



# PRÁCTICA DE LABORATORIO

SISTEMAS OPERATIVOS

Coyolt Oliveros Irving Ramón. 27BV.

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

1.- Obtener la ayuda del comando ping

ping -?

```
C:\Users\irvin>ping -?

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

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

C:\Users\irvin>
```

2.- Enviar un ping a 127.0.0.1 aplicando cualquier parametro

ping -t -l 1000 -n 10 127.0.0.1

-t hace que el envío se repita , -l se define el tamaño de los bytes en este caso son 1000 y -n la cantidad de paquetes que se enviaran antes de que se detenga que en este caso son 10

```
C:\Users\irvin>ping -t -l 1000 -n 10 127.0.0.1

Haciendo ping a 127.0.0.1 con 1000 bytes de datos:
Respuesta desde 127.0.0.1: bytes=1000 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=1000 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=1000 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=1000 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=1000 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=1000 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=1000 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=1000 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=1000 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=1000 tiempo<1m TTL=128

Estadísticas de ping para 127.0.0.1:
    Paquetes: enviados = 10, recibidos = 10, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\irvin>
```

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

```
C:\Users\irvin>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=19ms TTL=118
Respuesta desde 142.250.217.238: bytes=32 tiempo=80ms TTL=118
Respuesta desde 142.250.217.238: bytes=32 tiempo=18ms TTL=118
Respuesta desde 142.250.217.238: bytes=32 tiempo=19ms 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 = 18ms, Máximo = 80ms, Media = 34ms

C:\Users\irvin>
```

La conexión es bastante estable, no hubo pérdida de ningún paquete y fue realizada de manera exitosa.

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

```
C:\Users\irvin>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\irvin>
```

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

```
C:\Users\irvin>nslookup upqroo.edu.mx
Servidor:  dns.google
Address:  8.8.8.8

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

C:\Users\irvin>
```

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

```
C:\Users\irvin>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=119ms TTL=50
Respuesta desde 77.68.126.20: bytes=32 tiempo=120ms 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 = 118ms, Máximo = 122ms, Media = 119ms

C:\Users\irvin>
```

El ping se realizó de manera exitosa, con un tiempo de respuesta adecuado y sin ninguna perdida en los 4 paquetes que se enviaron.

## 7.- Obtener la ayuda del comando netstat

```
C:\Users\irvin>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.

C:\Users\irvin>
```

