UNIVERSIDAD POLITÉCNICA DE QUINTANA ROO

ELIAS IZQUIERDO COB

INGENIERÍA EN SOFTWARE

SISTEMAS OPERATIVOS

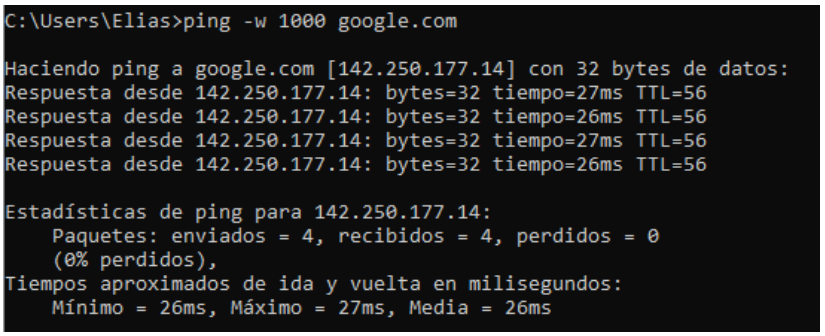
27BV

ACTIVIDAD:

1. ANOTAR LOS COMANDOS NECESARIOS PARA EJECUTAR LAS SIGUIENTES INSTRUCCIONES DESDE LA CONSOLA DE MSDOS

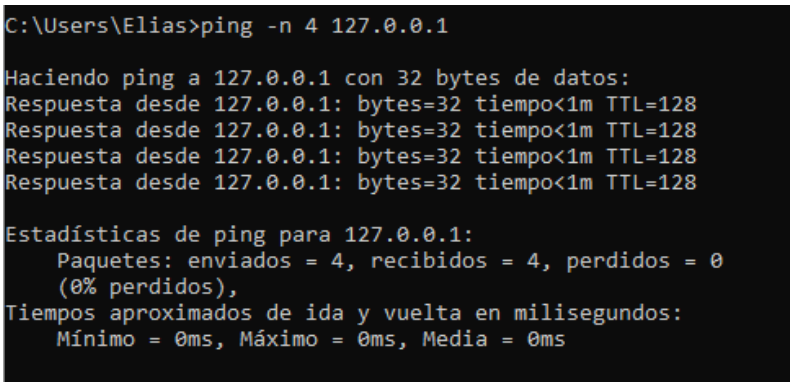
   A. OBTENER LA AYUDA DE COMANDO PING

      Comando:ping -w 1000 google.com



   B. ENVIAR UN PING A 127.0.0.1 APLICANDO CUALQUIER PARAMETRO

      Comando: ping -n 4 127.0.0.1



C. VERIFICAR LA CONECTIVIDAD DEL EQUIPO UTILIZANDO EL COMANDO PING, ANOTAR CONCLUSIONES

Comando:ping 127.0.0.1

```
C:\Users\Elias>ping 127.0.0.1

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

D. OBTENER LA AYUDA DEL COMANDO NSLOOKUP

Comando:nslookup /?

```
C:\Users\Elias>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'
```

E. RESOLVER LA DIRECCION IP DE HTTPS://UPQROO.EDU.MX/ USANDO NSLOOKUP

Comando: nslookup upqroo.edu.mx

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

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

F. HACER PING A LA IP OBTENIDA DEL PASO ANTERIOR, ANOTAR CONCLUSIONES

Comando: ping <dirección_IP_obtenida> = ping 77.68.126.20

```
C:\Users\Elias>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=164ms TTL=46
Respuesta desde 77.68.126.20: bytes=32 tiempo=164ms TTL=46
Respuesta desde 77.68.126.20: bytes=32 tiempo=164ms TTL=46
Respuesta desde 77.68.126.20: bytes=32 tiempo=164ms TTL=46

