# UNIVERSIDAD POLITÉCNICA DE QUINTANA ROO

Actividad: Tarea #987

SISTEMAS OPERATIVOS

Alumna: Tzuc Vázquez Ariana Patricia

7° CUATRIMESTRE. GRUPO:27BV.

DOCENTE: ISMAEL JIMÉNEZ SÁNCHEZ

## Contenido

Comandos	1
Preguntas	16
Investigación	17

## **Comandos**

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

Obtener la ayuda del comando ping
 Simplemente escribe el comando ping y presiona la tecla Enter o ping /? Para obtener información más detallada sobre cómo usar el comando ping y todas sus opciones.

```
C:\Users\arian>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:
                     Hacer ping al host especificado hasta que se detenga.
 -t
                     Para ver estadísticas y continuar, presione
                     Ctrl-Interrumpir; para detener, presione Ctrl+C.
                     Resolver direcciones en nombres de host.
                     Número de solicitudes de eco para enviar.
 -n count
 -l size
                     Enviar tamaño de búfer.
 -f
                     Establecer marca No fragmentar en paquetes (solo IPv4).
 -i TTL
                     Período de vida.
                     Tipo de servicio (solo IPv4. Esta opción está desusada y
 -v TOS
                     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.
                     Enrutamiento del identificador del compartimiento.
    -c compartment
                     Hacer ping a la dirección del proveedor de Virtualización
                     de red de Hyper-V.
                     Forzar el uso de IPv4.
    -4
                     Forzar el uso de IPv6.
```

```
C:\Users\arian>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.
                     Resolver direcciones en nombres de host.
                     Número de solicitudes de eco para enviar.
 -n count
 -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).
                     Ruta de origen estricta para lista-host (solo IPv4).
-k host-list
                     Tiempo de espera en milisegundos para cada respuesta.
 -w timeout
 -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.
   -р
                     Hacer ping a la dirección del proveedor de Virtualización
                     de red de Hyper-V.
    -4
                     Forzar el uso de IPv4.
    -6
                     Forzar el uso de IPv6.
```

## 2. Enviar un ping a 127.0.0.1 aplicando cualquier parámetro

```
C:\Users\arian>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

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
```

## Con parámetro -t:

```
C:\Users\arian>ping -t 127.0.0.1
Haciendo ping a 127.0.0.1 con 32 bytes de datos:
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Estadísticas de ping para 127.0.0.1:
    Paguetes: enviados = 21, recibidos = 21, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
   Mínimo = Oms, Máximo = Oms, Media = Oms
Control-C
^C
```

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

```
C:\Users\arian>ping www.google.com

Haciendo ping a www.google.com [192.178.52.132] con 32 bytes de datos:
Respuesta desde 192.178.52.132: bytes=32 tiempo=148ms TTL=114
Respuesta desde 192.178.52.132: bytes=32 tiempo=72ms TTL=114
Respuesta desde 192.178.52.132: bytes=32 tiempo=71ms TTL=114
Respuesta desde 192.178.52.132: bytes=32 tiempo=72ms TTL=114

Estadísticas de ping para 192.178.52.132:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 71ms, Máximo = 148ms, Media = 90ms
```

Tuvo una buena respuesta, se enviaron y recibieron todos los paquetes y no hubo pérdida de paquetes.

4. Obtener la ayuda del comando nslookup

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

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

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

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

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

Haciendo ping a 192.168.100.1 con 32 bytes de datos:
Respuesta desde 192.168.100.1: bytes=32 tiempo=1ms TTL=63
Respuesta desde 192.168.100.1: bytes=32 tiempo=1ms TTL=63
Respuesta desde 192.168.100.1: bytes=32 tiempo=2ms TTL=63
Respuesta desde 192.168.100.1: bytes=32 tiempo=1ms TTL=63

Estadísticas de ping para 192.168.100.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 2ms, Media = 1ms
```

Tuvo una buena respuesta, se enviaron y recibieron todos los paquetes y no hubo pérdida de paquetes.

7. Obtener la ayuda del comando netstat

```
C:\Users\arian>metstat /?

Ruestra estadisticas 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 asi 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 estadisticas 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 el tiempo gastado por una conexión TCP en su estado actual.
-n Muestra el did. 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, TCPyG, UDP o UDPyG. Si se usa con la opción -s para mostrar estadisticas por protocolo, petolo puede ser cualquiera de los siguientes: TP, UDP, TCPyG, UDP o UDPyG.
-q Muestra conexiones para el protocolo puedo pende ser cualquiera de los siguientes: TP, UDP, TCPyG, UDP o UDPyG.
-q Muestra la tabla de enutramiento.
-r Muestra la estadó de descarga de la conexión actual.
-r Muestra la estado de descarga de la conexión actual.
-r Muestra la estado de descarga de la conexión actual.
-r Muestra la estado de deceacra de la
```

