UNIVERSIDAD POLITÉCNICA DE QUINTANA ROO

SISTEMAS OPERATIVOS

JIMÉNEZ SÁNCHEZ ISMAEL

TAREA #987

BRYAN HERNÁNDEZ ANDRADE

INGENIERÍA EN SOFTWARE

27BV

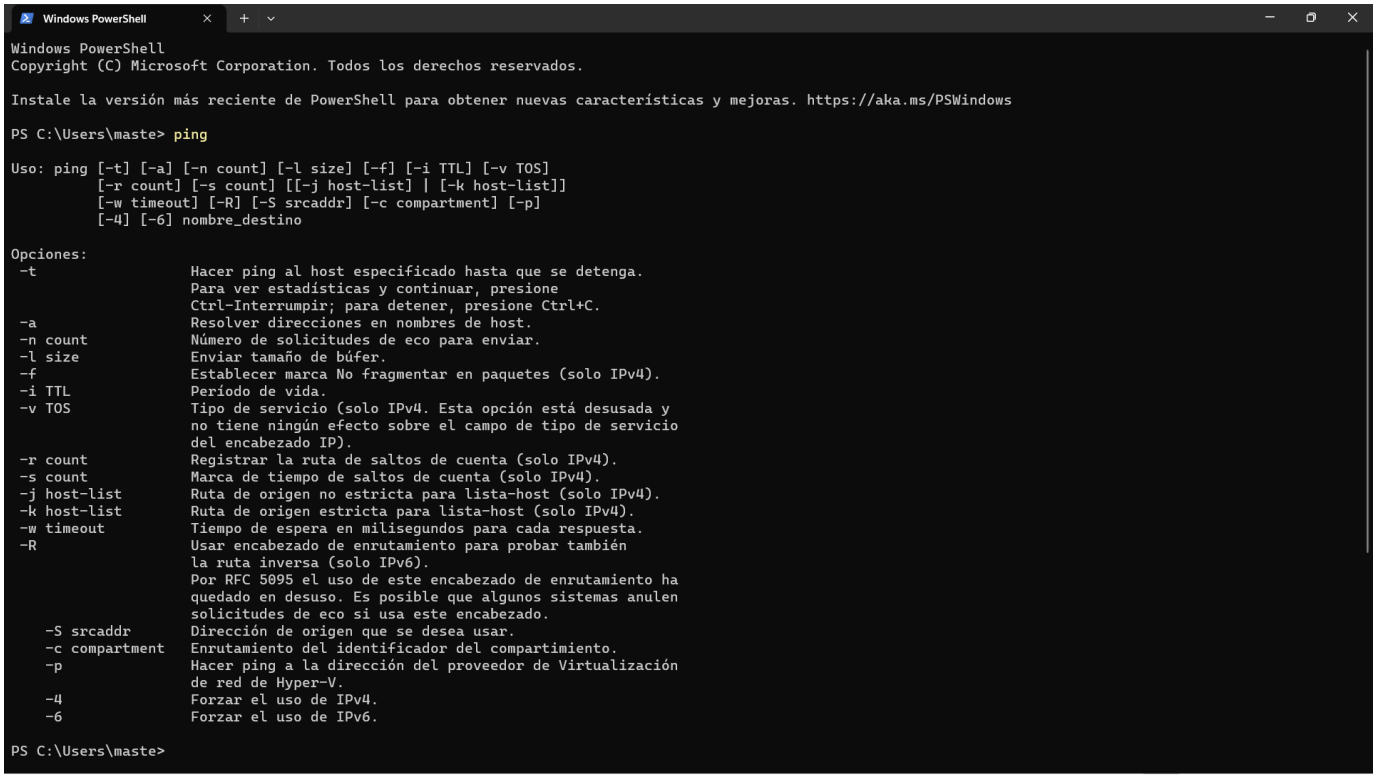
Practica de laboratorio

Comandos en MSDOS

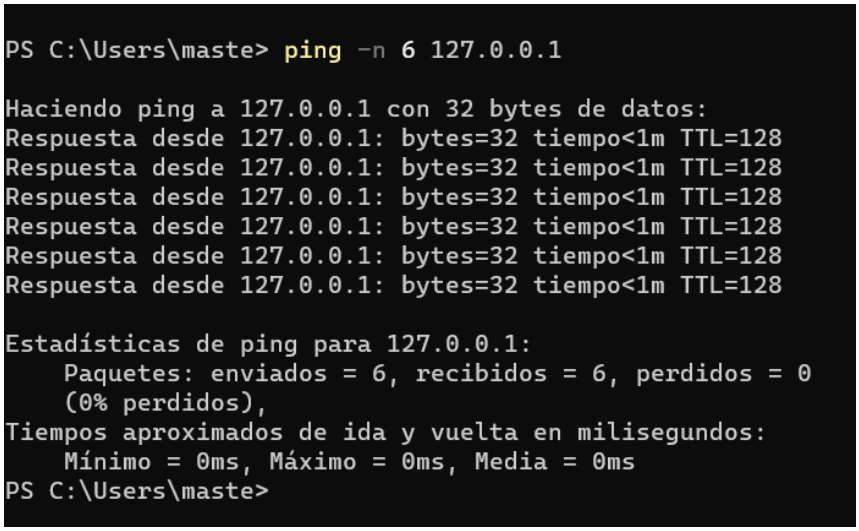
A) Anotar los comandos necesarios para ejecutar las siguientes instrucciones desde la consola de Msx

DQS

1." Obtener la ayuda del comando ping



2.- Enviar un ping a 127.0.0.1 aplicando cualquier param etro



3.- Verificar la conectividad del equipo utilizando el com an do ping, anotar conclusiones

```
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
PS C:\Users\maste> ping google.com

Haciendo ping a google.com [64.233.176.102] con 32 bytes de datos:
Respuesta desde 64.233.176.102: bytes=32 tiempo=31ms TTL=107
Respuesta desde 64.233.176.102: bytes=32 tiempo=31ms TTL=107
Respuesta desde 64.233.176.102: bytes=32 tiempo=31ms TTL=107
Respuesta desde 64.233.176.102: bytes=32 tiempo=31ms TTL=107

Estadísticas de ping para 64.233.176.102:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 31ms, Máximo = 31ms, Media = 31ms
PS C:\Users\maste>
```

4.- Obtener la ayuda del comando nslookup

```
    Mínimo = 31ms, Máximo = 31ms, Media = 31ms
PS C:\Users\maste> 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\maste>
```

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

```
   nslookup [-opt ...] host servidor # solo con
PS C:\Users\maste> nslookup upqroo.edu.mx
Servidor:  b.resolvers.level3.net
Address:  4.2.2.2

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

PS C:\Users\maste>
```

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

```
PS C:\Users\maste> 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=118ms TTL=50
Respuesta desde 77.68.126.20: bytes=32 tiempo=117ms TTL=50
Respuesta desde 77.68.126.20: bytes=32 tiempo=118ms TTL=50
Respuesta desde 77.68.126.20: bytes=32 tiempo=122ms TTL=50

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 = 117ms, Máximo = 122ms, Media = 118ms
PS C:\Users\maste>
```

7.- Obtener la ayuda del comando netstat

```
PS C:\Users\maste> 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.
```

8.- Mostrar todas las conexiones y puertos de escucha