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 = 164ms, Máximo = 164ms, Media = 164ms
```

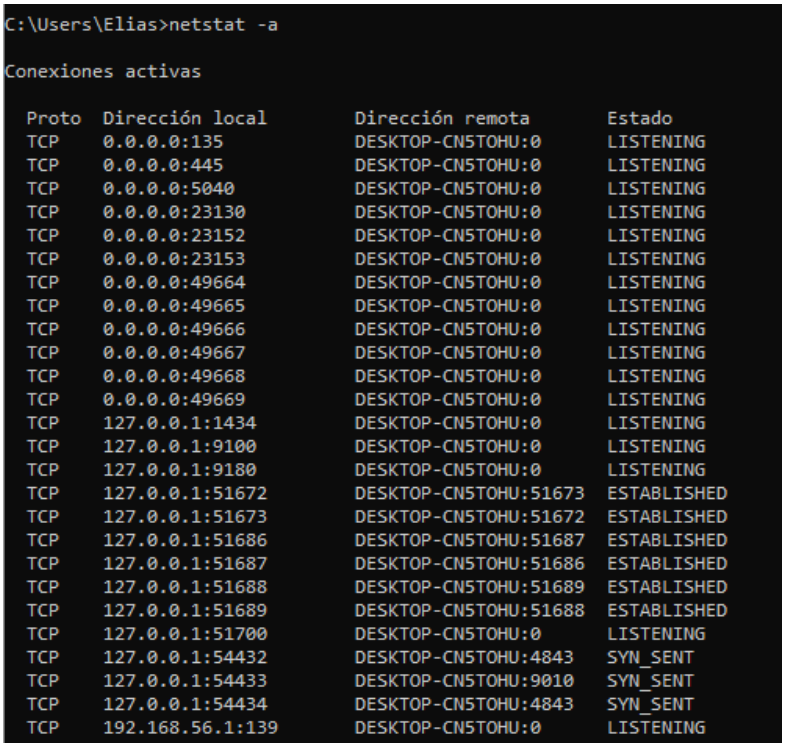
G. OBTENER LA AYUDA DEL COMANDO NETSTAT

Comando: netstat /?

```
C:\Users\Elias>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 suficien
tes
                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 segund
os
                entre cada visualización. Presiona CTRL+C para que dejen de mostrarse las
                estadísticas. Si omites esta opción, netstat imprimirá una sola vez
                la información de configuración.
```

H. MOSTRAR TODAS LAS CONEXIONES Y PUERTOS DE ESCUCHA

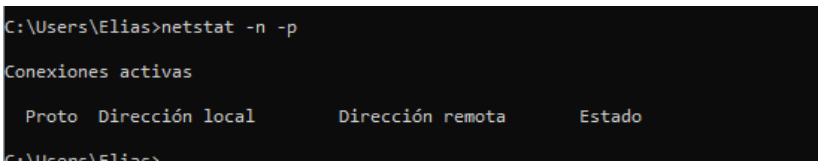
Comando: netstat -a



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

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    0.0.0.0:135            DESKTOP-CN5TOHU:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-CN5TOHU:0      LISTENING
  TCP    0.0.0.0:5040           DESKTOP-CN5TOHU:0      LISTENING
  TCP    0.0.0.0:23130          DESKTOP-CN5TOHU:0      LISTENING
  TCP    0.0.0.0:23152          DESKTOP-CN5TOHU:0      LISTENING
  TCP    0.0.0.0:23153          DESKTOP-CN5TOHU:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-CN5TOHU:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-CN5TOHU:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-CN5TOHU:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-CN5TOHU:0      LISTENING
  TCP    0.0.0.0:49668          DESKTOP-CN5TOHU:0      LISTENING
  TCP    0.0.0.0:49669          DESKTOP-CN5TOHU:0      LISTENING
  TCP    127.0.0.1:1434         DESKTOP-CN5TOHU:0      LISTENING
  TCP    127.0.0.1:9100         DESKTOP-CN5TOHU:0      LISTENING
  TCP    127.0.0.1:9180         DESKTOP-CN5TOHU:0      LISTENING
  TCP    127.0.0.1:51672        DESKTOP-CN5TOHU:51673  ESTABLISHED
  TCP    127.0.0.1:51673        DESKTOP-CN5TOHU:51672  ESTABLISHED
  TCP    127.0.0.1:51686        DESKTOP-CN5TOHU:51687  ESTABLISHED
  TCP    127.0.0.1:51687        DESKTOP-CN5TOHU:51686  ESTABLISHED
  TCP    127.0.0.1:51688        DESKTOP-CN5TOHU:51689  ESTABLISHED
  TCP    127.0.0.1:51689        DESKTOP-CN5TOHU:51688  ESTABLISHED
  TCP    127.0.0.1:51700        DESKTOP-CN5TOHU:0      LISTENING
  TCP    127.0.0.1:54432        DESKTOP-CN5TOHU:4843   SYN_SENT
  TCP    127.0.0.1:54433        DESKTOP-CN5TOHU:9010   SYN_SENT
  TCP    127.0.0.1:54434        DESKTOP-CN5TOHU:4843   SYN_SENT
  TCP    192.168.56.1:139       DESKTOP-CN5TOHU:0      LISTENING
```

