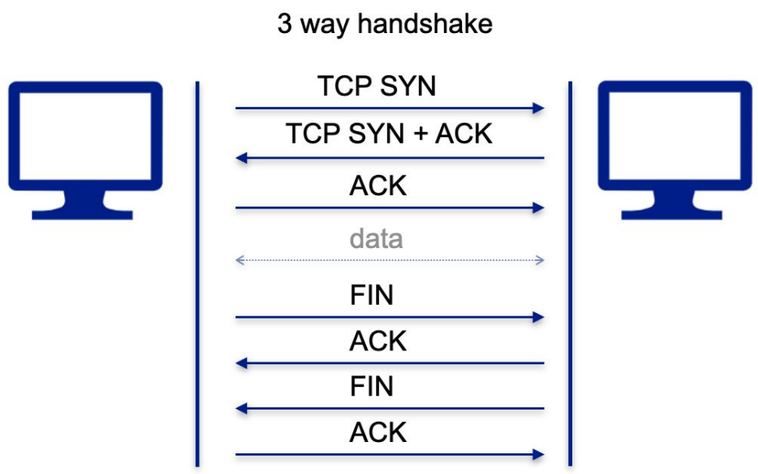
¿Qué es?

El **Protocolo de Control de Transmisión** (TCP) se define como un **protocolo de comunicación orientado a la conexión** que permite a dispositivos y aplicaciones **enviar datos a través de una red y verificar su entrega**, constituyendo uno de los pilares de internet. TCP se emplea en aquellos servicios que sacrifican la velocidad de carga en beneficio de la integridad y la exactitud de los datos que se transmiten, como es el caso de los servicios de correo electrónico IMAP/POP o la navegación web HTTP (anteriores a HTTP 3.0).

Orientado a la Conexión

Antes de poder enviar los datos es necesario establecer una conexión en la que se ponen de acuerdo ambos nodos, conocido como *3 way handshake*. Este acuerdo tiene **tres fases**, primero la fase de **conexión**, luego la fase de **transmisión de datos** y por último, la fase de **cierre de conexión**.



Características

Las virtudes de TCP hacen que sea un protocolo ideal para aquellos servicios que prefieren **sacrificar velocidad de transmisión en beneficio de la integridad** y la exactitud de los datos que se transmiten.

- **Ordenación:** el protocolo TCP garantiza que los paquetes enviados en un determinado orden, el destino los trata en el mismo orden.

- **Fiabilidad:** TCP cuenta con el sistema ARQ, cuya función es reenviar paquetes perdidos o corruptos de forma automática, garantizando así la integridad de los mensajes.

- **Control de flujo:** TCP se adecúa automáticamente al ancho de banda que existe entre los nodos que se comunican para evitar que la red se congestione.

UDP

autentia

¿Qué es?

El **Protocolo de Datagramas de Usuario** (UDP) se define como un **protocolo de comunicación no orientado a la conexión**, es decir, que no incorpora el establecimiento de la conexión y **se limita a transmitir paquetes de datos de un nodo a otro**. UDP se emplea principalmente en servicios como el VoIP, el streaming de contenido o los juegos en línea, ya que su prioridad es la inmediatez de la transmisión por encima de la integridad de los datos transmitidos.

Características

Comparado con otros protocolos, UDP realiza la comunicación de forma sencilla: **envía paquetes** (llamados datagramas) directamente a un ordenador de destino, **sin** necesidad de **establecer** primero una **conexión**, **ni indicar el orden** de dichos paquetes, **ni comprobar si han llegado** como estaba previsto.

Mientras que en TCP la comunicación se realiza a nivel de byte, UDP emplea datagramas completos en cada mensaje que se transmite.

Estas características son las que le otorgan su **particular velocidad de transmisión** que, por contra, pierde otras características como la ordenación y la fiabilidad.

Estructura de los datagramas

Un **datagrama** UDP **consta de una cabecera** de datagrama **seguida de una sección de datos** (los datos de carga útil para la aplicación). La cabecera del datagrama UDP consta de 4 campos, cada uno de 2 bytes (16 bits).

La identidad del emisor se especifica en el campo *source port* y la del destinatario en el *destination port*.

Los campos *length* y *checksum* son los responsables de verificar la corrección de los paquetes. Si esta verificación falla, los paquetes son descartados.

Bits	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
0	Source Port	Destination Port
32	Length	Checksum
64	Data	

Socket de red

autentia

¿Qué es?

Un socket de red es el **medio mediante el cuál dos procesos,** normalmente en diferentes máquinas o dentro de un mismo entorno, **establecen un intercambio de datos**.

Elementos principales

Un socket queda definido por una serie de elementos:

- **Protocolo** de la capa de transporte utilizado: TCP o UDP
- **Dirección IP de origen**: puede ser una IP pública o privada. Identifica al ordenador que envía los datos y es a donde hay que enviar la respuesta.
- **Dirección IP de destino**: puede ser una IP pública o privada. Identifica al ordenador que recibe los datos.
- **Puerto de origen o local**: Identifica a la aplicación, protocolo de más alto nivel, del ordenador que envía los datos y donde espera recibir la respuesta.
- **Puerto de destino o remoto**: Identifica a la aplicación, protocolo de más alto nivel, a la que hay que entregar los datos.

Puertos importantes

Aplicaciones o servicios como dns (53), ssh (22) o https (443) están estandarizados en la familia de protocolos de Internet y su número de puerto está ya definido y asignado. Estos números de puerto asignados se denominan puertos **bien-conocidos** (*well-known*).

Estos puertos ocupan **números en el rango de 0 a 1023** y los controla y asigna la Autoridad de Números Asignados de Internet (IANA).

Los **puertos registrados** ocupan números dentro del rango 1024-65535 pero no los controla la IANA.

Los puertos 49.152 a 65.535 son **puertos dinámicos** y se utilizan como puertos temporales, sobre todo por los clientes al comunicarse con los servidores.