PORTADA

NOMBRE: BRAYN SAHAGUN

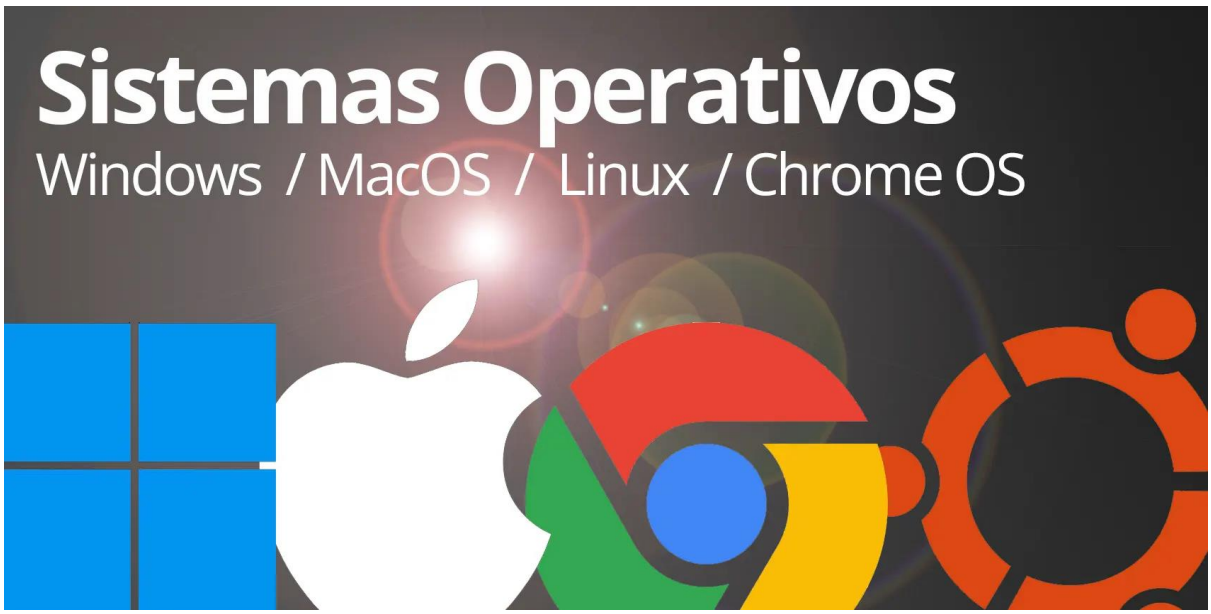
PROFESOR: JIMENEZ SANCHEZ ISMAEL

ESCUELA: UPQROO

CARRERA: INGENIERÍA EN SOFTWARE

MATERIA: SISTEMAS OPERATIVOS

GRUPO: 27BV **CUATRIMESTRE:** 7mo



PRACTICA DE LABORATORIO

Comandos en MSDOS

Comandos:

Anotar los comandos necesarios para ejecutar las siguientes instrucciones desde la consola de Ms- DOS

1.- Obtener la ayuda del comando ping

ping

```
Microsoft Windows [Versión 10.0.19045.3570]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\aiden>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 parametro

```
C:\Users\aiden>ping -t 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
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
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 127.0.0.1:
    Paquetes: enviados = 13, recibidos = 13, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
Control-C
^C
```

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

```
C:\Users\aiden>ping google.com

Haciendo ping a google.com [142.250.217.238] con 32 bytes de datos:
Respuesta desde 142.250.217.238: bytes=32 tiempo=28ms TTL=118
Respuesta desde 142.250.217.238: bytes=32 tiempo=24ms TTL=118
Respuesta desde 142.250.217.238: bytes=32 tiempo=23ms TTL=118
Respuesta desde 142.250.217.238: bytes=32 tiempo=23ms TTL=118

