# Utilización de herramientas TCP/IP adaptadas

## 1. Principios

El conjunto de protocolos TCP/IP proporciona numerosas herramientas que permiten comprobar el buen funcionamiento de la red o de un mecanismo específico: resolución de nombres, acceso a un ordenador...

Es importante conocer estas herramientas y familiarizarse con ellas.

## 2. Ejemplo de utilización de las herramientas

### a. arp

El protocolo ARP mantiene localmente en el ordenador una tabla de correspondencias entre las direcciones IP (lógicas) y MAC (física). El comando «arp» permite editar esta tabla, que se encuentra en la memoria RAM.

Cuando no se puede alcanzar un destinatario a través de la red, es importante ver la máscara ARP del ordenador remoto para saber si dispone de la dirección MAC de la puerta de enlace predeterminada. En este caso, esto puede querer decir que la ida funciona, pero la vuelta no. Efectivamente, a la llegada, el router, que dispone de una interfaz en la misma red de nivel 2 que el destinatario, generará una petición ARP para obtener la dirección MAC de este. El destinatario recibirá la petición ARP y aprovechará para poner en su máscara la dirección MAC del ordenador que origina la petición ARP (el router), para anticipar la vuelta.

ARP también se puede utilizar para identificar un conflicto de dirección IP y comprobar la dirección MAC del destinatario en la misma red de nivel 2.

Podemos utilizar la herramienta ARP para añadir una entrada estática (mapeo de una dirección IP con una dirección MAC) para llegar a un dispositivo de red que no dispone de dirección IP (impresora) cuya dirección MAC conocemos. Para ello, efectuaremos una reserva ARP con la opción s.

En Unix/Linux es posible crear un archivo que contenga el mapeo entre las direcciones MAC y las direcciones IP (/etc/ethers) con el fin de minimizar el tráfico vinculado a las numerosas difusiones ARP. Junto con eso, y para añadir seguridad, ARP se puede desactivar en cada equipo de modo que nadie responda a una petición ARP solicitada por un ordenador desconocido cuya dirección MAC no esté referenciada en las tablas.

A continuación, se puede ver una máscara ARP de un ordenador Windows que dispone de cuatro tarjetas de red.

Observe que cada red de nivel 2 dispone de su propia máscara ARP.

```
C:\>arp -a
Interfaz: 172.16.0.100 --- 0x2
  Dirección IP          Dirección física      Tipo
  172.16.0.200          00-50-da-b8-22-9d     dinámico
  172.16.101.1          00-60-97-37-12-3b     dinámico
  172.16.103.1          00-50-da-d6-3e-e8     dinámico
  172.16.104.1          00-10-4b-b6-5b-27     dinámico
  172.16.205.1          00-50-04-ec-ae-4c     dinámico
  172.16.206.254        00-50-da-84-cb-62     dinámico
  172.16.208.1          00-50-da-36-33-91     dinámico
```

```
Interfaz: 172.20.0.100 --- 0x3
  Dirección IP          Dirección física      Tipo
  172.20.0.3            00-50-fc-4b-06-9c     dinámico
  172.20.0.57           00-60-97-c5-a8-ad     dinámico

Interfaz: 195.101.229.57 --- 0x1000005
  Dirección IP          Dirección física      Tipo
  195.101.229.60        00-20-6f-0d-75-c8     dinámico

Interfaz: 172.17.0.100 --- 0x1000006
  Dirección IP          Dirección física      Tipo
  172.17.0.3            00-50-fc-0b-39-f1     dinámico
  172.17.0.4            00-50-fc-54-0e-28     dinámico
  172.17.64.48          00-50-56-50-00-7f     dinámico
  172.17.71.1           00-50-fc-1f-7a-3a     dinámico
  172.17.207.89         00-50-fc-20-3a-39     dinámico

C:\>
```

