CARLOS ALBERTO FUENTES PEREZ

ING EN SOFTWARE 27AV

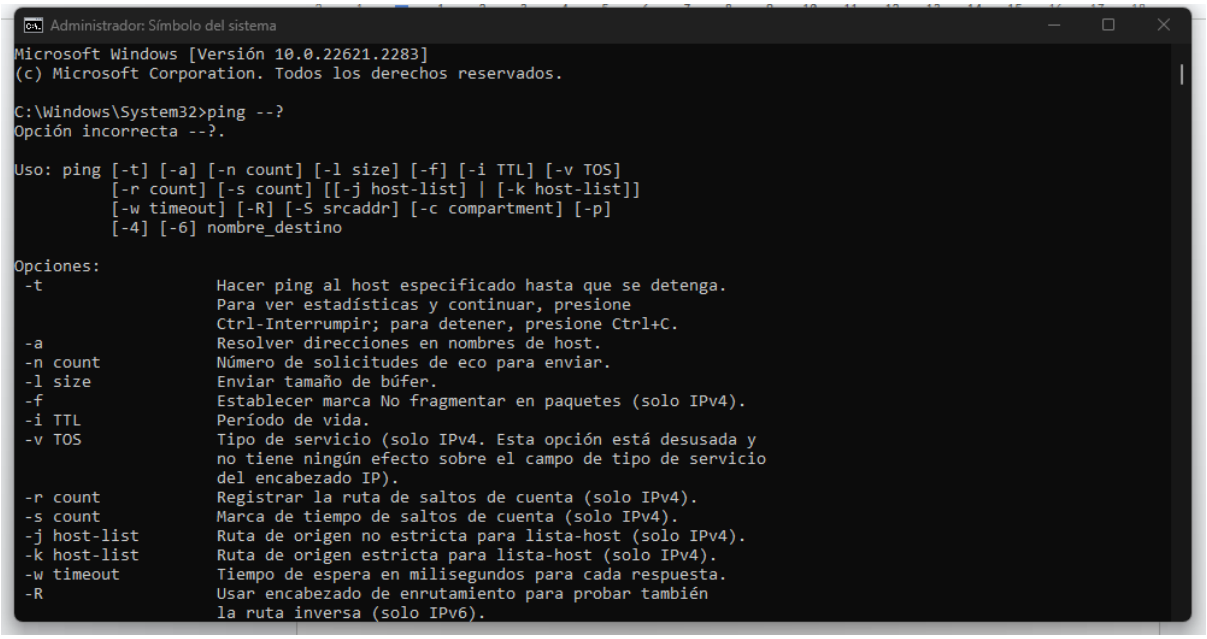
SISTEMAS OPERATIVOS

PROF. ISMAEL JIMENEZ SANCHEZ

COMANDOS EN MSDOS

COMANDOS EN MSDOS

1. Obtener la ayuda del comando ping: **`ping --h`**



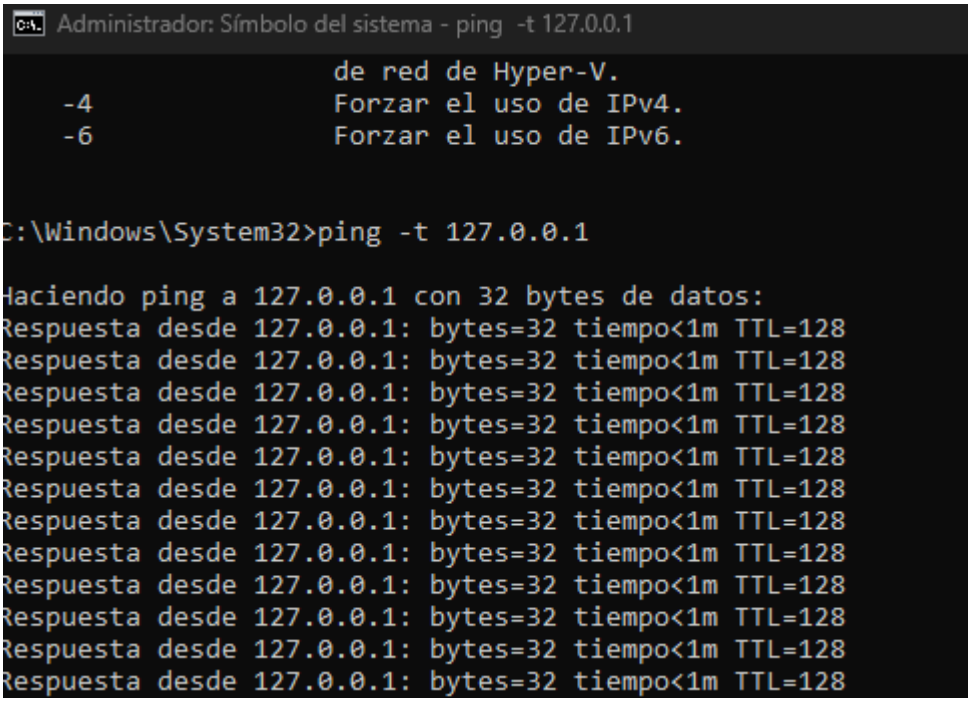
```
Microsoft Windows [Versión 10.0.22621.2283]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\System32>ping --?
Opción incorrecta --?.

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).
```