Estadísticas de ping para 142.250.217.238:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 23ms, Máximo = 28ms, Media = 24ms
```

El ping se realizo de manera correcta y no se perdió ningún paquete.

4.- Obtener la ayuda del comando nslookup

```
C:\Users\aiden>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'
```

5.- Resolver la direccion ip de https://upqroo.edu.mx/ usando nslookup

```
C:\Users\aiden>nslookup upqroo.edu.mx
Servidor:  UnKnown
Address:  192.168.100.1

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

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

```
C:\Users\aiden>ping 192.168.100.1

Haciendo ping a 192.168.100.1 con 32 bytes de datos:
Respuesta desde 192.168.100.1: bytes=32 tiempo=1ms TTL=63
Respuesta desde 192.168.100.1: bytes=32 tiempo=1ms TTL=63
Respuesta desde 192.168.100.1: bytes=32 tiempo=1ms TTL=63
Respuesta desde 192.168.100.1: bytes=32 tiempo=1ms TTL=63

Estadísticas de ping para 192.168.100.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 1ms, Media = 1ms
```

El ping se realizó de manera correcta y no se perdió ningún paquete.

7.- Obtener la ayuda del comando netstat

```
C:\Users\aiden>netstat /?

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

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

  -a            Muestra todas las conexiones y los puertos de escucha.
  -b            Muestra el archivo ejecutable implicado en la creación de cada conexión o
                puerto de escucha. En algunos casos los archivos ejecutables conocidos hospedan
                varios componentes independientes y, en esos casos, se muestra la
                secuencia de componentes implicados en la creación de la conexión
                o el puerto de escucha. En este caso, el nombre del archivo ejecutable
                está entre corchetes ([]) en la parte inferior; en la parte superior se encuentra el componente al que se llamó,
                y así hasta que se llega al valor de TCP/IP. Ten en cuenta que esta opción
                puede llevar bastante tiempo; además, es posible que se produzca un error si no tienes suficientes
                permisos.
  -e            Muestra las estadísticas de Ethernet. Este valor se puede combinar con la
                opción -s.
  -f            Muestra los nombres de dominio completos (FQDN) de las direcciones
                externas.
  -n            Muestra las direcciones y los números de puerto de forma numérica.
  -o            Muestra el id. de cada proceso de propiedad asociado a la conexión.
  -p proto      Muestra las conexiones del protocolo que especificó el valor proto; este valor proto
                puede ser: TCP, UDP, TCPv6 o UDPv6.  Si se usa con la opción -s
                para mostrar las estadísticas de cada protocolo, el valor proto será cualquiera de estos:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
  -q            Muestra todas las conexiones, puertos de escucha y puertos
                TCP enlazados que no sean para la escucha. Estos últimos pueden (o no) asociarse
                a una conexión activa.
  -r            Muestra la tabla de enrutamiento.
  -s            Muestra las estadísticas por protocolo. De forma predeterminada, las estadísticas se muestran
                en función de los valores de IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP y UDPv6;
                la opción -p se puede usar para especificar un subconjunto del valor predeterminado.
  -t            Muestra el estado de descarga de la conexión actual.
  -x            Muestra conexiones, agentes de escucha y puntos de conexión compartidos de
                 NetworkDirect.
  -y            Muestra la plantilla de conexión TCP para todas las conexiones.
                No se puede combinar con otras opciones
```

