

## Ejercicio 1: Comando ping (Windows) / ping (Linux)

El comando ping se usa para comprobar si existe conexión entre tu equipo y un equipo destino (el cual puede ser especificado por su dirección IP o por su nombre). Este comando envía una serie de paquetes de datos al destinatario (por defecto en Windows son 4 paquetes), y cuando lleguen al receptor, este responderá con paquetes de vuelta que contienen los mismos datos, confirmando así que existe una ruta entre emisor y receptor. El hecho de que se devuelvan los mismos datos que se enviaron hace que este comando sea conocido por hacer funciones de “eco”. De hecho, a enviar un ping se le denomina también realizar un “echo request” y a la respuesta, “echo reply”.

```
Haciendo ping a 192.168.1.1 con 32 bytes de datos:  
Respuesta desde 192.168.1.1: bytes=32 tiempo=3ms TTL=64  
Respuesta desde 192.168.1.1: bytes=32 tiempo=2ms TTL=64  
Respuesta desde 192.168.1.1: bytes=32 tiempo=4ms TTL=64  
Respuesta desde 192.168.1.1: bytes=32 tiempo=3ms TTL=64  
  
Estadísticas de ping para 192.168.1.1:  
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0  
    (0% perdidos),  
  Tiempos aproximados de ida y vuelta en milisegundos:  
    Mínimo = 2ms, Máximo = 4ms, Media = 3ms
```

Si se realiza ping por nombre en lugar de por IP, primero se realizará automáticamente la consulta DNS (si fuera necesario), por lo que ping también sirve para obtener rápidamente la IP de un equipo del cual conocemos su nombre:

```
Haciendo ping a www.google.es [216.58.215.131] con 32 bytes de datos:
```

Se haya especificado el nombre o la IP del destinatario, la respuesta de ping incluye, para cada mensaje enviado:

- Los bytes de datos del paquete de vuelta
- El tiempo que ha tardado en llegar la respuesta (ida+vuelta)
- El TTL del mensaje

```
Respuesta desde 192.168.1.1: bytes=32 tiempo=3ms TTL=64  
Respuesta desde 192.168.1.1: bytes=32 tiempo=2ms TTL=64  
Respuesta desde 192.168.1.1: bytes=32 tiempo=4ms TTL=64  
Respuesta desde 192.168.1.1: bytes=32 tiempo=3ms TTL=64
```

Además, se nos indican también estadísticas generales, como cuántos paquetes se enviaron, cuántos de ellos se recibieron, cuántos se han perdido (n.º de paquetes y porcentaje), además del tiempo mínimo, máximo y medio global.

```
Estadísticas de ping para 192.168.1.1:  
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0  
    (0% perdidos),  
  Tiempos aproximados de ida y vuelta en milisegundos:  
    Mínimo = 2ms, Máximo = 4ms, Media = 3ms
```

Así pues, el comando ping no solo sirve para hacerse una idea de si existe ruta entre dos equipos en este momento, sino también cómo es de rápida y estable dicha ruta. Si una ruta contiene errores o pérdidas, probablemente haya algún tipo de incidencia en el camino intermedio.

Si hacemos ping a un equipo y no responde, puede deberse a diversas causas:

- No existe ruta entre los dos equipos en este momento (que, a su vez, puede deberse a algún fallo en el emisor, en el receptor (por ejemplo, porque está apagado), o en cualquiera de los equipos que forman la ruta entre ambos)
- Existe ruta, pero los paquetes tardan demasiado en volver (cuando se envían pings, se pone un plazo máximo de tiempo, transcurrido el cual se asume que la ruta es demasiado lenta y se da por perdido el ping)
- El destinatario está conectado y hay ruta entre ambos, pero el receptor tiene deshabilitada la opción de responder pings (es decir, sí que le llegan pero no los responde, que es común en servidores que están destinados a otras tareas y no dedican tiempo a responder pings)

Como puedes comprobar, la herramienta ping es una herramienta básica de diagnóstico en una LAN, que nos permite, a base de mandar paquetes y comprobar hasta dónde son capaces de llegar, localizar y aislar el foco de la red donde puede haber problemas.

Para probarlo, desde la consola de Windows ("cmd"), teclea `ping` sin parámetros para ver todas las opciones posibles que ofrece el comando. Indica qué comando entero (parámetros incluidos) usarías en Windows para realizar las siguientes acciones (puedes enviar pings de prueba al router o puerta de enlace de tu LAN, a otro equipo de tu misma red o a cualquier equipo externo):

- Enviar sólo 3 pings a un equipo:  
`ping -n 3 8.8.8.8`
- Enviar pings a un equipo sin parar (hasta que se pulse CTRL+C):  
`ping -t 192.168.0.16`
- Enviar mensajes de datos de 500 bytes en cada ping:  
`ping -l 500 192.168.0.16`
- Enviar 5 pings, cada uno de 1000 bytes (combina dos opciones anteriores):  
`ping -n 5 -l 1000 192.168.0.16`
- Enviar pings a un equipo del cual se sabe su IPv6:  
`ping -6 fe80::621a:76c8:ecba:49fe`
- Enviarte un ping a ti mismo usando la dirección de loopback (útil para comprobar si tu tarjeta de red funciona correctamente):  
`ping -n 1 localhost`  
También: `ping -n 1 127.0.0.1`
- Enviar pings con TTL 24:  
`ping -i 24 192.168.0.20`
- Enviar pings obligando a que no se fragmenten aunque sea necesario (flag DF=1, ver unidad 6, punto 4 para recordar el uso del flag "Don't Fragment" en la cabecera IPv4):  
`ping -f -l 1500 192.168.0.20`  
El -l 1500 lo he puesto para forzar la fragmentación.

Averigua también las siguientes opciones pero en Linux. Para leer los parámetros disponibles en Linux, teclea `man ping`:

- Enviar 5 pings a un equipo:  
**`ping -c 5 192.168.0.16`**
- Esperar 6 segundos entre cada ping enviado:  
**`ping -c 5 -i 6 192.168.0.16`**
- Enviar 6 pings de 400 bytes cada uno:  
**`ping -c 6 -s 392 192.168.0.16`**
- Enviar 3 pings y mostrar solamente las estadísticas finales:  
**`ping -c 3 -q 192.168.0.16`**

Como ves, aunque ping en Windows y Linux realizan la misma función, tienen parámetros diferentes (incluso para usar la misma opción el nombre de parámetro empleado puede ser diferente según el SO).

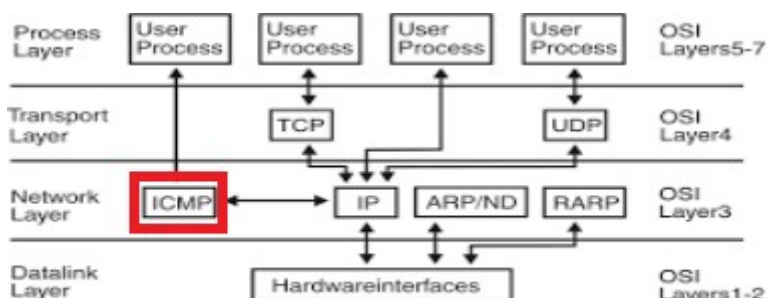
Internamente, el comando ping usa el protocolo de la capa de red ICMP (Internet Control Message Protocol). La estructura de todo paquete ICMP tiene el siguiente formato:



Para comprobarlo, empleando Wireshark realiza una captura mientras haces varios pings y contesta a las siguientes preguntas:

- ¿Qué n.º aparece en el campo “protocol” de la cabecera IP de cualquier ping?  
**ICMP**
- ¿Qué n.º aparece en el campo “type” del interior de un ping enviado?  
**8 con (echo (ping) request)**
- ¿Y en el de un ping recibido?  
**0 con (echo (ping) reply)**
- ¿Qué filtro usarías en Wireshark para que solo se te mostraran las peticiones de ping? (Puedes usar filtros como `icmp.algo==valor`)  
**`icmp.type == 8`**
- ¿Y para ver solo las respuestas?  
**`icmp.type == 0`**

Los dos valores numéricos del campo “type” obtenidos en las anteriores preguntas muestran que en realidad el protocolo ICMP se usa muchas ocasiones en la red, de las cuales enviar o responder pings son solo dos de ellas. ICMP, en general, se usa para “ayudar” al protocolo IP (que está al mismo nivel) a notificar ciertas situaciones.



En la siguiente tabla, tienes algunas de las situaciones que ICMP puede ayudar a notificar. Los campos “type” y “code” de la cabecera ICMP sirven para especificar qué situación en concreto se está dando:

ICMP Type	Code	Description
0	0	eco reply (to ping)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	7	destination host unknown
8	0	eco request
10	0	router discovery
11	0	TTL expired

Por ejemplo, estudiemos ahora el tipo ICMP 11 (“TTL expired”). En la unidad 5 se explicó que el campo TTL se decrementa en 1 a medida que el paquete de datos va atravesando routers, y que, en caso de llegar a 0, el paquete es descartado y se avisa al emisor, para que proceda a repetir el envío. La forma de avisar al emisor es precisamente enviando un paquete ICMP de tipo 11. De esta tarea “secundaria” no se encarga IP, sino ICMP. Es decir, IP se da cuenta de la situación pero es ICMP el protocolo que reacciona.

Otras situaciones que ICMP detecta (por ejemplo, el tipo 3 de la tabla anterior) es cuando no se puede alcanzar la red de la IP destinatario, o cuando sí se puede alcanzar la red pero no al host del destinatario, o cuando se alcanza la red y el host pero se está enviando paquetes a un puerto y el destinatario no tiene ningún programa escuchando peticiones en ese puerto y protocolo en concreto, etc. El campo “code” se encarga de distinguir entre situaciones diferentes que tienen el mismo “type”.

Como ves, el comando ping es solo un caso específico del protocolo ICMP. También se puede emplear ping para obtener información adicional, como por ejemplo, averiguar todas y cada una de las IP intermedias que hay entre dos equipos. Por ejemplo, teclea este comando: `ping -i 1 8.8.8.8` (en Windows) o `ping -t 1 8.8.8.8` (en Linux), que sirve para enviar pings a un equipo externo (en este caso, uno de los servidores DNS de Google), y los paquetes saldrán de nuestro equipo con TTL 1. Es decir, en cuanto lleguen al router, se decrementará el TTL del paquete a 0, se descartará el envío y se avisará al emisor, por lo que nunca llegarán al destinatario (“TTL expirado en tránsito”). Lo importante no es si llegan o no, sino que será el primer router quien nos responderá, así que sabremos su IP (en este caso, 192.168.1.1):

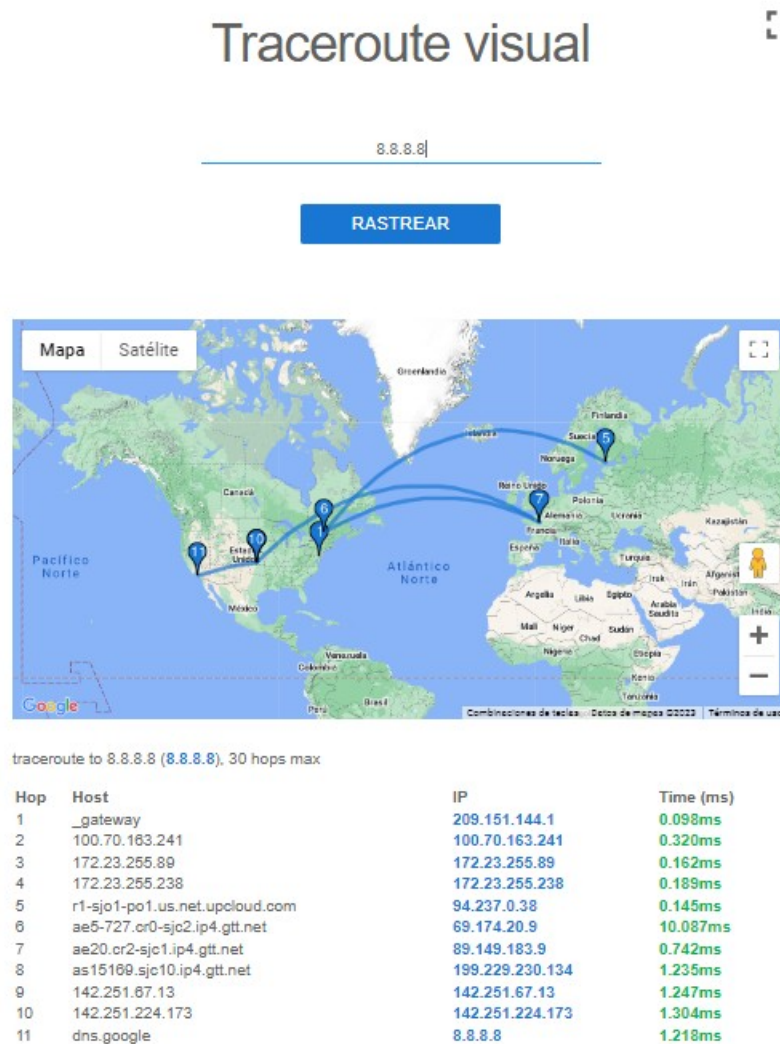
```
C:\Users>ping -i 1 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 192.168.1.1: TTL expirado en tránsito.
Respuesta desde 192.168.1.1: TTL expirado en tránsito.
Respuesta desde 192.168.1.1: TTL expirado en tránsito.
Respuesta desde 192.168.1.1: TTL expirado en tránsito.
```

Si repetimos el mismo comando pero con un TTL inicial de 2 (teclea `ping -i 2 8.8.8.8` o `ping -t 2 8.8.8.8`), el TTL de los paquetes llegará a 0 en el segundo router que hay en el camino, que será quien nos responda. Como ves, cuando el TTL es 2 probablemente ya sea una IP pública quien nos responda, es decir, los pings ya han

llegado fuera de nuestra LAN. Si repetimos el proceso con TTL 3, 4, 5, etc, podremos ir reconstruyendo todas las IP que hay entre nuestro equipo y el 8.8.8.8.