*A continuación, se puede ver la máscara ARP de un ordenador Linux que tiene dos interfaces:*

```
[root@linus /root]# arp -a
? (172.17.64.1) at 00:50:04:EC:AB:B8 [ether] on eth0
? (172.16.103.1) at 00:50:DA:D6:3E:E8 [ether] on eth1
? (172.16.102.1) at 00:50:FC:0B:39:F0 [ether] on eth1
? (172.16.208.1) at 00:50:DA:36:33:91 [ether] on eth1
? (172.17.1.146) at 00:10:5A:D8:3E:05 [ether] on eth0
? (172.17.0.218) at 00:50:FC:0B:3A:00 [ether] on eth0
? (172.16.1.253) at 00:04:00:A8:E0:B7 [ether] on eth1
router104 (172.16.104.1) at 00:10:4B:B6:5B:27 [ether] on eth1
jojo.eni.es (172.17.207.89) at 00:50:FC:20:3A:39 [ether] on eth0
? (172.17.3.6) at 00:50:FC:24:37:F3 [ether] on eth0
router205 (172.16.205.1) at 00:50:04:EC:AE:4C [ether] on eth1
? (172.16.206.254) at 00:50:DA:84:CB:62 [ether] on eth1
[root@linus /root]#
```

### b. ping

El comando ping utiliza el protocolo ICMP. Permite comprobar si hay una buena conectividad de red, haciendo el envío de peticiones «echo request». La respuesta normal que se espera es «echo reply».

Es importante, cuando se realiza esta prueba hacia un equipo situado detrás de un router, conocer la puerta de enlace. El destinatario también debe conocer su puerta de enlace para enviar correctamente la respuesta. A menudo, el fallo de un «Ping» puede estar relacionado con una configuración defectuosa de la puerta de enlace o puede deberse a que las rutas están mal definidas en los routers.

Atención: cuando hay routers de filtrado o cortafuegos en la ruta, los paquetes ICMP echo request e ICMP echo reply pueden estar bloqueados. Para comprobar que no es así, debemos intentar conectarnos a un servicio que se ejecute en el ordenador remoto aunque el ping no funcione.

En este caso, el cortafuegos o el router de filtrado no dejará pasar más que algunos tipos de ICMP cuyo código conoce para impedir que los piratas obtengan demasiada información acerca de la asignación de direcciones de la

red. Así, el ICMP echo request (ping de ida), corresponde al código 8 y al tipo 0, mientras que el ping de vuelta, ICMP echo reply, corresponde al código 0 y tipo 0.

La RFC 792 contiene los tipos y códigos ICMP, así como los mensajes asociados y su función.

El comando tracert/traceroute ayuda a establecer el diagnóstico en caso de que esta prueba no funcione.

*Por ejemplo*

*Aquí tenemos un resultado desde un equipo de Windows:*

```
C:\>ping 195.101.229.60
Haciendo ping a 195.101.229.60 con 32 bytes de datos:

Respuesta desde 195.101.229.60: bytes=32 tiempo<10 ms TTL=255
Respuesta desde 195.101.229.60: bytes=32 tiempo<10 ms TTL=255
Respuesta desde 195.101.229.60: bytes=32 tiempo<10 ms TTL=255
Respuesta desde 195.101.229.60: bytes=32 tiempo<10 ms TTL=255

Estadísticas de Ping para 195.101.229.60:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
C:\>
```

Este comando también se puede utilizar para obtener la lista de los equipos IP de una red de nivel 2, recurriendo a una difusión, como en Linux.

```
[root@linus /root]# ping 172.16.255.255
PING 172.16.255.255 (172.16.255.255): 56 data bytes
64 bytes from 172.16.0.2: icmp_seq=0 ttl=255 time=0.3 ms
64 bytes from 172.16.1.253: icmp_seq=0 ttl=255 time=98.7 ms
(DUP!)
64 bytes from 172.16.0.2: icmp_seq=1 ttl=255 time=0.1 ms
64 bytes from 172.16.1.253: icmp_seq=1 ttl=255 time=1.0 ms
(DUP!)
--- 172.16.255.255 ping statistics ---
2 packets transmitted, 2 packets received, +2 duplicates, 0%
packet loss
round-trip min/avg/max = 0.1/6.0/98.7 ms
```

