Unidad de Aprendizaje n°2

Direccionamiento en IPv6

Introducción al Protocolo IPv6

Núcleo Eléctrico

Instituto Nacional de Aprendizaje
Llave del Progreso

###.### Instituto Nacional de Aprendizaje (Costa Rica)
Título del Material Didáctico Respectivo /
Nombre de la persona que elabora el Material Didáctico, .—
Provincia, C. R. INA, AÑO.
cantidad p.; número cm.

Material didáctico – No comerciable
ISBN #### – ### – ## -#

Sub Títulos.
I. Nombre de la persona que elabora el Material Didáctico ¸
comp. II. Título.

Edición
Instituto Nacional de Aprendizaje,
San José, Costa Rica.

ISBN #### – ### – ## -#

Hecho el depósito de ley

Impreso en Costa Rica

INDICE

INTRODUCCIÓN

Con la llegada del Internet de las Cosas (IOT), se hace imperativo cambiar el sistema de numeración de los equipos conectados a la red de Internet, cada dispositivo de nuestro hogar es susceptible de ser conectado a la red: lámparas, televisores, refrigeradoras y demás enseres de casa; IPv4 no logró contener los equipos conectados a la fecha, entonces será menos viable soportar lo que se avecina.

No aceptar el cambio y continuar con el protocolo IPv4 implica un atraso, sería como utilizar lanzas de piedra en la era actual, en su momento fueron instrumentos útiles, hoy en día han sido superados por otras tecnologías y persistir en su empleo, es cerrarse las puertas a un futuro de oportunidades en el uso de nuevas tecnologías.

No basta solamente el dominio teórico del protocolo IPv6, sino que debemos profundizar en su estructura, conocer su comportamiento y alcances con relación al IPv4 para establecer desde su experiencia la forma de aprovechar el uso que se le ha dado y lograr a partir de él una mayor cobertura y aprovechamiento del nuevo protocolo.

CAPITULO 2

CARACTERÍSTICAS Y TIPOS DE DIRECCIONES EN IPv6

Subtemas

2.1 Necesidad de una actualización permanente ante demandas y expectativas de la sociedad.

2.2 Formatos de direcciones

2.3 Tipos de direcciones

2.4 Encabezados de IPv6

2.5 ICMP, Neighbor Discovery

Objetivo

Al finalizar el estudio de este capítulo, entre otras habilidades, usted será capaz de:

- Identificar la estructura, tipos de direcciones y comportamiento del protocolo IPv6.

2.1 Necesidad de una actualización permanente ante las demandas y expectativas de la sociedad

Las Tecnologías de la Información han impactado todas las áreas del quehacer humano en mayor o menor grado, la telemedicina, la economía, la educación, las ciudades inteligentes, son inmensos desafíos a los que se enfrenta la humanidad y la llegada del Internet de las Cosas, además de impulsar el desarrollo obliga a cambiar lo que hasta ahora se ha mantenido intacto en el área de las redes, el protocolo de comunicación IP.

El entorno actual obliga a las instituciones y a las personas a estar en una constante adquisición de conocimiento e implementación de este para poder ser competitivos, bien lo indican Farfán y Garzón (2006) con la siguiente cita:

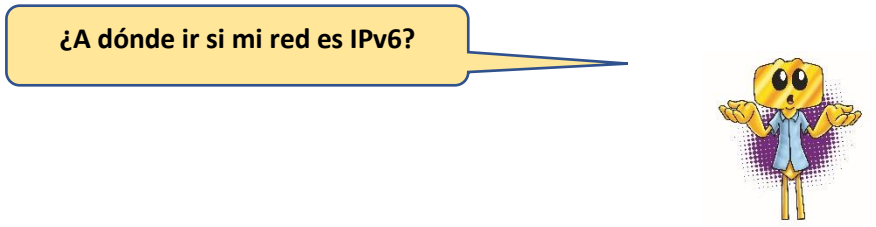
En el entorno competitivo actual, las empresas se ven enfrentadas a grandes retos, como lo son: la globalización, los avances tecnológicos, los acuerdos económicos, el constante crecimiento demográfico, cambios en los gustos de los consumidores, etc.; actividades dinámicas y cambiantes, que hacen necesaria la rápida adaptación a éstas y nuevas tendencias de la manera más eficiente y efectiva para sobrevivir en el mercado circundante". (p. 6)

Una actualización permanente tanto de las empresas como de las personas permite que además de ser competitivas, puedan sentir gratificación en su desempeño y el adquirir nuevos conocimientos que lleven no sólo a implementar acciones sino, poder participar en la toma de las decisiones permitirá junto a otras variables que el mantenerse actualizados sea una actividad que lleva a la plena satisfacción de la persona, como lo indica Farfán y Garzón:

Con el objeto de alcanzar un nivel más alto en el trabajo y desempeño, los trabajadores, son conscientes de la necesidad de exigir tareas y actividades que requieran mayor creatividad, innovación, competitividad y la posibilidad de ser partícipes en la toma de decisiones, para que sus trabajos

sean altamente gratificantes. La “satisfacción en el trabajo” es el resultado de varias actitudes que tiene un empleado hacia su trabajo, los factores conexos y la vida en general. (p. 7)

Las Tecnologías de la Información se han convertido en la columna vertebral de los desarrollos tecnológicos actuales, buscando hacer de un mundo tan diverso, una humanidad conectada gracias a Internet, de ahí que la implementación del protocolo IPv6 es un tema urgente para lograr una conexión global.



Si bien es cierto que el despliegue del protocolo IPv6 es lento, existen muchos sitios con los que interactuamos día a día que lo utilizan, por lo que la creencia de la imposibilidad de acceso a Internet no tiene sentido ya que sitios como Google, Facebook, YouTube, Yahoo y Apple tienen implementada la doble pila, permitiendo que usuarios de ambos protocolos los puedan tener acceso a ellos, lastimosamente la gran mayoría de sitios web únicamente utilizan el protocolo IPv4.

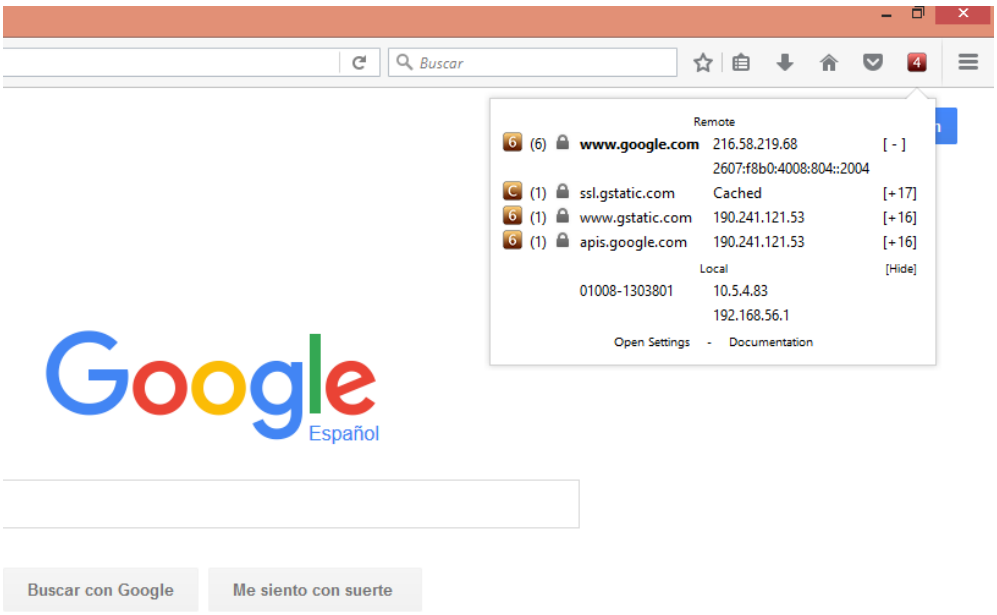


Figura 5. SixorNot Funcionando

No se ha logrado dejar de utilizar IPv4 por razones ya vistas y tampoco implementar toda la Internet en IPv6, ese es el paradigma a que nos enfrentamos, entonces ¿Qué hacer? La solución a corto plazo es implementar una doble pila, que no es otra cosa que nuestras redes entreguen servicios con ambos protocolos, por lo que las aplicaciones que pueden hacer uso del IPv6 lo harán y las que no, seguirán utilizando el IPv4; lo anterior asegura nuestra presencia en la red sin importar el protocolo del que hagan uso los clientes.

Actividad de Aprendizaje N° 8

1- Verifique el soporte para IPv6 de un sitio web instalando el addons SixOrNot en tu navegador Firefox.

La implementación del protocolo IPv6 es un proceso que requiere mucha atención, así como cuidado para no hacerlo apresuradamente, poniendo especial atención en primer instancia a evaluar si cumplimos con lo necesario a nivel de hardware, así como la capacidad de las aplicaciones que utilizamos a diario de soportar el protocolo IPv6, ya que dependiendo de la antigüedad de nuestros equipos y de la capacidad del software, tendremos un impacto económico muy fuerte con la actualización de hardware y software al día de hoy, a largo plazo los inconvenientes pueden aumentar debido a que los costos se incrementarían dada la cantidad de recursos humanos, tecnológicos, administrativos y otros involucrados, de ahí que el actuar a tiempo es la clave para no incurrir en gastos innecesarios.