```
-y Muestra la plantilla de conexión TCP para todas las conexiones.
No se puede combinar con otras opciones.
interval Vuelve a mostrar las estadísticas seleccionadas y realiza pausas en intervalos de varios segundos entre cada visualización. Presiona Ctrl+C para que dejen de volver a mostrarse las estadísticas. Si se omite, netstat mostrará la información de configuración una vez.
```

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

C:\Users\arian>netstat -a						
Conexion	Conexiones activas					
Proto	Dirección local	Dirección remota	Estado			
TCP	0.0.0.0:135	Ari:0	LISTENING			
TCP	0.0.0.0:445	Ari:0	LISTENING			
TCP	0.0.0.0:1042	Ari:0	LISTENING			
TCP	0.0.0.0:1043	Ari:0	LISTENING			
TCP	0.0.0.0:5040	Ari:0	LISTENING			
TCP	0.0.0.0:6646	Ari:0	LISTENING			
TCP	0.0.0.0:9012	Ari:0	LISTENING			
TCP	0.0.0.0:9013	Ari:0	LISTENING			
TCP	0.0.0.0:49664	Ari:0	LISTENING			
TCP	0.0.0.0:49665	Ari:0	LISTENING			
TCP	0.0.0.0:49666	Ari:0	LISTENING			
TCP	0.0.0.0:49667	Ari:0	LISTENING			
TCP	0.0.0.0:49668	Ari:0	LISTENING			
TCP	0.0.0.0:49671	Ari:0	LISTENING			
TCP	127.0.0.1:1042	Ari:49717	ESTABLISHED			
TCP	127.0.0.1:1042	Ari:49719	ESTABLISHED			
TCP	127.0.0.1:4699	Ari:0	LISTENING			
TCP	127.0.0.1:6463	Ari:0	LISTENING			
TCP	127.0.0.1:13010	Ari:0	LISTENING			
TCP	127.0.0.1:13030	Ari:0	LISTENING			
TCP	127.0.0.1:13030	Ari:49670	ESTABLISHED			
TCP	127.0.0.1:13031	Ari:0	LISTENING			
TCP	127.0.0.1:13032	Ari:0	LISTENING			
TCP	127.0.0.1:17532	Ari:0	LISTENING			
TCP	127.0.0.1:17532	Ari:49696	ESTABLISHED			
TCP	127.0.0.1:17945	Ari:0	LISTENING			
TCP	127.0.0.1:22112	Ari:0	LISTENING			
TCP	127.0.0.1:49670	Ari:13030	ESTABLISHED			
TCP	127.0.0.1:49696	Ari:17532	ESTABLISHED			
TCP	127.0.0.1:49717	Ari:1042	ESTABLISHED			
TCP	127.0.0.1:49719	Ari:1042	ESTABLISHED			
TCP	127.0.0.1:54135	Ari:54136	ESTABLISHED			
TCP	127.0.0.1:54136	Ari:54135	ESTABLISHED			
TCP	127.0.0.1:54137	Ari:54138	ESTABLISHED			

```
TCP
       127.0.0.1:49717
                               Ari:1042
                                                       ESTABLISHED
TCP
       127.0.0.1:49719
                               Ari:1042
                                                       ESTABLISHED
TCP
       127.0.0.1:54135
                               Ari:54136
                                                       ESTABLISHED
TCP
       127.0.0.1:54136
                               Ari:54135
                                                        ESTABLISHED
TCP
       127.0.0.1:54137
                               Ari:54138
                                                        ESTABLISHED
TCP
       127.0.0.1:54138
                               Ari:54137
                                                       ESTABLISHED
TCP
       169.254.85.122:139
                               Ari:0
                                                       LISTENING
TCP
       192.168.1.124:139
                               Ari:0
                                                       LISTENING
TCP
       192.168.1.124:49422
                               20.10.31.115:https
                                                        ESTABLISHED
TCP
       192.168.1.124:54318
                               20.7.1.246:https
                                                        ESTABLISHED
TCP
       192.168.1.124:54379
                               162.159.133.234:https
                                                       ESTABLISHED
TCP
       192.168.1.124:54393
                               192.168.1.119:8009
                                                        ESTABLISHED
TCP
       192.168.1.124:54407
                               ec2-3-211-37-212:https
                                                        ESTABLISHED
TCP
       192.168.1.124:54411
                               ec2-52-71-10-36:https
                                                       ESTABLISHED
TCP
       192.168.1.124:54414
                               uh-in-f190:https
                                                        ESTABLISHED
TCP
       192.168.1.124:54419
                               ec2-44-195-236-12:https
                                                         ESTABLISHED
TCP
       192.168.1.124:54540
                               a23-64-121-169:https
                                                       CLOSE_WAIT
TCP
       192.168.1.124:54643
                               ac9293e5fb5d2d1d2:5222
                                                        ESTABLISHED
TCP
       192.168.1.124:54734
                               ec2-18-214-45-220:https
                                                         CLOSE_WAIT
TCP
       192.168.1.124:54735
                               ec2-3-208-216-240:https
                                                         CLOSE_WAIT
       192.168.1.124:54736
TCP
                               20.42.65.84:https
                                                        TIME_WAIT
       192.168.1.124:54738
                               40.79.141.153:https
                                                        TIME_WAIT
TCP
TCP
       192.168.1.124:54739
                               52.109.12.12:https
                                                        TIME_WAIT
TCP
       192.168.1.124:54740
                               55:https
                                                       TIME_WAIT
TCP
       192.168.1.124:54741
                               55:https
                                                       ESTABLISHED
TCP
       192.168.1.124:54742
                               209:https
                                                        TIME_WAIT
TCP
       192.168.1.124:54744
                               dns:https
                                                        ESTABLISHED
TCP
       192.168.1.124:54745
                               13.89.178.26:https
                                                        ESTABLISHED
TCP
       192.168.1.124:54747
                               40.79.141.153:https
                                                        TIME_WAIT
TCP
       192.168.1.124:54749
                               ec2-3-13-175-152:https
                                                        ESTABLISHED
TCP
       192.168.1.124:54751
                               ec2-3-129-123-235:https
                                                         ESTABLISHED
TCP
       192.168.1.124:54752
                               ec2-3-129-123-235:https
                                                         ESTABLISHED
       192.168.1.124:54754
TCP
                               52.109.12.12:https
                                                        ESTABLISHED
TCP
       [::]:135
                               Ari:0
                                                       LISTENING
TCP
       [::]:445
                               Ari:0
                                                       LISTENING
TCP
       [::]:1042
                               Ari:0
                                                       LISTENING
       [::]:1043
TCP
                               Ari:0
                                                       LISTENING
TCP
       [::]:9012
                               Ari:0
                                                       LISTENING
TCP
       [::]:9013
                               Ari:0
                                                       LISTENING
TCP
       [::]:49664
                               Ari:0
                                                       LISTENING
```