### c. tracert/traceroute

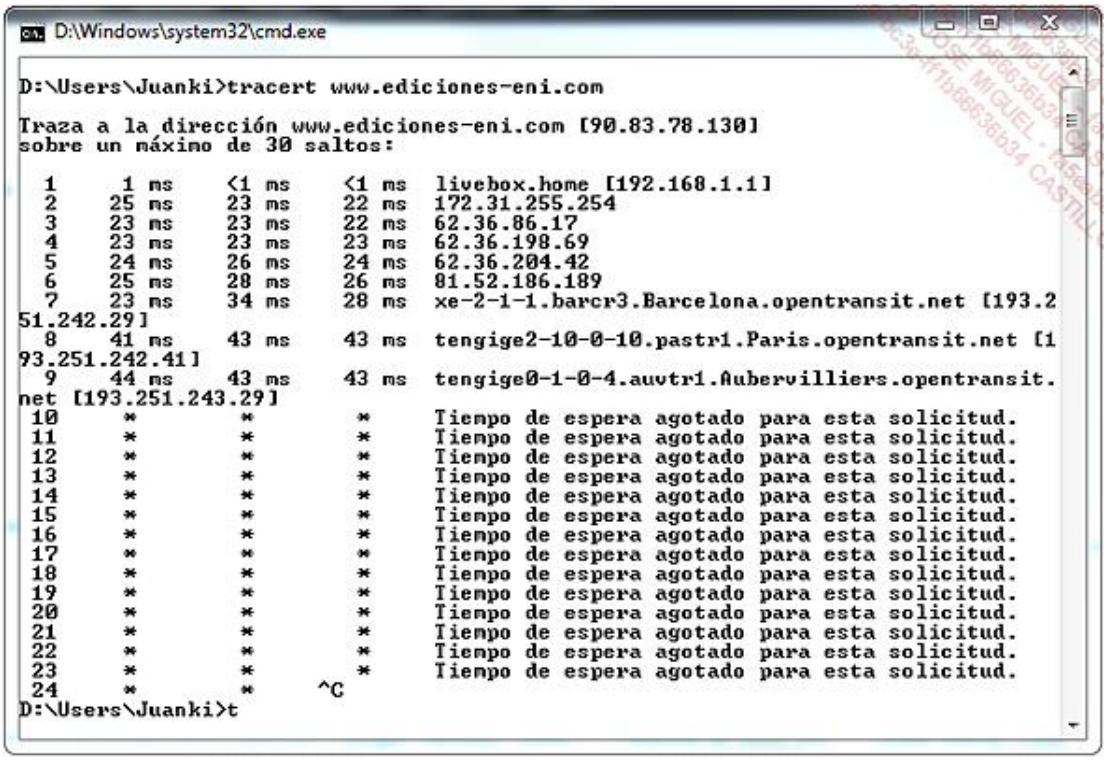
Este comando permite seguir la ruta completa del paquete IP hasta el destinatario y así identificar hasta dónde llega el paquete.

traceroute es una implementación Unix/Linux, mientras que los sistemas operativos Microsoft utilizan tracert.

Este comando intenta alcanzar la dirección IP o el nombre solicitados, limitándose a cruzar los routers de uno en

uno hasta que el paquete alcanza el destinatario.

Haremos un tracert hasta un router de filtrado que bloquee este tipo de trama; de ahí el mensaje final que se obtiene.




### d. ipconfig/ifconfig

Este comando en sus distintas versiones permite indicar, identificar o renovar una configuración IP para un ordenador que dispone de una dirección IP fija o dinámica (cliente DHCP). Permite, entre otras cosas, conocer la dirección MAC de un equipo, así como algunas opciones definidas según el sistema operativo.

El comando en línea ipconfig se utiliza en Windows. En los sistemas Unix y Linux, el comando es ifconfig.

Estos comandos no funcionan de la misma manera. Únicamente ifconfig permite identificar una dirección IP, reactivar o desactivar una interfaz, mientras que las versiones de Microsoft solo permiten visualizar la configuración, o renovar o liberar una asignación en el caso de un cliente DHCP.

De este modo, ipconfig permite comprobar todos los parámetros efectivamente disponibles: IP, máscara, IP de la puerta de enlace, IP DNS 1, IP DNS 2, nombre de dominio, dirección MAC, nombre de servidor DHCP (cuando proceda), tipo de nodo NetBIOS...

