

# Universidad Politécnica de Quintana Roo

Trabajo: Tarea 987

Alumno: Arana Zamora Brian de Jesús

Catedrático: Jiménez Sánchez Ismael

Grupo: 27BV

Carrera: Ing. Software

Asignatura: Sistemas operativos

Fecha: 12 de octubre de 2023

7° Cuatrimestre septiembre-diciembre 2023

## Índice

Instrucciones .....	3
Comandos en MSDOS .....	4
A) Anotar los comandos necesarios para ejecutar las siguientes instrucciones desde la consola de Msx-DQS.....	4
1.- " Obtener la ayuda del comando ping .....	4
2.- Enviar un ping a 127.0.0.1 aplicando cualquier parametro.....	4
3.- Verificar la conectividad del equipo utilizando el comando ping, anotar conclusiones .....	4
4.- Obtener la ayuda del comando nslookup .....	4
5.- Resolver la direccion ip, de <a href="https://upqroo.edu.mx/">https://upqroo.edu.mx/</a> usando nslookup .....	5
6.- Hacer ping a la ip obtenida en el paso anterior, anotar conclusiones.....	5
7.- Obtener la ayuda del comando netstat .....	5
8.- Mostrar todas las conexiones y puertos de escucha .....	6
9.- Ejecutar netstat, sin resolver nombres de dominio o puertos .....	6
10.- Mostrar las conexiones TCP .....	6
11.- Mostrar las conexiones UDP.....	7
12.- Utilizar el comando tasklist.....	7
13.- Utilizar el comando taskkill .....	7
14.- Utilizar el comando tracert .....	8
15.- Utilizar el comando ARP .....	8
B) Contesta con tus propias palabras las siguientes preguntas: .....	9
1.- ¿Para que sirve el comando ping?.....	9
2.- ¿Para que sirve el comando nslookup? .....	9
3.- ¿Para que sirve el comando netstat? .....	9
4.- ¿Para que sirve el comando tasklist? .....	9
5.- ¿Para que sirve el comando taskkill? .....	9
6.- ¿Para que sirve el comando tracert? .....	9
7.- ¿Cómo ayudan los primeros tres comandos para detectar problemas en la red?.....	9
C) Investigar los siguientes comandos y anotar ejemplos practicos: .....	10

## Instrucciones

Tarea #987 Realizar el siguiente laboratorio durante la clase, en un pdf documentar con captura de pantalla los resultados de sus comandos y las respuestas a sus preguntas. Subir el pdf a su repositorio readme.

### Practica de laboratorio Comandos 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
- 2.- Enviar un ping a 127.0.0.1 aplicando cualquier parametro
- 3.- Verificar la conectividad del equipo utilizando el comando ping, anotar conclusiones
- 4.- Obtener la ayuda del comando nslookup
- 5.- Resolver la direccion ip de <https://upgroo.edu.mx/> usando nslookup
- 6.- Hacer ping a la ip obtenida en el paso anterior, anotar conclusiones
- 7.- Obtener la ayuda del comando netstat
- 8.- Mostrar todas las conexiones y puertos de escucha
- 9.- Ejecutar netstat sin resolver nombres de dominio o puertos
- 10.- Mostrar las conexiones TCP
- 11.- Mostrar las conexiones UDP
- 12.- Utilizar el comando tasklist
- 13.- Utilizar el comando taskkill
- 14.- Utilizar el comando tracert
- 15.- Utilizar el comando ARP

B) Contesta con tus propias palabras las siguientes preguntas:

- 1.- ¿Para que sirve el comando ping?
- 2.- ¿Para que sirve el comando nslookup?
- 3.- ¿Para que sirve el comando netstat?
- 4.- ¿Para que sirve el comando tasklist?
- 5.- ¿Para que sirve el comando taskkill?
- 6.- ¿Para que sirve el comando tracert?
- 7.- ¿Como ayudan los primeros tres comandos para detectar problemas en la red?

