ARP	Comando MS-DOS que mantiene en cache la correspondencia entre las direcciones IP y las direcciones físicas del adaptador o tarjeta de red. Es utilizado en tareas de redes para optimizar el rendimiento de las conexiones y para solucionar conflictos.
ASSOC	Muestra o modifica las asociaciones de las extensiones de archivos, o sea la acción que Windows debe realizar de acuerdo a la extensión que posea el archivo.
AT	El comando AT programa la ejecución de comandos y programas en un equipo a una hora y fecha especificadas. El servicio de programación debe estar en ejecución para utilizar el comando AT.
ATTRIB	Muestra o cambia los atributos de un archivo. En Windows se le asigna a cada archivo, de acuerdo a la función o al objetivo que van a desempeñar en el equipo un atributo, ya sea de archivo oculto, de sistema, solo lectura, etc. Con el comando ATTRIB es posible saber los establecidos en un archivo determinado y retirárselo o asignarle otro.
AUDITPOL	Es usado para mostrar o cambiar configuraciones de permisos
BITSADMIN	Es usado para crear, administrar y monitorear tareas de descargas y subidas de archivos.
BREAK	Establece o elimina la comprobación extendida de Ctrl+C en la consola.
BCDBOOT	Herramienta de reparación y creación de archivos de arranque BCD. La herramienta de línea de comandos bcdboot.exe se usa para copiar archivos de arranque imprescindibles a la partición del sistema y para crear un nuevo almacén de BCD en el sistema.
BCDEDIT	Editor del almacén de datos de la configuración de arranque (BCD) Puedes usar Bcdedit.exe para agregar, eliminar, editar y anexar entradas en el almacén de datos de la configuración de arranque.
BOOTCFG	Esta herramienta de línea de comandos se puede usar para configurar, consultar, cambiar o eliminar la configuración de la entrada de arranque en el archivo BOOT.INI en sistemas operativos anteriores a Windows Vista.
CACLS	Comando MS-DOS que muestra o modifica las listas de control de acceso (ACLs) de archivos.
CALL	Llama a un segundo batch desde uno en ejecución.
CD	Muestra el nombre o cambia al directorio actual
CHCP	Muestra o establece el número de página de códigos activa.
CHDIR	Muestra el nombre o cambia al directorio actual, igual que CD
CHKDSK	Chequea, comprueba y repara errores de disco.
CHOICE	Esta herramienta permite que los usuarios seleccionen un elemento de una lista de opciones y devuelve el índice de la opción seleccionada.
CIPHER	Muestra o altera el cifrado de directorios [archivos] en particiones NTFS.
CLEANMGR	Comando MS-DOS que libera espacio en disco, permite guardar en memoria tus opciones.
CLIP	Redirecciona el resultado de las herramientas de la línea de comandos al Portapapeles de Windows. Esta salida de texto se puede pegar en otros programas.
CLS	Borra y aclara los símbolos o texto en la pantalla.
CMD	Inicia una nueva instancia de la consola
CMDKEY	Crea, presenta y elimina nombres de usuario y contraseñas almacenados.
COLOR	Establece los colores de primer plano y fondo de la consola
COMP	Comando DOS que compara el contenido de dos archivos o un conjunto de archivos.

COMPACT	Este comando CMD muestra o cambia el estado de compresión de archivos en particiones NTFS.
CONVERT	Comando MS-DOS que convierte volúmenes FAT a volúmenes NTFS. No puede convertir la unidad actual.
COPY	Copia uno o más archivos en otra ubicación
CSCRIPT	Permite ejecutar en la consola archivos VBS conteniendo scripts escritos en lenguaje VBScript. También puede utilizarse en archivos batch con la opción //B, con lo que se evitarán los mensajes de error y avisos de secuencias de comandos
DATE	Muestra o establece la fecha.
DEL	Elimina uno o más archivos.
DEFRAG	Localiza y consolida archivos fragmentados en volúmenes locales para mejorar el rendimiento del sistema.
DIR	Muestra una lista de archivos y subdirectorios en un directorio.
DISM	Ofrece información, instala, desinstala, configura y actualiza características adicionales y paquetes de imágenes de Windows. Por ejemplo, para mostrar las características instaladas de Windows que se pueden desinstalar usa: DISM.exe /Online /English /Get-Features /Format:Table
DISKCOMP	Compara el contenido de dos disquetes.
DISKCOPY	Copia el contenido de un disquete en otro.
DISKPART	Muestra o configura las propiedades de partición de disco.
DOSKEY	Este comando CMD edita líneas de comando, memoriza comandos de Windows y crea macros.
DRIVERQUERY	Muestra el estado y las propiedades actuales del controlador de dispositivo.
ECHO	Muestra mensajes, o activa y desactiva el eco
ENDLOCAL	Termina la búsqueda de variables de entorno del archivo por lotes
ERASE	Elimina uno o más archivos, igual que DEL
EXPAND	Comando MS-DOS que expande uno o varios archivos comprimidos
EXIT	Sale del programa CMD.EXE (interfaz de comandos)
FC	Compara dos archivos o conjunto de archivos y muestra las diferencias entre ellos
FIND	Busca una cadena de texto en uno o más archivos.
FINDSTR	Busca cadenas de texto en archivos.
FOR	Ejecuta un comando de forma simultánea en varios archivos, permite reducir la cantidad de código necesario en varias tareas. Es uno de los comandos que ofrece mayores beneficios prácticos.
FORFILES	Comando de uso algo similar a FOR, selecciona uno o varios archivos y ejecuta un comando en cada uno de ellos. Permite multitud de opciones útiles poco explotadas.
FORMAT	Permite darle diferentes formatos a discos duros u otros dispositivos para usarlo con Windows
FSUTIL	Comando DOS que muestra o configura las propiedades de sistema de archivos. Posee varios subcomandos para la administración efectiva del sistema de archivos y volúmenes.