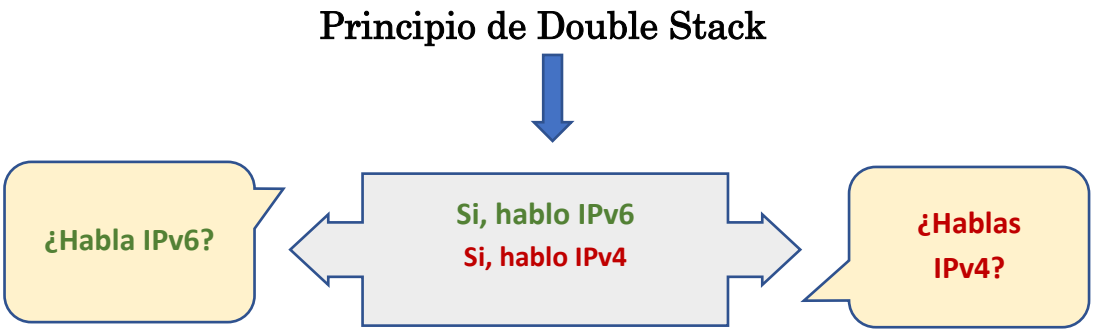


Figura 6. Principio de Double Stack

Un adecuado despliegue del protocolo IPv6 requiere que las personas asignadas tengan un profundo conocimiento de la parte técnica y que se base en los RFC (Request for Comments) del mismo, así como los conocimientos en redes que se emplean con el protocolo IPv4.

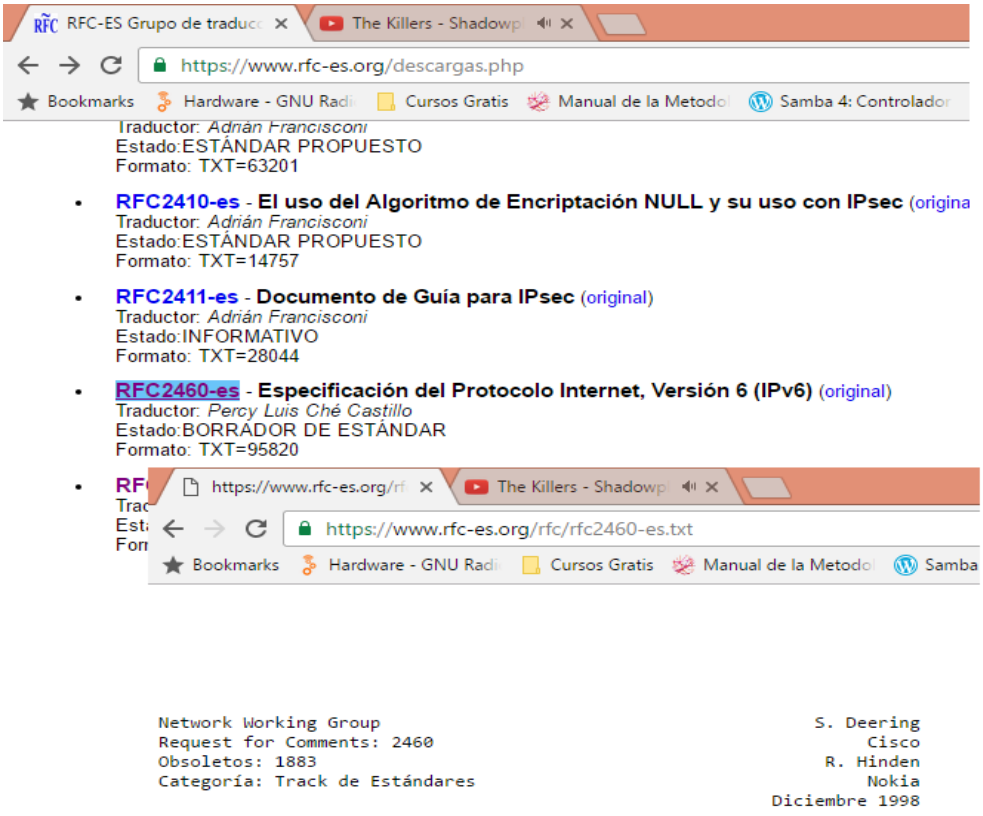


Figura 7. RFC del protocolo IPv6

Actividad de Aprendizaje N° 9

a. Se le invita a visitar la siguiente dirección web: https://www.youtube.com/watch?v=3DOcc18Bj2U y observar el video: “La triste historia de un ISP sin IPv6”.

- Enumere cuales fueron las consecuencias de una implementación tardía del protocolo IPv6

2.2 Formato de direcciones IPv6

Una dirección IPv6, es una secuencia de 128 bits, dividido en bloques de 16 bits cada uno, a su vez esos bloques se convierten a hexadecimal, que es un sistema numérico en base 16 donde representamos valores del 0 al 9 exactamente igual al sistema decimal y del 10 al 15 utilizamos letras empezando por la “A”, veamos la siguiente tabla, para más claridad:

Decimal	Binario	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Tabla 1: Conversión de bases

Cuando ya contamos con los bloques en hexadecimal, procedemos a separarlos utilizando el símbolo dos puntos (:); para una mejor comprensión de lo expresado, analicemos el siguiente ejemplo:

Primer Paso:

Una cadena de 128 bits en binario

00100000000000010000010000100100000000000000000000000000000000
10111111100100110111101101101001101111111001011100000001011110 01

Segundo Paso:

Dividirlo en bloques de 16 bits

0010000000000001 0000010000100100 0000000000000000 0000000000000000
1011111110010011 0111101101101001 1011111110010111 0000000101111001

Tercer Paso:

Separar los bloques con ":"

0010000000000001:0000010000100100: 0000000000000000: 0000000000000000:
1011111110010011: 0111101101101001: 1011111110010111: 0000000101111001

Cuarto Paso:

Convertir a Hexadecimal:

2001:0424:0000:0000:BF93:7B69:BF97:0179

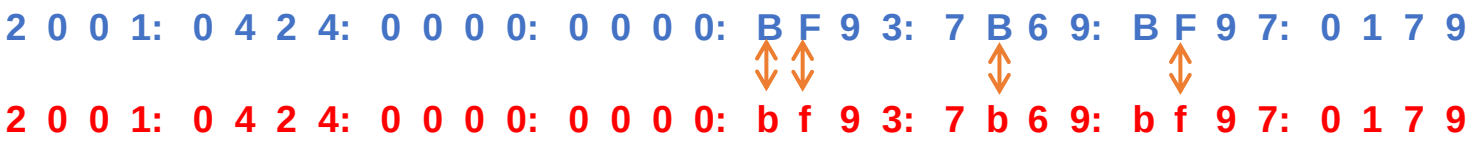
Una vez finalizado el proceso, ya contamos con una dirección IPv6, lo anterior es una demostración, no se refiere a ninguna en específico.

Podemos ver el proceso de forma más gráfica en el siguiente vídeo: https://youtu.be/HM7Ht0kLEq0

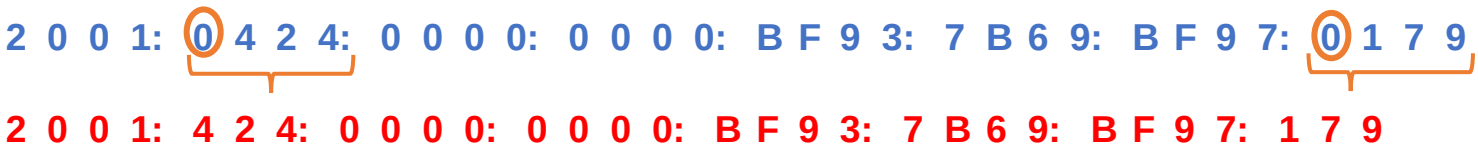
2.2.1 Simplificación de direcciones IPv6

La dirección IPv6 obtenida en el ejemplo anterior se muestra un poco confusa con tantos valores, sin embargo, existen una serie de reglas para simplificarla, las cuales las podemos encontrar en el **RFC 2373** "IP Version 6 Addressing Structure" y las mostramos a continuación:

a. Los números hexadecimales no son *case-sensitive*, en otras palabras, pueden ser mayúsculas o minúsculas:



b. Los ceros de la izquierda del bloque se pueden obviar:



c. La presencia de ":" de más, indica que existen 16 bits en ceros en esa posición y no se pueden escribir más que una vez, por lo que, si existieran varios bloques de ceros, los ":" sólo se indicarán en una ocasión, veamos dos ejemplos:

2001:424:0000:0000:BF93:7B69:BF97:179

2001:424::BF93:7B69:BF97:179

2001:0424:0000:0000:BF93:0000:0000:0179

2001:424::BF93:0000:0000:179

d. De existir uno o una serie de bloques en cero, bastará representarlo con un único ":", no se permite más que uno y para saber cuántos ceros representa, simplemente tenemos que restarle a 128 la cantidad de bloques presentes en la dirección:

4 0 2 1: 0 0 0 0: 0 0 0 0: 0 0 0 0: 0 0 0 0: 0 0 0 0: A C 2 1: B C D

128 bits

4 0 2 1: 0 0 0 0: 0 0 0 0: 0 0 0 0: 0 0 0 0: 0 0 0 0: **A C 2 1: B C D**

4 0 2 1: 0 0 0 0: 0 0 0 0: 0 0 0 0: 0 0 0 0: 0 0 0 0: **A C 2 1: B C D**

4 0 2 1: 0 0 0 0: 0 0 0 0: 0 0 0 0: 0 0 0 0: 0 0 0 0: **A C 2 1: B C D**

4 0 2 1: A C 2 1: B C D

4 0 2 1 :: A C 2 1: B C D = **48 bits**

128 – 48 = 80 bits, podemos entonces saber con certeza que los "::" representan 80 bits con valor cero en una cadena continua.

e. Cuando tenemos uno o varios bloques completos en cero, se puede representar con un solo por bloque:

2 0 0 1: 0 0 0 0: 1 2 3 4: A B C D: 1 2 A B: 0 0 0 0: C D E F: 0 0 0 1

2 0 0 1: 0 1 2 3 4: A B C D: 1 2 A B: 0 C D E F: 1

2 0 0 1: 0: 1 2 3 4: A B C D: 1 2 A B: 0: C D E F: 1

En el siguiente vídeo podemos observar el proceso de simplificación de direcciones IPv6 de una forma más gráfica: https://youtu.be/cxS8bcb0Irk

Actividad de Aprendizaje N° 10

1- Simplifique las siguientes direcciones IPv6 según lo leído
   1. 2001:0000:0000:0000:0000:0000:ABCD:0001
   2. 2001:0120:00AB:12AB:0000:0000:ABCD:0AB1
   3. 2001:0000:ABCD:CDEF:9876:0000:0000:1234

2.3 Tipos de Direcciones

Como se estudió en el capítulo anterior, los modos en que puede operar una dirección IPv6, son únicamente tres:

- unicast

- anycast

- multicast

¿Quieres saber si tu equipo tiene IPv6 o lo soporta?

Ve a la siguiente dirección en cualquier navegador: ***http://test-ipv6.com***

Los modos anteriores permiten que los paquetes IPv6 sean tratados de forma diferente al protocolo IPv4, donde un paquete se enviaba a la red interna y se utilizaba el broadcast, dicha técnica consistía en que cada equipo conectado a la red recibía una copia del paquete y si la dirección IP destino no era la suya lo desechaba; el método mejoró con el uso de switches, ya que el dispositivo no enviaba el paquete a todas las interfaces conectadas, sino, únicamente a la que tenía la dirección destino del paquete.

Antes de conocer los tipos de direcciones de los que podemos hacer uso al utilizar el direccionamiento IPv6, se debe mostrar el prefijo ***2001:0db8::/32***, que sirve únicamente y exclusivamente para documentación.

Toda dirección IPv6 se compone de dos partes, un prefijo de 64 bits y 64 bits que corresponden al identificador de interface (ID), dependiendo del método de configuración el prefijo puede cambiar.

Según los RFC de IPv6 existen dos tipos de configuración:

- Autoconfiguración:

Se define en el RFC 2462, también se le conoce como **Configuración Automática de Dirección sin Estado IPv6**, se aplica únicamente a los equipos finales (hosts), se refiere a que un router IPv6 anuncia los 64 bits del prefijo IPv6 de unicast global único a los equipos y ellos completan los otros 64 bits mediante un mecanismo que se basa en la dirección MAC de cada uno, denominado EUI-64 (aunque existen variantes según fabricantes).

- Configuración mediante Servidor:

Los parámetros y opciones para configurar la dirección IPv6 se obtienen de un servidor de DHCP versión 6, a este método se le denomina **Configuración de Direcciones con Estado IPv6.**

El método utilizando DHCP se explicará con más detalle en cursos posteriores.

2.3.1 PROCESO EUI-64

El método para generar el **EUI** (**Identificador Único Extendido)** por sus siglas en inglés, según se especifica en el RFC4291 se explica a continuación:

- Cada interfaz de red contenida en los dispositivos cuenta con una dirección MAC, que es un valor único que identifica la interface, tiene un tamaño de 48 bits en formato hexadecimal y se divide en dos partes de 24 bits, la primera se denomina **Identificador Único de Organización (OUI)** o código de proveedor**,** la segunda **Identificador de Dispositivo.**

- El **ID de Interfaz** se compone de tres partes representadas en formato binario: primeros 24 bits para el OUI y según el RFC5342 se debe invertir el bit U/L (sétimo bit), 16 bits **FFFE** y el identificador de dispositivo de 24 bits.

A continuación, realizamos un ejercicio para el ID de interfaz:

1. Obtener la dirección MAC de un equipo. En Windows ***INICIO->EJECUTAR->CMD [ENTER]***. Escribir *ipconfig /all*, buscar la dirección MAC (dirección física)

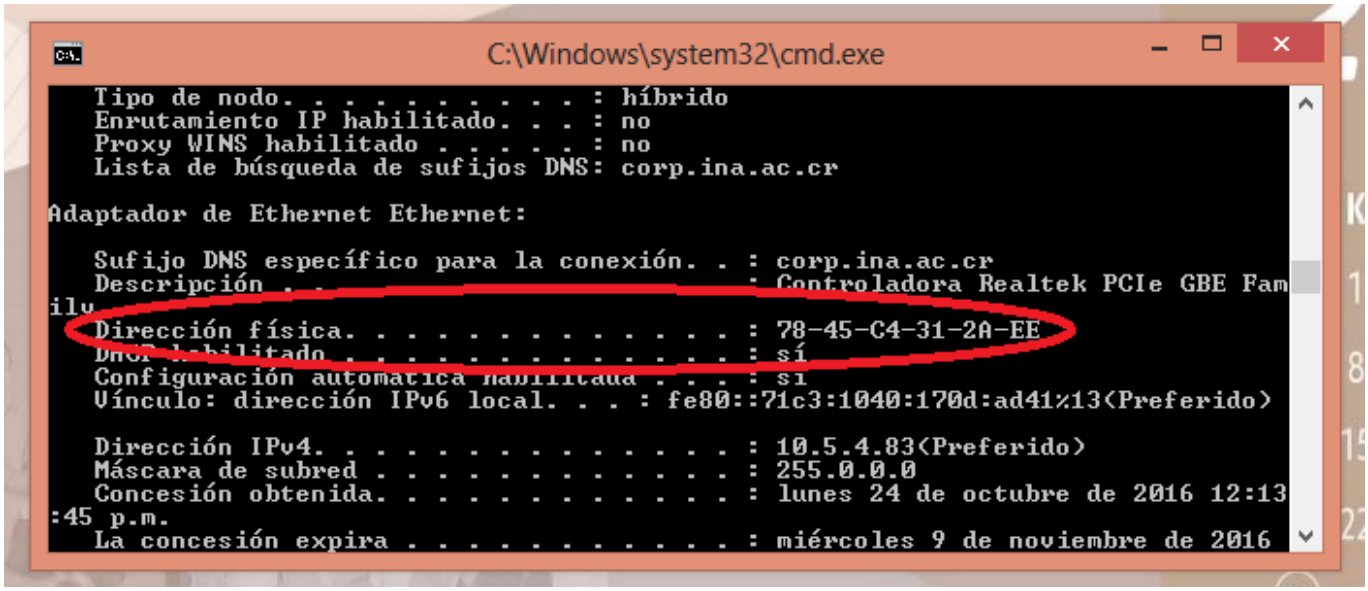
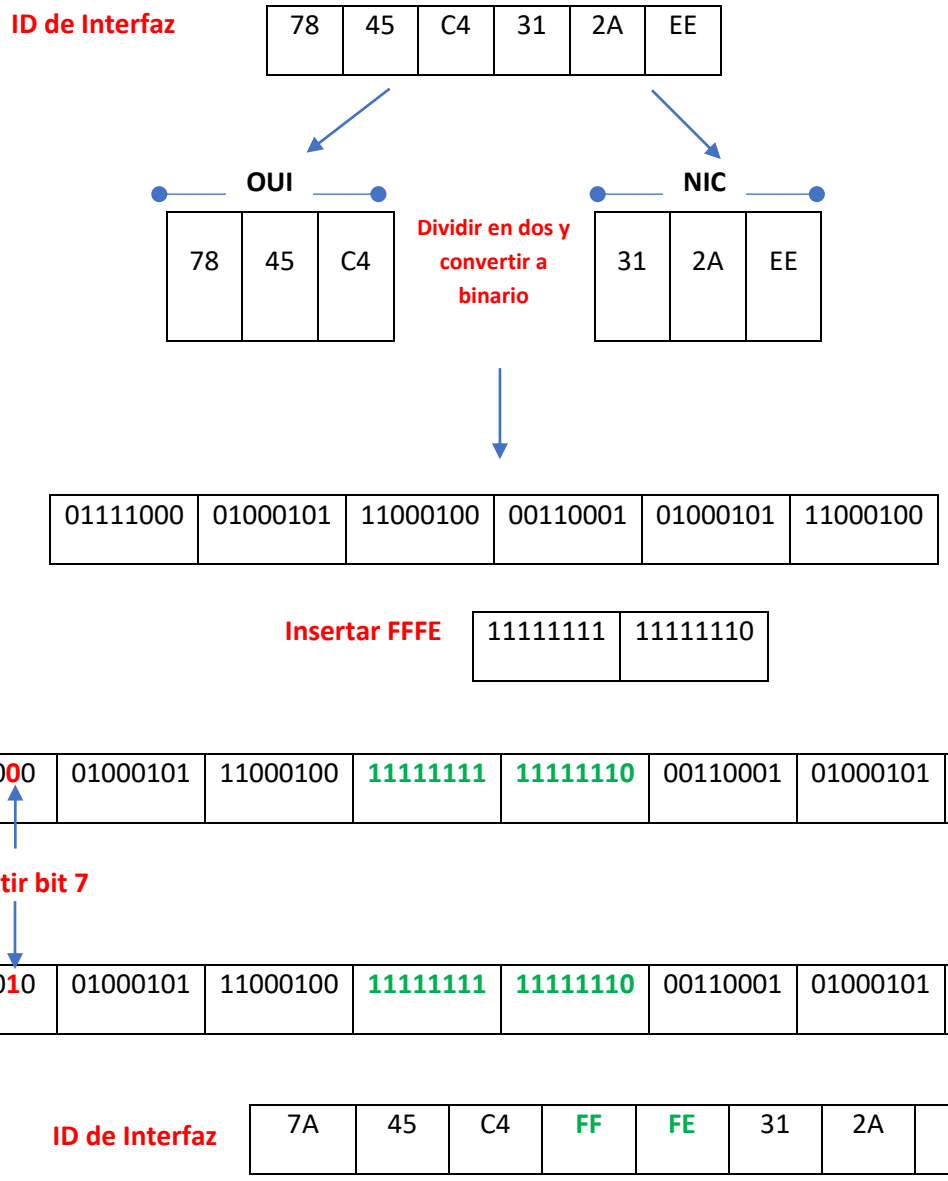