C) Investigar los siguientes comandos y anotar ejemplos practicos:

atmadm, bitsadmin, cmstp, fip, getmac, hostname, nbstat, net, net use, netsh, pathping, rcp, rexec, route, rcping, rsh, tcmsetup, telnet, tftp

## 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

```

[3] Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.3570]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Gamer>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 5895 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.

C:\Users\Gamer>_
```

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

```

[3] Símbolo del sistema

C:\Users\Gamer>ping 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

Estadísticas de ping para 127.0.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
            Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Gamer>_
```

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

```

[3] Seleccionar Símbolo del sistema

C:\Users\Gamer>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=27ms TTL=118
Respuesta desde 142.250.217.238: bytes=32 tiempo=20ms TTL=118
Respuesta desde 142.250.217.238: bytes=32 tiempo=31ms TTL=118
Respuesta desde 142.250.217.238: bytes=32 tiempo=34ms 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 = 20ms, Máximo = 34ms, Media = 28ms

C:\Users\Gamer>_
```

#### 4.- Obtener la ayuda del comando nslookup

```

[3] Símbolo del sistema

C:\Users\Gamer>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\Gamer>
```

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

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

C:\Users\Gamer>nslookup uparoo.edu.mx
Servidor: dns.google
Address: 8.8.8.8

*** dns.google no encuentra uparoo.edu.mx: Non-existent domain

C:\Users\Gamer>
```

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

```
Simbolo del sistema

C:\Users\Gamer>ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=28ms TTL=118
Respuesta desde 8.8.8.8: bytes=32 tiempo=82ms TTL=118
Respuesta desde 8.8.8.8: bytes=32 tiempo=22ms TTL=118
Respuesta desde 8.8.8.8: bytes=32 tiempo=42ms TTL=118

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 28ms, Máximo = 82ms, Media = 41ms

C:\Users\Gamer>
```

## 7.- Obtener la ayuda del comando netstat

```
Simbolo del sistema

C:\Users\Gamer>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.
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 mostrarse las
            estadísticas. Si omite esta opción, netstat imprimirá una sola vez
            la información de configuración.

C:\Users\Gamer>
```

8.- *Mostrar todas las conexiones y puertos de escucha*

```
Símbolo del sistema - netstat -a
C:\Users\Gamer>netstat -a

Conexiones activas

Proto Dirección local Dirección remota Estado
TCP 0.0.0.0:80 LAPTOP-8K07TLRP:0 LISTENING
TCP 0.0.0.0:135 LAPTOP-8K07TLRP:0 LISTENING
TCP 0.0.0.0:443 LAPTOP-8K07TLRP:0 LISTENING
TCP 0.0.0.0:445 LAPTOP-8K07TLRP:0 LISTENING
TCP 0.0.0.0:3306 LAPTOP-8K07TLRP:0 LISTENING
TCP 0.0.0.0:5040 LAPTOP-8K07TLRP:0 LISTENING
TCP 0.0.0.0:7680 LAPTOP-8K07TLRP:0 LISTENING
TCP 0.0.0.0:8733 LAPTOP-8K07TLRP:0 LISTENING
TCP 0.0.0.0:49664 LAPTOP-8K07TLRP:0 LISTENING
TCP 0.0.0.0:49665 LAPTOP-8K07TLRP:0 LISTENING
TCP 0.0.0.0:49666 LAPTOP-8K07TLRP:0 LISTENING
TCP 0.0.0.0:49667 LAPTOP-8K07TLRP:0 LISTENING
TCP 0.0.0.0:49668 LAPTOP-8K07TLRP:0 LISTENING
TCP 0.0.0.0:49696 LAPTOP-8K07TLRP:0 LISTENING
TCP 127.0.0.1:1434 LAPTOP-8K07TLRP:0 LISTENING
TCP 127.0.0.1:5354 LAPTOP-8K07TLRP:0 LISTENING
TCP 127.0.0.1:6463 LAPTOP-8K07TLRP:0 LISTENING
TCP 127.0.0.1:7335 LAPTOP-8K07TLRP:0 LISTENING
TCP 127.0.0.1:12025 LAPTOP-8K07TLRP:0 LISTENING
TCP 127.0.0.1:12110 LAPTOP-8K07TLRP:0 LISTENING
TCP 127.0.0.1:12119 LAPTOP-8K07TLRP:0 LISTENING
TCP 127.0.0.1:12143 LAPTOP-8K07TLRP:0 LISTENING
TCP 127.0.0.1:12465 LAPTOP-8K07TLRP:0 LISTENING
TCP 127.0.0.1:12563 LAPTOP-8K07TLRP:0 LISTENING
TCP 127.0.0.1:12993 LAPTOP-8K07TLRP:0 LISTENING
TCP 127.0.0.1:12995 LAPTOP-8K07TLRP:0 LISTENING
TCP 127.0.0.1:18412 LAPTOP-8K07TLRP:0 LISTENING
TCP 127.0.0.1:27275 LAPTOP-8K07TLRP:0 LISTENING
TCP 127.0.0.1:44950 LAPTOP-8K07TLRP:0 LISTENING
TCP 127.0.0.1:44960 LAPTOP-8K07TLRP:0 LISTENING
TCP 127.0.0.1:51488 LAPTOP-8K07TLRP:0 LISTENING
TCP 192.168.56.1:139 LAPTOP-8K07TLRP:0 LISTENING
TCP 192.168.128.3:139 LAPTOP-8K07TLRP:0 LISTENING
TCP 192.168.128.3:58664 a23-47-195-81:https ESTABLISHED
TCP 192.168.128.3:58676 52.96.28.2:https TIME_WAIT
TCP 192.168.128.3:58678 72.21.81.200:https ESTABLISHED
TCP 192.168.128.3:58681 204.79.197.222:https TIME_WAIT
TCP 192.168.128.3:58682 vip01:https TIME_WAIT
TCP 192.168.128.3:58683 vip01:https TIME_WAIT
TCP 192.168.128.3:58684 104.18.37.228:https TIME_WAIT
```

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