FTYPE	Muestra o modifica los tipos de archivo usados en una asociación de extensión de archivo
GOTO	Direcciona el intérprete de comandos de Windows a una línea en un archivo batch.
GPRESULT	Comando MS-DOS que muestra información de directivas de grupo por equipo o usuario
GPUPDATE	Actualiza los cambios hechos en el Editor de directivas de grupo local. Permite que se active cualquiera de las directivas establecidas ya sea inmediatamente, al reiniciar o al iniciar sesión. Para lograr que se activen inmediatamente usa: GPUPDATE /force
GRAFTABL	Permite a Windows mostrar un juego de caracteres extendidos en modo gráfico
HELP	Proporciona información de ayuda para los comandos de Windows
ICACLS	Comando MS-DOS que Mmestra, modifica, hace copias de seguridad o restaura listas de control de acceso (ACL) para archivos y directorios
IF	Ejecuta comandos de forma condicional, se utiliza para definir valores de error, comparar cadenas, demostrar existencia de archivos y hacer comparaciones matemáticas.
IPCONFIG	Muestra los parámetros de una conexión de red. De forma predeterminada, se muestra solamente la dirección IP, la máscara de subred y la puerta de enlace predeterminada para cada adaptador enlazado conTCP/IP.
LABEL	Este comando CMD Crea, cambia o elimina la etiqueta del volumen de un disco
MEM	Muestra la cantidad de memoria libre y usada en el sistema
MD	Crea un directorio o carpeta
MKDIR	Comando DOS para crea un directorio, igual que el anterior
MKLINK	Crea vínculos simbólicos y vínculos físicos
MODE	Configura un dispositivo de sistema
MORE	Comando MS-DOS que muestra la información pantalla por pantalla
MOVE	Mueve uno o más archivos de un directorio a otro en la misma unidad
MSTSC	Inicia una conexión remota al escritorio
NBTSTAT	Muestra las estadísticas del protocolo y las conexiones actuales de TCP/IP usando NBT (NetBIOS sobre TCP/IP)
NET	Configura una amplia variedad de parámetros en redes.
NETCFG	Es utilizado para instalar Windows Preinstallation Environment (WinPE), una versión minima y ligera de Windows usada por desarrolladores
NETSH	El comando NETSH (Network Shell) permite configurar, determinar conflictos y administrar diferentes componentes de redes mediante la línea de comandos de forma local o remota. Muestra y configura el estatus de los componentes de los protocolos de redes instalados. Los comandos de Netsh están organizado en forma de árbol, cada tecnología y protocolo tiene su propio contexto.
NETSTAT	Muestra estadísticas del protocolo y conexiones TCP/IP actuales. Permite el monitoreo de todas las conexiones activas
NLSFUNC	Carga la información especifica de un país o región

NLTEST	El comando NLTEST se utiliza para realizar pruebas mediante canales seguros entre los ordenadores Windows de diferentes dominios y entre controladores de dominio que son de confianza
NSLOOKUP	Este comando CMD muestra información sobre los servidores DNS asignados a tu conexión de red. Permite hacer peticiones a estos servidores.
OCSETUP	Inicia Windows Optional Component Setup herramienta que instala opciones adicionales de Windows
OPENFILES	Comando DOS que muestra archivos compartidos abiertos por usuarios remotos
PATH	Muestra o establece una ruta de búsqueda para archivos ejecutables
PAUSE	Comando MS-DOS que pausa la consola y muestra un mensaje
PING	Permite probar una conexión de red, enviando y recibiendo un paquete de datos.
POPD	Restaura el valor anterior del directorio actual guardado por PUSHD
POWERSHELL	Ejecuta una instancia de Windows PowerShell, la nueva consola de comandos que incluye Windows en sistemas posteriores a Windows Vista. Al mostrarse PS en el símbolo de la consola significa que te encuentras en el entorno de PowerShell, por lo que introduzcas a partir de ese momento estará relacionado con este intérprete, para volver a la consola solo escribe CMD y presiona Enter.
PRINT	Imprime un archivo de texto
PROMPT	Cambia el símbolo de comandos de Windows
PUSHD	Comando MS-DOS que guarda el directorio actual y después lo cambia
QAPPSRV	Muestra los servidores host de sesión de Escritorio remoto disponibles en la red
QPROCESS	Muestra información sobre procesos
QUERY	Muestra el status actual y los parámetros de un servicio especifico
QUSER	Mostrar información sobre los usuarios que han registrado la entrada en el sistema
QWINSTA	Muestra información sobre las sesiones de Escritorio remoto
RASDIAL	Es usado para iniciar o detener una conexión de acceso telefónico o dial up
RD	Quita o elimina un directorio o carpeta
RECOVER	Comando DOS para recuperar la información legible de un disco dañado o defectuoso
REG	Es usado para administrar todos los parámetros del Editor del Registro desde la línea de comandos y archivos batch. Es posible agregar, modificar claves, valores, exportar ramas, etc. El comando REG se compone de varios subcomandos, cada uno para un uso completamente diferente, son: REG QUERY, REG ADD, REG DELETE, REG COPY, REG SAVE , REG RESTORE, REG LOAD, REG UNLOAD, REG COMPARE, REG EXPORT, REG IMPORT y REG FLAGS
REGEDIT	El comando REGEDIT permite importar, exportar o eliminar configuraciones en el registro desde un archivo de texto plano de extensión .reg.
REGSVR32	Registra librerías DLL para incorporarlas al registro
RELOG	Relog crea nuevos registros de rendimiento a partir de datos de registros de rendimiento existentes cambiando el intervalo de muestreo o convirtiendo el formato de archivo.

