



TAREA #987

JOSE EDGARDO ROMERO EHUAN



[FECHA]

[NOMBRE DE LA COMPAÑÍA]

[Dirección de la compañía]

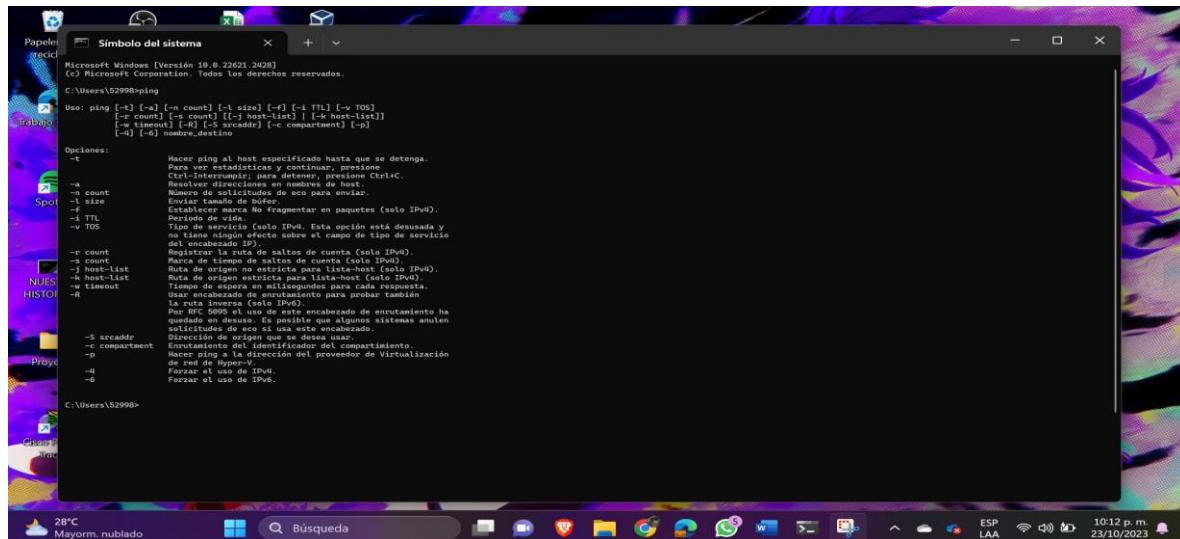
PRACTICA DE LABORATORIO

COMANDO EN MSDOS

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

MS-DOS

1." Obtener la ayuda del comando ping



```
Microsoft Windows [Versión 10.0.22623.2042]
(c) Microsoft Corporation. Todos los derechos reservados.

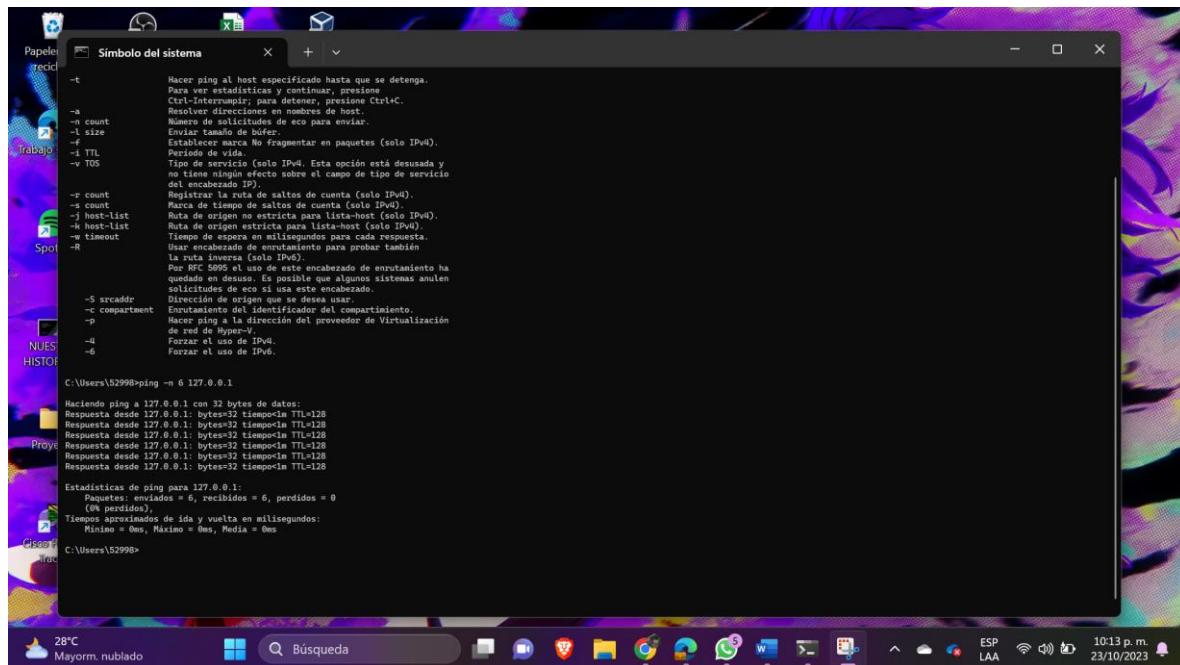
C:\Users\52998>ping /?

Uso: ping [-t] [-n count] [-l size] [-f] [-v TTL] [-w timeout]
        [-s=timeout] [-k scaddr] [-c compartment] [-r]
        [-q] [-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 salidas de eco para enviar.
  -l size     Envío de paquetes de tamaño.
  -f          Establecer marca No fragmentar en paquetes (solo IPv4).
  -v TTL      Período de vida.
  -w 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).
  -t host-list Direccionamiento de lista de host para enviar paquetes.
  -m timeout  Ruta de origen estricta para lista-host (solo IPv4).
  -k scaddr   Usar encabezado de enrutamiento para probar también
              la ruta inversa (solo IPv4).
  -c          Por defecto, el uso de este encabezado de enrutamiento ha
              quedado en desuso. Es posible que algunos sistemas anulen
              salidas de ping que usan este encabezado.
  -p          Dirección de origen que se desea usar.
  -c compartment  Enrutamiento del identificador del compartimiento.
  -q          Hacer ping a la dirección del proveedor de Virtualización
              de red de Hyper-V.
  -6          Forzar el uso de IPv6.
  -R          Forzar el uso de IPv4.

C:\Users\52998>
```

