**INSTITUTO POLITECNICO NACIONAL**

**Escuela Superior de Cómputo**

**Aplicaciones para Comunicaciones de Red**

**Moreno Cervantes Axel Ernesto**

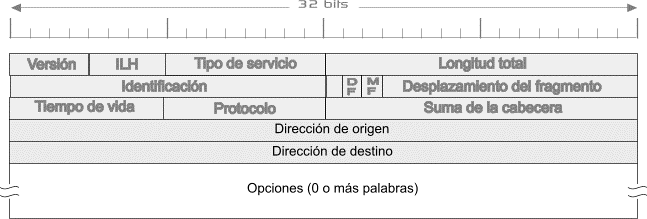
**Tarea: Encabezados IPV4 e IPV6**

**Miguel Ángel Morales García**

**Grupo: 3CM6**

**Encabezado IPv4**

IPv4 se utiliza desde 1983, cuando se implementó en la Advanced Research Projects Agency Network (ARPANET, Red de la Agencia de Proyectos de Investigación Avanzada), que fue la precursora de Internet. Internet se basa en gran medida en IPv4, que continúa siendo el protocolo de capa de red que más se utiliza. [2]



Los paquetes IPV4 tienen dos partes:

* **Encabezado IP:** identifica las características del paquete.
* **Contenido:** contiene la información del segmento de capa 4 y los datos propiamente dichos.

Como se muestra en la ilustración, los encabezados de paquetes IPV4 constan de campos que contienen información importante sobre el paquete. Estos campos contienen números binarios que se examinan en el proceso de capa 3. Los valores binarios de cada campo identifican las distintas configuraciones del paquete IP.

El campo **versión** lleva el registro de la versión del protocolo al que pertenece el datagrama. Al incluir la versión en cada datagrama es posible hacer que la transición entre versiones se lleve meses, o inclusive años.

La longitud de la cabecera no es constante, por eso se incluye un campo en la cabecera **IHL** para indicar la longitud en palabras de 32 bits. El campo **tipo de servicio** permite al host indicar a la subred el tipo de servicio que quiere. Son posibles varias combinaciones de confiabilidad y velocidad. El campo mismo contiene (de izquierda a derecha) un campo de precedencia; tres indicadores, D,T y R; y 2 bits no usados. El campo de precedencia es una prioridad, de 0 (normal) a 7 (paquete de control de red). Los tres bits indicadores permiten al host especificar lo que le interesa más del grupo (retardo, rendimiento, confiabilidad). [1]

La **longitud total** incluye todo el datagrama: tanto la cabecera como los datos. La longitud máxima es de 65535 bytes. El campo **identificación** es necesario para que el host destino determine a qué datagrama pertenece un fragmento recién llegado. Todos los fragmentos de un datagrama contienen el mismo valor de identificación.

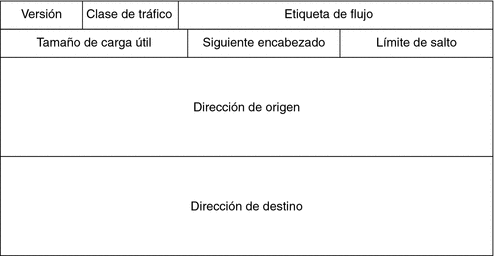
Luego viene un bit sin uso, y luego dos campos de 1 bit. **DF** significa no fragmentar, y **MF** significa más fragmentos. El **desplazamiento del fragmento** indica en qué parte del datagrama actual va este fragmento. Todos los fragmentos excepto el último del datagrama deben tener un múltiplo de 8 bytes que es la unidad de fragmento elemental. El campo **tiempo de vida** es un contador que sirve para limitar la vida del paquete. El campo **protocolo** indica la capa de transporte a la que debe entregarse (TCP o UDP o algún otro). La **suma de comprobación de la cabecera** verifica solamente a la cabecera. La **dirección IP de origen** contiene un valor binario de 32 bits que representa la dirección IP de origen del paquete, al igual que la **dirección IP de destino** que contiene un valor binario de 32 bits que representa la dirección IP de destino del paquete.

El campo **opciones** se rellena para completar múltiplos de cuatro bytes. Actualmente hay cinco opciones definidas, aunque no todos los encaminadores las reconocen: *Seguridad, Enrutamiento estricto desde el origen, Enrutamiento libre desde el origen,Registrar ruta y Marca de tiempo.*

Los dos campos que más comúnmente se toman como referencia son las direcciones IP de origen y de destino. Estos campos identifican de dónde proviene el paquete y adónde va. Por lo general, estas direcciones no se modifican durante la transferencia desde el origen hasta el destino.