Figura 8. Dirección MAC

2. En nuestro ejemplo, la dirección física es: 78-45-C4-31-2A-EE, recordar que es hexadecimal, para más claridad la colocaremos en una tabla y la pasaremos a binario.

Si ocupas una calculadora para conversiones de hexadecimal a binario, ve a la siguiente dirección: http://www.disfrutalasmatematicas.com/numeros/binario-decimal-hexadecimal-conversor.html

PROCESO EUI-64



Tras el proceso anterior, obtenemos el ID de Interfaz, al cual se le deberá agregar el prefijo que indique el tipo de dirección, sea unicast global o link local.

El siguiente video nos permite observar el proceso anterior ilustrado de forma gráfica: https://youtu.be/bQ5C3taocLc

2.3.2 Unicast

Son direcciones que permiten la comunicación de uno a uno, son acompañadas de un prefijo que indica la cantidad de bits significativos (tamaño del prefijo) por lo que pueden ser sumarizadas; dentro de las direcciones de tipo unicast, hay tres tipos diferentes agrupados:

- Enlace Local

Este tipo de enlace es temporal, se usa para enlaces sencillos y no debe ser enrutada hacia ninguna otra red, es utilizada para mecanismos de autoconfiguración como el EUI-64, agregando los prefijos **FE80::/10**, aunque los dispositivos comúnmente utilizan **FE80::/64.** Para nuestro ejemplo utilizaremos el segundo, por lo cual nuestra dirección IPv6 quedaría de la siguiente forma:

FE80::7A45:C4FF:FE31:2AEE/64

- Sitio Local

Este tipo de direcciones tenían como ámbito el sitio local, sin embargo, son obsoletas y se sustituyeron con unique-local.

- Unique Local (ULA)

Sustituyen a las direcciones denominadas Sitio-Local, son direcciones de tipo privado que tienen alta probabilidad de tener un prefijo único, son utilizables solamente dentro de un enlace o un grupo limitado de enlaces y no son enrutables a través de Internet, se especifican en el RFC4193.

Su estructura es la siguiente:

Prefijo: FC00::/7	8 bits.
ID Global pseudo-aleatorio	40 bits.
ID Subred	16 bits.
Identificador de Interfaz	64 bits

FC00::10:0:0:0/120

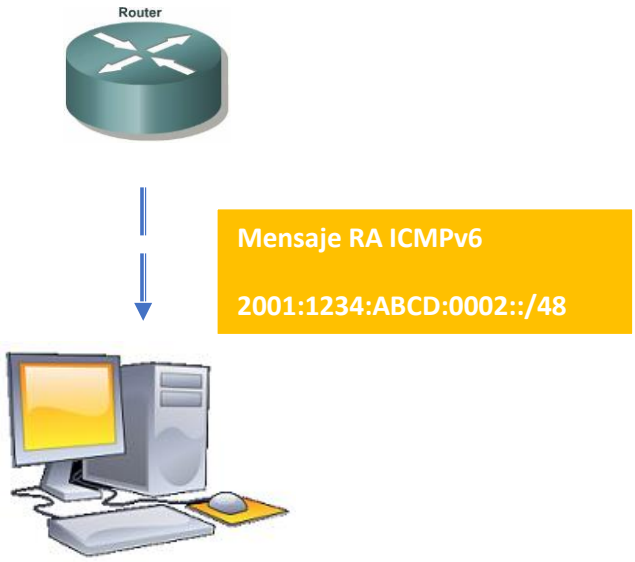
- Global

Las direcciones de tipo global no tienen límite de ámbito, son enrutables a través de Internet, cuentan con una estructura jerárquica de tres niveles:

1. Prefijo de enrutamiento global (red), es asignado por el proveedor de servicios, usualmente su tamaño es de 48 bits, aunque realmente depende del proveedor.
2. Identificador de enrutamiento local (subred), con un tamaño de 16 bits, este identificador lo define el ente dueño de la red.
3. Identificador de interfaz de 64 bits.

Cada una de las partes de la dirección IPv6 pueden ser de diferente tamaño, sin embargo, se respetan los 64 bits de la ID de Interface, para las direcciones globales se puede utilizar el mismo ID de Interfaz, sin embargo, el prefijo es asignado por medio de un mensaje RA (Router Advertisment) de ICMPv6 entregado por el router o servidor DHCP que se combina con él.

Prefijo: **2001:1234:ABCD::/48**



Dirección IPv6 HOST

2001:1234:ABCD:0002:7A45:C4FF:FE31:2AEE

Figura 9. Asignación de Prefijo por DHCP

Otra forma de presentar una dirección IPv6 de tipo global es la siguiente:

Proveedor de Servicios: **2001:1234:ABCD::/48**

SubRed de la Organización: **2001:1234:ABCD:0002::/64**

Dispositivo: **2001:1234:ABCD:0002:7A45:C4FF:FE31:2AEE**

- Loopback

  Las direcciones de tipo loopback se refieren a la dirección IPv6 para identificar al localhost, similar a la dirección 127.0.0.1 en IPv4.

  ::1/128

- Sin Especificar

  Una dirección sin especificar es utilizada con propósitos especiales, por ejemplo, en una solicitud de DHCP.

  ::/128

- Mapeada IPv4

  Una dirección mapeada IPv4, es un tipo de dirección que en su estructura IPv6, lleva embebida una dirección IPv4 en los 32 bits menos significativos, o sea, en los últimos de la dirección. Es utilizada como un mecanismo de transición y consiste en entregar direcciones IPv6 sobre túneles creados en redes IPv4.

  ::FFFF:192.168.10.3

  ::FFFF:C0A8:0A03

  No debe confundirse las direcciones mapeadas IPv6 con las direcciones IPv4 compatibles, ya que esas fueron un mecanismo de transición en las redes IPv4/IPv6, pero ya no se utilizan, su formato era:

  ::192.168.10.3/96

  ::C0A8:0A03/96

2.3.3 Anycast

Una dirección de tipo anycast sintácticamente no se diferencia de una de tipo unicast, ya que se toma del mismo bloque y se utilizan para ser asignadas a interfaces en dispositivos diferentes. Cuando un paquete tiene como destino una dirección IPv6 anycast es enrutado a la interface más cercana según lo indique la métrica del protocolo de enrutamiento utilizado y solamente se puede utilizar una dirección anycast como destino, nunca como fuente.

En resumen, una dirección de tipo unicast se convierte en anycast cuando se asigna a varias interfaces.