2.- Enviar un ping a 127.0.0.1 aplicando cualquier parámetro



```
Microsoft Windows [Versión 10.0.22623.2042]
(c) Microsoft Corporation. Todos los derechos reservados.

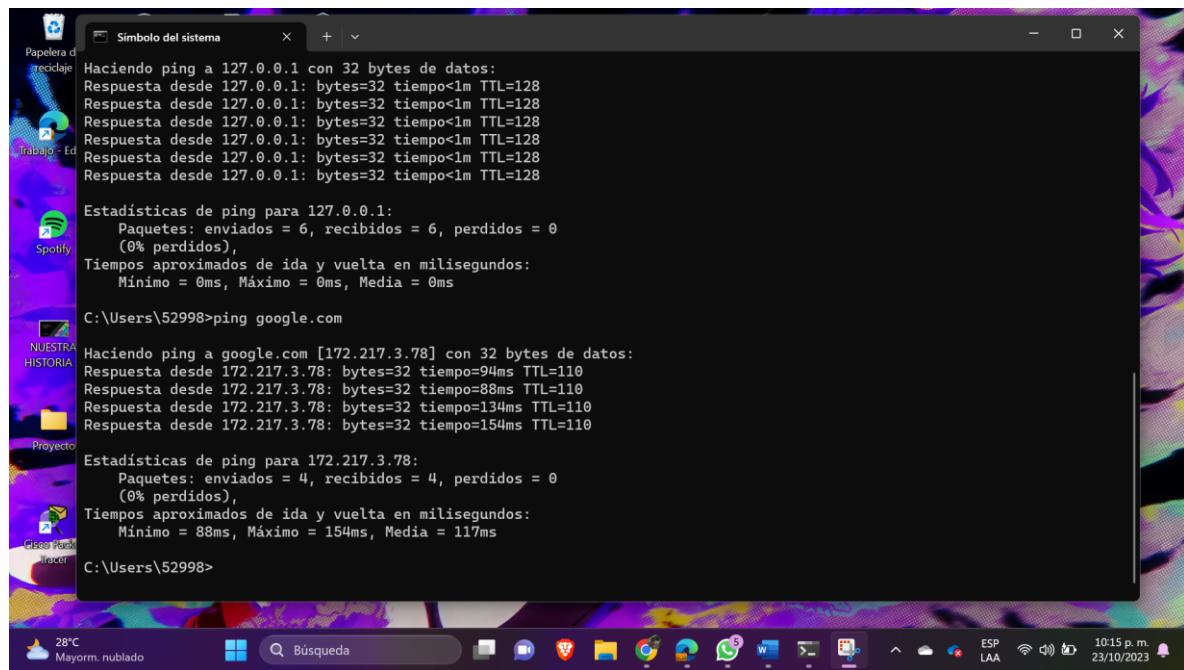
C:\Users\52998>ping -n 6 127.0.0.1

Haciendo ping a 127.0.0.1 con 32 bytes de datos:
Respuesta desde 127.0.0.1: bytes=32 tiempomin TTL=128

Estadísticas de ping para 127.0.0.1:
  Paquetes: enviados = 6, recibidos = 6, pendientes = 0
  (0% perdidos).
  Tiempos aproximados de ida y vuelta en milisegundos:
    Minimo = 0ms, Máximo = 0ms, Media = 0ms

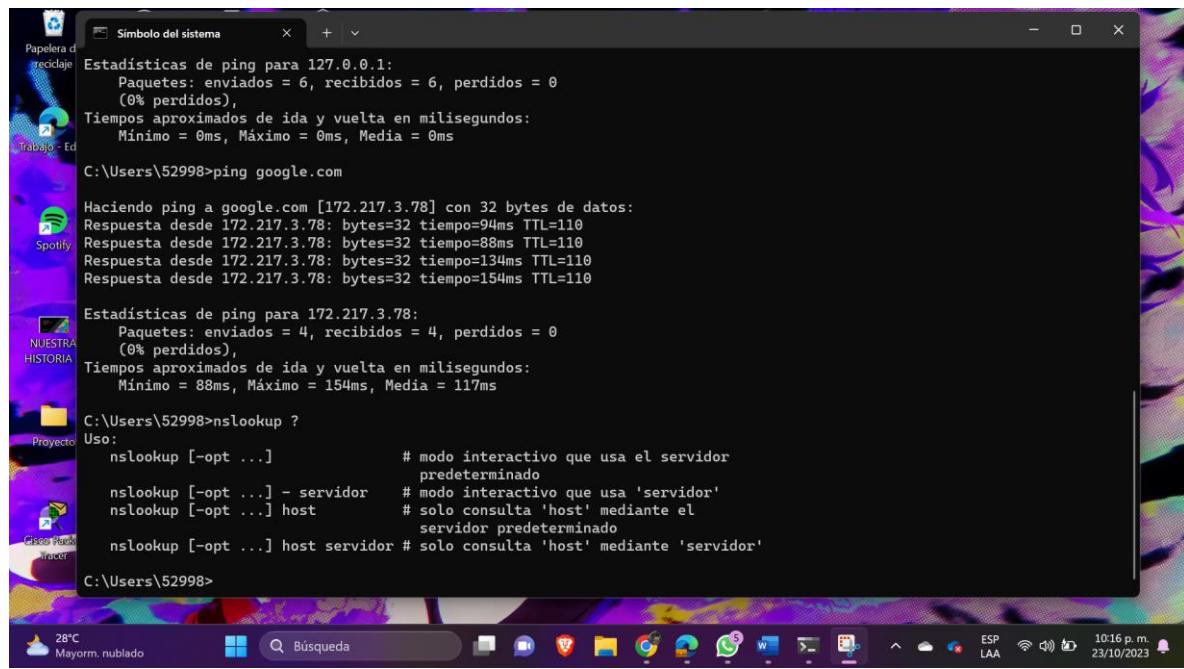
C:\Users\52998>
```

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



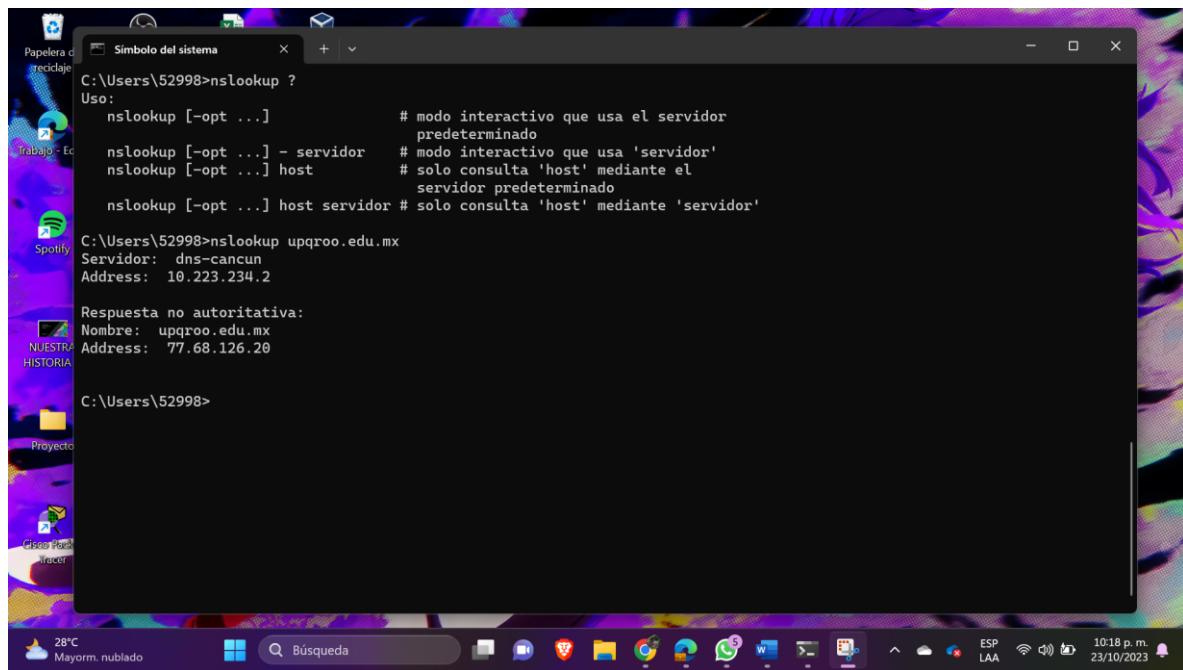
```
Haciendo ping a 127.0.0.1 con 32 bytes de datos:  
Respuesta desde 127.0.0.1: bytes=32 tiempo<1ms TTL=128  
  
Estadísticas de ping para 127.0.0.1:  
Paquetes: enviados = 6, recibidos = 6, perdidos = 0  
(0% perdidos),  
Tiempos aproximados de ida y vuelta en milisegundos:  
Mínimo = 0ms, Máximo = 0ms, Media = 0ms  
  
C:\Users\52998>ping google.com  
  
Haciendo ping a google.com [172.217.3.78] con 32 bytes de datos:  
Respuesta desde 172.217.3.78: bytes=32 tiempo=94ms TTL=110  
Respuesta desde 172.217.3.78: bytes=32 tiempo=88ms TTL=110  
Respuesta desde 172.217.3.78: bytes=32 tiempo=134ms TTL=110  
Respuesta desde 172.217.3.78: bytes=32 tiempo=154ms TTL=110  
  
Estadísticas de ping para 172.217.3.78:  
Paquetes: enviados = 4, recibidos = 4, perdidos = 0  
(0% perdidos),  
Tiempos aproximados de ida y vuelta en milisegundos:  
Mínimo = 88ms, Máximo = 154ms, Media = 117ms  
  
C:\Users\52998>
```