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

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

Conexiones activas

Proto	Dirección local	Dirección remota	Estado
TCP	0.0.0.0:80	LAPTOP-HKSHACEU:0	LISTENING
TCP	0.0.0.0:135	LAPTOP-HKSHACEU:0	LISTENING
TCP	0.0.0.0:443	LAPTOP-HKSHACEU:0	LISTENING
TCP	0.0.0.0:445	LAPTOP-HKSHACEU:0	LISTENING
TCP	0.0.0.0:5040	LAPTOP-HKSHACEU:0	LISTENING
TCP	0.0.0.0:5432	LAPTOP-HKSHACEU:0	LISTENING
TCP	0.0.0.0:7680	LAPTOP-HKSHACEU:0	LISTENING
TCP	0.0.0.0:8090	LAPTOP-HKSHACEU:0	LISTENING
TCP	0.0.0.0:27036	LAPTOP-HKSHACEU:0	LISTENING
TCP	0.0.0.0:49664	LAPTOP-HKSHACEU:0	LISTENING
TCP	0.0.0.0:49665	LAPTOP-HKSHACEU:0	LISTENING
TCP	0.0.0.0:49666	LAPTOP-HKSHACEU:0	LISTENING
TCP	0.0.0.0:49667	LAPTOP-HKSHACEU:0	LISTENING
TCP	0.0.0.0:49668	LAPTOP-HKSHACEU:0	LISTENING
TCP	0.0.0.0:49670	LAPTOP-HKSHACEU:0	LISTENING
TCP	127.0.0.1:1434	LAPTOP-HKSHACEU:0	LISTENING
TCP	127.0.0.1:2015	LAPTOP-HKSHACEU:0	LISTENING
TCP	127.0.0.1:6463	LAPTOP-HKSHACEU:0	LISTENING
TCP	127.0.0.1:27060	LAPTOP-HKSHACEU:0	LISTENING
TCP	127.0.0.1:27060	LAPTOP-HKSHACEU:58255	ESTABLISHED
TCP	127.0.0.1:58090	LAPTOP-HKSHACEU:65001	ESTABLISHED
TCP	127.0.0.1:58140	LAPTOP-HKSHACEU:0	LISTENING
TCP	127.0.0.1:58140	LAPTOP-HKSHACEU:58162	ESTABLISHED
TCP	127.0.0.1:58143	LAPTOP-HKSHACEU:0	LISTENING
TCP	127.0.0.1:58143	LAPTOP-HKSHACEU:58170	ESTABLISHED
TCP	127.0.0.1:58146	LAPTOP-HKSHACEU:0	LISTENING
TCP	127.0.0.1:58146	LAPTOP-HKSHACEU:58169	ESTABLISHED
TCP	127.0.0.1:58162	LAPTOP-HKSHACEU:58140	ESTABLISHED
TCP	127.0.0.1:58169	LAPTOP-HKSHACEU:58146	ESTABLISHED
TCP	127.0.0.1:58170	LAPTOP-HKSHACEU:58143	ESTABLISHED
TCP	127.0.0.1:58255	LAPTOP-HKSHACEU:27060	ESTABLISHED
TCP	127.0.0.1:58315	LAPTOP-HKSHACEU:0	LISTENING
TCP	127.0.0.1:58315	LAPTOP-HKSHACEU:58317	ESTABLISHED
TCP	127.0.0.1:58317	LAPTOP-HKSHACEU:58315	ESTABLISHED
TCP	127.0.0.1:65001	LAPTOP-HKSHACEU:0	LISTENING
TCP	127.0.0.1:65001	LAPTOP-HKSHACEU:58090	ESTABLISHED
TCP	172.16.128.3:139	LAPTOP-HKSHACEU:0	LISTENING
TCP	172.16.128.3:7680	192.168.128.248:61936	TIME_WAIT
TCP	172.16.128.3:7680	192.168.128.248:61939	TIME_WAIT
TCP	172.16.128.3:59385	181:https	ESTABLISHED
TCP	172.16.128.3:59386	ya-in-f188:5228	ESTABLISHED
TCP	172.16.128.3:59388	1:https	ESTABLISHED
TCP	172.16.128.3:59389	104.18.37.228:https	ESTABLISHED
TCP	172.16.128.3:59390	yq-in-f94:https	ESTABLISHED
TCP	172.16.128.3:59391	20.25.241.18:https	ESTABLISHED
TCP	172.16.128.3:59392	bingforbusiness:https	TIME_WAIT
TCP	172.16.128.3:59393	20.62.59.38:https	TIME_WAIT
TCP	172.16.128.3:59394	20.62.59.38:https	ESTABLISHED
TCP	172.16.128.3:59396	52.96.104.18:https	ESTABLISHED
TCP	172.16.128.3:59397	a23-61-255-138:http	TIME_WAIT
TCP	172.16.128.3:59398	162.159.135.234:https	ESTABLISHED
TCP	172.16.128.3:59400	162-254-195-71:27031	ESTABLISHED
TCP	172.16.128.3:59407	ac9293e5fb5d2d1d2:http	ESTABLISHED
TCP	172.16.128.3:59408	whatsapp-cdn-shv-02-iad3:https	ESTABLISHED
TCP	172.16.128.3:59409	13.107.3.254:https	TIME_WAIT
TCP	172.16.128.3:59410	a-0001:https	TIME_WAIT
TCP	172.16.128.3:59411	204.79.197.222:https	TIME_WAIT
TCP	172.16.128.3:59412	40.97.228.178:https	TIME_WAIT
TCP	172.16.128.3:59413	72.21.81.200:https	TIME_WAIT
TCP	172.16.128.3:59414	13.107.246.254:https	TIME_WAIT
TCP	172.16.128.3:59415	20.50.80.209:https	ESTABLISHED
TCP	192.168.56.1:139	LAPTOP-HKSHACEU:0	LISTENING
TCP	[::]:80	LAPTOP-HKSHACEU:0	LISTENING
TCP	[::]:135	LAPTOP-HKSHACEU:0	LISTENING
TCP	[::]:443	LAPTOP-HKSHACEU:0	LISTENING
TCP	[::]:445	LAPTOP-HKSHACEU:0	LISTENING

```

TCP [::]:445 LAPTOP-HKSHACEU:0 LISTENING
TCP [::]:5432 LAPTOP-HKSHACEU:0 LISTENING
TCP [::]:7680 LAPTOP-HKSHACEU:0 LISTENING
TCP [::]:49664 LAPTOP-HKSHACEU:0 LISTENING
TCP [::]:49665 LAPTOP-HKSHACEU:0 LISTENING
TCP [::]:49666 LAPTOP-HKSHACEU:0 LISTENING
TCP [::]:49667 LAPTOP-HKSHACEU:0 LISTENING
TCP [::]:49668 LAPTOP-HKSHACEU:0 LISTENING
TCP [::]:49670 LAPTOP-HKSHACEU:0 LISTENING
TCP [::1]:1434 LAPTOP-HKSHACEU:0 LISTENING
TCP [::1]:49669 LAPTOP-HKSHACEU:0 LISTENING
UDP 0.0.0.0:500 *: *
UDP 0.0.0.0:4500 *: *
UDP 0.0.0.0:5050 *: *
UDP 0.0.0.0:5353 *: *
UDP 0.0.0.0:5353 *: *
UDP 0.0.0.0:5353 *: *
UDP 0.0.0.0:5353 *: *
UDP 0.0.0.0:5353 *: *
UDP 0.0.0.0:5355 *: *
UDP 0.0.0.0:27036 *: *
UDP 0.0.0.0:59662 *: *
UDP 127.0.0.1:1900 *: *
UDP 127.0.0.1:10040 *: *
UDP 127.0.0.1:10041 *: *
UDP 127.0.0.1:54830 127.0.0.1:54830
UDP 127.0.0.1:55054 *: *
UDP 127.0.0.1:58441 *: *
UDP 172.16.128.3:137 *: *
UDP 172.16.128.3:138 *: *
UDP 172.16.128.3:1900 *: *
UDP 172.16.128.3:2177 *: *
UDP 172.16.128.3:5353 *: *
UDP 172.16.128.3:58440 *: *
UDP 172.16.129.144:27036 *: *
UDP 192.168.56.1:137 *: *
UDP 192.168.56.1:138 *: *
UDP 192.168.56.1:1900 *: *
UDP 192.168.56.1:2177 *: *
UDP 192.168.56.1:5353 *: *
UDP 192.168.56.1:58439 *: *
UDP [::]:500 *: *
UDP [::]:4500 *: *
UDP [::]:5353 *: *
UDP [::]:5353 *: *
UDP [::]:5353 *: *
UDP [::]:5355 *: *
UDP [::]:59663 *: *
UDP [::1]:1900 *: *
UDP [::1]:5353 *: *
UDP [::1]:54831 [::1]:54831
UDP [::1]:58438 *: *
UDP [fe80::1acb:b671:b596:93ed%3]:1900 *: *
UDP [fe80::1acb:b671:b596:93ed%3]:2177 *: *
UDP [fe80::1acb:b671:b596:93ed%3]:58437 *: *
UDP [fe80::940f:e935:7c64:30d4%6]:1900 *: *
UDP [fe80::940f:e935:7c64:30d4%6]:2177 *: *
UDP [fe80::940f:e935:7c64:30d4%6]:58436 *: *

C:\Users\irvin>

