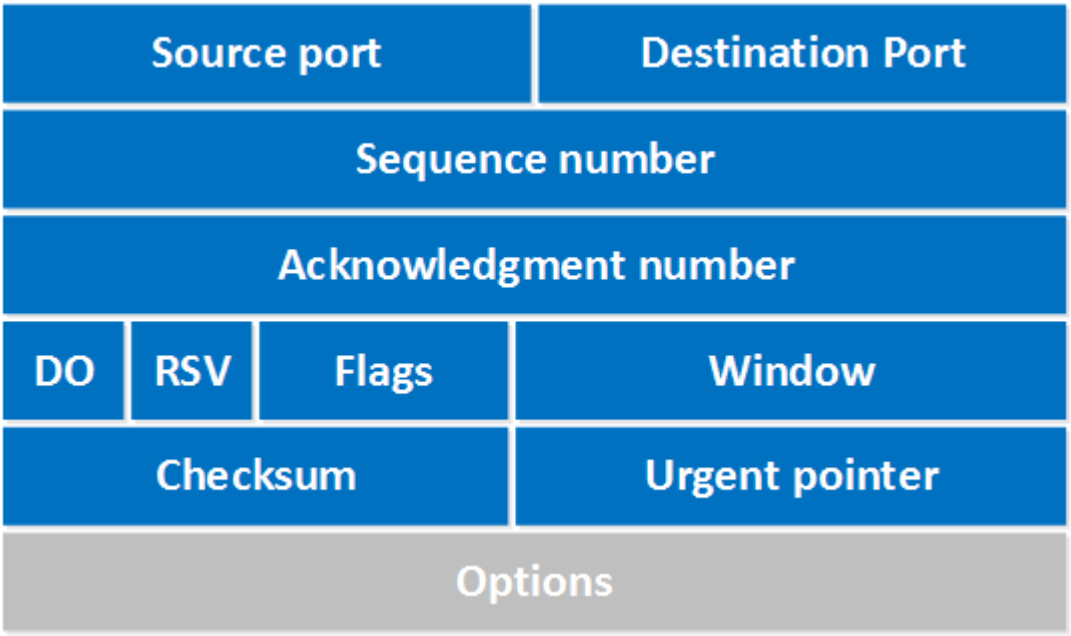
TCP HEADER

TCP (Protocolo de control de transmisión) es un protocolo de transporte confiable, ya que establece una conexión antes de enviar cualquier dato y el receptor reconoce todo lo que envía. En esta lección, veremos más de cerca el encabezado TCP y sus diferentes campos. Esto es lo que parece:



Recorramos todos estos campos:

- **Puerto de origen** : este es un campo de 16 bits que especifica el número de puerto del remitente.
- **Puerto de destino** : este es un campo de 16 bits que especifica el número de puerto del receptor.
- **Número de secuencia** : el número de secuencia es un campo de 32 bits que indica cuántos datos se envían durante la sesión TCP. Cuando establece una nueva conexión TCP (apretón de manos de 3 vías), el número de secuencia inicial es un valor aleatorio de 32 bits. El receptor utilizará este número de secuencia y enviará un acuse de recibo. Los analizadores de protocolos como Wireshark suelen utilizar un *número de secuencia relativo de 0* , ya que es más fácil de leer que un número aleatorio alto.
- **Número de acuse de recibo** : el receptor utiliza este campo de 32 bits para solicitar el siguiente segmento TCP. Este valor será el número de secuencia incrementado en 1.