```
PS C:\Users\maste> netstat -a

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    0.0.0.0:80             LAPTOP-0K95KC9I:0      LISTENING
  TCP    0.0.0.0:135            LAPTOP-0K95KC9I:0      LISTENING
  TCP    0.0.0.0:443            LAPTOP-0K95KC9I:0      LISTENING
  TCP    0.0.0.0:445            LAPTOP-0K95KC9I:0      LISTENING
  TCP    0.0.0.0:5040           LAPTOP-0K95KC9I:0      LISTENING
  TCP    0.0.0.0:8733           LAPTOP-0K95KC9I:0      LISTENING
  TCP    0.0.0.0:49664          LAPTOP-0K95KC9I:0      LISTENING
  TCP    0.0.0.0:49665          LAPTOP-0K95KC9I:0      LISTENING
  TCP    0.0.0.0:49666          LAPTOP-0K95KC9I:0      LISTENING
  TCP    0.0.0.0:49667          LAPTOP-0K95KC9I:0      LISTENING
  TCP    0.0.0.0:49668          LAPTOP-0K95KC9I:0      LISTENING
  TCP    0.0.0.0:49697          LAPTOP-0K95KC9I:0      LISTENING
  TCP    127.0.0.1:1434         LAPTOP-0K95KC9I:0      LISTENING
  TCP    127.0.0.1:8588         LAPTOP-0K95KC9I:0      LISTENING
  TCP    127.0.0.1:8588         cuevana:49712          ESTABLISHED
  TCP    127.0.0.1:9080         LAPTOP-0K95KC9I:0      LISTENING
  TCP    127.0.0.1:12025        LAPTOP-0K95KC9I:0      LISTENING
  TCP    127.0.0.1:12110        LAPTOP-0K95KC9I:0      LISTENING
  TCP    127.0.0.1:12119        LAPTOP-0K95KC9I:0      LISTENING
  TCP    127.0.0.1:12143        LAPTOP-0K95KC9I:0      LISTENING
  TCP    127.0.0.1:12465        LAPTOP-0K95KC9I:0      LISTENING
  TCP    127.0.0.1:12563        LAPTOP-0K95KC9I:0      LISTENING
  TCP    127.0.0.1:12993        LAPTOP-0K95KC9I:0      LISTENING
  TCP    127.0.0.1:12995        LAPTOP-0K95KC9I:0      LISTENING
  TCP    127.0.0.1:27275        LAPTOP-0K95KC9I:0      LISTENING
  TCP    127.0.0.1:49712        cuevana:8588           ESTABLISHED
  TCP    172.16.129.152:139     LAPTOP-0K95KC9I:0      LISTENING
  TCP    172.16.129.152:54125   52.159.126.152:https   ESTABLISHED
  TCP    172.16.129.152:54127   whatsapp-cdn-shv-02-mia3:https  ESTABLISHED
  TCP    172.16.129.152:54132   yx-in-f188:5228        ESTABLISHED
  TCP    172.16.129.152:54137   47:https               ESTABLISHED
  TCP    172.16.129.152:54139   server-108-157-162-11:https  ESTABLISHED
```

