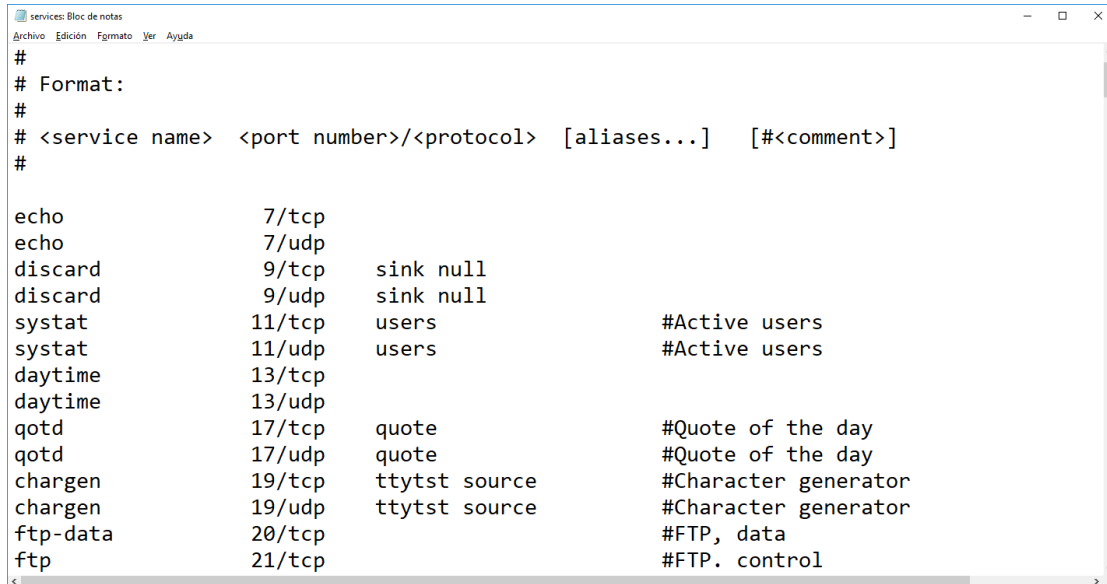


# Comandos de Linux para puertos

Los protocolos por defectos utilizados en windows se pueden ver en la carpeta Windows\System32\drivers\ en el fichero services se ve también el tipo de protocolo TCP o UDP.



```
#
# Format:
#
# <service name> <port number>/<protocol> [aliases...] [#<comment>]
#
echo                7/tcp
echo                7/udp
discard             9/tcp    sink null
discard             9/udp    sink null
systat              11/tcp    users          #Active users
systat              11/udp    users          #Active users
daytime             13/tcp
daytime             13/udp
qotd                17/tcp    quote         #Quote of the day
qotd                17/udp    quote         #Quote of the day
chargen             19/tcp    ttytst source #Character generator
chargen             19/udp    ttytst source #Character generator
ftp-data            20/tcp
ftp                 21/tcp    #FTP. control
```

Comandos para ver los puertos utilizados por el sistema operativo en los servicios activos.

## WINDOWS

NETSTAT, muestra información de los protocolos y conexiones TCP/IP.

- Sin parámetros muestra las conexiones activas.
- -a, muestra todas las conexiones y puertos de escucha.
- -b, muestra el ejecutable que crea la conexión o puerto de escucha.
- -o, muestra el Identificador del proceso a cada conexión.
- n°, si indicamos un número, es el número de segundos en volver a chequear la información.
- -n, muestra los puertos y direcciones en valor numérico.
- -e, muestra la estadística de internet, paquetes enviados, recibidos,...

Netstat -ano 6 > c:\datos\puetos.txt      enviamos la información a un fichero.

Nslookup, nos devuelve la dirección de internet de una dirección de internet o url.

Nslookup [www.google.es](http://www.google.es)  
Nos devuelve 72.125.140.94

## LINUX

netstat, muestra las conexiones en red, tablas de ruteo, estadísticas, etc...

netstat --inet    muestra solo las conexiones activas TCP/IP.  
netstat -l        lista los puertos que están abiertos (conexiones establecidas).  
netstat -r        muestra las rutas (similar a ejecutar route -r)

---

## Comandos de Linux para puertos

---

-u	para los puertos UDP.	-lu
-t	para los puertos TCP.	-lt
-n	muestra el número de puerto.	
-a	muestra las conexiones activas.	
-p	nos da el número de ID del proceso.	
-x	muestra todos los puertos de escucha.	

nmap, explora redes, determina el nombre del nodo y escanea puertos. Realiza funciones de auditoría y seguridad de redes. Hay que instalar el paquete.

nmap	ip o nombre	
nmap	ip/n	escanea un segmento de red.
	nmap 192.168.14.0/30	escanea el rango indicado
nmap	ip/n --exclude ip,ip,..	excluye esas ip dentro del rango.
nmap	-p nºpuerto ip	escanea un solo puerto de la ip indicada.
nmap	-sT ip	escanea puertos abiertos TCP de una máquina.
nmap	-sU ip	escanea puertos abiertos UDP de una máquina.
nmap	-sO ip	escanea puertos abiertos de cualquier protocolo.
nmap	-p mínimo-máximo ip	escanea un rango de puertos.

netcat o nc, herramienta para el análisis de la red. Trabajamos con cliente y servidor.

nc	-parámetros ip puerto	
nc -l nºpuerto		dejamos un puerto a la escucha. Servidor
nc localhost nº puerto		nos conectamos al puerto abierto. Cliente
Podemos utilizarlo para transferir archivos.		
En el servidor nc -l nº puerto > fichero recoge información.		
En el cliente cat fichero(a enviar)   nc localhost nº puerto		
nc -w numero localhost nºpuerto cierra la conexión después de los segundos indicados en número.		
-4 o -6 indicamos que protocolo IPv estamos utilizando.		
-z, cierra la conexión.		
-v, permite ver si el puerto esta abierto.		

lsof, lista los ficheros abiertos del sistema.

lsof -p PID	lista los ficheros abiertos de un PID.
lsof -u usuario	lista los ficheros abiertos de un usuario.
lsof -i	lista de puertos UDP y TCP en escucha y las conexiones activas del sistema.

Otros comandos o herramientas.

iptraf, monitor local de red muy completo, con el que podemos estar informados en todo momento de los paquetes que entran y salen de cada interfaz de red, así como la información adicional sobre paquetes con error, estadísticas y otras utilidades.

iftop, proporciona una visión continua e interactiva del tráfico de red que pasa por una interfaz.

tcpdump, es la mejor herramienta de línea de comandos en Linux y Unix para analizar e interceptar tráfico de red entrante y saliente de las redes a las que el equipo en el que se ejecuta está conectado.

<https://e1ement2048.wordpress.com/2007/10/26/herramientas-de-monitoreo/>

### HERRAMIENTA GRÁFICA DE WINDOWS

CURRENTPORTS. Pequeña utilidad para comprobar los puertos abiertos y conexiones creadas en tu Pc. Nos da bastante información sobre si hay una conexión abierta, el puerto remoto, el ID del proceso, protocolo utilizado, estado de la conexión, ruta del archivo en disco... También podemos cerrar los procesos, guardar un log, mirar las propiedades del proceso y archivo.

<http://www.nirsoft.net/utils/cports.html>

Existen herramientas gráficas para ello como tcpview.