4.- Obtener la ayuda del comando nslookup



```
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  
  
C:\Users\52998>ping google.com  
  
Haciendo ping a google.com [172.217.3.78] con 32 bytes de datos:  
Respuesta desde 172.217.3.78: bytes=32 tiempo=94ms TTL=110  
Respuesta desde 172.217.3.78: bytes=32 tiempo=88ms TTL=110  
Respuesta desde 172.217.3.78: bytes=32 tiempo=134ms TTL=110  
Respuesta desde 172.217.3.78: bytes=32 tiempo=154ms TTL=110  
  
Estadísticas de ping para 172.217.3.78:  
Paquetes: enviados = 4, recibidos = 4, perdidos = 0  
(0% perdidos),  
Tiempos aproximados de ida y vuelta en milisegundos:  
Mínimo = 88ms, Máximo = 154ms, Media = 117ms  
  
C:\Users\52998>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'  
  
C:\Users\52998>
```

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



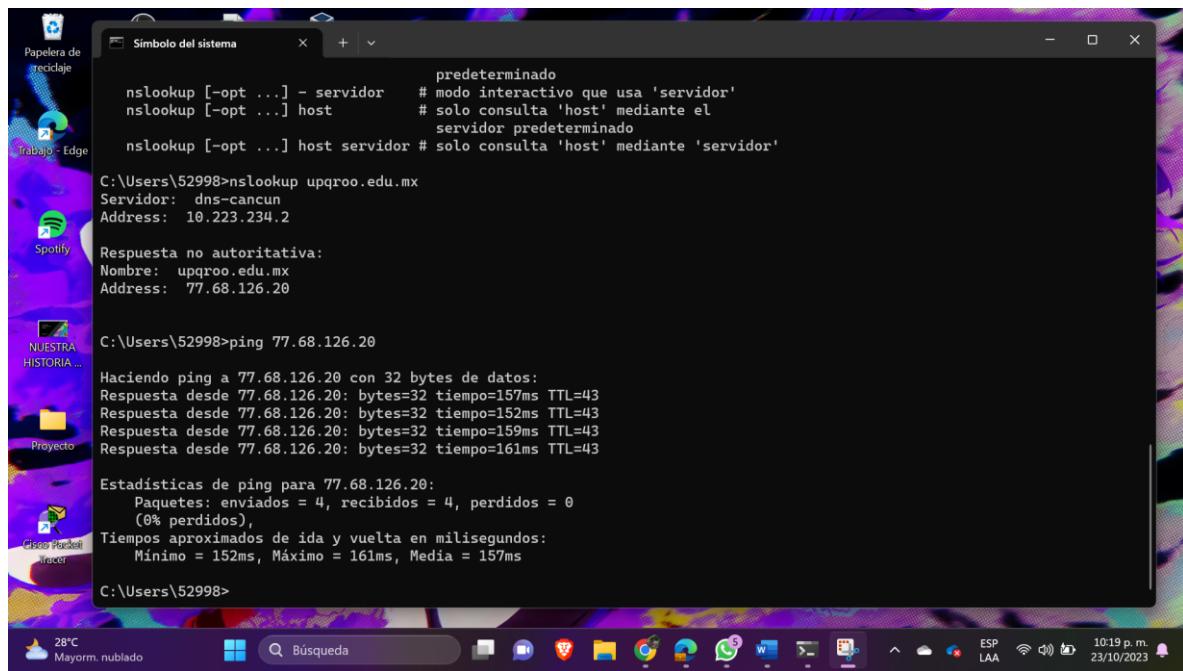
```
C:\Users\52998>nslookup ?
Usa:
  nslookup [-opt ...]          # modo interactivo que usa el servidor
                                # predeterminado
  nslookup [-opt ...] - servidor # modo interactivo que usa 'servidor'
  nslookup [-opt ...] host      # solo consulta 'host' mediante el
                                # servidor predeterminado
  nslookup [-opt ...] host servidor # solo consulta 'host' mediante 'servidor'

C:\Users\52998>nslookup upqroo.edu.mx
Servidor: dns-cancun
Address: 10.223.234.2

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

C:\Users\52998>
```

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



```
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'

C:\Users\52998>nslookup upqroo.edu.mx
Servidor: dns-cancun
Address: 10.223.234.2

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

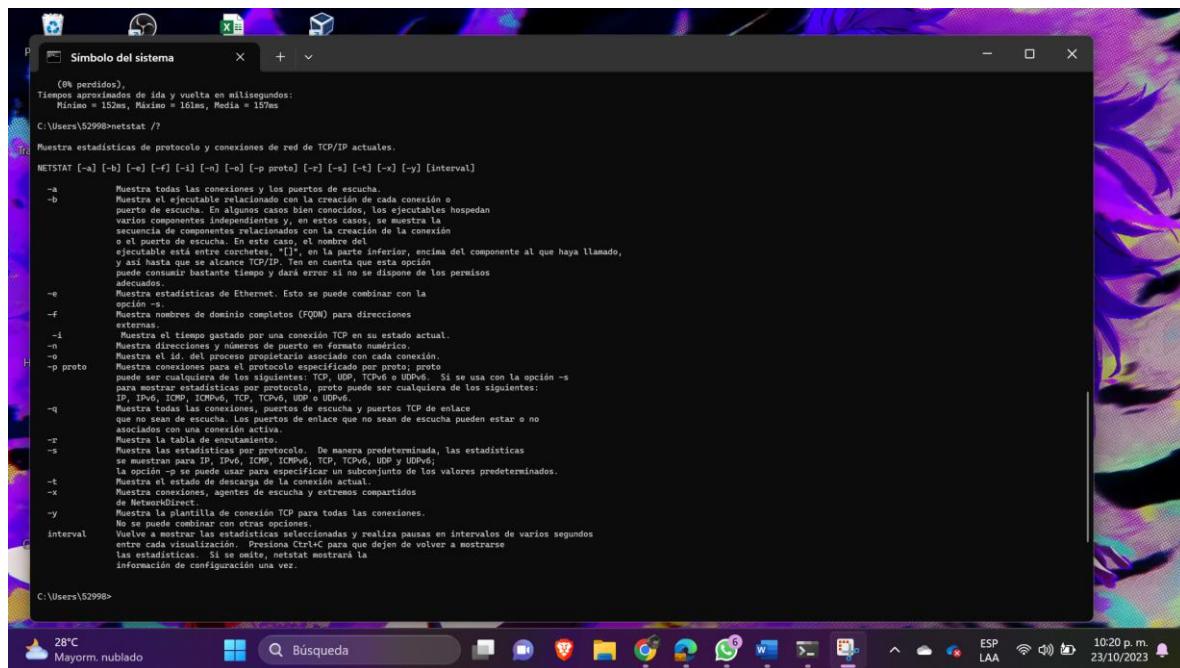
C:\Users\52998>ping 77.68.126.20

Haciendo ping a 77.68.126.20 con 32 bytes de datos:
Respuesta desde 77.68.126.20: bytes=32 tiempo=157ms TTL=43
Respuesta desde 77.68.126.20: bytes=32 tiempo=152ms TTL=43
Respuesta desde 77.68.126.20: bytes=32 tiempo=159ms TTL=43
Respuesta desde 77.68.126.20: bytes=32 tiempo=161ms TTL=43

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:
    Minimo = 152ms, Máximo = 161ms, Media = 157ms

C:\Users\52998>
```