	Admite todos los formatos de registro de rendimiento, incluidos los registros comprimidos de Windows NT 4.0
REM	Marca comentarios en archivos por lotes o CONFIG.SYS. La línea en un batch que comienza con REM es considerada un comentario
REN	Comando DOS que cambia el nombre de uno o más archivos
RENAME	Cambia el nombre de uno o más archivos, igual que el anterior
REPLACE	Reemplaza archivos
RMDIR	Quita un directorio
ROBOCOPY	Utilidad avanzada para copiar carpetas y directorios en Windows.
RESET SESSION	(Rwinsta) Volver a establecer el hardware y el software de subsistema de la sesión con los valores iniciales conocidos
ROUTE	Comando DOS para manipular tablas de enrutamiento de red
RPCPING	Hace ping al servidor mediante RPC
RUNAS	Es usado para ejecutar un programa utilizando credenciales o derechos de otro usuario
SECEDIT	Analiza la seguridad del sistema y hace la comparación con una plantilla determinada
SET	Muestra, establece o quita variables de entorno de Windows
SETLOCAL	Comienza la sección de cambios locales de entorno en la consola
SETVER	El comando SETVER se utiliza para establecer el número de versión de MS-DOS que se informa a un programa
SETX	Crea o modifica variables de entorno en el entorno de usuario o de sistema. Puede establecer variables basadas en argumentos, claves de Registro o entrada de archivos
SC	Muestra o configura servicios (procesos en segundo plano).
SCHTASKS	Ejecuta el Programador de tareas. Programa comandos y programas para ejecutarse en un equipo.
SFC	Comprobador de recursos de Microsoft Examina la integridad de todos los archivos de sistema protegidos y reemplaza las versiones incorrectas por las correctas de Microsoft
SHADOW	Supervisar otra sesión de Servicios de Escritorio remoto
SHARE	El comando SHARE se utiliza para bloquear archivos y funciones en MS-DOS
SXSTRACE	Utilidad de seguimiento de WinSxs
SHIFT	Cambia posición de modificadores reemplazables en archivos por lotes
SHUTDOWN	Permite el apagado, el reinicio, suspensión e hibernación local o remoto de un equipo
SORT	Ordena los resultados de un comando seleccionado, por ejemplo los resultados de una búsqueda con FIND
START	Inicia otra ventana para ejecutar un programa o comando
SUBST	Asocia una ruta de acceso con una letra de unidad
SYSTEMINFO	Muestra las propiedades y la configuración específicas del equipo
TAKEOWN	Esta herramienta permite que el administrador recupere el acceso a un archivo denegado mediante la reasignación de la propiedad del archivo.

TASKLIST	Muestra todas las tareas en ejecución, incluidos los servicios
TASKKILL	Comando MS-DOS que termina o interrumpe un proceso o aplicación que se está ejecutando
TCMSETUP	Este comando DOS es usado para configurar o deshabilitar el cliente de telefonía Telephony Application Programming Interface (TAPI)
TIME	Muestra o establece la hora del sistema
TIMEOUT	Esta utilidad acepta un parámetro de tiempo de espera para esperar el un período de tiempo determinado (en segundos) o hasta que se presiona alguna tecla. También acepta un parámetro para omitir la presión de tecla
TITLE	Establece el título de la ventana de una sesión de CMD.EXE
TRACERPT	El comando TRACERPT se utiliza para procesar los registros de seguimiento de sucesos o datos en tiempo real
TRACERT	Permite hacer un seguimiento de la ruta entre un equipo y otro en la red, es muy utilizado para conocer dónde se ha detenido un paquete de datos en la red.
TREE	Comando DOS que muestra gráficamente la estructura de directorios de una unidad o ruta de acceso
TSDISCON	Desconecta una sesión de Escritorio remoto
TSKILL	Termina un proceso
TYPE	Muestra el contenido de un archivo de texto
TYPEPERF	Typeperf escribe información de rendimiento en la ventana de comandos o en un archivo de registro. Para detener Typeperf presione CTRL+C
TZUTIL	Utilidad de zona horaria de Windows
UNLODCTR	Quita el nombre de contador y texto explicativo para el contador extensible especificado
VER	Muestra la versión de Windows
VERIFY	Comunica a Windows si debe comprobar que los archivos se escriben de forma correcta en un disco
VOL	Muestra la etiqueta del volumen y el número de serie del disco
VSSADMIN	Herramienta administrativa del Servicio de instantáneas de volumen, las imágenes creadas por Windows para la función Restaurar sistema. Por ejemplo, para listar todas las imágenes existentes usa: VSSADMIN list shadows
W32TM	Herramienta usada para diagnosticar conflictos del equipo local o de uno en la red con el servicio Hora de Windows (Windows time) al tratar de sincronizar o de actualizar el reloj del sistema
WAITFOR	Esta herramienta envía o espera a que llegue una señal en un sistema. Si no se especifica /S la señal se difundirá a todos los sistema de un dominio. Si se especifica /S la señal sólo se enviará al dominio especificado
WBADMIN	Herramienta de línea de comandos de copia de seguridad
WEVTUTIL	Utilidad de línea de comandos de eventos de Windows. Permite recuperar información acerca de registros de eventos y publicadores, instalar y desinstalar manifiestos de eventos, ejecutar consultas y exportar, archivar y borrar registros

