

1.-" Obtener la ayuda del comando ping 2.- Enviar un ping a 127.0.0.1 aplicando cualquier parámetro Comando usado: Ping

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows

PS C:\Users\scara\Desktop> ping

Uso: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
        [-r count] [-s count] [[-j host-list] | [-k host-list]]
        [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
        [-4] [-6] nombre_destino

Opciones:
-t          Hacer ping al host especificado hasta que se detenga.
            Para ver estadísticas y continuar, presione
            Ctrl-Interrumpir; para detener, presione Ctrl+C.
-a          Resolver direcciones en nombres de host.
-n count    Número de solicitudes de eco para enviar.
-l size     Enviar tamaño de búfer.
-f          Establecer marca No fragmentar en paquetes (solo IPv4).
-i TTL      Período de vida.
-v TOS      Tipo de servicio (solo IPv4. Esta opción está desusada y
            no tiene ningún efecto sobre el campo de tipo de servicio
            del encabezado IP).
-r count    Registrar la ruta de saltos de cuenta (solo IPv4).
-s count    Marca de tiempo de saltos de cuenta (solo IPv4).
-j host-list Ruta de origen no estricta para lista-host (solo IPv4).
-k host-list Ruta de origen estricta para lista-host (solo IPv4).
-w timeout  Tiempo de espera en milisegundos para cada respuesta.
-R          Usar encabezado de enrutamiento para probar también
            la ruta inversa (solo IPv6).
            Por RFC 5095 el uso de este encabezado de enrutamiento ha
            quedado en desuso. Es posible que algunos sistemas anulen
            solicitudes de eco si usa este encabezado.
-S srcaddr  Dirección de origen que se desea usar.
-c compartment Enrutamiento del identificador del compartimiento.
-p          Hacer ping a la dirección del proveedor de Virtualización
            de red de Hyper-V.
-4          Forzar el uso de IPv4.
-6          Forzar el uso de IPv6.
```

2.- Enviar un ping a 127.0.0.1 aplicando cualquier parámetro

```
Windows PowerShell

no tiene ningún efecto sobre el campo de tipo de servicio
del encabezado IP).
Registrar la ruta de saltos de cuenta (solo IPv4).
Marca de tiempo de saltos de cuenta (solo IPv4).
Ruta de origen no estricta para lista-host (solo IPv4). -k host-list    Ruta de origen estricta para lista-host (solo IPv4).
Tiempo de espera en milisegundos para cada respuesta.
Usar encabezado de enrutamiento para probar también
la ruta inversa (solo IPv6).
Por RFC 5095 el uso de este encabezado de enrutamiento ha
quedado en desuso. Es posible que algunos sistemas anulen
solicitudes de eco si usa este encabezado.
Dirección de origen que se desea usar.
Enrutamiento del identificador del compartimiento.
Hacer ping a la dirección del proveedor de Virtualización
de red de Hyper-V.
Forzar el uso de IPv4.
Forzar el uso de IPv6.

PS C:\Users\scara\Desktop> ping -n 6 127.0.0.1

Haciendo ping a 127.0.0.1 con 32 bytes de datos:
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 127.0.0.1:
    Paquetes: enviados = 6, recibidos = 6, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
PS C:\Users\scara\Desktop>
```

3.- Verificar la conectividad del equipo utilizando el comando ping, anotar conclusiones

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows

PS C:\Users\scara\Desktop> ping google.com

Haciendo ping a google.com [2607:f8b0:4008:806::200e] con 32 bytes de datos:
Respuesta desde 2607:f8b0:4008:806::200e: tiempo=82ms
Respuesta desde 2607:f8b0:4008:806::200e: tiempo=188ms
Respuesta desde 2607:f8b0:4008:806::200e: tiempo=183ms
Respuesta desde 2607:f8b0:4008:806::200e: tiempo=189ms

Estadísticas de ping para 2607:f8b0:4008:806::200e:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 82ms, Máximo = 189ms, Media = 160ms
PS C:\Users\scara\Desktop>
```

4.- Obtener la ayuda del comando nslookup

```
Windows PowerShell
PS C:\Users\scara\Desktop> nslookup ?
Uso:
    nslookup [-opt ...]                # modo interactivo que usa el servidor
                                      # predeterminado
    nslookup [-opt ...] - servidor    # modo interactivo que usa 'servidor'
    nslookup [-opt ...] host          # solo consulta 'host' mediante el
                                      # servidor predeterminado
    nslookup [-opt ...] host servidor # solo consulta 'host' mediante 'servidor'
PS C:\Users\scara\Desktop> |
```

5.- Resolver la dirección in, de https://upqroo.edu.mx/usando nslookup

```
Windows PowerShell
PS C:\Users\scara\Desktop> nslookup ?
Uso:
    nslookup [-opt ...]                # modo interactivo que usa el servidor
                                       # predeterminado
    nslookup [-opt ...] - servidor    # modo interactivo que usa 'servidor'
    nslookup [-opt ...] host          # solo consulta 'host' mediante el
                                       # servidor predeterminado
    nslookup [-opt ...] host servidor # solo consulta 'host' mediante 'servidor'
PS C:\Users\scara\Desktop> nslookup upqroo.edu.mx
Servidor:  mygpon.ip
Address:  192.168.1.254

Respuesta no autoritativa:
Nombre:  upqroo.edu.mx
Address:  77.68.126.20

PS C:\Users\scara\Desktop> |
```

6.- Hacer ping a la ip obtenida en el paso anterior, anotar conclusiones

```
Windows PowerShell
PS C:\Users\scara\Desktop> nslookup ?
Uso:
    nslookup [-opt ...]                # modo interactivo que usa el servidor
                                       # predeterminado
    nslookup [-opt ...] - servidor    # modo interactivo que usa 'servidor'
    nslookup [-opt ...] host          # solo consulta 'host' mediante el
                                       # servidor predeterminado
    nslookup [-opt ...] host servidor # solo consulta 'host' mediante 'servidor'
PS C:\Users\scara\Desktop> nslookup upqroo.edu.mx
Servidor:  mygpon.ip
Address:  192.168.1.254

Respuesta no autoritativa:
Nombre:  upqroo.edu.mx
Address:  77.68.126.20

PS C:\Users\scara\Desktop> ping 77.68.126.20

Haciendo ping a 77.68.126.20 con 32 bytes de datos:
Respuesta desde 77.68.126.20: bytes=32 tiempo=123ms TTL=52
Respuesta desde 77.68.126.20: bytes=32 tiempo=121ms TTL=52
Respuesta desde 77.68.126.20: bytes=32 tiempo=121ms TTL=52
Respuesta desde 77.68.126.20: bytes=32 tiempo=123ms TTL=52

Estadísticas de ping para 77.68.126.20:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 121ms, Máximo = 123ms, Media = 122ms

PS C:\Users\scara\Desktop>
```

7.- Obtener la ayuda del comando netstat

```
Windows PowerShell
PS C:\Users\scara\Desktop> netstat /?

Muestra estadísticas de protocolo y conexiones de red de TCP/IP actuales.

NETSTAT [-a] [-b] [-e] [-f] [-i] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

-a      Muestra todas las conexiones y los puertos de escucha.
-b      Muestra el ejecutable relacionado con la creación de cada conexión o
        puerto de escucha. En algunos casos bien conocidos, los ejecutables hospedan
        varios componentes independientes y, en estos casos, se muestra la
        secuencia de componentes relacionados con la creación de la conexión
        o el puerto de escucha. En este caso, el nombre del
        ejecutable está entre corchetes, "[ ]", en la parte inferior, encima del componente al que haya llamado,
        y así hasta que se alcance TCP/IP. Ten en cuenta que esta opción
        puede consumir bastante tiempo y dará error si no se dispone de los permisos
        adecuados.
-e      Muestra estadísticas de Ethernet. Esto se puede combinar con la
        opción -s.
-f      Muestra nombres de dominio completos (FQDN) para direcciones
        externas.
-i      Muestra el tiempo gastado por una conexión TCP en su estado actual.
-n      Muestra direcciones y números de puerto en formato numérico.
-o      Muestra el id. del proceso propietario asociado con cada conexión.
-p proto Muestra conexiones para el protocolo especificado por proto; proto
        puede ser cualquiera de los siguientes: TCP, UDP, TCPv6 o UDPv6. Si se usa con la opción -s
        para mostrar estadísticas por protocolo, proto puede ser cualquiera de los siguientes:
        IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
-q      Muestra todas las conexiones, puertos de escucha y puertos TCP de enlace
        que no sean de escucha. Los puertos de enlace que no sean de escucha pueden estar o no
        asociados con una conexión activa.
-r      Muestra la tabla de enrutamiento.
-s      Muestra las estadísticas por protocolo. De manera predeterminada, las estadísticas
        se muestran para IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP y UDPv6;
        la opción -p se puede usar para especificar un subconjunto de los valores predeterminados.
-t      Muestra el estado de descarga de la conexión actual.
-x      Muestra conexiones, agentes de escucha y extremos compartidos
        de NetworkDirect.
-y      Muestra la plantilla de conexión TCP para todas las conexiones.
        No se puede combinar con otras opciones.
interval Vuelve a mostrar las estadísticas seleccionadas y realiza pausas en intervalos de varios segundos
        entre cada visualización. Presiona Ctrl+C para que dejen de volver a mostrarse
        las estadísticas. Si se omite, netstat mostrará la
        información de configuración una vez.

PS C:\Users\scara\Desktop>
```