7.- Obtener la ayuda del comando netstat



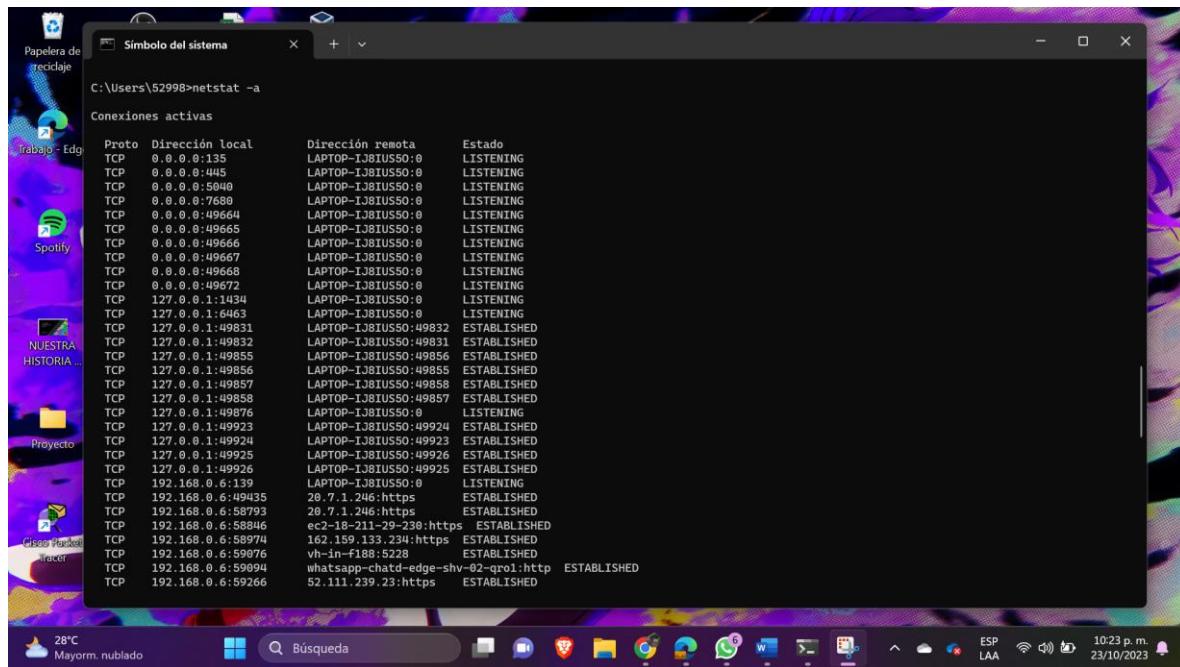
```
(0% perdidos).
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 152ms, Máximo = 161ms, Media = 157ms
C:\Users\52998>netstat /?

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
       proceso. Si se ejecutan más de dos procesos para un solo puerto, los ejecutables que
       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 de
       conexión aparecerá entre "()" y 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
       destino.
-i      Muestra el tiempo pasado por una conexión TCP en su estado actual.
-n      Muestra las 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. Los protocolos
       para los cuales es posible: TCP, UDP, ICMP, ICMPv6, TCPv6, UDP o UDPv6.
-q      Muestra el número de conexiones activas, 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 enruteamiento.
-s      Muestra estadísticas de 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 estadísticas, agentes de escucha y extremos compartidos
       de NetworkDirect.
-y      Muestra la plantilla de conexión TCP para todas las conexiones.
interval
       No se puede combinar con otras opciones. Se usan las selecciones 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.

C:\Users\52998>
```

8.- Mostrar todas las conexiones y puertos de escucha

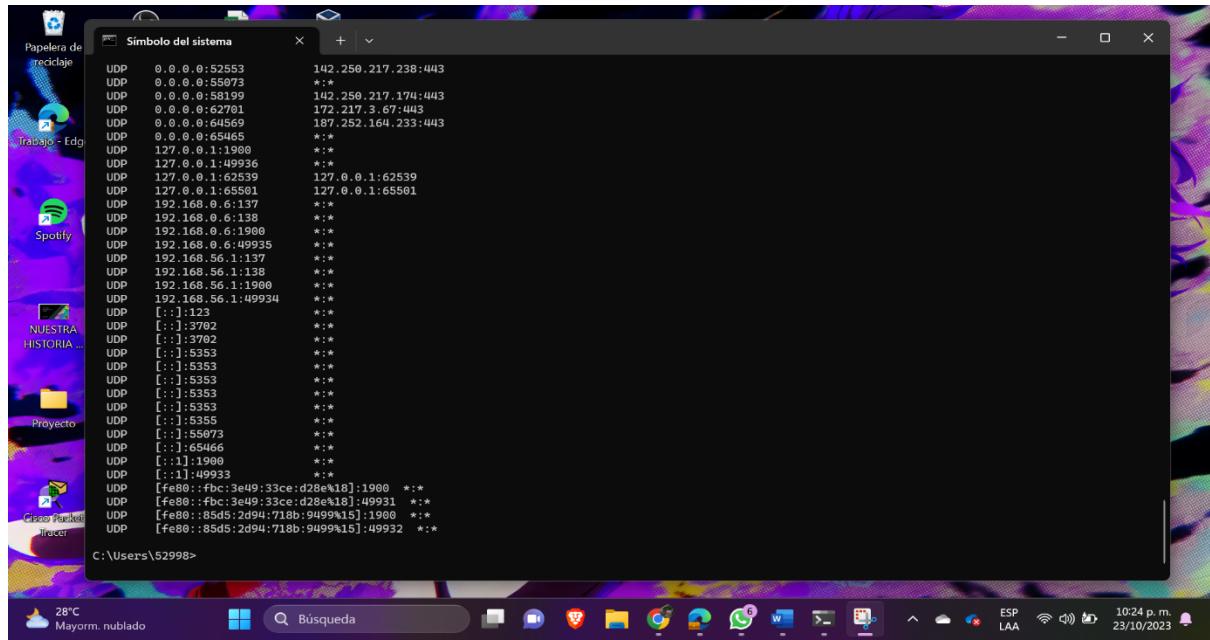


```
C:\Users\52998>netstat -a

Conexiones activas

  Proto  Dirección local        Dirección remota      Estado
  TCP    0.0.0.0:135           LAPTOP-IJBIUSS0:0      LISTENING
  TCP    0.0.0.0:445           LAPTOP-IJBIUSS0:0      LISTENING
  TCP    0.0.0.0:5040          LAPTOP-IJBIUSS0:0      LISTENING
  TCP    0.0.0.0:7680          LAPTOP-IJBIUSS0:0      LISTENING
  TCP    0.0.0.0:49664          LAPTOP-IJBIUSS0:0     LISTENING
  TCP    0.0.0.0:49665          LAPTOP-IJBIUSS0:0     LISTENING
  TCP    0.0.0.0:49666          LAPTOP-IJBIUSS0:0     LISTENING
  TCP    0.0.0.0:49667          LAPTOP-IJBIUSS0:0     LISTENING
  TCP    0.0.0.0:49668          LAPTOP-IJBIUSS0:0     LISTENING
  TCP    0.0.0.0:49672          LAPTOP-IJBIUSS0:0     LISTENING
  TCP    127.0.0.1:1434         LAPTOP-IJBIUSS0:0     LISTENING
  TCP    127.0.0.1:6463         LAPTOP-IJBIUSS0:0     LISTENING
  TCP    127.0.0.1:49831        LAPTOP-IJBIUSS0:49832 ESTABLISHED
  TCP    127.0.0.1:49832        LAPTOP-IJBIUSS0:49831 ESTABLISHED
  TCP    127.0.0.1:49855        LAPTOP-IJBIUSS0:49855 ESTABLISHED
  TCP    127.0.0.1:49857        LAPTOP-IJBIUSS0:49857 ESTABLISHED
  TCP    127.0.0.1:49858        LAPTOP-IJBIUSS0:49857 ESTABLISHED
  TCP    127.0.0.1:49876        LAPTOP-IJBIUSS0:0      LISTENING
  TCP    127.0.0.1:49923        LAPTOP-IJBIUSS0:49924 ESTABLISHED
  TCP    127.0.0.1:49924        LAPTOP-IJBIUSS0:49923 ESTABLISHED
  TCP    127.0.0.1:49925        LAPTOP-IJBIUSS0:49925 ESTABLISHED
  TCP    192.168.0.6:139         LAPTOP-IJBIUSS0:0      LISTENING
  TCP    192.168.0.6:49435       20.7.1.246:https   ESTABLISHED
  TCP    192.168.0.6:58793       20.7.1.246:https   ESTABLISHED
  TCP    192.168.0.6:58844       ec2-18-211-29-230:https ESTABLISHED
  TCP    192.168.0.6:58974       162.159.133.234:https ESTABLISHED
  TCP    192.168.0.6:59076       vh-in-f188:5228   ESTABLISHED
  TCP    192.168.0.6:59094       whatsapp-chatd-edge-shv-02-qrol:http ESTABLISHED
  TCP    192.168.0.6:59266       52.111.239.23:https ESTABLISHED

C:\Users\52998>
```