**Encabezado IPv6**

El protocolo IPv6 define un conjunto de encabezados, que se dividen en básicos y de extensión. La figura siguiente ilustra los campos que tiene un encabezado de IPv6 y el orden en que aparecen.



En la lista siguiente se describe la función de cada campo de encabezado.

* **Versión**: número de versión de 4 bits del protocolo de Internet = 6. Para los paquetes IPv6, este campo siempre se establece en 0110.
* **Clase de tráfico**: campo de clase de tráfico de 8 bits. Equivale al campo Servicios diferenciados (DS) de IPv4. También contiene un valor de Punto de código de servicios diferenciados (DSCP) de 6 bits utilizado para clasificar paquetes y un valor de Notificación explícita de congestión (ECN) de 2 bits utilizado para controlar la congestión del tráfico.
* **Etiqueta de flujo**: campo de 20 bits. Proporciona un servicio especial para aplicaciones en tiempo real. Se puede utilizar para indicar a los routers y switches que deben mantener la misma ruta para el flujo de paquetes, a fin de evitar que estos se reordenen.
* **Tamaño de carga útil**: entero sin signo de 16 bits, que representa el resto del paquete que sigue al encabezado de IPv6, en octetos.
* **Encabezado siguiente**: selector de 8 bits. Identifica el tipo de encabezado que va inmediatamente después del encabezado de IPv6. Emplea los mismos valores que el campo de protocolo IPv4. Indica el tipo de contenido de datos que transporta el paquete, lo que permite que la capa de red pase los datos al protocolo de capa superior correspondiente. Este campo también se usa si se agregan encabezados de extensión optativos al paquete IPv6.
* **Límite de salto**: entero sin signo de 8 bits. Disminuye en uno cada nodo que reenvía el paquete. El paquete se desecha si el límite de salto se reduce a cero y se reenvía un mensaje de ICMPv6 al host emisor en el que se indica que el paquete no llegó a destino.
* **Dirección de origen**: 128 bits. Dirección del remitente inicial del paquete.
* **Dirección de destino**: 128 bits. Dirección del destinatario previsto del paquete. El destinatario previsto no es necesariamente el destinatario si existe un encabezado de enrutamiento opcional. [3]

Los paquetes IPv6 también pueden contener encabezados de extensión (EH), que proporcionan información optativa de la capa de red. Los encabezados de extensión son optativos y se colocan entre el encabezado de IPv6 y el contenido. Los EH se utilizan para realizar la fragmentación, aportar seguridad, admitir la movilidad, y más. [4]

Comparativo de protocolos

La maravilla de IPv6 radica en su encabezado. Una dirección IPv6 es 4 veces más grande que IPv4, pero, sorprendentemente, el cabezal de una dirección IPv6 es sólo 2 veces más grande que el de IPv4. Cabeceras IPv6 tiene un cabezal fijo y cero o más opcional (Extensión) encabezados. Toda la información necesaria que es esencial para que un router se mantiene en el cabezal fijo. La Extensión de encabezado contiene información opcional que ayuda a los routers a entender cómo manejar un paquete/flujo. [5]

Las opciones de IPv6 se colocan en encabezados de extensión independientes que se ubican entre el encabezado de IPv6 y el encabezado de capa de transporte de un paquete. Ningún enrutador procesa ni examina la mayoría de los encabezados de extensión de IPv6 durante el recorrido de distribución del paquete hasta que éste llega a su destino. Esta función supone una mejora importante en el rendimiento de los enrutadores en paquetes que contienen opciones. En IPv4, la presencia de cualquier opción hace que el enrutador examine todas las opciones. [3]

A diferencia de las opciones de IPv4, los encabezados de extensión de IPv6 pueden tener un tamaño arbitrario. Asimismo, la cantidad de opciones que lleva un paquete no se limita a 40 bytes. Aparte de la forma de procesar las opciones de IPv6, esta función permite que las opciones de IPv6 se apliquen a funciones que no resultan viables en IPv4.

Para mejorar el rendimiento al controlar los encabezados de opciones subsiguientes, así como el protocolo de transporte que va después, las opciones de IPv6 siempre son un múltiplo entero de 8 octetos. El múltiplo entero de 8 octetos mantiene la alineación de los encabezados subsiguientes.

Hay definidos los siguientes encabezados de extensión de IPv6:

* **Encaminamiento**: enrutamiento extendido, por ejemplo ruta holgada fijada en origen de IPv4
* **Fragmentación**: fragmentación y montaje
* **Autenticación**: integridad y autenticación, y seguridad
* **Encapsulado de carga útil**: confidencialidad
* **Opciones de salto a salto**: opciones especiales que necesitan procesamiento salto a salto
* **Opciones de destino**: información opcional que el nodo de destino debe examinar