



UNIVERSIDAD
POLITÉCNICA
DE QUINTANA ROO

UPQROO

Cuatrimestre:

27AV

Materia:

Sistemas Operativos

Profesor:

Ismael Jimenez

Alumno:

Carlos Mauricio Camara Andueza

Tarea #987

Práctica de laboratorio

Comandos en MSDOS

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

1. Obtener la ayuda del comando ping

```
C:\Users\Forma>ping /?

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

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

C:\Users\Forma>_
```

2. Enviar un ping a 127.0.0.1 aplicando cualquier parámetro

```
C:\WINDOWS\system32\cmd.exe

C:\Users\Forma>ping 127.0.0.1 -n 4

Haciendo ping a 127.0.0.1 con 32 bytes de datos:
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128

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

C:\Users\Forma>
```

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

```
C:\WINDOWS\system32\cmd.exe

C:\Users\Forma>ping upqroo.edu.mx

Haciendo ping a upqroo.edu.mx [77.68.126.20] con 32 bytes de datos:
Respuesta desde 77.68.126.20: bytes=32 tiempo=121ms TTL=50
Respuesta desde 77.68.126.20: bytes=32 tiempo=122ms 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

Estadísticas de ping para 77.68.126.20:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 118ms, Máximo = 122ms, Media = 120ms

C:\Users\Forma>
```

Se envía todos los paquetes de la red a upqroo.edu.mx

4. Obtener la ayuda del comando nslookup

```
C:\WINDOWS\system32\cmd.exe - nslookup

C:\Users\Forma>nslookup
Servidor predeterminado: dns.google
Address: 8.8.8.8

> help
Comandos: (los identificadores se muestran en mayúsculas, [] significa opcional)
NOMBRE - imprimir información acerca de NOMBRE de host o de dominio con el servidor predeterminado
NOMBRE1 NOMBRE2 - igual que el anterior, pero se usa NOMBRE2 como servidor
help o ? - imprimir información acerca de comandos comunes
set OPCIÓN - establecer una opción
    all - opciones de impresión, servidor actual y host
    [no]debug - imprimir información de depuración
    [no]d2 - imprimir información de depuración exhaustiva
    [no]defname - anexas el nombre de dominio a cada consulta
    [no]recurse - pedir respuesta recursiva a la consulta
    [no]search - usar la lista de búsqueda de dominios
    [no]vc - usar siempre un circuito virtual
    domain=NOMBRE - establecer nombre de dominio predeterminado en NOMBRE
    srchlist=N1[/N2/.../N6] - establecer dominio en N1 y lista de búsqueda en N1,N2, etc.
    root=NOMBRE - establecer servidor raíz en NOMBRE
    retry=X - establecer número de reintentos en X
    timeout=X - establecer intervalo de tiempo de espera inicial en X segundos
    type=X - establecer tipo de consulta (p. ej., A,AAAA,A+AAAA,ANY,CNAME,MX,NS,PTR,SOA,SRV)
    querytype=X - igual que type
    class=X - establecer clase de consulta (p. ej., IN (Internet), ANY)
    [no]mxfr - usar transferencia de zona rápida MX
    ixfrver=X - versión actual que se usará en la solicitud de transferencia IXFR
    server NOMBRE - establecer el servidor predeterminado en NOMBRE con el servidor predeterminado actual
    lserver NOMBRE - establecer el servidor predeterminado en NOMBRE con el servidor inicial
    root - establecer el servidor predeterminado actual en la raíz
    ls [opt] DOMINIO [> ARCHIVO] - enumerar las direcciones de DOMINIO (opcional: enviar el resultado a ARCHIVO)
        -a - enumerar nombres canónicos y alias
        -d - enumerar todos los registros
        -t TIPO - enumerar los registros del tipo de registro RFC dado (p. ej., A,CNAME,MX,NS,PTR etc.)
    view ARCHIVO - ordenar un archivo de resultados 'ls' y verlo con pg
    exit - salir del programa

> _
```

5. Resolver la dirección ip de <https://upgroo.edu.mx/> usando nslookup

```
C:\WINDOWS\system32\cmd.exe

C:\Users\Forma>ping upgroo.edu.mx

Haciendo ping a upgroo.edu.mx [77.68.126.20] con 32 bytes de datos:
Respuesta desde 77.68.126.20: bytes=32 tiempo=121ms TTL=50
Respuesta desde 77.68.126.20: bytes=32 tiempo=122ms 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

Estadísticas de ping para 77.68.126.20:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 118ms, Máximo = 122ms, Media = 120ms

C:\Users\Forma>nslookup upgroo.edu.mx
Servidor: dns.google
Address: 8.8.8.8

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

C:\Users\Forma>_
```

