

Practica de laboratorio

Comandos en MSDOS

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

1. Obtener la ayuda del comando ping

Comando: Ping -w 1000 google.com

```
Microsoft Windows [Versión 10.0.22621.2715]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\famil>ping -w 1000 google.com

Haciendo ping a google.com [2607:f8b0:4012:82a::200e] con 32 bytes de datos:
Respuesta desde 2607:f8b0:4012:82a::200e: tiempo=78ms
Respuesta desde 2607:f8b0:4012:82a::200e: tiempo=79ms
Respuesta desde 2607:f8b0:4012:82a::200e: tiempo=78ms
Respuesta desde 2607:f8b0:4012:82a::200e: tiempo=78ms

Estadísticas de ping para 2607:f8b0:4012:82a::200e:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 78ms, Máximo = 79ms, Media = 78ms
```

2. Enviar un ping a 127.0.0.1 aplicando cualquier parámetro

Comando: ping -n 4 127.0.0.1

```
C:\Users\famil>ping -n 4 127.0.0.1

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
```

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

Comando: ping Google.com

```
C:\Users\famil>ping google.com

Haciendo ping a google.com [2607:f8b0:4012:808::200e] con 32 bytes de datos:
Respuesta desde 2607:f8b0:4012:808::200e: tiempo=77ms
Respuesta desde 2607:f8b0:4012:808::200e: tiempo=79ms
Respuesta desde 2607:f8b0:4012:808::200e: tiempo=78ms
Respuesta desde 2607:f8b0:4012:808::200e: tiempo=77ms

Estadísticas de ping para 2607:f8b0:4012:808::200e:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 77ms, Máximo = 79ms, Media = 77ms

C:\Users\famil>
```

4. Obtener la ayuda del comando nslookup

Comando: nslookup

```
C:\Users\famil>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 dirección ip de <https://upqroo.edu.mx/> usando nslookup

Comando: nslookup upqroo.edu.mx

```
C:\Users\famil>nslookup upqroo.edu.mx
Servidor:  UnKnown
Address:   2001:1278::38

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

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

Comando: ping <dirección_IP_obtenida> = ping 77.68.126.20

```
C:\Users\famil>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=45
Respuesta desde 77.68.126.20: bytes=32 tiempo=158ms TTL=45
Respuesta desde 77.68.126.20: bytes=32 tiempo=157ms TTL=45
Respuesta desde 77.68.126.20: bytes=32 tiempo=158ms TTL=45

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 = 157ms, Máximo = 164ms, Media = 159ms
```

7. Obtener la ayuda del comando netstat

Comando: netstat /?

```
C:\Users\famil>netstat /?

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

Comando: netstat -a

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

Conexiones activas

Proto	Dirección local	Dirección remota	Estado
TCP	0.0.0.0:135	HPRAFITA:0	LISTENING
TCP	0.0.0.0:445	HPRAFITA:0	LISTENING
TCP	0.0.0.0:5040	HPRAFITA:0	LISTENING
TCP	0.0.0.0:6646	HPRAFITA:0	LISTENING
TCP	0.0.0.0:7070	HPRAFITA:0	LISTENING
TCP	0.0.0.0:7680	HPRAFITA:0	LISTENING
TCP	0.0.0.0:49664	HPRAFITA:0	LISTENING
TCP	0.0.0.0:49665	HPRAFITA:0	LISTENING
TCP	0.0.0.0:49666	HPRAFITA:0	LISTENING
TCP	0.0.0.0:49667	HPRAFITA:0	LISTENING
TCP	0.0.0.0:49668	HPRAFITA:0	LISTENING
TCP	0.0.0.0:49669	HPRAFITA:0	LISTENING
TCP	127.0.0.1:1434	HPRAFITA:0	LISTENING
TCP	127.0.0.1:2015	HPRAFITA:0	LISTENING
TCP	127.0.0.1:12025	HPRAFITA:0	LISTENING
TCP	127.0.0.1:12110	HPRAFITA:0	LISTENING
TCP	127.0.0.1:12119	HPRAFITA:0	LISTENING
TCP	127.0.0.1:12143	HPRAFITA:0	LISTENING
TCP	127.0.0.1:12465	HPRAFITA:0	LISTENING
TCP	127.0.0.1:12563	HPRAFITA:0	LISTENING
TCP	127.0.0.1:12993	HPRAFITA:0	LISTENING
TCP	127.0.0.1:12995	HPRAFITA:0	LISTENING
TCP	127.0.0.1:27275	HPRAFITA:0	LISTENING
TCP	127.0.0.1:49786	HPRAFITA:49787	ESTABLISHED
TCP	127.0.0.1:49787	HPRAFITA:49786	ESTABLISHED
TCP	127.0.0.1:49818	HPRAFITA:49819	ESTABLISHED
TCP	127.0.0.1:49819	HPRAFITA:49818	ESTABLISHED
TCP	127.0.0.1:49820	HPRAFITA:49821	ESTABLISHED
TCP	127.0.0.1:49821	HPRAFITA:49820	ESTABLISHED
TCP	127.0.0.1:49832	HPRAFITA:0	LISTENING
TCP	192.168.0.235:139	HPRAFITA:0	LISTENING
TCP	192.168.0.235:49409	20.7.2.167:https	ESTABLISHED
TCP	192.168.0.235:49696	142:7500	ESTABLISHED