8.- Mostrar todas las conexiones y puertos de escucha

```
PS C:\Users\scara\Desktop> netstat -a

Conexiones activas

Proto Dirección local Dirección remota Estado
TCP 0.0.0.0:135 LAPTOP-CKIJCJEQ:0 LISTENING
TCP 0.0.0.0:445 LAPTOP-CKIJCJEQ:0 LISTENING
TCP 0.0.0.0:5040 LAPTOP-CKIJCJEQ:0 LISTENING
TCP 0.0.0.0:6646 LAPTOP-CKIJCJEQ:0 LISTENING
TCP 0.0.0.0:49664 LAPTOP-CKIJCJEQ:0 LISTENING
TCP 0.0.0.0:49665 LAPTOP-CKIJCJEQ:0 LISTENING
TCP 0.0.0.0:49666 LAPTOP-CKIJCJEQ:0 LISTENING
TCP 0.0.0.0:49667 LAPTOP-CKIJCJEQ:0 LISTENING
TCP 0.0.0.0:49668 LAPTOP-CKIJCJEQ:0 LISTENING
TCP 0.0.0.0:49670 LAPTOP-CKIJCJEQ:0 LISTENING
TCP 127.0.0.1:2015 LAPTOP-CKIJCJEQ:0 LISTENING
TCP 127.0.0.1:49608 LAPTOP-CKIJCJEQ:65001 ESTABLISHED
TCP 127.0.0.1:49609 LAPTOP-CKIJCJEQ:0 LISTENING
TCP 127.0.0.1:49609 LAPTOP-CKIJCJEQ:49674 ESTABLISHED
TCP 127.0.0.1:49674 LAPTOP-CKIJCJEQ:49609 ESTABLISHED
TCP 127.0.0.1:65001 LAPTOP-CKIJCJEQ:0 LISTENING
TCP 127.0.0.1:65001 LAPTOP-CKIJCJEQ:49608 ESTABLISHED
TCP 192.168.1.65:139 LAPTOP-CKIJCJEQ:0 LISTENING
TCP 192.168.1.65:49616 20.10.31.115:https ESTABLISHED
TCP 192.168.1.65:49821 whatsapp-chatd-edge-shv-01-mia3:https ESTABLISHED
TCP 192.168.1.65:50071 103.41.69.205:https ESTABLISHED
TCP 192.168.1.65:50072 20.83.119.107:https ESTABLISHED
TCP 192.168.1.65:50074 a96-17-60-11:https ESTABLISHED
TCP 192.168.1.65:50077 1drv:https ESTABLISHED
TCP 192.168.1.65:50098 52.168.112.66:https TIME_WAIT
TCP 192.168.56.1:139 LAPTOP-CKIJCJEQ:0 LISTENING
TCP [::]:135 LAPTOP-CKIJCJEQ:0 LISTENING
TCP [::]:445 LAPTOP-CKIJCJEQ:0 LISTENING
TCP [::]:49664 LAPTOP-CKIJCJEQ:0 LISTENING
```

9.- Ejecutar netstat, sin resolver nombres de dominio o puertos

```
Windows PowerShell
UDP [fe80::5ebc:71cb:976f:74aa%19]:50922 *:*
UDP [fe80::91e5:bfl6:6553:93e%8]:1900 *:*
UDP [fe80::91e5:bfl6:6553:93e%8]:50923 *:*
PS C:\Users\scara\Desktop> netstat -n

Conexiones activas

Proto Dirección local Dirección remota Estado
TCP 127.0.0.1:49688 127.0.0.1:65001 ESTABLISHED
TCP 127.0.0.1:49689 127.0.0.1:49674 ESTABLISHED
TCP 127.0.0.1:49674 127.0.0.1:49609 ESTABLISHED
TCP 127.0.0.1:65001 127.0.0.1:49608 ESTABLISHED
TCP 192.168.1.65:49616 20.10.31.115:443 ESTABLISHED
TCP 192.168.1.65:49821 31.13.67.53:443 ESTABLISHED
TCP 192.168.1.65:50071 103.41.69.205:443 ESTABLISHED
TCP 192.168.1.65:50072 20.83.119.107:443 ESTABLISHED
TCP 192.168.1.65:50074 96.17.60.11:443 ESTABLISHED
TCP 192.168.1.65:50111 54.69.44.20:443 TIME_WAIT
TCP 192.168.1.65:50112 52.11.252.22:443 TIME_WAIT
TCP 192.168.1.65:50116 13.107.42.12:443 ESTABLISHED
TCP [2806:10be:4:b814:9cbe:b106:e038:750]:49687 [2600:1403:9c00:1b::1732:71af]:443 CLOSE_WAIT
TCP [2806:10be:4:b814:9cbe:b106:e038:750]:49751 [2607:f8b0:400c:c13::bc]:5228 ESTABLISHED
TCP [2806:10be:4:b814:9cbe:b106:e038:750]:49800 [2600:9000:21f2:ac00:3:6eb2:3580:93a1]:443 ESTABLISHED
TCP [2806:10be:4:b814:9cbe:b106:e038:750]:49903 [2603:1063:2200:24::d]:443 ESTABLISHED
TCP [2806:10be:4:b814:9cbe:b106:e038:750]:50108 [2607:f8b0:4008:809::200e]:443 TIME_WAIT
TCP [2806:10be:4:b814:9cbe:b106:e038:750]:50109 [2607:f8b0:4008:809::200e]:443 TIME_WAIT
TCP [2806:10be:4:b814:9cbe:b106:e038:750]:50110 [2607:f8b0:4008:809::200e]:443 TIME_WAIT
TCP [2806:10be:4:b814:9cbe:b106:e038:750]:50113 [2600:1f16:598:e100:2a95:d51b:480e:58cd]:443 TIME_WAIT
TCP [2806:10be:4:b814:9cbe:b106:e038:750]:50114 [2607:f8b0:4008:809::2016]:443 TIME_WAIT
TCP [2806:10be:4:b814:9cbe:b106:e038:750]:50115 [2001:4c28:3000:622:37:228:108:132]:443 TIME_WAIT
TCP [2806:10be:4:b814:9cbe:b106:e038:750]:50117 [2607:f8b0:4008:80b::200e]:443 TIME_WAIT
TCP [2806:10be:4:b814:9cbe:b106:e038:750]:50118 [2600:141c:e000:183::52c]:443 ESTABLISHED
TCP [2806:10be:4:b814:9cbe:b106:e038:750]:50119 [2600:1f16:598:e100:2a95:d51b:480e:58cd]:443 ESTABLISHED
TCP [2806:10be:4:b814:9cbe:b106:e038:750]:50120 [2607:f8b0:4008:806::200e]:443 ESTABLISHED
PS C:\Users\scara\Desktop> |
```

