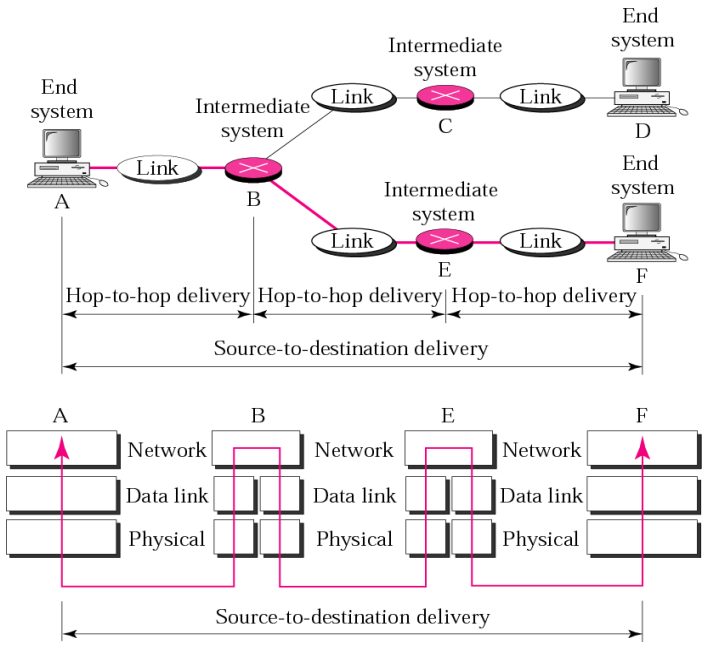
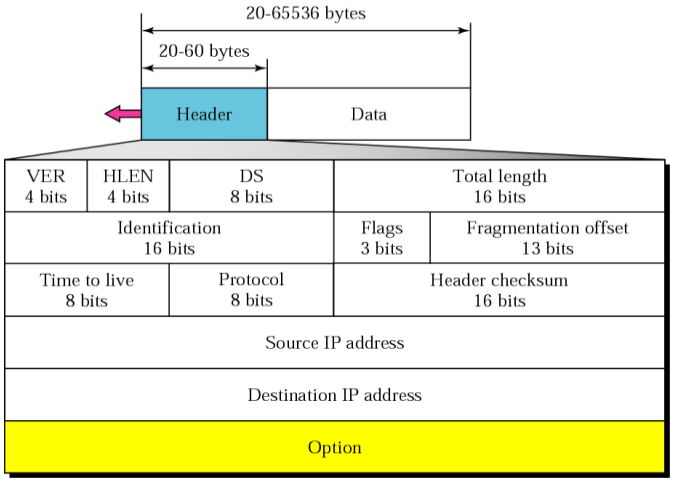
CAPITULO 14. NIVEL DE RED: PROTOCOLO DE INTERNET (IP)

- En el modelo de Internet, el principal protocolo de red es el protocolo de Internet (IP).
- INTERCONEXIÓN ENTRE REDES:
    - Los niveles físico y de enlace de datos de una red funcionan localmente, es decir, se responsabilizan de la entrega de datos en la red de un nodo al siguiente.
    - Pero, ¿qué ocurre si la entrega es a través de varios enlaces?.
    - Necesidad de nivel de red:
        - También llamado nivel de interconexión de redes.
        - Es el responsable de:
            - La entrega host a host y del encaminamiento de los paquetes a través de los encaminadores o conmutadores.
            - Crear un paquete a partir de de los datos que vienen de otro protocolo (transporte, encaminamiento, etc.), conteniendo en la cabecera del paquete las direcciones lógicas del origen y del destino.
            - Comprobar su tabla de encaminamiento para encontrar la información de encaminamiento.
            - Fragmentar, si el paquete es demasiado grande.
            - Asegurar en el destino, que la dirección del paquete corresponde con la dirección de red del host.
            - Esperar todos los fragmentos, en caso de que el paquete fuese un fragmento, reensamblado y entregando el paquete completo al nivel de transporte.

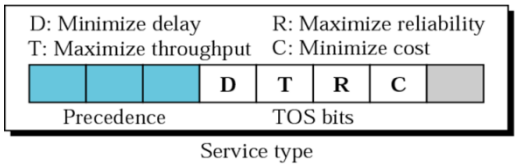


    - Internet como una red de datagramas:
        - La conmutación en el nivel de red en Internet utiliza datagramas para la conmutación de paquetes.
        - Se utiliza una dirección universal definida en el nivel de red para encaminar los paquetes del origen al destino.
    - Internet como red no orientada a conexión:
        - El protocolo de nivel de red, trata cada paquete de forma independiente y los paquetes no tienen relación entre ellos.
        - Los paquetes de un mensaje pueden viajar o no por el mismo camino.