```

TCP [2806:250:c10:c1fd:c9a8:f525:e769:752c]:59691 [2001:1278:1::322]:domain TIME_WAIT
TCP [2806:250:c10:c1fd:c9a8:f525:e769:752c]:59692 [2001:1278:1::322]:domain TIME_WAIT
TCP [2806:250:c10:c1fd:c9a8:f525:e769:752c]:59693 [2001:1278:1::322]:domain TIME_WAIT
TCP [2806:250:c10:c1fd:c9a8:f525:e769:752c]:59694 qro04s02-in-x01:https TIME_WAIT
TCP [2806:250:c10:c1fd:c9a8:f525:e769:752c]:59695 [2001:1278:1::322]:domain TIME_WAIT
TCP [2806:250:c10:c1fd:c9a8:f525:e769:752c]:59696 [2001:1278:1::322]:domain TIME_WAIT
TCP [2806:250:c10:c1fd:c9a8:f525:e769:752c]:59697 [2001:1278:1::322]:domain TIME_WAIT
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 0.0.0.0:6646 *: *
UDP 0.0.0.0:50001 *: *
UDP 0.0.0.0:51590 *: *
UDP 0.0.0.0:55627 0.0.0.9:443
UDP 0.0.0.0:58722 0.0.32.14:443
UDP 0.0.0.0:60373 *: *
UDP 0.0.0.0:60886 *: *
UDP 0.0.0.0:62962 *: *
UDP 0.0.0.0:63746 *: *
UDP 127.0.0.1:51627 127.0.0.1:51627
UDP 192.168.0.235:137 *: *
UDP 192.168.0.235:138 *: *
UDP 192.168.56.1:137 *: *
UDP 192.168.56.1:138 *: *
UDP [::]:5353 *: *
UDP [::]:5353 *: *
UDP [::]:5353 *: *
UDP [::]:5355 *: *
UDP [::]:51590 *: *
UDP [::]:55627 [2806:250:b:6::9]:443
UDP [::]:58722 [2607:f8b0:4012:820::200e]:443
UDP [::]:60373 *: *
UDP [::]:60886 *: *
UDP [::]:62962 *: *
UDP [::]:63746 *: *

```

9. Ejecutar netstat sin resolver nombres de dominio o puertos

Comando: netstat -n -p

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

Conexiones activas

Proto	Dirección local	Dirección remota	Estado
-------	-----------------	------------------	--------

10. Mostrar las conexiones TCP

Comando: netstat -n -p tcp

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

Conexiones activas