8.- Mostrar todas las conexiones y puertos de escucha

```
C:\Users\aiden>netstat -a

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    0.0.0.0:80             DESKTOP-U1N3SDL:0      LISTENING
  TCP    0.0.0.0:135            DESKTOP-U1N3SDL:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-U1N3SDL:0      LISTENING
  TCP    0.0.0.0:5040           DESKTOP-U1N3SDL:0      LISTENING
  TCP    0.0.0.0:7680           DESKTOP-U1N3SDL:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-U1N3SDL:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-U1N3SDL:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-U1N3SDL:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-U1N3SDL:0      LISTENING
  TCP    0.0.0.0:49668          DESKTOP-U1N3SDL:0      LISTENING
  TCP    0.0.0.0:49669          DESKTOP-U1N3SDL:0      LISTENING
  TCP    127.0.0.1:4699         DESKTOP-U1N3SDL:0      LISTENING
  TCP    127.0.0.1:6463         DESKTOP-U1N3SDL:0      LISTENING
  TCP    127.0.0.1:49709        voyovoy:65001          ESTABLISHED
  TCP    127.0.0.1:49712        DESKTOP-U1N3SDL:0      LISTENING
  TCP    127.0.0.1:49754        voyovoy:49755          ESTABLISHED
  TCP    127.0.0.1:49755        voyovoy:49754          ESTABLISHED
  TCP    127.0.0.1:49770        voyovoy:49771          ESTABLISHED
  TCP    127.0.0.1:49771        voyovoy:49770          ESTABLISHED
  TCP    127.0.0.1:49772        voyovoy:49773          ESTABLISHED
  TCP    127.0.0.1:49773        voyovoy:49772          ESTABLISHED
  TCP    127.0.0.1:49785        DESKTOP-U1N3SDL:0      LISTENING
  TCP    127.0.0.1:65001        DESKTOP-U1N3SDL:0      LISTENING
  TCP    127.0.0.1:65001        voyovoy:49709          ESTABLISHED
  TCP    192.168.1.138:139      DESKTOP-U1N3SDL:0      LISTENING
  TCP    192.168.1.138:49701    20.10.31.115:https     ESTABLISHED
```

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

```
C:\Users\aiden>netstat -n

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    127.0.0.1:49709        127.0.0.1:65001        ESTABLISHED
  TCP    127.0.0.1:49754        127.0.0.1:49755        ESTABLISHED
  TCP    127.0.0.1:49755        127.0.0.1:49754        ESTABLISHED
  TCP    127.0.0.1:49770        127.0.0.1:49771        ESTABLISHED
  TCP    127.0.0.1:49771        127.0.0.1:49770        ESTABLISHED
  TCP    127.0.0.1:49772        127.0.0.1:49773        ESTABLISHED
  TCP    127.0.0.1:49773        127.0.0.1:49772        ESTABLISHED
  TCP    127.0.0.1:65001        127.0.0.1:49709        ESTABLISHED
  TCP    192.168.1.138:49701    20.10.31.115:443       ESTABLISHED
  TCP    192.168.1.138:49766    162.247.241.2:443      CLOSE_WAIT
  TCP    192.168.1.138:49769    162.247.241.2:443      CLOSE_WAIT
  TCP    192.168.1.138:49781    162.247.241.2:443      CLOSE_WAIT
  TCP    192.168.1.138:49783    162.247.241.2:443      CLOSE_WAIT
  TCP    192.168.1.138:50425    192.168.1.119:8009     ESTABLISHED
  TCP    192.168.1.138:50426    108.177.11.188:5228    ESTABLISHED
  TCP    192.168.1.138:50486    157.240.14.52:443      ESTABLISHED
  TCP    192.168.1.138:50492    20.94.21.149:443       ESTABLISHED
  TCP    192.168.1.138:50542    162.159.130.234:443    ESTABLISHED
  TCP    192.168.1.138:50559    35.241.8.242:443       ESTABLISHED
  TCP    192.168.1.138:50566    20.94.21.149:443       ESTABLISHED
  TCP    192.168.1.138:50571    23.64.121.169:443      LAST_ACK
  TCP    192.168.1.138:50580    51.104.167.186:443     TIME_WAIT
  TCP    192.168.1.138:50581    23.15.160.213:443      ESTABLISHED
  TCP    192.168.1.138:50582    204.79.197.200:443     ESTABLISHED
  TCP    192.168.1.138:50583    23.64.121.169:443      ESTABLISHED
  TCP    192.168.1.138:50584    13.89.178.26:443       ESTABLISHED

C:\Users\aiden>
```