I. EJECUTAR NETSTAT SIN RESOLVER NOMBRES DE DOMINIO O PUERTOS

Comando: netstat -n -p



```
C:\Users\Elias>netstat -n -p

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
```

J. MOSTRAR LAS CONEXIONES TCP

Comando: netstat -n -p tcp

```
C:\Users\Elias>netstat -n -p tcp

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    127.0.0.1:51672        127.0.0.1:51673        ESTABLISHED
  TCP    127.0.0.1:51673        127.0.0.1:51672        ESTABLISHED
  TCP    127.0.0.1:51686        127.0.0.1:51687        ESTABLISHED
  TCP    127.0.0.1:51687        127.0.0.1:51686        ESTABLISHED
  TCP    127.0.0.1:51688        127.0.0.1:51689        ESTABLISHED
  TCP    127.0.0.1:51689        127.0.0.1:51688        ESTABLISHED
  TCP    127.0.0.1:54496        127.0.0.1:4843         SYN_SENT
  TCP    127.0.0.1:54497        127.0.0.1:9010         SYN_SENT
  TCP    127.0.0.1:54498        127.0.0.1:4843         SYN_SENT
  TCP    192.168.100.23:51630   20.10.31.115:443       ESTABLISHED
  TCP    192.168.100.23:53493   34.160.122.198:443     TIME_WAIT
  TCP    192.168.100.23:53670   23.63.230.71:80        TIME_WAIT
  TCP    192.168.100.23:53863   23.63.231.174:443      CLOSE_WAIT
  TCP    192.168.100.23:53866   23.63.231.174:443      CLOSE_WAIT
  TCP    192.168.100.23:53947   35.190.80.1:443        ESTABLISHED
  TCP    192.168.100.23:54012   142.251.208.99:443     TIME_WAIT
  TCP    192.168.100.23:54077   192.178.52.138:443     TIME_WAIT
  TCP    192.168.100.23:54308   34.104.35.123:80       TIME_WAIT
  TCP    192.168.100.23:54344   52.168.117.173:443     TIME_WAIT
  TCP    192.168.100.23:54350   204.79.197.239:443     ESTABLISHED
  TCP    192.168.100.23:54359   52.168.117.173:443     TIME_WAIT
  TCP    192.168.100.23:54372   52.182.143.212:443     TIME_WAIT
  TCP    192.168.100.23:54411   34.104.35.123:80       ESTABLISHED
  TCP    192.168.100.23:54415   20.189.173.20:443      TIME_WAIT
  TCP    192.168.100.23:54422   204.79.197.239:443     ESTABLISHED
  TCP    192.168.100.23:54423   13.107.246.57:443      ESTABLISHED
  TCP    192.168.100.23:54431   20.189.173.22:443      TIME_WAIT
  TCP    192.168.100.23:54443   52.168.117.173:443     TIME_WAIT
  TCP    192.168.100.23:54474   20.42.65.92:443        TIME_WAIT
  TCP    192.168.100.23:54488   20.42.65.92:443        TIME_WAIT
```

K. MOSTRAR LAS CONEXIONES UDP

Comando: netstat -n -p udp

```
C:\Users\Elias>netstat -n -p udp

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
```

L. UTILIZAR EL COMANDO TASKLIST

Comando: tasklist

```
C:\Users\Elias>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        32 KB
Registry                      108 Services                   0    77,696 KB
smss.exe                      396 Services                   0       516 KB
csrss.exe                     616 Services                   0     3,476 KB
wininit.exe                   740 Services                   0     3,636 KB
services.exe                  812 Services                   0     9,672 KB
lsass.exe                     844 Services                   0    22,524 KB
svchost.exe                  1020 Services                   0    37,152 KB
fontdrvhost.exe               432 Services                   0       516 KB
```

