# Principales puertos TCP y UDP y para qué sirven cada uno de ellos

Para comunicarnos extremo a extremo necesitamos usar lo que denomina puerto, ya que **TCP y UDP** se ubican en la capa de transporte de la pila de protocolos TCP/IP. Hay una serie de **puertos bien conocidos** que sirven para aplicaciones específicas, y otros puertos que son utilizados por diferentes software como juegos, servicios online etc.

Cualquier aplicación o servicio que usemos, desde videojuegos, gestores de correo electrónico, mensajería instantánea o incluso el propio sistema operativo, siempre tienen una serie de puertos abiertos transmitiendo o escuchando lo que sucede a su alrededor.

Los puertos pueden ser de dos tipos diferentes, dependiendo del protocolo de la capa de transporte que se utilice. El protocolo TCP es un protocolo conectivo, fiable y orientado a conexión, se encarga de que lleguen todos los segmentos correctamente, y realiza las retransmisiones necesarias en caso de que ocurra algún tipo de problema, además, también garantiza el orden, por lo que las capas superiores no tienen que encargarse de ello.

UDP es un protocolo no orientado a conexión, no es fiable, no garantiza que lleguen los paquetes ni tampoco su orden, para ello las capas superiores (capa de aplicación) garantizarán esto.

Una vez que ya conocemos las principales características de TCP y de UDP, veamos cuáles son los principales puertos que usamos a diario, para que son y para qué sirven:

## Principales puertos TCP

Cuando necesitamos acceder a un servicio desde Internet, es totalmente necesario abrir un puerto en nuestro router. Actualmente disponemos de dos protocolos en la capa de transporte, TCP y UDP, por tanto, dependiendo del tipo de servicio que queramos utilizar, tendremos que abrir el puerto TCP o UDP, aunque también podría haber servicios que necesiten abrir un puerto TCP y UDP simultáneamente.

El protocolo TCP es un protocolo conectivo, fiable y orientado a conexión, esto significa que es capaz de retransmitir los segmentos de paquetes en caso de que haya alguna pérdida desde el origen al destino. El protocolo TCP para establecer la conexión realiza el 3-way handshake, con el objetivo de que la conexión sea lo más fiable posible.

Si estamos utilizando algún protocolo en la capa de aplicación como HTTP, FTP o SSH que todos ellos utilizan el protocolo TCP, en la primera comunicación se realizará este intercambio de mensajes.

Si vas a montar en tu casa, oficina o empresa algún tipo de servidor, como un servidor FTP, SSH o OpenVPN, entonces deberás abrir uno o varios puertos para poder hacer uso de estos servicios y acceder desde Internet. Actualmente todos los routers hacen NAT con la IP pública, por tanto, es completamente necesario abrir puertos en la NAT, o mejor dicho, realizar el reenvío de puertos (port forwarding) para que sean accesibles desde Internet. A continuación, podrás ver un completo listado de los principales puertos TCP que usan muchos protocolos de la capa de aplicación y también aplicaciones:

- **Puerto 21**: El puerto 21 por norma general se usa para las conexiones a servidores FTP en su canal de control, siempre que no hayamos cambiado el puerto de escucha de nuestro servidor FTP o FTPES.
- **Puerto 22**: Por normal general este puerto se usa para conexiones seguras SSH y SFTP, siempre que no hayamos cambiado el puerto de escucha de nuestro servidor SSH.
- **Puerto 23**: Telnet, sirve para establecer conexión remotamente con otro equipo por la línea de comandos y controlarlo. Es un protocolo no seguro ya que la autenticación y todo el tráfico de datos se envía sin cifrar.

- **Puerto 25**: El puerto 25 es usado por el protocolo SMTP para él envió de correos electrónicos, también el mismo protocolo puede usar los puertos 26 y 2525.
- **Puerto 53**: Es usado por el servicio de DNS, Domain Name System.
- **Puerto 80**: Este puerto es el que se usa para la navegación web de forma no segura HTTP.
- **Puerto 101**: Este puerto es usado por el servicio Hostname y sirve para identificar el nombre de los equipos.
- **Puerto 110**: Este puerto lo usan los gestores de correo electrónico para establecer conexión con el protocolo POP3.
- **Puerto 143**: El puerto 143 lo usa el protocolo IMAP que es también usado por los gestores de correo electrónico.
- **Puerto 443**: Este puerto es también para la navegación web, pero en este caso usa el protocolo HTTPS que es seguro y utiliza el protocolo TLS por debajo.
- **Puerto 445**: Este puerto es compartido por varios servicios, entre el más importante es el Active Directory.
- **Puerto 587**: Este puerto lo usa el protocolo SMTP SSL y, al igual que el puerto anterior sirve para el envío de correos electrónicos, pero en este caso de forma segura.
- **Puerto 591**: Es usado por Filemaker en alternativa al puerto 80 HTTP.
- **Puerto 853**: Es utilizado por DNS over TLS.
- **Puerto 990**: Si utilizamos FTPS (FTP Implícito) utilizaremos el puerto por defecto 990, aunque se puede cambiar.