Si además, usamos webs como <https://www.geolocation.com/es> podemos ir averiguando dónde está aproximadamente localizada cada IP pública, e incluso dibujar después en un mapa la trayectoria exacta que ha seguido a nivel internacional nuestro paquete, paso a paso. En webs como <https://gsuite.tools/es/traceroute> puedes indicar una IP y mostrará cuál es el camino desde uno de **sus** servidores hasta el equipo que tú indiques.



Tanto Windows como Linux disponen de comandos (en modo texto) para obtener todas las IP intermedias entre tu equipo y otro. Prueba a teclear `tracert 8.8.8.8` en Windows o `traceroute 8.8.8.8` en Linux.

## Ejercicio 2: Comando ipconfig (Windows) / ip (Linux)

Desde Windows, teclea `ipconfig /all` y rellena la siguiente tabla con los valores de tu conexión real y una breve descripción de cada campo.

Configuración IP de Windows

Adaptador de Ethernet Ethernet:	<b>CAPTURA DESDE MI VB WINDOWS</b>
Sufijo DNS específico para la conexión. . . :	
Descripción . . . . . : Intel(R) PRO/1000 MT Desktop Adapter	
Dirección física. . . . . : 08-00-27-6E-29-8C	
DHCP habilitado . . . . . : sí	
Configuración automática habilitada . . . : sí	
Vínculo: dirección IPv6 local. . . : fe80::6e1f:aa10:51d0:9b1e%4(Preferido)	
Dirección IPv4. . . . . : 192.168.0.19(Preferido)	
Máscara de subred . . . . . : 255.255.255.0	
Concesión obtenida. . . . . : martes, 18 de abril de 2023 0:31:20	
La concesión expira . . . . . : miércoles, 19 de abril de 2023 0:31:22	
Puerta de enlace predeterminada . . . . . : 192.168.0.1	
Servidor DHCP . . . . . : 192.168.0.1	
IAID DHCPv6 . . . . . : 101187623	
DUID de cliente DHCPv6. . . . . : 00-01-00-01-2B-B3-C6-6C-08-00-27-6E-29-8C	
Servidores DNS. . . . . : 192.168.0.1	
NetBIOS sobre TCP/IP. . . . . : habilitado	

<b>Nombre</b>	<b>Valor</b>	<b>¿Para qué sirve?</b>
IPv4	192.168.0.19	Una IP sirve para diferenciar entre conexiones
Máscara	255.255.255.0	Sirve para identificar si la IP pertenece a la misma red o a distinta.
IPv6	fe80::6e1f:aa10:51d0:9b1e	Es el nuevo formato de IP. IPv4 ya estaba agotada.
MAC	08-00-27-6E-29-8C	Dirección que identifica la tarjeta de red.
Puerta de enlace	192.168.0.1	Dirección IP privada del equipo que se utilizará para mandar paquetes fuera de la LAN.
IP de los servidores DNS	192.168.0.1	Dirección IP del servidor DNS y tiene como función descifrar el número de IP a partir del nombre de una web.
¿DHCP activado? (Sí/No)	Sí	Indica si tu LAN tiene servidor DHCP o no.
IP del servidor DHCP	192.168.0.1	Encargado de repartir la configuración de manera dinámica y automática a cada cliente.
Fecha y hora de concesión	martes, 18 de abril de 2023 0:31:20	Fecha en la que el servidor te otorgó la dirección IP.
Fecha y hora de caducidad	miércoles, 19 de abril de 2023 0:31:22	Fecha en la que se te terminará la concesión de la dirección IP que se te otorgó.



En la tabla anterior, marca en amarillo los campos que son diferentes en otro equipo de tu misma LAN, y en azul los campos que son iguales en todos los equipos de tu misma LAN.

Pega aquí un pantallazo donde aparezcan los mismos datos que al ejecutar `ipconfig` pero de manera gráfica, en alguna sección de Windows, y sin ejecutar comando.

**Configuración > Red e Internet > Estado > Propiedades**



En el caso de que quisiéramos usar una IP estática, ¿cómo lo haríamos? Captura la pantalla que usarías en tu Windows.

**Configuración> Red e Internet> Estado> Propiedades> Configuración de IP> Editar**

### Configuración de IP

Asignación de IP: Automático (DHCP)

Editar

### Propiedades

Velocidad de vínculo (recepción/transmisión): 1000/1000 (Mbps)

Dirección IPv6 local de vínculo: fe80::6e1f:aa10:51d0:9b1e%4

Explica para qué sirven los siguientes parámetros de `ipconfig`:

- `ipconfig /release`  
Liberar la concesión de la IP asignada por el servidor DHCP.
- `ipconfig /renew`  
Renegocia el arrendamiento de una dirección IP con el servidor DHCP en su enrutador.
- `ipconfig /displaydns`  
Muestra el contenido de la memoria caché de la resolución del cliente DNS
- `ipconfig /flushdns`  
Limpiar la caché DNS.

Usando el comando `ip` (que poco a poco va sustituyendo al antiguo `ifconfig`) desde el terminal de Linux, asocia cada uno de los siguientes comandos con su definición del listado inferior. Recuerda que puedes usar `man ip` para obtener información sobre todos los parámetros posibles, o mejor aún, probar directamente cada comando en tu equipo y ver los resultados.

Comando	Definición
<code>ip link</code>	A
<code>ip address</code>	I
<code>ip address show enp0s3</code> (siendo <code>enp0s3</code> el nombre de una conexión, también puede ser <code>eth0</code> , etc)	B
<code>ip -s address</code>	L
<code>ip route</code>	G
<code>ip -br link</code> o también <code>ip -br address</code>	E
<code>ip -c link</code>	H
<code>ip -h -s address</code>	J
<code>sudo ip link set enp0s3 down</code> (siendo <code>enp0s3</code> el nombre de una conexión, también puede ser <code>eth0</code> , etc)	K
<code>sudo ip link set enp0s3 up</code> (siendo <code>enp0s3</code> el nombre de una conexión, también puede ser <code>eth0</code> , etc)	C
<code>ip neigh show</code>	M
<code>sudo ip neigh add 192.168.1.17 lladdr 11:22:33:aa:bb:cc dev enp0s3</code>	F
<code>sudo ip neigh del 192.168.1.17 lladdr 11:22:33:aa:bb:cc dev enp0s3</code>	D

#### Definiciones:

~~A) Mostrar el listado con todas las tarjetas de red (reales o virtuales) disponibles en el equipo, y sus MAC~~

~~B) Mostrar la IPv4, máscara y la IPv6 de una conexión concreta~~

~~C) Activar una conexión~~

~~D) Borrar una fila de la tabla ARP~~

~~E) Mostrar información sobre las tarjetas de red o las conexiones IP (mostradas como tabla con columnas)~~

~~F) Añadir una fila a la tabla ARP~~

~~G) Mostrar información sobre el enrutamiento (incluyendo la IP de la puerta de enlace)~~

~~H) Mostrar el listado de las tarjetas de red, usando colores~~

~~I) Mostrar la IPv4, máscara y la IPv6 de todas las tarjetas de red (reales o virtuales) disponibles en el equipo~~

~~J) Mostrar los paquetes recibidos (RX) y transmitidos (TX) usando expresiones con K, M, G, etc~~

~~K) Desactivar una conexión~~

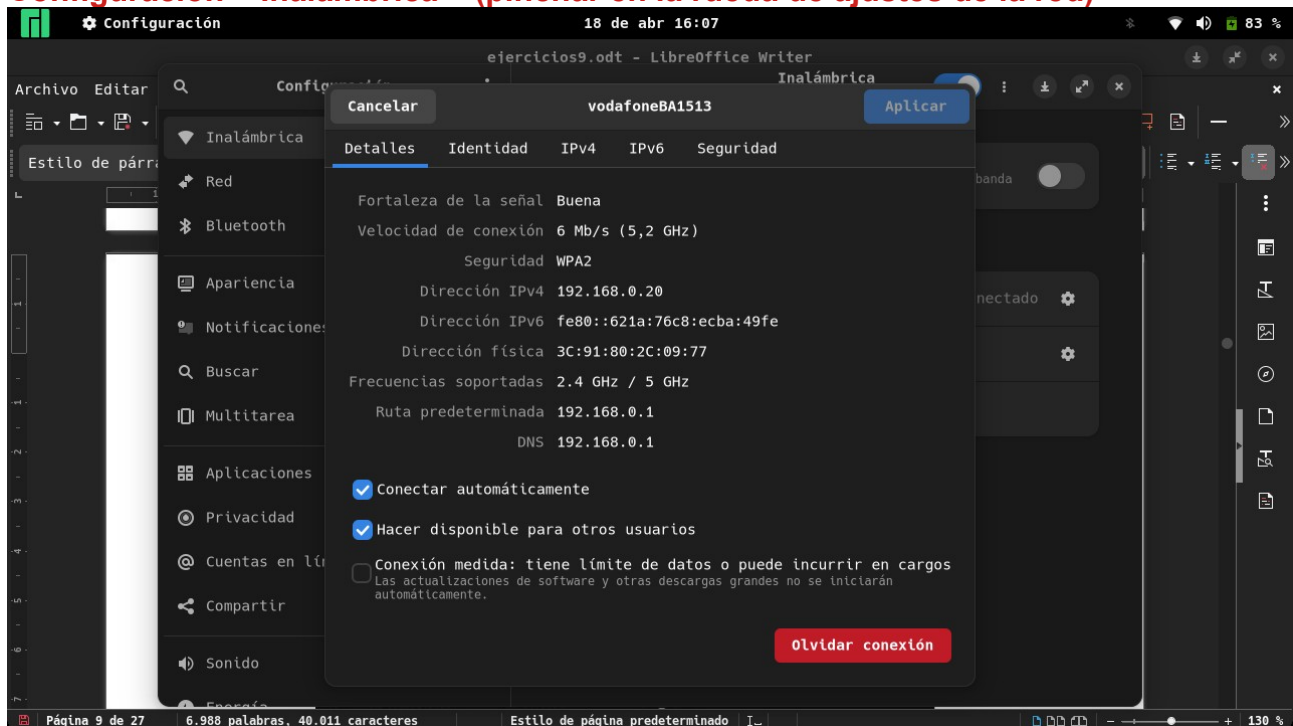
~~L) Mostrar la MTU y los paquetes recibidos (RX) y transmitidos (TX)~~

~~M) Mostrar el contenido de la tabla ARP (similar a `arp` a en Windows)~~



Finalmente, pega aquí un pantallazo de Linux donde aparezca la información de tu conexión (IP, MAC, máscara, DNS, gateway, etc) de manera gráfica, sin ejecutar comando.

