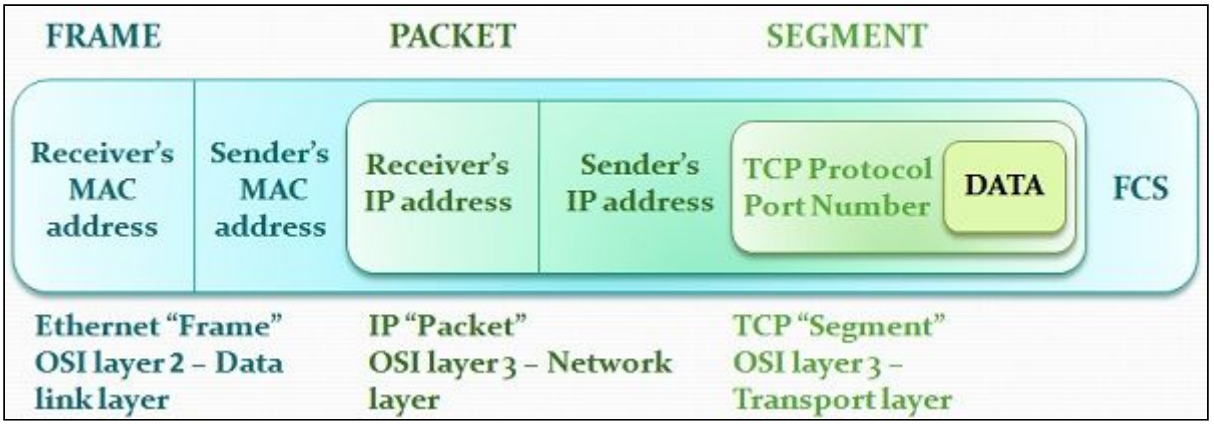


Paquete:

```
Frame 16322: 721 bytes on wire (5768 bits), 721 bytes captured (5768 bits) on interface 0
Ethernet II, Src: HewlettP_ba:26:b2 (50:65:f3:ba:26:b2), Dst: PaloAlto_00:02:33 (00:1b:17:00:02:33)
Internet Protocol Version 4, Src: 10.219.1.236 (10.219.1.236), Dst: fixedbyvonnie.com (198.57.208.223)
Transmission Control Protocol, Src Port: 41532 (41532), Dst Port: http (80), Seq: 1, Ack: 1, Len: 655
```

Según esta información se capturaron todos los bytes (721 de 721) del frame, posteriormente se muestra cada una de las capas las cuales serán explicadas con profundidad más adelante. El apartado *Ethernet II* corresponde a la capa de Enlace, el apartado *Internet protocol version 4* corresponde a la capa de Internet y el apartado *Transmission Control Protocol* corresponde a la capa de transporte.

Análisis de PDUs:
Información general del paquete:

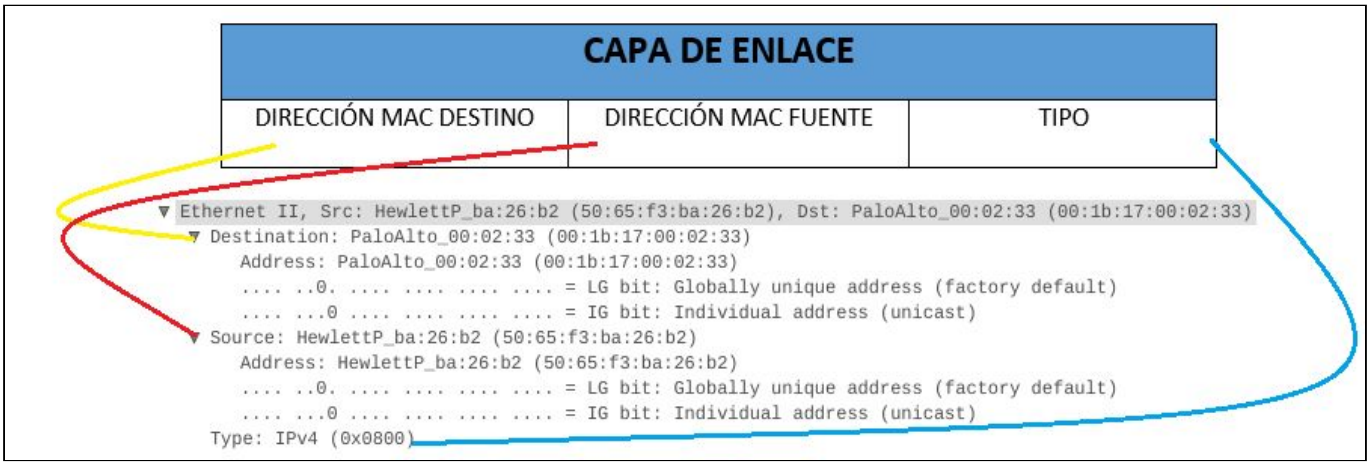
```
▼ Frame 16322: 721 bytes on wire (5768 bits), 721 bytes captured (5768 bits) on interface 0
  ▼ Interface id: 0 (eno1)
      Interface name: eno1
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 19, 2018 10:23:45.997319960 -05
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1539962625.997319960 seconds
