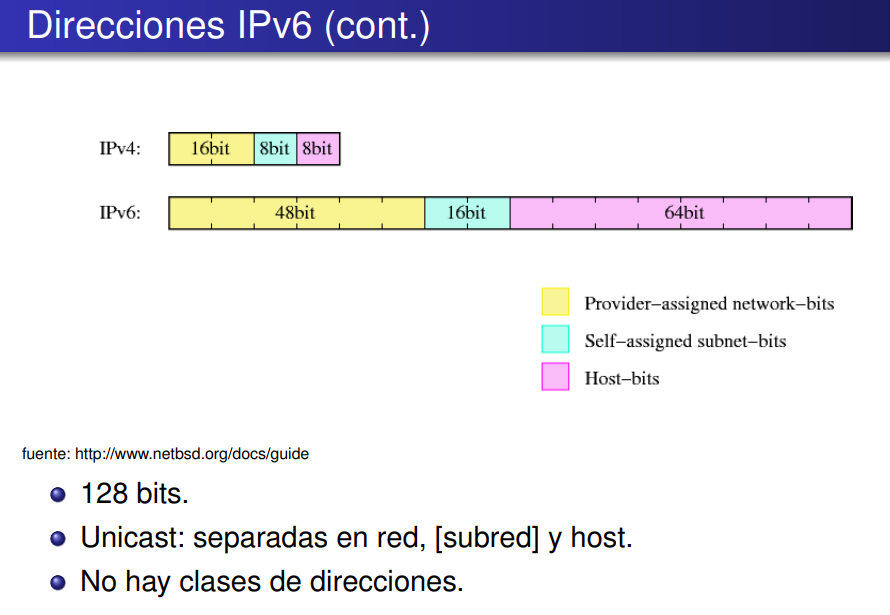
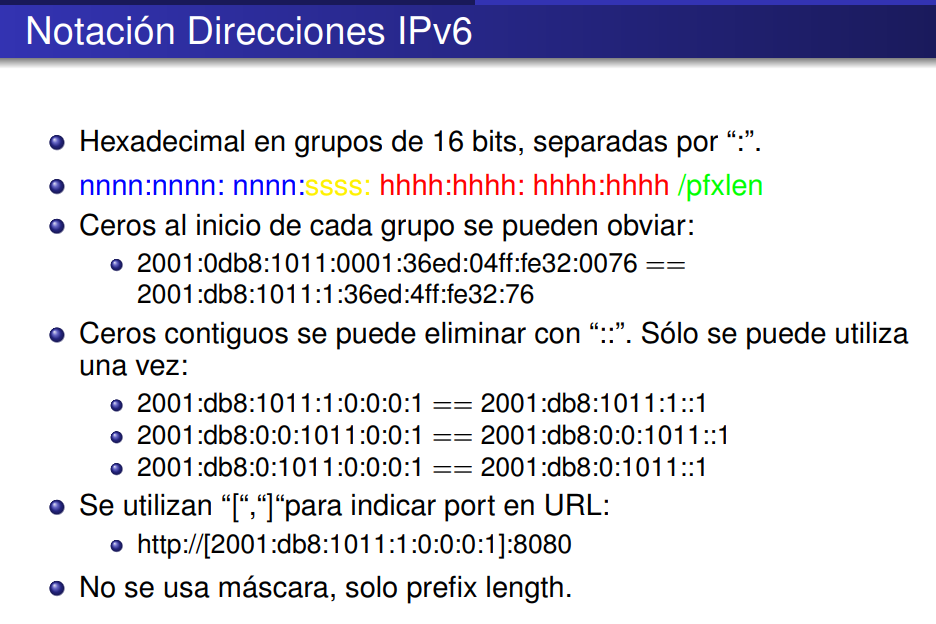
**Práctica 9  
Capa de Red - IPv6**

**IPv6**

**Introducción**

****

****

**1. ¿Qué es IPv6? ¿Por qué es necesaria su implementación?**

A principios de la década de 1990, el Internet Engineering Task Force comenzó a desarrollar un sucesor para el protocolo IPv4. La principal motivación de esta iniciativa fue que se dieron cuenta de que el espacio de direcciones IP de 32 bits estaba comenzando a agotarse, a causa de las nuevas subredes y nodos IP que estaban conectándose a Internet (a los que se les estaban asignando direcciones IP únicas) a una velocidad sobrecogedora. Para responder a esta necesidad de un espacio de direcciones IP más grande, se desarrolló un nuevo protocolo IP, el protocolo IPv6. Los diseñadores de IPv6 también vieron aquí la oportunidad de ajustar y aumentar otros aspectos de IPv4, basándose en la experiencia acumulada sobre el funcionamiento de IPv4.