```

Proto	Dirección local	Dirección remota	Estado
TCP	127.0.0.1:49786	127.0.0.1:49787	ESTABLISHED
TCP	127.0.0.1:49787	127.0.0.1:49786	ESTABLISHED
TCP	127.0.0.1:49818	127.0.0.1:49819	ESTABLISHED
TCP	127.0.0.1:49819	127.0.0.1:49818	ESTABLISHED
TCP	127.0.0.1:49820	127.0.0.1:49821	ESTABLISHED
TCP	127.0.0.1:49821	127.0.0.1:49820	ESTABLISHED
TCP	192.168.0.235:49409	20.7.2.167:443	ESTABLISHED
TCP	192.168.0.235:49696	34.141.79.142:7500	ESTABLISHED
TCP	192.168.0.235:52412	212.102.40.165:443	ESTABLISHED
TCP	192.168.0.235:52417	192.168.0.143:8009	ESTABLISHED
TCP	192.168.0.235:52418	192.168.0.49:8009	ESTABLISHED
TCP	192.168.0.235:59657	140.82.112.25:443	ESTABLISHED
TCP	192.168.0.235:59767	162.159.134.234:443	ESTABLISHED
TCP	192.168.0.235:61383	13.89.178.26:443	TIME_WAIT
TCP	192.168.0.235:61401	187.252.5.72:443	ESTABLISHED
TCP	192.168.0.235:61402	52.109.20.39:443	TIME_WAIT
TCP	192.168.0.235:61407	20.189.173.23:443	ESTABLISHED
TCP	192.168.0.235:61408	201.148.67.42:80	TIME_WAIT

11. Mostrar las conexiones UDP

Comando: netstat -au

```
C:\Users\famil>netstat -au

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.
```

12. Utilizar el comando tasklist

Comando: tasklist

```
C:\Users\famil>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	2,332 KB
Secure System	140	Services	0	32,072 KB
Registry	180	Services	0	27,156 KB
smss.exe	708	Services	0	1,060 KB
csrss.exe	744	Services	0	4,760 KB
wininit.exe	1156	Services	0	5,484 KB
csrss.exe	1176	Console	1	5,504 KB
services.exe	1228	Services	0	9,372 KB
LsaIso.exe	1244	Services	0	2,964 KB
lsass.exe	1272	Services	0	23,844 KB
winlogon.exe	1328	Console	1	9,012 KB
svchost.exe	1456	Services	0	31,060 KB
fontdrvhost.exe	1484	Services	0	2,428 KB
fontdrvhost.exe	1488	Console	1	6,508 KB
svchost.exe	1584	Services	0	16,164 KB
svchost.exe	1632	Services	0	7,784 KB
dwm.exe	1720	Console	1	79,376 KB
svchost.exe	1800	Services	0	4,892 KB
svchost.exe	1808	Services	0	5,796 KB
svchost.exe	1884	Services	0	4,828 KB
svchost.exe	1888	Services	0	6,744 KB
svchost.exe	1940	Services	0	5,800 KB
svchost.exe	1988	Services	0	9,744 KB

13. Utilizar el comando taskkill

Comando: taskkill /IM explorer.exe

```
C:\Users\famil>taskkill /IM explorer.exe  
CORRECTO: señal de terminación enviada al proceso "explorer.exe" con PID 10172.
```

14. Utilizar el comando tracert

Comando: tracert Google.com

```
C:\Users\famil>tracert google.com

Traza a la dirección google.com [2607:f8b0:4012:808::200e]
sobre un máximo de 30 saltos:

 1    7 ms    8 ms    8 ms  2806:250:c10:c1fd:10:18ff:feda:78e4
 2   17 ms   18 ms   22 ms  2806:250:c10:8000::1
 3   57 ms   27 ms   21 ms  2806:219:502:11::1f
 4   24 ms   23 ms   23 ms  2806:250:27::15
 5   24 ms   24 ms   24 ms  2806:250:6:3::
 6   53 ms   44 ms   44 ms  2001:4860:1:1:0:6f81::
 7   42 ms   40 ms   41 ms  2001:4860:0:1161::13
 8   42 ms   40 ms   39 ms  2001:4860::c:4000:fd87
 9    *      77 ms   76 ms  2001:4860::c:4001:e559
10   69 ms   70 ms   68 ms  2001:4860::9:4002:2b2f
11   79 ms   83 ms   79 ms  2001:4860::12:0:c557
12   77 ms   76 ms   76 ms  2001:4860:0:1::65c9
13   78 ms   77 ms   78 ms  qro01s14-in-x0e.1e100.net [2607:f8b0:4012:808::200e]