M. UTILIZAR EL COMANDO TASKILL

Comando: taskkill /IM explorer.exe

```
C:\Users\Elias>taskkill /IM explorer.exe
ERROR: no se pudo terminar el proceso "explorer.exe" con PID 104836.
Motivo: Acceso denegado.
CORRECTO: señal de terminación enviada al proceso "explorer.exe" con PID 101896.
```

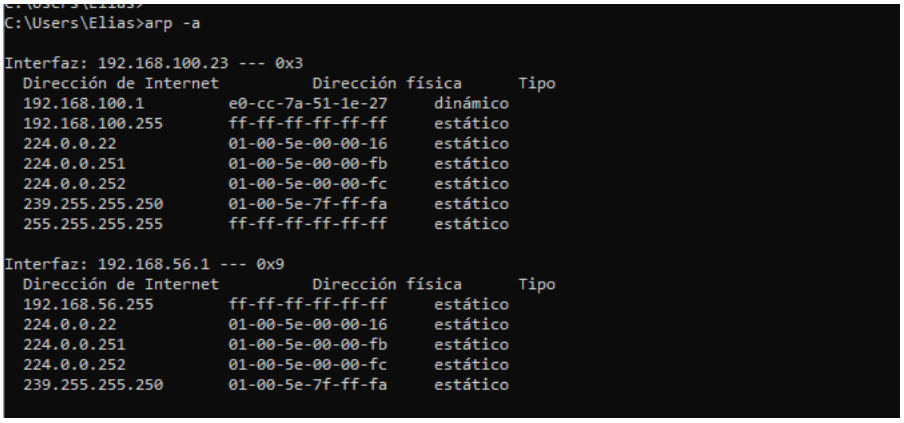
N. UTILIZAR EL COMANDO TRACERT

Comando: tracert www.google.com

```
Traza a la dirección www.google.com [192.178.56.132]
sobre un máximo de 30 saltos:

  1    <1 ms    <1 ms    <1 ms  192.168.100.1
  2     2 ms     1 ms     1 ms  172.16.84.1
  3     *        *        *     Tiempo de espera agotado para esta solicitud.
  4     2 ms     2 ms     2 ms  10.200.0.1
  5    29 ms    26 ms    25 ms  static-201-163-91-210.alestra.net.mx [201.163.91.210]
  6    23 ms    23 ms    23 ms  200-188-119-26.static.axtel.net [200.188.119.26]
  7    23 ms    23 ms    23 ms  host-148-243-141-177.alestra.net.mx [148.243.141.177]
^C
```

0. UTILIZAR EL COMANDO ARP

Comando: arp -a



2. CONTESTA CON TUS PROPIAS PALABRAS LAS SIGUIENTES PREGUNTAS

A. ¿PARA QUÉ SIRVE EL COMANDO PING?

a. El comando ping se utiliza para verificar la conectividad entre tu computadora y otra, enviando paquetes de prueba y recibiendo respuestas. Es una herramienta fundamental para diagnosticar la conectividad de red y verificar si un host remoto está accesible.

B. ¿PARA QUÉ SIRVE EL COMANDO NSLOOKUP?

a. El comando nslookup se emplea para realizar consultas de resolución de nombres de dominio (DNS). Proporciona información sobre la resolución de nombres y las direcciones IP asociadas con un nombre de dominio, lo que ayuda a diagnosticar problemas de resolución DNS.

C. ¿PARA QUÉ SIRVE EL COMANDO NETSTAT?

a. El comando netstat muestra información sobre conexiones de red, puertos de escucha y estadísticas de red. Es útil para entender qué procesos están utilizando la red, qué puertos están abiertos y qué conexiones están establecidas en un momento dado.

D. ¿PARA QUÉ SIRVE EL COMANDO TASKLIST?
    a. El comando tasklist muestra una lista de los procesos en ejecución en el sistema, proporcionando detalles como el nombre del proceso, el ID del proceso y el consumo de recursos. Es útil para obtener información sobre los procesos en ejecución en un sistema Windows.