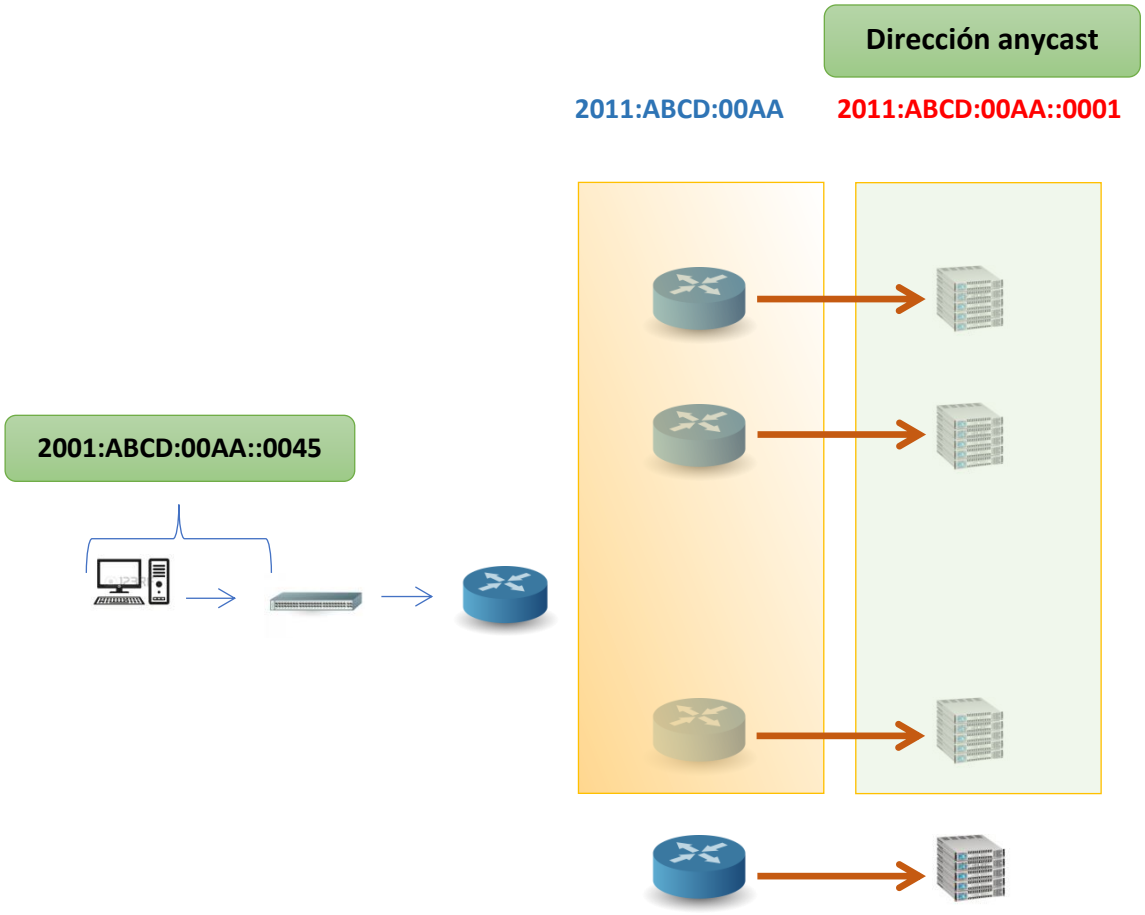


Figura 10. Dirección anycast

2.3.4 Multicast

Una dirección multicast permite identificar un grupo de interfaces que se encuentran en diferentes hosts como destino de mensajes IPv6, una interface puede pertenecer a varios grupos multicast, muchas veces se puede confundir su funcionamiento con el broadcast del IPv4, sin embargo, la diferencia más clara es que los mensajes broadcast se transmiten a todos los nodos en una red, el multicast lo hace a nodos específicos que se definen en su alcance.

Una dirección de tipo multicast es definida por el rango **FF00::/8** hasta el **FFFF::/8** para utilizar como prefijo, los primeros 8 bits tendrán un valor de 1 y los siguientes 8 están divididos en un primer grupo de 4 en donde los 3 más significativos (primeros) están siempre en 0 y el cuarto puede ser un 1 lo que indicaría es una dirección de tipo multicast temporal, mientras que 0 indica que es permanente, luego tenemos 4 bits que indican el alcance y por último los 112 bits menos significativos definen el ID de Grupo. De una manera gráfica sería así:

8 bits	4 bits	4 bits	112 bits
11111111	000X	Ámbito	ID de Grupo

El valor que establece el alcance no es arbitrario, sino que ya se encuentra definido y se muestran en la siguiente tabla:

VALOR	ALCANCE
0	Reservado
1	Ámbito Local de Nodo
2	Ámbito Local de Enlace
3	No Asignado
4	No Asignado

5	Ámbito Local de Sitio
6	No Asignado
7	No Asignado
8	Ámbito Local de Organización
9	No Asignado
A	No Asignado
B	No Asignado
C	No Asignado
D	No Asignado
E	Ámbito Global
F	Reservado

Resumiendo, cualquier dirección IPv6 cuyo prefijo se encuentre en el rango **FF00::/8** es una multicast.

Actividad de Aprendizaje N° 11

1- Clasifique las siguientes direcciones según lo leído
   a. ::FFFF:C1B2:1AA1
   b. FC00::10:0:0:0/120
   c. FE80::7A45:C4FF:FE31:2AEE/64
   d. FF01::0024
   e. ::1/128

2.4 Encabezados de IPv6

La estructura del protocolo IPv6 se define en el RFC2460, denominado: “Especificación del Protocolo de Internet Versión 6”, donde se enumeran los cambios del IPv6 con respecto al IPv4, mismos que se pueden categorizar de la siguiente forma:

- Capacidades de direccionamiento extendida

Aumento en la cantidad de direcciones con respecto al IPv4, más niveles de direccionamiento jerárquico y una configuración automática de direcciones más simple, además se mejora la escalabilidad del enrutamiento.

- Simplificación del formato de la cabecera

Campos utilizados en IPv4 se eliminaron o se establecieron como opcionales para disminuir el costo del proceso de tratamiento de paquete, permitiendo así que el costo de ancho de banda se reduzca.

- Soporte mejorado para las extensiones y opciones

Modificación de la forma en que se codifican las opciones de la cabecera, lo que permite un envío más eficiente, límites flexibles en la longitud de las opciones y la flexibilidad de poder agregar opciones nuevas a futuro.

- Capacidad de etiquetado de flujo

Una capacidad que no existió en el IPv4, que consiste en permitir etiquetar los paquetes pertenecientes a un tráfico particular, para lo cual el remitente del paquete tiene la posibilidad de solicitar un trato especial, puede ser QoS o tiempo real.

- Capacidades de autenticación y privacidad

Extensiones agregadas para la autenticación, integridad y confidencialidad de los datos (opcional).

A continuación, se presentan los campos que componen el encabezado IPv6.

CAMPO	TAMAÑO bits	DESCRIPCIÓN
Versión	4	Versión del Protocolo.
Clase de Tráfico	8	Etiqueta el paquete con un Punto de Código de Servicios Diferenciados (DSCP) indicando como debe ser manejado. Los valores que puede asumir son los siguientes: *0. Uncharacterized Traffic* *1. Filler Traffic Such as Netnews* *3. Reserved* *4. Attended Bulk Transfer Such as FTP* *5. Reserved* *6. Interactive Traffic Such as Telnet* *7. Internet Control Traffic Such as SNMP* *8 – 15. Aplicaciones de Usuario*
Etiqueta de Flujo	20	Marca un flujo o secuencia de paquetes IPv6 para que sean tratados de forma especial, lo que reduce el trabajo de los routers.
Longitud de Carga Útil	16	Indica el tamaño de la carga útil del paquete
Siguiente Encabezado	8	Identifica el encabezado siguiente que compone el datagrama
Límite de Saltos	8	Sustituye el TTL (Time to Live) de IPv4, contiene un número que indica la cantidad de saltos que el paquete deberá realizar para llegar a su destino, si el valor llega a 0 se destruye el paquete y se envía un mensaje de error. El TTL utilizaba una unidad de tiempo para realizar la misma operación
Dirección Fuente	128	Dirección IPv6 del emisor
Dirección Destino	128	Dirección IPv6 del receptor

Tabla 2. Campos de encabezado IPv6

Las siguientes imágenes muestran la estructura del encabezado del IPv4 y la del IPv6 y sus diferencias.