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

```
  TCP    172.16.129.152:56486   server-18-64-172-237:https  ESTABLISHED
PS C:\Users\maste> netstat -n

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    127.0.0.1:8588         127.0.0.1:49712        ESTABLISHED
  TCP    127.0.0.1:49712        127.0.0.1:8588         ESTABLISHED
  TCP    172.16.129.152:54125   52.159.126.152:443     ESTABLISHED
  TCP    172.16.129.152:54127   157.240.14.52:443      ESTABLISHED
  TCP    172.16.129.152:54132   64.233.177.188:5228    ESTABLISHED
  TCP    172.16.129.152:54137   34.89.155.47:443       ESTABLISHED
  TCP    172.16.129.152:54139   108.157.162.11:443     ESTABLISHED
  TCP    172.16.129.152:54140   13.249.96.211:443      ESTABLISHED
  TCP    172.16.129.152:54143   34.149.50.64:443       ESTABLISHED
  TCP    172.16.129.152:54149   34.120.63.153:443      ESTABLISHED
  TCP    172.16.129.152:54151   172.67.21.232:443      ESTABLISHED
  TCP    172.16.129.152:54152   104.18.3.114:443       ESTABLISHED
  TCP    172.16.129.152:54153   104.18.27.193:443      ESTABLISHED
  TCP    172.16.129.152:54154   44.214.115.20:443      ESTABLISHED
  TCP    172.16.129.152:54156   104.22.34.123:443      ESTABLISHED
  TCP    172.16.129.152:54157   104.36.115.111:443     ESTABLISHED
  TCP    172.16.129.152:54158   64.233.185.157:443     ESTABLISHED
  TCP    172.16.129.152:54159   64.233.177.154:443     ESTABLISHED
  TCP    172.16.129.152:54160   52.94.231.7:443        ESTABLISHED
  TCP    172.16.129.152:54161   35.241.34.106:443      ESTABLISHED
  TCP    172.16.129.152:54162   216.239.38.181:443     ESTABLISHED
  TCP    172.16.129.152:54163   64.233.176.94:443      ESTABLISHED
  TCP    172.16.129.152:54164   64.233.177.154:443     ESTABLISHED
  TCP    172.16.129.152:54167   142.250.105.157:443    ESTABLISHED
  TCP    172.16.129.152:54177   108.177.122.154:443    ESTABLISHED
  TCP    172.16.129.152:54181   64.233.185.157:443     ESTABLISHED
  TCP    172.16.129.152:55976   35.190.90.30:443       ESTABLISHED
  TCP    172.16.129.152:56160   23.48.105.214:443      CLOSE_WAIT
  TCP    172.16.129.152:56371   140.82.113.25:443      ESTABLISHED
  TCP    172.16.129.152:56481   162.248.18.31:443      ESTABLISHED
  TCP    172.16.129.152:56483   8.28.7.95:443          ESTABLISHED
  TCP    172.16.129.152:56486   18.64.172.237:443      ESTABLISHED
  TCP    172.16.129.152:56487   209.54.181.45:443      ESTABLISHED
  TCP    172.16.129.152:56514   35.241.34.106:443      ESTABLISHED
  TCP    172.16.129.152:56522   23.204.161.157:443     ESTABLISHED
  TCP    172.16.129.152:56524   23.204.161.157:443     ESTABLISHED
  TCP    172.16.129.152:56526   18.64.174.108:443      ESTABLISHED
  TCP    172.16.129.152:56528   72.246.252.29:443      ESTABLISHED
  TCP    172.16.129.152:56529   72.246.252.29:443      ESTABLISHED
  TCP    172.16.129.152:56530   72.246.252.29:443      ESTABLISHED
  TCP    172.16.129.152:56531   72.246.252.29:443      ESTABLISHED
  TCP    172.16.129.152:56558   64.233.177.103:443     TIME_WAIT
  TCP    172.16.129.152:56565   34.111.113.62:443      ESTABLISHED
  TCP    172.16.129.152:56569   104.18.25.173:443      ESTABLISHED
  TCP    172.16.129.152:56586   8.43.72.42:443         TIME_WAIT
  TCP    172.16.129.152:56594   162.159.135.234:443    ESTABLISHED
  TCP    172.16.129.152:56609   142.250.9.148:443      ESTABLISHED
  TCP    172.16.129.152:56610   172.253.124.94:443     ESTABLISHED
  TCP    172.16.129.152:56614   23.47.64.50:443        ESTABLISHED
  TCP    172.16.129.152:56622   23.212.248.20:443      ESTABLISHED
  TCP    172.16.129.152:56623   204.79.197.203:443     TIME_WAIT
  TCP    172.16.129.152:56625   204.79.197.203:443     ESTABLISHED
  TCP    172.16.129.152:56631   40.126.23.97:443       TIME_WAIT
  TCP    172.16.129.152:56632   13.107.42.12:443       TIME_WAIT
  TCP    172.16.129.152:56633   157.240.14.52:443      ESTABLISHED
  TCP    172.16.129.152:56634   142.250.9.105:443      CLOSE_WAIT
  TCP    172.16.129.152:56635   31.13.67.52:443        ESTABLISHED
  TCP    172.16.129.152:56636   23.56.6.57:443         ESTABLISHED
PS C:\Users\maste>
```