Ifconfig proporciona menos detalles de las opciones TCP/IP, pero cubre mejor el funcionamiento de la red física: *Maximum Transfer Unit* (MTU), interfaz habilitada (U por UP) o deshabilitada (no se visualiza UP), dirección IP de difusión, situación del *multicast*, número de paquetes enviados, recibidos, IRQ y direcciones utilizadas por la tarjeta de red.

*A continuación, podemos ver la versión ampliada de un comando ejecutado en un servidor Windows y después, la versión sin `/all`.*

```
C:\>ipconfig /all
```

```
Configuración IP de Windows 2000
        Nombre del host . . . . . : Ulysse
        Sufijo DNS principal . . .  . . . : eni-escuela.local
        Tipo de nodo. . . . . .  . . . : híbrido
        Enrutamiento habilitado . . . . . : Sí
        Proxy WINS habilitado . . . . . : No
        Lista de búsqueda de sufijo DNS . : eni-escuela.local
                                            eni.local
Ethernet tarjeta 172.16. - eni publica :
        Sufijo de conexión específica DNS : eni.local
        Descripción . . . . . : Tarjeta Realtek RTL8139(A)
PCI Fast
```

```
Ethernet #3
        Dirección física. . . . . : 00-50-FC-0B-9A-80
        DHCP habilitado . . . . . : No
        Dirección IP. . . . . : 172.16.0.100
        Máscara de subred . . . . . : 255.255.0.0
        Puerta de enlace predeterminada . :
        Servidores DNS. . . . . :

Ethernet tarjeta 172.17. - eni privada :
        Sufijo de conexión específica DNS : eni.local
        Descripción . . . . . : Tarjeta Realtek RTL8139(A)
PCI Fast
Ethernet #2
        Dirección física. . . . . : 00-50-FC-1F-3C-6F
        DHCP habilitado . . . . . : No
        Dirección IP. . . . . : 172.17.0.100
        Máscara de subred . . . . . : 255.255.0.0
        Puerta de enlace predeterminada . :
        Servidores DNS. . . . . : 172.17.0.3
                                  172.17.0.4

C:\>ipconfig
Configuración IP de Windows 2000
Ethernet tarjeta 172.16. - eni pública :
        Sufijo de conexión específica DNS : eni.local
        Dirección IP. . . . . : 172.16.0.100
        Máscara de subred . . . . . : 255.255.0.0
        Puerta de enlace predeterminada . :
Ethernet tarjeta 172.17. - eni privada :
        Sufijo de conexión específica DNS : eni.local
        Dirección IP. . . . . : 172.17.0.100
        Máscara de subred . . . . . : 255.255.0.0
        Puerta de enlace predeterminada . :
```

*El siguiente es un ejemplo obtenido en un sistema Linux que tiene dos tarjetas de red.*

```
[root@linus /root]# ifconfig
eth0   Link encap:Ethernet  HWaddr 00:80:C8:D4:98:01
       inet addr:172.17.0.2  Bcast:172.17.255.255  Mask:255.255.0.0
```

```
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:16868111 errors:0 dropped:0 overruns:0 frame:0
       TX packets:22140084 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:100
       Interrupt:11 Base address:0x6600
eth1   Link encap:Ethernet  HWaddr 00:50:FC:24:D8:6E
       inet addr:172.16.0.2  Bcast:172.16.255.255  Mask:255.255.0.0
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:38581402 errors:0 dropped:0 overruns:0 frame:0
       TX packets:60438451 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:100
       Interrupt:9 Base address:0x6500
lo     Link encap:Local Loopback
       inet addr:127.0.0.1  Mask:255.0.0.0
       UP LOOPBACK RUNNING  MTU:3924  Metric:1
       RX packets:12903 errors:0 dropped:0 overruns:0 frame:0
       TX packets:12903 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:0

[root@linus /root]#
```

### e. netstat

Este comando permite visualizar, por una parte, los puertos abiertos de un ordenador y, por otra parte, la tabla de enrutamiento del ordenador local o incluso las estadísticas de funcionamiento de la red.

