

[Redes] Comandos: netstat/ss

Función

- Son comandos de red que se usan para controlar las conexiones entrantes y salientes.

netstat

- **¿Cómo se usa?**. Para utilizar netstat en Windows deberemos abrir la consola del DOS (Ejecutar > cmd) y escribir netstat, a continuación podremos observar detalladamente las conexiones activas que tenemos, controlar esto tiene muchas utilidades como por ejemplo comprobar a donde redirigimos nuestras conexiones, verificar conexiones remotas, detectar intrusiones etc.
- **Afinando netstat**. Para concretar la búsqueda, netstat puede ir acompañado de ciertos parámetros que añaden o especifican funciones a la aplicación principal. A continuación se muestran todos los parámetros que se pueden utilizar con netstat sólo en Windows.
 - -a . Muestra todas las conexiones y puertos a la escucha.
 - -b . Muestra el ejecutable que crea cada conexión o puerto a la escucha.
 - -e . Estadísticas Ethernet de las visualizaciones, como el número de paquetes enviados y recibidos. Se puede combinar con la opción -s.
 - -n . Se muestran los puertos con su identificación en forma numérica y no de texto.
 - -o . En sistemas Windows XP y 2003 Server, muestra los identificadores de proceso **PID** para cada conexión. Se pueden verificar los identificadores de proceso en el Administrador de Tareas de Windows, al agregarlo a las columnas de la pestaña procesos.
 - -p . Muestra las conexiones para el protocolo especificado; el protocolo puede ser TCP o UDP. Si se utiliza con la opción de -s para visualizar la estadística por protocolo, proto puede ser TCP, UDP o IP.
 - -r . Visualiza la tabla de enrutamiento o encaminamiento. Equivale al comando route print.
 - -s . Estadística por protocolo de las visualizaciones. Por el valor por defecto, la estadística se muestra para TCP, UDP e IP; la opción -p se puede utilizar para especificar un subconjunto del valor por defecto.
 - -v . En sistemas Windows XP y 2003 Server, y usado en conjunto con -b, muestra la secuencia de componentes usados en la creación de la conexión por cada uno de los ejecutables.
 - **intervalo** . Vuelve a mostrar la información cada intervalo (en segundos). Si se presiona CTRL+C se detiene la visualización. si se omite este parámetro, netstat muestra la información solo una vez.

También se puede acceder a esta información desde la consola de comandos. Para obtener ayuda sobre las funciones de los parámetros del comando netstat y poder visualizarla en la pantalla solo tenéis que introducir:

```
netstat help
```

y no al revés, help netstat, la explicación de esto es que el que menú de ayuda del comando netstat no se encuentra en DOS sino dentro del mismo netstat por eso hay que escribir primero netstat y después help para solicitar ayuda.

Estado de las conexiones. Con netstat las conexiones se mostraran en un estado determinado dependiendo también de si añadimos parámetros o no a la función del comando principal. Por ejemplo para comprobar las conexiones que tenemos "a la escucha" debemos añadir el parámetro -a a netstat y nos mostrará las conexiones que estén en listening. Otros estados en las conexiones que nos podemos encontrar y su descripción:

- ESTABLISHED . El socket tiene una conexión establecida.
- SYN_SENT . El socket está intentando iniciar una conexión.
- SYN_RECV . Una petición de conexión fue recibida por la red.
- FIN_WAIT1 . El socket está cerrado, y la conexión esta finalizándose.
- FIN_WAIT2 . La conexión está cerrada, y el socket está esperando que finalice la conexión remota.
- TIME_WAIT . El socket está esperando después de cerrarse que concluyan los paquetes que siguen en la red.
- CLOSED . El socket no está siendo usado.
- CLOSE_WAIT . La conexión remota ha finalizado, y se espera que se cierre el socket.
- LAST_ACK . La conexión remota ha finalizado, y se espera que se cierre el socket. Esperando el acknowledgement.

- LISTEN . El socket está esperando posibles conexiones entrantes.
- CLOSING . Ambos sockets han finalizado pero aún no fueron enviados todos los datos.
- UNKNOWN . El estado del socket no se conoce.

