



---

# LINUX

---

Tarea #987



**Asignatura:**

Sistemas Operativos

**Nombre:**

Márquez Nahuat Bernardo Rommel

**Docente:**

Ismael Jimenez S

1.- Obtener la ayuda del comando ping

### ping --help

```
C:\Users\Bernardo>ping -help
Opción incorrecta -help.

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.
```

2.- Enviar un ping a 127.0.0.1 aplicando cualquier parametro.

### ping -c 4 127.0.0.1

```
C:\Users\Bernardo>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=64
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=64

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\Bernardo>
```

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

### ping

```
C:\Users\Bernardo>ping

Usos: 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\Bernardo>
```

- Si obtienes respuestas exitosas, significa que la conectividad en tu propia máquina (localhost) está funcionando correctamente.
- Si no obtienes respuestas, podría indicar un problema en tu configuración de red o en el funcionamiento de la red.

4.- Obtener la ayuda del comando nslookup

### nslookup /?

```
C:\Users\Bernardo>nslookup /?

Usos:
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\Bernardo>
```

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

**nslookup upqroo.edu.mx**

```
C:\Users\Bernardo>nslookup upqroo.edu.mx
Servidor:  b.resolvers.level3.net
Address:  4.2.2.2

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

C:\Users\Bernardo>
```

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

**ping 77.68.126.20**

```
C:\Users\Bernardo>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=118ms TTL=50
Respuesta desde 77.68.126.20: bytes=32 tiempo=119ms TTL=50
Respuesta desde 77.68.126.20: bytes=32 tiempo=140ms 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 = 140ms, Media = 124ms

C:\Users\Bernardo>
```

**Verifica si puedes alcanzar el servidor utilizando la dirección IP. Si obtienes respuestas, significa que el servidor es accesible.**

## 7.- Obtener la ayuda del comando netstat

### netstat /?

```
C:\Users\Bernardo>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.
```

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

### netstat -a

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

Conexiones activas

    Proto  Dirección local      Dirección remota      Estado
    TCP    0.0.0.0:80           DESKTOP-9Q7351T:0     LISTENING
    TCP    0.0.0.0:135          DESKTOP-9Q7351T:0     LISTENING
    TCP    0.0.0.0:443          DESKTOP-9Q7351T:0     LISTENING
    TCP    0.0.0.0:445          DESKTOP-9Q7351T:0     LISTENING
    TCP    0.0.0.0:3306         DESKTOP-9Q7351T:0     LISTENING
    TCP    0.0.0.0:5040         DESKTOP-9Q7351T:0     LISTENING
    TCP    0.0.0.0:49664        DESKTOP-9Q7351T:0     LISTENING
    TCP    0.0.0.0:49665        DESKTOP-9Q7351T:0     LISTENING
    TCP    0.0.0.0:49666        DESKTOP-9Q7351T:0     LISTENING
    TCP    0.0.0.0:49667        DESKTOP-9Q7351T:0     LISTENING
    TCP    0.0.0.0:49668        DESKTOP-9Q7351T:0     LISTENING
    TCP    0.0.0.0:49669        DESKTOP-9Q7351T:0     LISTENING
    TCP    127.0.0.1:1434        DESKTOP-9Q7351T:0     LISTENING
    TCP    127.0.0.1:6463        DESKTOP-9Q7351T:0     LISTENING
    TCP    192.168.56.1:139      DESKTOP-9Q7351T:0     LISTENING
    TCP    192.168.128.112:139   DESKTOP-9Q7351T:0     LISTENING
    TCP    192.168.128.112:49719 20.25.241.18:https     ESTABLISHED
    TCP    192.168.128.112:49722 a23-0-175-139:http     CLOSE_WAIT
    TCP    192.168.128.112:49746 a23-54-200-10:https     CLOSE_WAIT
    TCP    192.168.128.112:52753 52.159.127.243:https     ESTABLISHED
    TCP    192.168.128.112:52755 ya-in-f188:https        ESTABLISHED
    TCP    192.168.128.112:53384 20.72.146.34:https      CLOSE_WAIT
    TCP    192.168.128.112:54176 20.94.21.149:https      ESTABLISHED
    TCP    192.168.128.112:54863 162.159.133.234:https   ESTABLISHED
    TCP    192.168.128.112:54865 yq-in-f190:https        ESTABLISHED
^C
C:\Users\Bernardo>
C:\Users\Bernardo>
```

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

### netstat -n