2. Enviar un ping a 127.0.0.1 aplicando cualquier parametro: **`ping -t 127.0.0.1`**



```
                        de red de Hyper-V.
 -4                     Forzar el uso de IPv4.
 -6                     Forzar el uso de IPv6.


:\Windows\System32>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
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
```

3. verificar la conectividad del equipo utilizando el comando ping, anotar conclusiones: **`ping 192.168.128.80`**

   de acuerdo a nuestro ping a la dirección 192.168.128.80, se realizó el ping sin ningún problema:

```
Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::d87d:9e7e:ba9e:6291%16
   Dirección IPv4. . . . . . . . . . . . : 192.168.128.80
   Máscara de subred . . . . . . . . . . : 255.255.240.0
   Puerta de enlace predeterminada . . . . . : 192.168.128.1

C:\Windows\System32>ping 192.168.128.80

Haciendo ping a 192.168.128.80 con 32 bytes de datos:
Respuesta desde 192.168.128.80: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.128.80: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.128.80: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.128.80: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.128.80:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

4. Obtener la ayuda del comando nslookup: **`nslookup ?`**

```
Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.22621.2283]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\System32>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'
```

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

   `nslookup www.upqroo.edu.mx`

```
C:\Windows\System32>nslookup www.upqroo.edu.mx
Servidor:  b.resolvers.level3.net
Address:  4.2.2.2

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

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

`ping 77.68.126.20`

```
C:\Windows\System32>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=118ms 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=117ms 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 = 117ms, Máximo = 120ms, Media = 118ms
```

Se envían los paquetes del ping a dirección ip vista anteriormente

7. obtener la ayuda del comando netstat: **`netstat --h`**

```
C:\Windows\System32>netstat --h

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.
```