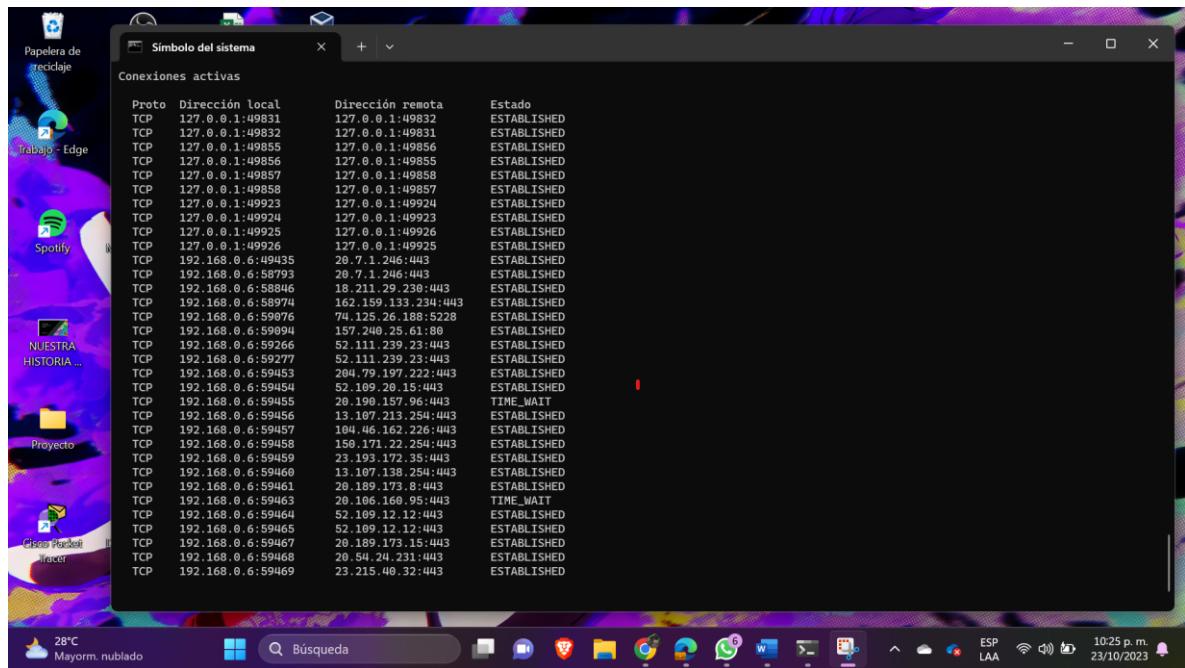
```
Symbolo del sistema
+ - x

C:\Users\52998> netstat -an | more

  UDP  0.0.0.0:52553      142.250.217.238:443
  UDP  0.0.0.0:55073      *:*
  UDP  0.0.0.0:58199      142.250.217.174:443
  UDP  0.0.0.0:62701      172.217.3.67:443
  UDP  0.0.0.0:64569      187.252.164.233:443
  UDP  0.0.0.0:65465      *:*
  UDP  127.0.0.1:1900     *:*
  UDP  127.0.0.1:49936    *:*
  UDP  127.0.0.1:62539    127.0.0.1:62539
  UDP  127.0.0.1:65501    127.0.0.1:65501
  UDP  192.168.0.6:137    *:*
  UDP  192.168.0.6:138    *:*
  UDP  192.168.0.6:1900   *:*
  UDP  192.168.0.6:49935   *:*
  UDP  192.168.56.1:137   *:*
  UDP  192.168.56.1:138   *:*
  UDP  192.168.56.1:1900  *:*
  UDP  192.168.56.1:49934  *:*
  UDP  [::]:123           *:*
  UDP  [::]:3762          *:*
  UDP  [::]:3902          *:*
  UDP  [::]:5353          *:*
  UDP  [::]:5355          *:*
  UDP  [::]:55073         *:*
  UDP  [::]:65464         *:*
  UDP  [::]:1900          *:*
  UDP  [::]:49933         *:*
  UDP  [fe80::fb0c:3e49%33ce::d28e%18]:1900  *:*
  UDP  [fe80::fb0c:3e49%33ce::d28e%18]:49931  *:*
  UDP  [fe80::85d5:2d94%718b:9499%15]:1900  *:*
  UDP  [fe80::85d5:2d94%718b:9499%15]:49932  *:*

C:\Users\52998>
```

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



```
Symbolo del sistema
+ - x

Conexiones activas

  Proto Dirección local      Dirección remota      Estado
  TCP  127.0.0.1:49831       127.0.0.1:49832      ESTABLISHED
  TCP  127.0.0.1:49832       127.0.0.1:49831      ESTABLISHED
  TCP  127.0.0.1:49855       127.0.0.1:49856      ESTABLISHED
  TCP  127.0.0.1:49856       127.0.0.1:49855      ESTABLISHED
  TCP  127.0.0.1:49857       127.0.0.1:49858      ESTABLISHED
  TCP  127.0.0.1:49858       127.0.0.1:49857      ESTABLISHED
  TCP  127.0.0.1:49823       127.0.0.1:49924      ESTABLISHED
  TCP  127.0.0.1:49824       127.0.0.1:49923      ESTABLISHED
  TCP  127.0.0.1:49925       127.0.0.1:49926      ESTABLISHED
  TCP  127.0.0.1:49926       127.0.0.1:49925      ESTABLISHED
  TCP  192.168.0.6:49435     20.7.1.246:443      ESTABLISHED
  TCP  192.168.0.6:58793     20.7.1.246:443      ESTABLISHED
  TCP  192.168.0.6:58846     18.211.29.230:443    ESTABLISHED
  TCP  192.168.0.6:58974     162.159.133.234:443  ESTABLISHED
  TCP  192.168.0.6:59076     74.125.26.188:5228  ESTABLISHED
  TCP  192.168.0.6:59094     157.240.25.61:80    ESTABLISHED
  TCP  192.168.0.6:59266     52.111.239.23:443   ESTABLISHED
  TCP  192.168.0.6:59277     52.111.239.23:443   ESTABLISHED
  TCP  192.168.0.6:59453     204.79.197.222:443  ESTABLISHED
  TCP  192.168.0.6:59454     52.169.20.15:443    ESTABLISHED
  TCP  192.168.0.6:59455     20.199.157.96:443   TIME_WAIT
  TCP  192.168.0.6:59456     13.167.213.254:443  ESTABLISHED
  TCP  192.168.0.6:59457     104.46.162.226:443  ESTABLISHED
  TCP  192.168.0.6:59458     159.171.22.254:443  ESTABLISHED
  TCP  192.168.0.6:59459     23.193.172.35:443   ESTABLISHED
  TCP  192.168.0.6:59460     13.167.138.254:443  ESTABLISHED
  TCP  192.168.0.6:59461     20.189.173.8:443    ESTABLISHED
  TCP  192.168.0.6:59463     20.166.168.95:443   TIME_WAIT
  TCP  192.168.0.6:59464     52.169.12.12:443   ESTABLISHED
  TCP  192.168.0.6:59465     52.169.12.12:443   ESTABLISHED
  TCP  192.168.0.6:59467     20.189.173.15:443  ESTABLISHED
  TCP  192.168.0.6:59468     20.94.24.231:443   ESTABLISHED
  TCP  192.168.0.6:59469     23.215.40.32:443   ESTABLISHED

C:\Users\52998>
```