**Configuración > Inalámbrica > (pinchar en la rueda de ajustes de la red)**



### Ejercicio 3: Comando netstat (Windows) / ss (Linux)

El comando `netstat` (de “network statistics”) de Windows permite ver, entre otras cosas, las conexiones actuales de un equipo. Si lo ejecutamos sin parámetros veremos algo parecido a esto:

```
Administrator: Command Prompt - netstat
Active Connections

Proto Local Address           Foreign Address         State
TCP    127.0.0.1:56304          hircv:9001             SYN_SENT
TCP    192.168.10.100:50310    104.20.27.217:https     ESTABLISHED
TCP    192.168.10.100:50312    104.20.27.217:https     ESTABLISHED
TCP    192.168.10.100:52943    40.67.251.132:https     ESTABLISHED
TCP    192.168.10.100:53069    wq-in-f188:5228        ESTABLISHED
TCP    192.168.10.100:55470    relay-033a5347:6568     ESTABLISHED
TCP    192.168.10.100:55839    server-99-86-116-19:https ESTABLISHED
TCP    192.168.10.100:55883    192.0.73.2:https       ESTABLISHED
TCP    192.168.10.100:55961    los02s04-in-f14:https  ESTABLISHED
TCP    192.168.10.100:55962    los02s04-in-f14:https  ESTABLISHED
TCP    192.168.10.100:55978    los02s03-in-f14:https  TIME_WAIT
TCP    192.168.10.100:55980    los02s03-in-f8:https   ESTABLISHED
TCP    192.168.10.100:55989    los02s04-in-f2:https   TIME_WAIT
TCP    192.168.10.100:55990    los02s03-in-f2:https   ESTABLISHED
TCP    192.168.10.100:55991    los02s04-in-f2:https   TIME_WAIT
TCP    192.168.10.100:55992    los02s03-in-f2:https   TIME_WAIT
TCP    192.168.10.100:55995    los02s04-in-f10:https  TIME_WAIT
TCP    192.168.10.100:55996    los02s04-in-f10:https  TIME_WAIT
TCP    192.168.10.100:55999    los02s04-in-f14:https  TIME_WAIT
TCP    192.168.10.100:56000    los02s04-in-f14:https  TIME_WAIT
TCP    192.168.10.100:56001    los02s04-in-f1:https   ESTABLISHED
TCP    192.168.10.100:56013    ec2-52-72-80-38:https  ESTABLISHED
TCP    192.168.10.100:56030    ec2-34-204-157-1:https ESTABLISHED
TCP    192.168.10.100:56032    ec2-34-204-157-1:https TIME_WAIT
TCP    192.168.10.100:56037    los02s03-in-f6:https   TIME_WAIT
TCP    192.168.10.100:56038    los02s03-in-f6:https   TIME_WAIT
TCP    192.168.10.100:56054    los02s03-in-f10:https  TIME_WAIT
TCP    192.168.10.100:56055    los02s03-in-f10:https  TIME_WAIT
TCP    192.168.10.100:56056    los02s04-in-f6:https   TIME_WAIT
TCP    192.168.10.100:56057    los02s04-in-f6:https   TIME_WAIT
TCP    192.168.10.100:56060    los02s04-in-f6:https   TIME_WAIT
TCP    192.168.10.100:56068    ec2-52-3-46-228:https  ESTABLISHED
TCP    192.168.10.100:56069    ec2-52-3-46-228:https  TIME_WAIT
```

Cada línea representa una conexión y está formada por cinco datos: IP origen, puerto origen, IP destino, puerto destino y estado de la conexión. Se denomina **socket** al conjunto de IP origen, puerto origen, IP destino y puerto destino. Por ejemplo, el socket formado por 192.168.1.5:23423 y 45.21.231.29:443 representa una conexión desde el puerto 23423 del equipo con dirección IP 192.168.1.5 hasta el puerto 443 (HTTPS) del equipo con dirección IP 45.21.231.29. Esa conexión probablemente representa que desde nuestro equipo (IP privada) se ha contactado con el servidor web del otro equipo, es decir, simplemente representa que desde el equipo se está viendo una página web.

En la salida de `netstat`, las direcciones IP pueden aparecer tanto en formato numérico como en nombre. Del mismo modo, los puertos pueden aparecer como número o como texto (“https” para el puerto 443, etc).

Cada conexión está en un estado concreto, que aparecen en la columna de la derecha (ESTABLISHED, SYN\_SENT, TIME\_WAIT, etc), que será explicado después.

Haz la prueba abriendo varias páginas web y ejecutando a continuación `netstat`. Verás que tu equipo aparece conectado a varias IP con el puerto 443. Conforme pase el tiempo, las conexiones se irán eliminando de la lista en sucesivas ejecuciones del comando `netstat`, para indicar que esas conexiones se han ido cerrando. Ten en cuenta que `netstat` no solo muestra tus conexiones salientes (aquellas que salen de tu equipo, es decir, aquellas cuya IP origen es la de tu equipo), sino también las entrantes (aquellas que llegan a tu equipo, es decir, aquellas cuya IP destino es la de tu equipo).

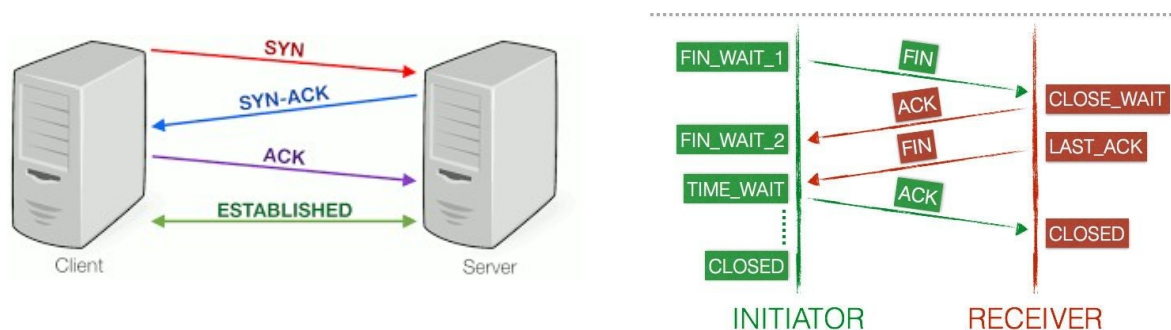
Para entender el uso de los parámetros de `netstat`, ejecuta cada uno de los siguientes comandos e indica cuál es la definición más adecuada. Para obtener ayuda con los parámetros puedes ejecutar primero `netstat -?`. Si alguno de los comandos tarda demasiado en obtener los resultados, puedes interrumpirlo con CTRL+C. Ten en cuenta que para algunos parámetros de `netstat` es necesario tener privilegios elevados, es decir, ser administrador. En ese caso, antes de ejecutar “cmd” para abrir la consola (o Símbolo del sistema) de Windows, haz clic derecho sobre el programa y selecciona “Ejecutar como administrador”.

Comando	Definición
<code>netstat</code>	A
<code>netstat -s</code>	G
<code>netstat -b</code>	D
<code>netstat -e</code>	F
<code>netstat -a</code>	B
<code>netstat -r</code>	I
<code>netstat -p tcp</code>	H
<code>netstat 3</code>	J
<code>netstat -n</code>	C
<code>netstat -n -b -a</code> o también <code>netstat -nba</code>	E

Definiciones:

- A: ~~Muestra las conexiones activas del equipo~~
- B: ~~Muestra todas las conexiones del equipo, estén activas o no~~
- C: ~~Muestra las IP y los puertos siempre con números, sin nombres de equipo ni de servicios~~
- D: ~~Muestra, además de las conexiones, el ejecutable asociado a dicha conexión~~
- E: ~~Muestra **todas** las conexiones con **números** y también el **ejecutable**~~
- F: ~~Muestra estadísticas de envío y recepción, como el n.º de bytes, paquetes, difusiones o errores~~
- G: ~~Muestra estadísticas de todos los protocolos (IPv4, IPv6, ICMP, TCP, UDP)~~
- H: ~~Muestra estadísticas según el protocolo de transporte (por ejemplo: TCP)~~
- I: ~~Muestra la tabla de enrutamiento del equipo~~
- J: ~~Muestra las conexiones, y los datos van actualizándose cada 3 segundos~~

Respecto al estado de una conexión (la columna de la derecha, con valores como ESTABLISHED, etc), es importante que recuerdes primero el proceso de conexión TCP (unidad 6, punto 7). En dicho apartado se explicaban los procesos de establecimiento y finalización de conexión de TCP (fases 1 y 3 del “handshaking”, representadas en las siguientes imágenes):



Como ves, los pasos a seguir son:

Fase -1) Conexión cerrada por ambas partes

Fase 0) El servidor está escuchando, a la espera de recibir alguna conexión

Fase 1a) El cliente envía el SYN y está a la espera de recibir el SYN+ACK

Fase 1b) El servidor envía el SYN+ACK y está a la espera de recibir el ACK

Fase 1c) El cliente envía el ACK

Fase 2) Transferencia de datos (conexión establecida)

Fase 3a) El cliente envía el FIN y está a la espera de recibir el FIN+ACK

Fase 3b1) El servidor envía el ACK

Fase 3b2) El servidor envía el FIN y está a la espera de recibir el ACK

Fase 3c) El cliente envía el ACK dando paso a la finalización de la conexión

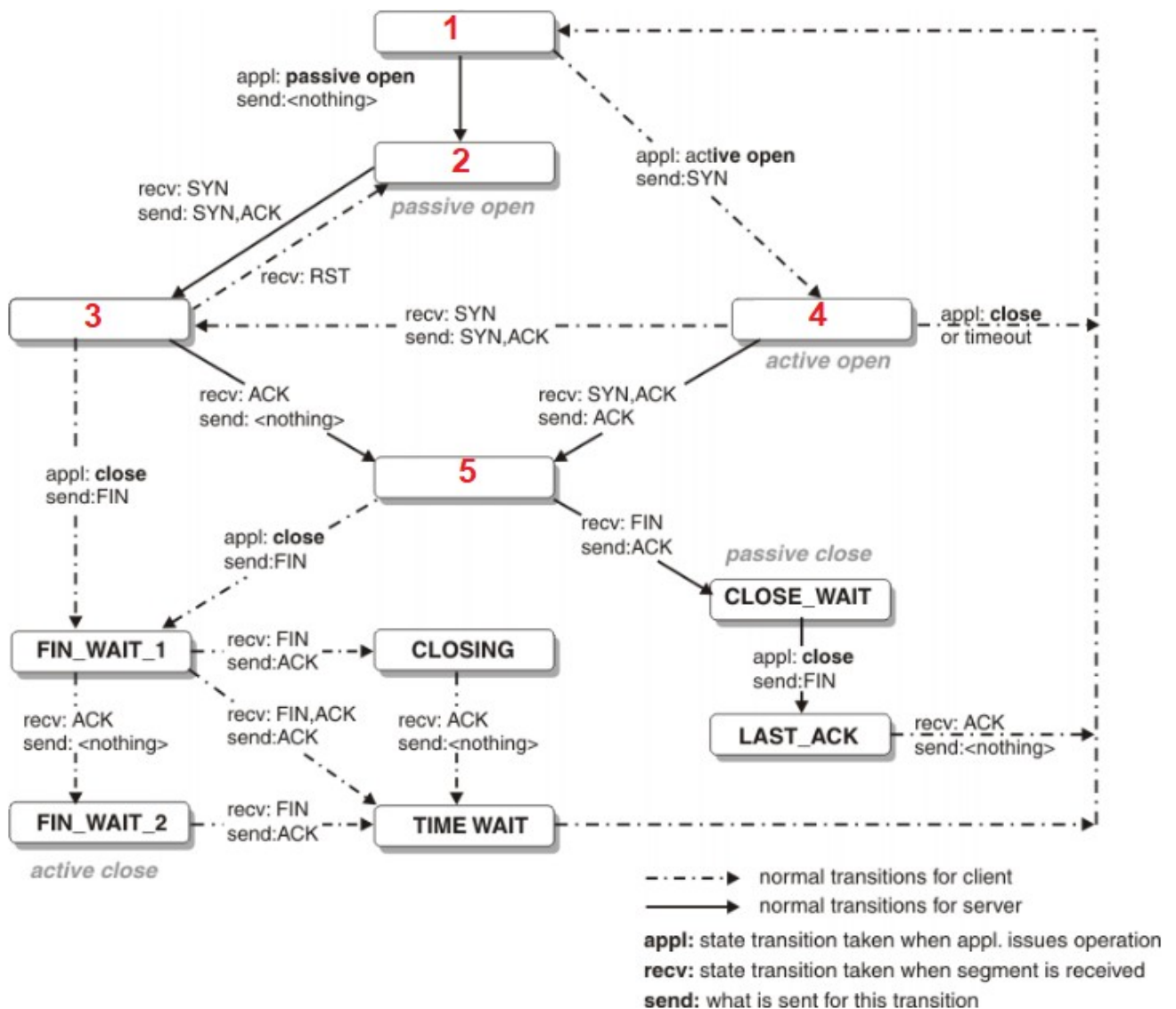
Fase 4) Conexión finalizada (se vuelve a la fase -1)

Se han marcado en **azul** los pasos que representan un envío por parte del cliente y en **naranja** los pasos asociados al servidor. Como ves, todas estas etapas son necesarias cuando se usa TCP en transporte, ya que para garantizar seguridad, ha de prepararse adecuadamente la conexión.

Cada una de las subetapas es un estado posible en `netstat` (ESTABLISHED, etc), según la fase (1, 3, etc) en la que estemos y según el rol (cliente o servidor).