```
C:\Users\Bernardo>netstat -n
```

#### Conexiones activas

Proto	Dirección local	Dirección remota	Estado
TCP	192.168.128.112:49719	20.25.241.18:443	ESTABLISHED
TCP	192.168.128.112:49722	23.0.175.139:80	CLOSE_WAIT
TCP	192.168.128.112:49746	23.54.200.10:443	CLOSE_WAIT
TCP	192.168.128.112:52753	52.159.127.243:443	ESTABLISHED
TCP	192.168.128.112:52755	173.194.219.188:443	ESTABLISHED
TCP	192.168.128.112:53384	20.72.146.34:443	CLOSE_WAIT
TCP	192.168.128.112:54176	20.94.21.149:443	ESTABLISHED
TCP	192.168.128.112:54863	162.159.133.234:443	ESTABLISHED
TCP	192.168.128.112:55106	142.250.9.101:443	ESTABLISHED
TCP	192.168.128.112:55107	142.251.15.95:443	ESTABLISHED
TCP	192.168.128.112:55112	64.233.177.119:443	ESTABLISHED
TCP	192.168.128.112:55115	108.177.122.102:443	ESTABLISHED
TCP	192.168.128.112:55116	173.194.219.157:443	ESTABLISHED
TCP	192.168.128.112:55118	142.251.40.227:443	ESTABLISHED
TCP	192.168.128.112:55214	216.239.32.116:443	TIME_WAIT
TCP	192.168.128.112:55221	216.239.36.117:443	TIME_WAIT
TCP	192.168.128.112:55222	108.177.122.94:443	TIME_WAIT
TCP	192.168.128.112:55223	192.178.49.195:443	ESTABLISHED
TCP	192.168.128.112:55224	64.233.185.94:443	ESTABLISHED
TCP	192.168.128.112:55225	142.250.105.136:443	TIME_WAIT
TCP	192.168.128.112:55231	187.190.14.108:443	CLOSE_WAIT
TCP	192.168.128.112:55234	172.253.124.132:443	ESTABLISHED
TCP	192.168.128.112:55235	142.251.15.157:443	ESTABLISHED
TCP	192.168.128.112:55236	142.250.105.132:443	ESTABLISHED
TCP	192.168.128.112:55237	64.233.176.139:443	ESTABLISHED
TCP	192.168.128.112:55240	104.18.37.228:443	ESTABLISHED
TCP	192.168.128.112:55244	172.253.124.190:443	ESTABLISHED
TCP	192.168.128.112:55245	108.177.122.95:443	ESTABLISHED
TCP	192.168.128.112:55246	13.107.21.200:443	ESTABLISHED
TCP	192.168.128.112:55247	13.107.21.200:443	ESTABLISHED
TCP	192.168.128.112:55249	72.21.81.200:443	ESTABLISHED
TCP	192.168.128.112:55250	13.107.237.254:443	ESTABLISHED
TCP	192.168.128.112:55251	20.141.10.212:443	ESTABLISHED
TCP	192.168.128.112:55252	204.79.197.222:443	ESTABLISHED
TCP	192.168.128.112:55254	142.250.9.94:443	ESTABLISHED
TCP	192.168.128.112:55255	64.233.176.113:443	ESTABLISHED
TCP	192.168.128.112:55256	142.250.9.138:443	ESTABLISHED



## 10.- Mostrar las conexiones TCP

**netstat -t**

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

Conexiones activas

Proto	Dirección local Estado de descarga	Dirección remota	Estado	
TCP	192.168.128.112:49719	20.25.241.18:https	ESTABLISHED	EnHost
TCP	192.168.128.112:49722	a23-0-175-139:http	CLOSE_WAIT	EnHost
TCP	192.168.128.112:49746	a23-54-200-10:https	CLOSE_WAIT	EnHost
TCP	192.168.128.112:52753	52.159.127.243:https	ESTABLISHED	EnHost
TCP	192.168.128.112:52755	ya-in-f188:https	ESTABLISHED	EnHost
TCP	192.168.128.112:53384	20.72.146.34:https	CLOSE_WAIT	EnHost
TCP	192.168.128.112:54176	20.94.21.149:https	ESTABLISHED	EnHost
TCP	192.168.128.112:54863	162.159.133.234:https	ESTABLISHED	EnHost
TCP	192.168.128.112:55106	yq-in-f101:https	ESTABLISHED	EnHost
TCP	192.168.128.112:55107	yl-in-f95:https	ESTABLISHED	EnHost
TCP	192.168.128.112:55112	yx-in-f119:https	ESTABLISHED	EnHost
TCP	192.168.128.112:55115	ym-in-f102:https	ESTABLISHED	EnHost
TCP	192.168.128.112:55116	ya-in-f157:https	TIME_WAIT	EnHost
TCP	192.168.128.112:55118	lga34s39-in-f3:https	ESTABLISHED	EnHost
TCP	192.168.128.112:55223	phx19s06-in-f3:https	ESTABLISHED	EnHost

## 11.- Mostrar las conexiones UDP

**netstat -u**