    [Time delta from previous captured frame: 0.000230910 seconds]
    [Time delta from previous displayed frame: 35.171569379 seconds]
    [Time since reference or first frame: 190.904314836 seconds]
    Frame Number: 16322
    Frame Length: 721 bytes (5768 bits)
    Capture Length: 721 bytes (5768 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
```

Aquí podemos ver la información básica del frame como el nombre de la interface (eno1) con la cual se está capturando el *frame*, también se puede ver la fecha y hora en que fue capturado y su tamaño (721 bytes) entre otra información general.

Capa de Enlace:

```
▼ Ethernet II, Src: HewlettP_ba:26:b2 (50:65:f3:ba:26:b2), Dst: PaloAlto_00:02:33 (00:1b:17:00:02:33)
  ▼ Destination: PaloAlto_00:02:33 (00:1b:17:00:02:33)
      Address: PaloAlto_00:02:33 (00:1b:17:00:02:33)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▼ Source: HewlettP_ba:26:b2 (50:65:f3:ba:26:b2)
      Address: HewlettP_ba:26:b2 (50:65:f3:ba:26:b2)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

La capa de enlace es responsable de la transferencia fiable de información a través de un circuito de transmisión de datos. Recibe peticiones de la capa de red y utiliza los servicios de la capa física.

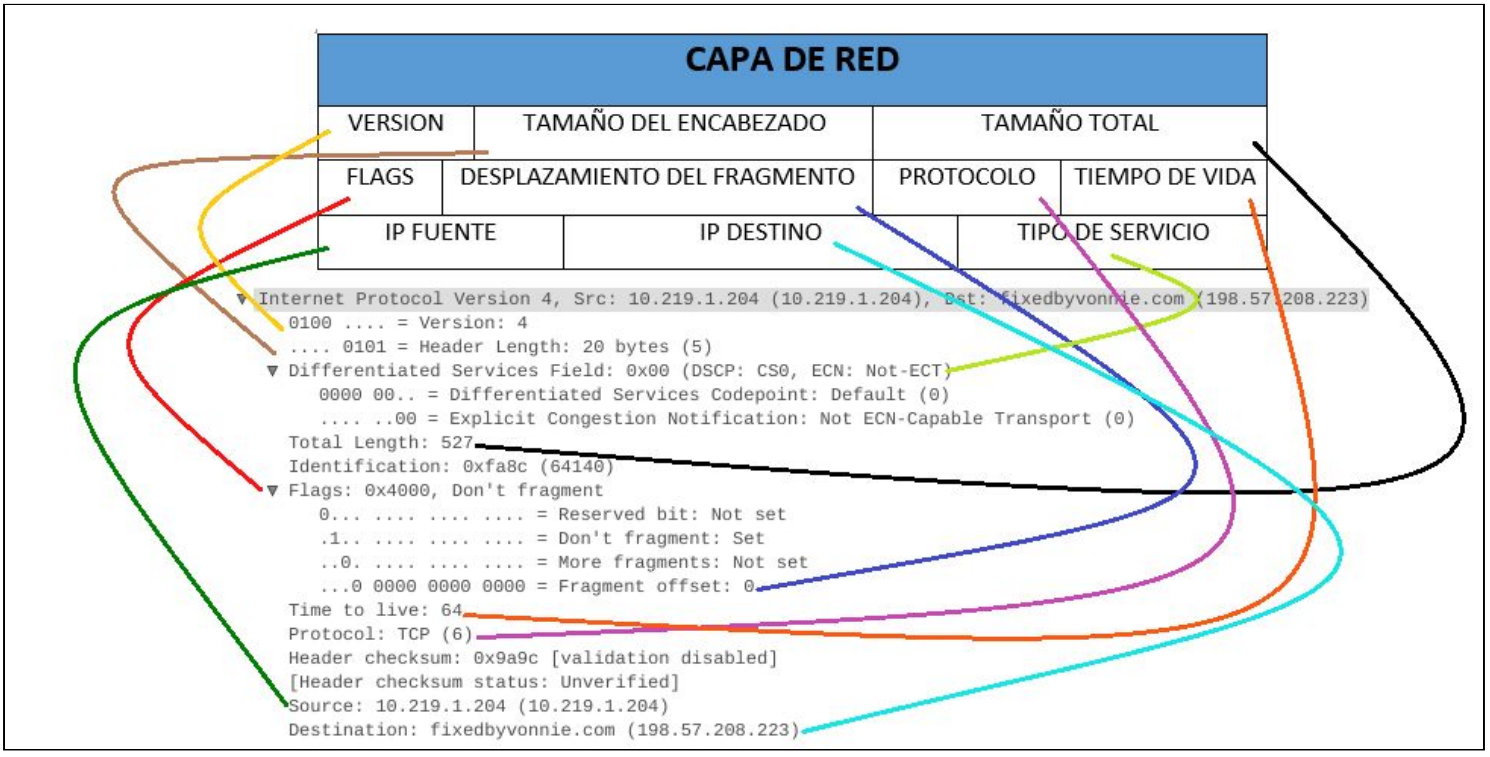