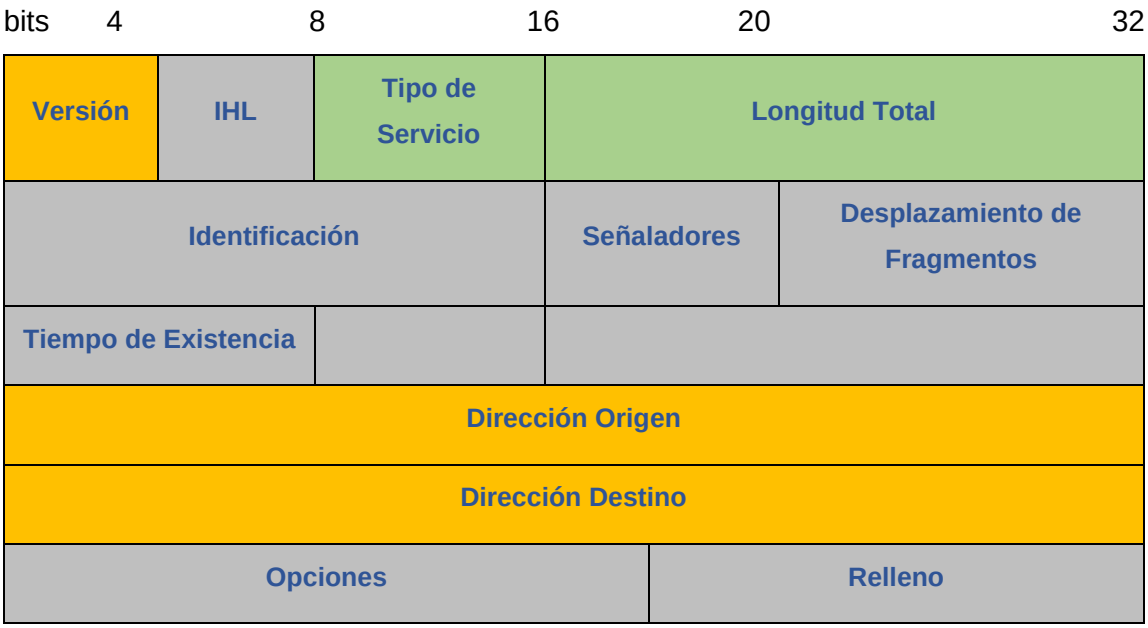


Figura 11. Estructura IPv4

De la estructura anterior, se eliminan los campos en color gris cuando se crea el IPv6 debido a varias razones, entre ellas podemos indicar una de las más importantes que ya no servían al tratar con un encabezado de tamaño variable, el nuevo encabezado queda con la siguiente estructura en donde el color azul muestra lo nuevo y el amarillo lo que se mantiene del IPv4:

Figura 12. Estructura IPv6

El nuevo encabezado logra un mejor desempeño del paquete del Protocolo IP, permitiendo entre otras cosas un menor peso de trabajo en las tablas de enrutamiento de los encaminadores de tráfico en Internet, una mayor carga de datos en el paquete IP y por supuesto una nueva forma de llevar a cabo la transmisión de esos paquetes a través de las redes, ya que utiliza encabezados de extensión que hacen más eficiente el ruteo de paquetes.

2.4.1 Encabezados de Extensión (Extension Header = EH)

Las opciones eliminadas del encabezado en IPv4, siguen existiendo en IPv6, pero esta vez no forman parte del encabezado, sino que se disponen en encabezados de extensión independientes que se van ubicando entre el encabezado del protocolo IPv6 (también denominado cabecera fija) y el encabezado del protocolo de transporte del paquete, esta flexibilidad permite que únicamente se revise la cabecera que le corresponde a cada dispositivo de la red, los encabezamientos de extensión más comunes en IPv6 definidos en el RFC2460 son los siguientes:

Hop-by-Hop: Esta cabecera debe ser examinada por cada host de la ruta por donde deba pasar el paquete IP. **Valor 0.**

TCP: Indica que el paquete es TCP (Protocolo de Control de Transporte). **Valor 6.**

UDP: Indica que el paquete es de tipo UDP (Protocolo de Datagrama de Usuario). **Valor 17.**

De Enrutado: Se utiliza para indicar los nodos que deben estar en la ruta seguida por el paquete. **Valor 43.**

De Fragmento: Cada host tiene una Unidad Máxima de Transmisión denominada MTU, cuando un paquete excede ese tamaño se debe fragmentar; originalmente en IPv4, la fragmentación de paquetes se llevaba a cabo en los enrutadores, ahora en IPv6, se gestiona de extremo a extremo, lo que quiere decir que cuando un origen desea enviar un paquete a un destino IPv6, primero debe determinar cuál es el tamaño máximo que puede utilizar para enviar un paquete (MTU) haciendo uso de Path MTU Discovery, si ese proceso fallara entonces se utilizará el tamaño 1280 bytes que es el valor mínimo permitido en IPv6 como MTU y si el tamaño del paquete es mayor a cualquiera de esos valores, entonces debe fragmentarse, por lo que la presencia de esta cabecera indica que el paquete está fragmentado. **Valor 44.**

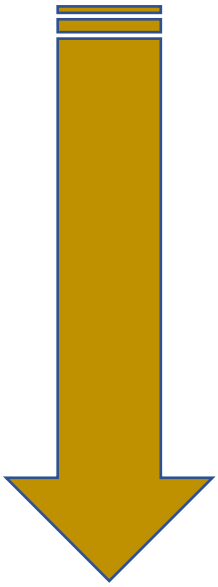
Carga útil de seguridad encriptada: Denominada ESP por sus siglas en Inglés (Encrypted Security Payload) y se referencia en el RFC4303, proporciona confidencialidad, integridad y autenticación de datos. **Valor 50**

De autenticación (AH): Referenciada en el RFC4302 y nos proporciona seguridad y autenticación para los paquetes IP enviados. Se soportan distintos mecanismos de autenticación. **Valor 51.**

No Next Header: Indica que no hay más cabeceras. **Valor 59.**

Opciones de Destino: Contiene información exclusiva para el host destino. **Valor 60**

Las cabeceras anteriores permiten una mayor flexibilidad al trabajar con paquetes IP, ya que cada cabecera será revisada por el dispositivo correspondiente, además, las cabeceras de extensión tienen un orden de ejecución siempre que exista más de una en el paquete, tal como se indica a continuación según la RFC2460:

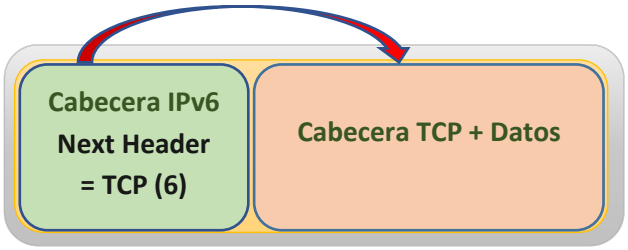


1. Cabecera IPv6
2. Cabecera de opciones Hop-by-Hop
3. Cabecera de Opciones destino que son opciones procesadas por el primer destino que existe en el campo de dirección destino.
4. Cabecera de Enrutamiento.
5. Cabecera de Fragmento.
6. Cabecera de autenticación.
7. Cabecera de carga útil de seguridad encapsulada
8. Cabecera de Opciones Destino.
9. Cabecera de Capa Superior.

En la figura a continuación se presenta un paquete IPv6 y el uso de cabeceras:

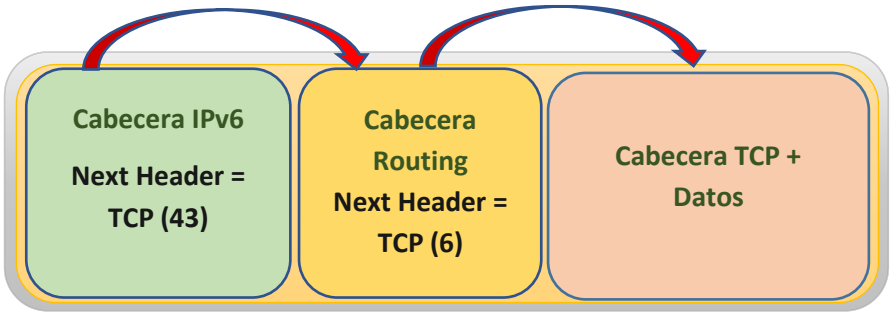
Sin Cabeceras de Extensión

La cabecera IPv6 o cabecera permanente indica que la siguiente cabecera es de tipo TCP (6), en esa cabecera van los datos sensibles y de control.



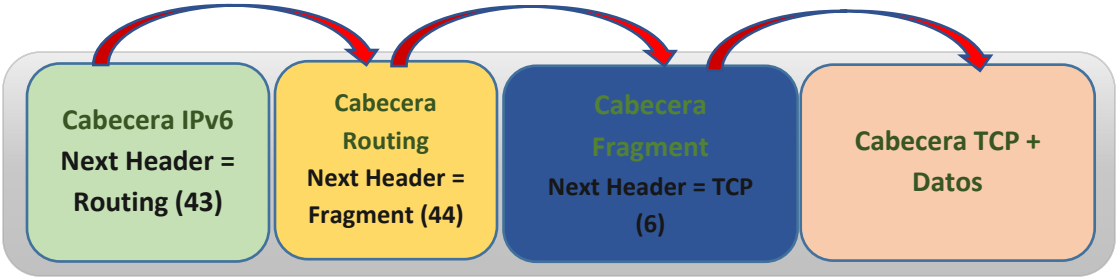
1. **Cabecera de Extensión**

El paquete se va a enviar a través de un router, entonces se le agrega una cabecera de routing (43), por lo que la cabecera permanente ahora apunta a la siguiente que sería routing y esta a su vez apunta a la cabecera TCP(43).



