Cabecera IPv4



**Versión:** lleva el registro de la versión del protocolo al que pertenece el datagrama.

**IHL:** Indica la longitud en palabras de 32 bits.

**Tipo de servicio:** permite al host indicar a la subred el tipo de servicio que quiere.

**Longitud total**: Incluye todo el datagrama: tanto la cabecera como los datos. La longitud máxima es de 65535 bytes.

**Identificación**: Es necesario para que el host destino determine a qué datagrama pertenece un fragmento recién llegado.

**DF:** No fragmentar.

**MF:** Mas fragmentos.

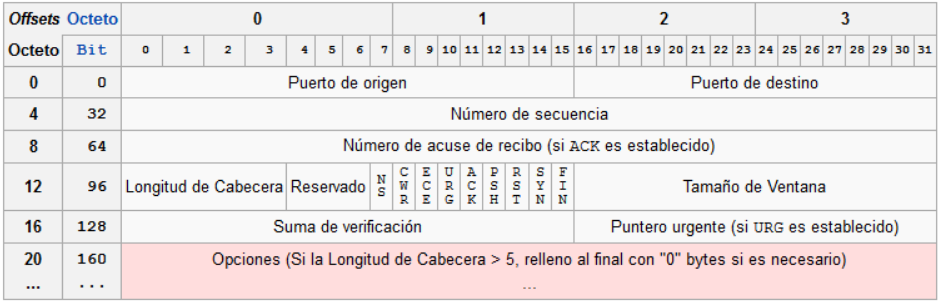
**Desplazamiento del fragmento:** Indica en qué parte del datagrama actual va este fragmento.

**Tiempo de vida/TTL:** es un contador que sirve para limitar la vida del paquete.

**Protocolo:** indica la capa de transporte a la que debe entregarse (TCP o UDP o algún otro).

**Suma de la cabecera:** Verifica solo a la cabecera.

Cabecera TCP



**Puerto origen:** Identifica el puerto emisor.

**Puerto destino:** Identifica el puerto receptor.

**Numero de secuencia:**  Identifica el byte del flujo de datos enviado por el emisor TCP al receptor TCP que representa el primer byte de datos del segmento.

**Numero de acuse de recibo:** Contiene el valor del siguiente número de secuencia que el emisor del segmento espera recibir.

**Longitud de cabecera:** Especifica el tamaño de la cabecera en palabras de 32 bits.

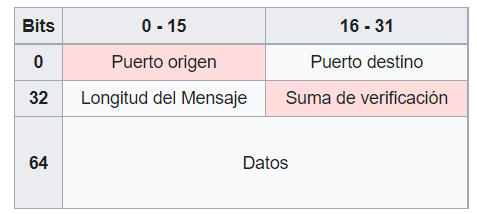
**Reservado:** Para uso futuro. Debe estar a 0.

**Tamaño de ventana:** Tamaño de la ventana de recepción que especifica el número máximo de bytes que pueden ser metidos en el buffer de recepción o dicho de otro modo, el número máximo de bytes pendientes de asentimiento.

**Suma de verificación:** utilizado para la comprobación de errores tanto en la cabecera como en los datos.

**Puntero urgente:** Cantidad de bytes desde el número de secuencia que indica el lugar donde acaban los datos urgentes.

Cabecera UDP



Puertos:

**http:** TCP 80

**ftp:** TCP 20/21

**dns:** UDP 53

Comandos Whiresark

dns.qry.name==”elmundo.com” 🡪 saber la IP del server DNS que responde

ip.src==192.168.1.140 🡪 IP origen

ip.dst==192.168.1.140 🡪 IP destino

tcp.flags.syn==1 && ack==0 🡪 FLAGS

http.response.code

GET consigue las cosas en HTTP y dentro esta la información del cliente

En User-Agent esta el sistema operativo del cliente

En HTTP código 200 esta dentro el sistema operativo del servidor (HTP “apache”)