0.0 UG 0 0 0 eth0
    
```

Listado 5: Salida de netstat

```

$ netstat -atp | less
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State (...)
tcp 0 0 *:ftp * LISTEN -
tcp 0 0 *:smtp * LISTEN - (...)
    
```