10.- Mostrar las conexiones TCP

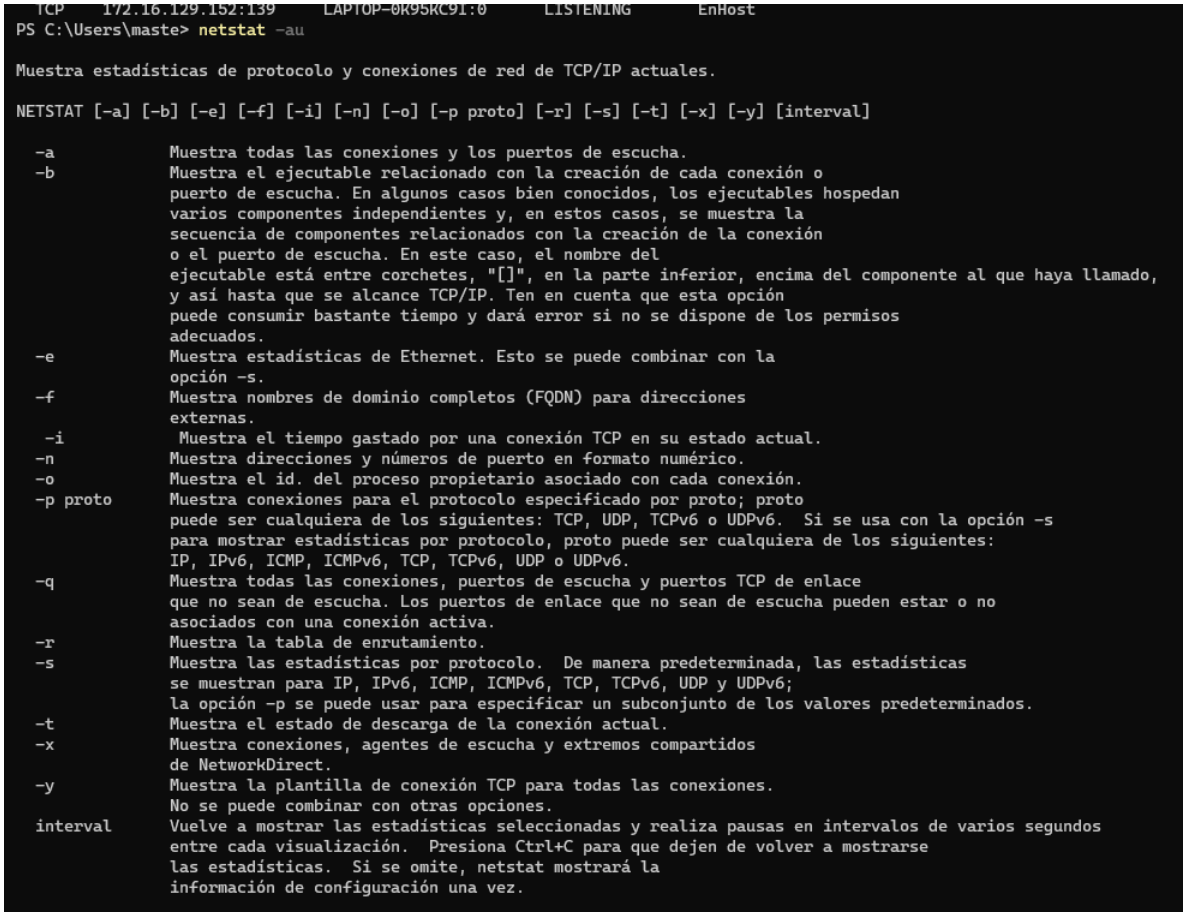
```
  TCP    172.16.129.152:56636   23.56.6.57:443         ESTABLISHED
PS C:\Users\maste> netstat -at

Conexiones activas

  Proto  Dirección local          Dirección remota        Estado
           Estado de descarga

  TCP    0.0.0.0:80             LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    0.0.0.0:135            LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    0.0.0.0:443            LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    0.0.0.0:445            LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    0.0.0.0:5040           LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    0.0.0.0:8733           LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    0.0.0.0:49664          LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    0.0.0.0:49665          LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    0.0.0.0:49666          LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    0.0.0.0:49667          LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    0.0.0.0:49668          LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    0.0.0.0:49697          LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    127.0.0.1:1434         LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    127.0.0.1:8588         LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    127.0.0.1:8588         cuevana:49712          ESTABLISHED     EnHost
  TCP    127.0.0.1:9080         LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    127.0.0.1:12025        LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    127.0.0.1:12110        LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    127.0.0.1:12119        LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    127.0.0.1:12143        LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    127.0.0.1:12465        LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    127.0.0.1:12563        LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    127.0.0.1:12993        LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    127.0.0.1:12995        LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    127.0.0.1:27275        LAPTOP-0K95KC9I:0      LISTENING       EnHost
  TCP    127.0.0.1:49712        cuevana:8588           ESTABLISHED     EnHost
  TCP    172.16.129.152:139     LAPTOP-0K95KC9I:0      LISTENING       EnHost
PS C:\Users\maste>
```

