1. **Capa de transporte**

La **capa de transporte** TCP/IP garantiza que los paquetes lleguen en secuencia y sin errores, al intercambiar la confirmación de la recepción de los datos y retransmitir los paquetes perdidos. Este tipo de comunicación se conoce como **transmisión de punto a punto**. Los protocolos de capa de transporte de este nivel son el Protocolo de control de transmisión (TCP), el Protocolo de datagramas de usuario (UDP) y el Protocolo de transmisión para el control de flujo (SCTP). Los protocolos TCP y SCTP proporcionan un servicio completo y fiable. UDP proporciona un servicio de datagrama poco fiable.

**Protocolo TCP**

TCP permite a las aplicaciones comunicarse entre sí como si estuvieran conectadas físicamente. TCP envía los datos en un formato que se transmite carácter por carácter, en lugar de transmitirse por paquetes discretos. Esta transmisión consiste en lo siguiente:

* Punto de partida, que abre la conexión.
* Transmisión completa en orden de bytes.
* Punto de fin, que cierra la conexión.

TCP conecta un encabezado a los datos transmitidos. Este encabezado contiene múltiples parámetros que ayudan a los procesos del sistema transmisor a conectarse a sus procesos correspondientes en el sistema receptor.

TCP confirma que un paquete ha alcanzado su destino estableciendo una conexión de punto a punto entre los hosts de envío y recepción. Por tanto, el protocolo TCP se considera un protocolo fiable orientado a la conexión.

**Protocolo SCTP**

SCTP es un protocolo de capa de transporte fiable orientado a la conexión que ofrece los mismos servicios a las aplicaciones que TCP. Además, SCTP admite conexiones entre sistema que tienen más de una dirección, o de **host múltiple**. La conexión SCTP entre el sistema transmisor y receptor se denomina **asociación**. Los datos de la asociación se organizan en bloques. Dado que el protocolo SCTP admite varios hosts, determinadas aplicaciones, en especial las que se utilizan en el sector de las telecomunicaciones, necesitan ejecutar SCTP en lugar de TCP.

**Protocolo UDP**

UDP proporciona un servicio de entrega de datagramas. UDP no verifica las conexiones entre los hosts transmisores y receptores. Dado que el protocolo UDP elimina los procesos de establecimiento y verificación de las conexiones, resulta ideal para las aplicaciones que envían pequeñas cantidades de datos.



* **La capa de Aplicación**
* Es la capa superior de los modelos OSI y TCP/IP. Es la capa que proporciona la interfaz entre las aplicaciones que utilizamos para comunicarnos y la red subyacente en la cual se transmiten los mensajes. Los protocolos de capa de aplicación se utilizan para intercambiar los datos entre los programas que se ejecutan en los hosts de origen y destino. Existen muchos protocolos de capa de aplicación y siempre se desarrollan protocolos nuevos.
* **Capa de Presentación Tiene tres funciones primarias:**
* Codificación y conversión de datos de la capa de aplicación para garantizar que los datos del dispositivo de origen puedan ser interpretados por la aplicación adecuada en el dispositivo de destino.
* Compresión de los datos de forma que puedan ser descomprimidos por el dispositivo de destino.
* Encriptación de los datos para transmisión y descifre de los datos cuando se reciben en el destino.
* Las implementaciones de la capa de presentación generalmente no se vinculan con una stack de protocolos determinada.
* Los estándares para vídeos y gráficos son algunos ejemplos. Dentro de los estándares más conocidos para vídeo encontramos QuickTime y el Grupo de expertos en películas (MPEG), intercambio gráfico (GIF), Grupo de expertos en fotografía (JPEG) y Formato de archivo de imagen etiquetada (TIFF). GIF y JPEG son estándares de compresión y codificación para imágenes gráficas, y TIFF es una formato de codificación estándar para imágenes gráficas
* **Capa de Sesión**

Las funciones en esta capa crean y mantienen diálogos entre las aplicaciones de origen y destino. La capa de sesión maneja el intercambio de información para iniciar los diálogos y mantenerlos activos, y para reiniciar sesiones que se interrumpieron o desactivaron durante un periodo de tiempo prolongado. La mayoría de las aplicaciones, como los exploradores Web o los clientes de correo electrónico, incorporan la funcionalidad de las capas 5, 6 y 7 del modelo OSI. Los protocolos de capa de aplicación de TCP/IP más conocidos son aquellos que proporcionan intercambio de la información del usuario.

Estos protocolos especifican la información de control y formato necesaria para muchas de las funciones de comunicación de Internet más comunes. Algunos de los protocolos TCP/IP son:

• El protocolo Servicio de nombres de dominio (DNS, Domain Name Service) se utiliza para resolver nombres de Internet en direcciones IP.

• El protocolo de transferencia de hipertexto (HTTP, Hypertext Transfer Protocol) se utiliza para transferir archivos que forman las páginas Web de la World Wide Web.

• El Protocolo simple de transferencia de correo (SMTP) se utiliza para la transferencia de mensajes de correo y adjuntos.

• Telnet, un protocolo de emulación de terminal, se utiliza para proporcionar acceso remoto a servidores y a dispositivos de red.

• El Protocolo de transferencia de archivos (FTP, File Transfer Protocol) se utiliza para la transferencia interactiva de archivos entre sistemas.

• Los protocolos de la suite TCP/IP generalmente son definidos por Solicitudes de comentarios (RFCS).

• El Grupo de trabajo de ingeniería de Internet mantiene las RFCS como los estándares para el conjunto TCP/IP.

1. **Analizadores de protocolo**

* **Wireshark:** antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de [software](https://es.wikipedia.org/wiki/Software) y protocolos, y como una herramienta didáctica. Cuenta con todas las características estándar de un analizador de protocolos.

La funcionalidad que provee es similar a la de [tcpdump](https://es.wikipedia.org/wiki/Tcpdump), pero añade una interfaz gráfica y muchas opciones de organización y filtrado de información. Así, permite ver todo el tráfico que pasa a través de una red (usualmente una red Ethernet, aunque es compatible con algunas otras) estableciendo la configuración en modo promiscuo. También incluye una versión basada en texto llamada tshark.

* [**tcpdump**](https://es.wikipedia.org/wiki/Tcpdump)**:** es una herramienta para línea de comandos cuya utilidad principal es analizar el tráfico que circula por la red.

Permite al usuario capturar y mostrar en tiempo real los paquetes transmitidos y recibidos por la red a la cual el ordenador está conectado. Fue escrito por Van Jacobson, Craig Leres, y Steven McCanne mientras trabajaban en el Grupo de Investigación de Red del Laboratorio Lawrence Berkeley. Más tarde el programa fue ampliado por Andrew Tridgell.

Tcpdump funciona en la mayoría de los sistemas operativos UNIX: Linux, Solaris, BSD, Mac OS X, HP-UX y AIX entre otros. En esos sistemas, tcpdump hace uso de la biblioteca libpcap para capturar los paquetes que circulan por la red.