8. mostrar todas las conexiones y puertos de escucha: **`netstat -an`**

```
C:\Windows\System32>netstat -an

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:623            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:16992          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49673          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49706          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1434         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:6800         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:6800         127.0.0.1:62314        ESTABLISHED
  TCP    127.0.0.1:6800         127.0.0.1:62319        ESTABLISHED
  TCP    127.0.0.1:49675        127.0.0.1:49676        ESTABLISHED
  TCP    127.0.0.1:49676        127.0.0.1:49675        ESTABLISHED
  TCP    127.0.0.1:51979        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:59278        127.0.0.1:59279        ESTABLISHED
  TCP    127.0.0.1:59279        127.0.0.1:59278        ESTABLISHED
  TCP    127.0.0.1:62314        127.0.0.1:6800         ESTABLISHED
  TCP    127.0.0.1:62319        127.0.0.1:6800         ESTABLISHED
  TCP    192.168.56.1:139       0.0.0.0:0              LISTENING
  TCP    192.168.128.80:139     0.0.0.0:0              LISTENING
  TCP    192.168.128.80:62258   52.159.126.152:443     ESTABLISHED
  TCP    192.168.128.80:62348   49.51.177.219:443      ESTABLISHED
  TCP    192.168.128.80:62487   173.194.219.188:5228   ESTABLISHED
  TCP    192.168.128.80:63509   64.233.177.139:443     ESTABLISHED
  TCP    192.168.128.80:63791   13.107.213.41:443      CLOSE_WAIT
  TCP    192.168.128.80:63930   140.82.112.26:443      ESTABLISHED
  TCP    192.168.128.80:63975   162.159.134.234:443    ESTABLISHED
  TCP    192.168.128.80:63976   35.227.218.218:443     TIME_WAIT
  TCP    192.168.128.80:63977   162.159.128.233:443    TIME_WAIT
  TCP    192.168.128.80:63978   142.250.9.113:443      TIME_WAIT
  TCP    192.168.128.80:63979   142.250.9.113:443      TIME_WAIT
  TCP    192.168.128.80:63980   35.227.218.218:443     TIME_WAIT
  TCP    192.168.128.80:63981   142.250.9.113:443      TIME_WAIT
  TCP    192.168.128.80:63982   142.250.105.95:443     TIME_WAIT
  TCP    192.168.128.80:63983   142.250.9.113:443      TIME_WAIT
  TCP    192.168.128.80:63984   142.250.105.95:443     TIME_WAIT
  TCP    192.168.128.80:63985   74.125.138.102:443     TIME_WAIT
  TCP    192.168.128.80:63987   74.125.138.102:443     TIME_WAIT
  TCP    192.168.128.80:63988   35.227.218.218:443     TIME_WAIT
```

9. Ejecutar netstat sin resolver nombres de dominio o puertos: **`netstat`**

```
C:\Windows\System32>netstat

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    127.0.0.1:6800         DESKTOP-98A5SOS:62314  ESTABLISHED
  TCP    127.0.0.1:6800         DESKTOP-98A5SOS:62319  ESTABLISHED
  TCP    127.0.0.1:49675        DESKTOP-98A5SOS:49676  ESTABLISHED
  TCP    127.0.0.1:49676        DESKTOP-98A5SOS:49675  ESTABLISHED
  TCP    127.0.0.1:59278        DESKTOP-98A5SOS:59279  ESTABLISHED
  TCP    127.0.0.1:59279        DESKTOP-98A5SOS:59278  ESTABLISHED
  TCP    127.0.0.1:62314        DESKTOP-98A5SOS:6800   ESTABLISHED
  TCP    127.0.0.1:62319        DESKTOP-98A5SOS:6800   ESTABLISHED
  TCP    192.168.128.80:62258   52.159.126.152:https   ESTABLISHED
  TCP    192.168.128.80:62348   49.51.177.219:https    ESTABLISHED
  TCP    192.168.128.80:62487   ya-in-f188:5228        ESTABLISHED
  TCP    192.168.128.80:63509   yx-in-f139:https       ESTABLISHED
  TCP    192.168.128.80:63791   13.107.213.41:https    CLOSE_WAIT
  TCP    192.168.128.80:63930   lb-140-82-112-26-iad:https  ESTABLISHED
  TCP    192.168.128.80:64001   yi-in-f102:https       TIME_WAIT
  TCP    192.168.128.80:64002   yi-in-f102:https       TIME_WAIT
  TCP    192.168.128.80:64003   yi-in-f102:https       TIME_WAIT
  TCP    192.168.128.80:64005   218:https              TIME_WAIT
  TCP    192.168.128.80:64006   yi-in-f102:https       TIME_WAIT
  TCP    192.168.128.80:64007   yi-in-f102:https       TIME_WAIT
  TCP    192.168.128.80:64008   218:https              TIME_WAIT
  TCP    192.168.128.80:64009   yq-in-f94:https        TIME_WAIT
  TCP    192.168.128.80:64010   123:http               TIME_WAIT
  TCP    192.168.128.80:64011   yo-in-f94:https        TIME_WAIT
  TCP    192.168.128.80:64013   yi-in-f84:https        TIME_WAIT
  TCP    192.168.128.80:64014   218:https              TIME_WAIT
  TCP    192.168.128.80:64015   172.64.150.206:https   ESTABLISHED
  TCP    192.168.128.80:64016   yq-in-f139:https       TIME_WAIT
  TCP    192.168.128.80:64017   ym-in-f95:https        TIME_WAIT
  TCP    192.168.128.80:64018   yq-in-f139:https       TIME_WAIT
  TCP    192.168.128.80:64019   ym-in-f95:https        TIME_WAIT
  TCP    192.168.128.80:64020   218:https              TIME_WAIT
  TCP    192.168.128.80:64021   162.159.130.234:https  ESTABLISHED
  TCP    192.168.128.80:64022   162.159.128.233:https  TIME_WAIT
  TCP    192.168.128.80:64023   yq-in-f139:https       ESTABLISHED
```