```
TCP
       [::]:1043
                                Ari:0
                                                         LISTENING
TCP
       [::]:9012
                                Ari:0
                                                         LISTENING
                                Ari:0
TCP
       [::]:9013
                                                         LISTENING
       [::]:49664
TCP
                                Ari:0
                                                         LISTENING
TCP
       [::]:49665
                                Ari:0
                                                         LISTENING
TCP
       [::]:49666
                                Ari:0
                                                         LISTENING
TCP
       [::]:49667
                                                         LISTENING
                                Ari:0
TCP
       [::]:49668
                                Ari:0
                                                         LISTENING
TCP
       [::]:49671
                                Ari:0
                                                         LISTENING
       [::1]:4699
TCP
                                Ari:0
                                                         LISTENING
       [::1]:49669
TCP
                                Ari:0
                                                        LISTENING
UDP
       0.0.0.0:123
                                *:*
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
       0.0.0.0:5355
                                *:*
UDP
       0.0.0.0:6646
                                *:*
UDP
       127.0.0.1:1900
                                *:*
UDP
       127.0.0.1:51244
                                127.0.0.1:51244
UDP
       127.0.0.1:57607
                                *:*
UDP
       169.254.85.122:137
                                *:*
UDP
       169.254.85.122:138
                                *:*
UDP
       169.254.85.122:1900
                                *:*
UDP
       169.254.85.122:57605
                                *:*
       192.168.1.124:137
UDP
                                *:*
UDP
       192.168.1.124:138
                                *:*
UDP
       192.168.1.124:1900
                                *:*
UDP
       192.168.1.124:57606
                                *:*
UDP
       [::]:123
                                *:*
UDP
       [::]:500
                                *:*
UDP
       [::]:4500
                                *:*
UDP
       [::]:5353
                                *:*
UDP
       [::]:5355
                                *:*
UDP
       [::1]:1900
                                *:*
       [::1]:57604
UDP
                                *:*
UDP
       [fe80::13fa:bc38:3516:7a5e%4]:1900
                                              *:*
UDP
       [fe80::13fa:bc38:3516:7a5e%4]:57602 *:*
UDP
       [fe80::ae35:2b6c:b3fc:45e%14]:1900 *:*
UDP
       [fe80::ae35:2b6c:b3fc:45e%14]:57603 *:*
```

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