*A continuación, se puede ver el resultado en un ordenador Windows.*

```
C:\>netstat -an
Conexiones activas
  Proto  Dirección local        Dirección remota       Estado
  TCP    0.0.0.0:23             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3911           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:4512           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:4610           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5000           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:12345          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1029         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1031         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1766         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:3532         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:3910         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:3928         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:4563         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:4564         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:4565         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:4566         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:4608         0.0.0.0:0              LISTENING
  TCP    172.17.0.89:1337       0.0.0.0:0              LISTENING
  TCP    172.17.0.89:1619       0.0.0.0:0              LISTENING
```

```
  TCP    172.17.0.89:1878       0.0.0.0:0              LISTENING
  TCP    172.17.207.89:139      0.0.0.0:0              LISTENING
  TCP    172.17.207.89:2411     0.0.0.0:0              LISTENING
  TCP    172.17.207.89:2904     0.0.0.0:0              LISTENING
  TCP    172.17.207.89:2964     0.0.0.0:0              LISTENING
  TCP    172.17.207.89:3299     0.0.0.0:0              LISTENING
  TCP    172.17.207.89:3514     0.0.0.0:0              LISTENING
  TCP    172.17.207.89:3799     0.0.0.0:0              LISTENING
  TCP    172.17.207.89:3905     0.0.0.0:0              LISTENING
  TCP    172.17.207.89:3905     172.17.0.2:1a39        ESTABLISHED
  TCP    172.17.207.89:3911     172.17.0.100:34703     ESTABLISHED
  TCP    172.17.207.89:4610     172.17.0.100:3389      ESTABLISHED
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1030           *:*
  UDP    0.0.0.0:1033           *:*
  UDP    0.0.0.0:1054           *:*
  UDP    0.0.0.0:3912           *:*
  UDP    0.0.0.0:4611           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:2234         *:*
  UDP    127.0.0.1:3929         *:*
  UDP    172.17.207.89:123      *:*
  UDP    172.17.207.89:137      *:*
  UDP    172.17.207.89:138      *:*
  UDP    172.17.207.89:1900     *:*
```