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

```
C:\WINDOWS\system32\cmd.exe

C:\Users\Forma>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=120ms TTL=50
Respuesta desde 77.68.126.20: bytes=32 tiempo=126ms TTL=50
Respuesta desde 77.68.126.20: bytes=32 tiempo=123ms TTL=50
Respuesta desde 77.68.126.20: bytes=32 tiempo=120ms 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 = 120ms, Máximo = 126ms, Media = 122ms

C:\Users\Forma>
```

Se envían todos los paquetes al ping 77.68.126.20 sin pérdida de paquetes.

7. Obtener la ayuda del comando netstat

```
C:\WINDOWS\system32\cmd.exe

C:\Users\Forma>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 omitas esta opción, netstat imprimirá una sola vez
        la información de configuración.

C:\Users\Forma>
```

8. Mostrar todas las conexiones y puertos de escucha

```
C:\WINDOWS\system32\cmd.exe
^C
C:\Users\Forma>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    0.0.0.0:5040          0.0.0.0:0             LISTENING
TCP    0.0.0.0:7680          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    0.0.0.0:49667         0.0.0.0:0             LISTENING
TCP    0.0.0.0:49668         0.0.0.0:0             LISTENING
TCP    0.0.0.0:49674         0.0.0.0:0             LISTENING
TCP    0.0.0.0:49676         0.0.0.0:0             LISTENING
TCP    127.0.0.1:6463        0.0.0.0:0             LISTENING
TCP    127.0.0.1:50342       127.0.0.1:65001       ESTABLISHED
TCP    127.0.0.1:50344       0.0.0.0:0             LISTENING
TCP    127.0.0.1:65001       0.0.0.0:0             LISTENING
TCP    127.0.0.1:65001       127.0.0.1:50342       ESTABLISHED
TCP    172.16.128.34:139     0.0.0.0:0             LISTENING
TCP    172.16.128.34:49741   52.159.127.243:443     ESTABLISHED
TCP    172.16.128.34:49768   3.232.144.130:443      ESTABLISHED
TCP    172.16.128.34:50106   162.159.133.234:443    ESTABLISHED
TCP    172.16.128.34:50224   187.190.14.12:443      ESTABLISHED
TCP    172.16.128.34:50225   209.85.231.39:443      ESTABLISHED
TCP    172.16.128.34:50308   20.94.21.149:443       ESTABLISHED
TCP    172.16.128.34:50321   20.7.1.246:443         ESTABLISHED
TCP    172.16.128.34:50379   8.8.8.8:443            ESTABLISHED
TCP    172.16.128.34:50442   157.240.14.15:443      ESTABLISHED
TCP    172.16.128.34:50444   157.240.14.1:443       ESTABLISHED
TCP    172.16.128.34:50445   157.240.14.15:443      ESTABLISHED
TCP    172.16.128.34:50454   157.240.14.15:443      ESTABLISHED
TCP    172.16.128.34:50456   157.240.14.50:443      ESTABLISHED
TCP    172.16.128.34:50466   20.94.21.149:443       ESTABLISHED
TCP    172.16.128.34:50584   172.64.150.28:443      ESTABLISHED
TCP    172.16.128.34:50589   108.177.13.190:443     ESTABLISHED
TCP    172.16.128.34:50596   8.8.4.4:443            TIME_WAIT
TCP    172.16.128.34:50598   172.217.3.67:443       TIME_WAIT
TCP    172.16.128.34:50607   8.8.8.8:443            ESTABLISHED
TCP    172.16.128.34:50608   172.217.3.67:443       ESTABLISHED
TCP    172.16.128.34:50610   189.203.151.145:443    ESTABLISHED
TCP    172.16.128.34:50611   20.69.137.228:443      ESTABLISHED
TCP    172.16.128.34:50612   13.107.5.80:443        ESTABLISHED
TCP    172.16.128.34:50613   13.107.246.57:443      CLOSE_WAIT
TCP    172.16.128.34:50614   204.79.197.200:443     ESTABLISHED
```