```
C:\Users\arian>netstat -n
Conexiones activas
  Proto
         Dirección local
                                 Dirección remota
                                                          Estado
 TCP
         127.0.0.1:1042
                                 127.0.0.1:49717
                                                          ESTABLISHED
         127.0.0.1:1042
                                 127.0.0.1:49719
                                                          ESTABLISHED
 TCP
 TCP
         127.0.0.1:13030
                                 127.0.0.1:49670
                                                          ESTABLISHED
 TCP
         127.0.0.1:17532
                                 127.0.0.1:49696
                                                          ESTABLISHED
 TCP
         127.0.0.1:49670
                                 127.0.0.1:13030
                                                          ESTABLISHED
 TCP
         127.0.0.1:49696
                                 127.0.0.1:17532
                                                          ESTABLISHED
 TCP
         127.0.0.1:49717
                                 127.0.0.1:1042
                                                          ESTABLISHED
 TCP
         127.0.0.1:49719
                                 127.0.0.1:1042
                                                          ESTABLISHED
 TCP
         127.0.0.1:54135
                                 127.0.0.1:54136
                                                          ESTABLISHED
 TCP
         127.0.0.1:54136
                                 127.0.0.1:54135
                                                          ESTABLISHED
 TCP
         127.0.0.1:54137
                                 127.0.0.1:54138
                                                          ESTABLISHED
 TCP
         127.0.0.1:54138
                                 127.0.0.1:54137
                                                          ESTABLISHED
 TCP
         192.168.1.124:49422
                                 20.10.31.115:443
                                                          ESTABLISHED
 TCP
         192.168.1.124:54318
                                 20.7.1.246:443
                                                          ESTABLISHED
 TCP
                                 162.159.133.234:443
         192.168.1.124:54379
                                                          ESTABLISHED
 TCP
         192.168.1.124:54393
                                 192.168.1.119:8009
                                                          ESTABLISHED
 TCP
         192.168.1.124:54407
                                 3.211.37.212:443
                                                          ESTABLISHED
 TCP
         192.168.1.124:54411
                                 52.71.10.36:443
                                                          ESTABLISHED
 TCP
         192.168.1.124:54414
                                 142.250.98.190:443
                                                          ESTABLISHED
 TCP
         192.168.1.124:54419
                                 44.195.236.12:443
                                                          ESTABLISHED
 TCP
         192.168.1.124:54540
                                 23.64.121.169:443
                                                          CLOSE_WAIT
 TCP
         192.168.1.124:54643
                                 3.33.252.61:5222
                                                          ESTABLISHED
 TCP
         192.168.1.124:54741
                                 34.117.65.55:443
                                                          ESTABLISHED
 TCP
         192.168.1.124:54764
                                 13.107.42.12:443
                                                          ESTABLISHED
 TCP
         192.168.1.124:54765
                                 40.79.141.153:443
                                                          ESTABLISHED
         192.168.1.124:54767