```
C:\Users\Bernardo>netstat -u
```

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.

## 12.- Utilizar el comando tasklist

### tasklist

```
C:\Users\Bernardo>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	3,792 KB
Registry	100	Services	0	96,432 KB
smss.exe	416	Services	0	984 KB
csrss.exe	560	Services	0	4,272 KB
wininit.exe	916	Services	0	5,488 KB
csrss.exe	924	Console	1	5,348 KB
winlogon.exe	476	Console	1	10,476 KB
services.exe	624	Services	0	9,464 KB
lsass.exe	636	Services	0	21,296 KB
svchost.exe	772	Services	0	31,580 KB
fontdrvhost.exe	796	Console	1	9,764 KB
fontdrvhost.exe	804	Services	0	2,120 KB
svchost.exe	908	Services	0	15,176 KB
svchost.exe	668	Services	0	7,200 KB
dwm.exe	1100	Console	1	77,256 KB
svchost.exe	1228	Services	0	9,368 KB
svchost.exe	1236	Services	0	10,816 KB
svchost.exe	1316	Services	0	14,384 KB
svchost.exe	1372	Services	0	12,312 KB
svchost.exe	1380	Services	0	5,124 KB
svchost.exe	1428	Services	0	12,988 KB
svchost.exe	1492	Services	0	10,376 KB
svchost.exe	1624	Services	0	5,992 KB
svchost.exe	1704	Services	0	10,292 KB
svchost.exe	1724	Services	0	5,888 KB
svchost.exe	1784	Services	0	6,884 KB
svchost.exe	1808	Services	0	6,812 KB
svchost.exe	1816	Services	0	13,280 KB
svchost.exe	1828	Services	0	5,012 KB
Memory Compression	1956	Services	0	176,244 KB
svchost.exe	1968	Services	0	7,712 KB
igfxCUIService.exe	2040	Services	0	8,304 KB
svchost.exe	656	Services	0	11,568 KB
svchost.exe	2072	Services	0	7,212 KB
svchost.exe	2080	Services	0	7,576 KB
svchost.exe	2148	Services	0	8,804 KB
svchost.exe	2208	Services	0	15,764 KB
svchost.exe	2308	Services	0	6,776 KB



### 13.- Utilizar el comando taskkill

#### taskkill /IM notepad.exe

```
C:\Users\Bernardo>taskkill /IM Discord.exe
CORRECTO: señal de terminación enviada al proceso "Discord.exe" con PID 6728.
CORRECTO: señal de terminación enviada al proceso "Discord.exe" con PID 8568.
CORRECTO: señal de terminación enviada al proceso "Discord.exe" con PID 424.
CORRECTO: señal de terminación enviada al proceso "Discord.exe" con PID 3568.
CORRECTO: señal de terminación enviada al proceso "Discord.exe" con PID 11396.
ERROR: no se pudo terminar el proceso "Discord.exe" con PID 6416.
Motivo: Este proceso se puede terminar solo de forma forzada (con la opción /F).

C:\Users\Bernardo>
```

### 14.- Utilizar el comando tracert

#### tracert www.upqroo.com

```
C:\Users\Bernardo>tracert www.ejemplo.com

Traza a la dirección www.ejemplo.com [199.59.243.225]
sobre un máximo de 30 saltos:

  1      1 ms      1 ms      1 ms  192.168.128.1
  2      2 ms      2 ms      2 ms  192.168.109.1
  3      6 ms      5 ms      5 ms  fixed-187-188-58-130.totalplay.net [187.188.58.130]
  4      5 ms      4 ms      5 ms  10.180.58.1
  5     17 ms     19 ms     32 ms  99.83.115.54
  6      *          *          *      Tiempo de espera agotado para esta solicitud.
  7      *          *          *      Tiempo de espera agotado para esta solicitud.
  8      *      ^C

C:\Users\Bernardo>
```

### 15.- Utilizar el comando ARP

#### arp -a

```
C:\Users\Bernardo>arp -a

Interfaz: 192.168.56.1 --- 0xd
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
224.0.1.60                 01-00-5e-00-01-3c    estático
239.255.255.250           01-00-5e-7f-ff-fa    estático
255.255.255.255           ff-ff-ff-ff-ff-ff    estático

Interfaz: 192.168.128.112 --- 0x13
Dirección de Internet      Dirección física      Tipo
192.168.128.1              00-0c-e6-f5-d8-75    dinámico
192.168.128.237            de-51-6e-46-f1-56    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
224.0.0.251                01-00-5e-00-00-fb    estático
224.0.0.252                01-00-5e-00-00-fc    estático
224.0.1.60                 01-00-5e-00-01-3c    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\Bernardo>
```

1.- ¿Para qué sirve el comando ping?