- **DO** : este es el campo de compensación de datos de 4 bits, también conocido como la longitud del encabezado. Indica la longitud del encabezado TCP para que sepamos dónde comienzan los datos reales.
- **RSV** : son 3 bits para el campo reservado. No se utilizan y siempre se establecen en 0.
- **Banderas** : hay 9 bits para banderas, también los llamamos bits de control. Los usamos para establecer conexiones, enviar datos y terminar conexiones:
    - **URG** : puntero urgente. Cuando se establece este bit, los datos deben tratarse con prioridad sobre otros datos.
    - **ACK** : se utiliza para el acuse de recibo.
    - **PSH** : esta es la función de empuje. Esto le dice a una aplicación que los datos deben transmitirse inmediatamente y que no queremos esperar para llenar todo el segmento TCP.
    - **RST** : esto restablece la conexión, cuando recibe esto, debe finalizar la conexión de inmediato. Esto solo se usa cuando hay errores irrecuperables y no es una forma normal de finalizar la conexión TCP.
    - **SYN** : usamos esto para el protocolo de enlace inicial de tres vías y se usa para establecer el número de secuencia inicial.
    - **FIN** : este bit de finalización se utiliza para finalizar la conexión TCP. TCP es dúplex completo, por lo que ambas partes tendrán que usar el bit FIN para finalizar la conexión. Este es el método normal de cómo finalizamos una conexión.
- **Ventana** : el campo de ventana de 16 bits especifica cuántos bytes está dispuesto a recibir el receptor. Se usa para que el receptor pueda decirle al remitente que le gustaría recibir más datos de los que está recibiendo actualmente. Lo hace especificando el número de bytes más allá del número de secuencia en el campo de reconocimiento.
- **Suma de verificación** : se utilizan 16 bits para una suma de verificación para verificar si el encabezado TCP está bien o no.
- **Puntero urgente** : estos 16 bits se utilizan cuando se ha establecido el bit URG, el puntero urgente se utiliza para indicar dónde terminan los datos urgentes.
- **Opciones** : este campo es opcional y puede tener entre 0 y 320 bits.

UDP: ¿qué es el protocolo UDP?

La comunicación de sistemas en redes domésticas y corporativas locales y en redes públicas como Internet se basa normalmente en la familia de protocolos de Internet. De todos ellos, el más conocido es sin duda el **Protocolo de Internet** (IP), que no solo

es responsable del direccionamiento y la fragmentación de los datagramas, sino que también define cómo se describe la información sobre el origen y el destino. No obstante, la transmisión de los datos se lleva a cabo normalmente mediante el **protocolo de transporte TCP** (Transmission Control Protocol), orientado a la conexión, por lo que las redes se denominan a menudo redes TCP/IP. Debido a que el protocolo TCP, aunque proporciona seguridad, también retrasa la transmisión, David Patrick Reed publicó en 1980 su idea del protocolo de datagramas de usuario (User datagram protocol o UDP) como una alternativa más simple y rápida al protocolo estándar.

¿Qué es UDP (User datagram protocol)?

El protocolo de datagramas de usuario, abreviado como UDP, es un protocolo **que permite la transmisión sin conexión de datagramas** en redes basadas en IP. Para obtener los servicios deseados en los hosts de destino, se basa en los puertos que están listados como uno de los campos principales en la cabecera UDP. Como muchos otros protocolos de red, UDP pertenece a la **familia de protocolos de Internet**, por lo que debe clasificarse en el **nivel de transporte** y, en consecuencia, se encuentra en una capa intermedia entre la capa de red y la capa de aplicación.

Mediante el protocolo de datagramas de usuario, una aplicación puede enviar información muy rápidamente, ya que no es necesario establecer una conexión con el receptor ni esperar una respuesta. Sin embargo, no hay garantía de que los paquetes vayan a llegar **completos** y respetando el **orden** en el que fueron enviados. Además, este protocolo no ofrece ninguna protección frente a la alteración o acceso por parte de terceros. Sin embargo, el UDP puede añadir **opcionalmente una suma de verificación** (que es obligatoria en IPv6) que permite detectar los paquetes defectuosos.