                                                          TIME_WAIT
 TCP
                                 3.13.175.152:443
 TCP
         192.168.1.124:54769
                                 34.117.237.239:443
                                                          TIME_WAIT
 TCP
         192.168.1.124:54771
                                 52.109.12.12:443
                                                          ESTABLISHED
                                 35.171.118.249:443
                                                          TIME_WAIT
 TCP
         192.168.1.124:54775
 TCP
         192.168.1.124:54776
                                 3.220.180.121:443
                                                          ESTABLISHED
 TCP
         192.168.1.124:54777
                                 34.207.38.86:443
                                                          ESTABLISHED
 TCP
         192.168.1.124:54778
                                 34.207.38.86:443
                                                          ESTABLISHED
 TCP
         192.168.1.124:54779
                                 34.207.38.86:443
                                                          ESTABLISHED
  TCP
         192.168.1.124:54780
                                 3.13.175.152:443
                                                          ESTABLISHED
                                                          TIME_WAIT
         192.168.1.124:54781
                                 52.109.0.140:443
```

10. Mostrar las conexiones TCP

#### C:\Users\arian>netstat -t Conexiones activas Proto Dirección local Dirección remota Estado Estado de descarga TCP 127.0.0.1:1042 Ari:49717 **ESTABLISHED** EnHost **TCP** 127.0.0.1:1042 Ari:49719 **ESTABLISHED** EnHost **TCP** Ari:49670 **ESTABLISHED** 127.0.0.1:13030 EnHost TCP 127.0.0.1:17532 Ari:49696 **ESTABLISHED** EnHost TCP 127.0.0.1:49670 Ari:13030 **ESTABLISHED** EnHost 127.0.0.1:49696 Ari:17532 **TCP ESTABLISHED** EnHost **TCP** 127.0.0.1:49717 Ari:1042 **ESTABLISHED** EnHost TCP **ESTABLISHED** 127.0.0.1:49719 Ari:1042 EnHost **TCP** 127.0.0.1:54135 Ari:54136 **ESTABLISHED** EnHost EnHost **TCP** 127.0.0.1:54136 Ari:54135 **ESTABLISHED ESTABLISHED TCP** 127.0.0.1:54137 Ari:54138 EnHost **ESTABLISHED TCP** 127.0.0.1:54138 Ari:54137 EnHost TCP 192.168.1.124:49422 20.10.31.115:https **ESTABLISHED** EnHost **TCP** 192.168.1.124:54318 20.7.1.246:https **ESTABLISHED** EnHost 162.159.133.234:https **TCP** 192.168.1.124:54379 **ESTABLISHED** EnHost TCP 192.168.1.124:54393 192.168.1.119:8009 **ESTABLISHED** EnHost TCP 192.168.1.124:54407 ec2-3-211-37-212:https ESTABLISHED EnHost ec2-52-71-10-36:https ESTABLISHED **TCP** 192.168.1.124:54411 EnHost 192.168.1.124:54414 **TCP** uh-in-f190:https **ESTABLISHED** EnHost 192.168.1.124:54419 **TCP** ec2-44-195-236-12:https ESTABLISHED EnHost TCP a23-64-121-169:https CLOSE\_WAIT 192.168.1.124:54540 EnHost **TCP** 192.168.1.124:54643 ac9293e5fb5d2d1d2:5222 ESTABLISHED EnHost **TCP** 192.168.1.124:54764 1drv:https TIME\_WAIT EnHost 192.168.1.124:54765 40.79.141.153:https TCP TIME\_WAIT EnHost 239:https TIME\_WAIT TIME\_WAIT **TCP** 192.168.1.124:54769 EnHost TCP 192.168.1.124:54771 52.109.12.12:https EnHost **TCP** 192.168.1.124:54775 EnHost ec2-3-220-180-121:https CLOSE\_WAIT **TCP** 192.168.1.124:54776 EnHost **TCP** ec2-34-207-38-86:https 192.168.1.124:54777 CLOSE\_WAIT EnHost ec2-34-207-38-86:https TCP 192.168.1.124:54778 CLOSE\_WAIT EnHost CLOSE\_WAIT **TCP** 192.168.1.124:54779 ec2-34-207-38-86:https EnHost **TCP** 192.168.1.124:54780 ec2-3-13-175-152:https ESTABLISHED EnHost TIME\_WAIT **TCP** 192.168.1.124:54781 52.109.0.140:https EnHost **TCP** 192.168.1.124:54782 **ESTABLISHED** EnHost 55:https **TCP** 192.168.1.124:54783 **ESTABLISHED** EnHost 55:https **TCP** 192.168.1.124:54784 209:https **ESTABLISHED** EnHost 192.168.1.124:54785 EnHost TCP 1drv:https **ESTABLISHED TCP** 192.168.1.124:54786 40.79.141.153:https EnHost **ESTABLISHED** TCP 192.168.1.124:54787 52.109.12.1:https **ESTABLISHED** EnHost

## 11. Mostrar las conexiones UDP