El comando ping se utiliza para enviar paquetes ICMP Echo Request a una dirección IP especificada. Si la dirección IP es accesible, el dispositivo de destino responderá con un paquete ICMP Echo Reply. El comando ping se puede utilizar para verificar la conectividad entre dos dispositivos en una red.

2.- ¿Para qué sirve el comando nslookup?

El comando nslookup se utiliza para resolver nombres de dominio en direcciones IP. El comando nslookup se puede utilizar para verificar la resolución de nombres de dominio en una red.

3.- ¿Para qué sirve el comando netstat?

El comando netstat se utiliza para mostrar información sobre las conexiones de red activas. El comando netstat se puede utilizar para verificar la actividad de la red en un dispositivo.

4.- ¿Para qué sirve el comando tasklist?

El comando tasklist se utiliza para mostrar una lista de los procesos que se están ejecutando en un dispositivo. El comando tasklist se puede utilizar para identificar procesos que pueden estar causando problemas de red.

5.- ¿Para qué sirve el comando taskkill?

El comando taskkill se utiliza para finalizar procesos en un dispositivo. El comando taskkill se puede utilizar para finalizar procesos que pueden estar causando problemas de red.

6.- ¿Para qué sirve el comando tracert?

El comando tracert se utiliza para rastrear el camino que toman los paquetes de datos a través de una red. El comando tracert se puede utilizar para identificar problemas de ruta en una red.

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

Los primeros tres comandos, ping, nslookup y netstat, se pueden utilizar para detectar problemas en la red de la siguiente manera:

- **Ping:** El comando ping se puede utilizar para verificar la conectividad entre dos dispositivos en una red. Si el comando ping no puede comunicarse con un dispositivo, es probable que haya un problema de conectividad.
- **Nslookup:** El comando nslookup se puede utilizar para verificar la resolución de nombres de dominio en una red. Si el comando nslookup no puede resolver un nombre de dominio, es probable que haya un problema de resolución de nombres.
- **Netstat:** El comando netstat se puede utilizar para verificar la actividad de la red en un dispositivo. Si el comando netstat muestra una gran cantidad de conexiones activas o conexiones sospechosas, es probable que haya un problema de red.


Investigar los siguientes comandos y anotar ejemplos prácticos:

atm, adm, bitsadmin, cmstp, ftp, getmac, hostname, nbtstat, net, net use, netsh, pathping, rcp, rexec, route, rpcping, rsh, tcmsetup, telnet, tftp.

- 1) **atmadm:** Este comando se utiliza para mostrar y modificar la configuración de los adaptadores de interfaz ATM (Asynchronous Transfer Mode) en un sistema Windows. ATM es una tecnología de red utilizada para transmitir datos a alta velocidad.
- 2) **bitsadmin:** BITS (Background Intelligent Transfer Service) es un servicio de Windows que administra la transferencia de archivos en segundo plano. `bitsadmin` es una herramienta de línea de comandos que permite administrar las tareas de transferencia de BITS desde el símbolo del sistema.
- 3) **cmstp:** CMSTP es una utilidad de línea de comandos que se utiliza para instalar o desinstalar perfiles de conexión de acceso telefónico y de red en sistemas Windows. Puede ser útil para configurar la conectividad a redes.
- 4) **ftp:** El comando FTP (File Transfer Protocol) se utiliza para transferir archivos entre computadoras a través de una red. Puedes conectarte a servidores FTP para descargar o cargar archivos.
- 5) **getmac:** `getmac` muestra la dirección MAC de los adaptadores de red en una computadora Windows. La dirección MAC es un identificador único asignado a cada adaptador de red.
- 6) **hostname:** Muestra el nombre de host de la computadora actual. El nombre de host es el nombre que se utiliza para identificar una máquina en una red.
- 7) **nbtstat:** Esta herramienta muestra estadísticas y datos relacionados con NetBIOS (Network Basic Input/Output System). NetBIOS es un protocolo de red que permite la comunicación entre computadoras en una red local.
- 8) **net:** El comando `net` es un comando genérico que se utiliza para realizar una variedad de tareas de administración de red, como agregar usuarios, administrar recursos compartidos, entre otros.
- 9) **net use:** `net use` se utiliza para conectar o desconectar unidades de red en un sistema Windows. Puedes utilizarlo para mapear unidades de red a recursos compartidos.
- 10) **netsh:** `netsh` es una utilidad de línea de comandos que permite configurar y administrar una variedad de configuraciones de red en sistemas Windows. Puede ser útil para configurar adaptadores de red, cortafuegos, y más.
- 11) **pathping:** `pathping` es una herramienta que combina la funcionalidad de `ping` y `tracert`. Proporciona información detallada sobre el camino que toma un paquete a través de la red, mostrando la latencia en cada salto.
- 12) **rcp:** RCP (Remote Copy Protocol) es un protocolo de transferencia de archivos que permite copiar archivos desde y hacia sistemas remotos. Sin embargo, es importante destacar que RCP no es ampliamente utilizado y puede ser menos seguro que otros métodos de transferencia de archivos.