- IPv4:
  - La versión 4 del protocolo de Internet es un mecanismo de entrega utilizado en los protocolo TCP/IP.
  - Es un protocolo de datagramas no orientado a conexión y no fiable (sin control de errores, ni control de flujo).
  - Si la fiabilidad es importante, IPv4 debe emparejarse con un protocolo de nivel superior, mas fiable como TCP.
  - Datagrama:
    - Los paquetes en IPv4 se llaman datagramas.
    - Un datagrama es un paquete de longitud variable que consta de dos partes:
      - Cabecera (Header):
        - Tiene una longitud de 20 a 60 bytes.
        - Contiene información esencial para el encaminamiento y la entrega.
      - Datos (Data):



    - Versión (VER):
      - Longitud: 4 bits.
      - Define: Versión del protocolo IPv4.
    - Longitud de cabecera (HLEN):
      - Longitud: 4 bits.
      - Define: La longitud total de la cabecera del datagrama en palabras de 4 bytes.
    - Servicios (DS):
      - Longitud: 8 bits.
      - Define:
        - Campo anteriormente denominado Tipo de servicio, se conoce ahora como servicios diferenciados.
        - Tipo de servicio:



Service type

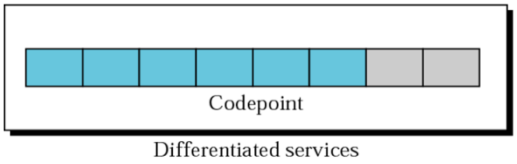
      - Precedencia:
        - Longitud: 3 bits.
        - Definición: La prioridad del datagrama en situaciones tales como la congestión, descartando aquellos de menor precedencia.
        - Este subcampo fue parte de la versión 4 pero nunca se utilizó.

- Bits TOS:
  - Longitud: 4 bits.
  - Define:
    - Los programas de aplicación pueden solicitar un tipo específico de servicio.
    - Patrón:

Bit TOS	Descripción
0000	Normal (Default)
0001	Minimizar coste
0010	Maximizar fiabilidad
0100	Maximizar productividad
1000	Minimizar retardo

    - Uno y solo uno de los cuatro bits puede tener el valor a uno en cada datagrama.

- Servicios diferenciados:

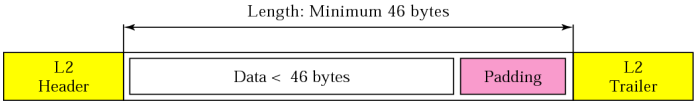


Differentiated services

- El subcampo de 6 bits denominado codepoint se puede utilizar de dos formas:
  - Cuando los 3 bits de la derecha son 0, los 3 bits de la izquierda se interpretan de igual forma que los bits de precedencia en la interpretación de tipo de servicio.
  - Cuando los 3 bits de la derecha no son todos 0, los 6 bits definen 64 servicios basados en la asignación de prioridad de:

Categoría	Codepoint	Autoridad que asigna	Nº. de servicios
1	XXXXXX0	Internet	32
2	XXXX11	Local	16
3	XXXX01	Temporal o experimental	16

- Longitud total:
  - Longitud: 16 bits.
  - Define:
    - La longitud total del datagrama incluyendo la cabecera.
    - Este campo se hace necesario en los casos en los que se añade empaquetamiento o padding cuando el datagrama es menor de 46 bytes.



- Identificación: Utilizado en la fragmentación.
- Indicadores: Utilizado en la fragmentación.
- Desplazamiento del fragmento: Utilizado en la fragmentación.

- Tiempo de vida:
  - Utilizado fundamentalmente para controlar el número máximo de saltos (encaminadores) visitados por el datagrama.
  - Este valor es aproximadamente el doble del número máximo de encaminadores entre cualquier par de host.
  - Cada encaminador que procesa el datagrama resta a este número 1, descartando el datagrama si se hace 0.
- Protocolo:
  - Longitud: 8 bits.
  - Define: El protocolo de nivel superior que utiliza los servicios del nivel IPv4.