En la siguiente imagen tienes representados todos los estados posibles (en forma de rectángulo), y cómo cambiar de uno a otro (en forma de flecha, siendo continua para los

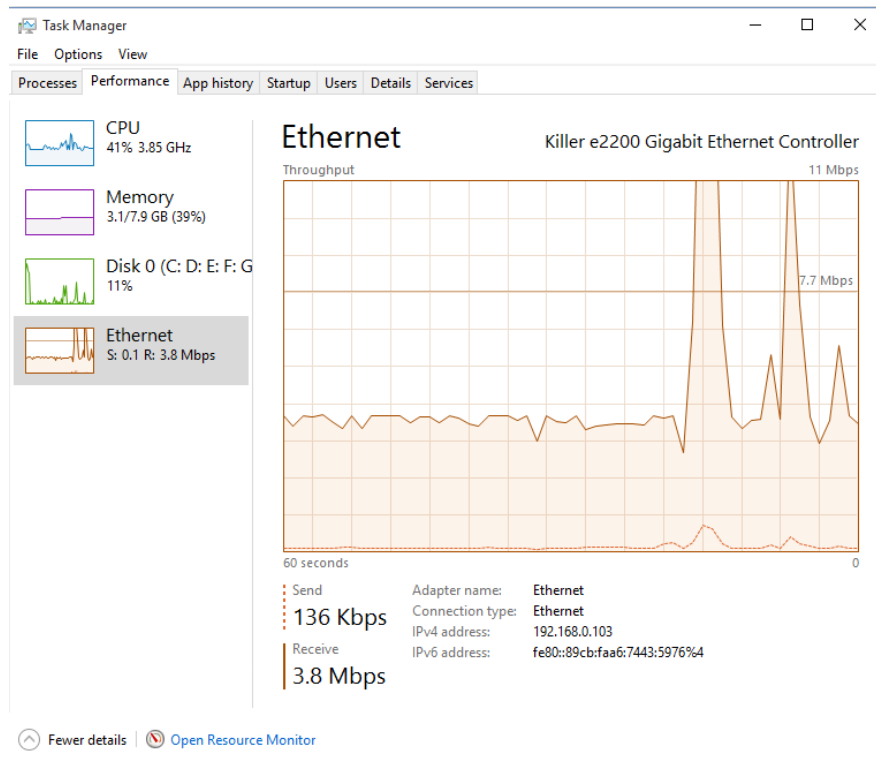
servidores y discontinua si se trata de clientes). El texto encima de cada flecha indica cómo pasar de un estado a otro. Aparecen casi todos los estados, excepto 5.



Completa el diagrama asociando los 5 estados que quedan (LISTEN, ESTABLISHED, CLOSED, SYN\_RCVD, SYN\_SENT ) con su correspondiente número:

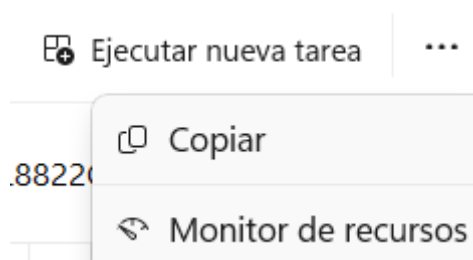
- 1: CLOSED
- 2: LISTEN
- 3: SYN\_RCVD
- 4: SYN\_SENT
- 5: ESTABLISHED

Windows también permite ver el estado de las conexiones de manera gráfica, sin usar el comando `netstat`. Para ello, pulsa CTRL+ALT+SUPR, Administrador de tareas, Rendimiento y selecciona tu conexión (Ethernet o WiFi) real. Verás **en tiempo real** la actividad de la conexión en forma de gráfica, con una línea continua para la recepción de datos y una discontinua para el envío de datos. Si abres varias webs y rápidamente vuelves a la gráfica, verás que la actividad ha aumentado. Esta herramienta sirve para monitorizar la actividad de la conexión.

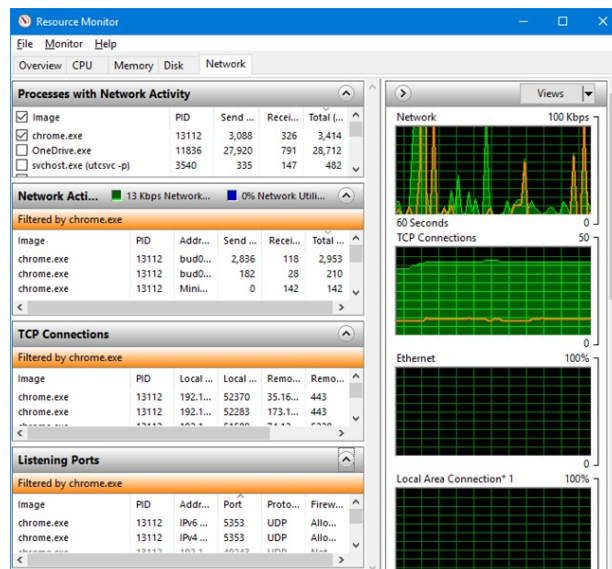


Desde esa pantalla, ahora haz clic en el monitor de recursos:

- En Windows 10, está en la parte inferior (“Open Resource Monitor”).
- En Windows 11, tienes que ir a los tres puntos de la parte superior.



Ya en el monitor de recursos, haz clic en Network o Red y aparecerá una ventana como esta:

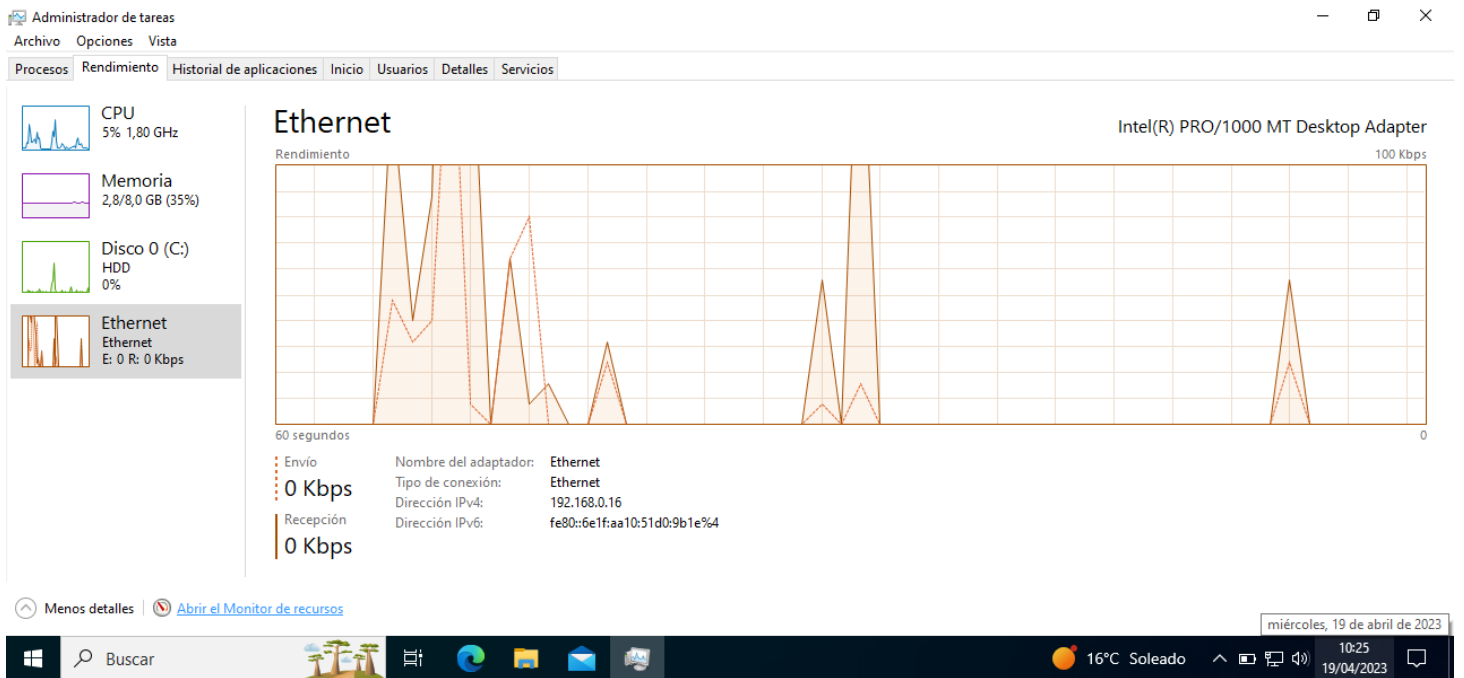


Ahí encontrarás cuatro secciones:

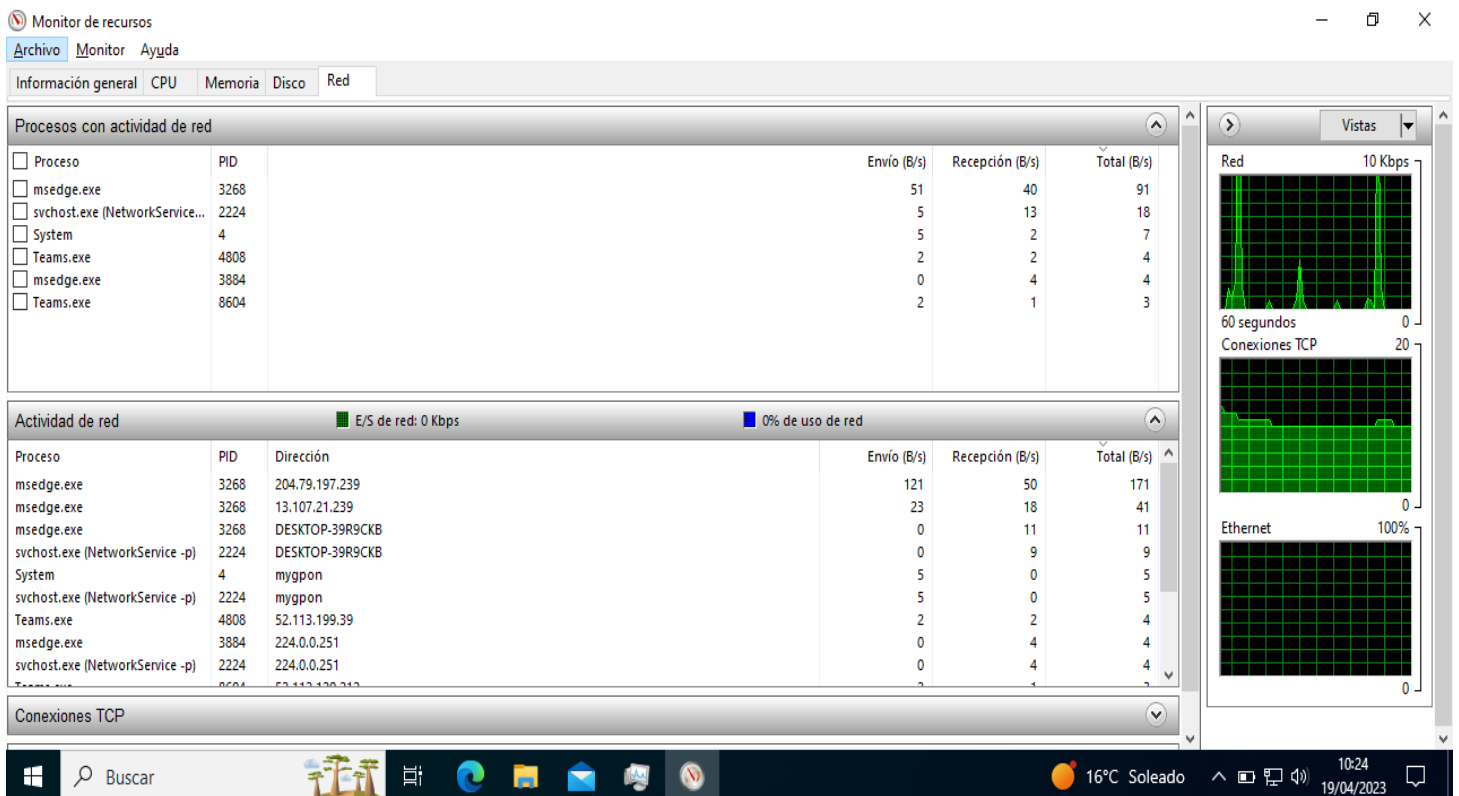
- **Procesos con actividad de red:** Es la lista de todos los programas ejecutables que están actualmente cargados en la RAM del equipo y que están usando, al menos, una conexión a la red. Para cada uno aparece: su PID (Process Identifier o Identificador de Proceso, un n.º usado por el SO para distinguir entre procesos), la cantidad de bytes por segundo enviados por tu equipo, idem para los bytes recibidos, y el total (enviados+recibidos). Este listado es útil, por ejemplo, para detectar qué procesos están usando demasiado la red. Si haces “check” en uno o varios de los procesos, las tres secciones inferiores cambiarán para mostrarte información relacionada con ese proceso. Si no haces clic en ninguno, se mostrará la información de todos los procesos. Selecciona, por ejemplo, varios procesos del navegador que tengas abierto en este momento.
- **Actividad de red:** Se muestra la misma información que en la parte superior, pero también aparece el nombre del equipo al que está conectado. Si un proceso consta de varios subprocesos, verás todos los procesos “hijo”.
- **Conexiones TCP:** Aquí se ven los sockets de cada conexión. Como ves, es similar a la salida del comando `netstat`.
- **Puertos de escucha:** Aparecen tus puertos locales que están siendo usados, el protocolo de transporte (TCP o UDP) y cómo reacciona el firewall (permitiendo o bloqueando la conexión).

Pega aquí dos pantallazos de tu Windows: el de Rendimiento de tu tarjeta de red y el de Monitor de Recursos de la sección Red.