10.- Mostrar las conexiones TCP

```
C:\Users\52998>netstat -at

Conexiones activas

Proto Dirección local         Dirección remota       Estado
Estado de descarga

TCP    0.0.0.0:125           LAPTOP-IJBTUSS0:0   LISTENING
TCP    0.0.0.0:445           LAPTOP-IJBTUSS0:0   LISTENING
TCP    0.0.0.0:5000          LAPTOP-IJBTUSS0:0   LISTENING
TCP    0.0.0.0:7680          LAPTOP-IJBTUSS0:0   LISTENING
TCP    0.0.0.0:49664         LAPTOP-IJBTUSS0:0   LISTENING
TCP    0.0.0.0:49665         LAPTOP-IJBTUSS0:0   LISTENING
TCP    0.0.0.0:49666         LAPTOP-IJBTUSS0:0   LISTENING
TCP    0.0.0.0:49667         LAPTOP-IJBTUSS0:0   LISTENING
TCP    0.0.0.0:49668         LAPTOP-IJBTUSS0:0   LISTENING
TCP    0.0.0.0:49672         LAPTOP-IJBTUSS0:0   LISTENING
TCP    127.0.0.1:1434        LAPTOP-IJBTUSS0:0   LISTENING
TCP    127.0.0.1:5463        LAPTOP-IJBTUSS0:0   LISTENING
TCP    127.0.0.1:49931       LAPTOP-IJBTUSS0:49931 ESTABLISHED
TCP    127.0.0.1:49932       LAPTOP-IJBTUSS0:49931 ESTABLISHED
TCP    127.0.0.1:49935       LAPTOP-IJBTUSS0:49935 ESTABLISHED
TCP    127.0.0.1:49956       LAPTOP-IJBTUSS0:49956 ESTABLISHED
TCP    127.0.0.1:49957       LAPTOP-IJBTUSS0:49957 ESTABLISHED
TCP    127.0.0.1:49958       LAPTOP-IJBTUSS0:49957 ESTABLISHED
TCP    127.0.0.1:49976       LAPTOP-IJBTUSS0:8    LISTENING
TCP    127.0.0.1:49923       LAPTOP-IJBTUSS0:49924 ESTABLISHED
TCP    127.0.0.1:49925       LAPTOP-IJBTUSS0:49925 ESTABLISHED
TCP    127.0.0.1:49926       LAPTOP-IJBTUSS0:49926 ESTABLISHED
TCP    192.168.0.6:139        LAPTOP-IJBTUSS0:0    LISTENING
TCP    192.168.0.6:49435      20.7.1.246:https  ESTABLISHED
```

11.- Mostrar las conexiones UDP

```
C:\Users\52998>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.
        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. En este caso, el nombre del ejecutable que se muestra
        ejecutable está entre comillas "[ ]", 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.
        Muestra direcciones y números de puerto en formato numérico.

-n      Muestra el id. del proceso propietario asociado con cada conexión.

-o      Muestra el nombre del ejecutable que ha iniciado la conexión; proto
        puede ser cualquiera de los siguientes: TCP, UDP, ICMPv6 o UDPv6. Si se usa con la opción -s
        para mostrar estadísticas por protocolo, proto puede ser cualquier uno 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 un dispositivo de red.

-r      Muestra la tabla de enruteamiento.

-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. Presione 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

```
C:\Users\52998>tasklist
Nombre de imagen          PID Nombre de sesión Núm. de ses Uso de memoria
System Idle Process        0 Services           0   8 KB
System                   4 Services           0   6,128 KB
Rundown                   112 Services         0   30,448 KB
smss.exe                  568 Services         0   976 KB
cssrss.exe                888 Services         0   5,796 KB
wininit.exe               972 Services         0   6,196 KB
cssrss.exe                998 Console          1   6,196 KB
win32k.exe                800 Services         1   11,040 KB
services.exe              968 Services         0   12,432 KB
lsass.exe                 1008 Services         0   27,588 KB
svchost.exe               1164 Services         0   33,924 KB
fontdrvhost.exe           1188 Console          1   7,312 KB
fontdrvhost.exe           1192 Services         0   3,928 KB
svchost.exe               1208 Services         0   18,768 KB
svchost.exe               1208 Services         0   7,768 KB
WUDFHost.exe              1408 Services         0   16,912 KB
svchost.exe               1408 Services         0   8,432 KB
dm.exe                    1488 Services         1   221,276 KB
svchost.exe               1512 Services         0   10,496 KB
svchost.exe               1608 Services         0   10,496 KB
svchost.exe               1668 Services         0   7,476 KB
svchost.exe               1708 Services         0   9,456 KB
svchost.exe               1752 Services         0   5,356 KB
svchost.exe               1768 Services         0   13,492 KB
IntelHDCPsvc.exe          184 Services          0   3,872 KB
svchost.exe               1908 Services         0   10,496 KB
svchost.exe               1928 Services         0   15,796 KB
2008 Services             0   8,156 KB
WUDFHost.exe              2032 Services         0   4,184 KB
svchost.exe               1288 Services         0   3,964 KB
svchost.exe               2188 Services         0   6,692 KB
svchost.exe               2188 Services         0   10,496 KB
svchost.exe               2192 Services         0   14,552 KB
svchost.exe               2296 Services         0   8,916 KB
2348 Services             0   5,132 KB
svchost.exe               2432 Services         0   13,916 KB
svchost.exe               2476 Services         0   8,868 KB
igfxCUEServiceN.exe      2488 Services         0   18,048 KB
svchost.exe               2632 Services         0   7,136 KB
```