WHERE	Comandos DOS que muestra la ubicación de archivos que coinciden con el patrón de búsqueda. De manera predeterminada, la búsqueda se realiza en el directorio actual y en las rutas especificadas por la variable de entorno PATH
WHOAMI	Esta utilidad se puede usar para obtener el destino de información de grupo y nombre de usuario junto con los respectivos identificadores de seguridad (SID), privilegios, identificador de inicio de sesión (Id. de inicio de sesión) del usuario actual (testigo de acceso) en el sistema local. Es decir, quién es el usuario actualmente conectado. Si no se especifica ningún modificador, la herramienta muestra nombre de usuario en formato NTLM (dominio\nombre_usuario)
WINHLP32	Comando de MS-DOS que ejecuta los archivos de ayuda de Windows que usan la extensión HLP
WINRM	Herramienta de la línea de comandos de Administración remota de Windows Administración remota de Windows (WinRM) es la implementación de Microsoft del protocolo WS-Management, que proporciona una forma segura de comunicarse con equipos locales y remotos mediante servicios Web
WINRS	Comando DOS que abre una ventana de comandos en modo seguro con un equipo en la red
WINSAT	Herramienta de evaluación del sistema de Windows (WinSAT)
WMIC	Muestra información de WMI en el shell de comandos interactivo. Permite acceder a todo tipo de informaciones, tanto de el equipo local o a otro en la red, enumera todos los datos del hardware y del software disponibles
XCOPY	Copia archivos y árboles de directorios

Ejemplos de uso:

- **copy *archivo_origen archivo_destino***: Crea un archivo duplicado de cualquier fichero.
- **del *archivo.txt***: Elimina el archivo seleccionado, en este caso, el fichero de nombre *fastboot.txt*.
- ***shutdown –r –f –t 5**: Reinicio de equipo tras 5 segundos de espera.*
- **net user *nombreusuario* /domain**: Muestra las propiedades de un usuario del dominio (ultimo cambio de contraseña, cuenta activa o no, grupos a los que pertenece…).
- **systeminfo**: Muestra todas las propiedades del equipo como el sistema operativo, procesador, nombre del equipo, memoria física y virtual etc.
- **nbtstat –a *ip_equipo***: Introduciendo la IP de un equipo puedes obtener el nombre de la maquina y la MAC
- **netsh wlan show profile *WIFI* key=clear**: Sustituyendo WIFI por el nombre de la red WiFi que nos interesa, podemos **sacar la contraseña de cualquier red wifi** a la que nos hayamos conectado previamente en un PC.

PING

Si necesitas una herramienta de diagnóstico que permita hacer verificaciones de estado de un determinado host local o remoto, te presento uno de los comandos más utilizados, este es, ni más ni menos que ping.

Siempre que necesites hacer una verificación sobre un dispositivo interconectado en una infraestructura de red se encuentra levantado o no, la primera prueba básica debe ser lanzar una consulta al protocolo de red ICMP (*Internet Control Message Protocol*) en una red de tipo TCP/IP (Protocolo de Control de Transmisión / Protocolo de Internet).

Ping es un acrónimo de *Packet Internet Groper* que en español se traduce a un buscador de paquetes en redes.

Aunque la mayoría de los usuarios que aplican un uso básico de la consola, usan este comando para saber si existe conectividad a internet.

```
ping -n 5 8.8.8.8
```

Se lanza una solicitud de conexión a la dirección 8.8.8.8, que representa el DNS de Google, a lo cual este siempre debería de responder, de lo que, si funciona, podemos deducir que se está llegando correctamente y que existe buena conectividad.

Además, se agrega un número de solicitudes, por lo que se abordarán 5.

Esta es la salida de la ejecución:

```
> ping -n 5 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=71ms TTL=113
Respuesta desde 8.8.8.8: bytes=32 tiempo=69ms TTL=113
Respuesta desde 8.8.8.8: bytes=32 tiempo=72ms TTL=113
Respuesta desde 8.8.8.8: bytes=32 tiempo=67ms TTL=113
Respuesta desde 8.8.8.8: bytes=32 tiempo=65ms TTL=113

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 5, recibidos = 5, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 65ms, Máximo = 72ms, Media = 68ms
```

En la respuesta existen datos generales a observar, dentro de ellos, las estadísticas de ping y tiempos aproximados de ida y vuelta en milisegundos para la dirección IP solicitada, devolviendo como datos de paquetes: `enviados = 5`, `recibidos = 5`, `perdidos = 0` (`0% perdidos`). Lo que es un buen indicio de que todo ha resultado correctamente.

También se puede notar que hay siglas como TTL (*Time To Live*) que significa que es el tiempo de vida del paquete enviado con un valor máximo de 113 según este caso.

Al ejecutar este comando sin parámetros, por omisión enviará 4 solicitudes eco, con tiempo de espera de 1 segundo, con tamaño del paquete de 32 bytes y permitiendo fragmentación.

Por supuesto, este comando tiene parámetros que hacen que sea más interesante, como seleccionar el `tipo de servicio`, `registrar rutas de saltos`, `dirección de origen que se desea usar`, entre otros.

IPCONFIG

Obtener datos de la configuración de red TCP/IP nunca fue tan sencillo como utilizar el comando `ipconfig`, que precisamente obtener esta información y actualiza la configuración del protocolo de configuración dinámica de host (DHCP) y del sistema de nombres de dominio (DNS).