Traza completa.
```

15. Utilizar el comando ARP

Comando: arp -a

```
C:\Users\famil>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

Interfaz: 192.168.0.235 --- 0x15
  Dirección de Internet      Dirección física      Tipo
192.168.0.1                 02-10-18-da-78-e4    dinámico
192.168.0.49                9c-2f-4e-d8-56-57    dinámico
192.168.0.143               dc-df-d6-b7-06-c5    dinámico
192.168.0.255               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
239.255.102.18              01-00-5e-7f-66-12    estático
239.255.255.250             01-00-5e-7f-ff-fa    estático
255.255.255.255             ff-ff-ff-ff-ff-ff    estático
```


B) Contesta con tus propias palabras las siguientes preguntas:

1.- ¿Para que sirve el comando ping?

Pues el comando ping se utiliza para verificar la conectividad de red entre dos dispositivos. Y envía paquetes de datos a una dirección IP o un nombre de dominio y espera respuestas ya que permite comprobar si un host remoto es accesible y medir la latencia de la red.

2.- ¿Para que sirve el comando nslookup?

Bueno, el comando nslookup se amplía para realizar consultas de resolución de nombres de dominio (DNS). Y proporciona información sobre una resolución de nombres y las direcciones de IP asociadas con un nombre de dominio.

3.- ¿Para que sirve el comando netstat?

Muestra información detallada sobre las conexiones de red y las estadísticas del sistema. Esto puede mostrar puertos abiertos, conexiones activas, estadísticas de enrutamiento y mucho más.

4.- ¿Para que sirve el comando tasklist?

Muestra una lista de procesos en ejecución en el sistema, proporcionando detalles como el nombre del proceso, el ID del proceso y el consumo de recursos.

5.- ¿Para que sirve el comando taskkill?

El comando taskkill se usa para terminar o finalizar un proceso en ejecución en sistemas Windows. Esto puede especificar el proceso que deseas detener utilizando su PID o el nombre del proceso. Es útil para cerrar aplicaciones o procesos que no responden.

6.- ¿Para que sirve el comando tracert?

Pues rastrea la ruta que toma un paquete desde tu computadora hasta un destino específico en la red y muestra los nodos intermedios a lo largo del camino proporcionando información sobre la latencia y la ruta que sigue un paquete.

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

El ping verifica si los hosts remotos son accesibles y si la red está funcionando correctamente al medir la latencia y la pérdida de paquetes.

El nslookup ayuda a diagnosticar problemas de resolución de nombres al verificar si los nombres del dominio se traducen correctamente en direcciones IP.

El siguiente es el netstat permite identificar problemas relacionadas con las conexiones de la red, como en puertos ocupados o conexiones no deseados.

En si estos comandos son herramientas útiles para diagnosticar y solucionar problemas de conectividad y las configuraciones en la red.

C) Investigar los siguientes comandos y anotar ejemplos prácticos:

1. ATMADM: Este comando se utiliza para mostrar o modificar parámetros de la interfaz de manejo de modo adaptador ATM (Asynchronous Transfer Mode).

Ejemplo: `atmadm.exe -status`

2. Bitsadmin: Permite administrar trabajos de transferencia de datos en segundo plano. Se puede utilizar para usarlo o para cargar archivos en segundo plano.

Ejemplo: `bitsadmin /transfer myDownloadJob /download/priority normal`

<http://www.example.com/file.txt>C:\path\to\save\file.txt<

```
bitsadmin /addfile myDownloadJob http://downloadsrv/10mb.zip c:\10mb.zip
```

3. Cmstp: Es un comando utilizado para instalar o desinstalar extensiones de configuración de Windows. Puede usarse para ejecutar archivos de configuración INF.

Ejemplo: `cmstp` /s C:\path\to\config.inf`

```
cmstp.exe /s /au filename.inf
```

4. Getmac: Muestra las direcciones MAC de las interfaces de red en el sistema.

Ejemplo: `getmac`

```
C:\Users\famil> getmac

Dirección física      Nombre de transporte
=====
AC-50-DE-05-54-87    \Device\Tcpip_{EB8734FD-41A3-4887-BA3A-1EBFC3657638}
00-FF-FF-D5-9C-61    Medios desconectados
N/A                  Medios desconectados
AC-50-DE-05-54-88    Medios desconectados
0A-00-27-00-00-0F    \Device\Tcpip_{9E3C3F0F-5A73-47ED-87D0-3BDE19CD231E}
```

5. Hostname: Muestra el nombre del host de la computadora.

Ejemplo: `hostname`