10.- Mostrar las conexiones TCP

```
Windows PowerShell
TCP [2806:10be:4:b814:9cbe:b106:e038:750]:50120 [2607:f8b0:4008:806::200e]:443 ESTABLISHED
PS C:\Users\scara\Desktop> netstat -at

Conexiones activas

Proto Dirección local Dirección remota Estado
TCP 0.0.0.0:135 LAPTOP-CKIJCJEQ:0 LISTENING EnHost
TCP 0.0.0.0:4445 LAPTOP-CKIJCJEQ:0 LISTENING EnHost
TCP 0.0.0.0:5040 LAPTOP-CKIJCJEQ:0 LISTENING EnHost
TCP 0.0.0.0:6646 LAPTOP-CKIJCJEQ:0 LISTENING EnHost
TCP 0.0.0.0:49664 LAPTOP-CKIJCJEQ:0 LISTENING EnHost
TCP 0.0.0.0:49665 LAPTOP-CKIJCJEQ:0 LISTENING EnHost
TCP 0.0.0.0:49666 LAPTOP-CKIJCJEQ:0 LISTENING EnHost
TCP 0.0.0.0:49667 LAPTOP-CKIJCJEQ:0 LISTENING EnHost
TCP 0.0.0.0:49668 LAPTOP-CKIJCJEQ:0 LISTENING EnHost
TCP 0.0.0.0:49670 LAPTOP-CKIJCJEQ:0 LISTENING EnHost
TCP 127.0.0.1:2015 LAPTOP-CKIJCJEQ:0 LISTENING EnHost
TCP 127.0.0.1:49608 LAPTOP-CKIJCJEQ:65001 ESTABLISHED EnHost
TCP 127.0.0.1:49609 LAPTOP-CKIJCJEQ:0 LISTENING EnHost
TCP 127.0.0.1:49609 LAPTOP-CKIJCJEQ:49674 ESTABLISHED EnHost
TCP 127.0.0.1:49674 LAPTOP-CKIJCJEQ:49609 ESTABLISHED EnHost
TCP 127.0.0.1:65001 LAPTOP-CKIJCJEQ:0 LISTENING EnHost
TCP 127.0.0.1:65001 LAPTOP-CKIJCJEQ:49608 ESTABLISHED EnHost
TCP 192.168.1.65:139 LAPTOP-CKIJCJEQ:0 LISTENING EnHost
TCP 192.168.1.65:49616 20.10.31.115:https ESTABLISHED EnHost
TCP 192.168.1.65:49821 whatsapp-chatd-edge-shv-01-mia3:https ESTABLISHED EnHost
TCP 192.168.1.65:50071 103.41.69.205:https ESTABLISHED EnHost
TCP 192.168.1.65:50072 20.83.119.107:https ESTABLISHED EnHost
TCP 192.168.1.65:50074 a96-17-60-11:https ESTABLISHED EnHost
TCP 192.168.1.65:50116 1drv:https ESTABLISHED EnHost
TCP 192.168.1.65:50122 20.44.229.112:https ESTABLISHED EnHost
TCP 192.168.56.1:139 LAPTOP-CKIJCJEQ:0 LISTENING EnHost
TCP [::]:135 LAPTOP-CKIJCJEQ:0 LISTENING EnHost
```

11.- Mostrar las conexiones UDP

```
Windows PowerShell
PS C:\Users\scara\Desktop>
PS C:\Users\scara\Desktop>
PS C:\Users\scara\Desktop> netstat -au

Muestra estadísticas de protocolo y conexiones de red de TCP/IP actuales.

NETSTAT [-a] [-b] [-e] [-f] [-i] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

-a          Muestra todas las conexiones y los puertos de escucha.
-b          Muestra el ejecutable relacionado con la creación de cada conexión o
            puerto de escucha. En algunos casos bien conocidos, los ejecutables hospedan
            varios componentes independientes y, en estos casos, se muestra la
            secuencia de componentes relacionados con la creación de la conexión
            o el puerto de escucha. En este caso, el nombre del
            ejecutable está entre corchetes, "[ ]", en la parte inferior, encima del componente al que haya llamado,
            y así hasta que se alcance TCP/IP. Ten en cuenta que esta opción
            puede consumir bastante tiempo y dará error si no se dispone de los permisos
            adecuados.
-e          Muestra estadísticas de Ethernet. Esto se puede combinar con la
            opción -s.
-f          Muestra nombres de dominio completos (FQDN) para direcciones
            externas.
-i          Muestra el tiempo gastado por una conexión TCP en su estado actual.
-n          Muestra direcciones y números de puerto en formato numérico.
-o          Muestra el id. del proceso propietario asociado con cada conexión.
-p proto    Muestra conexiones para el protocolo especificado por proto; proto
            puede ser cualquiera de los siguientes: TCP, UDP, TCPv6 o UDPv6. Si se usa con la opción -s
            para mostrar estadísticas por protocolo, proto puede ser cualquiera de los siguientes:
            IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
-q          Muestra todas las conexiones, puertos de escucha y puertos TCP de enlace
            que no sean de escucha. Los puertos de enlace que no sean de escucha pueden estar o no
            asociados con una conexión activa.
-r          Muestra la tabla de enrutamiento.
-s          Muestra las estadísticas por protocolo. De manera predeterminada, las estadísticas
            se muestran para IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP y UDPv6;
            la opción -p se puede usar para especificar un subconjunto de los valores predeterminados.
-t          Muestra el estado de descarga de la conexión actual.
-x          Muestra conexiones, agentes de escucha y extremos compartidos
            de NetworkDirect.
-y          Muestra la plantilla de conexión TCP para todas las conexiones.
            No se puede combinar con otras opciones.
```

12.- Utilizar el comando tasklist

```
Windows PowerShell
información de configuración una vez.

PS C:\Users\scara\Desktop> tasklist

Nombre de imagen          PID Nombre de sesión Núm. de ses Uso de memor
=====
System Idle Process        0 Services          0          8 KB
System                    4 Services          0      2,288 KB
Secure System             140 Services        0     31,752 KB
Registry                  184 Services        0     32,320 KB
smss.exe                   716 Services        0        692 KB
csrss.exe                  972 Services        0     4,188 KB
wininit.exe               1140 Services        0        4760 KB
services.exe              1212 Services        0     18,392 KB
lsalss.exe                 1232 Services        0     1,640 KB
lsass.exe                 1248 Services        0     19,440 KB
svchost.exe               1480 Services        0     28,420 KB
fontdrvhost.exe          1472 Services        0        520 KB
WUDFHost.exe              1520 Services        0     2,240 KB
svchost.exe               1616 Services        0     15,928 KB
svchost.exe               1660 Services        0     5,824 KB
svchost.exe               1828 Services        0        964 KB
svchost.exe               1916 Services        0     6,384 KB
svchost.exe               1924 Services        0     4,776 KB
svchost.exe               1976 Services        0     8,996 KB
IntelCpHDPSvc.exe        2016 Services        0        1332 KB
svchost.exe               2024 Services        0     4,956 KB
svchost.exe               2032 Services        0     4,052 KB
svchost.exe               1688 Services        0     2,684 KB
svchost.exe               1260 Services        0     4,560 KB
svchost.exe               2084 Services        0     5,160 KB
svchost.exe               2160 Services        0     12,248 KB
svchost.exe               2232 Services        0     14,748 KB
svchost.exe               2252 Services        0     5,068 KB
igfxCUIServiceN.exe      2412 Services        0     6,140 KB
svchost.exe               2620 Services        0     9,868 KB
svchost.exe               2672 Services        0     5,288 KB
svchost.exe               2748 Services        0     2,932 KB
svchost.exe               2916 Services        0     4,172 KB
AppHelperCap.exe         2928 Services        0     12,316 KB
DiagsCap.exe             2960 Services        0     3,716 KB
NetworkCap.exe           2984 Services        0     4,436 KB
OpenCap.exe              2992 Services        0     2,852 KB
SysInfoCap.exe           3024 Services        0     18,844 KB
svchost.exe               3064 Services        0     12,832 KB
svchost.exe               2180 Services        0     4,232 KB
svchost.exe               3080 Services        0     22,552 KB
svchost.exe               3092 Services        0     4,064 KB
```

13.- Utilizar el comando taskkill

```
Windows PowerShell
FileCoAuth.exe           13096 Console           6      17,228 KB
WINWORD.EXE              24184 Console           6      272,936 KB
WindowsTerminal.exe      18336 Console           6      134,080 KB
OpenConsole.exe          22352 Console           6        9,460 KB
powershell.exe            14416 Console           6       72,412 KB
RuntimeBroker.exe         7392 Console           6       10,740 KB
svchost.exe              10432 Console           6       13,036 KB
msedgewebview2.exe        2152 Console           6        5,632 KB
msedgewebview2.exe      12004 Console           6        8,060 KB
msedgewebview2.exe        8612 Console           6        972 KB
msedgewebview2.exe       16768 Console           6        484 KB
msedgewebview2.exe       27248 Console           6         16 KB
msedgewebview2.exe       21228 Console           6        172 KB
LocationNotificationWindo 25380 Console           6       7,052 KB
McUICnt.exe              11508 Console           6      27,256 KB
GameBar.exe              23676 Console           6      56,536 KB
svchost.exe              16740 Console           6      24,552 KB
GameBarFTServer.exe      10812 Console           6      16,048 KB
RuntimeBroker.exe        27140 Console           6      20,560 KB
QcShm.exe                16304 Services           0      14,208 KB
WhatsApp.exe             23748 Console           6     329,076 KB
svchost.exe              26960 Services           0        9,840 KB
WmiPrvSE.exe             3964 Services           0      11,412 KB
backgroundTaskHost.exe    17828 Console           6      39,236 KB
opera.exe                 14264 Console           6     204,516 KB
opera.exe                 27028 Console           6      52,888 KB
opera.exe                  7116 Console           6      33,188 KB
opera.exe                 16468 Console           6     161,964 KB
svchost.exe              17376 Services           0       7,532 KB
backgroundTaskHost.exe    16708 Console           6     49,592 KB
RuntimeBroker.exe        17280 Console           6      13,996 KB
tasklist.exe             17672 Console           6      10,320 KB
PS C:\Users\scara\Desktop> taskkill /F /PID 21012
Correcto: se terminó el proceso con PID 21012.
PS C:\Users\scara\Desktop> |
```