- 13) **rexec**: REXEC (Remote Execution) es un protocolo que permite ejecutar comandos en sistemas remotos. Al igual que RCP, REXEC también puede ser menos seguro y se utiliza raramente en entornos modernos.
- 14) **route**: El comando `route` se utiliza para ver y modificar la tabla de enrutamiento en sistemas Windows. Permite controlar cómo se dirigen los paquetes en una red.
- 15) **rpcping**: `rpcping` es una herramienta utilizada para probar la conectividad con servicios RPC (Remote Procedure Call) en sistemas Windows. Puede ayudar a diagnosticar problemas de comunicación con servicios RPC.
- 16) **rsh**: RSH (Remote Shell) es un protocolo que permite ejecutar comandos en sistemas remotos de manera similar a SSH. Al igual que RCP y REXEC, RSH es menos seguro y menos utilizado en la actualidad.
- 17) **tcmsetup**: `tcmsetup` se utiliza para configurar la autenticación de transacciones en sistemas Windows. Esta herramienta es relevante para aplicaciones empresariales que requieren transacciones seguras.
- 18) **telnet**: Telnet es un protocolo que permite la conexión a sistemas remotos a través de una interfaz de línea de comandos. Puede utilizarse para administrar sistemas o dispositivos de red de forma remota.
- 19) **tftp**: TFTP (Trivial File Transfer Protocol) es un protocolo de transferencia de archivos simple que se utiliza para cargar o descargar archivos desde sistemas remotos. Es más básico que FTP y se utiliza en entornos de red limitados.

## 1. atmadm

 Símbolo del sistema

```
C:\Users\Bernardo>atmadm
"atmadm" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\Bernardo>
```

No funciona pero este comando se utiliza para mostrar y modificar la configuración de los adaptadores de interfaz ATM.

## 2. bitsadmin

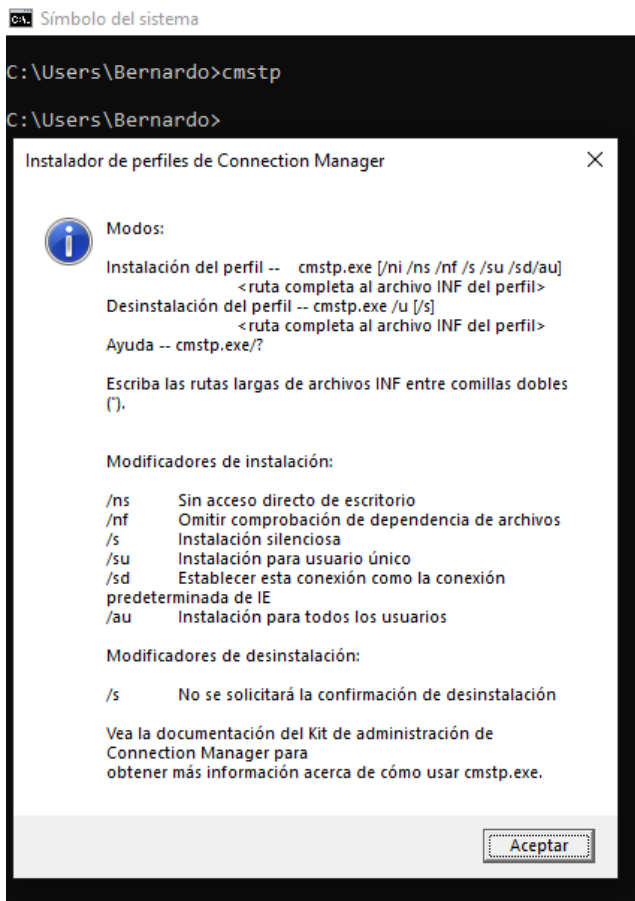
```
C:\Users\Bernardo>bitsadmin /LIST

BITSADMIN version 3.0
BITS administration utility.
(C) Copyright Microsoft Corp.

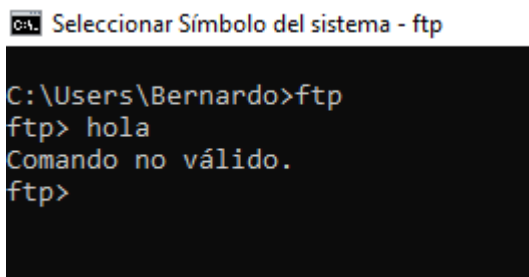
{5939D88B-7370-4679-94CE-272784890155} 'VsBitsDownloadJob - -2006652028' ERROR 0 / 1 811008 / 24481792
{493D3C39-DC03-4FC4-8F0F-248F25B73620} 'VsBitsDownloadJob - 604995949' ERROR 0 / 1 319488 / 26951680
Listed 2 job(s).

C:\Users\Bernardo>
```