```
C:\Users\famil> hostname  
HPRAFITA
```

6. Nbtstat: Es un comando para mostrar estadísticas de NetBIOS en una computadora.

Ejemplo: `nbtstat -a remote_computer_name`

```
C:\Users\famil> nbtstat -aHPRAFITA  
  
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.
```

7. Net: Es un comando para administrar diversos aspectos de la red, como usuarios, grupos, recursos compartidos, etc.

Ejemplo: `net user username password /add`

8. Net use: Se usa para conectar o desconectar unidades de red en un sistema Windows.

Ejemplo: `net use X: [\\server\share](#)/user:username password`

```
C:\Users\famil> net use X: \\server\share
```

9. Netsh: Es una herramienta en línea de comandos para configurar la red, incluyendo firewall, IP, Winsock, etc.

Ejemplo: netsh firewall set opmode mode-ENABLE

```
C:\Users\famil> netsh interface ipv4 show config

Configuración para la interfaz "Ethernet 2"
  DHCP habilitado:                Sí
  Métrica de interfaz:            5
  Servidores DNS configurados a través de DHCP: ninguno
  Registrar con el sufijo:        Solo el principal
  Servidores WINS configurados a través de DHCP: ninguno

Configuración para la interfaz "Conexión de área local"
  DHCP habilitado:                No
  Métrica de interfaz:            5
  Servidores DNS configurados estáticamente: ninguno
  Registrar con el sufijo:        Solo el principal
  Servidores WINS configurados estáticamente: ninguno

Configuración para la interfaz "Ethernet 3"
  DHCP habilitado:                No
  Dirección IP:                   192.168.56.1
  Prefijo de subred:              192.168.56.0/24 (máscara 255.255.255.0)
  Métrica de interfaz:            25
  Servidores DNS configurados estáticamente: ninguno
  Registrar con el sufijo:        Solo el principal
  Servidores WINS configurados estáticamente: ninguno

Configuración para la interfaz "Conexión de área local* 1"
  DHCP habilitado:                Sí
  Métrica de interfaz:            25
  Servidores DNS configurados a través de DHCP: ninguno
  Registrar con el sufijo:        Solo el principal
  Servidores WINS configurados a través de DHCP: ninguno

Configuración para la interfaz "Conexión de área local* 2"
  DHCP habilitado:                No
  Métrica de interfaz:            25
  Servidores DNS configurados estáticamente: ninguno
  Registrar con el sufijo:        Solo el principal
  Servidores WINS configurados estáticamente: ninguno
```

10. Pathping: Combina las funcionalidades de tracer y ping para proporcionar información detallada sobre la ruta y el rendimiento de la red.

Ejemplo: pathping example.com

```
C:\Users\famil> pathping google.com

Seguimiento de ruta a google.com [2607:f8b0:4012:821::200e]
sobre un máximo de 30 saltos:
 0  HPRAFITA [2806:250:c10:c1fd:c9a8:f525:e769:752c]
 1  2806:250:c10:c1fd:10:18ff:feda:78e4
 2  2806:250:c10:8000::1
 3  2806:219:502:11::1d
 4  2806:250:27::13
 5  2001:4860:1:1:0:6f81::
 6  2001:4860:0:1162::13
 7  2001:4860::c:4000:fd87
 8  *      2001:4860::c:4001:e559
 9  2001:4860::9:4002:2b2f
10  2001:4860:0:134a::1
11  2001:4860:0:1::f9b
12  tzqroa-ag-in-x0e.1e100.net [2607:f8b0:4012:821::200e]
```

11. telnet: Permite abrir una sesión de telnet a un host remoto.

Ejemplo: telnet remote_host

```
rexec hostname -l username -p password "comando" telnet example.com
tcmsetup /l` tftp -i 192.168.1.1 GET archivo.txt`
```

12. Tftp: es un protocolo de transferencia de archivos que permite la transferencia de archivos a través de la red.

Ejemplo: tftp -i 192.168.1.10 GET file.txt C:\local\path\file.txt