El modo de uso es tan sencillo como escribir: `ipconfig`.
Te muestro cómo filtra la información por el protocolo `IPv4`.

```
ipconfig | find "IPv4"
```

De este modo, en la salida generará las direcciones IPv4 de todos los adaptadores de red instalados en el equipo.

```
> ipconfig | find "IPv4"

Dirección IPv4. . . . . . . . . . . . . . : 192.168.56.1
Dirección IPv4. . . . . . . . . . . . . . : 192.168.2.1
Dirección IPv4. . . . . . . . . . . . . . : 192.168.0.2
```

Para mostrar la configuración de TCP/IP completa para todos los adaptadores, escriba `ipconfig /all`, sin embargo, para ser un poco más precisos, extraeremos la `Descripción` de cada adaptador de red. En caso de que tengas el ordenador en inglés, escribes `Description`.

```
ipconfig /all | find "Descripción"
```

Devuelve solo la descripción de los adaptadores de red que tiene instalado el equipo:

```
> ipconfig /all | find "Descripción"
Descripción . . . . . . . . . . . . . . . : Realtek PCIe GbE Family Controller
Descripción . . . . . . . . . . . . . . . : VirtualBox Host-Only Ethernet
Adapter
Descripción . . . . . . . . . . . . . . . : TAP-Windows Adapter V9
Descripción . . . . . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual
Adapter
Descripción . . . . . . . . . . . . . . . : Fortinet Virtual Ethernet Adapter
(NDIS 6.30)
```

```
Descripción . . . . . . . . . . . . . . . : Qualcomm Atheros QCA9377 Wireless
Network Adapter
Descripción . . . . . . . . . . . . . . . : Bluetooth Device (Personal Area
Network)
Descripción . . . . . . . . . . . . . . . : Hyper-V Virtual Ethernet Adapter
```

Este comando tiene más instrucciones interesantes como, por ejemplo: hacer `releases` para liberar direcciones IPv4 e IPv6 para un adaptador especificado; aplica una purga de memoria caché de resolución DNS, actualizar concesiones DHCP, entre otras.

HOSTNAME

Muestra el nombre del host actual. Este, probablemente es de los comandos de red más sencillos que existen.

Curiosamente, si no tienes una IP específica para conectarte a un host dentro de una red donde comparten un segmento de red, otra forma es haciéndolo por medio del nombre del host, que este caso, la forma de obtenerlo por consola sería ejecutando `hostname`.

```
> hostname
DESKTOP-V88H2KJ
```

Por supuesto, te comando un par de formas extras por la que se puede sacar este dato, uno de los comandos a utilizar es uno que he mostrado anteriormente, el `ipconfig`. A este, se le pasa un filtro, por ejemplo:

```
> ipconfig /all | find "Nombre de host"
Nombre de host. . . . . . . . . . : DESKTOP-V88H2KJ
```

Otra forma elegante de hacerlo, es imprimiendo la variable de entorno `%userdomain%`:

```
> echo %userdomain%
DESKTOP-V88H2KJ
```

Como lograste observar, existen muchas formas de obtener este dato.

GETMAC

Como lo dice su nombre, obtiene las direcciones MAC (*Media Access Control*) que tienen asociadas los adaptadores de red.

```
> getmac

Dirección física    Nombre de transporte
=================== ============================================================
94-E9-79-FC-C4-A1   \Device\Tcpip_{E37EA3CF-F069-4C00-A406-0353E99AEE57}
0A-00-27-00-00-02   \Device\Tcpip_{069DA379-D55C-4AA7-B3D8-F522C38CCA13}
0A-00-27-00-00-11   \Device\Tcpip_{746EABE9-EF7F-46E5-A08A-ABB9943613D2}
00-15-5D-66-50-5D   \Device\Tcpip_{70D4746D-922E-421B-AF07-F66CEA96527B}
N/A                 Hardware ausente
```

Por supuesto, el comando `ipconfig` es tan poderoso que esta información ya la tiene en cuenta, solo habría que hacer un filtro para generar específicamente las direcciones físicas, de la siguiente manera:

```
ipconfig /all | find "Dirección física"
```

Un comando muy sencillo, pero que te puede sacar de apuros cuando desees conocer información específica de un adaptador de red.

ARP

Muestra y modifica las tablas de conversión de direcciones IP en direcciones físicas que utiliza el protocolo de resolución de direcciones ARP (*Address Resolution Protocol*).

La caché ARP contiene una o más tablas que se utilizan para almacenar direcciones IP y sus direcciones físicas Ethernet o Token Ring resueltas.

Para mostrar las tablas de caché arp para todas las interfaces, escriba:

```
> arp /a

Interfaz: 192.168.56.1 --- 0x2
  Dirección de Internet          Dirección física      Tipo
  192.168.56.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.22             01-00-5e-00-00-16     estático
  224.0.0.251            01-00-5e-00-00-fb     estático
  224.0.0.252            01-00-5e-00-00-fc     estático
  239.255.255.250        01-00-5e-7f-ff-fa     estático

Interfaz: 192.168.2.1 --- 0x11
  Dirección de Internet          Dirección física      Tipo
  192.168.2.255          ff-ff-ff-ff-ff-ff     estático
  224.0.0.22             01-00-5e-00-00-16     estático
  224.0.0.251            01-00-5e-00-00-fb     estático
  224.0.0.252            01-00-5e-00-00-fc     estático
  239.255.255.250        01-00-5e-7f-ff-fa     estático
```

Las direcciones IP de `inetaddr` e `ifaceaddr` se expresan en notación decimal con puntos.

La dirección física de `etheraddr` consta de seis bytes expresados en notación hexadecimal y separados por guiones (por ejemplo, 00-AA-00-4F-2A-9C).

Las entradas agregadas con el parámetro `/s` son estáticas y no se agota el tiempo de espera de la caché arp. Las entradas se eliminan si el protocolo `TCP/IP` se detiene y se inicia. Para crear entradas de caché arp estáticas permanentes, coloque los comandos arp apropiados en un archivo por lotes y use tareas programadas para ejecutar el archivo por lotes al inicio.

También puede mostrar la tabla caché de una interfaz de red específica e incluso, agregar una entrada que resuelve una dirección IP.