14.- Utilizar el comando tracert

```
Windows PowerShell
svchost.exe              26960 Services           0        9,840 KB
WmiPrvSE.exe             3964 Services           0      11,412 KB
backgroundTaskHost.exe    17828 Console           6      39,236 KB
opera.exe                 14264 Console           6     204,516 KB
opera.exe                 27028 Console           6      52,888 KB
opera.exe                  7116 Console           6      33,188 KB
opera.exe                 16468 Console           6     161,964 KB
svchost.exe              17376 Services           0       7,532 KB
backgroundTaskHost.exe    16708 Console           6     49,592 KB
RuntimeBroker.exe        17280 Console           6      13,996 KB
tasklist.exe             17672 Console           6      10,320 KB
PS C:\Users\scara\Desktop> taskkill /F /PID 21012
Correcto: se terminó el proceso con PID 21012.
PS C:\Users\scara\Desktop> tracert google.com

Traza a la dirección google.com [2607:f8b0:4008:809::200e]
sobre un máximo de 30 saltos:

 1  67 ms   1 ms   2 ms  2806-10be-0004-b814-c29f-51ff-fee5-1e30.ipv6.infinetum.net.mx [2806:10be:4:b814:c29f:51ff:fee5:1e30]
 2  *      *      *      Tiempo de espera agotado para esta solicitud.
 3  *      *      *      Tiempo de espera agotado para esta solicitud.
 4  53 ms   51 ms   51 ms  2806-1030-c000-0008-0000-0000-0000.ipv6.infinetum.net.mx [2806:1030:c000:8::]
 5  49 ms   50 ms   52 ms  2607:f8b0:85a2:c0::1
 6  179 ms  100 ms  101 ms  2001:4860:0:1::747a
 7  117 ms  87 ms   55 ms  2001:4860:0:134a::8
 8  52 ms   53 ms   54 ms  2001:4860::c:4002:74b3
 9  185 ms  100 ms  100 ms  2001:4860::c:4002:510e
10  111 ms  97 ms   104 ms  2001:4860::1:4000:fd89
11  111 ms  100 ms  97 ms   2001:4860:0:12e2::1
12  144 ms  98 ms   99 ms  2001:4860:0:1::5beb
13  205 ms  98 ms  101 ms  mia09s26-in-x0e.1e100.net [2607:f8b0:4008:809::200e]

Traza completa.
PS C:\Users\scara\Desktop>
PS C:\Users\scara\Desktop> |
```

15.- Utilizar el comando ARP

```
Windows PowerShell
3      *      *      *      Tiempo de espera agotado para esta solicitud.
4      53 ms   51 ms   51 ms   2806-1030-c000-0008-0000-0000-0000.ipv6.infinitem.net.mx [2806:1030:c000:8::]
5      49 ms   50 ms   52 ms   2607:f8b0:85a2:c0::1
6      179 ms  100 ms  101 ms  2001:4860:0:1::747a
7      117 ms  87 ms   55 ms   2001:4860:0:134a::8
8      52 ms   53 ms   54 ms   2001:4860::c:4002:74b3
9      185 ms  100 ms  100 ms  2001:4860::c:4002:510e
10     111 ms  97 ms   104 ms  2001:4860::1:4000:fd89
11     111 ms  100 ms  97 ms   2001:4860:0:12e2::1
12     144 ms  98 ms   99 ms   2001:4860:0:1::5beb
13     205 ms  98 ms   101 ms  mia09s26-in-x0e.1e100.net [2607:f8b0:4008:809::200e]

Traza completa.
PS C:\Users\scara\Desktop>
PS C:\Users\scara\Desktop> arp -a

Interfaz: 192.168.1.65 --- 0x8
Dirección de Internet      Dirección física      Tipo
192.168.1.254              c0-9f-51-e5-1e-30    dinámico
192.168.1.255              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
255.255.255.255            ff-ff-ff-ff-ff-ff    estático

Interfaz: 192.168.56.1 --- 0x13
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
255.255.255.255            ff-ff-ff-ff-ff-ff    estático
PS C:\Users\scara\Desktop> |
```


B) Contesta con tus propias palabras las siguientes preguntas:

1.- ¿Para qué sirve el comando ping?

El comando ping se utiliza para comprobar la conectividad entre dos hosts en una red. Envía paquetes de solicitud de eco a un host remoto y espera las respuestas. Si el host remoto recibe los paquetes y responde, el ping se considera exitoso.

El comando ping se puede utilizar para diagnosticar problemas de conectividad en una red. Si el ping a un host remoto no es exitoso, es posible que haya un problema con la conexión entre los dos hosts.

El comando ping también se puede utilizar para medir el rendimiento de una conexión de red. El tiempo de respuesta del ping indica la cantidad de tiempo que tarda en viajar un paquete de datos entre dos hosts.

Sintaxis básica

ping [opciones] [dirección]

Opciones

- /t - Realiza pings continuos hasta que se cancele con Ctrl+C.
- /n - Envía un número específico de pings.
- /l - Tamaño del paquete de datos en bytes.
- /w - Tiempo de espera en milisegundos para recibir una respuesta.

2.- ¿Para qué sirve el comando nslookup?

El comando nslookup se utiliza para realizar consultas al sistema de nombres de dominio (DNS). El DNS es un sistema que traduce nombres de dominio a direcciones IP.

Sintaxis básica

nslookup [opciones] [dominio]

Opciones

- /d - Realizar una búsqueda inversa.
- /l - Especificar el servidor DNS a utilizar.
- /q - Especificar el tipo de registro de DNS a consultar.
- /r - Utilizar un servidor DNS específico.
- /s - Utilizar un servidor proxy DNS.

3.- ¿Para que sirve el comando netstat?

El comando netstat se utiliza para mostrar información sobre las conexiones de red activas y los puertos abiertos en un sistema informático.

Sintaxis básica

netstat [opciones]

Opciones

- /a - Mostrar todas las conexiones, incluidos los puertos TCP, UDP y RAW.
- /b - Mostrar la pila de llamadas para cada conexión.
- /c - Actualizar la salida cada segundo.
- /e - Mostrar las estadísticas de enrutamiento.
- /i - Mostrar las estadísticas de interfaces de red.
- /n - Mostrar las direcciones IP y los puertos en formato numérico.
- /o - Mostrar las conexiones en formato de tabla.
- /p - Mostrar los procesos asociados con las conexiones.
- /r - Mostrar la tabla de enrutamiento.
- /s - Mostrar las estadísticas de protocolo.
- /t - Mostrar las conexiones TCP.
- /u - Mostrar las conexiones UDP.

4.-¿Para que sirve el comando tasklist?

El comando tasklist se utiliza para mostrar una lista de procesos en ejecución actualmente en el equipo local o en un equipo remoto. Tasklist sustituye a la herramienta tlist.

Sintaxis básica

tasklist [opciones]

Opciones

- /fo - Especifica el formato de salida. Los formatos disponibles son:
 - table (por defecto): Muestra la salida en formato de tabla.
 - list : Muestra la salida en formato de lista.
 - csv : Muestra la salida en formato CSV.

- /v - Muestra información detallada de la tarea en la salida.
- /svc - Muestra el nombre del servicio asociado a cada proceso.
- /si - Especifica el equipo remoto o local.
- /s - Especifica el usuario con privilegios para obtener la lista de procesos.
- /fi - Filtra la lista de procesos según un criterio.

5.- ¿Para que sirve el comando taskkill?

El comando taskkill se utiliza para finalizar uno o más procesos o tareas en Windows. Se puede utilizar para finalizar un proceso que no responde, un proceso que está causando problemas o un proceso que simplemente ya no necesita.

Sintaxis básica

taskkill [/F] [/T] [/PID PID] [/IM imagen]

Opciones

- /F - Fuerza la finalización del proceso, incluso si está en un estado bloqueado.
- /T - También finaliza los procesos secundarios del proceso especificado.
- /PID PID - Especifica el ID de proceso del proceso que se va a finalizar.
- /IM imagen - Especifica el nombre de la imagen del proceso que se va a finalizar.

6.- ¿Para que sirve el comando tracert?

El comando tracert se utiliza para mostrar la ruta que toma un paquete de datos para llegar a un destino. El comando utiliza el protocolo de mensajes de control de Internet (ICMP) para enviar paquetes de solicitud de eco a un destino y luego esperar las respuestas.

Sintaxis básica:

tracert [opciones] [destino]

Opciones:

- /d - Realizar una búsqueda inversa.
- /h - Especificar el número máximo de saltos.
- /i - Utilizar un servidor de origen específico.
- /l - Especificar el tamaño del paquete de datos.
- /m - Especificar el número de paquetes a enviar.
- /n - Mostrar las direcciones IP en formato numérico.
- /r - Mostrar los tiempos de viaje en milisegundos.