Value	*Protocol*
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF

- Suma de comprobación (CheckSum): Véase más adelante.
- Dirección origen:
  - Longitud: 32 bits.
  - Define:
    - La dirección IPv4 de un origen.
    - Este campo ha de permanecer sin cambio durante todo el tiempo en el que viaje el datagrama.
- Dirección destino:
  - Longitud: 32 bits.
  - Define:
    - La dirección IPv4 de un destino.
    - Este campo ha de permanecer sin cambio durante todo el tiempo en el que viaje el datagrama.

o Fragmentación:
- El formato y el tamaño de la trama recibida por un encaminador dependen del protocolo utilizado por el nivel físico por el cual llega la trama.
- El formato y el tamaño de la trama enviada por un encaminador dependen del protocolo utilizado por el nivel físico por el cual se envía la trama.
- Unidad de transferencia máxima (MTU):
  - Cada protocolo de nivel de enlace de datos tiene su propio formato de trama en la mayoría de los protocolos.
  - Uno de los campos definidos en el formato es el tamaño máximo del campo de datos.
  - El valor de la MTU depende del protocolo de red físico.

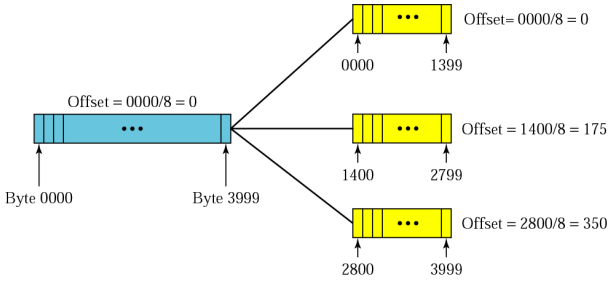
Protocol	*MTU*
Hyperchannel	65,535
Token Ring (16 Mbps)	17,914
Token Ring (4 Mbps)	4,464
FDDI	4,352
Ethernet	1,500
X.25	576
PPP	296

  - Para que el protocolo IPv4 sea independiente de la red física, la longitud máxima de un datagrama IPv4 es de 65535 bytes.

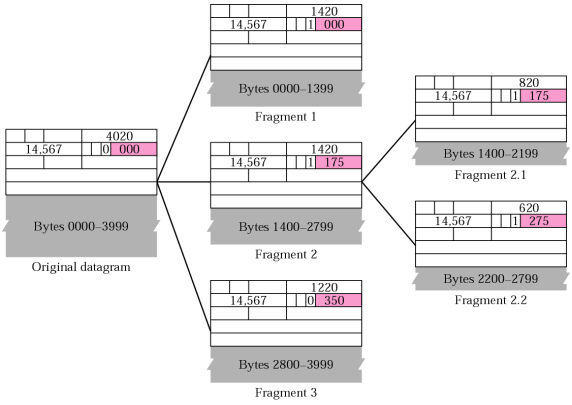
- Al proceso de dividir el datagrama IPv4 para acomodarlo a redes físicas con MTU menor que la longitud del datagrama Ipv4 se le llama fragmentación.
- El datagrama pude ser fragmentado por el host origen o por cualquier encaminador encontrado en el camino, pudiendo fragmentarse varias veces antes de alcanzar el destino.
- El reensamblado del datagrama se hace en el host destino.
- Cuando se fragmenta un datagrama, las partes necesarias de la cabecera deben ser copiadas en todos los fragmentos.
- Campos relacionados con la fragmentación:
    - Identificación:
        - Longitud: 16 bits.
        - Identifica un datagrama que procede de un host origen.
        - La combinación de la identificación y de la dirección origen IPv4 deben definir de forma única un datagrama cuando deja el host origen.
        - Para garantizar esta unicidad Ipv4 utiliza un contador inicializado con un valor positivo, copiando el valor en el campo identificación en todos los fragmentos y aumentándolo en una unidad en cada nuevo datagrama.
    - Indicadores:

D: Do not fragment
M: More fragments

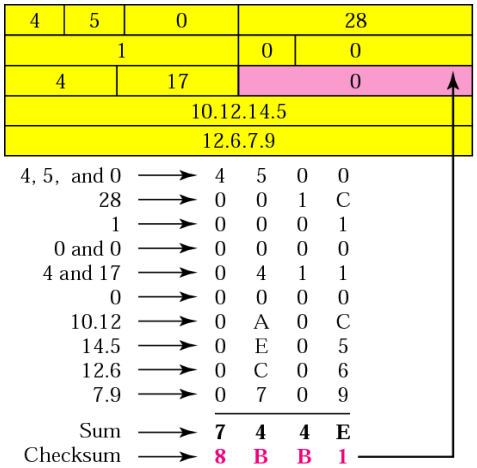
        - Longitud: 3 bits.
        - El primer bit está reservado.
        - El segundo bit se denomina bit de no fragmentación:
            - Si su valor es 0, la máquina puede fragmentar el datagrama.
            - Si su valor es 1, la máquina no debe fragmentar el datagrama. Si no puede pasar el datagrama a través de la red física disponible, lo descarta y envía un mensaje de error ICMP al host origen.
        - El tercer bit se denomina bit de más fragmentos:
            - Si su valor es 0, significa que este es el último fragmento o que solo hay un fragmento.
            - Si su valor es 1, significa que hay más fragmentos detrás de él.
    - Desplazamiento de fragmento:
        - Longitud: 13 bits.
        - Muestra la posición relativa del fragmento respecto al datagrama completo.
        - Es el desplazamiento de los datos en el datagrama original medido en unidades de 8 bytes.



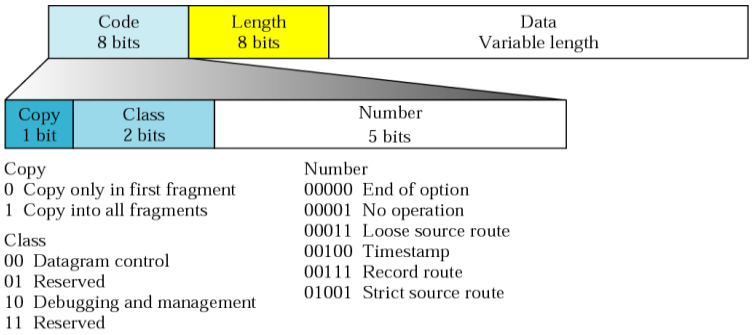
- Estrategia de reensamblado:
  - El primer fragmento tiene un campo de desplazamiento de cero.
  - El segundo fragmento tiene un desplazamiento igual a la longitud del primer fragmento dividido por 8.
  - El tercer fragmento tiene un desplazamiento igual a la longitud total del primer y segundo fragmento dividido por 8.
  - Se continúa el proceso. El último fragmento tiene el bit que indica más fragmentos a 0.



- Suma de comprobación:
  - Control de errores que cubre solamente la cabecera del paquete IPv4.
  - Pasos:
    - La suma de comprobación se pone a cero.
    - Se divide la cabecera en secciones de 16 bits y se suman todas ellas.
    - Se trunca a 16 bits la suma obtenida y se complementa el resultado.



- Opciones:
  - Este campo corresponde con la parte variable de la cabecera de un datagrama IPv4.
  - Pueden ocupar un máximo de 40 bytes.
  - No son ni obligatorias ni requeridas para un datagrama.
  - Se puede utilizar para probar y depurar la red.



- Descripción breve de las opciones:
  - No operación: Utilizada como elemento de relleno entre opciones.
  - Fin de opción: Utilizada como relleno al final del campo de opciones.
  - Registrar ruta:
    - Registra los encaminadores de Internet que tratan el datagrama.
    - Puede listar hasta 9 direcciones.
  - Camino estricto desde el origen:
    - El origen determina estrictamente el camino por el cual debe viajar el datagrama a través de Internet.
    - Si el datagrama no cumple con el viaje planificado se descarta, enviando un mensaje de error.
  - Camino relajado desde el origen:
    - Cada encaminador de la lista debe ser visitado, pero el datagrama puede visitar además otros caminos.
  - Marca de tiempo:
    - Registra la hora de procesamiento en un encaminador.
    - Se expresa en milisegundos desde la medianoche utilizando el tiempo Universal o de Greenwich.

- Un ejemplo de datagrama IPv4 real:

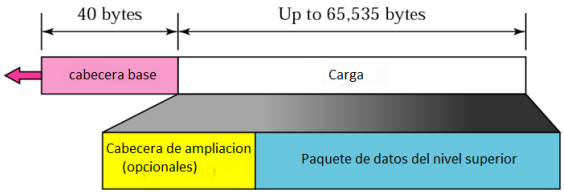
DATAGRAMA (marcado de azul)

```
00 1d e0 c6 11 f9 00 30  da 71 1f 2a 08 00 45 00
01 fa 27 3e 00 00 35 06  e4 38 d1 55 e5 68 c0 a8
01 21 00 50 e9 b4 89 3d  3a 9e 83 84 5b f6 50 18
```