11.- Mostrar las conexiones UDP



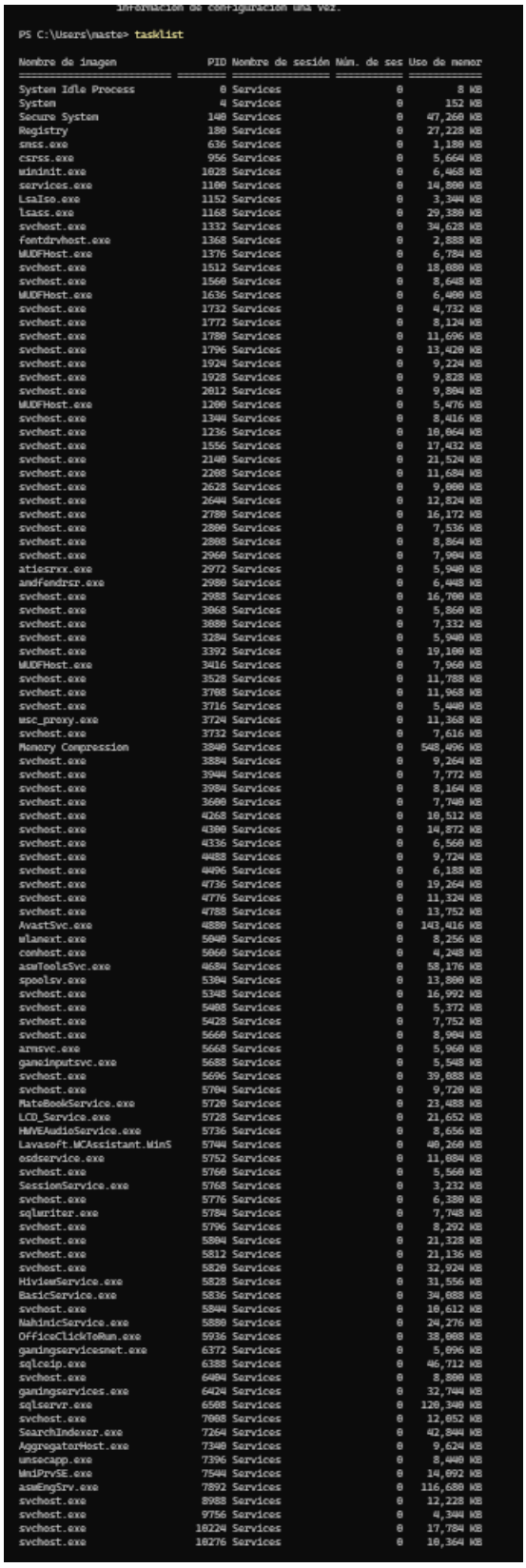
```
  TCP    172.16.129.152:139     LAPTOP-0R95RC91:0      LISTENING       EnHost
PS C:\Users\maste> netstat -au

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.
  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.
```