9. Ejecutar netstat sin resolver nombres de dominio o puertos

```
C:\WINDOWS\system32\cmd.exe
^C
C:\Users\Forma>netstat -a

Conexiones activas

Proto  Dirección local      Dirección remota      Estado
TCP    0.0.0.0:135           LAPTOP-TUACSKFP:0     LISTENING
TCP    0.0.0.0:445           LAPTOP-TUACSKFP:0     LISTENING
TCP    0.0.0.0:5040          LAPTOP-TUACSKFP:0     LISTENING
TCP    0.0.0.0:7680          LAPTOP-TUACSKFP:0     LISTENING
TCP    0.0.0.0:49664         LAPTOP-TUACSKFP:0     LISTENING
TCP    0.0.0.0:49665         LAPTOP-TUACSKFP:0     LISTENING
TCP    0.0.0.0:49666         LAPTOP-TUACSKFP:0     LISTENING
TCP    0.0.0.0:49667         LAPTOP-TUACSKFP:0     LISTENING
TCP    0.0.0.0:49668         LAPTOP-TUACSKFP:0     LISTENING
TCP    0.0.0.0:49674         LAPTOP-TUACSKFP:0     LISTENING
TCP    0.0.0.0:49676         LAPTOP-TUACSKFP:0     LISTENING
TCP    127.0.0.1:6463        LAPTOP-TUACSKFP:0     LISTENING
TCP    127.0.0.1:50342       LAPTOP-TUACSKFP:65001 ESTABLISHED
TCP    127.0.0.1:50344       LAPTOP-TUACSKFP:0     LISTENING
TCP    127.0.0.1:65001       LAPTOP-TUACSKFP:0     LISTENING
TCP    127.0.0.1:65001       LAPTOP-TUACSKFP:50342 ESTABLISHED
TCP    172.16.128.34:139     LAPTOP-TUACSKFP:0     LISTENING
TCP    172.16.128.34:49741   52.159.127.243:https   ESTABLISHED
TCP    172.16.128.34:49768   ec2-3-232-144-130:https ESTABLISHED
TCP    172.16.128.34:50106   162.159.133.234:https  ESTABLISHED
TCP    172.16.128.34:50224   fixed-187-190-14-12:https ESTABLISHED
TCP    172.16.128.34:50225   mia07s69-in-f7:https   ESTABLISHED
TCP    172.16.128.34:50308   20.94.21.149:https     ESTABLISHED
TCP    172.16.128.34:50321   20.7.1.246:https       ESTABLISHED
TCP    172.16.128.34:50379   dns:https              ESTABLISHED
TCP    172.16.128.34:50442   edge-star-shv-02-mia3:https ESTABLISHED
TCP    172.16.128.34:50444   edge-dgw-shv-02-mia3:https ESTABLISHED
TCP    172.16.128.34:50445   edge-star-shv-02-mia3:https ESTABLISHED
TCP    172.16.128.34:50454   edge-star-shv-02-mia3:https ESTABLISHED
TCP    172.16.128.34:50456   edge-z-p3-shv-02-mia3:https ESTABLISHED

^C
C:\Users\Forma>
```

10. Mostrar las conexiones TCP

```
C:\WINDOWS\system32\cmd.exe - netstat -t
C:\Users\Forma>netstat -t

Conexiones activas

Proto  Dirección local      Dirección remota      Estado
Estado de descarga

TCP    127.0.0.1:50342       LAPTOP-TUAC5KFP:65001 ESTABLISHED           EnHost
TCP    127.0.0.1:65001       LAPTOP-TUAC5KFP:50342 ESTABLISHED           EnHost
TCP    172.16.128.34:49741   52.159.127.243:https  ESTABLISHED           EnHost
TCP    172.16.128.34:49768   ec2-3-232-144-130:https ESTABLISHED           EnHost
TCP    172.16.128.34:50106   162.159.133.234:https ESTABLISHED           EnHost
TCP    172.16.128.34:50224   fixed-187-190-14-12:https ESTABLISHED           EnHost
TCP    172.16.128.34:50225   mia07s69-in-f7:https  ESTABLISHED           EnHost
TCP    172.16.128.34:50308   20.94.21.149:https    ESTABLISHED           EnHost
TCP    172.16.128.34:50321   20.7.1.246:https      ESTABLISHED           EnHost
TCP    172.16.128.34:50379   dns:https             ESTABLISHED           EnHost
TCP    172.16.128.34:50442   edge-star-shv-02-mia3:https ESTABLISHED           EnHost
TCP    172.16.128.34:50444   edge-dgw-shv-02-mia3:https ESTABLISHED           EnHost
TCP    172.16.128.34:50445   edge-star-shv-02-mia3:https ESTABLISHED           EnHost
TCP    172.16.128.34:50454   edge-star-shv-02-mia3:https ESTABLISHED           EnHost
TCP    172.16.128.34:50456   edge-z-p3-shv-02-mia3:https ESTABLISHED           EnHost
```