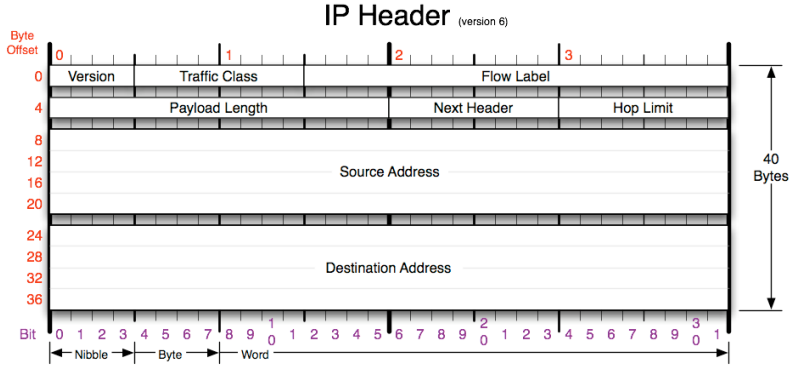
ANÁLISIS

```
Internet Protocol, Src: 209.85.229.104 (209.85.229.104), Dst: 192.168.1.33 (192.168.1.33)
  Version: 4
  Header length: 20 bytes
⊟ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..0. = ECN-Capable Transport (ECT): 0
    .... ...0 = ECN-CE: 0
  Total Length: 506
  Identification: 0x273e (10046)
⊟ Flags: 0x00
    0.. = Reserved bit: Not Set
    .0. = Don't fragment: Not Set
    ..0 = More fragments: Not Set
  Fragment offset: 0
  Time to live: 53
  Protocol: TCP (0x06)
⊟ Header checksum: 0xe438 [correct]
    [Good: True]
    [Bad : False]
  Source: 209.85.229.104 (209.85.229.104)
  Destination: 192.168.1.33 (192.168.1.33)
```

- IPv6:
  - Soluciona alguna de las carencias de IPv4:
    - Aumento del direccionamiento en Internet.
    - Transmisión de audio / video en tiempo real.
    - Permite autenticación y cifrado.
  - También conocido como IPng (Internet Protocol next generation).
  - Ventajas:
    - Espacio de direcciones mayor: Una dirección en IPv6 tiene 128 bits.
    - Mejor formato de cabecera:
      - Las opciones de separan de la cabecera base y se insertan, cuando se necesitan, entre la cabecera base y los datos del nivel superior.
    - Nuevas opciones:
    - Capacidad de ampliación: Escalable.
    - Soporte para la reserva de recursos:
      - Incluye un mecanismo (campo de etiqueta de flujo) que permite al origen solicitar un tratamiento especial para el paquete.
    - Soporte para seguridad: Cifrado y autenticación.
  - Formato del paquete:



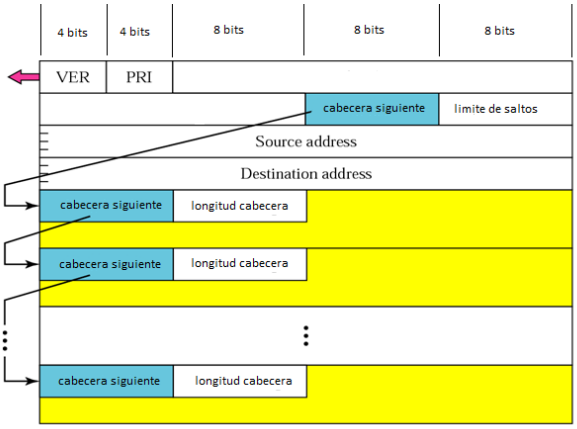
    - Compuesto por una cabecera base (de 40 bytes) obligatoria seguido por una carga.
    - La carga (hasta 6553 bytes) consta de :
      - Cabeceras de extensión opcionales.
      - Datos del nivel superior.
    - Cabecera base:



      - Versión:
        - Longitud: 4 bits.
        - Define: El número de versión.
      - Prioridad:
        - Longitud: 4 bits.
        - Define: La prioridad del paquete respecto a la congestión del tráfico.
      - Etiqueta de flujo:
        - Longitud: 24 bits.
        - Define: Un tratamiento especial para un flujo de datos particular.
      - Longitud de la carga:
        - Longitud: 16 bits.

- Define: La longitud la longitud del datagrama IP excluyendo la cabecera base.