En este caso mi servidor DHCP me repartió la IP 192.168.0.16, y con el ejercicio 2 me repartió la 192.168.0.19. Pero sigue siendo la misma maquina virtual windows de todo el ejercicio.



(Se comprobará que tus imágenes son reales comparándolas con tu IP obtenida en el ejercicio 2 mediante ipconfig).

Respecto a Linux, el equivalente a `netstat` es el comando `ss` (socket statistics). Ejecuta `ss` en un terminal. Por defecto, se muestran solo los sockets abiertos (o conexiones ya



establecidas). Las columnas más importantes son la segunda (“state”), la quinta (“local address:port”) y la sexta (peer address:port), que corresponden al estado, conexión local y conexión remota. Si salen demasiadas líneas de golpe, puedes paginarlas tecleando `ss | more` e ir pulsando la barra espaciadora para pasar de página (esto es aplicable a cualquier comando Linux).

```
bitnami@debian:~$ ss
Netid State Recv-Q Send-Q           Local Address:Port           Peer Address:Port    Process
u_str  ESTAB  0      0               * 10749                       * 10750
u_str  ESTAB  0      0  /run/systemd/journal/stdout 10750                    * 10749
u_str  ESTAB  0      0  /run/systemd/journal/stdout 10644                    * 10643
u_str  ESTAB  0      0  /run/systemd/journal/stdout 11046                    * 11045
u_str  ESTAB  0      0               * 10643                       * 10644
u_str  ESTAB  0      0               * 10923                       * 10924
u_str  ESTAB  0      0  /run/systemd/journal/stdout 11067                    * 11066
u_str  ESTAB  0      0               * 11066                       * 11067
u_str  ESTAB  0      0  /run/systemd/journal/stdout 11209                    * 11208
u_str  ESTAB  0      0               * 11208                       * 11209
u_str  ESTAB  0      0  /run/systemd/journal/stdout 10924                    * 10923
u_str  ESTAB  0      0               * 11045                       * 11046
icmp6  UNCONN 0      0                *%enp0s3:ipv6-icmp        *:*
tcp    ESTAB  0      0  [::ffff:10.0.2.15]:mysql    [::ffff:10.0.2.21]:64704
tcp    ESTAB  0      0  [::ffff:10.0.2.15]:mysql    [::ffff:10.0.2.21]:62253
tcp    ESTAB  0      0  [::ffff:10.0.2.15]:mysql    [::ffff:10.0.2.21]:64703
tcp    ESTAB  0      0  [::ffff:10.0.2.15]:mysql    [::ffff:10.0.2.21]:62252
bitnami@debian:~$ _
```

Teclea cada uno de estos comandos y asocialos con su correspondiente definición. Puedes ayudarte con `man ss` o `ss -?`

Comando	Definición
<code>ss</code>	A
<code>ss -t</code>	C
<code>ss -u</code>	L
<code>ss -ua</code>	H
<code>ss -nt</code>	F
<code>ss -ltn</code>	G
<code>ss -lun</code>	B
<code>ss -o state established</code>	J
<code>ss -t4</code>	K
<code>ss -nt dst :443 or dst :80</code>	E
<code>ss -nt dst 20.45.32.21</code>	M
<code>ss -nt dst 20.45.32.21/16</code>	D
<code>ss -nt src 127.0.0.1 sport gt :5000</code>	I

Definiciones:

- ~~A) Muestra las conexiones~~
- ~~B) Muestra las conexiones UDP que estén a la escucha, usando n.º~~
- ~~C) Muestra las conexiones TCP~~
- ~~D) Muestra, usando n.º, las conexiones TCP destinadas a un rango concreto de IP~~
- ~~E) Muestra, usando n.º, las conexiones TCP destinadas a puertos HTTP o HTTPS~~
- ~~F) Muestra, usando n.º, las conexiones TCP~~
- ~~G) Muestra las conexiones TCP que estén a la escucha, usando n.º~~
- ~~H) Muestra todas las conexiones UDP, en cualquier estado~~

- I) ~~Muestra, usando n.º, las conexiones TCP que salgan de tu equipo, de un puerto > 5000~~  
 J) ~~Muestra las conexiones que estén establecidas~~  
 K) ~~Muestra las conexiones TCP e IPv4~~  
 L) ~~Muestra las conexiones UDP~~  
 M) ~~Muestra, usando n.º, las conexiones TCP destinadas a una IP concreta~~

#### Ejercicio 4: Comando route (Windows) / ip (Linux)

Como acabas de ver en el ejercicio anterior, en Windows podemos ver la tabla de encaminamiento de nuestro equipo tecleando `netstat -r`. Sin embargo, existe otro comando para trabajar más a fondo con la tabla de encaminamiento, y es el comando `route`. Para ver la tabla de encaminamiento con el comando, teclea `route print`. Se mostrará, en primer lugar, el listado de conexiones (reales o virtuales) y sus MAC. Luego aparece la tabla de encaminamiento de IPv4 (nos centraremos en el resto de esta sección en esta tabla) y después la de IPv6.

Aquí tienes la tabla de un equipo con IP 192.168.0.12, máscara 255.255.255.0 y puerta de enlace 192.168.0.1. En este equipo también hay una MV con IP 192.168.56.1. En esta sección no se tendrán en cuenta las filas de la tabla relacionadas con MV.

```
IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de enlace      Interfaz      Métrica
0.0.0.0             0.0.0.0             192.168.0.1           192.168.0.12  50
127.0.0.0           255.0.0.0           En vínculo            127.0.0.1     331
127.0.0.1           255.255.255.255     En vínculo            127.0.0.1     331
127.255.255.255     255.255.255.255     En vínculo            127.0.0.1     331
192.168.0.0         255.255.255.0       En vínculo            192.168.0.12  306
192.168.0.12        255.255.255.255     En vínculo            192.168.0.12  306
192.168.0.255       255.255.255.255     En vínculo            192.168.0.12  306
192.168.56.0        255.255.255.0       En vínculo            192.168.56.1   281
192.168.56.1        255.255.255.255     En vínculo            192.168.56.1   281
192.168.56.255      255.255.255.255     En vínculo            192.168.56.1   281
224.0.0.0           240.0.0.0           En vínculo            127.0.0.1     331
224.0.0.0           240.0.0.0           En vínculo            192.168.56.1   281
224.0.0.0           240.0.0.0           En vínculo            192.168.0.12  306
255.255.255.255     255.255.255.255     En vínculo            127.0.0.1     331
255.255.255.255     255.255.255.255     En vínculo            192.168.56.1   281
255.255.255.255     255.255.255.255     En vínculo            192.168.0.12  306
=====
```

La tabla de encaminamiento consta de 5 columnas:

- **Destino de red:** Cuando el equipo envía un paquete, comprueba la IP destino en la cabecera IP del paquete y la compara con los valores de la primera columna empezando por la última, desde abajo hacia arriba. El primer valor que coincida nos indicará qué fila de entre todas las que tiene la tabla será la que se use para enrutar. Las otras filas serán descartadas.
- La segunda columna (**máscara de red**) especifica qué sección de la primera columna usaremos. Por ejemplo, las filas con 255.255.255.255 en la segunda columna indican que la IP entera de la primera columna será la que comparemos con la del paquete. Las filas con el valor 255.255.255.0 en la segunda columna indican que sólo los tres primeros bytes de la primera columna serán los que se comparen con la IP del paquete, etc.

- La tercera columna (**puerta de enlace**) indica a dónde se envían los paquetes. Como puedes ver en la tabla de la imagen anterior, únicamente la primera fila tiene un valor (el resto pone “En vínculo”). Esto es así porque, en un equipo, las filas sirven para la tarjeta de red local (que normalmente solo se tiene una), y solo se usa la primera fila cuando se desea salir al exterior del equipo. Recuerda que la primera fila es la última que se tendrá en cuenta (las filas se examinan de abajo a arriba), por lo que solo se aplicará cuando el paquete tenga que ser enviado al exterior. Es decir, esta primera fila es similar a las filas “default” de las tablas que hiciste en los ejercicios de la unidad 6.
- **Interface:** La cuarta columna especifica la IP de la tarjeta de red donde enviaremos el paquete. Recuerda que un equipo puede tener varias tarjetas de red (reales o virtuales), cada una con su IP.
- **Métrica:** La métrica es un valor que se le asigna a una ruta y que se interpreta como el “coste” asociado a usar esa ruta. De este modo, en caso de que podamos elegir varias rutas, se escogerá la de menor coste. La métrica puede variar dependiendo de la velocidad de la ruta, el máximo n.º de saltos o el retraso temporal de dicha ruta.

Ahora veamos con más detalle las filas de la tabla anteriormente mostrada:

255.255.255.255	255.255.255.255	En vínculo	192.168.0.12	306
-----------------	-----------------	------------	--------------	-----

- Esta fila se interpreta como que si al equipo llega un paquete destinado exactamente a la IP 255.255.255.255 (broadcast), debe ser enviado a la IP 192.168.0.12 (es decir, la del equipo). Por tanto, los paquetes de broadcast serán aceptados.

192.168.0.255	255.255.255.255	En vínculo	192.168.0.12	306
---------------	-----------------	------------	--------------	-----

- Esta fila indica que si llega un paquete destinado exactamente a la IP 192.168.0.255 (dirección de difusión de la red), deberá ser enviado a la IP 192.168.0.12 (la del equipo). Es decir, se acepta ese paquete.

127.0.0.1	255.255.255.255	En vínculo	127.0.0.1	331
-----------	-----------------	------------	-----------	-----

- Esta fila especifica que si nos llega un paquete cuya IP destino es exactamente 127.0.0.1 (loopback), lo enviaremos a 127.0.0.1 (nuestro equipo). Es decir, los paquetes de loopback los enviamos a nuestra propia máquina, y por tanto, no llegan a salir fuera.

127.0.0.0	255.0.0.0	En vínculo	127.0.0.1	331
-----------	-----------	------------	-----------	-----

- Esta fila especifica que si nos llega un paquete con IP destino 127.\*.\* (la máscara de la segunda columna indica que solo se tiene en cuenta el primer byte), aceptaremos el paquete. Recuerda que aunque se usa 127.0.0.1 como loopback, en realidad es el rango 127.\*.\* el que se puede usar como loopback. Esto significa que, por ejemplo, un paquete destinado a 127.2.3.6 también será aceptado por nuestro equipo e interpretado como loopback gracias a esta fila.

0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.12	50
---------	---------	-------------	--------------	----

- Esta fila indica que un paquete destinado a cualquier IP, será enviado a la puerta de enlace 192.168.0.1 a través de nuestra conexión 192.168.0.12. Recuerda que esta fila es evaluada en último lugar, por lo que tiene sentido que si un paquete no encaja con difusión o loopback o ninguna otra fila, sea enviado fuera. Es decir, si esta fila no estuviera, no podríamos salir al exterior.

Dada esta tabla de enrutamiento capturada en un equipo:

IPv4 Route Table				
Active Routes:				
Network	Destination	Netmask	Gateway	Interface Metric
0.0.0.0		0.0.0.0	10.18.6.1	10.18.6.211 10
10.18.6.0		255.255.255.0	On-link	10.18.6.211 266
10.18.6.211		255.255.255.255	On-link	10.18.6.211 266
10.18.6.255		255.255.255.255	On-link	10.18.6.211 266
127.0.0.0		255.0.0.0	On-link	127.0.0.1 306
127.0.0.1		255.255.255.255	On-link	127.0.0.1 306
127.255.255.255		255.255.255.255	On-link	127.0.0.1 306
224.0.0.0		240.0.0.0	On-link	127.0.0.1 306
224.0.0.0		240.0.0.0	On-link	10.18.6.211 266
255.255.255.255		255.255.255.255	On-link	127.0.0.1 306
255.255.255.255		255.255.255.255	On-link	10.18.6.211 266

- ¿Cuál es la IP del equipo que posee esta tabla?  
**10.18.6.211**
- ¿Cuál es la puerta de enlace del equipo?  
**10.18.6.1**
- Indica qué fila (primera, segunda, etc) de la tabla representa la siguiente información:
  - “Los paquetes de difusión global o broadcast son aceptados por la tarjeta de red”  
**Cuarta**
  - “Los paquetes destinados a 127.0.0.1 son aceptados por la tarjeta de red”  
**Sexta**
  - “Los paquetes destinados a cualquier IP que empiece por 127 son aceptados por la tarjeta de red”  
**Séptima**
  - “Los paquetes destinados a 10.18.6.211 son aceptados por la tarjeta de red”  
**Tercera**
  - “Los paquetes destinados a la dirección de difusión de la LAN son aceptados por la tarjeta de red”  
**Cuarta**
  - “Los paquetes que no encajen con ninguna de las otras filas serán enviados a la puerta de enlace”  
**Primera**

Completa esta tabla de enrutamiento, correspondiente a un equipo con IP 192.168.0.1, sin subnetting y con puerta de enlace 192.168.0.254:

<i><b>Destino de red</b></i>	<i><b>Máscara</b></i>	<i><b>Puerta de enlace</b></i>	<i><b>Interface</b></i>
0.0.0.0	0.0.0.0	192.168.0.254	192.168.0.1
192.168.0.255	255.255.255.255	On-Link	192.168.0.1
192.168.0.1	255.255.255.255	On-Link	192.168.0.1
127.0.0.0	255.0.0.0	On-Link	127.0.0.1
127.0.0.1	255.255.255.255	On-Link	127.0.0.1
255.255.255.255	255.255.255.255	On-Link	127.0.0.1
255.255.255.255	255.255.255.255	On-Link	192.168.0.1

Pega aquí un pantallazo de la tabla de encaminamiento de tu equipo.