*Seguidamente, se representa un extracto de la tabla de enrutamiento de un servidor Windows.*

```
C:\>netstat -rn
Tabla de rutas
===========================================================================
Lista de interfaces
0x1 ........................... MS TCP Loopback interface
0x2 ...00 50 fc 0b 9a 80 ...... NDIS 5.0 driver
                                  (Microsoft’s Packet Scheduler)
0x3 ...00 80 c8 ec 81 e5 ...... VIA PCI 10/100Mb Fast Ethernet
Adapter (Microsoft’s Packet Scheduler)
0x1000005 ...00 50 fc 0b af 96 ...... NDIS 5.0 driver
                                  (Microsoft’s Packet Scheduler)

===========================================================================
Rutas activas:
Destino de red     Máscara de red    Puerta de acceso Interfaz   Métrica
      127.0.0.0         255.0.0.0       127.0.0.1     127.0.0.1        1
     172.16.0.0       255.255.0.0    172.16.0.100  172.16.0.100        1
   172.16.0.100   255.255.255.255       127.0.0.1     127.0.0.1        1
 172.16.255.255   255.255.255.255    172.16.0.100  172.16.0.100        1
     172.17.0.0       255.255.0.0    172.17.0.100  172.17.0.100        1
   172.17.0.100   255.255.255.255       127.0.0.1     127.0.0.1        1
  72.17.255.255   255.255.255.255    172.17.0.100  172.17.0.100        1
```

```
     172.20.0.0        255.255.0.0    172.20.0.100  172.20.0.100        1
   172.20.0.100   255.255.255.255       127.0.0.1     127.0.0.1        1
 172.20.255.255   255.255.255.255    172.20.0.100  172.20.0.100        1
    192.168.1.0     255.255.255.0    172.16.101.1  172.16.0.100        1
    192.168.2.0     255.255.255.0    172.16.102.1  172.16.0.100        1
    192.168.3.0     255.255.255.0    172.16.103.1  172.16.0.100        1
    192.168.4.0     255.255.255.0    172.16.104.1  172.16.0.100        1
    192.168.5.0     255.255.255.0    172.16.205.1  172.16.0.100        1
    192.168.6.0     255.255.255.0    172.16.206.1  172.16.0.100        1
    192.168.7.0     255.255.255.0    172.16.207.1  172.16.0.100        1
    192.168.8.0     255.255.255.0    172.16.208.1  172.16.0.100        1
   192.168.11.0     255.255.255.0    172.16.101.1  172.16.0.100        1
   192.168.12.0     255.255.255.0    172.16.102.1  172.16.0.100        1
   192.168.13.0     255.255.255.0    172.16.103.1  172.16.0.100        1
   192.168.14.0     255.255.255.0    172.16.104.1  172.16.0.100        1
   192.168.15.0     255.255.255.0    172.16.205.1  172.16.0.100        1
   192.168.16.0     255.255.255.0    172.16.206.1  172.16.0.100        1
   192.168.17.0     255.255.255.0    172.16.207.1  172.16.0.100        1
   192.168.18.0     255.255.255.0    172.16.208.1  172.16.0.100        1
      224.0.0.0         224.0.0.0    172.16.0.100  172.16.0.100        1
      224.0.0.0         224.0.0.0    172.17.0.100  172.17.0.100        1
      224.0.0.0         224.0.0.0    172.20.0.100  172.20.0.100        1
255.255.255.255   255.255.255.255    172.16.0.100  172.16.0.100        1

Puerta de enlace predeterminada:
===========================================================================
Rutas persistentes:
Dirección de red    Máscara de red       Dirección puerta enl. Métrica
    192.168.11.0    255.255.255.0        172.16.101.1          1
     192.168.1.0    255.255.255.0        172.16.101.1          1
     192.168.2.0    255.255.255.0        172.16.102.1          1
    192.168.12.0    255.255.255.0        172.16.102.1          1
     192.168.3.0    255.255.255.0        172.16.103.1          1
    192.168.13.0    255.255.255.0        172.16.103.1          1
     192.168.4.0    255.255.255.0        172.16.104.1          1
    192.168.14.0    255.255.255.0        172.16.104.1          1
     192.168.5.0    255.255.255.0        172.16.205.1          1
    192.168.15.0    255.255.255.0        172.16.205.1          1
     192.168.6.0    255.255.255.0        172.16.206.1          1
    192.168.16.0    255.255.255.0        172.16.206.1          1
     192.168.7.0    255.255.255.0        172.16.207.1          1
    192.168.17.0    255.255.255.0        172.16.207.1          1
     192.168.8.0    255.255.255.0        172.16.208.1          1
    192.168.18.0    255.255.255.0        172.16.208.1          1
   192.168.206.0    255.255.255.0      172.16.206.254          1
```

### f. nbtstat

Esta herramienta NBT permite, en un sistema operativo Microsoft, visualizar las aplicaciones NetBIOS arrancadas o ver la caché local de los nombres NetBIOS resueltos en direcciones IP.

Es fácil comprobar, con la ayuda de este comando, que el ordenador inicializó sus servicios NetBIOS correctamente.

*A continuación, indicamos las aplicaciones NetBIOS inicializadas en un ordenador Windows Server multiservicios (que además dispone de varias interfaces):*

```
C:\>nbtstat -n

172.16. - eni pública:
Dirección IP: [172.16.0.100] ID de ámbito: []

             Tabla de nombres locales NetBIOS
    Nombre               Tipo        Estado
    ---------------------------------------
    ULYSSE         <00>  único       Registrado
    ENI-ESCUELA          Grupo       Registrado
    ULYSSE               único       Registrado
    ULYSSE         <20>  único       Registrado
    ENI-ESCUELA    <1E>  Grupo       Registrado
    INet~Services        Grupo       Registrado
    IS~ULYSSE......<00>  único       Registrado

172.20. - DMZ privada:
Dirección IP: [172.20.0.100] ID de ámbito: []
   No hay nombres en la caché

172.17. - eni privada:
Dirección IP: [172.17.0.100] ID de ámbito : []

             Tabla de nombres locales NetBIOS
    Nombre               Tipo        Estado
    ---------------------------------------
    ULYSSE         <00>  único       Registrado
    ENI-ESCUELA    <00>  Grupo       Registrado
    ULYSSE         <03>  único       Registrado
    ULYSSE         <20>  único       Registrado
    ENI-ESCUELA    <1E>  Grupo       Registrado
    INet~Services  <1C>  Grupo       Registrado
    IS~ULYSSE......<00>  único       Registrado

C:\>
```

También podremos (con la opción -n) comprobar si efectivamente un servidor es controlador de dominio (Nombre de dominio). Observe que esta operación se puede realizar en remoto con -a o -A.

