Comandos
Que son?

Es una instrucción que el usuario proporciona a un sistema informático, desde la línea de órdenes o desde una llamada de programación. Puede ser interno o externo. Suele admitir parámetros o argumentos de entrada, lo que permite modificar su comportamiento predeterminado

Entre ellos existen:

Ip Config

Es una de las herramientas de línea de comandos más conocidas disponibles en Windows, ya que es muy útil para configurar y analizar redes. Los administradores utilizan principalmente este comando porque les permite realizar sus tareas de forma rápida y directa, sin tener que rebuscar en los engorrosos menús anidados de la interfaz de usuario de Windows. Incluso los usuarios finales pueden utilizar esta herramienta para resolver problemas de conexión a Internet y de red. En el siguiente artículo, echaremos un vistazo al comando ipconfig, que es útil para la instalación, configuración y administración de la red.

¿Para qué sirve?

Ipconfig es especialmente útil para obtener una visión rápida y concisa de los ajustes de configuración principales en la red TCP/IP y cubre todos los adaptadores e interfaces de red existentes (por ejemplo, LAN, WLAN, Bluetooth, RDSI y adaptadores VPN).

Administración y resolución de problemas de la red

Ser capaz de encontrar las direcciones IP asignadas puede ser muy útil para la administración de la red local y la resolución de problemas. El comando ipconfig puede mostrar tanto direcciones IPv4 como IPv6. El IPv6 todavía no es tan relevante como su predecesor el IPv4, pero en el futuro será cada vez más importante a la hora de asignar direcciones en las redes. Las direcciones IPv6 ya se utilizan más en el Internet de las Cosas (IoT, infraestructuras domésticas inteligentes).

Obtención y configuración de direcciones IP

La dirección IP de la ruta de acceso por defecto utilizada para navegar por Internet también puede obtenerse mediante el comando ipconfig (para los usuarios domésticos, suele ser la dirección de su router DSL). Además, este comando puede mostrar la información de la dirección de la máscara de subred y la puerta de enlace por defecto de todos los adaptadores de red. Incluso puedes utilizarlo para averiguar si se ha activado un proxy WINS (proxy de resolución de nombres con WINS) o el enrutamiento IP (un PC puede configurarse para reenviar paquetes de datos IP a otras redes).

Configuración de DHCP

Hoy en día, cualquier persona que configure una red utilizará generalmente el Dynamic Host Configuration Protocol (DHCP) para asignar direcciones IP. Así, los dispositivos conectados se integran en la red doméstica sin que el usuario tenga que intervenir mediante la asignación automática de direcciones IP. Si tienes algún problema al utilizar este tipo de configuración dinámica de la red o si quieres modificar manualmente la asignación de direcciones por otros motivos, ipconfig puede ayudarte.

Puedes gestionar y modificar las rutinas DHCP con ipconfig. Por ejemplo, puedes liberar y renovar una dirección IP si fue asignada incorrectamente por el servidor DHCP durante el proceso de asignación automática o si no es la que el usuario quería. También puedes encontrar información sobre los permisos DHCP y, por tanto, sobre cuándo se asignó una dirección DHCP y cuánto tiempo será válida. Las direcciones IP no son asignadas permanentemente por DHCP; solo son válidas durante un periodo de tiempo determinado. Los servidores y los clientes pueden finalizar, modificar o renovar esta asignación en cualquier momento.

Borrar la caché del DNS

La memoria caché del DNS acelera la recuperación de las páginas web almacenando los datos que se necesitan con frecuencia en una memoria temporal local para un acceso más rápido. Si los archivos que se almacenan allí para acelerar la resolución de nombres están corruptos, esto puede dar lugar a mensajes de error y problemas de acceso a las páginas web (por ejemplo, error HTTP 400). Las cachés también suponen un riesgo para la seguridad, ya que los hackers pueden extraer información importante de ellas y utilizarla, por ejemplo, para causar estragos en la banca online a través de la suplantación de DNS. Utilizando ipconfig, puedes borrar la caché de DNS y así eliminar problemas y riesgos de seguridad.

ipconfig también puede proporcionar información sobre el servidor DNS responsable de tu ordenador. Hay aún más aplicaciones que se pueden aprovechar con el comando ipconfig, que puedes encontrar en la siguiente tabla resumen.