IP HEADER

Un **IP header** es un prefijo de un paquete IP que contiene información sobre la versión de IP, la longitud del paquete, las direcciones IP de origen y destino, etc. Consta de los siguientes campos:

<table>
<tr><td colspan="2">Version (4 bits)</td><td>Header length (4 bits)</td><td>Priority and Type of Service (8 bits)</td><td>Total length (16 bits)</td></tr>
<tr><td colspan="3">Identification (16 bits)</td><td>Flags (3 bits)</td><td>Fragmented offset (13 bits)</td></tr>
<tr><td colspan="2">Time to live (8 bits)</td><td>Protocol (8 bits)</td><td colspan="2">Header checksum (16 bits)</td></tr>
<tr><td colspan="5">Source IP address (32 bits)</td></tr>
<tr><td colspan="5">Destination IP address (32 bits)</td></tr>
<tr><td colspan="5">Options (up to 32 bits)</td></tr>
</table>

Aquí hay una descripción de cada campo:

- **Versión** : la versión del protocolo IP. Para IPv4, este campo tiene un valor de 4.
- **Longitud del encabezado** : la longitud del encabezado en palabras de 32 bits. El valor mínimo es de 20 bytes y el valor máximo es de 60 bytes.

- **Prioridad y tipo de servicio** : especifica cómo se debe manejar el datagrama. Los primeros 3 bits son los bits de prioridad.
- **Longitud total** : la longitud de todo el paquete (encabezado + datos). La longitud mínima es de 20 bytes y la máxima es de 65.535 bytes.
- **Identificación** : se utiliza para diferenciar paquetes fragmentados de diferentes datagramas.
- **Banderas** : se utilizan para controlar o identificar fragmentos.
- **Desplazamiento fragmentado** : se utiliza para la fragmentación y el reensamblaje si el paquete es demasiado grande para colocarlo en un marco.
- **Tiempo de vida** : limita la vida útil de un datagrama. Si el paquete no llega a su destino antes de que expire el TTL, se descarta.
- **Protocolo** : define el protocolo utilizado en la porción de datos del datagrama IP. Por ejemplo, TCP se representa con el número 6 y UDP con el 17.
- **Suma de comprobación del encabezado** : se utiliza para la comprobación de errores del encabezado. Si un paquete llega a un enrutador y el enrutador calcula una suma de verificación diferente a la especificada en este campo, el paquete será descartado.
- **Dirección IP de origen** : la dirección IP del host que envió el paquete.
- **Dirección IP de destino** : la dirección IP del host que debe recibir el paquete.
- **Opciones** : se utiliza para pruebas de red, depuración, seguridad y más. Este campo suele estar vacío.

Ethernet header

El Ethernet header se compone de los siguientes campos, como se ve a continuación:

Preámbulo: este es un patrón de 7 bytes de unos y ceros y se utiliza para la sincronización.

SFD: el "delimitador de marco de inicio" marca el final del preámbulo y le dice al receptor que los siguientes campos serán el marco Ethernet real, comenzando con el campo de destino.

Destino: esta es la dirección MAC de destino del receptor.

Origen: la dirección MAC de origen del dispositivo que envió la trama.

Tipo de éter o longitud:

Para las tramas de Ethernet II, este es el campo EtherType que nos dice qué se transporta dentro de la trama de Ethernet. Un paquete IPv4 , un paquete IPv6 o algo más.

Para tramas IEEE 802.3, este es el campo de longitud que indica la longitud o el tamaño de los datos o la carga útil en bytes.

Para obtener más información, eche un vistazo a los tipos de tramas de Ethernet

Datos: esto lleva los datos reales que estamos tratando de transmitir, por ejemplo, un paquete IPv4.

FCS: la secuencia de verificación de tramas ayuda al receptor a determinar si la trama es correcta o está dañada.

El tamaño total del encabezado es de 22 bytes. Sin embargo, estrictamente hablando, el Preámbulo y el SFD se consideran parte de la encapsulación de la Capa Física. Esto se debe a que estos campos se utilizan principalmente para la sincronización de los marcos recibidos y, en realidad, no contienen ninguna información sobre el marco en sí.

Tenga en cuenta que cuando se trata de la configuración de MTU , el preámbulo y el SFD no se cuentan dentro del tamaño de la trama, por lo que se considera que una trama Ethernet regular tiene un tamaño de encabezado de 14 bytes y un tamaño de carga útil de 1500 para un total de 1514.