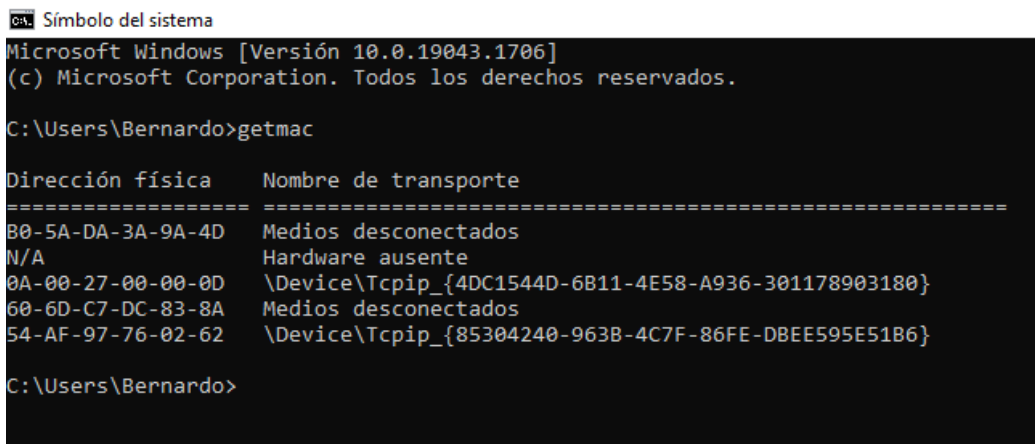
### 3. cmstp




### 4. ftp



### 5. getmac




## 6. hostname

 Símbolo del sistema

```
C:\Users\Bernardo>hostname
DESKTOP-9Q7351T

C:\Users\Bernardo>
```

## 7. nbtstat

 Símbolo del sistema

```
C:\Users\Bernardo>nbtstat

Muestra las estadísticas del protocolo y las conexiones actuales de TCP/IP
usando NBT (NetBIOS sobre TCP/IP).

NBTSTAT [ [-a NombreRemoto] [-A dirección IP] [-c] [-n] [-r] [-R] [-RR]
[-s] [-S] [intervalo] ]


-a (estado del adaptador) Hace una lista de la tabla de nombres de
los equipos remotos según su nombre
-A (estado del adaptador) hace una lista de la tabla de nombres de
los equipos remotos según sus direcciones de IP.
-c (caché) Hace una lista de los nombres [equipo]remotos de la caché
NBT y sus direcciones de IP
-n (nombres) Hace una lista de los nombres NetBIOS locales.
-r (resueltos) Lista de nombres resueltos por difusión y vía WINS
-R (Volver a cargar) Purga y vuelve a cargar la tabla de nombres de
la caché remota
-S (Sesiones) Hace una lista de la tabla de sesiones con las
direcciones de destino de IP
-s (sesiones) Hace una lista de la tabla de sesiones convirtiendo
las direcciones de destino de IP en nombres de equipo NETBIOS.
-RR (LiberarActualizar) Envía paquetes de Liberación de nombres a WINS
y después, inicia Actualizar

NombreRemoto Nombre del equipo de host remoto.
Dirección IP Representación del Punto decimal de la dirección de IP.
intervalo Vuelve a mostrar estadísticas seleccionadas, pausando
segundos de intervalo entre cada muestra. Presionar Ctrl+C
para parar volver a mostrar las estadísticas.

C:\Users\Bernardo>
```



