PUERTO	NOMBRE	DESCRIPCIÓN
20	**FTPS-datos**	Protocolo de Transferencia de Ficheros - datos
21	**FTP-control**	Protocolo de Transferencia de Ficheros - control
22	**SSH**	**S**ecure **SH**ell - Intérprete de órdenes seguro
23	**TELNET**	**Tel**etype **Net**work
25	**SMTP**	**S**imple **M**ail **T**ransfer **P**rotocol
53	**DNS**	Sistema de Nombres de Dominio
67	**DHCP**	Puerto para el servidor DHCP
68	**DHCP**	Puerto para el cliente DHCP
69	**TFTP**	Protocolo Trivial de Transferencia de Ficheros
80	**HTTP**	Protocolo de Transferencia de HiperTexto
109	**POP2**	Post Office Protocol versión 2 (Correo electrónico)
110	**POP3**	Post Office Protocol versión 3(Correo electrónico)
123	**NTP**	**N**etwork **T**ime **P**rotocol (sincronizar los relojes del sistema)
143	**IMAP4**	Internet Message Access Protocol (Correo electrónico)
220	**IMAP3**	Internet Message Access Protocol versión 3
443	**HTTPS**	Usado para la transferencia segura de páginas web

COMANDO PING EN LINUX Y WINDOWS		
ARGUMENTO	LINUX	WINDOWS
Número específico de pings	-c	-n
Pings sin parar		-t
Especificar tamaño del paquete icmp en bytes	-s	-l
Especificar el ttl de paquete icmp	-t	-i
No fragmentar el paquete icmp	-M dont	-f
Intervalo de espera entre paquetes	-i	
Mostrar solamente las estadísticas finales	-q	
Forzar el uso de ipv4 o ipv6	-4 o -6	-4 o -6

COMANDO IP LINUX	
DEFINICIÓN	COMANDO
Mostrar ipv4 e ipv6 y la máscara de todas las tarjetas de red	ip addres
Mostrar la MTU y los paquetes recibidos (RX) y transmitidos (TX)	ip -s addres
Mostrar la MTU, (RX) y (TX) en formato legible K, M, G...	ip -s -h addres
Mostrar todas las tarjetas de red y sus MACs	ip link
Mostrar información usando colores	ip -c link
Mostrar información en formato tabla	ip -br link
Mostrar información del enrutamiento	ip route
Mostrar el contenido de la tabla ARP	ip neigh show

COMANDO NETSTAT WINDOWS (SS EN LINUX)	
DEFINICIÓN	COMANDO
Muestra las conexiones activas del equipo	netstat
Muestra **todas** las conexiones del equipo estén activas o no	netstat -a
Muestra, además de las conexiones, el **ejecutable** asociado a dicha conexione	netstat -b
Muestra **estadísticas** de envío y recepción	netstat -e
Muestra las IP y los puertos siempre con **números**	netstat -n
Muestra estadísticas según el **protocolo** especificado (IPv4, IPv6, ICMP...)	netstat -p **tcp**
Muestra la tabla de **enrutamiento** del equipo	netstat -r
Muestra estadísticas de **todos los protocolos** (IPv4, IPv6, ICMP, UDP y TCP)	netstat -s
Muestra las conexiones, y los datos van **actualizándose cada 3 segundos**	netstat 3
Muestra **todas** las conexiones con **números** y también el **ejecutable**	netstat -nba

COMANDO SS LINUX (NETSTAT EN WINDOWS)	
DEFINICIÓN	COMANDO
Muestra las conexiones	ss
Muestra todas las conexiones	ss -a
Muestra las conexiones en formato número	ss -n
Muestra las conexiones que estén en escucha (listening)	ss -l
Muestra las conexiones con la opción que le demos	ss -o
Muestra las conexiones tcp	ss -t
Muestra las conexiones udp	ss -u
Muestra las conexiones IPv4	ss -4
Muestra las conexiones IPv6	ss -6

CLASE	EL BINARIO EMPIEZA	PRIVADAS	PÚBLICAS
A	**0**000 0000.	10.0.0.0 - 10.255.255.255	1.0.0.0 - 126.255.255.255
B	**10**00 0000.	172.16.0.0 - 172.31.255.255	128.0.0.0 - 191.255.255.255
C	**110**0 0000.	192.168.0.0 - 192.168.255.255	192.0.0.0 - 223.255.255.255
D	**1110** 0000.	224.0.0.0 - 239.255.255.255	
lopback		127.0.0.0 - 127.255.255.255	
APIPA		169.0.0.0 - 169.255.255.255	

NAT

Network Address Translation o NAT (Traducción de direcciones de red) es la técnica empleada para asociar IP privadas de los equipos de una LAN en una IP pública para cuando los paquetes salen al exterior.

- **NAT estático o SNAT**: en este caso, el router tiene una tabla donde está guardada la IP pública externa a la que tiene que traducir cada IP privada interna de la LAN. Se necesitarán por tanto varias IP públicas. Cada IP privada siempre tendrá una IP pública asociada, que será la misma para ese equipo.
- **NAT dinámico o DNAT**: al igual que el anterior, el router tiene un conjunto de IP públicas, pero en este caso cada equipo no recibirá siempre la misma, sino que se escogerá una IP pública libre de entre todas las que tiene el router.
- **NAT por puertos o PAT**: Este es el reparto más usado en la actualidad. En este caso, el router solo dispone de una IP pública, la misma para todos. Es la unión entre IP y puerto la que se usa para distinguir conexiones.

FILTROS WIRESHARK

QUE HACE EL FILTRO	FILTRO
Paquetes enviados a tu tarjeta de red	eth.dst == mi IP
Paquetes enviados por tu tarjeta de red	eth.src == mi IP
Paquetes enviados a tu IP	ip.dst == mi IP
Paquetes enviados por tu IP	ip.src == mi IP
Paquetes que tengan parte opcional al final de la cabecera IP	ip.hdr_len > 20
Paquetes con longitud mayor que 500 bytes	ip.len > 500
Paquetes con TTL mayor que 10	ip.ttl > 10
Paquetes que no usen TCP en la capa de transporte	ip.proto != 6
Paquetes que usen UDP en la capa de transporte	ip.proto == 17
Paquetes que usen ICMP en la capa de transporte	ip.proto == 1
Paquetes que no puedan fragmentarse	ip.flags.df == 1
Respuestas DNS	udp.srcport == 53
Peticiones HTTPS	tcp.dstport == 443
Paquetes SYN+ACK	tcp.flags == 0x012
Respuestas DHCP	udp.srcport == 67
Paquetes FTP	tcp.port == 21
Paquetes IPv6 enviados a tu ordenador	ipv6.dst == mi IPv6
Paquetes IPv6 con ttl mayor que 10	ipv6.hlim > 10
Paquetes IPv6 con zona de datos mayor que 500	ipv6.plen > 500
Paquetes IPv6 que usen UDP en el nivel de transporte	ipv6.nxt == 17