- Cabecera siguiente:
  - Longitud: 8 bits.
  - Define:
    - La cabecera que sigue a la cabecera base en el datagrama pudiendo ser:
      - Una de las cabeceras de extensión opcionales.
      - Un paquete encapsulado de UDP o TCP.
    - Cada cabecera de extensión también contiene este campo



    - Códigos para la cabecera siguiente en IPv4:

Código	Cabecera siguiente
0	Opción salto a salto
2	ICMP
6	TCP
17	UDP
43	Encaminamiento desde el origen
44	Fragmentación
50	Carga cifrada
51	Autenticación
59	Nulo (No hay siguiente cabecera)
60	Opción destino.

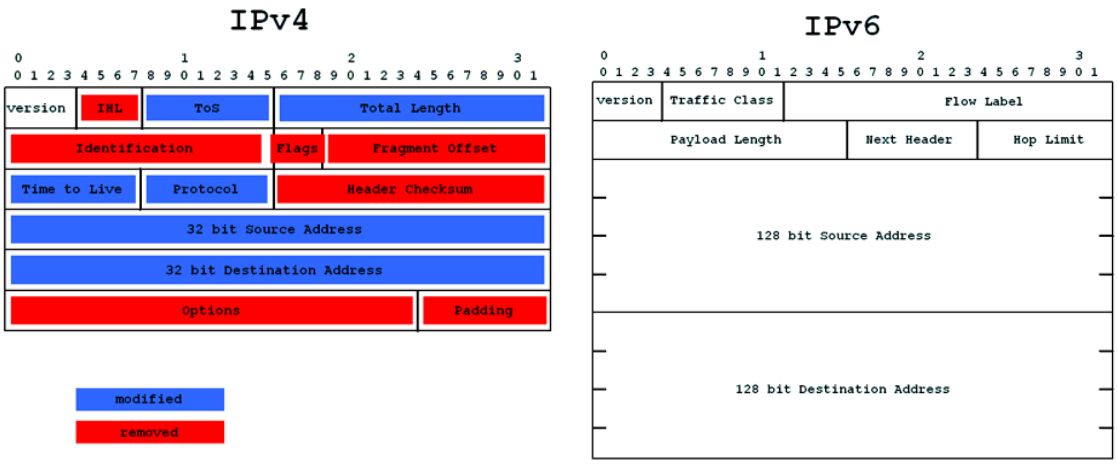
    - Limite de salto:
      - Longitud: 8 bits.
      - Define: Igual que TTL en IPv4.
    - Dirección origen:
      - Longitud: 128 bits.
      - Define: La longitud de origen.
    - Dirección destino:
      - Longitud: 128 bits.
      - Define: La longitud de destino

- Prioridad:
  - Si uno de los datagramas consecutivos debe ser descartado debido a la congestión, el datagrama con menor prioridad será descartado.
  - IPv6 divide el tráfico en dos categorías tráfico con control de congestión y tráfico sin control de congestión.
  - Tráfico con control de congestión:

        - Se acepta que los paquetes puedan retrasarse, perderse o llegar desordenados.
        - Asignamiento de prioridades:
            - Tráfico no específico (Prioridad 0): Sin prioridad.
            - Datos de fondo (Prioridad 1):
                - Datos que se entregan de fondo (entrega de noticias, etc).
            - Tráfico de datos no esperado (Prioridad 2):
                - Datos en que el retardo no tiene consecuencias (email, etc)
            - Tráfico con gran cantidad de datos esperado (Prioridad 4):
                - Transferencia elevada de datos con cliente a la espera (HTTP, FTP, etc).
            - Tráfico interactivo (Prioridad 6):
                - Necesaria la interacción con el cliente (Telnet, etc).
            - Tráfico de control (Prioridad 7):
                - Asignado a protocolos de encaminamiento (OSPF, RIP) o a protocolos de gestión (SNMP).
    - Tráfico sin control de congestión:
        - Tipo de tráfico que espera un mínimo retardo.
        - No es deseable el descarte de paquetes, dado que la retransmisión se hace casi imposible.
        - Las prioridades van del 8 al 15 y de acuerdo a como la calidad de los datos recibidos puede ser afectada por el descarte de paquetes.
- Etiqueta de flujo:
    - Longitud: 24 bits.
    - Define:
        - Es un número aleatorio entre 1 y 2^{24}-1 que un origen define de forma única a un flujo de paquetes.
        - Un flujo de paquetes es una secuencia de paquetes, enviada por un emisor concreto a un destino, que necesita una gestión especial en los encaminadores.
        - Para los encaminadores, un flujo es un secuencia de paquetes que comparten las mismas características, como seguir el mismo camino, utilizar los mismos recursos, tener el mismo tipo de seguridad, etc.
        - Un encaminador que soporta la gestión de etiquetas de flujo tiene una tabla de etiquetas de flujo.
        - La tabla tiene una entrada por cada etiqueta de flujo activa.
        - Cada entrada define los servicios requeridos por la etiqueta de flujo definida en el paquete.
        - A continuación proporciona al paquete los servicios mencionados en la entrada.
        - La etiqueta de flujo no proporciona la información para las entradas de la tabla de etiquetas de flujo, siendo las opciones de la cabecera quien la ofrece.
        - En su forma más sencilla, una etiqueta de flujo acelera el procesamiento de un paquete en un encaminador.
        - En su forma más sofisticada, una etiqueta de flujo soporta la transmisión de audio / video en tiempo real.
        - Se han definido tres reglas para el uso efectivo de etiquetas de flujo:

- La estación de origen es la que asigna la etiqueta de flujo a un paquete. Un emisor no debe reutilizar una etiqueta de flujo para otro flujo mientras el flujo existente siga activo.
- Si una estación no soporta la etiqueta de flujo, pone este campo a cero. Si un encaminador no soporta la etiqueta de flujo simplemente lo ignora.
- Todos los paquetes que pertenecen al mismo flujo tienen el mismo origen, el mismo destino, la misma prioridad y las mismas opciones.

- Comparación entre las cabeceras IPv4 e IPv6:



- El campo con la longitud de la cabecera se ha eliminado en IPv6 debido a que la longitud de la cabecera es fijo en esta versión.
- El campo con el tipo de servicio se ha eliminado en IPv6. El campo con la prioridad y la etiqueta de flujo juntas toman la misma función que el campo eon el tipo de servicio.
- La longitud total se ha eliminado en IPv6 y se ha reemplazado por la longitud de carga.
- La identificación, los indicadores y el desplazamiento se ha eliminado de la cabecera base en IPv6. Se ha incluido en la cabecera de ampliación.
- El campo TTL se denomina en IPv6 límite de saltos.
- El campo protocolo se ha reemplazado por el campo cabecera siguiente.
- La suma de comprobación de la cabecera se ha eliminado debido a que la suma de comprobación es ofrecida por los protocolos de nivel superior.
- El campo opciones en IPv4 se implementa como cabeceras de ampliación en IPv6.

- Un ejemplo de datagrama IPv6 real:

DATAGRAMA (marcado de azul)

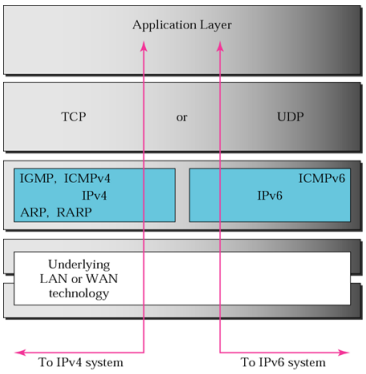
```
33 33 00 01 00 02 00 1d  e0 c6 11 f9 86 dd 60 00
00 00 00 65 11 01 fe 80  00 00 00 00 00 00 94 58
0d b5 2e 2d 85 e0 ff 02  00 00 00 00 00 00 00 00
00 00 00 01 00 02 02 22  02 23 00 65 14 ae 01 da
```

ANÁLISIS

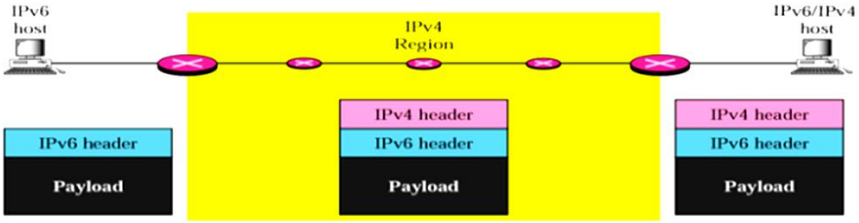
```
Internet Protocol Version 6
⊟ 0110 .... = Version: 6
    [0110 .... = This field makes the filter "ip.version == 6" possible: 6]
  .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
  .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 101
  Next header: UDP (0x11)
  Hop limit: 1
  Source: fe80::9458:db5:2e2d:85e0 (fe80::9458:db5:2e2d:85e0)
  Destination: ff02::1:2 (ff02::1:2)
```