NSLOOKUP

Este es de los comandos más útiles al momento de diagnosticar la infraestructura del sistema de nombres de dominio (DNS).

La herramienta de línea de comandos `nslookup` tiene dos modos: interactivo y no interactivo.

Si necesita buscar solo un dato, se recomienda que utilice el modo no interactivo. Para el primer parámetro, escriba el nombre o la dirección IP de la computadora que desea buscar. Para el segundo parámetro, escriba el nombre o la dirección IP de un servidor de nombres DNS.

```
> nslookup openwebinars.net 8.8.8.8
Servidor:  dns.google
Address:  8.8.8.8

Respuesta no autoritativa:
Nombre:  openwebinars.net
Address:  82.196.7.188
```

.

NBTSTAT

Muestra las estadísticas del protocolo `NetBIOS` sobre TCP/IP (`NetBT`), las tablas de nombres NetBIOS para la computadora local, las computadoras remotas y la caché.

Este comando está disponible solo si el Protocolo de Internet (TCP/IP) está instalado como un componente en las propiedades de un adaptador de red en Conexiones de red.

Para mostrar la tabla de nombres NetBIOS de la computadora local:

```
nbtstat /n
```

Para mostrar el contenido de la caché de nombres NetBIOS del equipo local:

```
nbtstat /c
```

Para mostrar las estadísticas de la sesión NetBIOS por dirección IP cada cinco segundos, escriba:

```
nbtstat /S 5
```

Para purgar la caché de nombres NetBIOS y volver a cargar las entradas *preetiquetadas en el* archivo *Lmhosts* local, escriba lo siguiente:

```
nbtstat /R
nbtstat /RR
```

Este último también sirve para liberar los nombres NetBIOS con el servidor WINS y volver a registrarlos.

NETSTAT

Muestra las conexiones TCP activas, los puertos en los que la computadora está escuchando, las estadísticas de Ethernet, la tabla de enrutamiento de IP, las estadísticas de IPv4 (para los protocolos `IP`, `ICMP`, `TCP` y `UDP`) y las estadísticas de IPv6 (para `IPv6`, `ICMPv6`, `TCP` sobre IPv6 y `UDP` sobre protocolos IPv6).

Para mostrar tanto las estadísticas de Ethernet como las estadísticas de todos los protocolos:

```
netstat -e -s
```

Para mostrar las estadísticas solo para los protocolos TCP y UDP:

```
netstat -s -p tcp udp
```

Para mostrar las conexiones TCP activas y los ID de proceso cada 5 segundos:

```
netstat -o 5
```

Para mostrar las conexiones TCP activas y los ID de proceso en forma numérica:

```
netstat -n -o
```

La diferencia con el anterior `nbtstat` es que este no usa NetBIOS.

NET USE

Este comando `net use` es una instrucción que se utiliza para conectarse, eliminar y configurar conexiones a recursos compartidos, como unidades asignadas e impresoras de red.

Es uno de los muchos como `net send`, `net user`, `net time`, `net view` , etc.

```
net use * "\\hostname_o_ip_servidor\mi_unidad" /persistent:no
```

En este ejemplo, usamos el comando `net use` para conectarnos a la carpeta compartida *mi_unidad* en una computadora llamada *hostname_o_ip_servidor* . La carpeta *mi_unidad* se asignará a la letra de unidad más alta disponible [*****], que en nuestro ejemplo es `y:`, pero no queremos seguir mapeando esta unidad cada vez que iniciamos sesión en la computadora [**/persistent: no**].

Este comando es muy interesante, ya que permite conectarse a discos de equipos remotos, permitiendo loguearse en red.

TASKKILL

Es probable que te sorprenda ver este comando en la lista, pues este lo que hace es finalizar procesos o tareas en ejecución, sin embargo, una característica que lo

hace estar aquí es que también puede finalizar procesos en equipos remotos, de la siguiente manera:

```
taskkill /s remote_host /u maindom\user_profile /p p@ssW23 /fi "IMAGENAME eq
nota*" /im *
```

Para finalizar todos los procesos en la computadora remota *remote_host* con un nombre de imagen que comience con una *nota* , mientras usa las credenciales de la cuenta de usuario *user_profile* y la contraseña *p@ssW23*.

SHUTDOWN

Le permite apagar o reiniciar computadoras locales o remotas, una a la vez.

Para forzar el cierre de las aplicaciones y reiniciar la computadora local después de un retraso de un minuto, con el motivo *Aplicación: Mantenimiento (planificado)* y el comentario “Reconfiguración de miapp.exe”.

```
shutdown /r /t 60 /c "Reconfiguración miapp.exe" /f /d p:4:1
```

Para reiniciar la computadora remota *mi_servidor_remoto* con los mismos parámetros que en el ejemplo anterior:

```
shutdown /r /m \\mi_servidor_remoto /t 60 /c "Reconfiguración miapp.exe" /f /d
p:4:1
```

Finalmente, si lo que deseas es apagarla, bastará con pasar el parámetro: `/s`.

TRACERT

Esta es una de las principales herramientas de diagnóstico que determina la ruta tomada a un destino mediante el envío de solicitudes de eco del protocolo ICMP o mensajes ICMPv6 al destino con valores de campo de tiempo de vida (TTL) que se mantienen incrementando.

Cada enrutador a lo largo de la ruta debe disminuir el TTL en un paquete IP en al menos 1 antes de reenviarlo. Efectivamente, el TTL es un contador de enlaces máximo. Cuando el TTL de un paquete llega a 0, se espera que el enrutador devuelva un mensaje de tiempo ICMP excedido a la computadora de origen.