```

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

```

C:\Users\irvin>netstat -n

Conexiones activas

Proto  Dirección local      Dirección remota      Estado
TCP    127.0.0.1:27060      127.0.0.1:58255      ESTABLISHED
TCP    127.0.0.1:58090      127.0.0.1:65001      ESTABLISHED
TCP    127.0.0.1:58140      127.0.0.1:58162      ESTABLISHED
TCP    127.0.0.1:58143      127.0.0.1:58170      ESTABLISHED
TCP    127.0.0.1:58146      127.0.0.1:58169      ESTABLISHED
TCP    127.0.0.1:58162      127.0.0.1:58140      ESTABLISHED
TCP    127.0.0.1:58169      127.0.0.1:58146      ESTABLISHED
TCP    127.0.0.1:58170      127.0.0.1:58143      ESTABLISHED
TCP    127.0.0.1:58255      127.0.0.1:27060      ESTABLISHED
TCP    127.0.0.1:58315      127.0.0.1:58317      ESTABLISHED
TCP    127.0.0.1:58317      127.0.0.1:58315      ESTABLISHED
TCP    127.0.0.1:65001      127.0.0.1:58090      ESTABLISHED
TCP    172.16.128.3:7680    192.168.128.248:61978 TIME_WAIT
TCP    172.16.128.3:59385    34.120.214.181:443    ESTABLISHED
TCP    172.16.128.3:59386    173.194.219.188:5228  ESTABLISHED
TCP    172.16.128.3:59388    35.190.80.1:443       ESTABLISHED
TCP    172.16.128.3:59389    104.18.37.228:443     ESTABLISHED
TCP    172.16.128.3:59391    20.25.241.18:443      ESTABLISHED
TCP    172.16.128.3:59394    20.62.59.38:443       ESTABLISHED
TCP    172.16.128.3:59398    162.159.135.234:443   ESTABLISHED
TCP    172.16.128.3:59400    162.254.195.71:27031  ESTABLISHED
TCP    172.16.128.3:59407    3.33.252.61:80        ESTABLISHED
TCP    172.16.128.3:59416    64.233.176.190:443    ESTABLISHED
TCP    172.16.128.3:59417    142.251.15.138:443    ESTABLISHED
TCP    172.16.128.3:59418    157.90.91.71:443      ESTABLISHED
TCP    172.16.128.3:59419    157.90.91.71:443      ESTABLISHED
TCP    172.16.128.3:59420    13.35.115.79:443      ESTABLISHED
TCP    172.16.128.3:59423    142.251.15.94:443     ESTABLISHED
TCP    172.16.128.3:59425    20.94.21.149:443      ESTABLISHED
TCP    172.16.128.3:59426    20.94.204.65:443      ESTABLISHED
TCP    172.16.128.3:59427    103.41.69.238:443     ESTABLISHED
TCP    172.16.128.3:59428    13.89.223.27:443      ESTABLISHED
TCP    172.16.128.3:59429    20.112.85.203:443     ESTABLISHED
TCP    172.16.128.3:59430    184.25.164.10:443     ESTABLISHED
TCP    172.16.128.3:59431    13.107.5.91:443       ESTABLISHED
TCP    172.16.128.3:59432    40.69.147.210:443     ESTABLISHED
TCP    172.16.128.3:59433    51.143.58.193:443     ESTABLISHED
TCP    172.16.128.3:59434    20.98.74.233:443      ESTABLISHED
TCP    172.16.128.3:59435    20.98.74.233:443      ESTABLISHED
TCP    172.16.128.3:59436    20.109.167.1:443      ESTABLISHED
TCP    172.16.128.3:59437    184.25.164.10:443     ESTABLISHED
TCP    172.16.128.3:59438    40.91.95.75:443       ESTABLISHED

C:\Users\irvin>

```

10.- Mostrar las conexiones TCP



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

Conexiones activas

Proto	Dirección local Estado de descarga	Dirección remota	Estado	
TCP	127.0.0.1:27060	LAPTOP-HKSHACEU:58255	ESTABLISHED	EnHost
TCP	127.0.0.1:58090	LAPTOP-HKSHACEU:65001	ESTABLISHED	EnHost
TCP	127.0.0.1:58140	LAPTOP-HKSHACEU:58162	ESTABLISHED	EnHost
TCP	127.0.0.1:58143	LAPTOP-HKSHACEU:58170	ESTABLISHED	EnHost
TCP	127.0.0.1:58146	LAPTOP-HKSHACEU:58169	ESTABLISHED	EnHost
TCP	127.0.0.1:58162	LAPTOP-HKSHACEU:58140	ESTABLISHED	EnHost
TCP	127.0.0.1:58169	LAPTOP-HKSHACEU:58146	ESTABLISHED	EnHost
TCP	127.0.0.1:58170	LAPTOP-HKSHACEU:58143	ESTABLISHED	EnHost
TCP	127.0.0.1:58255	LAPTOP-HKSHACEU:27060	ESTABLISHED	EnHost
TCP	127.0.0.1:58315	LAPTOP-HKSHACEU:58317	ESTABLISHED	EnHost
TCP	127.0.0.1:58317	LAPTOP-HKSHACEU:58315	ESTABLISHED	EnHost
TCP	127.0.0.1:65001	LAPTOP-HKSHACEU:58090	ESTABLISHED	EnHost
TCP	172.16.128.3:7680	192.168.128.248:61978	TIME_WAIT	EnHost
TCP	172.16.128.3:7680	192.168.128.248:62000	TIME_WAIT	EnHost
TCP	172.16.128.3:59385	181:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59386	ya-in-f188:5228	ESTABLISHED	EnHost
TCP	172.16.128.3:59388	1:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59389	104.18.37.228:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59391	20.25.241.18:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59394	20.62.59.38:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59398	162.159.135.234:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59400	162-254-195-71:27031	ESTABLISHED	EnHost
TCP	172.16.128.3:59407	ac9293e5fb5d2d1d2:http	ESTABLISHED	EnHost
TCP	172.16.128.3:59416	yw-in-f190:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59417	yl-in-f138:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59418	static:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59419	static:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59420	server-13-35-115-79:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59423	yl-in-f94:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59425	20.94.21.149:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59426	20.94.204.65:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59427	103.41.69.238:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59428	13.89.223.27:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59429	20.112.85.203:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59430	a184-25-164-10:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59431	13.107.5.91:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59432	40.69.147.210:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59433	51.143.58.193:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59434	20.98.74.233:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59435	20.98.74.233:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59436	20.109.167.1:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59437	a184-25-164-10:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59438	40.91.95.75:https	ESTABLISHED	EnHost
TCP	172.16.128.3:59439	a23-209-36-64:https	ESTABLISHED	EnHost