## 8. net


 Símbolo del sistema

```
C:\Users\Bernardo>net
La sintaxis de este comando es:

NET
    [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
      STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\Users\Bernardo>
```

## 9. net use

 Símbolo del sistema

```
C:\Users\Bernardo>net use /?
La sintaxis de este comando es:


NET USE
[devicename | *] [\\computername\sharename[\volume] [password | *]]
    [/USER:[domainname\]username]
    [/USER:[dotted domain name\]username]
    [/USER:[username@dotted domain name]
    [/SMARTCARD]
    [/SAVECRED]
    [/REQUIREINTEGRITY]
    [/REQUIREPRIVACY]
    [/WRITETHROUGH]
    [[/DELETE] | [/PERSISTENT:{YES | NO}]]

NET USE {devicename | *} [password | *] /HOME

NET USE [/PERSISTENT:{YES | NO}]

C:\Users\Bernardo>
```

## 10. netsh

 Símbolo del sistema


```
C:\Users\Bernardo>netsh /?

Uso: netsh [-a ArchAlias] [-c Contexto] [-r EquipoRemoto] [-u
[NombreDominio\]NombreUsuario] [-p Contraseña | *]
[Comando | -f ArchivoScript]

Los siguientes comandos están disponibles:

Comandos en este contexto:
?                - Muestra una lista de comandos.
add              - Agrega una entrada de configuración a una lista de entradas.
advfirewall      - Cambia al contexto `netsh advfirewall'.
branchcache      - Cambia al contexto `netsh branchcache'.
bridge           - Cambia al contexto `netsh bridge'.
delete           - Elimina una entrada de configuración de una lista de entradas.
dhcpclient       - Cambia al contexto `netsh dhcpclient'.
dnsclient        - Cambia al contexto `netsh dnsclient'.
dump             - Muestra un script de configuración.
exec             - Ejecuta un archivo de script.
firewall         - Cambia al contexto `netsh firewall'.
help            - Muestra una lista de comandos.
http            - Cambia al contexto `netsh http'.
interface       - Cambia al contexto `netsh interface'.
ipsec           - Cambia al contexto `netsh ipsec'.
lan             - Cambia al contexto `netsh lan'.
mbn             - Cambia al contexto `netsh mbn'.
namespace       - Cambia al contexto `netsh namespace'.
netio           - Cambia al contexto `netsh netio'.
p2p             - Cambia al contexto `netsh p2p'.
ras             - Cambia al contexto `netsh ras'.
rpc            - Cambia al contexto `netsh rpc'.
```

## 11. pathping

 Símbolo del sistema

```
Microsoft Windows [Versión 10.0.19043.1706]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Bernardo>pathping

Uso: pathping [-g lista_host] [-h saltos_máx] [-i dirección] [-n]
[-p período] [-q núm_consultas] [-w tiempo_espera]
[-4] [-6] nombre_destino

Opciones:
-g lista_host      Ruta de origen no estricta en la lista de host.
-h saltos_máx     Número máximo de saltos para buscar en el destino.
-i dirección      Utilizar la dirección de origen especificada.
-n               No resolver direcciones como nombres de host.
-p período        Período de espera en milisegundos entre llamadas ping.
-q núm_consultas  Número de consultas por salto.
-w tiempo_espera  Tiempo de espera en milisegundos para cada respuesta.
-4               Fuerza utilizando IPv4.
-6               Fuerza utilizando IPv6.

C:\Users\Bernardo>
```

## 12. rcp

Si MASK no es válido se genera un error, como cuando (DEST & MASK) != DEST  
Ejemplo> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1  
Error al agregar la ruta: El parámetro de máscara especificado no es válido. (Destino & Máscara) != Destino.

Ejemplos:

```
> route PRINT
> route PRINT -4
> route PRINT -6
> route PRINT 157*      .... solo imprime lo que coincida con 157*

> route ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 METRIC 3 IF 2
      destino^      ^máscara  ^puerta de  métrica^  ^
                        enlace      interfaz^

Si no se proporciona IF, intenta buscar la mejor interfaz para una
puerta de enlace específica.
> route ADD 3ffe::/32 3ffe::1

> route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2

CHANGE solo se usa para modificar la puerta de enlace o la métrica.

> route DELETE 157.0.0.0
> route DELETE 3ffe::/32
```

## 13. rexec

Este comando está en desuso.