### Tabla de enrutamiento normal.

```

Administrador: Windows PowerShell (x86)
PS C:\Users\SMR> route PRINT -4
=====
Lista de interfaces
4...08 00 27 6e 29 8c .....Intel(R) PRO/1000 MT Desktop Adapter
1.....Software Loopback Interface 1
=====

IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de enlace      Interfaz      Métrica
-----
0.0.0.0             0.0.0.0             192.168.0.1           192.168.0.16  25
127.0.0.0           255.0.0.0           En vínculo            127.0.0.1     331
127.0.0.1           255.255.255.255     En vínculo            127.0.0.1     331
127.255.255.255     255.255.255.255     En vínculo            127.0.0.1     331
192.168.0.0         255.255.255.0       En vínculo            192.168.0.16  281
192.168.0.16        255.255.255.255     En vínculo            192.168.0.16  281
192.168.0.255       255.255.255.255     En vínculo            192.168.0.16  281
224.0.0.0           240.0.0.0           En vínculo            127.0.0.1     331
224.0.0.0           240.0.0.0           En vínculo            192.168.0.16  281
255.255.255.255     255.255.255.255     En vínculo            127.0.0.1     331
255.255.255.255     255.255.255.255     En vínculo            192.168.0.16  281
=====
Rutas persistentes:
Ninguno
PS C:\Users\SMR>

```

### Tabla de enrutamiento sin puerta de enlace al la WAN.

```

Administrador: Windows PowerShell (x86)
PS C:\Users\SMR> route PRINT -4
=====
Lista de interfaces
4...08 00 27 6e 29 8c .....Intel(R) PRO/1000 MT Desktop Adapter
1.....Software Loopback Interface 1
=====

IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de enlace      Interfaz      Métrica
-----
127.0.0.0           255.0.0.0           En vínculo            127.0.0.1     331
127.0.0.1           255.255.255.255     En vínculo            127.0.0.1     331
127.255.255.255     255.255.255.255     En vínculo            127.0.0.1     331
192.168.0.0         255.255.255.0       En vínculo            192.168.0.16  281
192.168.0.16        255.255.255.255     En vínculo            192.168.0.16  281
192.168.0.255       255.255.255.255     En vínculo            192.168.0.16  281
224.0.0.0           240.0.0.0           En vínculo            127.0.0.1     331
224.0.0.0           240.0.0.0           En vínculo            192.168.0.16  281
255.255.255.255     255.255.255.255     En vínculo            127.0.0.1     331
255.255.255.255     255.255.255.255     En vínculo            192.168.0.16  281
=====
Rutas persistentes:
Ninguno
PS C:\Users\SMR>

```

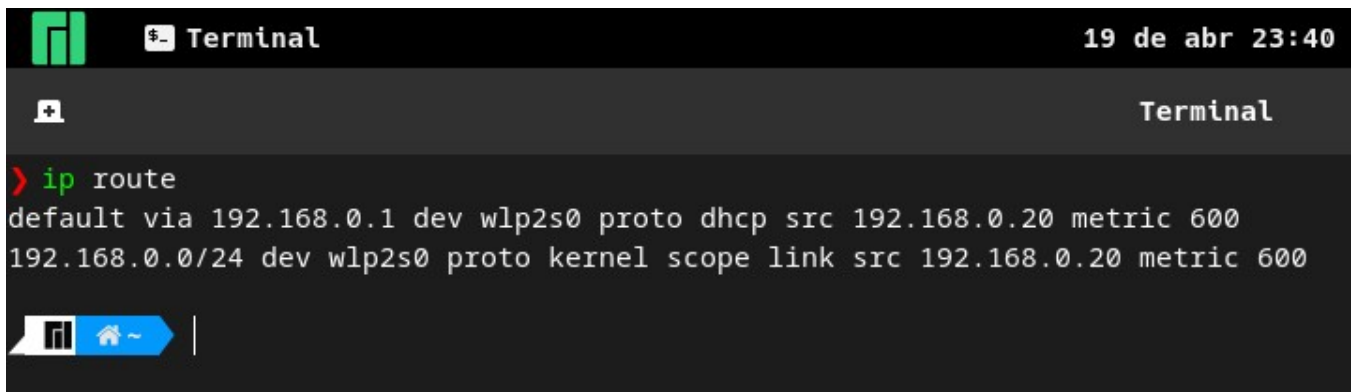
Ahora vamos a cambiar un poco tu tabla de encaminamiento (necesitarás privilegios de administrador). Teclea `route` sin parámetros para ver los ejemplos de cómo añadir y eliminar filas a una tabla.

- Elimina la fila “default” (la primera, con 0.0.0.0) de tu tabla. ¿Qué comando has tecleado? **route DELETE 0.0.0.0**  
Imprime de nuevo la tabla y comprueba que ha desaparecido la fila.  
¿Tienes acceso a Internet? **No**  
¿Por qué? **Porque he eliminando la puerta de enlace para acceder fuera de la LAN.**
- Lo más probable es que la fila “default” se añada automáticamente al cabo de unos instantes, ya que es fundamental para poder tener acceso al exterior. Si no se añadiera, ¿qué comando teclearías para hacerlo?  
**route ADD 0.0.0.0 MASK 0.0.0.0 192.168.0.1 METRIC 25**  
Si te equivocas o sigues sin tener acceso a la red, la tabla de enrutamiento se genera automáticamente cada vez que reinicias el equipo.
- ¿Qué fila de la tabla borrarías si no quisieras responder pings destinados a tu equipo?  
**route DELETE 192.168.0.16**

- Si elimináramos las filas que tienen 255.255.255.255 en la primera columna, ¿podrías enviar peticiones ARP? **Si porque tenemos la fila 192.168.0.255**  
¿Y responder a peticiones ARP de otros? **No**

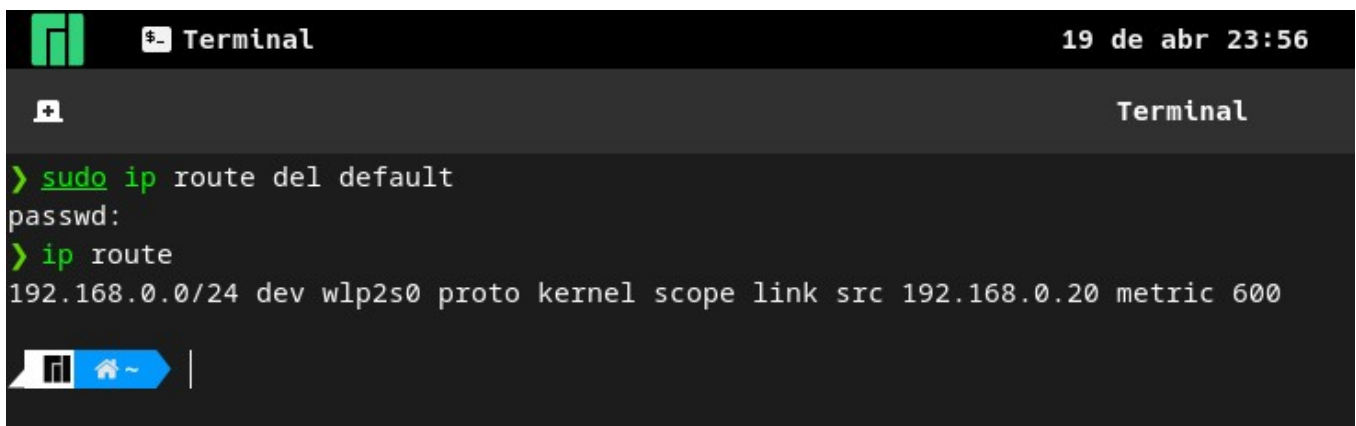
Desde Linux:

- Pega un pantallazo de tu tabla de encaminamiento (comando `ip route`)



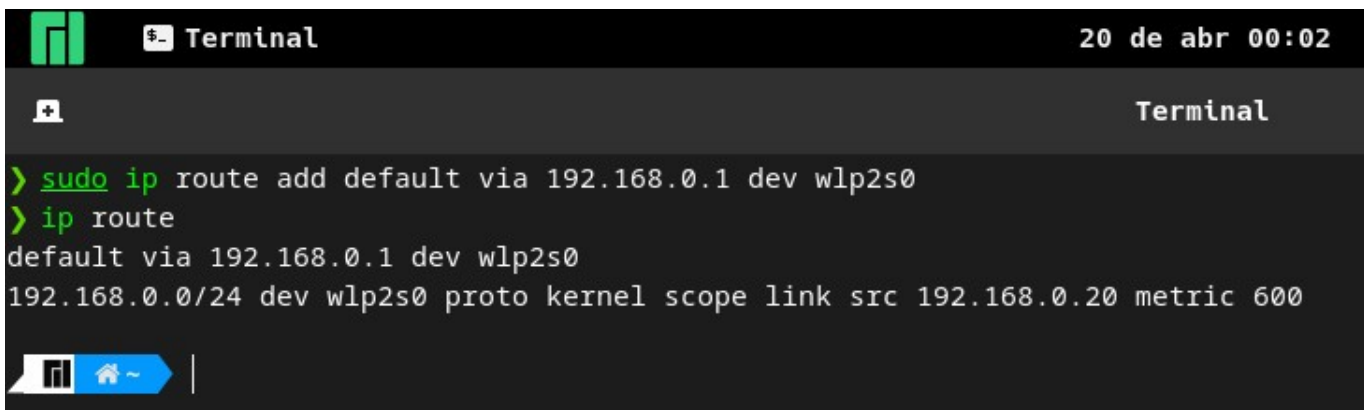
```
Terminal 19 de abr 23:40
Terminal
> ip route
default via 192.168.0.1 dev wlp2s0 proto dhcp src 192.168.0.20 metric 600
192.168.0.0/24 dev wlp2s0 proto kernel scope link src 192.168.0.20 metric 600
```

- Busca con qué parámetros borrarías la fila “default”  
**sudo ip route del default**



```
Terminal 19 de abr 23:56
Terminal
> sudo ip route del default
passwd:
> ip route
192.168.0.0/24 dev wlp2s0 proto kernel scope link src 192.168.0.20 metric 600
```

- Busca con qué parámetros añadirías una fila  
**sudo ip route add default via 192.168.0.1 dev wlp2s0**



```
Terminal 20 de abr 00:02
Terminal
> sudo ip route add default via 192.168.0.1 dev wlp2s0
> ip route
default via 192.168.0.1 dev wlp2s0
192.168.0.0/24 dev wlp2s0 proto kernel scope link src 192.168.0.20 metric 600
```

## Ejercicio 5: Windows PowerShell

El “Símbolo del sistema” de Windows (comando “cmd”) se lleva usando tradicionalmente en Windows desde hace décadas, y aunque es completamente funcional, las últimas versiones del SO proporcionan un shell mucho más potente y avanzado (por ejemplo, para autocompletar comandos y rutas con el tabulador). Puedes acceder a él buscando “Windows PowerShell” entre los programas de tu equipo.

En el siguiente ejercicio deberás teclear cada uno de los comandos desde PowerShell y, observando el resultado devuelto, indicar qué comando de los vistos en los ejercicios anteriores sería el equivalente.

Comando Windows PowerShell	Comando cmd/Símbolo del sistema
Get-NetAdapter	g)
Get-NetIPConfiguration	e)
Test-NetConnection <a href="http://www.google.es">www.google.es</a>	a)
Test-NetConnection <a href="http://www.google.es">www.google.es</a> -TraceRoute	c)
Get-NetTCPConnection	d)
Get-NetRoute	f)
Get-DnsClientCache	h)
Clear-DnsClientCache	b)

Los comandos del Símbolo del Sistema son:

- a) ~~ping [www.google.es](http://www.google.es)~~
- b) ~~ipconfig /flushdns~~
- c) ~~tracert [www.google.es](http://www.google.es)~~
- d) ~~netstat -na~~
- e) ~~ipconfig /all~~
- f) ~~route print~~
- g) ~~ipconfig~~
- h) ~~ipconfig /displaydns~~



### Ejercicio 6: Comparativa comandos de red Windows/Linux

Dada la siguiente tabla, completa con el comando Windows o Linux equivalente (incluyendo parámetros):

Windows	Linux
ping -n 5 www.google.es	ping -c 5 www.google.es
ping -n 6 -l 300 192.168.0.1	ping -c 6 -s 300 192.168.0.1
arp -a	ip neigh show
ipconfig /all	ip address
netstat -p tcp	ss -nt
route print	ip route o en mi caso también route -n me imprime la tabla de manera más entendible.