Este agotamiento de direcciones IPv4 generó un conjunto de mecanismos para poder seguir

agregando subredes a la Internet. Por ejemplo, NAT y NAPT, con los cuales se perdía el

principio end-to- end del protocolo IP.

Problemas de IPv4:

- Direcciones IPv4 no disponibles, uso de NAT.

- Tablas de ruteo muy grandes en el backbone de Internet.

- Congestión en los routers, demasiado procesamiento.

Otras cuestiones no contempladas desde el inicio:

- Seguridad a nivel L3, IP.

- Extensiones al modelo de Calidad de Servicio (QoS).

- Fácil auto-configuración y re-numeración de direcciones.

- Movilidad a nivel de red no contemplada en el diseño del protocolo.

**Es importante decir que IPv4 e IPv6 no son versiones del mismo protocolo, sino que son protocolos diferentes.**

Beneficios de IPv6:

-Mayor espacio de direcciones

- 128 bits: 340.282.366.920.938.463.463.374.607.431.768.211.456 direcciones.

-Formato de cabecera simplificado. Menor overhead de procesamiento.

-Ordenar las tablas de enrutamiento.

-Conectar todo, usar auto-configuración de direcciones (plug and play).

-Arquitectura de red jerárquica para un ruteo eficiente.

-Seguridad a nivel IP (IPSec obligatorio).

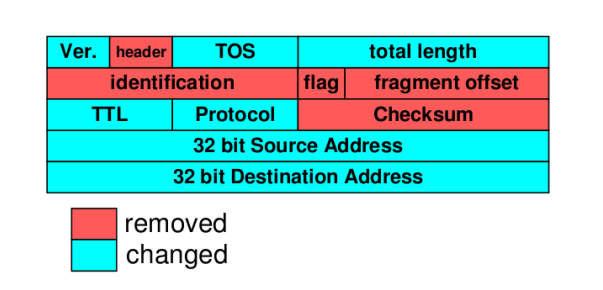
-Jumbogramas, size(datagrama) > 64KB.

-Movilidad y más direcciones de multicast.

**2. ¿Por qué no es necesario el campo Header Length en IPv6?**

Porque IPv6 tiene una cabecera de 40 bytes simplificada. Algunos de los campos de IPv4 se han eliminado o se han hecho opcionales. La cabecera de longitud fija de 40 bytes permite un procesamiento más rápido del datagrama IP. Una nueva codificación de las opciones permite un procesamiento más flexible de las mismas. Es decir, la eliminación del campo opciones que fue reemplazado por cabeceras adicionales y opcionales, permitió tener una **cabecera de IPv6 de 40 bytes fijos (no incluye el campo “Header length”, el cual era necesario en IPV4. En IPV4 era necesario porque el header era variable, por su campo opciones, y por eso era necesario especificar la longitud del header)**.

Cambios en IPV6 respecto a IPV4:



Comparación de cabeceras de IPV4 e IPV6



**3. ¿En qué se diferencia el checksum de IPv4 e IPv6? Y en cuánto a los campos checksum de TCP y UDP, ¿sufren alguna modificación?**

En IPv6 se eliminó. Y se delegó a la capa de transporte. En UDP, con esta modificación, la funcionalidad de comprobación de errores será obligatoria.