11.- Mostrar las conexiones UDP

```
C:\Users\irvin> netstat -a -p UDP -n
```

Conexiones activas

Proto	Dirección local	Dirección remota	Estado
UDP	0.0.0.0:500	*:*	
UDP	0.0.0.0:4500	*:*	
UDP	0.0.0.0:5050	*:*	
UDP	0.0.0.0:5353	*:*	
UDP	0.0.0.0:5353	*:*	
UDP	0.0.0.0:5353	*:*	
UDP	0.0.0.0:5353	*:*	
UDP	0.0.0.0:5353	*:*	
UDP	0.0.0.0:5355	*:*	
UDP	0.0.0.0:27036	*:*	
UDP	0.0.0.0:57309	*:*	
UDP	0.0.0.0:57310	*:*	
UDP	0.0.0.0:57311	*:*	
UDP	0.0.0.0:57312	*:*	
UDP	0.0.0.0:59662	*:*	
UDP	127.0.0.1:1900	*:*	
UDP	127.0.0.1:10040	*:*	
UDP	127.0.0.1:10041	*:*	
UDP	127.0.0.1:54830	127.0.0.1:54830	
UDP	127.0.0.1:55054	*:*	
UDP	127.0.0.1:58441	*:*	
UDP	172.16.128.3:137	*:*	
UDP	172.16.128.3:138	*:*	
UDP	172.16.128.3:1900	*:*	
UDP	172.16.128.3:2177	*:*	
UDP	172.16.128.3:5353	*:*	
UDP	172.16.128.3:58440	*:*	
UDP	172.16.129.144:27036	*:*	
UDP	192.168.56.1:137	*:*	
UDP	192.168.56.1:138	*:*	
UDP	192.168.56.1:1900	*:*	
UDP	192.168.56.1:2177	*:*	
UDP	192.168.56.1:5353	*:*	
UDP	192.168.56.1:58439	*:*	

12. Utilizar el comando tasklist

C:\Users\irvin>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	6,544 KB
Secure System	140	Services	0	41,896 KB
Registry	212	Services	0	36,652 KB
smss.exe	708	Services	0	1,164 KB
csrss.exe	204	Services	0	5,732 KB
wininit.exe	736	Services	0	6,392 KB
services.exe	1084	Services	0	15,232 KB
LsaIso.exe	1100	Services	0	3,152 KB
lsass.exe	1116	Services	0	29,412 KB
svchost.exe	1300	Services	0	33,120 KB
fontdrvhost.exe	1336	Services	0	3,180 KB
WUDFHost.exe	1432	Services	0	9,204 KB
svchost.exe	1492	Services	0	19,676 KB
svchost.exe	1540	Services	0	8,856 KB
svchost.exe	1708	Services	0	4,928 KB
svchost.exe	1792	Services	0	10,044 KB
svchost.exe	1800	Services	0	9,236 KB
svchost.exe	1872	Services	0	15,544 KB
IntelCpHDCPSvc.exe	1896	Services	0	6,868 KB
svchost.exe	1904	Services	0	8,664 KB
svchost.exe	1964	Services	0	9,964 KB
svchost.exe	1984	Services	0	7,616 KB
svchost.exe	2032	Services	0	13,252 KB
svchost.exe	2052	Services	0	6,244 KB
IntelCpHeciSvc.exe	2076	Services	0	6,988 KB
svchost.exe	2096	Services	0	17,376 KB
svchost.exe	2136	Services	0	9,240 KB
svchost.exe	2144	Services	0	11,468 KB
igfxCUIService.exe	2304	Services	0	8,876 KB
svchost.exe	2468	Services	0	14,192 KB
svchost.exe	2576	Services	0	27,272 KB
OmenCap.exe	2584	Services	0	7,280 KB
AppHelperCap.exe	2596	Services	0	22,360 KB
SysInfoCap.exe	2616	Services	0	28,856 KB
DiagsCap.exe	2624	Services	0	13,232 KB
NetworkCap.exe	2632	Services	0	30,220 KB
svchost.exe	2788	Services	0	9,040 KB
TouchpointAnalyticsClient	2828	Services	0	55,392 KB
svchost.exe	3016	Services	0	6,132 KB
svchost.exe	3024	Services	0	8,000 KB
svchost.exe	2256	Services	0	16,456 KB
svchost.exe	2836	Services	0	25,748 KB
svchost.exe	3152	Services	0	7,180 KB
SynTPEnhService.exe	3368	Services	0	8,472 KB
NVDisplay.Container.exe	3424	Services	0	19,992 KB
svchost.exe	3464	Services	0	17,904 KB
svchost.exe	3500	Services	0	5,396 KB
svchost.exe	3508	Services	0	11,784 KB
svchost.exe	3556	Services	0	8,488 KB
svchost.exe	3564	Services	0	8,648 KB
Memory Compression	3600	Services	0	414,096 KB
svchost.exe	3700	Services	0	28,636 KB
svchost.exe	3892	Services	0	15,348 KB
svchost.exe	3924	Services	0	6,596 KB
svchost.exe	4012	Services	0	6,268 KB
svchost.exe	4020	Services	0	10,176 KB
svchost.exe	4104	Services	0	11,944 KB
svchost.exe	4152	Services	0	19,164 KB