10.- Mostrar las conexiones TCP

```
C:\Users\aiden>netstat -t

Conexiones activas

  Proto  Dirección local          Dirección remota        Estado
           Estado de descarga

  TCP    127.0.0.1:49709         voyovoy:65001          ESTABLISHED     EnHost
  TCP    127.0.0.1:49754         voyovoy:49755          ESTABLISHED     EnHost
  TCP    127.0.0.1:49755         voyovoy:49754          ESTABLISHED     EnHost
  TCP    127.0.0.1:49770         voyovoy:49771          ESTABLISHED     EnHost
  TCP    127.0.0.1:49771         voyovoy:49770          ESTABLISHED     EnHost
  TCP    127.0.0.1:49772         voyovoy:49773          ESTABLISHED     EnHost
  TCP    127.0.0.1:49773         voyovoy:49772          ESTABLISHED     EnHost
  TCP    127.0.0.1:65001         voyovoy:49709          ESTABLISHED     EnHost
  TCP    192.168.1.138:49701     20.10.31.115:https     ESTABLISHED     EnHost
  TCP    192.168.1.138:49766     162.247.241.2:https    CLOSE_WAIT      EnHost
  TCP    192.168.1.138:49769     162.247.241.2:https    CLOSE_WAIT      EnHost
  TCP    192.168.1.138:49781     162.247.241.2:https    CLOSE_WAIT      EnHost
  TCP    192.168.1.138:49783     162.247.241.2:https    CLOSE_WAIT      EnHost
  TCP    192.168.1.138:50425     192.168.1.119:8009     ESTABLISHED     EnHost
  TCP    192.168.1.138:50426     vz-in-f188:5228        ESTABLISHED     EnHost
  TCP    192.168.1.138:50486     whatsapp-cdn-shv-02-mia3:https  ESTABLISHED     EnHost
  TCP    192.168.1.138:50492     20.94.21.149:https     ESTABLISHED     EnHost
  TCP    192.168.1.138:50542     162.159.130.234:https  ESTABLISHED     EnHost
  TCP    192.168.1.138:50559     242:https              ESTABLISHED     EnHost
  TCP    192.168.1.138:50566     20.94.21.149:https     ESTABLISHED     EnHost
  TCP    192.168.1.138:50580     51.104.167.186:https   TIME_WAIT       EnHost
  TCP    192.168.1.138:50581     a23-15-160-213:https   ESTABLISHED     EnHost
  TCP    192.168.1.138:50582     a-0001:https           ESTABLISHED     EnHost
  TCP    192.168.1.138:50583     a23-64-121-169:https   ESTABLISHED     EnHost
  TCP    192.168.1.138:50584     13.89.178.26:https     ESTABLISHED     EnHost
  TCP    192.168.1.138:50586     13.107.237.254:https   ESTABLISHED     EnHost
  TCP    192.168.1.138:50587     4.150.240.254:https    ESTABLISHED     EnHost
```

11.- Mostrar las conexiones UDP

```
C:\Users\aiden>netstat -u

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

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

  -a            Muestra todas las conexiones y los puertos de escucha.
  -b            Muestra el archivo ejecutable implicado en la creación de cada conexión o
                puerto de escucha. En algunos casos los archivos ejecutables conocidos hospedan
                varios componentes independientes y, en esos casos, se muestra la
                secuencia de componentes implicados en la creación de la conexión
                o el puerto de escucha. En este caso, el nombre del archivo ejecutable
                está entre corchetes ([]) en la parte inferior; en la parte superior se encuentra el componente al que
e llamó,
                y así hasta que se llega al valor de TCP/IP. Ten en cuenta que esta opción
                puede llevar bastante tiempo; además, es posible que se produzca un error si no tienes suficientes
                permisos.
  -e            Muestra las estadísticas de Ethernet. Este valor se puede combinar con la
                opción -s.
  -f            Muestra los nombres de dominio completos (FQDN) de las direcciones
                externas.
  -n            Muestra las direcciones y los números de puerto de forma numérica.
  -o            Muestra el id. de cada proceso de propiedad asociado a la conexión.
  -p proto      Muestra las conexiones del protocolo que especificó el valor proto; este valor proto
                puede ser: TCP, UDP, TCPv6 o UDPv6.  Si se usa con la opción -s
                para mostrar las estadísticas de cada protocolo, el valor proto será cualquiera de estos:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
  -q            Muestra todas las conexiones, puertos de escucha y puertos
```