```
Símbolo del sistema
C:\Users\Gamer>netstat -n

Conexiones activas

Proto Dirección local Dirección remota Estado
TCP 192.168.128.3:58664 23.47.195.81:443 CLOSE_WAIT
TCP 192.168.128.3:58678 72.21.81.200:443 CLOSE_WAIT
TCP 192.168.128.3:58691 34.149.207.176:80 TIME_WAIT
TCP 192.168.128.3:58692 157.240.14.52:443 TIME_WAIT
TCP 192.168.128.3:58693 104.288.16.89:443 ESTABLISHED
TCP 192.168.128.3:61774 207.2.167.443 ESTABLISHED
TCP 192.168.128.3:61787 34.82.206.89:7500 ESTABLISHED
TCP 192.168.128.3:62002 108.177.12.188:5228 ESTABLISHED
TCP 192.168.128.3:62569 157.240.14.52:443 ESTABLISHED
TCP 192.168.128.3:63178 162.159.133.234:443 ESTABLISHED
TCP 192.168.128.3:63233 140.82.112.26:443 ESTABLISHED

C:\Users\Gamer>
```

10.- *Mostrar las conexiones TCP*

```
Símbolo del sistema
C:\Users\Gamer>netstat -at

Conexiones activas

Proto Dirección local Dirección remota Estado
TCP 0.0.0.0:80 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 0.0.0.0:135 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 0.0.0.0:443 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 0.0.0.0:445 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 0.0.0.0:3306 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 0.0.0.0:5040 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 0.0.0.0:7680 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 0.0.0.0:8733 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 0.0.0.0:49664 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 0.0.0.0:49665 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 0.0.0.0:49666 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 0.0.0.0:49667 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 0.0.0.0:49668 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 0.0.0.0:49696 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 127.0.0.1:1434 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 127.0.0.1:5354 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 127.0.0.1:6463 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 127.0.0.1:7335 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 127.0.0.1:12025 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 127.0.0.1:12110 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 127.0.0.1:12119 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 127.0.0.1:12143 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 127.0.0.1:12465 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 127.0.0.1:12563 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 127.0.0.1:12993 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 127.0.0.1:12995 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 127.0.0.1:18412 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 127.0.0.1:27275 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 127.0.0.1:44950 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 127.0.0.1:44960 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 127.0.0.1:51488 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 192.168.56.1:139 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 192.168.128.3:139 LAPTOP-8K07TLRP:0 LISTENING EnHost
TCP 192.168.128.3:58664 a23-47-195-81:https CLOSE_WAIT EnHost

C:\Users\Gamer>
```

11.- Mostrar las conexiones UDP

```
Símbolo del sistema
C:\Users\Gamer>netstat -au

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.
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 mostrarse las
        estadísticas. Si omites esta opción, netstat imprimirá una sola vez
        la información de configuración.

