



Ejercicio Comandos de Red en Windows

1. PING

Descripción: El comando ping se usa para verificar la conectividad entre el equipo local y otro dispositivo en la red. Envía paquetes de prueba ICMP (Internet Control Message Protocol) y espera respuestas.

Ejemplo:

```
ping -n 4 8.8.8.8
```

Este comando envía 4 paquetes al servidor de Google DNS (8.8.8.8) y muestra el resultado.

Ejercicio: Haz ping a la dirección de tu router local (normalmente 192.168.1.1) y verifica la conectividad. Anota los tiempos de respuesta y posibles errores.

Por defecto, cada sistema operativo tiene un TimeToLive, el mecanismo que limita la vida útil de los datos en una red. Es un valor de los paquetes de red que determina durante cuánto tiempo se deben conservar los datos antes de descartarlos.

TTL ayuda a administrar los recursos de red de manera eficiente y garantiza que los datos no persistan más tiempo del necesario, pero es que además te permite identificar que equipo está enviando o recibiendo los paquetes que mandas.

Y es que el valor TTL varía según la versión del sistema operativo y del dispositivo.

Por ejemplo: un TTL

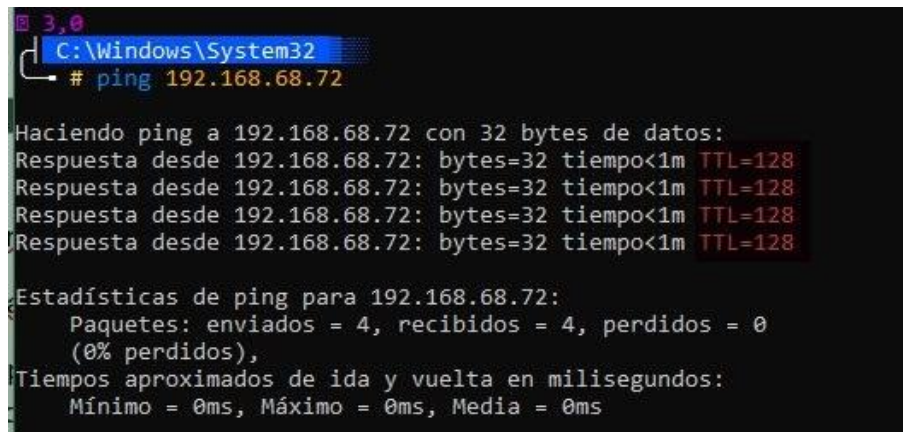
✓ 128 = WindowsXP, 7, 8, 10, 11 y servidores

✓ 32 = Windows de 32 bits (95/98/ME)

✓ MacOS=64

✓ Linux= 64Y

un simple ping nos mostrará el TTL



```
3,0
C:\Windows\System32
# ping 192.168.68.72

Haciendo ping a 192.168.68.72 con 32 bytes de datos:
Respuesta desde 192.168.68.72: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.68.72: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.68.72: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.68.72: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.68.72:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Si un ping devuelve **TTL=116**, significa que el sistema operativo original probablemente configuró un TTL de **128**, pero ha pasado por **12 saltos** ($128 - 116 = 12$).

Dado que **Windows** usa TTL=128 por defecto, es muy probable que el destino sea un sistema operativo **Windows** (Windows XP, 7, 8, 10, 11 o un servidor Windows) que ha atravesado algunos nodos en la red antes de llegar a su destino.

Si necesitas confirmarlo con más precisión, puedes analizar la ruta con el comando:

- **Windows:** tracert [IP o dominio]
- **Linux/macOS:** traceroute [IP o dominio]

Así verás cuántos saltos han afectado el TTL

2. IPCONFIG

Descripción: Muestra la configuración de la red del equipo, como direcciones IP, máscara de subred y puerta de enlace predeterminada.

Ejemplo:

ipconfig

Muestra la configuración básica de red.

Ejercicio: Ejecuta el comando ipconfig /all y anota la dirección MAC de uno de los adaptadores de red.

3. HOSTNAME

Descripción: Muestra el nombre del host del equipo.

Ejemplo:

hostname

Ejercicio: Consulta el nombre de tu equipo usando hostname y compáralo con el valor mostrado en la configuración del sistema.

4. GETMAC

Descripción: Obtiene las direcciones MAC (Media Access Control) de los adaptadores de red instalados en el equipo.

Ejemplo:

getmac

Ejercicio: Ejecuta el comando y anota la dirección MAC de tu adaptador de red principal.

5. ARP

Descripción: Muestra y modifica las tablas de conversión de direcciones IP en direcciones físicas (ARP).

Ejemplo:

arp -a

Muestra la tabla ARP para todas las interfaces.

Ejercicio: Ejecuta arp -a y observa las entradas. Identifica si alguna corresponde a la dirección de tu router.

6. NSLOOKUP

Descripción: Permite consultar información sobre el DNS (Domain Name System).

Ejemplo:

nslookup marca.com 8.8.8.8

Consulta la dirección IP de marca.com usando el servidor DNS de Google.

Ejercicio: Consulta la dirección IP de cualquier dominio de tu elección usando nslookup.

7. NBTSTAT

Descripción: Muestra las estadísticas del protocolo NetBIOS sobre TCP/IP (NetBT) y las tablas de nombres NetBIOS.

Ejemplo:

```
nbtstat -n
```

Muestra la tabla de nombres NetBIOS del equipo local.

Ejercicio: Ejecuta `nbtstat -c` y observa el contenido de la caché de nombres NetBIOS.

8. NETSTAT

Descripción: Muestra las conexiones TCP activas, puertos de escucha y estadísticas de la red.

Ejemplo:

```
netstat -a
```

Muestra todas las conexiones activas y puertos en escucha.

Ejercicio: Ejecuta `netstat -n` y observa las conexiones activas en forma numérica.

9. NET USE

Descripción: Conecta, elimina y configura conexiones a recursos compartidos en red.

Ejemplo:

```
net use * "\\servidor\recurso_compartido" /persistent:no
```

Conecta el recurso compartido `recurso_compartido` en servidor.

Ejercicio: Intenta mapear una unidad de red en tu equipo (si tienes acceso a un servidor o recurso compartido).

10. TASKKILL

Descripción: Finaliza procesos o tareas en ejecución.

Ejemplo:

```
taskkill /im notepad.exe /f
```

Finaliza el proceso de Notepad.

Ejercicio: Abre el Bloc de notas, ejecuta el comando anterior y verifica si el proceso se cierra.

11. SHUTDOWN

Descripción: Permite apagar o reiniciar computadoras locales o remotas. También puede forzar el cierre de aplicaciones.

Ejemplo:

```
shutdown /r /t 60 /c "Reconfiguración miapp.exe" /f
```

Reinicia el equipo local después de 60 segundos mostrando el comentario "Reconfiguración miapp.exe".

Ejercicio: Programa el apagado de tu equipo con un retraso de 2 minutos y un mensaje personalizado.

12. TRACERT

Descripción: Determina la ruta que toman los paquetes para llegar a un destino mediante el envío de solicitudes de eco ICMP.

Ejemplo:

```
tracert marca.com
```

Muestra los saltos que hacen los paquetes para llegar al servidor de marca.com.

Ejercicio: Haz un trazado de ruta hacia cualquier página web de tu elección y anota la cantidad de saltos.

13. PATHPING

Descripción: Combina las funciones de ping y tracert, proporcionando información sobre la latencia y la pérdida de paquetes en la ruta.

Ejemplo:

```
pathping marca.com
```

Ejercicio: Ejecuta pathping hacia una dirección pública y analiza el resultado.

14. TELNET

Descripción: Abre comunicación con un equipo remoto que ejecuta el servicio de servidor Telnet.

Ejemplo:

```
telnet telnet.microsoft.com
```

Ejercicio: Intenta conectarte a un servidor de prueba usando telnet (si está habilitado en tu sistema).

15. ROUTE

Descripción: Manipula las tablas de enrutamiento de red. Permite agregar, modificar o eliminar rutas.

Ejemplo:

route PRINT

Muestra las tablas de enrutamiento.

Ejercicio: Ejecuta route PRINT y analiza las rutas configuradas en tu equipo.

16. NETSH

Descripción: Permite mostrar o modificar la configuración de red del sistema de forma local o remota.

Ejemplo:

netsh int ip reset

Restablece la configuración de TCP/IP.

Ejercicio: Ejecuta el comando anterior y reinicia tu equipo. Observa si hay cambios en la conectividad.

17. WINRM

Descripción: Permite la administración remota de equipos mediante servicios web.

Ejemplo:

winrm get winrm/config -format:pretty

Ejercicio: Ejecuta el comando anterior y analiza la configuración mostrada.

18. WGET

Descripción: Herramienta para descargar archivos desde internet, ya sea de forma directa o recursiva.

Ejemplo:

wget http://example.com/file.iso

Ejercicio: Descarga un archivo de prueba desde cualquier servidor accesible.

19. FTP

Descripción: Permite la transferencia de archivos hacia y desde una computadora que ejecuta un servidor FTP.

Ejemplo:

ftp ftp.microsoft.com

Ejercicio: Intenta conectarte a un servidor FTP público y lista su contenido.

20. SSH

Descripción: Permite acceder de forma segura a un host remoto mediante una conexión cifrada.

Ejemplo:

ssh username@domain_or_ip_address

Ejercicio: Conéctate a un servidor remoto usando SSH (si tienes acceso) o configura un servidor local para practicar.