Resumen de las opciones de ipconfig

El comando básico ipconfig mostrará información importante sobre la red. Sin embargo, esto no es, ni mucho menos, el alcance total de las capacidades de la herramienta. Añadiendo opciones al comando ipconfig, se convierte en una herramienta versátil para la administración y configuración de la red. En la siguiente tabla encontrarás una lista de las opciones básicas del comando ipconfig, así como explicaciones sobre su funcionamiento y la función de parámetros importantes:

- /? Muestra la ayuda de ipconfig

- /all Muestra toda la información de configuraciónPor ejemplo, muestra el servidor DNS correspondiente, las direcciones IP de todos los controladores si hay varias tarjetas de red, la ruta por defecto y la máscara de subred

- /allcompartments Muestra información sobre todos los compartimentos

- /release Publica la dirección IPEs posible indicar un adaptador específico (si hay varios adaptadores de red); el comando posterior /renew asigna entonces una nueva IP tras la publicación

- /release6 Publica la(s) dirección(es) IPv6 Se dirige específicamente al servidor DHCPv6 y publica direcciones IPv6

- /renew Renueva la dirección IPEs posible indicar un adaptador específico (si hay varios adaptadores de red)

- /renew6 Renueva la(s) dirección(es) IPv6Se dirige específicamente al servidor DHCPv6 y modifica la configuración DHCPv6

- /flushdns Borra la caché de resolución DNSRecomendado para cuando el contenido de una caché se ha dañado y puede resolver problemas, aumentar la seguridad y acelerar la navegación web

- /registerdns Renueva todos los permisos DHCP y el registro de nombres DNSRenueva el registro del servidor DNS; resuelve los problemas de actualización dinámica entre un cliente y el servidor DNS; este parámetro evita la necesidad de reiniciar el ordenador del cliente; la renovación de la configuración también puede resolver los problemas de conexión entre el ordenador y el ISP

- /displaydns Muestra el contenido de la caché de resolución DNS

- /showclassid Muestra todos los ID de clase DHCP de un adaptadorLos ID de clase DHCP permiten una gestión más precisa de la comunicación entre un cliente y un servidor DHCP. Son especialmente importantes para la configuración profesional de la red, como para implementar clases de usuarios específicas o para asignar opciones DHCP especiales a un grupo de clientes. A menudo, el objetivo es aumentar la seguridad de la red

- /setclassid Modifica el ID de la clase DHCPLos identificadores de clase DHCP permiten una gestión más precisa de la comunicación interna de la red. Son especialmente importantes para la configuración profesional de la red, como para implementar clases de usuario específicas o para integrar mecanismos de seguridad en la comunicación entre un cliente y el servidor DHCP

-

NetStat
Netstat, término derivado de “network” (red) y “statistics” (estadísticas), es un programa dirigido con órdenes ejecutadas en la línea de comandos que entrega estadísticas básicas sobre la totalidad de las actividades de red. También puede entregar información acerca de los puertos y direcciones a través de los cuales se ejecutan las conexiones TCP y UDP, al igual que los puertos abiertos para solicitudes.

Netstat se implementó por primera vez en 1983 en la BSD (Berkeley Software Distribution), uno de los derivados del sistema UNIX, cuya versión 4.2 fue la primera en soportar la familia de protocolos de Internet TCP/IP. Linux integró netstat por defecto en la versión de 1991, al igual que Windows desde la versión 3.11 (1993). Las diversas implementaciones son muy similares en cuanto a funcionalidad, aunque los parámetros de los comandos netstat y las salidas presentan ligeras diferencias de un sistema a otro.

¿Por qué es importante utilizar netstat?
En la lucha contra el tráfico desproporcionado y el software dañino, se está en posesión de una gran ventaja cuando se conocen las conexiones entrantes y salientes del ordenador o el servidor. Estas se establecen a través de la correspondiente dirección de red, que indica, entre otras cosas, qué puerto se abrió para el intercambio de datos.

El problema principal de estos puertos abiertos es que, de esta manera, se le da la oportunidad a terceros de introducir un software malicioso en el sistema. También existe la posibilidad de que un troyano que ya reside en tu sistema instale una backdoor (puerta trasera) y abra un puerto. Por ello, es recomendable comprobar regularmente los puertos abiertos del sistema, tarea en la que destaca especialmente netstat.

Además, las estadísticas detalladas no solo ofrecen información sobre los paquetes transmitidos desde el último inicio del sistema, sino también los errores que se hayan producido. En cuanto a la tabla de routing, que proporciona información sobre la ruta de los paquetes de datos a través de la red, también es posible acceder a ella mediante netstat.

¿Cómo funciona netstat?
Los servicios de netstat se utilizan a través de la línea de comandos del sistema. Si tienes un ordenador con un sistema operativo de Windows, vas a necesitar el símbolo del

sistema, que se puede iniciar en cualquier momento a través del cuadro de diálogo “Ejecutar”. Solo debes utilizar la combinación [tecla de Windows] + [R] e introducir “cmd”. A diferencia de Windows, en macOs y Linux se accede a la herramienta de red a través del terminal.