11. Mostrar las conexiones UDP

```
C:\WINDOWS\system32\cmd.exe
C:\Users\Forma>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.

C:\Users\Forma>
```

12. Utilizar el comando tasklist

```
C:\WINDOWS\system32\cmd.exe

C:\Users\Forma>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    8.232 KB
Registry                  108 Services        0   53.980 KB
smss.exe                  664 Services        0    1.044 KB
csrss.exe                 760 Services        0    5.752 KB
csrss.exe                 864 Console         1    6.612 KB
wininit.exe              888 Services        0    6.744 KB
winlogon.exe             964 Console         1    2.184 KB
services.exe             984 Services        0   13.200 KB
lsass.exe                 72 Services        0   11.192 KB
svchost.exe              708 Services        0   15.576 KB
fontdrvhost.exe          724 Services        0    936 KB
fontdrvhost.exe          504 Console         1    5.456 KB
WUDFHost.exe             1076 Services        0    364 KB
svchost.exe              1156 Services        0   11.000 KB
svchost.exe              1208 Services        0    3.824 KB
dwm.exe                  1272 Console         1   35.276 KB
svchost.exe              1384 Services        0    3.956 KB
svchost.exe              1392 Services        0    892 KB
svchost.exe              1428 Services        0    1.144 KB
svchost.exe              1436 Services        0    1.004 KB
svchost.exe              1444 Services        0    5.084 KB
svchost.exe              1596 Services        0    2.412 KB
svchost.exe              1672 Services        0    332 KB
svchost.exe              1852 Services        0    356 KB
svchost.exe              1880 Services        0   11.612 KB
svchost.exe              1980 Services        0    2.484 KB
svchost.exe              1204 Services        0    8.996 KB
svchost.exe              1788 Services        0    1.160 KB
svchost.exe              2088 Services        0    980 KB
svchost.exe              2120 Services        0    4.832 KB
svchost.exe              2188 Services        0    3.256 KB
svchost.exe              2248 Services        0    4.452 KB
dashost.exe              2256 Services        0    5.044 KB
NVDisplay.Container.exe   2316 Services        0    2.672 KB
svchost.exe              2500 Services        0    5.488 KB
svchost.exe              2532 Services        0    5.688 KB
svchost.exe              2620 Services        0   94.780 KB
svchost.exe              2628 Services        0    840 KB
svchost.exe              2640 Services        0    4.128 KB
svchost.exe              2740 Services        0    5.464 KB
svchost.exe              2776 Services        0    2.620 KB
svchost.exe              2804 Services        0    336 KB
```

13. Utilizar el comando taskkill

```
C:\WINDOWS\system32\cmd.exe

CalculatorApp.exe          8428 Console         1    86.800 KB
RuntimeBroker.exe         4584 Console         1    20.860 KB
WmiPrvSE.exe              16076 Services        0    10.980 KB
tasklist.exe              10252 Console         1     9.288 KB

C:\Users\Forma>taskkill /PID 8428
Correcto: se envió la señal de término al proceso con PID 8428.

C:\Users\Forma>
```


14. Utilizar el comando tracert

```
C:\WINDOWS\system32\cmd.exe

C:\Users\Forma>tracert /?

Uso: tracert [-d] [-h saltos_máximos] [-j lista_de_hosts] [-w tiempo_de_espera]
      [-R] [-S srcaddr] [-4] [-6] nombre_destino

Opciones:
  -d          No convierte direcciones en nombres de hosts.
  -h saltos_máximos  Máxima cantidad de saltos en la búsqueda del objetivo.
  -j lista-host  Enrutamiento relajado de origen a lo largo de la
                  lista de hosts (solo IPv4).
  -w tiempo_espera  Tiempo de espera en milisegundos para esperar cada
                    respuesta.
  -R          Seguir la ruta de retorno (solo IPv6).
  -S srcaddr  Dirección de origen para utilizar (solo IPv6).
  -4          Forzar usando IPv4.
  -6          Forzar usando IPv6.

C:\Users\Forma>
```