Suma de comprobación (checksum) de cabecera. Puesto que los protocolos de transporte (Ej. TCP y UDP) y de la capa de enlace de datos (ej. Ethernet) en las capas de Internet realizan sumas de comprobación, los diseñadores de IP probablemente pensaron que esta funcionalidad ya era suficientemente redundante en la capa de red y podía eliminarse. Una vez más, el procesamiento rápido de los paquetes IP era la preocupación principal. En IPv4 dado que la cabecera tiene un campo TTL (similar al campo límite de saltos de IPv6), la suma de comprobación de la cabecera de IPv4 necesitaba ser calculada en cada router. Al igual que la fragmentación y el reensamblado, esta también era una operación muy costosa en IPv4.

Entonces, IPv6 no implementa protección de integridad ya que asume que esta protección se realiza en los protocolos de transporte de capa superior como UDP o TCP, esto mejora la performance de IPv6 por sobre el protocolo versión cuatro. IPv4 si implementaba este campo y la suma debía ser recalculada cada vez que campos como el TTL cambiaba (basicamente en cada salto).

Los campos checksum de TCP y UDP no deben cambiar nada en la protección de integridad checksum.

**4. ¿Es necesario el protocolo ICMP en IPv6? ¿Cumple las mismas funciones que en IPv4?**

En IPv6 si es necesario (en IPv4 no).

Los nodos IP utilizan el protocolo ICMP para informar de condiciones de error y proporcionar información limitada (por ejemplo, la respuesta de eco de un mensaje ping) a un sistema terminal.

En el documento RFC 4443 se ha definido una nueva versión de ICMP para IPv6. Además de reorganizar las definiciones de tipos y códigos ICMP existentes, ICMPv6 también añadió nuevos tipos y códigos requeridos por la nueva funcionalidad de IPv6, entre los que se incluyen el tipo “Paquete demasiado grande” y el código de error “Opciones IPv6 no reconocidas”. Además, ICMPv6 incluye la funcionalidad del Protocolo de gestión de grupos de Internet (IGMP, Internet Group Management Protocol) que se emplea para gestionar el modo en que un host se une a un grupo de multidifusión y lo abandona, anteriormente era un protocolo separado de ICMP en IPv4.

Resuelve: Multicast Listener Discovery (MLD), reemplazo de IGMP. Neighbor Discovery Protocol (NDP), reemplazo de ARP y mensajes Router Discovery, Redirect. Mensajes de control de ICMP: informativos (ping), errores.

**5. Transforme las siguientes direcciones MACs en Identificadores de Interfaces de 64 bits.**

* **00:1b:77:b1:49:a1**
* **e8:1c:23:a3:21:f4**

Esto se hace porque la computadora puede calcular su dirección IPv6 local a partir de

su MAC (*es un identificador de 48* [*bits*](https://es.wikipedia.org/wiki/Bit) *(6 bloques de dos caracteres* [*hexadecimales*](https://es.wikipedia.org/wiki/Sistema_hexadecimal)*(4 bits)) que corresponde de forma única a una* [*tarjeta o dispositivo de red*](https://es.wikipedia.org/wiki/Tarjeta_de_red)*. Se la conoce también como* ***dirección física****, y es única para cada dispositivo*). Con esa dirección ya pueden tener una comunicación en la red con los hosts de la misma red (no pueden salir a Internet).

Una dirección de enlace-local es una dirección IP creada únicamente para comunicaciones dentro de una subred local. Los routers no enrutan paquetes con direcciones de enlace local.

Las direcciones de enlace local se asignan usando los procedimientos de stateless address autoconfiguration para Internet Protocol versión 4 (IPv4) e IPv6.​ **En IPv4, las direcciones de enlace local pueden usarse cuando no hay disponible un mecanismo externo de configuración de direcciones, tal como DHCP, u otro mecanismo principal de configuración ha fallado. En IPv6, las direcciones de enlace local son necesarias para el funcionamiento interno de varios componentes del protocolo.**

Las direcciones de enlace local para IPv4 están definidas en el bloque 169.254.0.0/16. En IPv6, están reservadas con el prefijo fe80::/64.

Proceso EUI-64

El IEEE definió el identificador único extendido (EUI) o proceso EUI-64 modificado. Este proceso utiliza la dirección MAC de Ethernet de 48 bits de un cliente e introduce otros 16 bits en medio de la dirección MAC de 48 bits para crear una ID de interfaz de 64 bits.