- Cabeceras de ampliación:
  - Opción salto a salto:
    - Utilizada cuando el emisor necesita pasar información a todos los encaminadores visitados por el datagrama.
    - Se han definido tres opciones:
      - Pad1: Tiene 1 byte de carga y se ha diseñado para el alineamiento.
      - PadN: Similar a Pad1 pero con 2 o más bytes para alineamiento.
      - Carga jumbo: Define una carga mayor de 65535.
  - Encaminamiento desde origen:
    - Combina los conceptos de las opciones camino estricto desde el origen y camino relajado desde el origen de IPv4.
  - Fragmentación:
    - Un emisor debe utilizar la técnica de descubrimientos de caminos MTU para encontrar la MTU más pequeña soportada por cualquier red del camino.
  - Autenticación:
    - El objetivo es validar el mensaje y asegurar la integridad de los datos.
  - Carga de seguridad cifrada (ESP):
    - Ampliación que ofrece confidencialidad y guarda contra la interceptación.
  - Opción destino:
    - Usada cuando el emisor necesita pasar información al destino.
    - Los encaminadores intermedios no pueden acceder a esta información.
  - Comparación entre las opciones en IPv4 y las cabeceras IPv6:
    - Las opciones de no operación y fin de opción en IPv4 se han reemplazado por las opciones Pad1 y PadN en IPv6.
    - La opción registrar camino no se implementa en IPv6 debido a que nunca fue utilizado.
    - La opción de marca de tiempo no se implementa debido a que no se utilizó.
    - La opción camino desde el origen se denomina cabecera de ampliación de camino desde el origen en IPv6.
    - Los campos de fragmentación en la sección de cabecera base de IPv4 se han movido a la cabecera de ampliación de fragmentación.
    - La cabecera de ampliación para autenticación es nueva en IPv6.
    - La cabecera de ampliación para la carga de seguridad cifrada es nueva en IPv6.

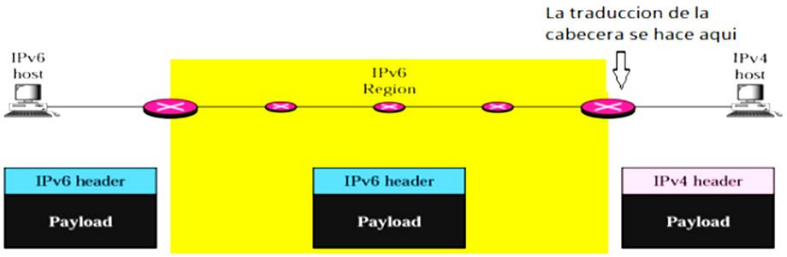
- TRANSICIÓN DE IPv4 E IPv6:
  - Para que la transición sea suave se han desarrollado tres estrategias por parte del IETF.
  - Pila dual:
    - Se recomienda que todas las direcciones tengan una pila dual de protocolos.
    - Para determinar que versión utilizar cuando se envía un paquete a un destino, el emisor consulta el DNS, decidiendo porqué protocolo enviar en función de la respuesta.



- Túneles:
  - Utilizada cuando dos computadoras que utilizan IPv6 quieren comunicarse entre sí y los paquetes deben atravesar una región que usa IPv4.
  - El paquete IPv6 se encapsula en un paquete IPv4 cuando entra en la región y se extrae cuando la deja.



- Traducción de cabeceras:
  - Necesaria cuando la mayor parte de Internet migre a IPv6 y permanezcan algunos sistemas utilizando IPv4.
  - El formato de la cabecera debe cambiarse totalmente mediante un proceso de traducción de cabeceras.
  - La cabecera del paquete IPv6 se convierte a una cabecera IPv4.



  - Algunas reglas de transformación son:
    - La dirección IPv6 se cambia a una dirección IPv4 extrayendo los 32 bits situados a la derecha.
    - El valor del campo de prioridad del paquete IPv6 se descarta.
    - El tipo del campo de servicio del paquete Ipv4 se pone a cero.
    - La suma de la cabecera del paquete IPv4 se calcula y se inserta en el campo correspondiente.
    - La etiqueta de flujo del paquete IPv6 se ignora.
    - Las cabeceras de ampliación compatibles se convierten a opciones y se insertan en la cabecera del paquete IPv4.
    - La longitud de la cabecera del paquete IPv4 se calcula y se inserta en el campo correspondiente.
    - Se calcula la longitud total del paquete IPv4 y se inserta en el campo correspondiente.