12.- Utilizar el comando tasklist



```
Información de configuración del VGA V02:

PS C:\Users\maste> 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        152 KB
Secure System                 140 Services                   0     47,260 KB
Registry                      180 Services                   0     27,228 KB
smss.exe                      636 Services                   0      1,180 KB
csrss.exe                     956 Services                   0      5,664 KB
wininit.exe                  1028 Services                   0      6,468 KB
services.exe                 1100 Services                   0     14,880 KB
LsaIso.exe                   1152 Services                   0      3,344 KB
lsass.exe                    1168 Services                   0     29,380 KB
svchost.exe                  1332 Services                   0     34,628 KB
fontdrvhost.exe              1368 Services                   0      2,888 KB
WUDFHost.exe                 1376 Services                   0      6,784 KB
svchost.exe                  1512 Services                   0     18,880 KB
svchost.exe                  1560 Services                   0      8,648 KB
WUDFHost.exe                 1636 Services                   0      6,400 KB
svchost.exe                  1732 Services                   0      4,732 KB
svchost.exe                  1772 Services                   0      8,124 KB
svchost.exe                  1780 Services                   0     11,696 KB
svchost.exe                  1796 Services                   0     13,420 KB
svchost.exe                  1924 Services                   0      9,224 KB
svchost.exe                  1928 Services                   0      9,828 KB
svchost.exe                  2012 Services                   0      9,804 KB
WUDFHost.exe                 1200 Services                   0      5,476 KB
svchost.exe                  1344 Services                   0      8,416 KB
svchost.exe                  1236 Services                   0     10,864 KB
svchost.exe                  1556 Services                   0     17,432 KB
svchost.exe                  2140 Services                   0     21,524 KB
svchost.exe                  2208 Services                   0     11,684 KB
svchost.exe                  2628 Services                   0      9,000 KB
svchost.exe                  2644 Services                   0     12,824 KB
svchost.exe                  2780 Services                   0     16,172 KB
svchost.exe                  2800 Services                   0      7,536 KB
svchost.exe                  2808 Services                   0      8,864 KB
svchost.exe                  2960 Services                   0      7,904 KB
atiesrxx.exe                 2972 Services                   0      5,940 KB
amdfendrsr.exe               2980 Services                   0      6,448 KB
svchost.exe                  2988 Services                   0     16,700 KB
svchost.exe                  3068 Services                   0      5,860 KB
svchost.exe                  3080 Services                   0      7,332 KB
svchost.exe                  3284 Services                   0      5,940 KB
svchost.exe                  3392 Services                   0     19,100 KB
WUDFHost.exe                 3416 Services                   0      7,960 KB
svchost.exe                  3528 Services                   0     11,788 KB
svchost.exe                  3708 Services                   0     11,968 KB
svchost.exe                  3716 Services                   0      5,448 KB
wsc_proxy.exe                3724 Services                   0     11,368 KB
svchost.exe                  3732 Services                   0      7,616 KB
Memory Compression           3840 Services                   0    548,496 KB
svchost.exe                  3884 Services                   0      9,264 KB
svchost.exe                  3944 Services                   0      7,772 KB
svchost.exe                  3984 Services                   0      8,164 KB
svchost.exe                  3600 Services                   0      7,740 KB
svchost.exe                  4268 Services                   0     10,512 KB
svchost.exe                  4300 Services                   0     14,872 KB
svchost.exe                  4336 Services                   0      6,560 KB
svchost.exe                  4488 Services                   0      9,724 KB
svchost.exe                  4496 Services                   0      6,188 KB
svchost.exe                  4736 Services                   0     19,264 KB
svchost.exe                  4776 Services                   0     11,324 KB
svchost.exe                  4788 Services                   0     13,752 KB
AvastSvc.exe                 4880 Services                   0    143,416 KB
wlanext.exe                  5040 Services                   0      8,256 KB
conhost.exe                  5060 Services                   0      4,248 KB
asmToolsSvc.exe              4684 Services                   0     58,176 KB
spoolsv.exe                  5304 Services                   0     13,800 KB
svchost.exe                  5348 Services                   0     16,992 KB
svchost.exe                  5408 Services                   0      5,372 KB
svchost.exe                  5428 Services                   0      7,752 KB
svchost.exe                  5660 Services                   0      8,904 KB
armsvc.exe                   5668 Services                   0      5,960 KB
gameinputsvc.exe             5688 Services                   0      5,548 KB
svchost.exe                  5696 Services                   0     39,888 KB
svchost.exe                  5704 Services                   0      9,720 KB
MateBookService.exe          5720 Services                   0     23,488 KB
LCD_Service.exe              5728 Services                   0     21,652 KB
HMVEAudioService.exe         5736 Services                   0      8,656 KB
Lavasoft.WCAssistant.WinS    5744 Services                   0     40,260 KB
osdservice.exe               5752 Services                   0     11,884 KB
svchost.exe                  5760 Services                   0      5,560 KB
SessionService.exe           5768 Services                   0      3,232 KB
svchost.exe                  5776 Services                   0      6,380 KB
sqlwriter.exe                5784 Services                   0      7,748 KB
svchost.exe                  5796 Services                   0      8,292 KB
svchost.exe                  5804 Services                   0     21,328 KB
svchost.exe                  5812 Services                   0     21,136 KB
svchost.exe                  5820 Services                   0     32,924 KB
HiviewService.exe            5828 Services                   0     31,556 KB
BasicService.exe             5836 Services                   0     34,088 KB
svchost.exe                  5844 Services                   0     10,612 KB
NahimicService.exe           5880 Services                   0     24,276 KB
OfficeClickToRun.exe         5936 Services                   0     38,008 KB
gamingservicesnet.exe        6372 Services                   0      5,096 KB
sqlceip.exe                  6388 Services                   0     46,712 KB
svchost.exe                  6404 Services                   0      8,800 KB
gamingservices.exe           6424 Services                   0     32,744 KB
sqlservr.exe                 6508 Services                   0    120,340 KB
svchost.exe                  7008 Services                   0     12,052 KB
SearchIndexer.exe            7264 Services                   0     42,844 KB
AggregatorHost.exe           7340 Services                   0      9,624 KB
unsecapp.exe                 7396 Services                   0      8,440 KB
WmiPrvSE.exe                 7544 Services                   0     14,092 KB
asmEngSrv.exe                7892 Services                   0    116,680 KB
svchost.exe                  8988 Services                   0     12,228 KB
svchost.exe                  9756 Services                   0      4,344 KB
svchost.exe                 10224 Services                   0     17,784 KB
svchost.exe                 10276 Services                   0     10,364 KB
```