svchost.exe	4176	Services	0	6,492 KB
svchost.exe	4240	Services	0	11,648 KB
PresentationFontCache.exe	4356	Services	0	17,512 KB
svchost.exe	4404	Services	0	37,260 KB
spoolsv.exe	4720	Services	0	13,668 KB
svchost.exe	4976	Services	0	7,320 KB
svchost.exe	5128	Services	0	8,720 KB
svchost.exe	5136	Services	0	30,916 KB
svchost.exe	5160	Services	0	43,264 KB
svchost.exe	5188	Services	0	7,660 KB
svchost.exe	5200	Services	0	10,120 KB
nssm.exe	5208	Services	0	5,600 KB
OneApp.IGCC.WinService.ex	5216	Services	0	43,468 KB
ibtsiva.exe	5224	Services	0	4,884 KB
svchost.exe	5232	Services	0	18,924 KB
svchost.exe	5240	Services	0	9,580 KB
DtsApo4Service.exe	5248	Services	0	10,832 KB
gameinputsvc.exe	5256	Services	0	4,968 KB
IntelAudioService.exe	5280	Services	0	20,592 KB
RZSurroundService.exe	5288	Services	0	7,896 KB
svchost.exe	5300	Services	0	5,232 KB
RzUpdateEngineService.exe	5312	Services	0	15,760 KB
nvcontainer.exe	5320	Services	0	37,788 KB
servicehost.exe	5328	Services	0	40,560 KB
svchost.exe	5344	Services	0	16,680 KB
WsNativePushService.exe	5360	Services	0	4,228 KB
pg_ctl.exe	5372	Services	0	5,564 KB
sqlwriter.exe	5396	Services	0	7,592 KB
RtkAudUService64.exe	5404	Services	0	15,948 KB
RstMwService.exe	5416	Services	0	6,652 KB
MsMpEng.exe	5448	Services	0	269,540 KB
OfficeClickToRun.exe	5684	Services	0	38,736 KB
LMS.exe	5712	Services	0	9,372 KB
svchost.exe	5856	Services	0	8,692 KB
expressvpnd.exe	6244	Services	0	19,976 KB
conhost.exe	6496	Services	0	7,748 KB
wlanext.exe	6532	Services	0	7,184 KB
jhi_service.exe	6548	Services	0	5,656 KB
conhost.exe	6584	Services	0	4,968 KB
gamingservicesnet.exe	6764	Services	0	4,556 KB
gamingservices.exe	6780	Services	0	32,856 KB
sqlservr.exe	6964	Services	0	113,160 KB
sqlceip.exe	6980	Services	0	50,808 KB
postgres.exe	7284	Services	0	16,948 KB
conhost.exe	7292	Services	0	7,320 KB
AggregatorHost.exe	7916	Services	0	9,876 KB
postgres.exe	7924	Services	0	7,112 KB
svchost.exe	8172	Services	0	20,028 KB
unsecapp.exe	10068	Services	0	8,352 KB
svchost.exe	8628	Services	0	4,584 KB
svchost.exe	8724	Services	0	8,240 KB
svchost.exe	10404	Services	0	11,592 KB
svchost.exe	10632	Services	0	28,368 KB
svchost.exe	11004	Services	0	11,936 KB
svchost.exe	11256	Services	0	10,804 KB
postgres.exe	13592	Services	0	7,504 KB
postgres.exe	13600	Services	0	7,932 KB
postgres.exe	13616	Services	0	11,376 KB
postgres.exe	13628	Services	0	8,048 KB
postgres.exe	13640	Services	0	7,516 KB
postgres.exe	13660	Services	0	7,808 KB
GoogleCrashHandler.exe	13180	Services	0	1,300 KB
GoogleCrashHandler64.exe	13176	Services	0	1,040 KB

NisSrv.exe	14856	Services	0	11,404 KB
SearchIndexer.exe	14704	Services	0	41,148 KB
svchost.exe	16164	Services	0	15,476 KB
SecurityHealthService.exe	1044	Services	0	17,452 KB
svchost.exe	17288	Services	0	9,244 KB
svchost.exe	9696	Services	0	17,280 KB
svchost.exe	14168	Services	0	8,852 KB
HPCommRecovery.exe	8104	Services	0	24,132 KB
SgrmBroker.exe	7560	Services	0	9,140 KB
svchost.exe	9944	Services	0	12,792 KB
svchost.exe	7452	Services	0	9,992 KB
svchost.exe	12872	Services	0	6,680 KB
svchost.exe	16476	Services	0	12,788 KB
svchost.exe	12892	Services	0	14,404 KB
svchost.exe	13800	Services	0	8,984 KB
svchost.exe	5152	Services	0	20,624 KB
svchost.exe	10532	Services	0	6,036 KB
svchost.exe	18948	Services	0	9,460 KB
svchost.exe	11652	Services	0	7,188 KB
svchost.exe	8860	Services	0	6,584 KB
MoUsrCoreWorker.exe	5840	Services	0	31,724 KB
svchost.exe	17296	Services	0	11,556 KB
csrss.exe	7384	Console	4	7,316 KB
winlogon.exe	18868	Console	4	10,900 KB
fontdrvhost.exe	16408	Console	4	9,336 KB
dwm.exe	4728	Console	4	148,036 KB
gameinputsvc.exe	18376	Console	4	14,776 KB
NVDisplay.Container.exe	12156	Console	4	52,016 KB
nvcontainer.exe	12196	Console	4	29,196 KB
nvcontainer.exe	19580	Console	4	37,452 KB
sihost.exe	12108	Console	4	33,912 KB
svchost.exe	5196	Console	4	24,396 KB
igfxEM.exe	17560	Console	4	13,908 KB
svchost.exe	1460	Console	4	7,440 KB
svchost.exe	13296	Console	4	35,344 KB
LightStudioHelper.exe	8572	Console	4	52,844 KB
taskhostw.exe	17692	Console	4	21,440 KB
OverlayHelper.exe	11916	Console	4	25,260 KB
OmenInstallMonitor.exe	21272	Console	4	24,676 KB
SystemOptimizer.exe	5916	Console	4	26,880 KB
uihost.exe	10492	Console	4	25,760 KB
SynTPEnh.exe	17332	Console	4	20,984 KB
explorer.exe	14664	Console	4	251,860 KB
svchost.exe	15332	Console	4	45,820 KB
SearchHost.exe	15672	Console	4	139,356 KB
StartMenuExperienceHost.exe	7568	Console	4	94,784 KB
Widgets.exe	2216	Console	4	35,996 KB
RuntimeBroker.exe	10244	Console	4	25,728 KB
RtkAudUService64.exe	11744	Console	4	14,224 KB
RuntimeBroker.exe	11540	Console	4	57,660 KB
dllhost.exe	12904	Console	4	15,396 KB
svchost.exe	19928	Console	4	14,892 KB
dllhost.exe	13516	Console	4	17,228 KB
ctfmon.exe	16416	Console	4	24,044 KB
NVIDIA Web Helper.exe	18784	Console	4	16,612 KB
conhost.exe	15220	Console	4	1,076 KB
TextInputHost.exe	6064	Console	4	101,336 KB
OmenCommandCenterBackground.exe	19096	Console	4	213,096 KB
svchost.exe	1392	Services	0	5,500 KB
LightStudio-background.exe	20620	Console	4	96,976 KB
ShellExperienceHost.exe	1836	Console	4	80,956 KB
RuntimeBroker.exe	4160	Console	4	33,628 KB
svchost.exe	4232	Console	4	15,184 KB