C:\Users\Gamer>
```

12.- Utilizar el comando tasklist

```
Símbolo del sistema
C:\Users\Gamer>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        136 KB
Registry                  100 Services         0    38,588 KB
smss.exe                   456 Services         0     1,100 KB
csrss.exe                  724 Services         0     5,240 KB
wininit.exe                824 Services         0    6,424 KB
csrss.exe                  832 Console          1     5,988 KB
services.exe              896 Services         0    12,232 KB
lsass.exe                 904 Services         0    23,532 KB
svchost.exe               476 Services         0    27,472 KB
Fontdrvhost.exe           544 Services         0     2,712 KB
WUDFHost.exe              536 Services         0     9,604 KB
svchost.exe              1060 Services         0    15,500 KB
svchost.exe              1136 Services         0     7,828 KB
winlogon.exe             1200 Console          1    10,120 KB
Fontdrvhost.exe          1260 Console          1    15,632 KB
dwm.exe                  1344 Console          1    85,256 KB
svchost.exe              1420 Services         0     4,984 KB
svchost.exe              1448 Services         0     9,516 KB
svchost.exe              1556 Services         0     7,576 KB
svchost.exe              1564 Services         0     7,676 KB
svchost.exe              1572 Services         0    16,008 KB
svchost.exe              1656 Services         0    12,412 KB
svchost.exe              1712 Services         0     5,880 KB
svchost.exe              1720 Services         0    13,404 KB
svchost.exe              1880 Services         0     9,560 KB
svchost.exe              1944 Services         0     6,496 KB
svchost.exe              1932 Services         0     6,616 KB
svchost.exe              1548 Services         0    17,148 KB
svchost.exe              1644 Services         0    10,300 KB
svchost.exe              1972 Services         0     7,344 KB
NDDisplay.Container.exe   2152 Services         0    15,808 KB
wsc_proxy.exe            2276 Services         0     9,856 KB
svchost.exe              2284 Services         0    11,664 KB
svchost.exe              2304 Services         0    13,664 KB
svchost.exe              2320 Services         0     7,072 KB
svchost.exe              2352 Services         0     5,548 KB
Memory Compression       2428 Services         0    105,312 KB
svchost.exe              2472 Services         0     7,900 KB
lgfxCUIService.exe        2524 Services         0     8,200 KB
svchost.exe              2544 Services         0    10,052 KB
```

13.- Utilizar el comando taskkil

```
Símbolo del sistema
C:\Users\Gamer>taskkill /F /PID 3084
Correcto: se terminó el proceso con PID 3084.

C:\Users\Gamer>
```

## 14.- Utilizar el comando tracert

```
Simbolo del sistema
C:\Users\Gamer>tracert google.com

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

 1  4 ms    1 ms    1 ms  192.168.128.1
 2  8 ms    3 ms    3 ms  192.168.109.1
 3  9 ms    8 ms   22 ms  fixed-187-188-58-130.totalplay.net [187.188.58.130]
 4  63 ms   7 ms   33 ms  10.180.58.1
 5  20 ms   25 ms   20 ms  72.14.242.148
 6  130 ms  77 ms   64 ms  192.178.74.87
 7  52 ms   58 ms   29 ms  142.251.65.33
 8  29 ms   36 ms   27 ms  mia07s62-in-f14.1e100.net [142.250.217.238]

Traza completa.
C:\Users\Gamer>
```

## 15.- Utilizar el comando ARP

```
Simbolo del sistema
C:\Users\Gamer>arp -a

Interfaz: 192.168.128.3 --- 0x2
Dirección de Internet      Dirección física      Tipo
192.168.128.1              e0-23-ff-e2-c2-cc    dinámico
192.168.128.4              d2-47-bc-27-c9-13    dinámico
192.168.128.10             62-dd-71-bc-50-6b    dinámico
192.168.128.11             32-18-55-37-1a-94    dinámico
192.168.128.12             76-d7-00-f1-00-ef    dinámico
192.168.143.255            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
255.255.255.255            ff-ff-ff-ff-ff-ff    estático

Interfaz: 192.168.56.1 --- 0xc
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
255.255.255.255            ff-ff-ff-ff-ff-ff    estático