12.- Utilizar el comando tasklist

```
C:\Users\aiden>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     22,496 KB
Registry                      148 Services                   0     53,372 KB
smss.exe                      544 Services                   0        456 KB
csrss.exe                     700 Services                   0      2,940 KB
wininit.exe                   800 Services                   0      1,328 KB
csrss.exe                     808 Console                    1      4,388 KB
services.exe                  872 Services                   0      8,384 KB
lsass.exe                     884 Services                   0     18,916 KB
svchost.exe                  1008 Services                   0     21,180 KB
fontdrvhost.exe               632 Services                   0      1,676 KB
winlogon.exe                  948 Console                    1      3,004 KB
fontdrvhost.exe              1028 Console                    1      5,712 KB
svchost.exe                  1072 Services                   0     13,204 KB
svchost.exe                  1132 Services                   0      4,040 KB
svchost.exe                  1288 Services                   0      1,492 KB
svchost.exe                  1292 Services                   0      9,444 KB
svchost.exe                  1304 Services                   0      6,684 KB
svchost.exe                  1312 Services                   0      2,268 KB
svchost.exe                  1412 Services                   0     15,908 KB
svchost.exe                  1428 Services                   0      3,820 KB
svchost.exe                  1448 Services                   0      5,028 KB
dwm.exe                      1504 Console                    1     60,656 KB
svchost.exe                  1612 Services                   0      1,868 KB
svchost.exe                  1732 Services                   0      6,612 KB
svchost.exe                  1804 Services                   0      3,304 KB
svchost.exe                  1840 Services                   0      2,520 KB
svchost.exe                  1964 Services                   0      6,876 KB
svchost.exe                  2004 Services                   0     28,128 KB
svchost.exe                  2028 Services                   0      9,852 KB
NVDisplay.Container.exe      1092 Services                   0      9,012 KB
svchost.exe                  1892 Services                   0      6,288 KB
svchost.exe                  2104 Services                   0      7,036 KB
```

13.- Utilizar el comando taskkill

```
C:\Users\aiden>taskkill /F /IM WmiPrvSE.exe
ERROR: no se pudo terminar el proceso "WmiPrvSE.exe" con PID 6700.
Motivo: Acceso denegado.
```