Este comando determina la ruta enviando el primer mensaje de solicitud de eco con un TTL de 1 e incrementando el TTL en 1 en cada transmisión subsiguiente hasta que el objetivo responda o se alcance el número máximo de saltos. El número máximo de saltos es 30 de forma predeterminada y se puede especificar mediante el parámetro /h .

Para rastrear la ruta al host llamado *openwebinars.net*:

```
> tracert openwebinars.net

Traza a la dirección openwebinars.net [82.196.7.188]
```

```
sobre un máximo de 30 saltos:

  1     3 ms     4 ms     3 ms  192.168.0.1
  2    23 ms    30 ms    18 ms  10.36.128.1
  3    14 ms    13 ms    11 ms  10.5.38.145
  4     *        *        *     Tiempo de espera agotado para esta solicitud.
  5    13 ms    13 ms    11 ms  10.5.38.13
  6    13 ms     *       14 ms  one.one.one.one [1.1.1.1]
  7    14 ms    15 ms    13 ms  ip-190-53-44-121.ni.amnetdatos.net
[190.53.44.121]
  8    17 ms    14 ms    14 ms  190.124.33.241
  9    68 ms    68 ms    66 ms  10.30.1.1
 10    71 ms    73 ms    70 ms  mai-b1-link.telia.net [62.115.56.164]
 11    96 ms    96 ms    93 ms  rest-bb1-link.telia.net [62.115.119.230]
 12   204 ms   193 ms   185 ms  prs-bb4-link.telia.net [62.115.122.158]
 13   185 ms   183 ms   184 ms  adm-bb4-link.telia.net [213.155.136.167]
 14   187 ms   188 ms   183 ms  adm-b1-link.telia.net [62.115.137.65]
 15   184 ms   186 ms   184 ms  digitalocean-ic-335926-adm-b1.c.telia.net
[213.248.81.75]
 16   186 ms   185 ms   182 ms  138.197.244.74
 17     *        *        *     Tiempo de espera agotado para esta solicitud.
 18   187 ms   185 ms   184 ms  82.196.7.188

Traza completa.
```

Para rastrear la ruta al host llamado *openwebinars.net* y evitar la resolución de cada dirección IP a su nombre:

```
tracert /d openwebinars.net
```

Como pueden observar, además de extraer los saltos que se hacen para llegar a un destino, se podría escudriñar más información relevante.

PATHPING

Este comando proporciona información sobre la latencia de red y la pérdida en saltos intermedios entre un origen y un destino. Este comando envía varios mensajes de solicitud de eco a cada enrutador entre un origen y un destino, durante un período de tiempo, y luego calcula los resultados en función de los paquetes devueltos por cada enrutador.

Debido a que este comando muestra el grado de pérdida de paquetes en cualquier enrutador o enlace determinado, puede determinar qué enrutadores o subredes podrían tener problemas de red.

```
> pathping openwebinars.net

Seguimiento de ruta a openwebinars.net [82.196.7.188]
sobre un máximo de 30 saltos:
  0  DESKTOP-V88H2KJ [192.168.0.2]
  1  192.168.0.1
  2  10.36.128.1
  3  10.5.38.145
  4     *        *        *
Procesamiento de estadísticas durante 75 segundos...
              Origen hasta aquí   Este Nodo/Vínculo
```

```
Salto  RTT    Perdido/Enviado = Pct  Perdido/Enviado = Pct  Dirección
  0                                                 DESKTOP-V88H2KJ [192.168.0.2]
                               0/ 100 =  0%   |
  1    3ms     0/ 100 =  0%     0/ 100 =  0%  192.168.0.1
                               0/ 100 =  0%   |
  2   32ms     0/ 100 =  0%     0/ 100 =  0%  10.36.128.1
                               0/ 100 =  0%   |
  3   10ms     0/ 100 =  0%     0/ 100 =  0%  10.5.38.145

Traza completa.
```

Una nota interesante: este comando identifica qué enrutadores están en la ruta, al igual que usar el comando `tracert`. También envía `pings` periódicamente a todos los enrutadores durante un período de tiempo específico y calcula estadísticas basadas en el número devuelto por cada uno.

TELNET

Abrir comunicación con un equipo remoto que ejecuta el servicio del servidor telnet.

Importante: debe instalar el software de cliente telnet antes de poder ejecutar este comando.

Para usar telnet para conectarse a la computadora que ejecuta el servicio del servidor telnet en *telnet.microsoft.com* , escriba:

```
telnet telnet.microsoft.com
```

Para usar telnet para conectarse a la computadora que ejecuta el servicio del servidor telnet en *telnet.microsoft.com en el puerto TCP 44* y registrar la actividad de la sesión en un archivo local llamado *telnetlog.txt* :

```
telnet /f telnetlog.txt telnet.microsoft.com 44
```

ROUTE

Manipula tablas de enrutamiento de red. Este comando tiene la capacidad de borrar las tablas de enrutamiento de todas las entradas de puerta de enlace. Además, cuando se usa el comando `ADD`, hace una ruta persistente en el arranque de los sistemas.

El siguiente comando permite mostrar las direcciones MAC asociadas a un adaptador (lista de interfaces) y IPv4 y IPv6 tablas de enrutamiento:

```
route PRINT
```

Algunos ejemplos:

```
> route PRINT
> route PRINT -4
> route PRINT -6
```

```
> route PRINT 157*          .... solo imprime lo que coincida con 157*

> route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
                destino^      ^máscara   ^puerta de  métrica^    ^
                                          enlace         interfaz^

      Si no se proporciona IF, intenta buscar la mejor interfaz para una
      puerta de enlace específica.
> route ADD 3ffe::/32 3ffe::1

> route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2

      CHANGE solo se usa para modificar la puerta de enlace o la métrica.

> route DELETE 157.0.0.0
> route DELETE 3ffe::/32
```

En tu tabla de enrutamiento podrás encontrar atributos como: `Destino de red`, `Máscara de red`, `Puerta de enlace`, `Interfaz` y`Métrica`.