```
::\Users\arian>netstat -u
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]
                                              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 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.
                                               Muestra estadísticas de Ethernet. Esto se puede combinar con la
                                              opción -s.
Muestra nombres de dominio completos (FQDN) para direcciones
                                            externas.

Muestra el tiempo gastado por una conexión TCP en su estado actual.

Muestra direcciones y números de puerto en formato numérico.

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

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.

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.

Muestra la tabla de enrutamiento.
      -p proto
      -q
                                              Muestra la tabla de enrutamiento.

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. Muestra el estado de descarga de la conexión actual.

Muestra conexiones, agentes de escucha y extremos compartidos de Naturolizact.
                                               de NetworkDirect.
                                               Muestra la plantilla de conexión TCP para todas las conexiones.
                                              nuestra la plantita de conexión (CP para todas las conexiónes.)
No se puede combinar con otras opciones.
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.
      interval
```

## 12. Utilizar el comando tasklist

C:\Users\arian>tasklist				
Nombre de imagen		Nombre de sesión		
System Idle Process		Services	 0	
System	4	Services	Θ	3,012 KB
Secure System	140	Services	Θ	
Registry	180	Services	0	
smss.exe	680	Services	Θ	
csrss.exe	732	Services	0	
wininit.exe	1084	Services	0	
csrss.exe	1104	Console	1	
services.exe	1156	Services	Θ	8,224 KB
LsaIso.exe	1172	Services	0	2,216 KB
lsass.exe	1192	Services	Θ	21,384 KB
svchost.exe	1308	Services	Θ	23,052 KB
fontdrvhost.exe	1336	Services	Θ	1,804 KB
WUDFHost.exe	1372	Services	Θ	4,000 KB
svchost.exe	1468	Services	Θ	16,452 KB
svchost.exe	1516	Services	Θ	5,752 KB
WUDFHost.exe	1556	Services	Θ	12,984 KB
winlogon.exe	1640	Console	1	6,780 KB
fontdrvhost.exe	1688	Console	1	5,836 KB
dwm.exe	1776	Console	1	216,232 KB
svchost.exe	1832	Services	Θ	
svchost.exe	1840	Services	Θ	
svchost.exe	1848	Services	Θ	
svchost.exe	2000	Services	Θ	
svchost.exe	2036	Services	Θ	
svchost.exe	2044	Services	Θ	
svchost.exe	828	Services	Θ	6,600 KB
svchost.exe	860	Services	0	
svchost.exe	816	Services	0	10,868 KB
svchost.exe	2120	Services	0	
svchost.exe		Services	0	
svchost.exe	2148	Services	0	
svchost.exe		Services	0	
IntelCpHDCPSvc.exe	2236	Services	0	
svchost.exe		Services	0	
svchost.exe		Services	0	5,120 KB
svchost.exe		Services	0	
svchost.exe	2516	Services	0	
svchost.exe	2536	Services	0	
svchost.exe		Services	0	
svchost.exe		Services	0	,
svchost.exe		Services	9	8,952 KB
svchost.exe		Services	0	6.980 KB

				0.050.110
svchost.exe		Services	0	8,952 KB
svchost.exe		Services	0	6,980 KB
svchost.exe		Services	0	6,740 KB
svchost.exe		Services	0	8,432 KB
		Services	0	14,512 KB
svchost.exe		Services	0	18,920 KB
WUDFHost.exe		Services	0	6,812 KB
AsusCertService.exe		Services	0	7,484 KB
svchost.exe	3520	Services	0	15,896 KB
svchost.exe	3580	Services	0	5,412 KB
svchost.exe	3728	Services	0	5,308 KB
svchost.exe	3736	Services	Θ	6,240 KB
svchost.exe	3744	Services	Θ	6,620 KB
Memory Compression	3828	Services	0	96,704 KB
	3868	Services	0	7,308 KB
igfxCUIServiceN.exe	3920	Services	0	8,096 KB
svchost.exe	3964	Services	0	7,772 KB
svchost.exe		Services	Θ	7,784 KB
svchost.exe		Services	0	13,104 KB
svchost.exe		Services	0	6,156 KB
NVDisplay.Container.exe		Console	1	29,004 KB
svchost.exe	4252	Services	0	18,028 KB
svchost.exe		Services	0	6,036 KB
		Services	0	13,848 KB
		Services	0	12,692 KB
		Services	0	7,280 KB
WmiPrvSE.exe		Services	0	12,620 KB
svchost.exe		Services	0	6,428 KB
svchost.exe		Services	0	16,116 KB
spoolsv.exe		Services	0	11,400 KB
svchost.exe		Services	0	7,372 KB
svchost.exe		Services	0	6,052 KB
ArmouryCrateControlInterf			0	9,136 KB
OneApp.IGCC.WinService.ex		Services	0	21,456 KB
svchost.exe		Services	0	
		Services	0	32,876 KB
AsusAppService.exe AsusSystemDiagnosis.exe		Services		17,056 KB
Asussystembiagnosis.exe			0	9,116 KB