13.- Utilizar el comando taskkill

```
tasklist.exe                  10752 Console
PS C:\Users\maste> taskkill /F /PID 10624
Correcto: se terminó el proceso con PID 10624.
PS C:\Users\maste>
```

14.- Utilizar el comando tracet

```
Correcto: se terminó el proceso con PID 10624.
PS C:\Users\maste> tracert google.com

Traza a la dirección google.com [64.233.177.139]
sobre un máximo de 30 saltos:

  1    <1 ms     2 ms     1 ms  172.16.128.1
  2     7 ms     1 ms     1 ms  192.168.109.1
  3     6 ms     6 ms     4 ms  fixed-187-188-58-130.totalplay.net [187.188.58.130]
  4     5 ms     8 ms     5 ms  10.180.58.1
  5   220 ms    47 ms    39 ms  72.14.242.148
  6    38 ms    25 ms    40 ms  209.85.253.117
PS C:\Users\maste>
```

15.- Utilizar el comando ARP

```
  6    38 ms    25 ms    40 ms  209.85.253.117
PS C:\Users\maste> arp -a

Interfaz: 172.16.129.152 --- 0x5
  Dirección de Internet          Dirección física      Tipo
  172.16.128.1          00-0c-e6-f5-d8-73     dinámico
  172.16.128.3          dc-41-a9-67-bc-54     dinámico
  172.16.128.74         5c-fb-3a-69-44-ef     dinámico
  172.16.143.255        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 --- 0x10
  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
PS C:\Users\maste>
```

B) Contesta con tus propias palabras las siguientes preguntas:

1.- Para qué sirve el comando ping?

El comando ping se utiliza para verificar la conectividad entre dos dispositivos en una red. Envía paquetes de datos a una dirección IP específica y espera una respuesta

2.- Para qué sirve el comando nslookup?

El comando nslookup se emplea para consultar servidores de nombres de dominio (DNS) y obtener información sobre direcciones IP asociadas a nombres de dominio y viceversa. Es útil para resolver problemas de resolución de nombres o para verificar la configuración DNS de un sistema.

3.- Para qué sirve el comando netstat?

El comando netstat proporciona información detallada sobre las conexiones de red activas, puertos abiertos y estadísticas de red en un sistema. Esto incluye información sobre direcciones IP locales y remotas, puertos y protocolos utilizados en las conexiones

4.-Para qué sirve el comando tasklist?