Las direcciones MAC de Ethernet, por lo general, se representan en formato hexadecimal y constan de dos partes:

* Identificador único de organización (OUI): el OUI es un código de proveedor de 24 bits (seis dígitos hexadecimales) que asigna el IEEE.
* Identificador de dispositivo: el identificador de dispositivo es un valor único de 24 bits (seis dígitos hexadecimales) dentro de un OUI común.
* Las ID de interfaz EUI-64 se representan en sistema binario y constan de tres partes:
* OUI de 24 bits de la dirección MAC del cliente, pero el séptimo bit (bit universal/local, U/L) se invierte. Esto significa que si el séptimo bit es un 0, se convierte en 1, y viceversa.
* Valor de 16 bits FFFE introducido (en formato hexadecimal)
* Identificador de dispositivo de 24 bits de la dirección MAC del cliente

En la figura 1, se ilustra el proceso EUI-64, con la siguiente dirección MAC de GigabitEthernet de R1: FC99:4775:CEE0.

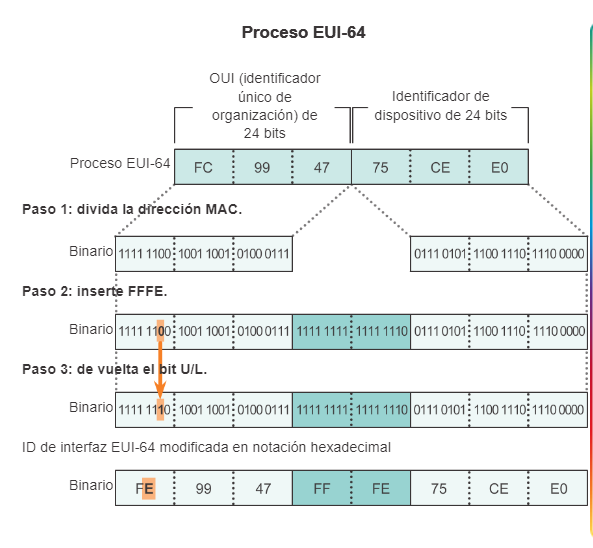
* Paso 1: Dividir la dirección MAC entre el OUI y el identificador de dispositivo
* Paso 2: Insertar el valor hexadecimal FFFE, que en formato binario es: 1111 1111 1111 1110
* Paso 3: Convertir los primeros dos valores hexadecimales del OUI a binario e invertir el bit U/L (séptimo bit) En este ejemplo, el 0 en el bit 7 se cambia a 1.

→ El resultado es una ID de interfaz de FE99:47FF:FE75:CEE0 generada mediante EUI-64.

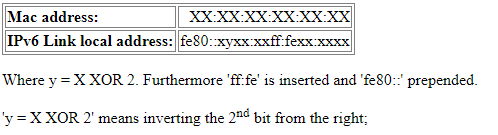
Nota: el uso del bit U/L y los motivos para invertir su valor se analizan en RFC 5342.

La ventaja de EUI-64 es que se puede utilizar la dirección MAC de Ethernet para determinar la ID de interfaz. También permite que los administradores de red rastreen fácilmente una dirección IPv6 a un dispositivo final mediante la dirección MAC única. Sin embargo, esto generó inquietudes con respecto a la privacidad a muchos usuarios. Les preocupa que los paquetes puedan ser rastreados a la PC física real. Debido a estas inquietudes, se puede utilizar en cambio una ID de interfaz generada aleatoriamente.