### Ejercicio 7: Resolución de errores en una LAN (I)

Dadas las siguientes situaciones, indica una posible causa y una posible solución para cada caso. Si hay múltiples causas de error, solo será necesario que indiques una.

a) Envías pings a equipos del exterior usando su nombre y no funcionan, pero si envías pings con la IP sí que funcionan

Causa:

Fallo en el servidor DNS.  
Fallo en el servidor DHCP cuando reparte la puerta de enlace DNS.

Solución:

Cambiar de servidor DNS.  
Cambiar la puerta de enlace del servidor DNS en el servidor DHCP.

b) Envías pings a [www.google.es](http://www.google.es) y no funcionan pero si envías pings a [www.bing.es](http://www.bing.es) o cualquier otro nombre, sí que funcionan

Causa:

La página [www.google.es](http://www.google.es) no acepta pings.  
La página [www.google.es](http://www.google.es) no funciona.

Solución:

No tiene solución pero tampoco es un problema.  
Esperar a que solucionen el problema los administradores de la página.

c) Envías pings a otro equipo de tu LAN y sí que funcionan pero al enviar cualquier ping al exterior no funciona

Causa:

Problemas con el router y la conexión al exterior (cable roto o mal conectado).  
Problemas con tu ISP.

Solución:

Cambiar el cable que le da acceso al exterior o si está mal conectado conectarlo bien.  
Llamar al proveedor y ver si está caído o que problema tiene.

d) Envías pings a otro equipo de tu LAN situado en la misma sala y sí que funcionan, pero al enviar cualquier ping a otro equipo de la LAN situado fuera de tu sala, no funciona. Tampoco funcionan pings al exterior.

Causa:

Problemas con la conexión del switch al router (cable roto o mal conectado).

Solución:

Cambiar la conexión que sale del switch al router.

e) Envías pings a cualquier equipo de tu LAN o del exterior y sí que funcionan, excepto al enviar ping a un equipo concreto situado en la misma sala que el tuyo.

Causa:

El equipo no funciona.  
El equipo tiene un firewall que filtra los paquetes ICMP.  
Está apagado o no conectado a la LAN.  
El cable de red está roto o desconectado.  
La tarjeta de red de ese equipo no funciona.

Solución:

Ver si el equipo funciona.  
Desactivar el filtro del firewall.  
Ver si está conectado a la LAN.  
Ver si el cable de red está conectado y en buen estado.  
Ver si su tarjeta de red funciona haciendo ping desde ese equipo a su localhost (127.0.0.1).

f) No funciona ningún ping enviado por tu equipo. El resto de equipos de tu LAN sí funcionan bien y tienen acceso

Causa:

Tu equipo no está conectado a la LAN.  
El cable de red está roto o desconectado.  
La tarjeta de red de tu equipo no funciona.

Solución:

Ver si está conectado a la LAN.  
Ver si el cable de red está conectado y en buen estado.  
Ver si tu tarjeta de red funciona haciendo ping a tu localhost (127.0.0.1).

g) No funciona ningún ping enviado por tu equipo y el resto de equipos de tu LAN tampoco funcionan bien

Causa:

Router de tu LAN averiado.

Solución:

Cambiar el router.

### **Ejercicio 8: Resolución de errores en una LAN (II)**

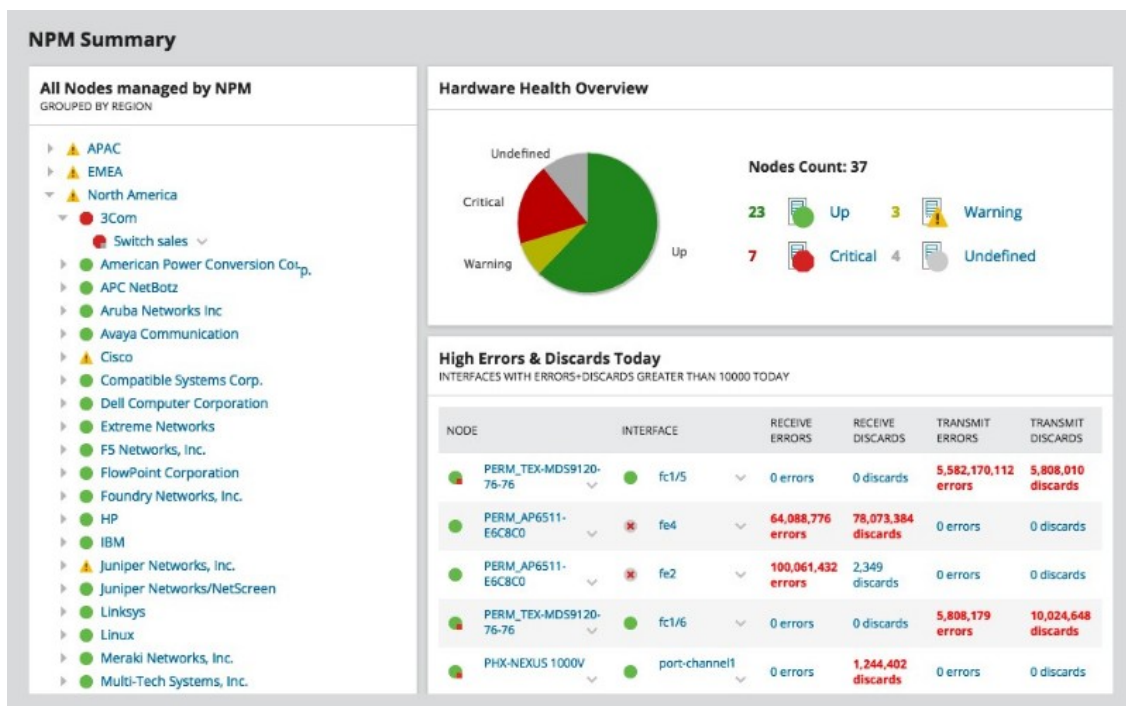
Como has visto en los ejercicios anteriores, es fácil comprobar desde un equipo cómo funciona el propio equipo, y también podemos hacernos una idea de cómo funciona el resto de la red. En redes muy grandes y complejas, existe la posibilidad de instalar una herramienta de monitorización de la red o NPM (Network Performance Monitor). Gracias a este tipo de herramientas, el administrador puede, de un vistazo, analizar el estado actual de toda la red desde un equipo. Este tipo de aplicaciones, pese a ser bastante complicadas tanto de instalar como de configurar, proporcionan al administrador una manera sencilla de detectar, aislar e incluso resolver problemas en una red.

Como ejemplo, vas a usar una herramienta (SolarWinds) que dispone de un simulador para que pruebes cómo funcionan este tipo de aplicaciones. Para ello, ve al siguiente enlace:

<https://www.solarwinds.com/network-performance-monitor?CMP=ORG-BLG-DNS>

Haz clic en el botón “Interactive Demo” y rellena los datos del formulario (no es necesario que sean datos reales). Después, haz clic en “Proceed to Online Demo” y luego en “Try Advanced”.

Verás un ejemplo de red en funcionamiento (la pantalla puede variar):



Veamos solamente algunas de las numerosas secciones que tiene esta herramienta:

- **All nodes managed by NPM:** Aquí aparece un listado de TODOS los dispositivos de la LAN, clasificados por su fabricante (Cisco, IBM,...) o el tipo de SO (Windows, Linux,...). Haz clic en “Manage nodes” para ver todos los nodos o dispositivos conectados. Luego haz clic en “Windows”. Verás una tabla con cuatro columnas.

¿Qué indica cada una de las cuatro columnas?

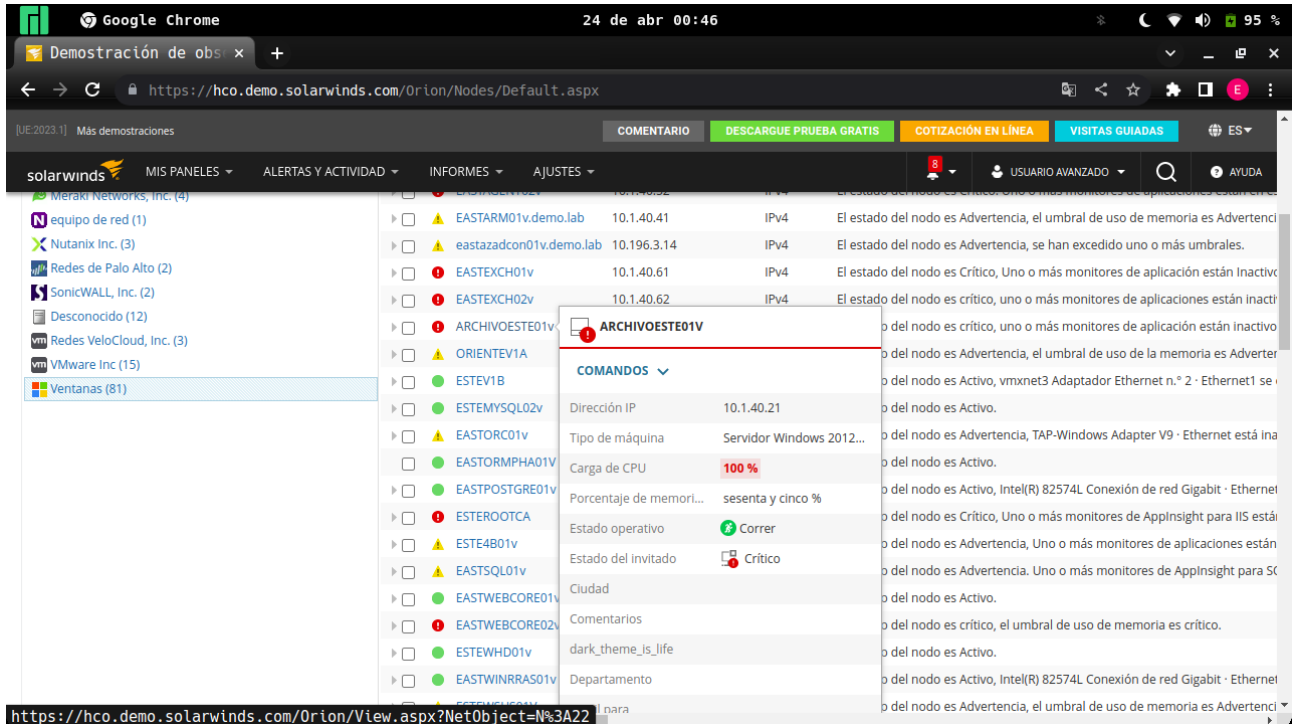
Name	Polling IP Address	IP Version	Status
Nombre	Dirección IP de sondeo	Versión IP	Estado

Cada dispositivo está clasificado con un color (rojo, amarillo, verde). ¿Qué indican los colores?

Verde:	Node status is Up. (El estado del nodo es Activo.)
Amarillo:	Node status is Warning. (El estado del nodo es Advertencia.)
Rojo:	Node status is Critical. (El estado del nodo es Crítico.)

Si dejas el ratón quieto unos instantes sobre un equipo (sin hacer clic en él), verás información adicional como el tiempo **promedio** de respuesta, la **carga** de la CPU o el porcentaje de **memoria** usada.

Pega aquí un pantallazo donde se vea un equipo que tenga una carga de CPU extremadamente alta.



Vuelve a la pantalla principal haciendo clic en My Dashboards, Network, NPM Summary.

- **MPLS network:** Aquí aparece un esquema de los diferentes routers de la red y cómo están organizados. Haz clic en “View Mode”.

En cada router aparece el estado actual (rojo o verde) de tres características. ¿Cuáles?

Temperature	Temperatura
Fan	Ventilador
Power supply	Fuente de alimentación

Las líneas que unen dispositivos están etiquetadas con dos números en cada extremo. ¿Qué indican esos datos?

Los kbps. El ancho de banda en kilo bits por segundo.

Finalmente, ve a My Dashboards, Network Configuration, Config Summary.

- **Config Summary:** Pega un pantallazo para cada apartado donde se vea claramente la respuesta a cada pregunta:

¿Cuántos dispositivos hicieron copia de seguridad (backup) de su configuración hace más de 7 días?

The screenshot shows the 'Config Summary' page in SolarWinds Hybrid Cloud Manager. The breadcrumb trail is 'Últimos archivos de configuración'. The left sidebar shows filters for 'Estado de la copia de seguridad' (Failed: 21, Successful: 3), 'Desajuste de la línea de base' (N/A: 21), 'Tipo de configuración' (Correr: 9), and 'Última fecha de copia de seguridad' (Los últimos 7 días: 1). The main table lists backup actions with columns: Nombre, Proveedor, Tipo de configuración, Estado de la copia de seguridad, and Fecha de la última copia de seguridad.