El comando tasklist muestra una lista de los procesos en ejecución en un sistema Windows. Proporciona información como el ID del proceso (PID), nombre del proceso y el uso de recursos asociado a cada proceso.

5.- Para qué sirve el comando taskill?

El comando taskkill se utiliza para finalizar o terminar un proceso en un sistema Windows. Puede detener un proceso específico utilizando su ID de proceso (PID) o el nombre del proceso.

6.- Para qué sirve el comando tracent?

tracert, es un comando que se utiliza para rastrear la ruta que toma un paquete de datos desde tu computadora hasta una dirección IP de destino, lo que ayuda a identificar los puntos de fallo o congestión en la red.

7.- Como ayudan los primeros tres con ambos para detectar problemas en la red?

-Ping verifica la conectividad básica entre dos dispositivos, lo que ayuda a determinar si hay un problema de comunicación entre ellos.

-Nslookup permite verificar si la resolución de nombres está funcionando correctamente al traducir nombres de dominio a direcciones IP y viceversa.

-Netstat proporciona una visión detallada de las conexiones activas, lo que puede revelar si hay problemas de congestión, puertos bloqueados o conexiones inesperadas.

C) Investigar los siguientes comandos y anotar ejemplos prácticos:

Atmadm

Este comando es utilizado para administrar adaptadores de modo de transferencia asíncrona (ATM) en sistemas operativos Windows. Puede usarse para mostrar información y configurar propiedades de interfaces ATM.

Bitsadmin

Este es un administrador de transferencia inteligente en segundo plano que permite la administración de trabajos de transferencia de archivos desde la línea de comandos. Es útil para descargar o cargar archivos desde o hacia un servidor.

Cmstp

Este comando es utilizado para instalar o desinstalar perfiles de conexión en Windows. Puede ser útil en la configuración de conexiones de red.

ftp

El Protocolo de Transferencia de Archivos (FTP) es un protocolo estándar de Internet que se utiliza para transferir archivos entre computadoras. El comando ftp en la línea de comandos de Windows permite interactuar con servidores FTP.

Getmac

Este comando muestra la dirección MAC (Media Access Control) de un adaptador de red. La dirección MAC es un identificador único asignado a cada tarjeta de red.

Hostname

Este comando muestra o configura el nombre del host de un sistema. El nombre del host es una etiqueta que se asigna a una computadora para identificarla en una red.

Nbtstat

Es un comando que muestra estadísticas y conexiones actuales utilizando NetBIOS sobre TCP/IP. Puede ser útil para resolver problemas de conectividad en redes.

Net

El comando net es una herramienta multifuncional que permite realizar varias operaciones de red como mapeo de unidades, gestión de usuarios y grupos, entre otras.

net use

Este comando permite conectar o desconectar una computadora a una red compartida o una impresora.

Netsh

Es una herramienta de línea de comandos que proporciona un conjunto de comandos para configurar y diagnosticar varios aspectos de la red en sistemas Windows.

Pathping

Es una utilidad que combina las funcionalidades de ping y tracert. Proporciona información detallada sobre la ruta que un paquete de datos sigue para llegar a su destino.

Top

Aunque no es un comando nativo en Windows, en entornos UNIX y Linux, top muestra información en tiempo real sobre el uso del sistema y los procesos en ejecución

Texec

es un comando que se utiliza para ejecutar un programa o comando en un dispositivo de red remoto a través de una conexión de red.

Route

es un comando de línea de comandos que se utiliza para ver y manipular la tabla de enrutamiento en un sistema operativo. Permite al usuario ver cómo se dirigen los paquetes de datos en una red. route varían según el sistema operativo, pero generalmente se utilizan para agregar o eliminar rutas, así como para mostrar información sobre las rutas existentes.

tRsking

No hay un comando estándar llamado `tRsking` en la mayoría de los sistemas operativos comunes. Podría ser específico de un software o sistema particular.

Tsh

una abreviación que se refiere a un tipo de shell o entorno de línea de comandos específico. Sin más contexto, no puedo proporcionar detalles específicos sobre este comando.

Tomsetup

No hay un comando estándar llamado `tomsetup` en la mayoría de los sistemas operativos comunes. Podría ser específico de un software o sistema particular.

telnet

es un protocolo de red que se utiliza para establecer una conexión remota con otro sistema a través de la red. También es el nombre del comando que se utiliza para iniciar una sesión de telnet desde la línea de comandos.

Tftp

"Trivial File Transfer Protocol". Es un protocolo de transferencia de archivos simple, sin autenticación, que se utiliza principalmente para la transferencia de archivos entre dispositivos en una red local.