ArmouryCrate.Service.exe		Services	0	18,964 KB
AsusLinkNear.exe		Services	0	8,972 KB
AsusLinkRemote.exe		Services	0	8,108 KB
		Services	0	27,832 KB
		Services	0	6,544 KB
DtsApo4Service.exe	5344	Services	0	7,764 KB
AsusSystemAnalysis.exe	5360	Services	0	11,888 KB
,		Services	0	10,480 KB
svchost.exe		Services	0	7,512 KB
		Services	0	12,728 KB
OfficeClickToRun.exe	5440	Services	0	22,856 KB

PEFService.exe		Services	Θ	13,380 KB
mfemms.exe		Services	0	14,712 KB
ModuleCoreService.exe		Services	0	9,336 KB
RefreshRateService.exe		Services	Θ	16,456 KB
LightingService.exe		Services	Θ	18,784 KB
svchost.exe		Services	0	8,608 KB
RstMwService.exe	5752	Services	Θ	12,388 KB
RtkAudUService64.exe	5764	Services	Θ	13,172 KB
TbtP2pShortcutService.exe	5780	Services	Θ	5,172 KB
sqlwriter.exe	5788	Services	Θ	7,152 KB
ROGLiveService.exe	5812	Services	Θ	11,576 KB
svchost.exe	5820	Services	0	5,208 KB
WMIRegistrationService.ex	5908	Services	Θ	12,440 KB
MsMpEng.exe		Services	0	79,288 KB
svchost.exe	6108	Services	Θ	15,420 KB
jhi_service.exe	4756	Services	Θ	5,740 KB
svchost.exe	6648	Services	0	7,904 KB
svchost.exe	7160	Services	0	7,768 KB
svchost.exe	7456	Services	0	9,660 KB
AggregatorHost.exe	7492	Services	0	4,484 KB
MMSSHOST.exe		Services	0	55,768 KB
mfevtps.exe	7864	Services	0	12,672 KB
ProtectedModuleHost.exe	8060	Services	Θ	14,836 KB
ModuleCoreService.exe	9136	Services	0	53,388 KB
conhost.exe	9152	Services	0	4,716 KB
svchost.exe	5400	Services	Θ	12,816 KB
McCSPServiceHost.exe	10136	Services	0	19,320 KB
svchost.exe	3492	Services	Θ	10,436 KB
AsusOptimizationStartupTa	9076	Console	1	14,748 KB
sihost.exe	6148	Console	1	41,544 KB
svchost.exe	8912	Console	1	7,716 KB
svchost.exe	2712	Console	1	24,328 KB
igfxEMN.exe	9712	Console	1	11,288 KB
svchost.exe	9532	Console	1	6,612 KB
svchost.exe	9936	Console	1	25,164 KB
svchost.exe	9684	Services	0	15,340 KB
taskhostw.exe		Console	1	22,104 KB
ArmourySocketServer.exe	9180	Console	1	1,992 KB
asus_framework.exe		Console	1	12,428 KB
AcPowerNotification.exe	4988	Console	1	4,596 KB
ASUSSmartDisplayControl.e	9768	Console	1	1,060 KB
AsHotplugCtrl.exe	9828	Console	1	1,700 KB
GoogleCrashHandler.exe	10608	Services	0	1,424 KB
GoogleCrashHandler64.exe	10628	Services	0	1,120 KB
explorer.exe	10832	Console	1	180,696 KB
svchost.exe	10880	Services	0	18,216 KB
svchost.exe		Console	1	23,052 KB
svchost.exe	10384	Services	Θ	12,012 KB

s	vchost.exe	24140	Services	0	6,984 KB	
S			Services	0	6,940 KB	
			Services	0	11,268 KB	
t	askhostw.exe		Console	1	14,784 KB	
W	lanext.exe	11548	Services	Θ	9,600 KB	
C	onhost.exe	23440	Services Services Services	0	5,688 KB	
Ι	ntel_PIE_Service.exe		3411111	0	9,888 KB	
	irefox.exe	25212	Console	1	243,816 KB	
			Console	1	163,984 KB	
	irefox.exe		Console	1	15,672 KB	
			Console	1	69,976 KB	
			Console	Τ.	11,832 KB	
			Console	1	83,740 KB	
			Console	1	14,900 KB	
			Console	1	,	
	irefox.exe		Console	1	159,124 KB	
			Services	0	19,632 KB	
	irefox.exe	2260	Console	1	26,996 KB	
	irefox.exe	3540	Console	1	17,276 KB	
			Console	1	78,132 KB	
			Console	1	19,436 KB	
	hotosService.exe		Console	1	19,524 KB	
	tkUWP.exe	22292	Console Console	1	30,064 KB	
	untimeBroker.exe	15468	Console	1	13,808 KB	
	ONOCITICACIONOX.EXE	19000	COLIZOTE	1	10,360 KB	
	vchost.exe		Services	0	16,608 KB	
	vchost.exe		Services	0	14,496 KB	
	miPrvSE.exe		Services	0	17,780 KB	
	vchost.exe		Services	0	6,000 KB	
	CCIMonitor.exe		Console	1	9,972 KB	
	md.exe		Console	1	5,464 KB	
	onhost.exe		Console	1	7,956 KB	
	•		Console	1	14,876 KB	
	indowsTerminal.exe			1	83,548 KB	
			Console	1	10,704 KB	
	nippingTool.exe	10100	Console Console Console	1	194,664 KB	
	ackgroundTaskHost.exe	22000	Console	1	2,128 KB	
	venose exe	23000	20112022	1 1	13,260 KB	
	hatsApp.exe earchFilterHost.exe		Console Services		288,172 KB	
	irefox.exe			1	9,312 KB	
	earchProtocolHost.exe		Console	1	42,892 KB	
	irefox.exe		Console Console	1	8,976 KB 31,448 KB	
	irefox.exe irefox.exe		Console	1	31,448 KB 31,444 KB	
	irefox.exe		Console	1	31,520 KB	
	cShm.exe		Services	0	14,492 KB	
•	earchProtocolHost.exe		Services	0	15,432 KB	
	asklist.exe		Console	1	10,616 KB	
	asketse.exe	20404	COIISO CE	_	10,010 KB	

## 13. Utilizar el comando taskkill

		,
wininit.exe	1084 Services	0 3.180 KB

C:\Users\arian>taskkill /F /PID 1084 Error: no se pudo terminar el proceso con PID 1084. Motivo: Acceso denegado.

#### 14. Utilizar el comando tracert