Nombre	Proveedor	Tipo de configuración	Estado de la copia de seguridad	Fecha de la última copia de seguridad
ESTE-FW-A	cisco	Correr	Exitoso	21/4/2023, 16:07
ESTE-FW-B	cisco	Correr	Exitoso	21/4/2023, 13:39
nexo-2	cisco	Correr	Exitoso	21/4/2023, 10:20
R1	cisco	Correr	Fallido	19/4/2023, 12:52

¿Cuántas vulnerabilidades del firmware son catalogadas como altas? 3257

The screenshot shows the 'Config Summary' page in SolarWinds Hybrid Cloud Manager. The breadcrumb trail is 'Firmware vulnerabilities'. The main dashboard shows 'All NCM nodes' with a polling status of 12 Warning, 0 Unknown, and 0 Other. Below this, there is a table of 'All NCM nodes' and a 'Firmware vulnerabilities' section showing a donut chart with 4,885 total vulnerabilities, 3257 High, and 1328 Medium.

Node	Vendor
DEN-7200-1A.demo.lab	Cisco
DEN-7200-2A.demo.lab	Cisco

Listado donde aparezca cuándo expira el soporte técnico para cada dispositivo.

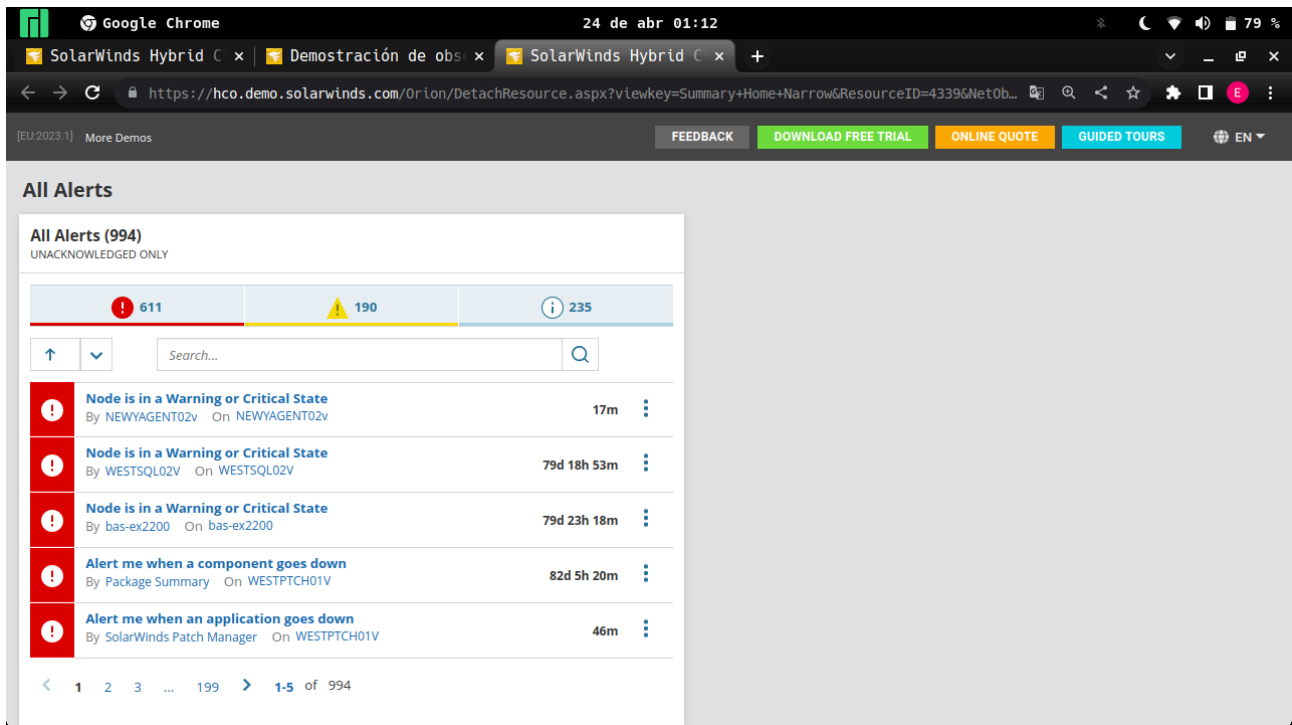
The screenshot shows the 'End of Support' table in SolarWinds Hybrid Cloud Manager. The table has columns: 'Expiration Date', 'Days Until Expiration', and 'Host Name'.

Expiration Date	Days Until Expiration	Host Name
2023-06-30T13:45:20.12	68	EASTFILE01V
2023-06-16T13:45:20.12	54	EASTROOTCA
2023-04-26T13:45:20.12	3	EASTADDC01V

Para terminar con SolarWinds, busca en sus numerosos menús, escoge dos secciones adicionales que no hayan sido mencionadas y te parezcan interesantes, y explica para qué crees que sirven, junto a un pantallazo de cada una.

*En MY DASHBOARDS > HOME > SUMMARY > ALL ALERTS*

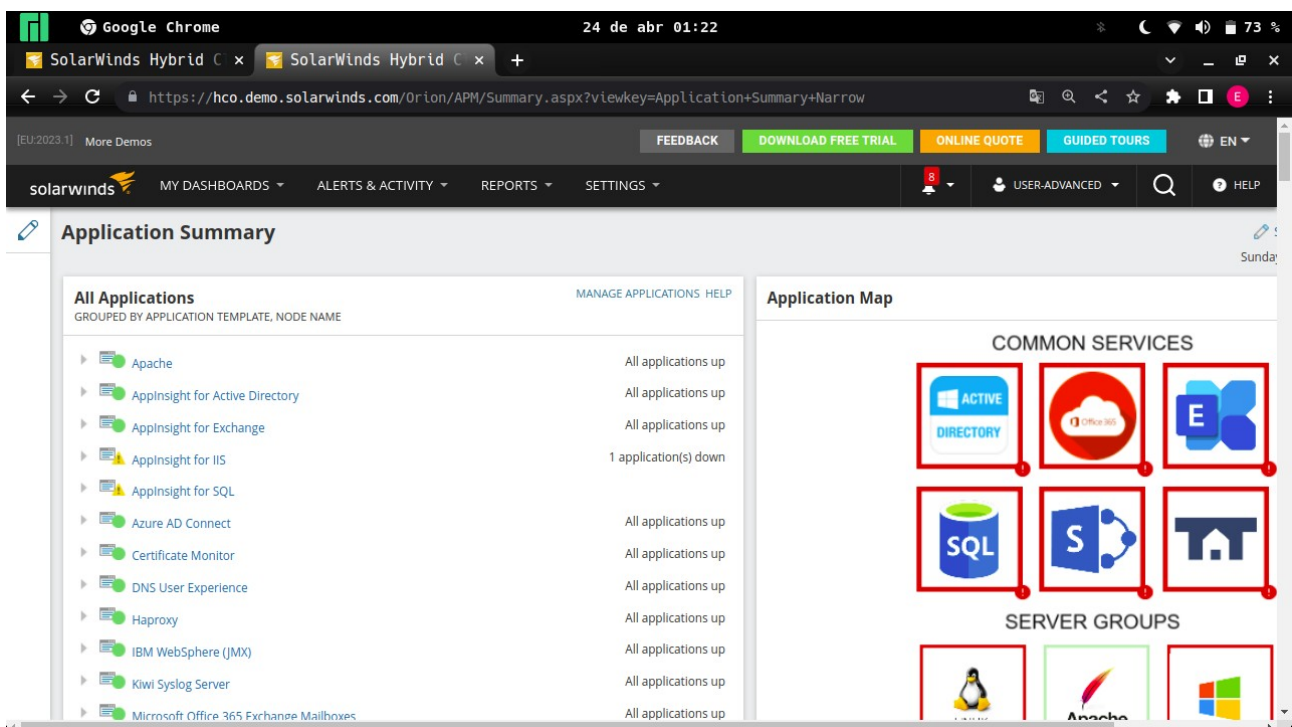
**Podemos saber todas las alertas críticas de todos los nodos.**



The screenshot shows the 'All Alerts' section of the SolarWinds Hybrid Cloud Manager interface. At the top, there's a summary of 994 alerts, with 611 critical (red exclamation mark), 190 warning (yellow triangle), and 235 informational (blue 'i'). Below this, a search bar and a list of alerts are visible. The list includes alerts like 'Node is in a Warning or Critical State' and 'Alert me when a component goes down'.

*En MY DASHBOARDS > APPLICATIONS > SAM SUMMARY*

**Podemos ver todas la aplicaciones instaladas y su estado.**



The screenshot shows the 'Application Summary' page in the SolarWinds Hybrid Cloud Manager. It displays a list of applications grouped by template, including Apache, AppInsight for Active Directory, AppInsight for Exchange, AppInsight for IIS, AppInsight for SQL, Azure AD Connect, Certificate Monitor, DNS User Experience, Haproxy, IBM WebSphere (JMX), Kiwi Syslog Server, and Microsoft Office 365 Exchange Mailboxes. The status of each application is shown as 'All applications up' or '1 application(s) down'. On the right, there's an 'Application Map' section showing 'COMMON SERVICES' and 'SERVER GROUPS' with icons for various services and servers.



## Ejercicio 9: Resolución de errores en una LAN (III)

A continuación verás dos listados, uno con problemas y otro con posibles soluciones. Asocia en la hoja final los problemas con la solución más adecuada para cada caso. Las soluciones propuestas son orientativas y genéricas.

### Problemas

1. La tarjeta de red no funciona. Sus LEDs aparecen siempre apagados, incluso probando con otro cable de repuesto.

a) Reemplazar la tarjeta de red por otra idéntica.

2. La conexión de un PC va demasiado lenta. La tarjeta de red es Fast Ethernet. El equipo no parece tener ningún otro problema.

e) Actualizar la tarjeta de red sustituyéndola por una Gigabit Ethernet. Estudiar el rendimiento general del equipo si persistiera el problema.

3. El router tiene funcionalidad limitada y problemas de estabilidad. Se detectan también incompatibilidades entre el router y algunos dispositivos.

i) Actualizar el firmware del router por una versión más reciente.

4. Un PC no se conecta a la red, pese a que en días anteriores sí que lo hacía correctamente. El resto de equipos funcionan con normalidad.

c) Comprobar si ambos extremos del cable están bien conectados y verificar si el cable no está dañado. Sustituirlo, de ser así.

5. Un portátil (conexión inalámbrica) va demasiado lento al acceder a la red.

g) Intentar acercar el portátil al router inalámbrico o punto de acceso. Analizar el uso de los canales y elegir un canal más libre. Comprobar la compatibilidad entre los estándares soportados por la tarjeta de red inalámbrica y el router o punto de acceso. Estudiar el rendimiento general del portátil.

6. En un servidor aparece el mensaje "Conflicto de direcciones"

b) El administrador recientemente cambió la IP estática de un equipo, y esa IP está dentro del rango de direcciones a repartir por el servidor DHCP. Hay que modificar la IP estática que se cambió, o excluirla del rango a repartir.

7. Un equipo con IP dinámica, al que antes siempre se le asignaba la misma IP dinámica sin problema, recibe una IP del rango 169.x.x.x desde hace unos días. Recientemente se sustituyó su tarjeta de red por otra más potente y desde entonces no tiene conexión. Los LEDs de la tarjeta y del switch se iluminan correctamente.

j) Realizar la nueva reserva asociada con la MAC adecuada en el servidor DHCP.

8. Toda la red en general va lenta.

d) Comprobar mediante un analizador de tráfico que los usuarios no están viendo contenido no permitido que posiblemente sature la red (por ejemplo, streaming o continuas descargas de gran tamaño). Estudiar el rendimiento de los servidores de manera individualizada. Comprobar el estado general de los switches.

9. A determinadas horas y solo en determinadas zonas de la LAN, la red va lenta.

k) Usar un analizador del tráfico para comprobar si hay equipos que tal vez envían demasiado tráfico por difusión en esas zonas de la red. Estudiar la posibilidad de usar

VLAN o subnetting para disminuir la difusión. Reiniciar los switches de las zonas afectadas.

10. De repente, ningún equipo recibe IP dinámica.

h) El firewall de la red (situado también en el servidor DHCP) avisa de que su log ha desbordado el disco duro interno. Limpiar o eliminar el log y reiniciar el servidor.

11. El antivirus de un equipo alerta de una posible infección

f) Confinar todos los archivos sospechosos y dejarlos en cuarentena. Aislar el equipo para que no intercambie datos con el resto. Desinfectar el equipo. Registrar los posibles envíos de datos llevados a cabo por el usuario del equipo (posible compartición de pendrives o de archivos infectados). Estudiar el uso de los puertos del equipo en busca de un virus que intente propagarse por la red. Obtener el ejecutable asociado a la infección y eliminarlo (de la RAM, del disco y de su posible carga al iniciar el equipo). Restaurar la copia de seguridad más reciente del equipo para evitar una mayor pérdida de datos y dejarlo en un estado correcto. Analizar el resto de la red por si hubiera posibles infecciones adicionales.

Problema	Solución
1	a
2	e
3	i
4	c
5	g
6	b
7	j
8	d
9	k
10	h
11	f