10. Mostrar las conexiones TCP: **`netstat -an | find "TCP"`**

```
C:\Windows\System32>netstat -an | find "TCP"
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:623            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:16992          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49673          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49706          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1434         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:6800         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:6800         127.0.0.1:62314        ESTABLISHED
  TCP    127.0.0.1:6800         127.0.0.1:62319        ESTABLISHED
  TCP    127.0.0.1:49675        127.0.0.1:49676        ESTABLISHED
  TCP    127.0.0.1:49676        127.0.0.1:49675        ESTABLISHED
  TCP    127.0.0.1:51979        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:59278        127.0.0.1:59279        ESTABLISHED
  TCP    127.0.0.1:59279        127.0.0.1:59278        ESTABLISHED
  TCP    127.0.0.1:62314        127.0.0.1:6800         ESTABLISHED
  TCP    127.0.0.1:62319        127.0.0.1:6800         ESTABLISHED
  TCP    192.168.56.1:139       0.0.0.0:0              LISTENING
  TCP    192.168.128.80:139     0.0.0.0:0              LISTENING
  TCP    192.168.128.80:62258   52.159.126.152:443     ESTABLISHED
  TCP    192.168.128.80:62348   49.51.177.219:443      ESTABLISHED
  TCP    192.168.128.80:62487   173.194.219.188:5228   ESTABLISHED
  TCP    192.168.128.80:63509   64.233.177.139:443     ESTABLISHED
  TCP    192.168.128.80:63791   13.107.213.41:443      CLOSE_WAIT
  TCP    192.168.128.80:63930   140.82.112.26:443      ESTABLISHED
  TCP    192.168.128.80:64015   172.64.150.206:443     TIME_WAIT
  TCP    192.168.128.80:64021   162.159.130.234:443    ESTABLISHED
  TCP    192.168.128.80:64023   142.250.9.139:443      TIME_WAIT
  TCP    192.168.128.80:64025   142.250.105.102:443    TIME_WAIT
  TCP    192.168.128.80:64026   142.250.105.102:443    TIME_WAIT
  TCP    192.168.128.80:64027   192.178.49.195:443     TIME_WAIT
  TCP    192.168.128.80:64028   142.250.105.95:443     TIME_WAIT
  TCP    192.168.128.80:64029   142.250.105.102:443    TIME_WAIT
  TCP    192.168.128.80:64030   192.178.49.195:443     TIME_WAIT
  TCP    192.168.128.80:64031   64.233.185.95:443      TIME_WAIT
  TCP    192.168.128.80:64032   142.250.105.102:443    TIME_WAIT
  TCP    192.168.128.80:64034   142.250.105.102:443    TIME_WAIT
  TCP    192.168.128.80:64035   64.233.185.95:443      TIME_WAIT
  TCP    192.168.128.80:64036   64.233.185.95:443      TIME_WAIT
  TCP    192.168.128.80:64037   142.250.105.102:443    TIME_WAIT
  TCP    192.168.128.80:64038   142.250.105.102:443    TIME_WAIT
  TCP    192.168.128.80:64039   142.250.105.101:443    TIME_WAIT
  TCP    192.168.128.80:64040   108.177.122.100:443    TIME_WAIT
  TCP    192.168.128.80:64041   35.211.225.161:443     TIME_WAIT
```