```
C:\Users\52998>
Nombre de imagen          PID Nombre de sesión Núm. de ses Uso de memoria
svchost.exe               4832 Services         0   6,924 KB
svchost.exe               1008 Services         0   9,248 KB
svchost.exe               1088 Services         0   10,496 KB
svchost.exe               1272 Console          1   9,732 KB
svchost.exe               11924 Services        0   9,628 KB
chrome.exe                20972 Console         1   144,388 KB
chrome.exe                14456 Console         1   7,948 KB
chrome.exe                4688 Console          1   157,528 KB
chrome.exe                18080 Console         1   1,456 KB
chrome.exe                1292 Console          1   18,096 KB
chrome.exe                20276 Console         1   189,476 KB
chrome.exe                11928 Console         1   83,932 KB
chrome.exe                6988 Console          1   21,824 KB
chrome.exe                20748 Console         1   275,636 KB
chrome.exe                21312 Console         1   25,096 KB
msedge.exe                10652 Console         1   1,940 KB
msedge.exe                15672 Console         1   96,032 KB
msedge.exe                12720 Console         1   32,008 KB
msedge.exe                12948 Console         1   56,448 KB
msedge.exe                20832 Console         1   52,988 KB
msedge.exe                15484 Console         1   42,832 KB
msedge.exe                9848 Console          1   1,632 KB
RuntimeBroker.exe          15188 Console          1   21,480 KB
WINWORD.exe                17124 Console         1   295,088 KB
ai.exe                     2832 Console          1   23,888 KB
msedge.exe                6996 Console          1   24,840 KB
msedge.exe                8592 Console          1   18,096 KB
splmon4.exe                17680 Console         1   13,952 KB
svchost.exe               11868 Console         1   9,792 KB
cad.exe                     17108 Console         1   1,60 KB
conhost.exe               1688 Console          1   8,372 KB
OpenConsole.exe             17888 Console         1   15,544 KB
WindowsTerminal.exe       21208 Console         1   142,624 KB
RuntimeBroker.exe          9364 Console          1   10,748 KB
SnippingTool.exe           12916 Console         1   3,888 KB
blocklayerTaskHost.exe     13172 Console         1   1,416 KB
SearchProtocolHost.exe    1624 Console          1   8,696 KB
RuntimeBroker.exe          16292 Console         1   18,868 KB
SearchProtocolHost.exe    9684 Services          0   14,668 KB
SearchFilterHost.exe      19644 Services         0   9,052 KB
svchost.exe               15188 Services         0   7,620 KB
tasklist.exe                10400 Console          1   9,228 KB
WMIPrvSE.exe               10716 Services         0   9,944 KB
```

13.- Utilizar el comando taskkill

```
C:\Users\52998>taskkill /F /PID 16156
C:\Users\52998>taskkill
Error: Sintaxis incorrecta. No se han especificado los parámetros /FI ni /PID ni /IM.
Escriba "TASKKILL /?" para obtener más información de uso.

C:\Users\52998>taskkill /F /PID
Error: Sintaxis no válida. Se esperaba un valor para "/PID".
Escriba "TASKKILL /?" para su uso.

C:\Users\52998>taskkill /F /PID 1
Error: no se encontró el proceso "1".
ERROR: no se encontró el proceso "1".

C:\Users\52998>taskkill /F /PID 14124
Error: no se encontró el proceso "14124".
ERROR: no se encontró el proceso "14124".

C:\Users\52998>taskkill /F /PID 18716
Error: no se encontró el proceso "18716".
ERROR: no se encontró el proceso "18716".

C:\Users\52998>taskkill /F /PID 0
Error: no se pudo terminar el proceso con PID 0.
Motivo: Éste es un proceso crítico del sistema. Taskkill no puede terminar este proceso.

C:\Users\52998>taskkill /F /PID 112
Error: no se pudo terminar el proceso con PID 112.
Motivo: Acceso denegado.

C:\Users\52998>taskkill /F /PID 112
Error: no se pudo terminar el proceso con PID 112.
Motivo: Acceso denegado.

C:\Users\52998>
```

14.- Utilizar el comando tracert

```
C:\Users\52998>tracert
Error: Sintaxis no válida. Se esperaba un valor para "/PID".
Escriba "TASKKILL /?" para su uso.

C:\Users\52998>taskkill /F /PID 1
Error: no se encontró el proceso "1".
ERROR: no se encontró el proceso "1".

C:\Users\52998>taskkill /F /PID 14124
Error: no se encontró el proceso "14124".
ERROR: no se encontró el proceso "14124".

C:\Users\52998>taskkill /F /PID 18716
Error: no se encontró el proceso "18716".
ERROR: no se encontró el proceso "18716".

C:\Users\52998>taskkill /F /PID 0
Error: no se pudo terminar el proceso con PID 0.
Motivo: Éste es un proceso crítico del sistema. Taskkill no puede terminar este proceso.

C:\Users\52998>taskkill /F /PID 112
Error: no se pudo terminar el proceso con PID 112.
Motivo: Acceso denegado.

C:\Users\52998>taskkill /F /PID 112
Error: no se pudo terminar el proceso con PID 112.
Motivo: Acceso denegado.

C:\Users\52998>
C:\Users\52998>tracert google.com

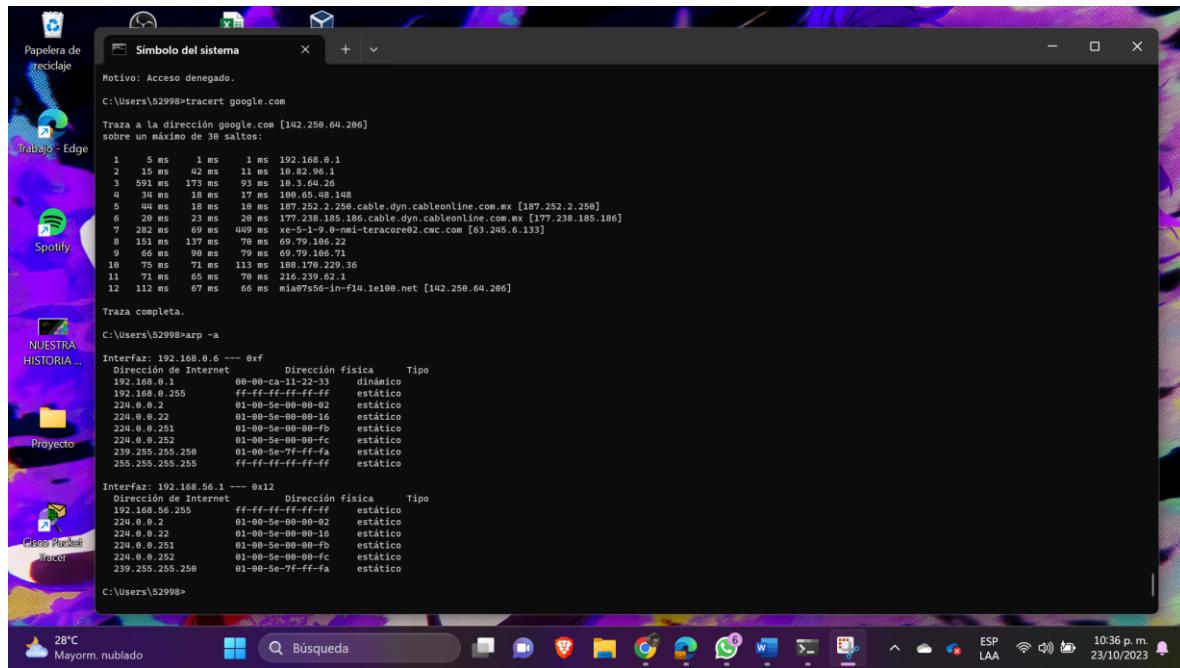
Traza a la dirección google.com [142.250.64.206]
sobre un máximo de 30 saltos:

 1  5 ms   1 ms   1 ms 192.168.0.1
 2  15 ms  42 ms  11 ms 10.82.96.1
 3  591 ms 173 ms  93 ms 10.3.64.26
 4  34 ms   8 ms   17 ms 10.3.65.104
 5  38 ms   8 ms   10 ms 109.232.2.258
 6  20 ms   23 ms   28 ms cable.dyn.cableonline.com.mx [107.252.2.256]
 7  282 ms  69 ms  409 ms xe-5-1-9.0-nml-teracore02.cwc.com [63.245.6.133]
 8  151 ms  137 ms   78 ms 69.79.106.22
 9  66 ms   98 ms   79 ms 69.79.106.71
10  75 ms   71 ms  113 ms 108.170.229.16
11  75 ms   68 ms   70 ms 216.239.62.1
12  112 ms   67 ms   66 ms mia07256-in-f14.1e100.net [142.250.64.206]

Traza completa.

C:\Users\52998>
```

15.- Utilizar el comando ARP



```
Motivo: Acceso denegado.