LightStudio-background.exe	20620	Console	4	96,976 KB
ShellExperienceHost.exe	1836	Console	4	80,956 KB
RuntimeBroker.exe	4160	Console	4	33,628 KB
svchost.exe	4232	Console	4	15,184 KB
SystemSettingsBroker.exe	15432	Console	4	32,608 KB
PhoneExperienceHost.exe	18100	Console	4	197,716 KB
svchost.exe	20160	Console	4	8,936 KB
WidgetService.exe	18612	Console	4	22,128 KB
RuntimeBroker.exe	2812	Console	4	15,708 KB
OMENOverlay.exe	18472	Console	4	68,704 KB
HPSystemEventUtilityHost.	12240	Console	4	68,044 KB
SecurityHealthSystray.exe	10124	Console	4	10,044 KB
steam.exe	9656	Console	4	62,660 KB
nvspHelper64.exe	20380	Console	4	13,588 KB
NVIDIA Share.exe	18776	Console	4	64,684 KB
steamwebhelper.exe	18688	Console	4	179,556 KB
steamservice.exe	20696	Services	0	12,940 KB
NVIDIA Share.exe	3660	Console	4	38,184 KB
steamwebhelper.exe	9868	Console	4	13,732 KB
steamwebhelper.exe	20140	Console	4	63,672 KB
NVIDIA Share.exe	6900	Console	4	61,452 KB
steamwebhelper.exe	17960	Console	4	29,352 KB
steamwebhelper.exe	9244	Console	4	186,664 KB
RtkAudUService64.exe	3528	Console	4	16,000 KB
HPAudioSwitch.exe	18244	Console	4	40,960 KB
unsecapp.exe	18884	Console	4	8,776 KB
steamwebhelper.exe	16092	Console	4	102,368 KB
HP.JumpStarts.exe	10020	Console	4	2,464 KB
RuntimeBroker.exe	5664	Console	4	8,328 KB
RZSurroundHelper.exe	18928	Console	4	10,132 KB
jusched.exe	12320	Console	4	21,692 KB
WSHelper.exe	18524	Console	4	21,944 KB
ExpressVPNNotificationSer	8796	Console	4	46,412 KB
svchost.exe	13968	Console	4	19,256 KB
dllhost.exe	8764	Console	4	8,988 KB
SDXHelper.exe	3112	Console	4	22,340 KB
jucheck.exe	5652	Console	4	17,752 KB
MoNotificationUx.exe	9100	Console	4	11,404 KB
Discord.exe	21420	Console	4	74,864 KB
Discord.exe	3972	Console	4	26,532 KB
Discord.exe	15472	Console	4	88,472 KB
Discord.exe	2880	Console	4	45,244 KB
Discord.exe	19144	Console	4	257,332 KB
Discord.exe	13568	Console	4	64,264 KB
VirtualBox.exe	5992	Console	4	83,128 KB
VBoxSVC.exe	20952	Console	4	19,928 KB
VBoxSDS.exe	15988	Services	0	10,776 KB
SystemSettings.exe	3980	Console	4	2,180 KB
ApplicationFrameHost.exe	5484	Console	4	36,224 KB
UserOOBEBroker.exe	1620	Console	4	9,228 KB
chrome.exe	6412	Console	4	233,532 KB
chrome.exe	18752	Console	4	8,880 KB
chrome.exe	13464	Console	4	175,572 KB
chrome.exe	20048	Console	4	47,320 KB
chrome.exe	11080	Console	4	20,432 KB
chrome.exe	21160	Console	4	65,820 KB
chrome.exe	11720	Console	4	165,540 KB
chrome.exe	12620	Console	4	38,428 KB
chrome.exe	15876	Console	4	73,216 KB
chrome.exe	19028	Console	4	67,748 KB
chrome.exe	16400	Console	4	66,452 KB
chrome.exe	20896	Console	4	59,596 KB
chrome.exe	2768	Console	4	264,336 KB
cmd.exe	5732	Console	4	3,960 KB

conhost.exe	19840	Console	4	9,680 KB
browserhost.exe	11100	Console	4	12,668 KB
chrome.exe	18708	Console	4	22,016 KB
taskhostw.exe	8088	Console	4	13,968 KB
WsToastNotification.exe	16332	Console	4	14,084 KB
conhost.exe	14972	Console	4	9,576 KB
WINWORD.EXE	1452	Console	4	261,400 KB
ai.exe	18604	Console	4	22,368 KB
svchost.exe	5776	Services	0	8,516 KB
svchost.exe	11988	Services	0	12,092 KB
RuntimeBroker.exe	5036	Console	4	34,328 KB
WhatsApp.exe	2084	Console	4	995,060 KB
VirtualBoxVM.exe	15340	Console	4	8,128 KB
VirtualBoxVM.exe	14380	Console	4	5,028 KB
VirtualBoxVM.exe	1188	Console	4	4,485,292 KB
RuntimeBroker.exe	9328	Console	4	11,380 KB
chrome.exe	17752	Console	4	160,328 KB
svchost.exe	20508	Console	4	13,468 KB
audiodg.exe	6620	Services	0	30,652 KB
cmd.exe	16436	Console	4	5,640 KB
conhost.exe	20924	Console	4	9,092 KB
OpenConsole.exe	13684	Console	4	15,408 KB
WindowsTerminal.exe	9952	Console	4	84,140 KB
backgroundTaskHost.exe	19364	Console	4	5,092 KB
RuntimeBroker.exe	11248	Console	4	8,428 KB
svchost.exe	3032	Console	4	311,884 KB
chrome.exe	15136	Console	4	109,608 KB
chrome.exe	10080	Console	4	131,720 KB
chrome.exe	19396	Console	4	76,456 KB
chrome.exe	3252	Console	4	66,228 KB
chrome.exe	12704	Console	4	79,396 KB
svchost.exe	6052	Services	0	13,276 KB
SearchProtocolHost.exe	4824	Services	0	15,160 KB
svchost.exe	21184	Services	0	8,092 KB
backgroundTaskHost.exe	13876	Console	4	14,268 KB
RuntimeBroker.exe	3008	Console	4	9,952 KB
RuntimeBroker.exe	11288	Console	4	19,648 KB
SearchFilterHost.exe	13676	Services	0	9,576 KB
WmiPrvSE.exe	15804	Services	0	12,592 KB
chrome.exe	14952	Console	4	48,824 KB
chrome.exe	1776	Console	4	29,124 KB
tasklist.exe	4440	Console	4	9,816 KB
WmiPrvSE.exe	6776	Services	0	11,424 KB

### 13.- Utilizar el comando taskkill

```
C:\Users\irvin>taskkill /pid 2084
Correcto: se envió la señal de término al proceso con PID 2084.

C:\Users\irvin>
```

### 14.- Utilizar el comando tracert

```
PS C:\Users\irvin> tracert google.com
```

```
Traza a la dirección google.com [64.233.185.138]  
sobre un máximo de 30 saltos:
```