14.- Utilizar el comando tracert

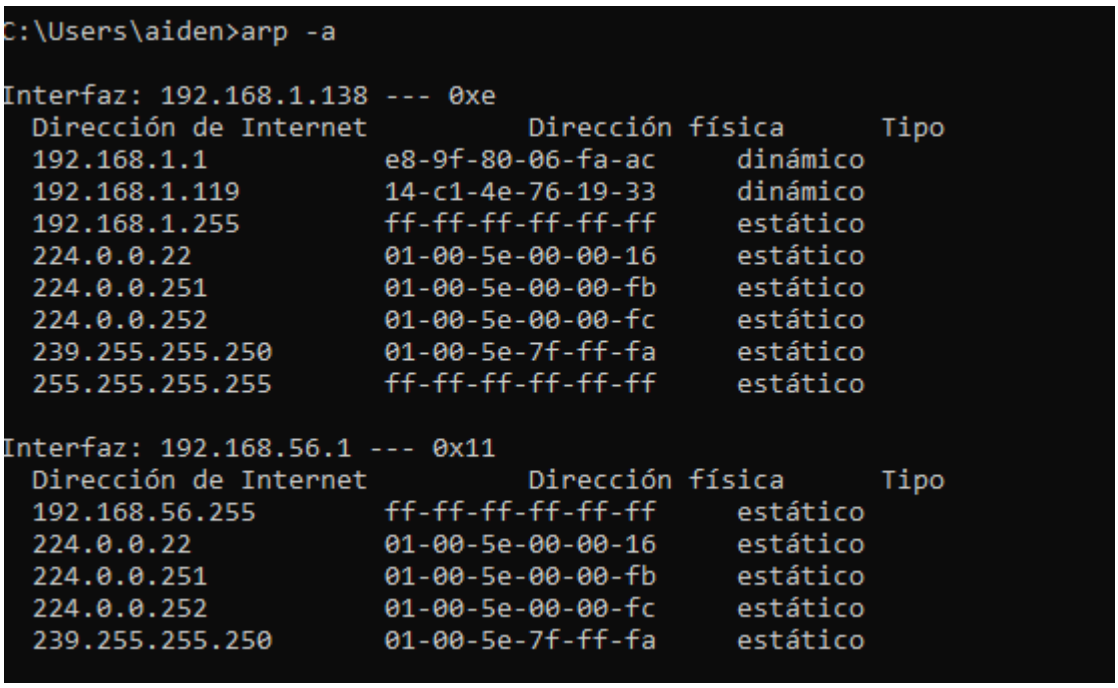
```
C:\Users\aiden>tracert google.com

Traza a la dirección google.com [142.250.217.238]
sobre un máximo de 30 saltos:

  1     1 ms     1 ms     1 ms  192.168.1.1
  2     1 ms     1 ms     1 ms  192.168.100.1
  3     5 ms     3 ms     4 ms  fixed-187-188-58-130.totalplay.net [187.188.58.130]
  4     4 ms     4 ms     4 ms  10.180.58.1
  5    19 ms    19 ms    20 ms  72.14.242.148
  6    52 ms    49 ms    19 ms  192.178.74.85
  7    19 ms    20 ms    18 ms  172.253.69.129
  8    24 ms    19 ms    18 ms  mia07s62-in-f14.1e100.net [142.250.217.238]

Traza completa.
```

15.- Utilizar el comando ARP



```
C:\Users\aiden>arp -a

Interfaz: 192.168.1.138 --- 0xe
  Dirección de Internet          Dirección física      Tipo
  192.168.1.1           e8-9f-80-06-fa-ac     dinámico
  192.168.1.119         14-c1-4e-76-19-33     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 --- 0x11
  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
```

Preguntas:

¿Para qué sirve el comando ping? El comando "ping" se utiliza para comprobar si dos dispositivos pueden comunicarse en una red. Es como un saludo digital. Envía un mensaje a otro dispositivo y verifica si obtiene una respuesta. Si lo hace, significa que hay una buena conexión. Si no, podría haber un problema en la red.

¿Para qué sirve el comando nslookup? El comando "nslookup" es como una libreta de direcciones de Internet. Te permite averiguar la dirección IP de un sitio web o servidor cuando solo conoces su nombre de dominio. Es útil para solucionar problemas si no puedes acceder a un sitio web, ya que te ayuda a verificar si el nombre de dominio se traduce correctamente en una dirección IP.

¿Para qué sirve el comando netstat? El comando "netstat" es como un espía de la red. Muestra una lista de las conexiones de red activas en tu computadora, los puertos que están abiertos y estadísticas sobre el tráfico de red. Ayuda a descubrir si algo inusual está ocurriendo en tu red, como aplicaciones que utilizan demasios recursos o posibles problemas de seguridad.

¿Para qué sirve el comando tasklist? El comando "tasklist" es como una lista de invitados para una fiesta en tu computadora. Muestra todos los programas y aplicaciones que se están ejecutando en ese momento, junto con detalles sobre ellos. Es útil para entender qué está sucediendo en tu computadora y para identificar programas problemáticos.