15. Utilizar el comando ARP

```
C:\WINDOWS\system32\cmd.exe

C:\Users\Forma>ARP /?

Muestra y modifica las tablas de conversión de direcciones IP en direcciones
físicas que utiliza el protocolo de resolución de direcciones (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

-a          Pide los datos de protocolo actuales y muestra las
            entradas ARP actuales. Si se especifica inet_addr, solo se
            muestran las direcciones IP y física del equipo especificado.
            Si existe más de una interfaz de red que utilice ARP, se
            muestran las entradas de cada tabla ARP.
-g          Igual que -a.
-v          Muestra las entradas actuales de ARP en modo detallado.
            Se mostrarán todas las entradas no válidas y las entradas
            en la interfaz de bucle invertido.
inet_addr  Especifica una dirección de Internet.
-N if_addr Muestra las entradas ARP para la interfaz de red especificada
            por if_addr.
-d          Elimina el host especificado por inet_addr. inet_addr puede
            incluir el carácter comodín * (asterisco) para eliminar todos
            los host.
-s          Agrega el host y asocia la dirección de Internet inet_addr
            con la dirección física eth_addr. La dirección física se
            indica como 6 bytes en formato hexadecimal, separados por
            guiones. La entrada es permanente.
eth_addr   Especifica una dirección física.
if_addr    Si está presente, especifica la dirección de Internet de la
            interfaz para la que se debe modificar la tabla de conversión
            de direcciones. Si no está presente, se utilizará la primera
            interfaz aplicable.

Ejemplo:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Agrega una entrada estática
> arp -a .... Muestra la tabla ARP

C:\Users\Forma>
```

B) Contesta con tus propias palabras las siguientes preguntas:

1.- ¿Para que sirve el comando ping?

Sirve para comprobar una conexión al servidor de una web o de equipos.

2.- ¿Para que sirve el comando nslookup?

Sirve para consultar la dirección IP de un servidor o equipo determinado.

3.- ¿Para que sirve el comando netstat?

Nos sirve para mostrar un listado de las conexiones activas de una computadora.

4.- ¿Para que sirve el comando tasklist?

Con el tasklist nos permite obtener una lista de los procesos activos que se está ejecutando en la computadora.

5.- ¿Para que sirve el comando taskkill?

El taskkill nos permite detener tareas o procesos que están consumiendo recursos del sistema.

6.- ¿Para que sirve el comando tracert?

Tracert es una herramienta de diagnóstico de red que muestra la ruta que sigue un paquete de datos desde su origen hasta su destino.

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

Como se mencionó en la respuesta anterior, los tres comandos nos permite detectar los problemas en la red cuando notamos las pérdidas de paquetes entre el servidor y cuando el acceso al puerto se nos niegan.

C) Investigar los siguientes comandos y anotar ejemplos prácticos:

Comando	Que es	Ejemplos
atmadm	Supervisa las conexiones y direcciones registradas por el administrador de llamadas atM en una red de modo asincrónica.	atmadm -f status
bitsadmin	Se usa para crear, descargar o cargar trabajos, y para supervisar su progreso. La herramienta bitsadmin usa conmutadores para identificar el trabajo a realizar.	bitsadmin /create /job MiDescarga
cmstp	Instala o quita un perfil de servicio de Administrador de conexiones. Se usa sin parámetros opcionales.	cmstp /u <nombre_perfil>
ftp	Transfiere archivos hacia y desde un equipo que ejecuta un servicio de servidor del Protocolo de transferencia de archivos (ftp). Este comando se puede usar de forma interactiva o en modo por lotes mediante el procesamiento de archivos de texto ASCII.	ftp ftp.upqroo.edu.mx
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.	getmac /s srvmain /u maindom\hiropln /p p@ssW23
hostname	Muestra la parte del nombre de host del	hostname