Las conexiones más habituales son establish, time wait, closed y listen. El resto son para usos mas avanzados.

Nota. Te sugiero que si no controlas demasiado bien las conexiones entrantes y salientes con netstat, antes que nada cierres todos los programas y aplicaciones que requieran conexión a internet (incluido el navegador para no liarte) y después te fijes en los procesos que está usando cada conexión, para eso utiliza:

```
netstat -o
```

y podrás ver que cada conexión tiene digitos numericos asociados (normalmente entre uno y cuatro), ahora lo que tienes que hacer es ir al administrador de tareas de Windows (ctrl+alt+spr) y en el administrador de procesos busca los digitos que aparecen en el msn y los compruebas con los de las conexiones del netstat. Para mi esta es la forma más sencilla para evitar confundirte con otras conexiones y más fiable porque no tienes que enviar nada por tanto no resulta sospechoso.

SS

- La utilidad en Linux más semejante a netstat es **ss**. Es la alternativa moderna y suele ser más rápida; por ejemplo, `ss -tln` muestra puertos TCP en escucha, igual que `netstat -tln`.
- Otras equivalentes útiles son:
 1. `lsof -i`, para ver qué procesos tienen sockets de red abiertos.
 2. `ip addr` y `ip route`, para ver interfaces y rutas, en lugar de partes de la funcionalidad clásica de netstat.
 3. `nmap` o `nc`, si lo que quieres es comprobar puertos desde fuera o probar conectividad.
- Tabla de equivalencias de netstat y ss:

netstat	equivalente	Descripción breve
netstat -t	ss -t	Conexiones TCP activas.
netstat -u	ss -u	Conexiones UDP activas.
netstat -l	ss -l	Sockets en modo escucha.
netstat -p	ss -p	Incluir información del proceso asociado.
netstat -n	ss -n	No resolver nombres (IP/puertos en crudo).
netstat -a	ss	Todos los sockets o conexiones (TCP/UDP/unix, etc.).
netstat -at	ss -t	Todos los sockets o conexiones TCP (equivalente a <code>`-a`</code> implícito).
netstat -tuln	ss -tuln	Mostrar servicios TCP/UDP en escucha, sin DNS.
netstat -r	ip route	Tabla de enrutamiento (no ss, sino ip).
netstat -i	ip -s link	Estadísticas de interfaces de red.
netstat -s	no tiene un único equivalente directo	Estadísticas por protocolo; ss se enfoca más en sockets individuales.

netstat	ss	Descripción
netstat -a	ss o ss -a	Todas las conexiones/sockets
netstat -t	ss -t	Solo conexiones TCP
netstat -u	ss -u	Solo conexiones UDP
netstat -l	ss -l	Sockets en escucha (LISTEN)
netstat -tln	ss -tln	TCP listening, numérico
netstat -p	ss -p	Muestra PIDs/procesos (usa sudo)
netstat -s	ss -s	Estadísticas de sockets
netstat -r	ip route	Tabla de enrutamiento
netstat -i	ip -s link	Estadísticas de interfaces
netstat -n	ss -n	Numérico (sin resolución DNS)
netstat -tulpn	ss -tulpn	TCP/UDP listening con procesos

Enlaces

- Material obtenido en parte del artículo escrito por S3L3N1TY para Hacker's Land.
- <https://go.lightnode.com/es/tech/linux-netstat-command>
- <https://blog.elhacker.net/2014/11/ejemplos-con-el-comando-de-red-netstat-en-windows-linux.html>
- Youtube:
- <https://www.elarraydejota.com/utilidades-para-comprobar-sockets-en-linux/>
- <https://juncotic.com/ss-usas-netstat-es-hora-de-actualizarse/>
- <https://esgeeks.com/escanear-puertos-abiertos-ss-netstat-lsof-nmap/>

From:

<https://euloxio.myds.me/dokuwiki/> - **Euloxio wiki**

Permanent link:

<https://euloxio.myds.me/dokuwiki/doku.php/doc:tec:net:cmd:netstat:inicio?rev=1775722042>

Last update: **2026/04/09 10:07**