1	1 ms	<1 ms	<1 ms	172.16.128.1
2	1 ms	1 ms	<1 ms	192.168.109.1
3	5 ms	7 ms	3 ms	fixed-187-188-58-130.totalplay.net [187.188.58.130]
4	3 ms	4 ms	7 ms	10.180.58.1
5	22 ms	17 ms	17 ms	72.14.242.148
6	25 ms	18 ms	160 ms	192.178.74.85
7	18 ms	19 ms	20 ms	108.170.249.2
8	20 ms	18 ms	19 ms	142.250.213.95
9	38 ms	43 ms	43 ms	142.251.51.128
10	30 ms	31 ms	30 ms	142.251.51.106
11	34 ms	33 ms	33 ms	216.239.48.63
12	*	*	*	Tiempo de espera agotado para esta solicitud.
13	*	*	*	Tiempo de espera agotado para esta solicitud.
14	*	*	*	Tiempo de espera agotado para esta solicitud.
15	*	*	*	Tiempo de espera agotado para esta solicitud.
16	*	*	*	Tiempo de espera agotado para esta solicitud.
17	*	*	*	Tiempo de espera agotado para esta solicitud.
18	*	*	*	Tiempo de espera agotado para esta solicitud.
19	*	*	*	Tiempo de espera agotado para esta solicitud.
20	*	*	*	Tiempo de espera agotado para esta solicitud.
21	30 ms	32 ms	31 ms	yb-in-f138.1e100.net [64.233.185.138]

```
Traza completa.
```

15. Utilizar el comando ARP

```
PS C:\Users\irvin> arp -a
```

```
Interfaz: 172.16.128.3 --- 0x3
```

Dirección de Internet	Dirección física	Tipo
172.16.128.1	00-0c-e6-f5-d8-73	dinámico
172.16.129.120	ec-5c-68-11-fa-3f	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 --- 0x6
```

Dirección de Internet	Dirección física	Tipo
192.168.56.255	ff-ff-ff-ff-ff-ff	estático
224.0.0.22	01-00-5e-00-00-16	estático
224.0.0.251	01-00-5e-00-00-fb	estático
224.0.0.252	01-00-5e-00-00-fc	estático
239.255.255.250	01-00-5e-7f-ff-fa	estático
255.255.255.255	ff-ff-ff-ff-ff-ff	estático

```
PS C:\Users\irvin>
```



**B) Contesta con tus propias palabras las siguientes preguntas:**

**1.- ¿Para que sirve el comando ping?**

El comando ping a mi parecer sirve para poder hacer un diagnostico de la red del equipo para poder localizar posibles problemas que se presenten en el intercambio de información/paquetes y solucionarlos.

**2.- ¿Para que sirve el comando nslookup?**

Para obtener toda la información relación con el DNS de los dominios solicitados.

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

Para verificar todas las conexiones que tiene mi computadoras y los puertos que tiene disponible.

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

El tasklist muestra todos los procesos y servicios que se están ejecutando al momento de hacer el comando.

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

El taskkill lo que hace es detener uno de los servicios o procesos que se estén ejecutando en el momento.

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

El comando tracert hace un seguimiento del paquete que se esta mandando desde la computadora hasta la dirección final, lanzando las estadísticas de cada salto.

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

Estos 3 combinados nos ayudan a tener toda la información completa de las conexiones de nuestra computadora por lo que tenemos acceso a la información completa y aun diagnostico más detallado.

**C) Investigar los siguientes comandos y anota ejemplos prácticos:**

**BITSADMIN**

Sirve entre otras cosas para realizar descargas en segundo plano

Crear una nueva tarea:

Para crear una nueva tarea de transferencia de archivos, usa el siguiente comando:

```
bitsadmin /create myDownloadJob
```

Esto crea una nueva tarea llamada "myDownloadJob" que estará lista para la configuración.

Agregar archivos para descargar:

A continuación, usa el siguiente comando para agregar el archivo que deseas descargar a la tarea:

```
bitsadmin /addfile myDownloadJob URL-del-archivo ruta-de-guardado
```

URL-del-archivo es la URL del archivo que deseas descargar.

ruta-de-guardado es la ubicación en la que deseas guardar el archivo descargado.

Ejemplo:

```
bitsadmin /addfile myDownloadJob http://example.com/archivo.zip C:\Descargas\archivo.zip
```

Iniciar la tarea de transferencia:

Una vez que hayas agregado los archivos, inicia la tarea con el siguiente comando:

```
bitsadmin /resume myDownloadJob
```

Monitorear el progreso:

Puedes verificar el progreso de la tarea con el comando:

```
bitsadmin /list /verbose
```

Esto mostrará el estado de todas las tareas BITS, incluida la que acabas de crear.

Finalizar la tarea:

Cuando la descarga esté completa, puedes finalizar la tarea con:

```
bitsadmin /complete myDownloadJob
```

## **FTP**

Transfiere archivos hacia y desde una computadora que ejecuta un servicio de servidor de Protocolo de transferencia de archivos (FTP). Este comando se puede utilizar de forma interactiva o por lotes procesando archivos de texto ASCII.