En la capa de nivel de enlace, tenemos ethernet, la dirección MAC fuente la cual corresponde a nuestro equipo de trabajo es (***50:65:f3:ba:26:b2***) , y la dirección de destino es otra dirección MAC (***00:1b:17:00:02:33***) a la cual va a llegar la trama.

Capa de Internet:

```
▼ Internet Protocol Version 4, Src: 10.219.1.204 (10.219.1.204), Dst: fixedbyvonnie.com (198.57.208.223)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 527
    Identification: 0xfa8c (64140)
  ▼ Flags: 0x4000, Don't fragment
      0... .... .... .... = Reserved bit: Not set
      .1.. .... .... .... = Don't fragment: Set
      ..0. .... .... .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x9a9c [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.219.1.204 (10.219.1.204)
    Destination: fixedbyvonnie.com (198.57.208.223)
```

Esta capa proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas.

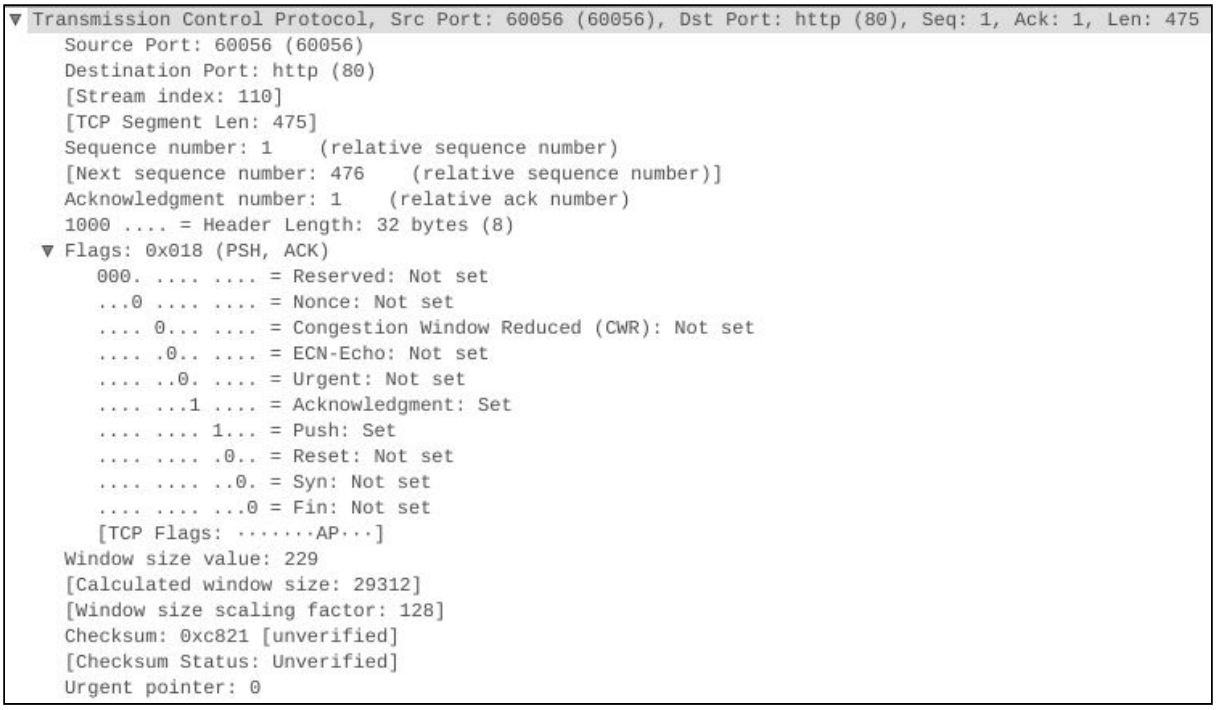


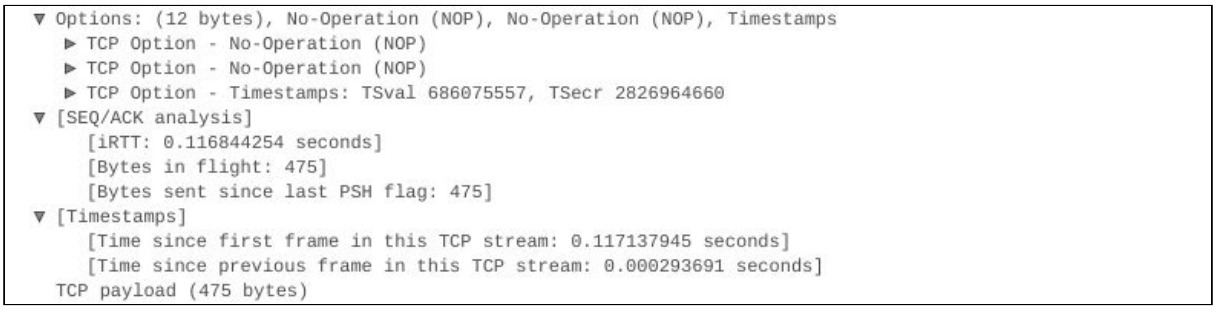
Aquí podemos ver la dirección IP fuente (**10.219.1.204**) la cual corresponde a la dirección IP de la máquina con que capturamos el tráfico y también la dirección IP destino (**198.57.208.223**) a la cual va a llegar el paquete.

Otra información que tenemos en este PDU:

- **Version :** IPv4
- **Tamaño del encabezado :** Número de palabras de 32 bits que forman el encabezado.
- **Tamaño total :** Tamaño total del paquete capturado en bytes.
- **Identificación :** Número de 16 bits que, junto con la dirección de origen, identifica de forma única este paquete, utilizado durante el reensamblado de paquetes fragmentados.
- **Flags :** Una secuencia de tres banderas (uno de los 4 bits no se utiliza) que se utiliza para controlar si los routers pueden fragmentar un paquete.
- **Desplazamiento de la fragmentación :** Un conteo de bytes que comienza desde el paquete enviado originalmente, puesto por cualquier router que pueda realizar fragmentación.
- **Tiempo de vida :** Número de saltos o enlaces por los que se puede enrutar un paquete, disminuido por la mayoría de los routers, utilizado para evitar loops de enrutamiento accidentales.
- **Protocolo :** Punto de acceso al servicio el cual indica el tipo de paquete de transporte que se transporta (por ejemplo, 1 = ICMP; 2 = IGMP; 6 = TCP; 17 = UDP).
- **Encabezado del checksum :** Se utiliza para detectar errores de procesamiento introducidos en el paquete dentro de un enrutador o puente donde el paquete no está protegido por una verificación de redundancia cíclica de la capa de enlace. Los paquetes con un checksum inválido son descartados por todos los nodos en una red IP.