NETSH

Puedo afirmar que este es uno de los comandos más potentes del sistema en cuestiones de redes.

La utilidad de secuencia de comandos de la línea de comandos `Network Shell` que le permite, ya sea de forma local o remota, mostrar o modificar la configuración de red de una computadora en ejecución.

Restablecer la pila TCP / IP con Netsh

Un uso común de los comandos Netsh es el restablecimiento de la pila TCP/IP que maneja el intercambio de paquetes de datos en las redes. Si aparecen problemas en la red y en Internet, esta medida puede ser de utilidad, ya que elimina, por ejemplo, los defectos o la configuración incorrecta de protocolos TCP/IP. El siguiente comando de **reparación** realiza un restablecimiento y reinstala el TCP/IPv4:

```
netsh int ip reset
```

También puede crearse un **archivo de registro** que documente los cambios realizados:

```
netsh int ip reset c:\tcpipreset.txt
```

Después del restablecimiento, es preciso **reiniciar el ordenador**.

Una de las instrucciones útiles es:

```
netsh wlan show profile name=nombrered key=clear
```

WINRM

Herramienta de la línea de comandos de Administración remota de Windows.

Administración remota de Windows (WinRM) es la implementación de Microsoft del protocolo WS-Management, que proporciona una forma segura de comunicarse con equipos locales y remotos mediante servicios web.

Recuperar la configuración actual en formato XML:

```
winrm get winrm/config -format:pretty
REM Recuperar instancia de spooler de la clase Win32_Service:
winrm get wmicimv2/Win32_Service?Name=spooler

REM Modifique una propiedad de configuración de WinRM:
winrm set winrm/config @{MaxEnvelopeSizekb="100"}

REM Deshabilite un oyente en esta máquina:
winrm set winrm/config/Listener?Address=*+Transport=HTTPS @{Enabled="false"}

REM Crear instancia de escucha HTTP en la dirección IPv6:
winrm delete winrm/config/Listener?Address=IP:192.168.2.1+Transport=HTTP
```

Puedes también recuperar y modificar información de administración. Configura este equipo para que acepte solicitudes de `WS-Management` de otros equipos.

WGET

Wget es una utilidad gratuita, disponible para Mac, `Windows` y Linux (incluida), que puede ayudarlo a lograr todo esto y más. Lo que lo diferencia de la mayoría de los administradores de descargas es que wgetpuede seguir los enlaces HTML en una página web y descargar los archivos de forma recursiva.

Muestro esta herramienta porque en Windows, existe de forma nativa el comando `bitsadmin`, pero que ya se encuentra en desuso.

Descargue un solo archivo de Internet

```
wget http://example.com/file.iso
```

Descargue un archivo, pero guárdelo localmente con un nombre diferente

```
wget --output-document=filename.html example.com
```

Descarga un archivo y guárdalo en una carpeta específica

```
wget --directory-prefix=folder/subfolder example.com
```

Reanudar una descarga interrumpida previamente iniciada por el propio wget

```
wget --continue example.com/big.file.iso
```

Descargue un archivo, pero solo si la versión en el servidor es más reciente que su copia local

```
wget --continue --timestamping wordpress.org/latest.zip
```

El comando wget ejercerá una presión adicional sobre el servidor del sitio porque atravesará continuamente los enlaces y descargará archivos.

FTP

Transfiere archivos hacia y desde una computadora que ejecuta un servicio de servidor de Protocolo de transferencia de archivos (FTP). Este comando se puede utilizar de forma interactiva o por lotes procesando archivos de texto ASCII.

```
> ftp ftp.microsoft.com
Conectado a ftp.microsoft.com.
220 cpmsftftpa03 Microsoft FTP Service (Version 5.0).
Usuario (ftp.microsoft.com:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Contraseña:<strong>******</strong>
230-This is FTP.MICROSOFT.COM. Please see the
230-dirmap.txt for more information.
230 Anonymous user logged in.
_
```

Observaciones

> Los parámetros de la línea de comandos de ftp distinguen entre mayúsculas y minúsculas.
>
> Este comando está disponible solo si el protocolo Protocolo de Internet (TCP / IP) está instalado como un componente en las propiedades de un adaptador de red en Conexiones de red.
>
> El comando ftp se puede utilizar de forma interactiva. Una vez iniciado, ftp crea un subentorno en el que puede utilizar comandos ftp . Puede volver a la línea de comandos escribiendo el comando ftp . Cuando se está ejecutando el subentorno ftp , se indica mediante el `ftp >`símbolo del sistema.
>
> El comando ftp admite el uso de IPv6 cuando está instalado el protocolo IPv6.

Para iniciar sesión en el servidor ftp nombrado `ftp.example.microsoft.com` y ejecutar los comandos ftp contenidos en un archivo llamado *resync.txt* , escriba:

```
ftp -s:resync.txt ftp.example.microsoft.com
```

Existe una variedad de comandos para acceder, subir, bajar información y por supuesto, navegar sobre el flujo del FTP.

SSH

En Windows 10, SSH ya viene incorporado. Esta, es una herramienta para iniciar sesión en una máquina remota y para ejecutar comandos.

Proporciona una conexión cifrada segura entre dos hosts a través de una red insegura. Esta conexión también se puede utilizar para acceso a terminales, transferencias de archivos y para tunelizar otras aplicaciones.

Realizar una conexión a un host remoto:

```
ssh username@domain_or_ip_address
```

Otra manera es especificando el parámetro `-l`:

```
ssh -l username domain_or_ip_address
```