- **Puerto 993**: El puerto 993 lo usa el protocolo IMAP SSL que es también usado por los gestores de correo electrónico para establecer la conexión de forma segura.
- **Puerto 995**: Al igual que el anterior puerto, sirve para que los gestores de correo electrónico establezcan conexión segura con el protocolo POP3 SSL.
- **Puerto 1194**: Este puerto está tanto en TCP como en UDP, es utilizado por el popular protocolo OpenVPN para las redes privadas virtuales.
- **Puerto 1723**: Es usado por el protocolo de VPN PPTP.
- **Puerto 1812**: se utiliza tanto con TCP como con UDP, y sirve para autenticar clientes en un servidor RADIUS.
- **Puerto 1813**: se utiliza tanto con TCP como con UDP, y sirve para el accounting en un servidor RADIUS.
- **Puerto 2049**: es utilizado por el protocolo NFS para el intercambio de ficheros en red local o en Internet.
- **Puertos 2082 y 2083**: es utilizado por el popular CMS cPanel para la gestión de servidores y servicios, dependiendo de si se usa HTTP o HTTPS, se utiliza uno u otro.
- **Puerto 3074**: Lo usa el servicio online de videojuegos de Microsoft Xbox Live.
- **Puerto 3306**: Puerto usado por las bases de datos MySQL.
- **Puerto 3389**: Es el puerto que usa el escritorio remoto de Windows, muy recomendable cambiarlo.

- **Puerto 4662 TCP y 4672 UDP**: Estos puertos los usa el mítico programa eMule, que es un programa para descargar todo tipo de archivos.
- **Puerto 4899**: Este puerto lo usa Radmin, que es un programa para controlar remotamente equipos.
- **Puerto 5000**: es el puerto de control del popular protocolo UPnP, y que por defecto, siempre deberíamos desactivarlo en el router para no tener ningún problema de seguridad.
- **Puertos 5400, 5500, 5600, 5700, 5800 y 5900**: Son usados por el programa VNC, que también sirve para controlar equipos remotamente.
- **Puertos 6881 y 6969**: Son usados por el programa BitTorrent, que sirve para e intercambio de ficheros.
- **Puerto 8080**: es el puerto alternativo al puerto 80 TCP para servidores web, normalmente se utiliza este puerto en pruebas.
- **Puertos 51400**: Es el puerto utilizado de manera predeterminada por el programa Transmission para descargar archivos a través de la red BitTorrent.
- **Puerto 25565**: Puerto usado por el famoso videojuego Minecraft.

Un aspecto muy importante de los puertos TCP, es que existe un rango de puertos desde el 49152 al 65535 que son los puertos efímeros, es decir, con cada conexión de origen que nosotros realicemos, se utilizan estos puertos que son dinámicos. Por ejemplo, si realizamos una petición a una web, el puerto de origen estará en este rango 49152-65535, y el puerto de destino será el 80 (HTTP) o 443 (HTTPS).

Y estos serían los puertos más usados e importantes cuando hacen uso del protocolo TCP. En los equipos siempre los tendremos abiertos a no ser que un firewall lo esté cerrando explícitamente, pero en el router deberemos abrir todos estos puertos (port-forwarding o también conocido como reenvío de puertos) ya que estamos en un entorno NAT, y todos los puertos están cerrados.

## Principales puertos UDP

- **Puerto 23**: Este puerto es usado en dispositivos Apple para su servicio de Facetime.
- **Puerto 53**: Es utilizado para servicios DNS, este protocolo permite utilizar tanto TCP como UDP para la comunicación con los servidores DNS.
- **Puerto 500**: este puerto es utilizado por el protocolo de VPN IPsec, concretamente se usa por ISAKMP para la fase 1 del establecimiento de la conexión con IPsec.
- **Puerto 514**: Es usado por Syslog, el log del sistema operativo.

- **Puerto 1194**: este puerto es el predeterminado del protocolo OpenVPN, aunque también se puede utilizar el protocolo TCP. Lo más normal es usar UDP 1194 porque es más rápido a la hora de conectarnos y también de transferencia, obtendremos más ancho de banda.
- **Puerto 1701**: Es usado por el protocolo de VPN L2TP.
- **Puerto 1812**: se utiliza tanto con TCP como con UDP, y sirve para autenticar clientes en un servidor RADIUS.
- **Puerto 1813**: se utiliza tanto con TCP como con UDP, y sirve para el accounting en un servidor RADIUS.
- **Puerto 4500**: este puerto también es utilizado por el protocolo de VPN IPsec, se utiliza este puerto para que el funcionamiento de la NAT sea perfecto. Este puerto se utiliza en la fase 2 del establecimiento IPsec, pero también tenemos que tener abierto el puerto UDP 500.
- **Puerto 51871**: es utilizado por el protocolo de VPN Wireguard de manera predeterminada.

Tal y como habéis visto, tenemos una gran cantidad de puertos TCP y UDP que utilizaremos muy a menudo. Estos son los principales puertos que podemos utilizar para los diferentes servicios, no obstante, hay cientos de puertos TCP y UDP más que utilizan diferentes aplicaciones, pero estos son los más importantes y utilizados.