Capa de Transporte:



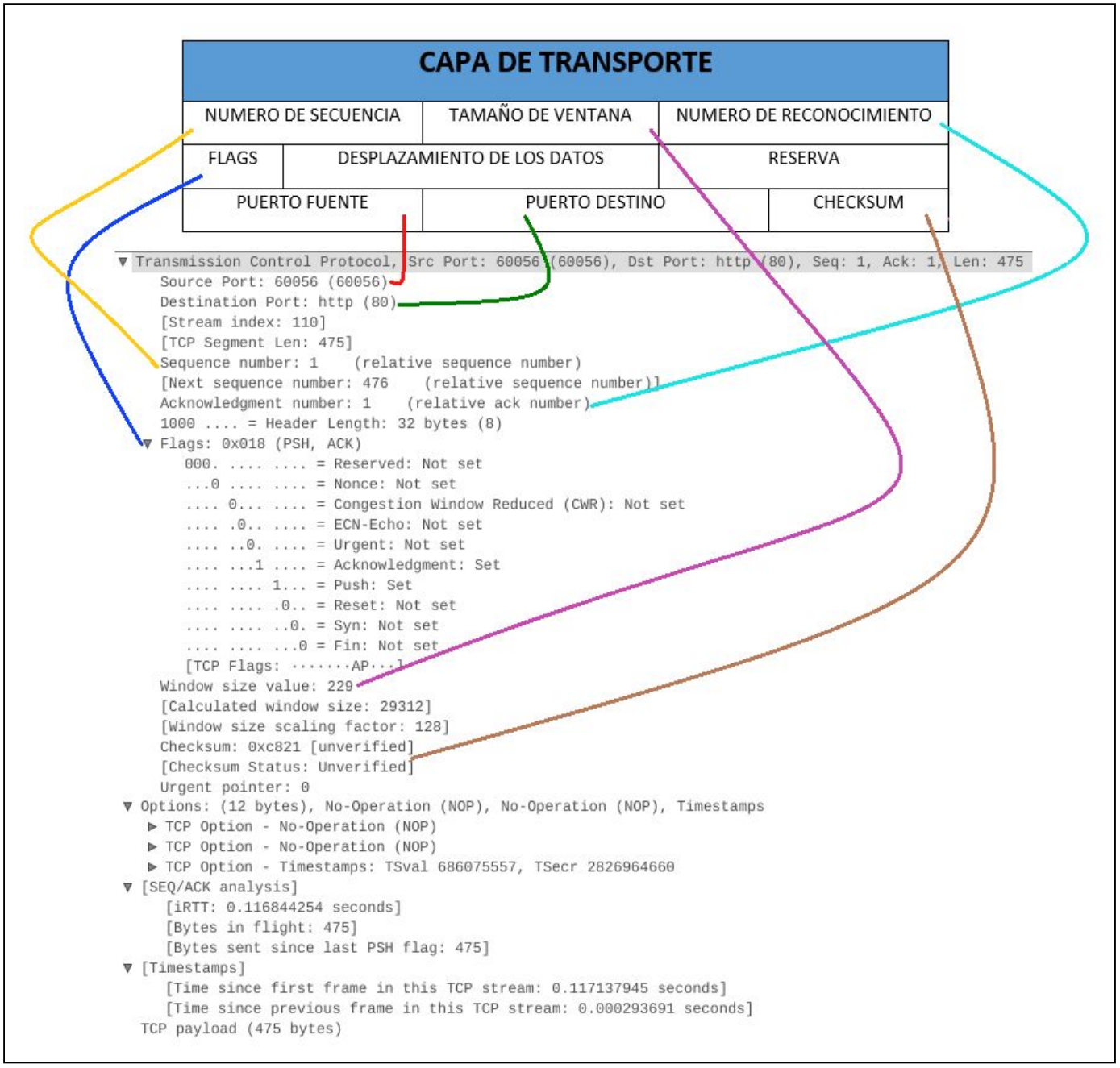


La capa de transporte se encarga de la transferencia libre de errores de los datos entre el emisor y el receptor, aunque no estén directamente conectados, así como de mantener el flujo de la red. Es la base de toda la jerarquía de protocolo.

En esta capa ya se trabaja es con puertos (de 16 bits), y como en las capas anteriores tenemos una fuente y un destino, en este caso el puerto fuente es el (**41532**) y el puerto destino es el http (**80**).

Otra información que tenemos en este PDU:

- **Número de secuencia :** Número de 32 bits y su comportamiento varía en función de la bandera SYN.