## 14. route

☐ Símbolo del sistema


```
C:\Users\Bernardo>route PRINT 157*
=====
Lista de interfaces
25...b0 5a da 3a 9a 4d .....Realtek PCIe FE Family Controller
13...0a 00 27 00 00 0d .....VirtualBox Host-Only Ethernet Adapter
22...56 af 97 76 02 62 .....Microsoft Wi-Fi Direct Virtual Adapter #5
12...54 af 97 76 02 62 .....Microsoft Wi-Fi Direct Virtual Adapter #6
19...54 af 97 76 02 62 .....TP-Link Wireless USB Adapter
17...60 6d c7 dc 83 8a .....Bluetooth Device (Personal Area Network) #2
1.....Software Loopback Interface 1
=====

IPv4 Tabla de enrutamiento
=====
Rutas activas:
    Ninguno
Rutas persistentes:
    Ninguno

IPv6 Tabla de enrutamiento
=====
Rutas activas:
    Ninguno
Rutas persistentes:
    Ninguno

C:\Users\Bernardo>
```

## 15. rpcping

 Símbolo del sistema

```
C:\Users\Bernardo>rpcping
Excepción 5 (0x00000005)
Número de registros: 1
ProcessID: 2084
Hora del sistema: 10/18/2023 6:12:38:45
Generación de componentes: 2
Estado: 0x5, 5
La ubicación de detección: 1750
Marcas: 0
NumberOfParameters: 1
Valor Long: 0x5

C:\Users\Bernardo>
```

## 16. rsh

### Ejecutar comandos a distancia (rsh)

El comando `rsh` (del **shell remoto**) le permite ejecutar un único comando en un sistema remoto sin tener que conectar anteriormente. Esto le puede ahorrar mucho tiempo cuando sólo quiera hacer una cosa en el sistema remoto.

Para ejecutar un comando en un sistema remoto escriba:

`rsh comando del nombre_del_sistema`

El siguiente ejemplo muestra cómo se vería el contenido del directorio `/home/solitario/guitarra` del sistema `solitario`:

```
$ rsh solitario ls /home/solitario/guitarra
collings      gibson      santacruz
fender        martin      taylor
$
```

De forma parecida a los comandos `rlogin` y `rcp`, `rsh` usa los archivos `/etc/hosts.equiv` y `/etc/passwd` del sistema remoto para determinar si el usuario tiene derecho de acceso a dicho sistema.

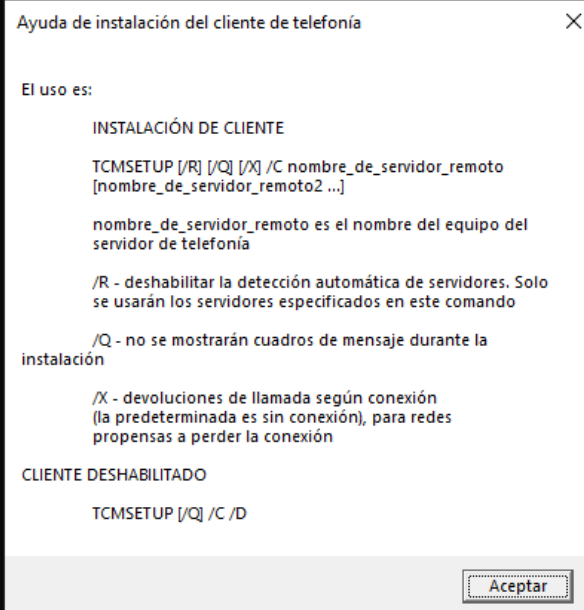
Si desea más información sobre el comando `rsh(1)` y sus opciones, consulte *man Pages(1): User Commands*.

## 17. tcmsetup

 Símbolo del sistema

```
C:\Users\Bernardo>tcmsetup
```

```
C:\Users\Bernardo>
```



## 18. telnet

C:\> Seleccionar Símbolo del sistema

```
C:\Users\Bernardo>telnet
"telnet" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.
C:\Users\Bernardo>
```

No funcionó el comando pero debería de conectarse al servidor

## 19. tftp

C:\> Símbolo del sistema

```
C:\Users\Bernardo>tftp
"tftp" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.
C:\Users\Bernardo>
```

No funcionó el comando pero debería de permitir la transferencia de archivos.