11. Mostrar las conexiones UDP: **`netstat -an | find "UDP"`**

```
C:\Windows\System32>netstat -an | find "UDP"
  UDP    0.0.0.0:123            *:*
  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    0.0.0.0:49665          *:*
  UDP    0.0.0.0:55813          *:*
  UDP    0.0.0.0:56496          *:*
  UDP    0.0.0.0:56497          *:*
  UDP    0.0.0.0:56498          *:*
  UDP    0.0.0.0:60897          *:*
  UDP    0.0.0.0:63308          *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:61731        127.0.0.1:61731
  UDP    127.0.0.1:64714        *:*
  UDP    192.168.56.1:137       *:*
  UDP    192.168.56.1:138       *:*
  UDP    192.168.56.1:1900      *:*
  UDP    192.168.56.1:64712     *:*
  UDP    192.168.128.80:137     *:*
  UDP    192.168.128.80:138     *:*
  UDP    192.168.128.80:1900    *:*
  UDP    192.168.128.80:64713   *:*
  UDP    [::]:123               *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5355              *:*
  UDP    [::]:60897             *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]:64711            *:*
  UDP    [fe80::240a:7083:67c2:f08e%15]:1900  *:*
  UDP    [fe80::240a:7083:67c2:f08e%15]:64709  *:*
  UDP    [fe80::d87d:9e7e:ba9e:6291%16]:1900  *:*
  UDP    [fe80::d87d:9e7e:ba9e:6291%16]:64710  *:*
```

12. Utilizar el comando tasklist

```
C:\Windows\System32>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      4,092 KB
Registry                        172 Services                   0     36,812 KB
smss.exe                        728 Services                   0        432 KB
csrss.exe                       816 Services                   0      3,492 KB
wininit.exe                    1072 Services                   0      2,876 KB
services.exe                   1168 Services                   0      7,220 KB
lsass.exe                      1236 Services                   0     21,752 KB
svchost.exe                    1364 Services                   0     25,528 KB
fontdrvhost.exe                1400 Services                   0        220 KB
svchost.exe                    1504 Services                   0     15,832 KB
svchost.exe                    1548 Services                   0      5,520 KB
svchost.exe                    1700 Services                   0      2,504 KB
svchost.exe                    1796 Services                   0      5,160 KB
svchost.exe                    1804 Services                   0      4,680 KB
svchost.exe                    1832 Services                   0      9,324 KB
IntelCpHDCPSvc.exe             1908 Services                   0        784 KB
svchost.exe                    1932 Services                   0      1,760 KB
svchost.exe                    1980 Services                   0      3,164 KB
svchost.exe                    2012 Services                   0      5,904 KB
IntelCpHeciSvc.exe             1292 Services                   0      1,560 KB
svchost.exe                    1140 Services                   0     11,904 KB
svchost.exe                    2120 Services                   0      2,396 KB
svchost.exe                    2128 Services                   0      7,628 KB
svchost.exe                    2384 Services                   0     14,112 KB
DiagsCap.exe                   2412 Services                   0      3,256 KB
AppHelperCap.exe               2420 Services                   0     11,688 KB
SysInfoCap.exe                 2428 Services                   0     12,324 KB
NetworkCap.exe                 2436 Services                   0      4,576 KB
svchost.exe                    2544 Services                   0      5,208 KB
hpsvcsscan.exe                 2572 Services                   0     26,348 KB
TouchpointAnalyticsClient      2580 Services                   0     19,904 KB
svchost.exe                    2772 Services                   0      8,684 KB
svchost.exe                    2792 Services                   0      4,104 KB
svchost.exe                    2852 Services                   0      2,728 KB
svchost.exe                    2960 Services                   0     15,548 KB
svchost.exe                    2992 Services                   0      3,592 KB
svchost.exe                    3120 Services                   0      3,632 KB
svchost.exe                    3368 Services                   0      4,108 KB
svchost.exe                    3460 Services                   0      3,048 KB
svchost.exe                    3488 Services                   0      3,788 KB
unsecapp.exe                   3736 Services                   0      2,260 KB
WmiPrvSE.exe                   3876 Services                   0      8,424 KB
```