¿Para qué sirve el comando taskkill? El comando "taskkill" es como una forma de expulsar a un invitado no deseado de la fiesta en tu computadora. Te permite cerrar o finalizar programas o aplicaciones que se están ejecutando. Esto puede ser útil si una aplicación no responde o está causando problemas en tu computadora.

¿Para qué sirve el comando tracert? El comando "tracert" es como un rastreador de paquetes en la red. Muestra la ruta que siguen los datos desde tu computadora hasta un destino en la red, como un sitio web. Si hay problemas en el camino, "tracert" te ayudará a identificarlos al mostrar dónde se detiene o demora la comunicación.

¿Cómo ayudan los primeros tres comandos para detectar problemas en la red?
"Ping" verifica si los dispositivos pueden comunicarse, identificando pérdida de datos o demoras.
"Nslookup" soluciona problemas de resolución de nombres de dominio, ayudándote a encontrar la dirección IP de un sitio web.
"Netstat" muestra información sobre conexiones de red y puertos abiertos, lo que te permite identificar congestiones o configuraciones incorrectas en la red, así como problemas de seguridad. Estos comandos son herramientas valiosas para solucionar problemas de red.

Investigación:

atm:
Descripción: Muestra información sobre conexiones de alta velocidad.
Ejemplo: atmstat muestra estadísticas de conexiones de alta velocidad en tu sistema.

bitsadadmin:

Descripción: Administra trabajos de transferencia de archivos en segundo plano.
Ejemplo: bitsadadmin /list muestra una lista de trabajos de transferencia en segundo plano en tu computadora.

cmstp:
Descripción: Utilizado para instalar o desinstalar archivos en tu sistema.
Ejemplo: cmstp /s archivo.inf instala un archivo con la extensión .inf en tu sistema.

ftp:
Descripción: Se usa para transferir archivos a través de Internet.
Ejemplo: ftp ejemplo.com te conecta a un servidor para transferir archivos.

getmac:
Descripción: Muestra las direcciones únicas de tus adaptadores de red.
Ejemplo: getmac te mostrará las direcciones únicas de tus adaptadores de red.

hostname:
Descripción: Muestra o configura el nombre de tu computadora.
Ejemplo: hostname te mostrará el nombre actual de tu computadora.

nbtstat:
Descripción: Muestra estadísticas y detalles sobre un protocolo de red.
Ejemplo: nbtstat -a nombre_del_equipo muestra información sobre un equipo de la red.

net:
Descripción: Realiza varias tareas relacionadas con la red.
Ejemplo: net user muestra una lista de usuarios en el sistema.

net use:
Descripción: Conecta o desconecta recursos compartidos en red.
Ejemplo: net use Z: \\servidor\recurso conectará el recurso compartido en la unidad "Z:".

netsh:
Descripción: Configura aspectos de la red en tu sistema.
Ejemplo: netsh interface ipv4 show interfaces muestra información sobre las interfaces de red IPv4.

pathping:
Descripción: Combina traceroute y ping para seguir la ruta de paquetes de manera detallada.
Ejemplo: pathping ejemplo.com realizará un seguimiento de la ruta hacia "ejemplo.com".

rcp:
Descripción: Copia archivos desde un sistema remoto al tuyo.
Ejemplo: rcp archivo.txt usuario@servidor:/ruta/destino copia "archivo.txt" al sistema remoto.

telnet:
Descripción: Permite la comunicación con un host remoto a través de la línea de comandos.
Ejemplo: telnet ejemplo.com 80 abre una conexión a "ejemplo.com" en el puerto 80.

tftp:
Descripción: Se utiliza para transferir archivos de manera simple.
Ejemplo: tftp -i dirección_destino GET archivo transferirá un archivo desde un servidor TFTP a tu ubicación local.