C:\Users\52998>tracert google.com [142.250.64.206]
sobre un máximo de 30 saltos:

  1   5 ms    1 ms    1 ms 192.168.0.1
  2   15 ms   42 ms   11 ms 10.82.96.1
  3   591 ms  173 ms   93 ms 10.82.96.250
  4   36 ms   17 ms   17 ms 100.65.1.148
  5   44 ms   18 ms   18 ms 187.252.2.258 cable.dyn.cableonline.com.mx [187.252.2.258]
  6   20 ms   23 ms   20 ms 177.238.185.186 cable.dyn.cableonline.com.mx [177.238.185.186]
  7   282 ms  69 ms  449 ms xe-5-1-9-0-mi-teracore02.cwc.com [63.245.6.133]
  8   151 ms  137 ms   70 ms 69.79.106.22
  9   66 ms   90 ms   79 ms 69.79.106.22
  10  73 ms   71 ms   79 ms 178.239.36
  11  71 ms   65 ms   78 ms 216.239.62.1
  12  112 ms  67 ms   66 ms mia@7556-in-f14.ie100.net [142.250.64.206]

Traza completa.

C:\Users\52998>arp -a

Interfaz: 192.168.0.6 ---- 0xf
Dirección de Internet   Dirección física   Tipo
192.168.0.1   00-0c-a1-11-22-22   dinámico
192.168.0.255 ff-ff-ff-ff-ff-ff   dinámico
224.0.0.2     01-00-5e-00-00-02   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
239.255.255.255 ff-ff-f7-ff-ff-ff   estático

Interfaz: 192.168.56.1 --- 0x12
Dirección de Internet   Dirección física   Tipo
192.168.56.255 ff-ff-ff-ff-ff-ff   estático
224.0.0.2     01-00-5e-00-00-02   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
239.255.255.255 ff-ff-f7-ff-ff-ff   estático

C:\Users\52998>
```

B) Contesta con tus propias palabras las siguientes preguntas:

1.- Para que sirve el comando ping?

El comando "ping" se utiliza para comprobar la conectividad entre dos dispositivos en una red. Envía paquetes de datos a una dirección IP o un nombre de dominio y espera respuestas para determinar si el dispositivo de destino está disponible y cuánto tiempo tarda en responder. Es una herramienta básica para diagnosticar problemas de conectividad de red.

2.- Para que sirve el comando nslookup?

El comando "nslookup" se utiliza para realizar consultas de resolución de nombres en servidores DNS (Domain Name System). Permite obtener información sobre la dirección IP asociada a un nombre de dominio o viceversa. Es útil para diagnosticar problemas de resolución de nombres y para verificar la configuración de servidores DNS.

3.- Para que sirve el comando netstat?

El comando "netstat" se utiliza para mostrar información sobre las conexiones de red activas, las tablas de enrutamiento y las estadísticas de red en un sistema. Puede ayudar a identificar qué puertos están en uso, las conexiones establecidas y las que escuchan, lo que es útil para diagnosticar problemas de red y seguridad.

4.- Para que sirve el comando tasklist?

El comando "tasklist" muestra una lista de los procesos en ejecución en un sistema Windows. Proporciona información detallada sobre cada proceso, incluyendo su nombre, ID de proceso y uso de recursos. Es útil para supervisar y administrar los procesos en un sistema.

5.- Para que sirve el comando taskkill?

El comando "taskkill" se utiliza para finalizar o detener procesos en un sistema Windows. Permite terminar procesos de manera forzada si es necesario, lo que puede ser útil para solucionar problemas cuando una aplicación no responde.

6.- Para que sirve el comando tracert?

El comando "tracert" (o "traceroute" en sistemas Unix) se utiliza para rastrear la ruta que toman los paquetes de datos desde un origen hasta un destino en una red. Muestra una lista de los saltos o enrutadores intermedios que los paquetes atraviesan en su camino hacia el destino. Es útil para diagnosticar la latencia o problemas de enrutamiento en la red.

7.- Como ayudan los primeros tres comandos para detectar problemas de red?

Los primeros tres comandos (ping, nslookup y netstat) ayudan a detectar problemas de red de la siguiente manera:

"Ping" permite verificar si un dispositivo remoto es accesible y si la latencia es aceptable.

"Nslookup" ayuda a confirmar la correcta resolución de nombres de dominio, identificando posibles problemas de DNS.

"Netstat" proporciona información sobre las conexiones de red y puertos en uso, lo que ayuda a identificar problemas de conectividad o seguridad en el sistema.

C) Investigar los siguientes comandos y anotar ejemplos prácticos: atm adm, bitsadmin, cmstp, ftp, getmac, hostname, nbtstat, net, net use, netsh, pathping, rcp, rexec, route, rpcping, rsh, tcmsetup, telnet, tftp

1. **atmadm:** Este comando se utiliza para administrar interfaces ATM (Asynchronous Transfer Mode) en Windows. Puede configurar y supervisar conexiones ATM. Por lo general, se utiliza en entornos de red especializados.

Ejemplo: Para mostrar información sobre las interfaces ATM en el sistema, puedes usar el comando:

```
atmadm show interfaces
```

2. **bitsadmin:** Bitsadmin es una herramienta de línea de comandos para administrar el servicio de transferencia inteligente en segundo plano (BITS), que se utiliza para la descarga y carga de archivos de forma asíncrona.

Ejemplo: Para crear una nueva tarea BITS para descargar un archivo, puedes usar el siguiente comando:

```
bitsadmin /create myDownloadJob bitsadmin /addfile myDownloadJob  
https://ejemplo.com/archivo.zip C:\ruta\local\archivo.zip bitsadmin /resume myDownloadJob
```

3. **ftp:** El comando FTP se utiliza para transferir archivos a través del Protocolo de Transferencia de Archivos (FTP). Puedes conectarte a un servidor FTP y realizar operaciones como subir y descargar archivos.

Ejemplo: Para conectarte a un servidor FTP y descargar un archivo, puedes usar el siguiente comando:

```
ftp servidor_ftp get archivo_remoto archivo_local
```

4. **getmac**: El comando Getmac muestra las direcciones MAC de las interfaces de red en tu sistema.

Ejemplo: Para ver las direcciones MAC de todas las interfaces de red, simplemente ejecuta:

```
getmac
```

5. **hostname**: Este comando muestra el nombre del host de tu sistema.

Ejemplo: Para ver el nombre de host de tu máquina, simplemente ejecuta:

```
hostname
```

6. **nbtstat**: Nbtstat muestra estadísticas y datos de resolución de nombres NetBIOS en un sistema Windows.

Ejemplo: Para ver las conexiones NetBIOS en tu sistema, puedes ejecutar:

```
nbtstat -n
```

7. **net**: El comando 'net' se utiliza para realizar varias operaciones relacionadas con la red, como ver y administrar recursos compartidos y usuarios.

Ejemplo: Para ver una lista de recursos compartidos en un servidor, puedes usar:

```
net view \\nombre_del_servidor
```

8. **net use**: Este comando se utiliza para conectar o desconectar unidades de red.

Ejemplo: Para mapear una unidad de red a una carpeta compartida, puedes usar:

```
net use Z: \\servidor\\nombre_compartido /user:nombre_usuario contraseña
```

9. **netsh**: Netsh es una utilidad para configurar y administrar configuraciones de red en Windows.

Ejemplo: Para ver la configuración IP de una interfaz de red, puedes usar:

```
netsh interface ipv4 show config "Nombre de la interfaz"
```

10. **telnet**: Telnet se utiliza para conectarse a un servidor remoto a través del protocolo Telnet.

Ejemplo: Para conectarte a un servidor Telnet, puedes usar:

```
telnet dirección_ip Puerto
```

11. **tftp**: TFTP (Trivial File Transfer Protocol) se utiliza para transferir archivos de forma sencilla a través de la red.

Ejemplo: Para enviar un archivo a un servidor TFTP, puedes usar:

```
tftp -i dirección_ip -p puerto -t put archivo_origen archivo_destino
```