Este comando también es interesante para identificar los nombres NetBIOS de ordenadores duplicados en la red.

*En este ejemplo, el comando nbtstat -c permite ver la lista de nombres NetBIOS que se han resuelto en direcciones IP:*

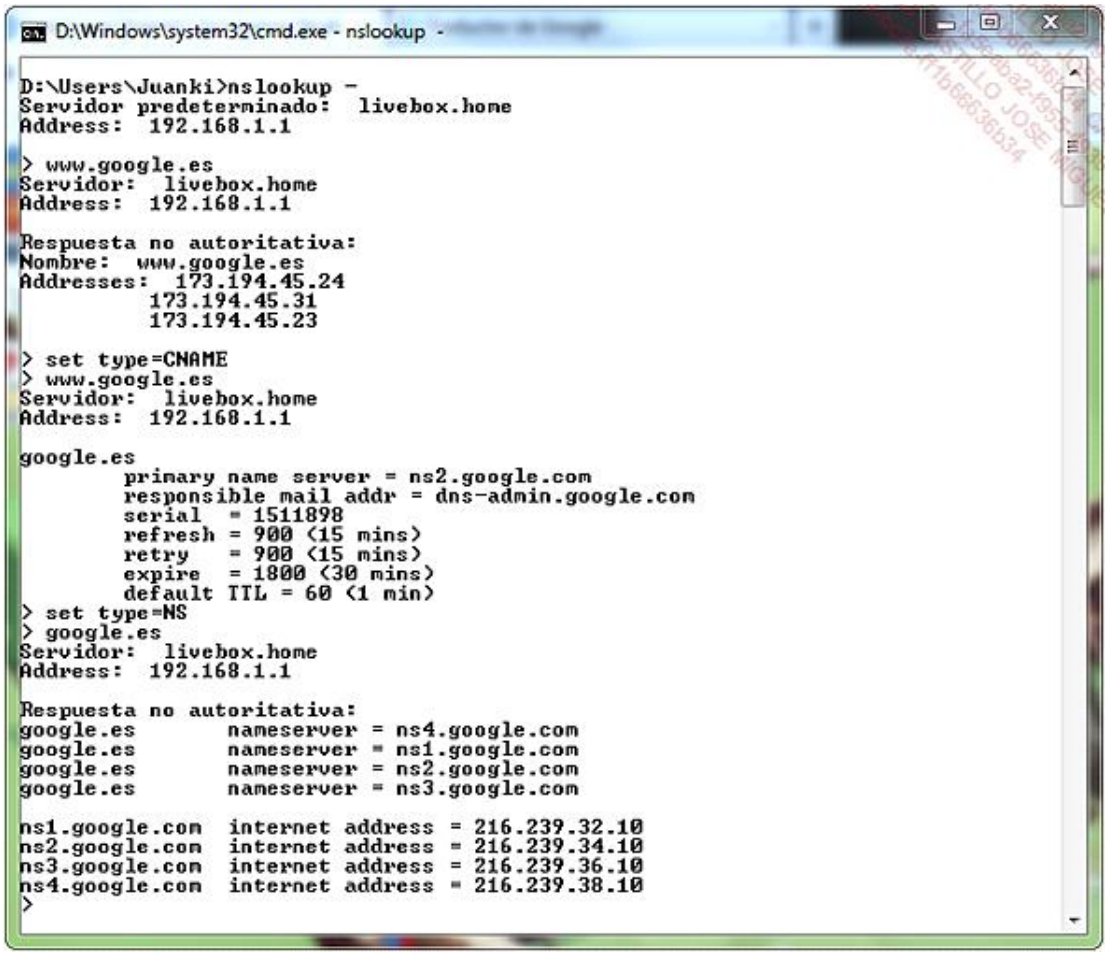
```
C:\>nbtstat -c

172.16. - eni pública:
Dirección IP: [172.16.0.100] ID de ámbito: []

                 Tabla de nombres de caché remota NetBIOS
```

```
    Nombre               Tipo     Dirección de host    Duración [sec]
    ----------------------------------------------------------------
    DEMETER        <20>  único        172.16.0.200               422

172.20. - DMZ privada:
Dirección IP: [172.20.0.100] ID de ámbito: []

    No hay nombres en la caché
172.17. - eni privada:
Dirección IP: [172.17.0.100] ID de ámbito: []

                Tabla de nombres de caché remota NetBIOS

    Nombre               Tipo     Dirección de host    Duración [sec]
    ----------------------------------------------------------------
    CD1            <20>  único          172.17.0.4               440
    HERMES         <20>  único          172.17.0.3               340

C:\>
```