2. **Cabeceras de Extensión**

El paquete resulta muy grande, entonces debe fragmentarse y se le agrega una cabecera de Fragmentación (44), entonces la cabecera de routing apunta a esa nueva y esa apunta a TCP (43).

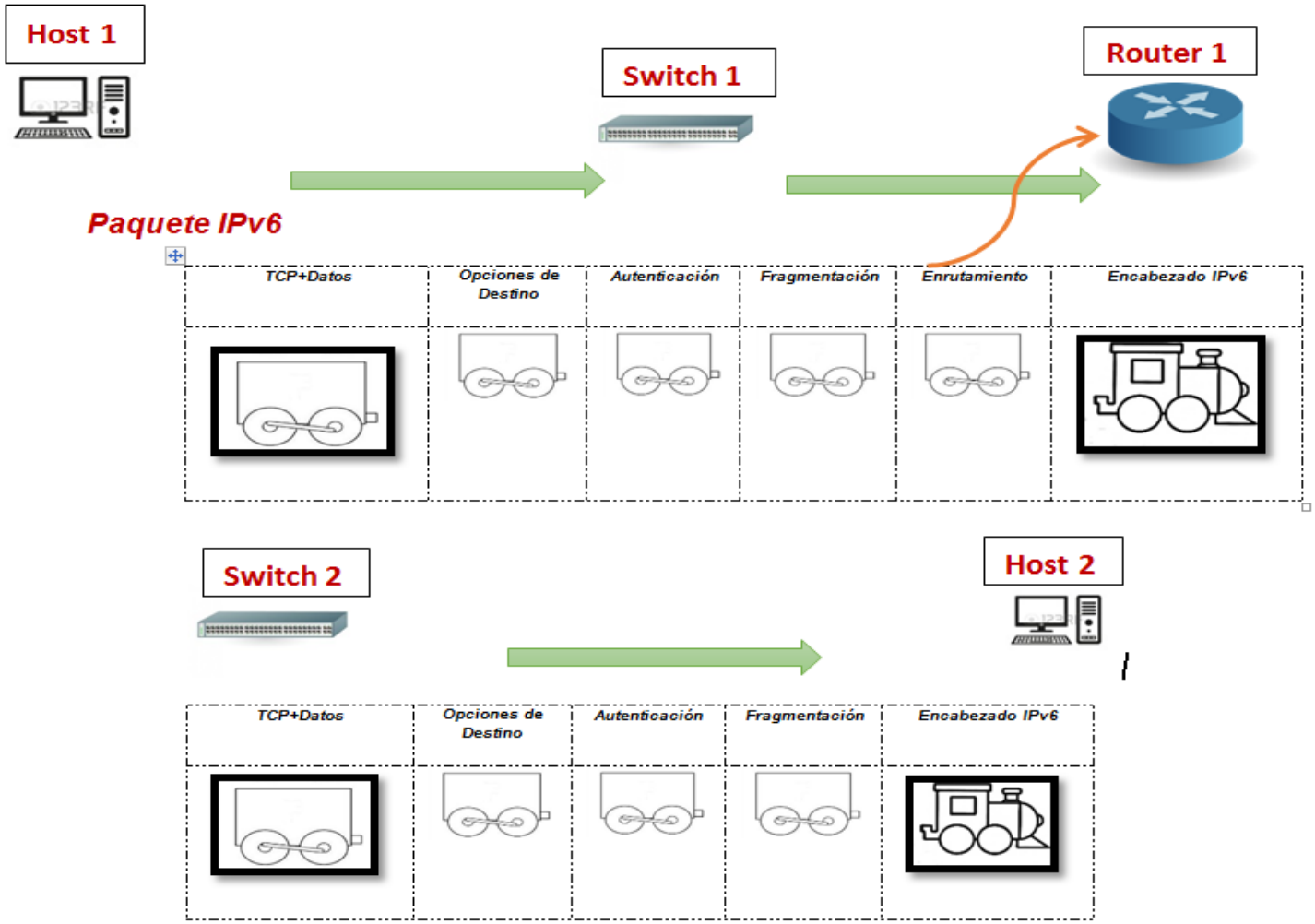


	**Actividad de Aprendizaje N° 12**
	Lea el enunciado e indique a qué campo del encabezado IPv6 se refiere: 1- Marca un flujo o secuencia de paquetes IPv6 para que sean tratados de forma especial, lo que reduce el trabajo de los routers 2- Sustituye el TTL (Time to Live) de IPv4 3- Etiqueta el paquete con un Punto de Código de Servicios Diferenciados 4- Identifica el encabezado siguiente que compone el datagrama

Esta nueva estructura del paquete IP, logra que el tiempo de proceso sea menor y que la carga útil sea mayor, permitiendo de esa forma que el procesamiento de paquetes de una creciente Internet sea más eficiente.

En el siguiente video se representa de forma gráfica el comportamiento de las cabeceras en IPv6: https://www.youtube.com/watch?v=aIPEOXhXN5U

Representación Gráfica del uso de cabeceras



2.5 ICMPv6, Neighbor Discovery

ICMPv6, es la versión para IPv6 del Internet Control Message Protocol (Protocolo de Control de Mensaje de Internet) del IPv4, tiene un tamaño de 32 bits, según lo define el RFC4443 y aunque realiza iguales funciones de su antecesor, no es compatible con el mismo, entre sus funciones están:

1. Reenvío de mensajes de estado de la red.
2. Reenvío de mensajes de características de la red.
3. Informar sobre errores en el procesamiento de paquetes.

Las funciones enumeradas, son las mismas que se tienen en ICMP de IPv4, pero además de ellas cuenta con una serie de funciones nuevas para el protocolo IPv6, como las siguientes:

1. Funciones de ARP (Address Resolution Protocol) o Protocolo de Resolución, que mapea las direcciones de capa 2 a direcciones IP y viceversa.
2. Funciones del IGMP (Internet Group Management Protocol) o Protocolo de Administración de Grupos de Internet, que se encargaba de gestionar miembros de grupos multicast en IPv4.

El valor en el encabezado de IPv6, para que la opción Next Header indique que continúa ICMPv6 es el 58, y a diferencia del IPv4 este protocolo se debe implementar en todos los hosts de la red y permitírsele el paso a través de los routers, ya que de ese paso depende que los equipos con IPv6 se puedan reconocer.

ICMPv6 utiliza dos tipos de mensajes, estos son: mensajes de error y mensajes de información y es llevado al final de las cabeceras de extensiones del encabezado de IPv6, además, se compone de 4 campos definidos, estos son:

1. Campo Tipo: Identifica el tipo de mensaje ICMP.
2. Campo Código: Detalles específicos del tipo de mensaje.

3. Campo Checksum: Valor resultante del procesamiento completo del paquete ICMP para que el destino pueda verificar la integridad del paquete.
4. Campo Datos: Datos enviados que el destino utiliza para tareas de diagnóstico y operación.

A continuación, la estructura en forma gráfica:

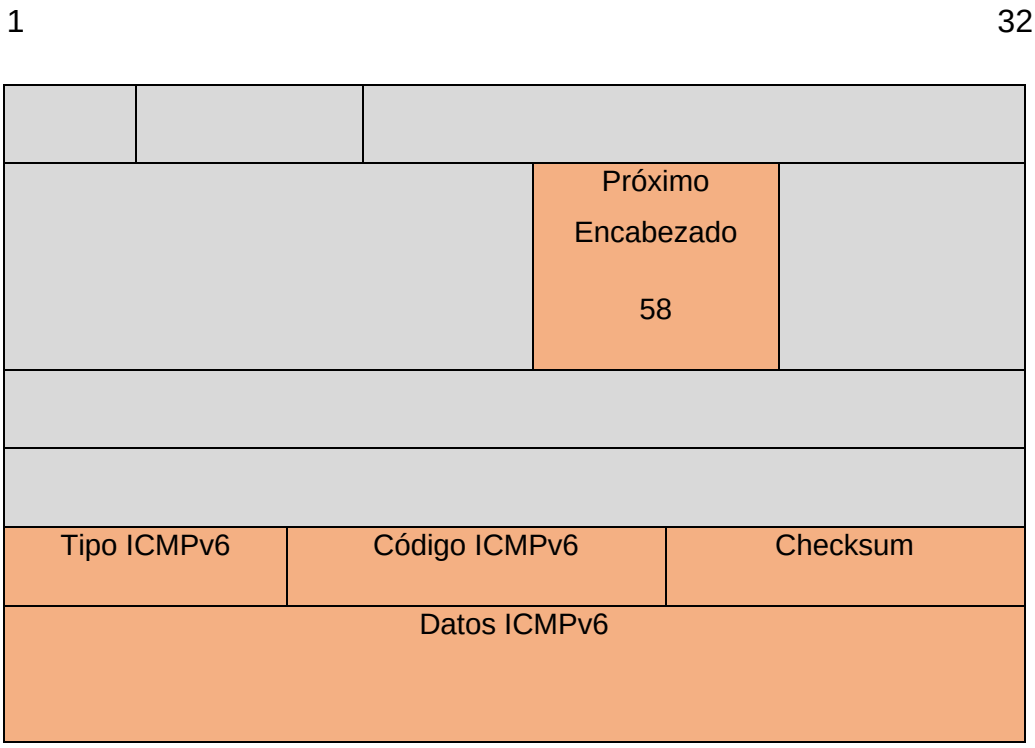


Figura 16. Estructura ICMPv6

2.5.1 Procedimientos de ICMPv6

El ICMPv6, es muy importante, ya que contiene una serie de procedimientos que permiten el uso del protocolo IPv6 en las redes. Los procedimientos son los siguientes:

- **Path MTU Discovery (PMTUD)**

La fragmentación de paquetes que se presentaba en IPv4, se reemplaza por el descubrimiento de MTU de la ruta. PMTUD permite que el emisor emita paquetes utilizando el MTU de su interfaz y si en la ruta del paquete existe un MTU de menor tamaño le responde con un mensaje de ICMPv6 tipo 2, que se denomina PACKET TOO BIG indicando el tamaño de su MTU, por lo que el emisor ajusta el tamaño de su paquete al MTU menor. Si se bloquea ese tipo de mensajes no se puede realizar la negociación descrita, una posibilidad para lidiar con esta situación es activar siempre que se pueda, la opción denominada “Garanteed Not To Be Too Big” que genera paquetes de tamaño mínimo (1280 bytes) para IPv6, evitando con esto utilizar el PMTUD.