- /s - Especificar el número de saltos iniciales.
- /t - Mostrar los tiempos de viaje en milisegundos.
- /w - Tiempo de espera en milisegundos para recibir una respuesta.

7.- ¿Como ayudan los primeros tres comandos para detectar problemas en la red?

Los tres comandos que se han mencionado, ping, nslookup y netstat, pueden ser muy útiles para detectar problemas en la red.

Ping se utiliza para comprobar la conectividad entre dos hosts. Si un ping a un destino no tiene éxito, es probable que haya un problema con la conectividad de la red.

Nslookup se utiliza para resolver nombres de dominio en direcciones IP. Si un nslookup a un nombre de dominio no tiene éxito, es probable que haya un problema con el servidor DNS.

Netstat se utiliza para mostrar información sobre las conexiones de red activas. Si netstat muestra conexiones que no deberían estar activas, o si muestra conexiones con problemas, es probable que haya un problema con la configuración de la red.

En concreto, estos comandos pueden ayudar a detectar los siguientes problemas:

Problemas de conectividad: Si un ping a un destino no tiene éxito, es probable que haya un problema con la conectividad de la red. Esto podría ser causado por un cable roto, un problema de configuración de la red o un problema con el servidor DNS.

Problemas de DNS: Si un nslookup a un nombre de dominio no tiene éxito, es probable que haya un problema con el servidor DNS. Esto podría ser causado por un problema con el servidor DNS en sí, un problema con la configuración del servidor DNS o un problema con la configuración del cliente DNS.

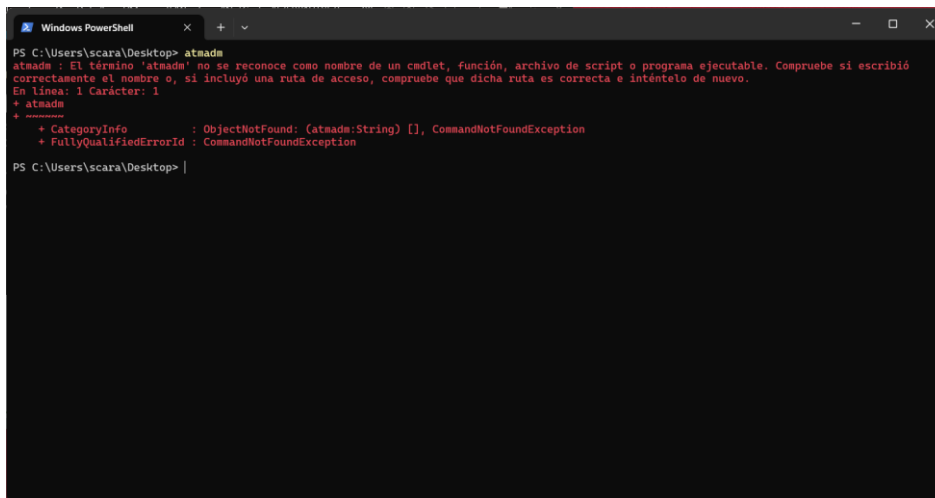
Problemas de configuración de la red: Si netstat muestra conexiones que no deberían estar activas, o si muestra conexiones con problemas, es probable que haya un problema con la configuración de la red. Esto podría ser causado por una configuración incorrecta de los parámetros de red, un problema con un dispositivo de red o un problema con un software de red.

C) Investigar los siguientes comandos y anotar ejemplos practicos:

atmadm, bitsadmin, cmstp, ftp, getmac, hostname, nbtstat, net, net use, netsh, pathping, top, texec, route, tRsking, tsh, tomsetup, telnet, tftp

atmadm:

El comando atmadm se utiliza para monitorear y administrar las conexiones y direcciones ATM (Asynchronous Transfer Mode) en un ordenador con Windows.



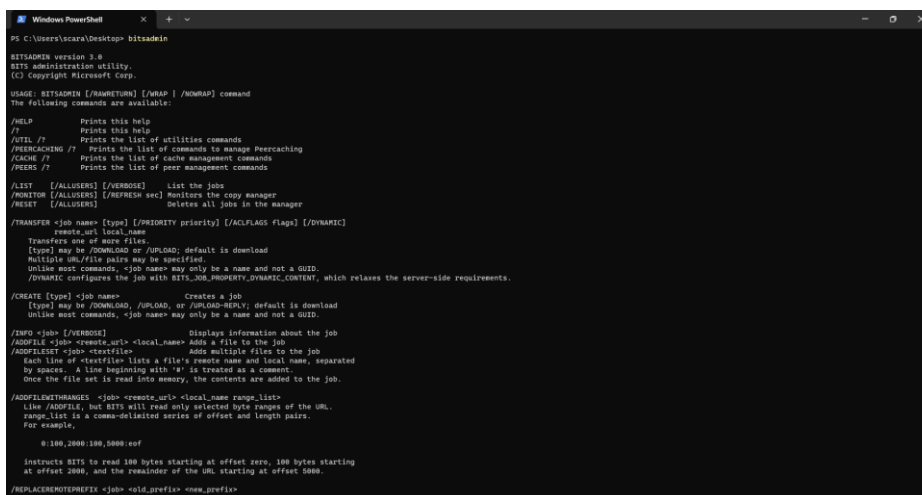
```
Windows PowerShell
PS C:\Users\scara\Desktop> atmadm
atmadm : El término 'atmadm' no se reconoce como nombre de un cmdlet, función, archivo de script o programa ejecutable. Compruebe si escribió correctamente el nombre o, si incluyó una ruta de acceso, compruebe que dicha ruta es correcta e inténtelo de nuevo.
En línea: 1 Carácter: 1
+ atmadm
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (atmadm:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\scara\Desktop> |
```

Bitsadmin:

El comando bitsadmin se puede utilizar para descargar múltiples archivos al mismo tiempo. Para ello, se puede utilizar el siguiente procedimiento:

1. Crear un nuevo trabajo de descarga de archivos utilizando el parámetro /create.
2. Añadir los archivos que se desean descargar al trabajo utilizando el parámetro /add.
3. Iniciar la descarga utilizando el parámetro /start.



```
Windows PowerShell
PS C:\Users\scara\Desktop> bitsadmin

BITSADMIN version 3.0
BITS administration utility.
(C) Copyright Microsoft Corp.

USAGE: BITSADMIN [/name:NAME] [/wrap | /nowrap] command
The following commands are available:

/HELP           Prints this help
/?             Prints this help
/UTIL /?       Prints the list of utilities commands
/RECEACHING /? Prints the list of commands to manage Peercaching
/CACHE /?      Prints the list of cache management commands
/PEERS /?      Prints the list of peer management commands

/LIST [/allusers] [/verbose] List the jobs
/MONITOR [/allusers] [/refresh sec] Monitors the copy manager
/RESET [/allusers] Deletes all jobs in the manager

/TRANSFER <job name> [type] [/priority priority] [/ACL:flags] [/dynamic]
    remote_url local_name
    Transfers one or more files.
    [type] may be /download, /upload, or /upload-reply; default is download
    Multiple URL/file pairs may be specified.
    Unless most commands, <job name> may only be a name and not a GUID.
    /dynamic configures the job with BITS_JOB_PROPERTY_DYNAMIC_CONTENT, which relaxes the server-side requirements.

/CREATE [type] <job name> Creates a job
    [type] may be /download, /upload, or /upload-reply; default is download
    Unless most commands, <job name> may only be a name and not a GUID.

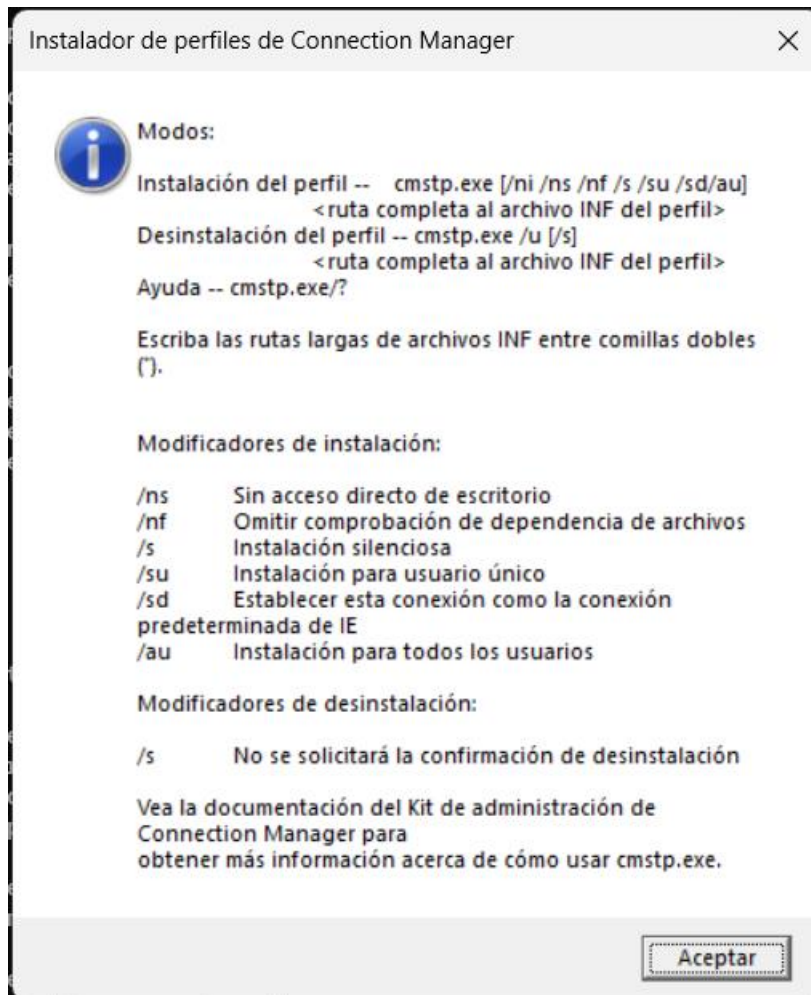
/INFO <job> [/verbose] Displays information about the job
/ADDFILE <job> <remote_url> <local_name> Adds a file to the job
/ADDFILESET <job> <testfile> Adds multiple files to the job
    Each line of <testfile> lists a file's remote name and local name, separated by spaces. A line beginning with '#' is treated as a comment.
    Once the file set is read into memory, the contents are added to the job.

/ADDFILEXCHANGES <job> <remote_url> <local_name range list>
    Line /ADDFILE, but BITS will read only selected byte ranges of the URL.
    range list is a comma-delimited series of offset and length pairs.
    For example,
        0:100,2000:100,5000:eof
    instructs BITS to read 100 bytes starting at offset zero, 100 bytes starting at offset 2000, and the remainder of the URL starting at offset 5000.

/REPLACENOTEPREFIX <job> <old_prefix> <new_prefix>
```