### g. nslookup

nslookup permite comprobar el buen funcionamiento de las resoluciones de nombres DNS.

Una vez ejecutada la herramienta, se pueden hacer diversas consultas, tal y como muestra la pantalla que se reproduce a continuación en un sistema Windows.




Por ejemplo, para comprobar que el equipo es capaz de resolver nombres DNS (para llegar al servidor DNS adecuado), basta con indicar el nombre del dominio, incluso de un equipo. Si el servidor DNS de referencia no puede dar la respuesta directamente, indicará la dirección IP del servidor que autoriza. También es posible consultar a un DNS para saber cuál es o cuáles son los servidores de correo registrados (Tipo = MX).

Esta herramienta es muy avanzada y su dominio requiere un poco más de conocimiento que las anteriores.

La pila de protocolos TCP/IP de los sistemas operativos Windows utiliza una caché DNS, que permite sistemáticamente consultar al servidor de nombres. El contenido de esta caché se puede visualizar con el comando «ipconfig /displaydns». Es muy útil en las tareas diarias, pero puede resultar negativa si hay algún error. De hecho, si no se resuelve un nombre, la información permanece unos instantes en la caché, aunque se haya corregido el error. En este caso es necesario reinicializar la información con el comando «ipconfig /flushdns».

Como se ve a continuación, este comando funciona en modo interactivo o en modo de línea de comandos. En este último caso, cualquier operación se introduce en una sola línea.

```
C:\>nslookup
Servidor predeterminado: hermes.eni-escuela.local
Dirección:  172.17.0.3

> ls eni-escuela.local
[hermes.eni-escuela.local]
 eni-escuela.local.           A      172.20.0.3
 eni-escuela.local.           A      172.17.0.3
 eni-escuela.local.           A      172.17.0.4
```

```
 eni-escuela.local.           NS     server = cd1.eni-escuela.local
 eni-escuela.local.           NS     server = hermes.eni-escuela.local
 2000test                     A      172.17.71.4
 gc._msdcs                    A      172.17.0.4
 gc._msdcs                    A      172.17.0.3
 gc._msdcs                    A      172.20.0.3
 ADW2KSRV                     A      172.17.35.31
 adxppro                      A      172.17.35.35
 bmartin                      A      172.17.1.159
 brunom                       A      172.17.159.1
 cd1                          A      172.17.0.4
 demeter                      A      172.17.0.200
 dyonisos                     A      172.17.0.89
 eliane2                      A      172.17.202.1
 erickpro                     A      172.17.71.3
 ericxp                       A      172.17.71.1
 gilles                       A      172.17.201.10
 gilles2                      A      172.17.201.3
 hermes                       A      172.20.0.3
 hermes                       A      172.17.0.3
 jerome                       A      172.17.1.146
 linus                        A      172.17.0.2
 lotus                        NS     server = ptmail01.lotus.
eni-escuela.local
 ptmail01.lotus               A      172.17.35.31
 ptmail01                     A      172.17.35.31
 sandrine2                    A      172.17.202.2
 sophie3                      A      172.17.1.18
 srv-h                        A      172.17.64.12
 stephane                     A      172.17.104.205
 ulysse                       A      172.17.0.100
 vero-xp                      A      172.17.3.6
 xp-pro-vm-eric               A      172.17.71.100
>

C:\>nslookup www.microsoft.com
Servidor :  hermes.eni-escuela.local
Dirección:  172.17.0.3

Respuesta no autoritativa:
Nombre :    www.microsoft.akadns.net
Dirección:  207.46.134.155
Aliases  :  www.microsoft.com

c:_>
```