La sintaxis de los comandos netstat es diferente de un sistema a otro. Sin embargo, tienen el siguiente patrón en común:

netstat [-a] [-b] [-e] [-f] [-n] [-o] [-p Protocolo] [-r] [-s] [-t] [-x] [-y] [Intervalo] En la mayoría de los casos se coloca un guión (-) delante de los parámetros, pero cuando se combinan varias opciones, solo es necesario colocarlo delante del primer enlace:

netstat [-OPTION1] [-OPTION2] [-OPTION3] …

Los comandos netstat para Windows

Comando	Descripción de la opción
netstat	Modo estándar que informa sobre todas las conexiones de red activas
netstat -a	Enumerar también los puertos abiertos
netstat -e	Estadísticas de interfaz (paquetes de datos recibidos y enviados, etc.)
netstat -i	Abrir el menú general de netstat
netstat -n	Visualización numérica de direcciones y números de puerto
netstat -p	Mostrar las conexiones para el protocolo especificado, en este caso TCP (también posible: UDP, TCPv6 o UDPv6).
netstat -q	Listar todas las conexiones, todos los puertos TCP en escucha y todos los puertos TCP abiertos que no están en escucha.
netstat -r	Mostrar la tabla de routing
netstat -s	Recuperar las estadísticas sobre los protocolos de red importantes como TCP, IP o UDP.

Ping
Comprueba la conectividad a nivel de IP con otro equipo TCP/IP mediante el envío de mensajes de solicitud de eco del protocolo de mensajes de control de Internet (ICMP). Se muestra la recepción de los mensajes de respuesta de eco correspondientes, junto con los tiempos de ida y vuelta. ping es el comando TCP/IP principal que se usa para solucionar problemas de conectividad, disponibilidad y resolución de nombres. Si se usa sin parámetros, este comando muestra el contenido de la Ayuda.

También puede usar este comando para probar el nombre del equipo y la dirección IP del equipo. Si el ping a la dirección IP se realiza correctamente, pero el ping al nombre del equipo no, es posible que tenga un problema de resolución de nombres. En este caso, asegúrese de que el nombre de equipo que especifique se puede resolver a través del archivo hosts local, utilizando consultas del sistema de nombres de dominio (DNS) o mediante técnicas de resolución de nombres NetBIOS.

Parámetros del comando ping

Parámetro	Descripción
/t	Especifica que ping continúa enviando mensajes de solicitud de eco al destino hasta que se interrumpa. Para interrumpir y mostrar estadísticas, presione CTRL+ENTRAR. Para interrumpir y salir de este comando, presione CTRL+C.
/a	Especifica que la resolución inversa de nombres se realice en la dirección IP de destino. Si esta operación se completa con éxito, ping muestra el nombre del host correspondiente.
/n <count>	Especifica el número de mensajes de solicitud de eco que se envían. El valor predeterminado es 4.
/l <size>	Especifica la longitud, en bytes, del campo Data en los mensajes de solicitud de eco. El valor predeterminado es 32. El tamaño máximo es de 65,500.

/f	Especifica que los mensajes de solicitud de eco se envían con la marca No fragmentar en el encabezado IP establecido en 1 (disponible solo en IPv4).
/l <TTL>	Especifica el valor del campo Período de vida (TTL) en el encabezado IP para los mensajes de solicitud de eco enviados. El valor predeterminado es el valor TTL predeterminado para el host. El TTL máximo es 255.
/v <TOS>	Especifica el valor del campo Tipo de servicio (TOS) en el encabezado IP para los mensajes de solicitud de eco enviados (disponible solo en IPv4).
/r <count>	Especifica la opción Ruta de registro del encabezado IP que se usa para registrar la ruta de acceso tomada por el mensaje de solicitud de eco y el mensaje de respuesta de eco correspondiente (disponible solo en IPv4).
/s <count>	Especifica que se use la opción Internet timestamp en el encabezado IP para registrar la hora de llegada del mensaje de solicitud de eco y del correspondiente mensaje de respuesta de eco para cada salto.
/j <hostlist>	Especifica que los mensajes de solicitud de eco usan la opción Ruta de origen flexible en el encabezado IP con el conjunto de destinos intermedios especificados en hostlist (solo disponible en IPv4).
/k <hostlist>	Especifica que los mensajes de solicitud de eco usan la opción Ruta de origen estricta en el encabezado IP con el conjunto de destinos intermedios especificados en hostlist (solo disponible en IPv4).
/w <timeout>	Especifica la cantidad de tiempo, en milisegundos, para esperar el mensaje de respuesta de eco correspondiente a un mensaje de solicitud de eco determinado.

/R	Especifica que se realiza un seguimiento de la ruta de acceso de ida y vuelta (disponible solo en IPv6).
/S <Srcaddr>	Especifica la dirección de origen que se va a usar (disponible solo en IPv6).
/4	Especifica qué IPv4 se usa para hacer ping.
/6	Especifica qué IPv6 se usa para hacer ping.
<targetname>	Especifica el nombre del host o la dirección IP del destino.
/?	Muestra la ayuda en el símbolo del sistema.