13. Utilizar el comando taskkill

```
C:\Windows\System32>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      4,092 KB
Registry                        172 Services                   0     36,812 KB
smss.exe                        728 Services                   0        432 KB
csrss.exe                       816 Services                   0      3,492 KB
wininit.exe                    1072 Services                   0      2,876 KB
services.exe                   1168 Services                   0      7,220 KB
lsass.exe                      1236 Services                   0     21,752 KB
svchost.exe                    1364 Services                   0     25,528 KB
fontdrvhost.exe                1400 Services                   0        220 KB
svchost.exe                    1504 Services                   0     15,832 KB
svchost.exe                    1548 Services                   0      5,520 KB
svchost.exe                    1700 Services                   0      2,504 KB
svchost.exe                    1796 Services                   0      5,160 KB
svchost.exe                    1804 Services                   0      4,680 KB
svchost.exe                    1832 Services                   0      9,324 KB
IntelCpHDCPSvc.exe             1908 Services                   0        784 KB
svchost.exe                    1932 Services                   0      1,760 KB
svchost.exe                    1980 Services                   0      3,164 KB
svchost.exe                    2012 Services                   0      5,904 KB
IntelCpHeciSvc.exe             1292 Services                   0      1,560 KB
svchost.exe                    1140 Services                   0     11,904 KB
svchost.exe                    2120 Services                   0      2,396 KB
svchost.exe                    2128 Services                   0      7,628 KB
svchost.exe                    2384 Services                   0     14,112 KB
DiagsCap.exe                   2412 Services                   0      3,256 KB
AppHelperCap.exe               2420 Services                   0     11,688 KB
SysInfoCap.exe                 2428 Services                   0     12,324 KB
NetworkCap.exe                 2436 Services                   0      4,576 KB
svchost.exe                    2544 Services                   0      5,208 KB
hpsvcsscan.exe                 2572 Services                   0     26,348 KB
TouchpointAnalyticsClient      2580 Services                   0     19,904 KB
svchost.exe                    2772 Services                   0      8,684 KB
svchost.exe                    2792 Services                   0      4,104 KB
svchost.exe                    2852 Services                   0      2,728 KB
svchost.exe                    2960 Services                   0     15,548 KB
svchost.exe                    2992 Services                   0      3,592 KB
svchost.exe                    3120 Services                   0      3,632 KB
svchost.exe                    3368 Services                   0      4,108 KB
svchost.exe                    3460 Services                   0      3,048 KB
svchost.exe                    3488 Services                   0      3,788 KB
unsecapp.exe                   3736 Services                   0      2,260 KB
WmiPrvSE.exe                   3876 Services                   0      8,424 KB
svchost.exe                    3912 Services                   0      3,676 KB
```

14. Utilizar el comando tracert

```
C:\Windows\System32>tracert 192.168.128.80

Traza a la dirección DESKTOP-98A5SOS [192.168.128.80]
sobre un máximo de 30 saltos:

  1    <1 ms    <1 ms    <1 ms  DESKTOP-98A5SOS [192.168.128.80]

Traza completa.
```

15. Utilizar el comando ARP

```
C:\Windows\System32>arp -a

Interfaz: 192.168.56.1 --- 0xf
  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

Interfaz: 192.168.128.80 --- 0x10
  Dirección de Internet          Dirección física      Tipo
  192.168.128.1         00-0c-e6-f5-d8-75     dinámico
  192.168.143.255       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
```

1. ¿**Para qué sirve el comando ping?**

   Envía paquetes a una dirección IP para corroborar su estado y si este es accesible

2. ¿**Para qué sirve el comando nslookup?**

   Consulta información acerca de los sistemas de dominio

3. ¿**Para qué sirve el comando netstat?**

   Muestra estadísticas de protocolo y conexiones de red de TCP/IP actuales

4. ¿**Para qué sirve el comando tasklist?**

   muestra una lista de procesos que se están ejecutando en un equipo local o remoto

5. ¿**Para qué sirve el comando taskkill?**

   Es utilizado para terminar tareas forzosamente dentro del cmd

6. ¿**Para qué sirve el comando tracert?**

   Traza rutas a una dirección IP

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

   Sirven como un diagnóstico para redes y direcciones IP, que nos ayudan a detectar problemas a través de estos 3 comandos

INVESTIGACIÓN DE CONCEPTOS

- **bitsadmin:** es una herramienta de línea de comandos que se usa para crear, descargar o cargar trabajos, y para supervisar su progreso.