```
C:\Users\arian>tracert www.google.com

Traza a la dirección www.google.com [142.250.189.132]
sobre un máximo de 30 saltos:

1 * Error general.

Traza completa.
```

## 15. Utilizar el comando ARP

```
C:\Users\arian>arp -a
Interfaz: 169.254.85.122 --- 0x4
                                 Dirección física
                                                       Tipo
  Dirección de Internet
  169.254.255.255
                        ff-ff-ff-ff-ff
                                              estático
  224.0.0.22
                        01-00-5e-00-00-16
                                              estático
  224.0.0.251
                                              estático
                        01-00-5e-00-00-fb
  224.0.0.252
                        01-00-5e-00-00-fc
                                              estático
  239.255.255.250
                        01-00-5e-7f-ff-fa
                                              estático
                        ff-ff-ff-ff-ff
  255.255.255.255
                                              estático
Interfaz: 192.168.1.124 --- 0xe
                                 Dirección física
  Dirección de Internet
                                                       Tipo
  192.168.1.1
                        e8-9f-80-06-fa-ac
                                              dinámico
  192.168.1.119
                        14-c1-4e-76-19-33
                                              dinámico
  192.168.1.255
                        ff-ff-ff-ff-ff
                                              estático
                                              estático
  224.0.0.22
                        01-00-5e-00-00-16
  224.0.0.251
                        01-00-5e-00-00-fb
                                              estático
  224.0.0.252
                                              estático
                        01-00-5e-00-00-fc
  239.255.255.250
                        01-00-5e-7f-ff-fa
                                              estático
  255.255.255.255
                        ff-ff-ff-ff-ff
                                              estático
```

## **Preguntas**

- 1. ¿Para qué sirve el comando ping? Sirve para verificar la conectividad entre un dispositivo y otro en una red, así como para medir el tiempo de ida y vuelta de los paquetes.
- 2. ¿Para qué sirve el comando nslookup? Se utiliza para consultar servidores DNS y obtener información sobre nombres de dominio, como la dirección IP asociada.

- 3. ¿Para qué sirve el comando netstat? Proporciona información detallada sobre las conexiones de red, puertos abiertos y estadísticas de red en un sistema.
- 4. ¿Para qué sirve el comando tasklist? Muestra una lista de los procesos en ejecución en un sistema, incluyendo sus identificadores de proceso (PID) y otros detalles.
- 5. ¿Para qué sirve el comando taskill? Permite finalizar o terminar un proceso en ejecución, utilizando su identificador de proceso (PID).
- 6. ¿Para qué sirve el comando tracert? Ayuda a determinar la ruta tomada por los paquetes desde el origen hasta un destino en una red, mostrando cada salto intermedio.
- 7. ¿Cómo ayudan los primeros tres comandos para detectar problemas en la red?
  - Ping permite verificar la conectividad entre dispositivos y detectar posibles pérdidas de paquetes o latencias altas.
  - Nslookup ayuda a identificar problemas de resolución de nombres de dominio, como servidores DNS inaccesibles.
  - Netstat proporciona información sobre conexiones activas y puertos abiertos, lo que puede revelar problemas de congestión o configuración incorrecta.

## Investigación

Instrucciones: Investigar los siguientes comandos y anotar ejemplos prácticos.

#### atm:

Descripción: El comando atm se utiliza para mostrar información y estadísticas sobre interfaces ATM (Asynchronous Transfer Mode) en un sistema.

Ejemplo: atmstat mostrará estadísticas sobre las interfaces ATM configuradas en el

sistema.

bitsadadmin:

Descripción: Este comando está asociado con BITS (Background Intelligent Transfer

Service) y se utiliza para administrar trabajos de transferencia de archivos en segundo

plano.

Ejemplo: bitsadadmin /list mostrará una lista de todos los trabajos de transferencia en

segundo plano.

cmstp:

Descripción: cmstp es una herramienta utilizada para instalar o desinstalar archivos

.inf y .cab en un sistema.

Ejemplo: cmstp /s archivo.inf instalará el archivo .inf especificado.

ftp:

Descripción: ftp (File Transfer Protocol) es un protocolo utilizado para la transferencia

de archivos a través de una red.

Ejemplo: ftp ejemplo.com se conectará a un servidor FTP llamado "ejemplo.com".

getmac:

Descripción: Este comando muestra la dirección MAC de los adaptadores de red en

un sistema.

Ejemplo: getmac mostrará las direcciones MAC de todos los adaptadores de red.

hostname:

Descripción: hostname se utiliza para mostrar o configurar el nombre del sistema.

18

Ejemplo: hostname mostrará el nombre del sistema actual.

### nbtstat:

Descripción: nbtstat (NetBIOS over TCP/IP Statistics) muestra estadísticas y otra información sobre el protocolo NetBIOS en un sistema.

Ejemplo: nbtstat -a nombre\_del\_equipo mostrará información sobre un equipo remoto.

#### net:

Descripción: net es un comando amplio que permite realizar varias operaciones relacionadas con la red.

Ejemplo: net user mostrará una lista de usuarios en el sistema.

#### net use:

Descripción: net use se utiliza para conectar o desconectar recursos compartidos de red.

Ejemplo: net use Z: \\servidor\\recurso conectará el recurso compartido en "Z:".

### netsh:

Descripción: netsh permite configurar varios aspectos de la red en un sistema.

Ejemplo: netsh interface ipv4 show interfaces mostrará información sobre las interfaces de red IPv4.

## pathping:

Descripción: pathping combina las funcionalidades de traceroute y ping, proporcionando información detallada sobre la ruta de un paquete a un destino.

Ejemplo: pathping ejemplo.com realizará un seguimiento de la ruta a "ejemplo.com".

## rcp:

Descripción: rcp (Remote Copy Protocol) se utiliza para copiar archivos de un sistema remoto a un sistema local.

Ejemplo: rcp archivo.txt usuario@servidor:/ruta/destino copiará "archivo.txt" al sistema remoto.

## telnet:

Descripción: telnet es un protocolo de red que permite la comunicación con un host remoto a través de la línea de comandos.

Ejemplo: telnet ejemplo.com 80 abrirá una conexión a "ejemplo.com" en el puerto 80.

## tftp:

Descripción: tftp (Trivial File Transfer Protocol) es un protocolo simple utilizado para la transferencia de archivos.

Ejemplo: tftp -i dirección\_destino GET archivo transferirá un archivo desde el servidor TFTP a la ubicación local.