- **Neighbor Discovery (ND)**

Al no existir ARP (Address Resolution Address) en IPv6 el ND asume esa operación, la cual le permite a un host IPv6 lo siguiente:

- ✓ Obtener direcciones de capa de enlace de los vecinos.
- ✓ Encontrar los routers en la ruta.
- ✓ Detectar los hosts vecinos que utilizan IPv6.
- ✓ Evita la renumeración.

Para la ejecución de este procedimiento ICMPv6 utiliza el siguiente conjunto de mensajes:

- ✓ Tipo 133: Router Solicitation.
- ✓ Tipo 134: Router Advertisement.
- ✓ Tipo 135: Neighbor Solicitation.
- ✓ Tipo 136: Neighbor Advertisement.
- ✓ Tipo 137: Redirect Message.

El descubrimiento de vecinos es una operación fundamental para la comunicación de extremo a extremo que pretende IPv6, basándose en utilizar

direcciones multicast específicas denominadas “solicited-node” y se ejecutan en la red local ya que son de alcance local.

- **Autoconfiguración stateless**

La autoconfiguración sin presencia de un servidor en la red es una de las características principales de IPv6 y está basado en la operacionalidad del ICMPv6, los routers envían paquetes de tipo 134 anunciando con esto su presencia en la red y los hosts utilizan ese mensaje para aprender los prefijos /64 y generar automáticamente el ID de interfaz para completar la dirección IPv6.

Al arrancar una interface de red, envía un mensaje ICMPv6 de tipo 133 pidiendo información de algún router disponible en la red, este proceso permite tener una red de IPv6 sin necesidad de tener un servidor DHCPv6, así como numerar masivamente hosts con IPv6.

- **Duplicated Address Detection (DAD)**

Este procedimiento utiliza paquetes de tipo 135 durante la autoconfiguración para verificar si otro host ha utilizado la dirección que se pretende utilizar para no implementarla, se utiliza únicamente en el segmento local de red.

- **Neighbor Redirect**

Es utilizado por el Gateway para redirigir los paquetes IPv6 a otro router que estuviera presente en el segmento de red que tiene mejor ruta de salida, utiliza paquetes de tipo 137, esta función pone en riesgo la seguridad de la red, por lo que se recomienda desactivarla.

- **Renumeración**

Los paquetes de tipo 134, permiten desarrollar procesos de renumeración automáticos en la red IPv6 que aplican la autoconfiguración de tipo stateless, permitiendo anunciar 2 prefijos dentro de la misma red, denominados válido y

preferido, estableciendo un período de tiempo para el prefijo válido y así lograr una migración gradual hacia el prefijo preferido.

- **Mensajes de eco**

Al igual que en IPv4 el programa ping está presente para saber si un host está presente en la red, son paquetes de tipo 128 (Echo Request) y 129 (Echo Reply).

El ICMPv6 podría denominarse la columna vertebral del IPv6, ya que permite la conexión, el descubrimiento y la autoconfiguración de los hosts, por lo que al desplegar una red en IPv6 no se debe bloquear como se hacía anteriormente en IPv4.

<table>
<tr><td rowspan="2">  </td><td>Actividad de Aprendizaje N° 13</td></tr>
<tr><td>Analice cuidadosamente las funciones de:
✓ ICMPv6 similares con el ICMP versión 4
✓ procedimiento DAD?
✓ campo checksum en el ICMPv6

¿Cuáles son los dos tipos de mensajes que maneja ICMPv6?</td></tr>
</table>

2.6. ACTIVIDADES DE AUTOEVALUACIÓN DEL CAPITULO 2

2.6.1. Marque una equis sobre la opción u opciones correctas

1. Una dirección IPv6 está compuesta por 8 bloques de 4 dígitos en formato hexadecimal, a partir de la siguiente secuencia de números binarios obtenga la dirección IPv6 siguiendo los tres pasos vistos en el punto 1.2 del capítulo 2. No acorte la dirección resultante.

    a) 0010001000000101000001000010010100000010000000000000000010000001010101111000100110111101011101000101111110001011100000001011111001

    b) 0010011000100101000101000010010100000000000000000000000000000000101010011100011011011010101110100010001111001111110000011101111101

2. Resuma las siguientes direcciones IPv6 según lo estudiado en el capítulo 2.

    a. 2001:424:0000:0000:bf93:0b69:b007:179

    b. 2001:0365:0FFF:ABCD:0093:7b00:bf00:AF

    c. 2002:0000:0:0:0:9:bf00:CAFÉ

    d. 2001:0000:0000:0000:0000:0000:00000:10A0

3. ¿Cuántos bits en cero representa el símbolo “:”?

    a. 2015::1234:acbd:1

    b. 2001:bd1::café:ace0:12

    c. 2001::1

    d. 2002:123::1

4. En el capítulo 2 se explica para que se utiliza y como se efectúa el proceso EUI-64. Utilizando las siguientes direcciones MAC realice el proceso EUI-64, presentando todo el proceso ejecutado:

   a. 7845A2101103
   b. 7845AFEA1222
   c. 56251245FFA1
   d. C8C6A1AB1234

5. Según la clasificación de los modos en que operan las direcciones IPv6, cuáles son los 3 tipos principales.

6. Según los modos de la pregunta anterior, ¿qué tipo de dirección IPv6 representan los siguientes prefijos?

   a. FE80:000:0000:1234:ABCD:
   b. FC00::/7
   c. ::FFFF:ACBD:1234
   d. 2001:bd1:1000::1

2.6.2. ORDENAMIENTO

Según la RFC 2460, cuando exista más de una cabecera de extensión, éstas deben llevar un orden. Aplicando lo anterior, ordene en forma ascendente los números que representan las cabeceras de la columna de la izquierda, en los paréntesis de la columna de la derecha.

CABECERAS	ORDENADO
1. Cabecera de Fragmentación	( )
2. Cabecera de Opciones de Destino para el primer destino	( )
3. Cabecera de autenticación	( )
4. Cabecera de capa superior	( )
5. Cabecera de Enrutamiento	( )
6. Cabecera de Opciones Hop-by-Hop	( )
7. Cabecera IPv6	( )
8. Cabecera de carga útil	( )
9. Cabecera de Opciones de Destino para el destino final del paquete	( )

2.6.3. EMPAREJAMIENTO

Según lo leído en el capítulo 2 del ICMPv6, relacione los conceptos de la columna de la izquierda con las descripciones que corresponden en la columna de la derecha.

CONCEPTOS		OPCIONES
10. Renumeración	( )	Es utilizado por el Gateway para redirigir los paquetes IPv6 a otro router que estuviera presente en el segmento de red que tiene mejor ruta de salida
11. Mensajes de eco	( )	La fragmentación de paquetes que se presentaba en IPv4, se reemplaza por el descubrimiento de MTU de la ruta.
12. Neighbor Redirect	( )	Está para saber si un host está presente en la red, son paquetes de tipo 128 (Echo Request) y 129 (Echo Reply).
13. Autoconfiguración stateless	( )	Este procedimiento utiliza paquetes de tipo 135 durante la autoconfiguración para verificar si otro host ha utilizado la dirección que se pretende utilizar
14. Path MTU Discovery (PMTUD)	( )	La autoconfiguración sin presencia de un servidor en la red es una de las características principales de IPv6 y está basado en la operacionalidad del ICMPv6
15. Duplicated Address Detection (DAD)	( )	Al no existir ARP (Address Resolution Address) en IPv6 el ND asume esa operación.
16. Neighbor Discovery (ND)	( )	Los paquetes de tipo 134, permiten desarrollar procesos de renumeración automáticos en la red IPv6 que aplican la autoconfiguración de tipo stateless, permitiendo anunciar 2 prefijos dentro de la misma red.