- **Número de reconocimiento :** Número de 32 bits y su comportamiento varía en función de la bandera ACK.
- **Desplazamiento de los datos :** (4 bits) Especifica el tamaño del encabezado TCP en palabras de 32 bits. El encabezado de tamaño mínimo es de 5 palabras y el

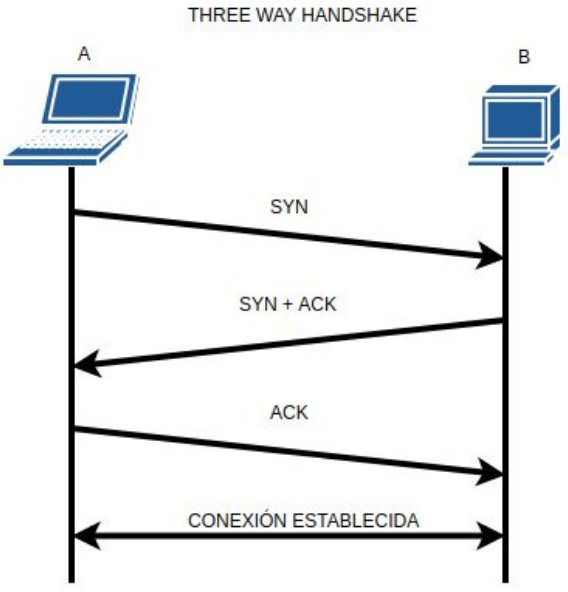


máximo de 15 palabras, lo que da un tamaño mínimo de 20 bytes y un máximo de 60 bytes, permitiendo hasta 40 bytes de opciones en el encabezado. Este campo recibe su nombre del hecho de que también es el desplazamiento desde el inicio del segmento TCP a los datos reales.

- **Reservado :** (3 bits) Se tienen para un uso futuro y sus valores deben estar puestos en cero.
- **Flags :** (9 bits) contiene 9 banderas, cada una de un bit.
    - **NS :** Protección de ocultación.
    - **CWR :** Reducción de la ventana de congestión (Congestion Window Reduced). El host emisor establece la bandera para indicar que recibió un

segmento TCP con la bandera ECE establecida y ha respondido con un mecanismo de control de congestión.
    - **ECE :** Indica eco.
    - **URG :** Indica que el campo del puntero urgente es significativo.
    - **ACK :** Indica que el campo de reconocimiento o *acknowledgment* es significativo. Todos los paquetes después del SYN del paquete inicial enviado por el cliente deben tener este indicador establecido.
    - **PSH :** *Push Function* o función de empuje. Pide enviar los datos almacenados a la aplicación receptora.
    - **RST :** Reinicia la conexión.
    - **SYN :** Sincroniza los números de secuencia. Solo el primer paquete enviado desde cada extremo debe tener este indicador establecido. Algunas otras banderas cambian de significado en función de esta bandera, y algunas solo son válidas para cuando se establece, y otras cuando está clara.
    - **FIN :** No hay más datos del emisor.
- **Tamaño de ventana :** (16 bits) Es el tamaño de la ventana de recepción, especifica el número de bytes que el remitente de este segmento está actualmente dispuesto a recibir.
- **Checksum :** Campo de 16 bits usado para verificar errores del encabezado y los datos.
- **Opciones :** La longitud de este campo es determinada por el desplazamiento de los datos.

En esta capa para establecer la conexión se usa procedimiento conocido como *3-way handshake* el cual consiste en enviar una señal de sincronización (SYN) desde un cliente a un servidor, este responde con un reconocimiento de la sincronización (SYN-ACK) y finalmente el cliente reenvia el reconocimiento de lo recibido y se puede establecer la conexión.



Referencias :

- http://networkstatic.net/what-are-ethernet-ip-and-tcp-headers-in-wireshark-captures/
- http://www.fixedbyvonnie.com/2015/05/wireshark-101-getting-around-step-by-step/
- https://seguridadyredes.wordpress.com/2008/02/14/analisis-de-red-con-wireshark-interpretando-los-datos/
- https://es.wikipedia.org/wiki/Protocolo_de_control_de_transmisi%C3%B3n
- https://www.inetdaemon.com/tutorials/internet/tcp/3-way_handshake.shtml
- https://es.wikipedia.org/wiki/Familia_de_protocolos_de_internet