Cmstp:

El comando cmstp (Microsoft Connection Manager Profile Installer) se utiliza para instalar o desinstalar perfiles de servicio de Conexión a redes. Los perfiles de servicio se utilizan para configurar conexiones a redes de área local (LAN), redes privadas virtuales (VPN) y otros tipos de redes.



ftp:

FTP (File Transfer Protocol) es un protocolo de red que se utiliza para transferir archivos entre dos ordenadores. FTP es un protocolo muy popular y se utiliza en una amplia gama de aplicaciones, como la descarga de archivos de Internet, la transferencia de archivos entre servidores y el acceso a archivos en dispositivos de almacenamiento conectados a la red (NAS).

```
Windows PowerShell
PS C:\Users\scara\Desktop> ftp /?

Transfiere archivos a y desde un equipo que ejecute un servicio de servidor
de FTP (a veces conocido como demonio). FTP se puede usar interactivamente.

FTP [-v] [-d] [-i] [-n] [-g] [-s:archivo] [-a] [-A] [-x:búfer_envío]
    [-r:búfer_recep] [-b:búfers_asínc] [-w:tam_ventana] [host]

-v          Suprime la presentación de las respuestas del servidor
            remoto.
-n          Suprime el inicio de sesión automático cuando se
            establece la conexión inicial.
-i          Desactiva la intervención interactiva del usuario cuando
            se transfieren varios archivos.
-d          Activa la depuración.
-g          Desactiva el uso de comodines en nombres de archivo
            (ver GLOB).
-s:archivo  Especifica un archivo de texto con comandos de FTP;
            los comandos se ejecutarán automáticamente cuando FTP
            se inicie.
-a          Usa cualquier interfaz local para vincular una conexión
            de datos.
-A          Inicio de sesión anónimo.
-x:búfer_envío Invalida el tamaño de SO_SNDBUF predeterminado (8192).
-r:búfer_recep Invalida el tamaño de SO_RCVBUF predeterminado (8192).
-b:cuenta_async Invalida la cuenta asíncrona de 3
-w:tam_ventana Invalida el tamaño del búfer de transferencia
            predeterminado (65535).
host        Especifica el nombre del host o la dirección IP del host
            remoto al que se conecta.

Notas:
- Los comandos mget and mput aceptan s/n/c para sí/no/cancelar.
- Use Control-C para cancelar comandos.
PS C:\Users\scara\Desktop>
```

Getmac:

El comando getmac se utiliza para mostrar la dirección MAC (Media Access Control) de todas las interfaces de red en un ordenador con Windows. La dirección MAC es un identificador único que se asigna a cada interfaz de red.

```
Windows PowerShell
-d          Activa la depuración.
-g          Desactiva el uso de comodines en nombres de archivo
            (ver GLOB).
-s:archivo  Especifica un archivo de texto con comandos de FTP;
            los comandos se ejecutarán automáticamente cuando FTP
            se inicie.
-a          Usa cualquier interfaz local para vincular una conexión
            de datos.
-A          Inicio de sesión anónimo.
-x:búfer_envío Invalida el tamaño de SO_SNDBUF predeterminado (8192).
-r:búfer_recep Invalida el tamaño de SO_RCVBUF predeterminado (8192).
-b:cuenta_async Invalida la cuenta asíncrona de 3
-w:tam_ventana Invalida el tamaño del búfer de transferencia
            predeterminado (65535).
host        Especifica el nombre del host o la dirección IP del host
            remoto al que se conecta.

Notas:
- Los comandos mget and mput aceptan s/n/c para sí/no/cancelar.
- Use Control-C para cancelar comandos.
PS C:\Users\scara\Desktop> getmac

Dirección física      Nombre de transporte
=====
N/A                   Medios desconectados
00-FF-A2-46-9A-00     Medios desconectados
2C-3B-70-66-FC-AD     \Device\Tcpip_{44456F6D-A33E-447A-BCD4-09D1DE3764E5}
7C-4D-8F-A0-A7-DD     Medios desconectados
0A-00-27-00-00-13     \Device\Tcpip_{D10D3714-EA7E-43F7-B0BF-0FD845CD12D0}
PS C:\Users\scara\Desktop> |
```

Hostname:

El comando hostname se utiliza para obtener o establecer el nombre de host de un ordenador. El nombre de host es un identificador único que se asigna a un ordenador en una red.

```
Windows PowerShell
de datos.
-A Inicio de sesión anónimo.
-x:búfer_envio Invalida el tamaño de SO_SNDBUF predeterminado (8192).
-r:búfer_recep Invalida el tamaño de SO_RCVBUF predeterminado (8192).
-b:cuenta_async Invalida la cuenta asíncrona de 3
-w:tam_ventana Invalida el tamaño del búfer de transferencia
predeterminado (65535).
host Especifica el nombre del host o la dirección IP del host
remoto al que se conecta.

Notas:
- Los comandos mget and mput aceptan s/n/c para sí/no/cancelar.
- Use Control-C para cancelar comandos.
PS C:\Users\scara\Desktop> getmac

Dirección física      Nombre de transporte
=====
N/A                   Medios desconectados
00-FF-A2-46-9A-00     Medios desconectados
2C-3B-70-66-FC-AD     \Device\Tcpip_{44456F6D-A33E-447A-BCD4-09D1DE3764E5}
7C-4D-8F-A0-A7-DD     Medios desconectados
0A-00-27-00-00-13     \Device\Tcpip_{D10D3714-EA7E-43F7-B0BF-0FD845CD12D0}
PS C:\Users\scara\Desktop>
PS C:\Users\scara\Desktop>
PS C:\Users\scara\Desktop>
PS C:\Users\scara\Desktop>
PS C:\Users\scara\Desktop>
PS C:\Users\scara\Desktop> hostname
LAPTOP-CKIJCJEQ
PS C:\Users\scara\Desktop> |
```

Nbtstat:

El comando nbtstat es una herramienta de diagnóstico de red que se utiliza para mostrar información sobre NetBIOS sobre TCP/IP (NetBIOS over TCP/IP, NBT). NBT es un protocolo que permite a los ordenadores Windows comunicarse entre sí utilizando nombres NetBIOS.

```
Windows PowerShell
LAPTOP-CKIJCJEQ
PS C:\Users\scara\Desktop> nbtstat

Muestra las estadísticas del protocolo y las conexiones actuales de TCP/IP
usando NBT (NetBIOS sobre TCP/IP).

NBTSTAT [ [-a NombreRemoto] [-A dirección IP] [-c] [-n] [-r] [-R] [-RR]
[-s] [-S] [intervalo] ]

-a (estado del adaptador) Hace una lista de la tabla de nombres de
los equipos remotos según su nombre
-A (estado del adaptador) Hace una lista de la tabla de nombres de
los equipos remotos según sus direcciones de IP.
-c (caché) Hace una lista de los nombres [equipo]remotos de la caché
NBT y sus direcciones de IP
-n (nombres) Hace una lista de los nombres NetBIOS locales.
-r (resueltos) Lista de nombres resueltos por difusión y vía WINS
-R (Volver a cargar) Purga y vuelve a cargar la tabla de nombres de
la caché remota
-S (Sesiones) Hace una lista de la tabla de sesiones con las
direcciones de destino de IP
-s (sesiones) Hace una lista de la tabla de sesiones convirtiendo
las direcciones de destino de IP en nombres de equipo NETBIOS.
-RR (LiberarActualizar) Envía paquetes de Liberación de nombres a WINS
y después, inicia Actualizar

NombreRemoto Nombre del equipo de host remoto.
Dirección IP Representación del Punto decimal de la dirección de IP.
intervalo Vuelve a mostrar estadísticas seleccionadas, pausando
segundos de intervalo entre cada muestra. Presionar Ctrl+C
para parar volver a mostrar las estadísticas.

PS C:\Users\scara\Desktop> |
```

Net:

El comando net es una herramienta de línea de comandos que se utiliza para administrar redes en sistemas operativos Windows. El comando net puede utilizarse para realizar una variedad de tareas, como:

- Ver y configurar la configuración de red

- Ver y administrar conexiones de red
- Ver y administrar cuentas de usuario y grupos
- Ver y administrar servicios
- Ver y administrar recursos compartidos

```

Windows PowerShell
los equipos remotos según su nombre
-A (estado del adaptador) hace una lista de la tabla de nombres de
los equipos remotos según sus direcciones de IP.
-c (caché) Hace una lista de los nombres [equipo]remotos de la caché
NBT y sus direcciones de IP
-n (nombres) Hace una lista de los nombres NetBIOS locales.
-r (resueltos) Lista de nombres resueltos por difusión y vía WINS
-R (Volver a cargar) Purga y vuelve a cargar la tabla de nombres de
la caché remota
-S (Sesiones) Hace una lista de la tabla de sesiones con las
direcciones de destino de IP
-s (sesiones) Hace una lista de la tabla de sesiones convirtiendo
las direcciones de destino de IP en nombres de equipo NETBIOS.
-RR (LiberarActualizar) Envía paquetes de Liberación de nombres a WINS
y después, inicia Actualizar

NombreRemoto Nombre del equipo de host remoto.
Dirección IP Representación del Punto decimal de la dirección de IP.
intervalo Vuelve a mostrar estadísticas seleccionadas, pausando
segundos de intervalo entre cada muestra. Presionar Ctrl+C
para parar volver a mostrar las estadísticas.

PS C:\Users\scara\Desktop> net
La sintaxis de este comando es:

NET
[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
STATISTICS | STOP | TIME | USE | USER | VIEW ]

PS C:\Users\scara\Desktop>

```

net use:

El comando net use se utiliza para conectar y desconectar recursos compartidos de red en sistemas operativos Windows. Los recursos compartidos de red son archivos, carpetas o impresoras que se han compartido con otros usuarios en la red.

```
Windows PowerShell
PS C:\Users\scara\Desktop> net use /?
La sintaxis de este comando es:

NET USE
[devicename | *] [\\computername\sharename[\volume] [password | *]]
[/USER:[domainname\]username]
[/USER:[dotted domain name\]username]
[/USER:[username@dotted domain name]
[/SMARTCARD]
[/SAVECRED]
[/REQUIREINTEGRITY]
[/REQUIREPRIVACY]
[/WRITETHROUGH]
[/TRANSPORT:{TCP | QUIC} [/SKIPCERTCHECK]]
[/REQUESTCOMPRESSION:{YES | NO}]
[/GLOBAL]
[[/DELETE] [/GLOBAL]]

NET USE {devicename | *} [password | *] /HOME

NET USE [/PERSISTENT:{YES | NO}]

PS C:\Users\scara\Desktop> |
```

Netsh:

Netsh (Network Shell) es una utilidad de línea de comandos que se utiliza para configurar y mostrar el estado de varios componentes de red en Windows. Netsh es una herramienta muy poderosa y puede utilizarse para realizar una amplia gama de tareas de administración de redes, como:

- Configurar interfaces de red
- Configurar el protocolo TCP/IP
- Configurar el DNS
- Configurar el firewall de Windows
- Configurar el enrutamiento
- Configurar el DHCP
- Configurar el VPN
- Configurar la QoS
- Configurar el proxy
- Solucionar problemas de red

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows

PS C:\Users\scara\Desktop> netsh /?

Uso: C:\windows\system32\netsh.exe [-a ArchAlias] [-c Contexto] [-r EquipoRemoto] [-u
[NombreDominio\NombreUsuario] [-p Contraseña] [*]
[Comando] [-f ArchivoScript]

Los siguientes comandos están disponibles:

Comandos en este contexto:
? - Muestra una lista de comandos.
add - Agrega una entrada de configuración a una lista de entradas.
advfirewall - Cambia al contexto 'netsh advfirewall'.
bridge - Cambia al contexto 'netsh bridge'.
delete - Elimina una entrada de configuración de una lista de entradas.
dhcpcclient - Cambia al contexto 'netsh dhcpcclient'.
dnsclient - Cambia al contexto 'netsh dnsclient'.
dump - Muestra un script de configuración.
exec - Ejecuta un archivo de script.
firewall - Cambia al contexto 'netsh firewall'.
help - Muestra una lista de comandos.
http - Cambia al contexto 'netsh http'.
interface - Cambia al contexto 'netsh interface'.
ipsec - Cambia al contexto 'netsh ipsec'.
lan - Cambia al contexto 'netsh lan'.
mbn - Cambia al contexto 'netsh mbn'.
namespace - Cambia al contexto 'netsh namespace'.
netio - Cambia al contexto 'netsh netio'.
nlm - Cambia al contexto 'netsh nlm'.
p2p - Cambia al contexto 'netsh p2p'.
ras - Cambia al contexto 'netsh ras'.
rpc - Cambia al contexto 'netsh rpc'.
set - Actualiza las opciones de configuración.
show - Muestra información.
trace - Cambia al contexto 'netsh trace'.
wcn - Cambia al contexto 'netsh wcn'.
wfp - Cambia al contexto 'netsh wfp'.
winhttp - Cambia al contexto 'netsh winhttp'.
winsock - Cambia al contexto 'netsh winsock'.
wlan - Cambia al contexto 'netsh wlan'.

Los siguientes subcontextos están disponibles:
advfirewall bridge dhcpcclient dnsclient firewall http interface ipsec lan mbn namespace netio nlm p2p ras rpc trace wcn wfp winhttp winsock wlan
```

pathping:

El comando pathping es una herramienta de línea de comandos que se utiliza para identificar problemas de red entre un origen y un destino. Combina las características de los comandos ping y traceroute, pero proporciona información más detallada.

```
Windows PowerShell

nlm - Cambia al contexto 'netsh nlm'.
p2p - Cambia al contexto 'netsh p2p'.
ras - Cambia al contexto 'netsh ras'.
rpc - Cambia al contexto 'netsh rpc'.
set - Actualiza las opciones de configuración.
show - Muestra información.
trace - Cambia al contexto 'netsh trace'.
wcn - Cambia al contexto 'netsh wcn'.
wfp - Cambia al contexto 'netsh wfp'.
winhttp - Cambia al contexto 'netsh winhttp'.
winsock - Cambia al contexto 'netsh winsock'.
wlan - Cambia al contexto 'netsh wlan'.

Los siguientes subcontextos están disponibles:
advfirewall bridge dhcpcclient dnsclient firewall http interface ipsec lan mbn namespace netio nlm p2p ras rpc trace wcn wfp winhttp winsock wla
n

Para ver más ayuda acerca de un comando, escríbalo seguido de un espacio y
después escriba ?.
PS C:\Users\scara\Desktop> pathping

Uso: pathping [-g lista_host] [-h saltos_máx] [-i dirección] [-n]
[-p periodo] [-q núm_consultas] [-w tiempo_espera]
[-4] [-6] nombre_destino

Opciones:
-g lista_host Ruta de origen no estricta en la lista de host.
-h saltos_máx Número máximo de saltos para buscar en el destino.
-i dirección Utilizar la dirección de origen especificada.
-n No resolver direcciones como nombres de host.
-p periodo Período de espera en milisegundos entre llamadas ping.
-q núm_consultas Número de consultas por salto.
-w tiempo_espera Tiempo de espera en milisegundos para cada respuesta.
-4 Fuerza utilizando IPv4.
-6 Fuerza utilizando IPv6.
PS C:\Users\scara\Desktop> |
```

Rcp:

El comando rcp es una herramienta de línea de comandos que se utiliza para copiar archivos o directorios entre un sistema local y un sistema remoto, o entre dos sistemas remotos.