	nombre del equipo completo del equipo.	
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.	nbtstat /n
net	es una herramienta de línea de comandos que proporciona una variedad de funcionalidades relacionadas con la administración de redes y servicios	net start [nombre_del_servicio]
net use	El comando NET USE conecta o desconecta un ordenador a un recurso de red compartido o muestra información sobre las conexiones establecidas en el ordenador.	net use [Letra_de_unidad]: \\equipo\recurso /user:usuario contraseña
netsh	La utilidad de scripting de línea de comandos Network Shell que le permite, de forma local o remota, visualizar o modificar la configuración de red de un equipo que se esté ejecutando en ese momento.	netsh interface ipv4 set address name="Nombre_de_la_interfaz" static [Dirección_IP] [Máscara_de_red] [Puerta_de_enlace]
pathping	Proporciona información sobre la latencia de red y la pérdida de red en saltos intermedios entre un origen y un destino.	D:\>pathping /n contoso1
rcp	El comando rcp le permite copiar archivos de una sistema a otro.	\$ 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.	Enable-PSRemoting -Force
route	El comando route muestra la tabla de enrutamiento que reside en el kernel y también se usa para modificarla. La tabla que especifica cómo se enrutan los paquetes a un host se llama tabla de enrutamiento.	route add 192.168.2.0 mask 255.255.255.0 192.168.1.1
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.	rpcping /t ncacn_http /s exchange_server /o RpcProxy=front_end_proxy /P username,domain,* /H Basic /u NTLM /a connect /F 3
rsh	Ejecuta comandos en equipos remotos que ejecutan el servicio o demonio de RSH.	ssh usuario@192.168.1.100
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.	tcmsetup [/q] [/x] /c <server1> [<server2> ...]
telnet	Se comunica con un equipo que ejecuta el servicio de servidor telnet. Al ejecutar este comando sin parámetros, puede escribir el contexto de telnet como se indica en el símbolo del sistema telnet.	telnet /f telnetlog.txt telnet.microsoft.com 44
tftp	Transfiere archivos hacia y desde un equipo remoto, normalmente un equipo que ejecuta UNIX, que ejecuta el servicio Trivial File Transfer Protocol (tftp) o demonio.	tftp -i Host1 get boot.img

Referencias bibliográficas

- JasonGerend (no date) *Atmadm*, *Microsoft Learn*. Available at: <https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/atmadm> (Accessed: 12 October 2023).
- JasonGerend (no date b) *Bitsadmin*, *Microsoft Learn*. Available at: <https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/bitsadmin> (Accessed: 12 October 2023).
- JasonGerend (no date c) *Cmstp*, *Microsoft Learn*. Available at: <https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/cmstp> (Accessed: 12 October 2023).
- JasonGerend (no date d) *FTP*, *Microsoft Learn*. Available at: <https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/ftp> (Accessed: 12 October 2023).
- JasonGerend (no date e) *Getmac*, *Microsoft Learn*. Available at: <https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/getmac> (Accessed: 12 October 2023).
- JasonGerend (no date f) *Hostname*, *Microsoft Learn*. Available at: <https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/hostname> (Accessed: 12 October 2023).
- JasonGerend (no date g) *NBTSTAT*, *Microsoft Learn*. Available at: <https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/nbtstat> (Accessed: 12 October 2023).
- Admin (2007) *El Comando Net del CMD - modificadores Al Completo*, *El Blog de soporteTI*. Available at: <https://blog.soporteti.net/el-comando-net-de-nuestro-cmd/> (Accessed: 12 October 2023).
- JasonGerend (no date h) *Netsh*, *Microsoft Learn*. Available at: <https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/netsh> (Accessed: 12 October 2023).
- JasonGerend (no date i) *Pathping*, *Microsoft Learn*. Available at: <https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/pathping> (Accessed: 12 October 2023).
- *Copiar Archivos a Distancia (RCP)* (no date) *Moved*. Available at: <https://docs.oracle.com/cd/E19620-01/805-7644/6j76kloqn/index.html#:~:text=Copiar%20archivos%20a%20distancia%20%28rcp%29%20El%20comando%20rcp,rcp%20es%20similar%20a%20la%20usada%20con%20cp.> (Accessed: 12 October 2023).
- JasonGerend (no date) *Rexec*, *Microsoft Learn*. Available at: <https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/rexec> (Accessed: 12 October 2023).
- *Comando Route* (no date) *EcuRed*. Available at: https://www.ecured.cu/Comando_Route#:~:text=Comando%20Route%201%20Descripci%C3%B3n%20El%20comando%20route%20muestra,de%20la%20tabla%20de%20enrutamiento%20IP%2C%20escriba%3A%20 (Accessed: 12 October 2023).
- JasonGerend (no date b) *Rpcping*, *Microsoft Learn*. Available at: <https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/rpcping> (Accessed: 12 October 2023).

- JasonGerend (no date c) *RSH*, *Microsoft Learn*. Available at: <https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/rsh> (Accessed: 12 October 2023).
- JasonGerend (no date d) *TFTP*, *Microsoft Learn*. Available at: <https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/tftp> (Accessed: 12 October 2023).
- JasonGerend (no date d) *Telnet*, *Microsoft Learn*. Available at: <https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/telnet> (Accessed: 12 October 2023).