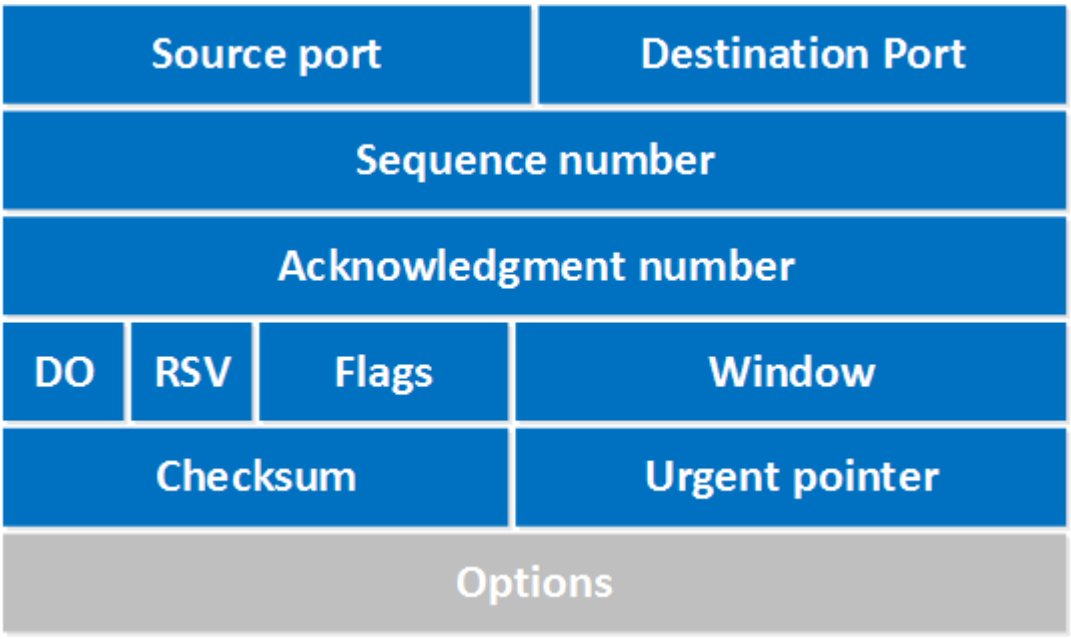
TCP Header

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:

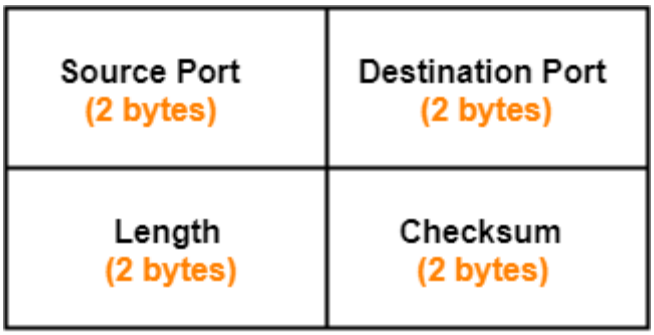
- **Puerto de origen**: este es un campo de 16 bits que especifica el número de puerto del remitente.
- **Puerto de destino**: este es un campo de 16 bits que especifica el número de puerto del receptor.
- **Número de secuencia**: el número de secuencia es un campo de 32 bits que indica cuántos datos 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 Header

Encabezado UDP-

El siguiente diagrama representa el formato de encabezado UDP:



UDP Header

1. Puerto de origen-

- El puerto de origen es un campo de 16 bits.
- Identifica el puerto de la aplicación emisora.

2. Puerto de destino-

- Puerto de destino es un campo de 16 bits.
- Identifica el puerto de la aplicación receptora.

3. Longitud-

- La longitud es un campo de 16 bits.
- Identifica la longitud combinada del encabezado UDP y los datos encapsulados.

Longitud = Longitud del encabezado UDP + Longitud de los datos encapsulados

4. Suma de verificación-

- **La suma de comprobación** es un campo de 16 bits que se utiliza para el control de errores.
- Se calcula sobre el encabezado UDP, los datos encapsulados y el pseudo encabezado IP.
- El cálculo de la suma de comprobación no es obligatorio en UDP.

Aplicaciones que utilizan UDP-

Las siguientes aplicaciones usan UDP-

- Las aplicaciones que requieren una respuesta para una solicitud utilizan UDP. Ejemplo **: DNS** .
- Los protocolos de enrutamiento como RIP y OSPF usan UDP porque tienen una cantidad muy pequeña de datos para transmitir.
- **El protocolo** trivial de transferencia de archivos (TFTP) utiliza UDP para enviar archivos de tamaño muy pequeño.
- Las aplicaciones de transmisión y multidifusión utilizan UDP.
- Las aplicaciones de transmisión como multimedia, videoconferencias, etc. usan UDP ya que requieren velocidad sobre confiabilidad.
- Las aplicaciones en tiempo real, como el chat y los juegos en línea, usan UDP.
- Los protocolos de gestión como SNMP (Protocolo simple de gestión de red) utilizan UDP.
- Bootp/DHCP usa UDP.
- Otros protocolos que utilizan UDP son: Kerberos, Network Time Protocol (NTP), Network News Protocol (NNP), Quote of the day protocol, etc.

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:

Version (4 bits)	Header length (4 bits)	Priority and Type of Service (8 bits)	Total length (16 bits)
Identification (16 bits)		Flags (3 bits)	Fragmented offset (13 bits)
Time to live (8 bits)	Protocol (8 bits)	Header checksum (16 bits)	
Source IP address (32 bits)			
Destination IP address (32 bits)			
Options (up to 32 bits)			

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.