```
Windows PowerShell
PS C:\Users\scara\Desktop> rcp /?
rcp : El término 'rcp' no se reconoce como nombre de un cmdlet, función, archivo de script o programa ejecutable. Compruebe si escribió correctamente el nombre o, si incluyó una ruta de acceso, compruebe que dicha ruta es correcta e inténtelo de nuevo.
En línea: 1 Carácter: 1
+ rcp /?
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (rcp:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\scara\Desktop> |
```

rexec:

El comando rexec es una herramienta de línea de comandos que se utiliza para ejecutar comandos en un sistema remoto. El comando rexec utiliza el protocolo REXEC (Remote Execution Protocol) para comunicarse con el sistema remoto.

```
Windows PowerShell
PS C:\Users\scara\Desktop> rexec /?
rexec : El término 'rexec' no se reconoce como nombre de un cmdlet, función, archivo de script o programa ejecutable. Compruebe si escribió correctamente el nombre o, si incluyó una ruta de acceso, compruebe que dicha ruta es correcta e inténtelo de nuevo.
En línea: 1 Carácter: 1
+ rexec /?
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (rexec:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\scara\Desktop> |
```

Route:

El comando route se utiliza para ver y manipular la tabla de enrutamiento en un sistema operativo. La tabla de enrutamiento es una base de datos que contiene información sobre cómo llegar a diferentes redes.

```
Windows PowerShell
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\scara\Desktop> route

Manipula tablas de enrutamiento de red.

ROUTE [-f] [-p] [-4|-6] comando [destino] [MASK máscara_red] [puerta_enlace]
[METRIC métrica] [IF interfaz]

-f          Borra las tablas de enrutamiento de todas las entradas
            de puerta de enlace. Si se usa junto con uno de los
            comandos, se borrarán las tablas antes de ejecutarse el
            comando.

-p          Cuando se usa con el comando ADD, hace una ruta
            persistente en los arranques del sistema. De manera
            predeterminada, las rutas no se conservan cuando se
            reinicia el sistema. Se pasa por alto para todos los
            demás comandos, que siempre afectan a las rutas
            persistentes apropiadas.

-4          Forzar el uso de IPv4.

-6          Forzar el uso de IPv6.

comando     Alguno de los siguientes:
            PRINT      Imprime una ruta
            ADD        Agrega una ruta
            DELETE     Elimina una ruta
            CHANGE     Modifica una ruta existente

destino     Especifica el host.

MASK        Especifica que el siguiente parámetro es el valor de
            'máscara_red'.

máscara_red Especifica un valor de máscara de subred para esta
            entrada de ruta.
            Si no se especifica, se usa de forma predeterminada el
```

Rpcping:

El comando rpcping es una herramienta de línea de comandos que se utiliza para probar la conectividad a un servicio RPC (Remote Procedure Call) en un ordenador remoto. El comando rpcping envía una serie de solicitudes de RPC al servicio remoto y mide el tiempo de respuesta.

```
Windows PowerShell

Error al agregar la ruta: El parámetro de máscara especificado
no es válido. (Destino & Máscara) != Destino.

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
PS C:\Users\scara\Desktop> rpcping
Excepción 5 (0x00000005)
Número de registros: 1
ProcessID: 15540
Hora del sistema: 10/20/2023 2:54:892
Generación de componentes: 2
Estado: 0x5, 5
La ubicación de detección: 1750
Marcas: 0
NumberOfParameters: 1
Valor Long: 0x5
PS C:\Users\scara\Desktop> |
```

Rsh:

El comando rsh (Remote Shell) es una herramienta de línea de comandos que se utiliza para ejecutar comandos en un sistema remoto sin tener que iniciar sesión en ese sistema. El comando rsh utiliza el protocolo RSH (Remote Shell Protocol) para comunicarse con el sistema remoto.

```
Windows PowerShell

> 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

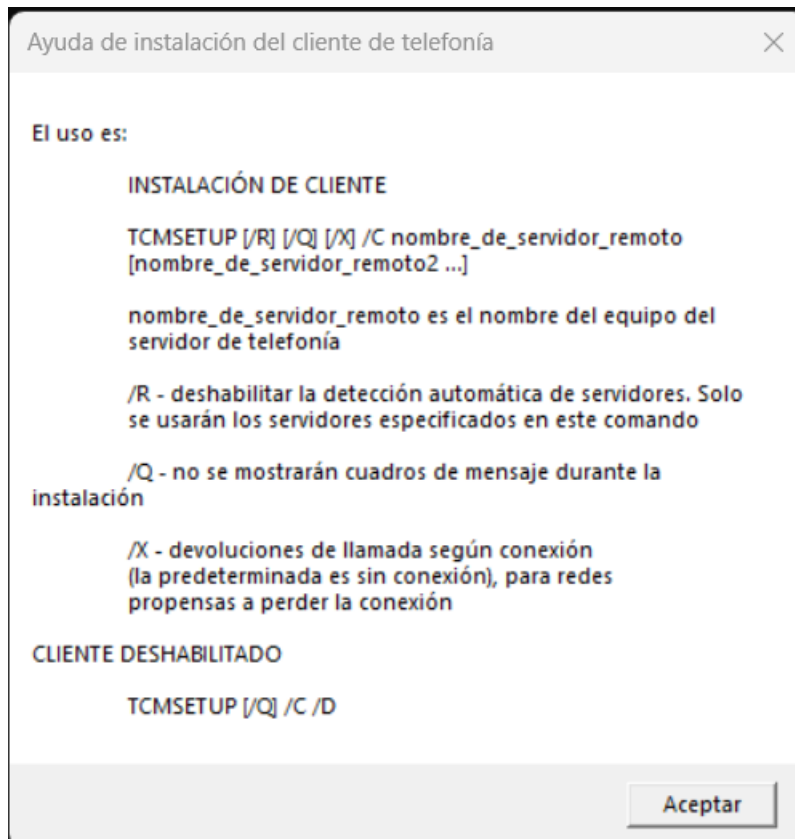
CHANGE solo se usa para modificar la puerta de enlace o la métrica.

> route DELETE 157.0.0.0
> route DELETE 3ffe::/32
PS C:\Users\scara\Desktop> rpsping
Excepción 5 (0x00000005)
Número de registros: 1
ProcessID: 15540
Hora del sistema: 10/20/2023 2:5:54:892
Generación de componentes: 2
Estado: 0x5, 5
La ubicación de detección: 1750
Marcas: 0
NumberOfParameters: 1
Valor Long: 0x5
PS C:\Users\scara\Desktop> rsh
rsh : El término 'rsh' no se reconoce como nombre de un cmdlet, función, archivo de script o programa ejecutable. Compruebe si escribió
correctamente el nombre o, si incluyó una ruta de acceso, compruebe que dicha ruta es correcta e inténtelo de nuevo.
En línea: 1 Carácter: 1
+ rsh
+ ~~~~
+ CategoryInfo          : ObjectNotFound: (rsh:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\scara\Desktop> |
```

Tcmsetup:

El comando tcmsetup se utiliza para configurar y deshabilitar el cliente TAPI (Telephony Application Programming Interface) en un sistema operativo Windows. TAPI es un conjunto de interfaces de programación de aplicaciones que permite a las aplicaciones de software comunicarse con dispositivos telefónicos.



telnet:

Telnet es un protocolo de red que permite a los usuarios conectarse a un ordenador remoto y ejecutarlo como si estuvieran sentados frente a él. Telnet utiliza una conexión de texto sin formato, lo que significa que los usuarios pueden ver y escribir comandos directamente en el ordenador remoto.

```
Windows PowerShell
PS C:\Users\scara\Desktop> telnet
telnet : El término 'telnet' no se reconoce como nombre de un cmdlet, función, archivo de script o programa ejecutable. Compruebe si escribió correctamente el nombre o, si incluyó una ruta de acceso, compruebe que dicha ruta es correcta e inténtelo de nuevo.
En línea: 1 Carácter: 1
+ telnet
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (telnet:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\scara\Desktop> |
```

Tftp:

TFTP (Trivial File Transfer Protocol) es un protocolo de red simple que se utiliza para transferir archivos entre dos ordenadores. TFTP es un protocolo sin conexión, lo que significa que cada paquete se transfiere por separado y no se requiere una conexión establecida entre los dos ordenadores.

```
Windows PowerShell
PS C:\Users\scara\Desktop> tftp
tftp : El término 'tftp' no se reconoce como nombre de un cmdlet, función, archivo de script o programa ejecutable. Compruebe si escribió correctamente el nombre o, si incluyó una ruta de acceso, compruebe que dicha ruta es correcta e inténtelo de nuevo.
En línea: 1 Carácter: 1
+ tftp
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (tftp:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\scara\Desktop> |
```