```
ftp ftp.microsoft.com
```

Conectado a ftp.microsoft.com.

220 cpmsftftpa03 Microsoft FTP Service (Version 5.0).

Usuario (ftp.microsoft.com:(none)): anonymous

331 Anonymous access allowed, send identity (e-mail name) as password.

Contraseña:<strong>\*\*\*\*\*</strong>

230-This is FTP.MICROSOFT.COM. Please see the

230-dirmap.txt for more information.

230 Anonymous user logged in.

## GETMAC

Obtiene las direcciones MAC (Media Access Control) que tienen asociadas a los adaptadores de red.

C:\Users\irvin>getmac

Dirección física    Nombre de transporte

=====

00-FF-5C-F7-1B-F9    Medios desconectados

DC-41-A9-67-BC-54    \Device\Tcpip\_{08ADFFDA-A639-4613-9EEA-9C8189882752}

30-24-A9-82-B9-5E    Desconectado

0A-00-27-00-00-06    \Device\Tcpip\_{5ACA5D24-831A-4E2B-A164-BD5A1B6BD78E}

## NBTSTAT

Muestra las estadísticas del protocolo NetBIOS sobre TCP/IP (NETBT), las tablas de nombres NetBIOS para la computadora local, las computadoras remotas y la caché.

Este comando está disponible solo si el Protocolo de Internet (TCP/IP) está instalado como un componente en las propiedades de un adaptador de red en Conexiones de red.

C:\Users\irvin>nbtstat /S 5

Ethernet 3:

Dirección IP del nodo: [192.168.56.1] Id. de ámbito : []

    No hay conexiones

Ethernet 2:

Dirección IP del nodo: [0.0.0.0] Id. de ámbito : []

    No hay conexiones

Ethernet:

Dirección IP del nodo: [0.0.0.0] Id. de ámbito : []

No hay conexiones

Wi-Fi:

Dirección IP del nodo: [172.16.128.3] Id. de ámbito : []

No hay conexiones

Conexión de área local\* 3:

Dirección IP del nodo: [0.0.0.0] Id. de ámbito : []

No hay conexiones

Conexión de área local\* 4:

Dirección IP del nodo: [0.0.0.0] Id. de ámbito : []

No hay conexiones

Ethernet 3:

Dirección IP del nodo: [192.168.56.1] Id. de ámbito : []

No hay conexiones

Ethernet 2:

Dirección IP del nodo: [0.0.0.0] Id. de ámbito : []

No hay conexiones

Ethernet:

Dirección IP del nodo: [0.0.0.0] Id. de ámbito : []

No hay conexiones

Wi-Fi:

Dirección IP del nodo: [172.16.128.3] Id. de ámbito : []

No hay conexiones

Conexión de área local\* 3:

Dirección IP del nodo: [0.0.0.0] Id. de ámbito : []

No hay conexiones

Conexión de área local\* 4:

Dirección IP del nodo: [0.0.0.0] Id. de ámbito : []

No hay conexiones

HOSTNAME

Muestra el nombre del host.

```
C:\Users\irvin>hostname  
LAPTOP-HKSHACEU
```

## NET

El comando net se utiliza para varias acciones relacionadas con las redes y servicios.

Agregar un nuevo usuario:

```
net user nombre_usuario contraseña /add
```

## NET USE

Este comando net use es una instrucción que se utiliza para conectarse, eliminar y configurar conexiones a recursos compartidos, como unidades asignadas e impresoras de red.

Ejemplo:

```
net use Z: \\192.168.1.100\CompartidoDocs /user:nombre_usuario contraseña
```

## NETSH

La utilidad de secuencia de comandos de la línea de comandos Network Shell que le permite, ya sea de forma local o remota, mostrar o modificar la configuración de red de una computadora en ejecución.

Restablecer la pila TCP / IP con Netsh

Un uso común de los comandos Netsh es el restablecimiento de la pila TCP/IP que maneja el intercambio de paquetes de datos en las redes. Si aparecen problemas en la red y en Internet, esta medida puede ser de utilidad, ya que elimina, por ejemplo, los defectos o la configuración incorrecta de protocolos TCP/IP. El siguiente comando de reparación realiza un restablecimiento y reinstala el TCP/IPv4:

```
netsh int ip reset
```

También puede crearse un archivo de registro que documente los cambios realizados:

```
netsh int ip reset c:\tcpipreset.txt
```

Después del restablecimiento, es preciso reiniciar el ordenador.

Una de las instrucciones que personalmente uso, es la siguiente:

```
netsh wlan show profile name="FullDevOps" key=clear
```

Investiga absolutamente todo, la línea de arriba orienta al sistema a mostrar todos aquellos perfiles de red con nombre “FullDevOps” y buscó la clave de la red donde se encuentra conectado.

## **PATHPING**

Este comando proporciona información sobre la latencia de red y la pérdida en saltos intermedios entre un origen y un destino. Este comando envía varios mensajes de solicitud de eco a cada enrutador entre un origen y un destino, durante un período de tiempo, y luego calcula los resultados en función de los paquetes devueltos por cada enrutador.

Ejemplo:

```
C:\Users\irvin>pathping openwebinars.net
```

Seguimiento de ruta a openwebinars.net [198.199.125.132]

sobre un máximo de 30 saltos:

```
0  LAPTOP-HKSHACEU [172.16.128.3]
1  172.16.128.1
2  192.168.109.1
3  fixed-187-188-58-130.totalplay.net [187.188.58.130]
4  10.180.58.1
5  81.173.106.145
6  94.142.107.213
7  rest-bb1-link.ip.twelve99.net [62.115.119.230]
8  nyk-bb1-link.ip.twelve99.net [62.115.141.245]
9  *      *      *
```

Procesamiento de estadísticas durante 200 segundos...

## **ROUTE**

Ver la tabla de enrutamiento:

Para ver la tabla de enrutamiento actual en tu sistema, simplemente escribe:

```
route print
```

Esto mostrará una lista de rutas y sus métricas, lo que te permite ver cómo se enrutan los paquetes en tu red.

Añadir una ruta estática:

Puedes agregar manualmente una entrada a la tabla de enrutamiento utilizando el comando route add. Por ejemplo:

```
route add 192.168.1.0 mask 255.255.255.0 192.168.0.1
```

Esto agrega una ruta estática para la red 192.168.1.0 con una máscara de subred de 255.255.255.0 a través del gateway 192.168.0.1.

Eliminar una ruta estática:

Si deseas eliminar una ruta estática específica de la tabla de enrutamiento, puedes utilizar el comando route delete. Por ejemplo:

```
route delete 192.168.1.0
```

Esto eliminará la ruta estática para la red 192.168.1.0.

Modificar una ruta:

Para modificar una ruta estática existente, puedes utilizar el comando route change. Por ejemplo:

```
route change 192.168.1.0 mask 255.255.255.0 192.168.0.2
```

Esto cambiará la ruta existente para que los paquetes se enruten a través del gateway 192.168.0.2 en lugar de 192.168.0.1.

## **TELNET**

Abrir comunicación con un equipo remoto que ejecuta el servicio del servidor telnet.

Importante: debe instalar el software de cliente telnet antes de poder ejecutar este comando.

Para usar telnet para conectarse a la computadora que ejecuta el servicio del servidor telnet en telnet.microsoft.com , escriba:

```
telnet telnet.microsoft.com
```

Para usar telnet para conectarse a la computadora que ejecuta el servicio del servidor telnet en telnet.microsoft.com en el puerto TCP 44 y registrar la actividad de la sesión en un archivo local llamado telnetlog.txt :

```
telnet /f telnetlog.txt telnet.microsoft.com 44
```