E. ¿PARA QUÉ SIRVE EL COMANDO TASKILL?
    a. El comando taskkill se utiliza para terminar o finalizar procesos en ejecución en un sistema Windows. Puede forzar la terminación de procesos y es útil para cerrar aplicaciones que no responden.

F. ¿PARA QUÉ SIRVE EL COMANDO TRACERT?
    a. El comando tracert (traceroute) rastrea la ruta que toma un paquete desde tu computadora hasta un destino específico en la red. Muestra los nodos intermedios a lo largo del camino, proporcionando información sobre la latencia y la ruta que sigue un paquete.

G. ¿CÓMO AYUDAN LOS PRIMEROS TRES COMANDOS PARA DETECTAR PROBLEMAS EN LA RED?
    a. Ping ayuda a identificar problemas de conectividad y latencia.
    b. Nslookup ayuda a diagnosticar problemas de resolución de nombres de dominio.
    c. Netstat revela información sobre conexiones y puertos, útil para identificar actividades inusuales o problemas de red.

Nota: En combinación, estos comandos pueden ayudar a identificar y diagnosticar problemas de red, como conexiones no deseadas, fallos de DNS, o problemas de conectividad.

3. INVESTIGAR LOS SIGUIENTES COMANDOS Y ANOTAR EJEMPLOS PRACTICOS:

A. ATMADM: Este comando se utiliza para mostrar o modificar parámetros de la interfaz de manejo de modo de adaptador ATM (Asynchronous Transfer Mode).
   + Ejemplo: atmadm.exe -status

B. BITASDMIN: Este comando se utiliza para administrar el servicio de servidor de bits distribuido.
   + Ejemplo: bitasadmin /status

C. CMSTP: Este comando se utiliza para instalar o desinstalar un componente de conexión de red.
   + Ejemplo: cmstp.exe /s archivo_inf

D. FTP: El comando FTP se utiliza para transferir archivos entre computadoras a través de una red.
   + Ejemplo: ftp ejemplo.com

E. GETMAC: Este comando muestra las direcciones MAC de los adaptadores de red en un sistema.
   + Ejemplo: getmac

F. HOSTNAME: Muestra el nombre del host de la computadora.
   + Ejemplo: hostname

G. NBSTAT: Muestra estadísticas del protocolo NetBIOS sobre TCP/IP.
   + Ejemplo: nbstat -a nombre_del_equipo

H. NET: Muestra o modifica la configuración de red.
   + Ejemplo: net view

I. NET USE: Conecta o desconecta un equipo de un recurso compartido de red.
    + Ejemplo: net use Z: \\servidor\recurso

J. NETSH: Permite la configuración de diversos aspectos del sistema operativo, incluyendo la configuración de red.
    + Ejemplo: netsh interface ip show config

K. PATHPING: Combina características de tracert y ping, mostrando detalles sobre la ruta que toman los paquetes hacia un destino.
    + Ejemplo: pathping ejemplo.com

L. RCP: Este comando se utiliza para copiar archivos entre computadoras en una red.
    + Ejemplo: rcp archivo.txt usuario@host:/ruta/destino

M. REXEC Descripción: Ejecuta comandos en una computadora remota.
    + Ejemplo: rexec nombre_del_equipo comando

N. ROUTE: Muestra o modifica la tabla de enrutamiento.
    + Ejemplo: route print

O. RCPING: Realiza un ping a una máquina remota usando el protocolo RCP.
    + Ejemplo: rcping nombre_del_equipo

P. RSH: Ejecuta comandos en una computadora remota.
    + Ejemplo: rsh nombre_del_equipo comando

Q. TCMSETUP: Configura el servicio de transporte de tarjetas inteligentes.
    + Ejemplo: tcmsetup /register /reader:NombreLector

R. TELNET: Permite la comunicación con otra computadora a través del protocolo Telnet.
    + Ejemplo: telnet ejemplo.com

S. TFTP: Transfiere archivos hacia o desde una máquina remota usando el protocolo TFTP.
    + Ejemplo: tftp -i dirección_remota PUT archivo.txt