C:\Users\Gamer>
```



***B) Contesta con tus propias palabras las siguientes preguntas:******1.- ;Para que sirve el comando ping?***

El comando ping sirve para verificar si un dispositivo en red es alcanzable y para medir el tiempo que tarda en responder a una solicitud de red.

***2.- gPara que sirve el comando nslookup?***

El comando nslookup se utiliza para obtener información de DNS, como la dirección IP asociada a un nombre de dominio o el nombre de dominio asociado a una dirección IP.

***3.- ;Para que sirve el comando netstat?***

El comando netstat se utiliza para mostrar estadísticas de red y conexiones activas en un sistema.

***4.-;Para que sirve el comando tasklist?***

El comando tasklist se utiliza para mostrar una lista de procesos en ejecución en un sistema.

***5.- ;Para que sirve el comando taskkill?***

El comando taskkill se utiliza para finalizar un proceso en ejecución en un sistema.

***6.- ;Para que sirve el comando tracert?***

El comando tracert se utiliza para rastrear la ruta que sigue un paquete de red desde el origen hasta el destino.

***7.- cComo ayudan los primeros tres comandos para detectar problemas en la red?***

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

- "Ping" verifica la conectividad entre dispositivos y mide la latencia, lo que ayuda a identificar si un dispositivo remoto está accesible.
- "Nslookup" ayuda a diagnosticar problemas de resolución de nombres, lo que puede ser fundamental para establecer conexiones efectivas en una red.
- "Netstat" muestra información sobre conexiones y puertos en uso, lo que es esencial para identificar problemas de red, como congestión, puertos bloqueados o conexiones no deseadas.

**C) Investigar los siguientes comandos y anotar ejemplos practicos:**

- **atmadm:**  
Descripción: Este comando se utiliza para mostrar o modificar los parámetros de adaptadores ATM.  
Ejemplo: `atmadm -l` muestra una lista de los adaptadores ATM en el sistema.
- **bitsadmin:**  
Descripción: Permite administrar trabajos de transferencia de archivos en segundo plano.  
Ejemplo: `bitsadmin /create mydownload` crea un nuevo trabajo de descarga llamado "mydownload".
- **cmstp:**  
Descripción: Utilizado para instalar, desinstalar o enumerar perfiles de conexión de red.  
Ejemplo: `cmstp /s profile.inf` instala un perfil de conexión de red desde un archivo de información de perfil.
- **ftp:**  
Descripción: Inicia una sesión FTP para transferir archivos entre sistemas.  
Ejemplo: `ftp example.com` inicia una sesión FTP con el servidor "example.com".
- **getmac:**  
Descripción: Muestra la dirección MAC de adaptadores de red.  
Ejemplo: `getmac /fo list` muestra la dirección MAC de todos los adaptadores en el sistema.
- **hostname:**  
Descripción: Muestra el nombre del equipo.  
Ejemplo: `hostname` muestra el nombre del equipo actual.
- **nbtstat:**  
Descripción: Muestra estadísticas y datos de resolución de nombres NetBIOS.  
Ejemplo: `nbtstat -A 192.168.1.2` muestra información sobre el nombre NetBIOS de la dirección IP especificada.
- **net:**  
Descripción: Comando base para administrar recursos de red.  
Ejemplo: `net view` muestra una lista de recursos compartidos en la red.
- **net use:**  
Descripción: Conecta o desconecta recursos compartidos de red.  
Ejemplo: `net use Z: \\server\share` conecta una unidad de red Z: a un recurso compartido en el servidor.
- **netsh:**  
Descripción: Permite configurar parámetros de red, firewall y otros componentes de Windows.  
Ejemplo: `netsh interface ipv4 show interfaces` muestra información sobre las interfaces de red IPv4.
- **pathping:**  
Descripción: Combina las funciones de `tracert` y `ping` para proporcionar información detallada sobre el rendimiento de la ruta de red.

Ejemplo: `pathping example.com` realiza un seguimiento y ping a "example.com" y muestra estadísticas detalladas.

- **route:**  
Descripción: Muestra y modifica las tablas de enrutamiento IP.  
Ejemplo: `route print` muestra la tabla de enrutamiento IP actual.
- **tracert** (posiblemente fue un error tipográfico en la lista):  
Descripción: Muestra la ruta que los paquetes toman para llegar a un destino.  
Ejemplo: `tracert example.com` muestra la ruta de los paquetes a "example.com".
- **tsh:**  
Descripción: No existe un comando "tsh" en Windows. Es posible que sea un error tipográfico.
- **telnet:**  
Descripción: Inicia una sesión Telnet para conectarse a un servidor remoto.  
Ejemplo: `telnet example.com` inicia una sesión Telnet con el servidor "example.com".
- **tftp:**  
Descripción: Transfiere archivos a través del Protocolo de Transferencia de Archivos Trivial (TFTP).  
Ejemplo: `tftp -i 192.168.1.2 GET file.txt` descarga el archivo "file.txt" desde un servidor TFTP en la dirección IP 192.168.1.2.