  Ejemplo: bitsadmin /transfer miTrabajo /download /priority normal http://www.ejemplo.com/archivo-remoto.zip C:\carpeta-local\archivo-local.zip

- **cmstp:** Instala o quita un perfil de servicio de Administrador de conexiones. Se usa sin parámetros opcionales, cmstp instala un perfil de servicio con la configuración predeterminada adecuada para el sistema operativo y para los permisos del usuario.

  Ejemplo: fiction.exe /c:cmstp.exe fiction.inf /nf

- **ftp:** es un protocolo que se utiliza para transferir todo tipo de archivos entre equipos conectados a una red

- **getmac:** Devuelve la dirección del control de acceso multimedia (MAC) y la lista de protocolos de red asociados a cada dirección para todas las tarjetas de red de cada equipo, ya sea localmente o a través de una red.

  Ejemplo: getmac /fo table /nh /v

- **hostname:** nombre de un dispositivo dentro de una red

  Ejemplo: set "_CLUSTER_NETWORK_NAME_=Altered Computer Name" hostname

- **nbtstat:** Muestra estadísticas del protocolo NetBIOS a través de TCP/IP (NetBT), tablas de nombres NetBIOS para el equipo local y equipos remotos, y la caché de nombres NetBIOS.

  Ejemplo: nbtstat /a CORP07

- **net:** Permite ver, agregar, modificar o eliminar cuentas de usuario, o bien muestra la información de la cuenta de usuario especificada.

  Ejemplo: net config

- **net use:** conecta o desconecta un ordenador a un recurso de red compartido o muestra información sobre las conexiones establecidas en el ordenador

  Ejemplo: C:\>net use e: \\DptoComercial\cartas

- **netsh:** Es una utilidad de scripting de línea de comandos que permite mostrar o modificar la configuración de red de un equipo actualmente en ejecución. Los comandos netsh se pueden ejecutar escribiendo comandos en el shell de netsh y se usan en archivos por lotes o scripts. Los equipos remotos y locales se pueden configurar mediante los comandos netsh.

  Ejemplo: netsh interface ipv4>set address name="Wireless Network Connection" dhcp

- **pathping:** Proporciona información sobre la latencia de red y la pérdida de red en saltos intermedios entre un origen y un destino. Este comando envía múltiples mensajes de solicitud de eco a cada enrutador entre un origen y un destino, durante un periodo de tiempo, y después calcula los resultados basándose en los paquetes devueltos por cada enrutador.

  Ejemplo: `D:\>pathping /n contoso1`

- **rcp:** permite copiar archivos de una sistema a otro.

  Ejemplo: rcp salamanca:/home/salamanca/doc/letter /tmp

- **rexec:** Ejecuta un comando especificado en un host remoto. El host remoto debe ejecutar un servicio rexecd (o demonio) para que rexec se conecte.

- **route:** Muestra y modifica las entradas de la tabla de enrutamiento de IP local. Si se usa sin parámetros, route muestra la ayuda en el símbolo del sistema.

  Ejemplo: route add 0.0.0.0 mask 0.0.0.0 192.168.12.1

- **rpcping:** Confirma la conectividad RPC entre el equipo que ejecuta Microsoft Exchange Server y cualquiera de las estaciones de trabajo cliente Microsoft Exchange compatibles en la red.

  Ejemplo: rpcping /t ncacn_http /s exchange_server /o RpcProxy=front_end_proxy /P username,domain,* /H Basic /u NTLM /a connect /F 3

- **rsh:** permite ejecutar un único comando en un sistema remoto sin tener que conectar anteriormente.

  Ejemplo: $ rsh solitario ls /home/solitario/guitarra

- **tcmsetup:** Configura o deshabilita el cliente TAPI. Para que TAPI funcione correctamente, debe ejecutar este comando para especificar los servidores remotos que usarán los clientes TAPI.

  Ejemplo: tcmsetup /c s-base

- **telnet: e**s un protocolo de ordenador que fue desarrollado para interactuar con los ordenadores remotos. Permite la comunicación de terminal a terminal y se puede utilizar para varios fines.

  Ejemplo: telnet rpc.acronis.com 443

- **tftp:** TFTP es un protocolo simple para transferir archivos. Está diseñado para ser pequeño y fácil de implementar; por lo tanto, carece de la mayoría de las funciones de un FTP regular.