Figura:



**Resumen del procedimiento:**

****

**Resolución del ejercicio:**

* **Transformo 00:1b:77:b1:49:a1**

En IPV6 las direcciones de enlace local tienen la forma FE80::X/64

Paso 1 → Dividir la dirección MAC entre el OUI y el identificador de dispositivo

OUI → 00:1b:77 → 00000000:00011011:01110111

ID → b1:49:a1 → 10110001:01001001:10100001

Paso 2 → Insertar el valor hexadecimal FFFE, que en formato binario es: 1111 1111 1111 1110

00000000:00011011:01110111:1111:1111:1111:1110:10110001:01001001:10100001

Paso 3 → Convertir los primeros dos valores hexadecimales del OUI a binario e invertir el bit U/L (séptimo bit)

00000010:00011011:01110111:1111:1111:1111:1110:10110001:01001001:10100001

Resultado final en hexadecimal: FE80::**2**1b:77ff:feb1:49a1/64

**Transformo e8:1c:23:a3:21:f4**

En IPV6 las direcciones de enlace local tienen la forma FE80::X/64

Paso 1 → Dividir la dirección MAC entre el OUI y el identificador de dispositivo

OUI → e8:1c:23 → 11101000:00011100:00100011

ID → a3:21:f4 → 10100011:00100001:11110100

Paso 2 → Insertar el valor hexadecimal FFFE, que en formato binario es: 1111 1111 1111 1110

11101000:00011100:00100011:1111:1111:1111:1110:10100011:00100001:11110100

Paso 3 → Convertir los primeros dos valores hexadecimales del OUI a binario e invertir el bit U/L (séptimo bit)

11101010:00011100:00100011:1111:1111:1111:1110:10100011:00100001:11110100

Resultado final en hexadecimal: FE80::e**a**1c:23ff:fea3:21f4/64

**6. ¿Cuál de las siguientes direcciones IPv6 no son válidas?**

**2001:0:1019:afde::1**

**2001::1871::4 - :: solo se puede usar una vez**

**3ffg:8712:0:1:0000:aede:aaaa:1211 - Algunos 0 abreviados y otros no. G no válida.**

**3::1**

**::**

**2001::**

**3ffe:1080:1212:56ed:75da:43ff:fe90:affe**

**3ffe:1080:1212:56ed:75da:43ff:fe90:affe:1001**

[**https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-overview-10/index.html**](https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-overview-10/index.html)

[**http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6**](http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6)

**7. ¿Cuál sería una abreviatura correcta de 3f80:0000:0000:0a00:0000:0000:0000:0845?**

* **3f80::a00::845 - :: mas de una vez.**
* **3f80::a:845 - No se representan :0000:0000:0000:. Además, se sacan 0 a la derecha de a, lo cual no representa al mismo número.**
* **3f80::a00:0:0:0:845:4567 - Se agregan nuevos bits**
* **3f80:0:0:a00::845**
* **3f8:0:0:a00::845 - Se saca un 0 a la derecha. No representa al mismo número.**

**8. Si quisiese que IPv6 soporte una nueva funcionalidad, ¿cómo lo haría?**

Habría que basarse las cabeceras opcionales (campo Next Header, que indica el tipo del siguiente header) para extender el protocolo IPv6. Pero previamente, habría que desarrollar un RFC y que este se apruebe como estándar (para que lo implementen todos los dispositivos que soportan IPv6). O implementarlo dentro de todos los dispositivos del sistema autónomo (pero solo funcionaría dentro de este).

**Info extra:**

En la cabecera de IPv4, después de los campos de información general y de las direcciones de origen y destino, y antes de los datos, se coloca en campo de "Opciones".

Estas "Opciones" ocupan un máximo de 40 bytes y dan indicaciones a los nodos que se encuentran en el camino (o path) que va del equipo origen al destino, acerca de cuestiones relacionadas con seguridad, enrutamiento, timestamping, etc. Concretamente, las opciones disponibles en IPv4 son:

•Crear un registro de la ruta.

En el datagrama se van guardando las direcciones IP de los routers visitados. Cada router intenta poner su dirección al final de la lista existente. Si la lista está llena y no puede hacerlo, simplemente reenvía el datagrama sin añadir su dirección.

•Marcas de tiempo (Timestamp).

•Seguridad básica del Departamento de Defensa.

Permite asegurar que el origen del datagrama tiene autorización para ser transmitido. Son opciones usadas por la NSA, la CIA...

•Seguridad extendida del Departamento de Defensa.

Es una opción que permite a los departamentos antes mencionados hacer configuraciones de seguridad específicas según sus necesidades.

•Sin operación (No Operation).

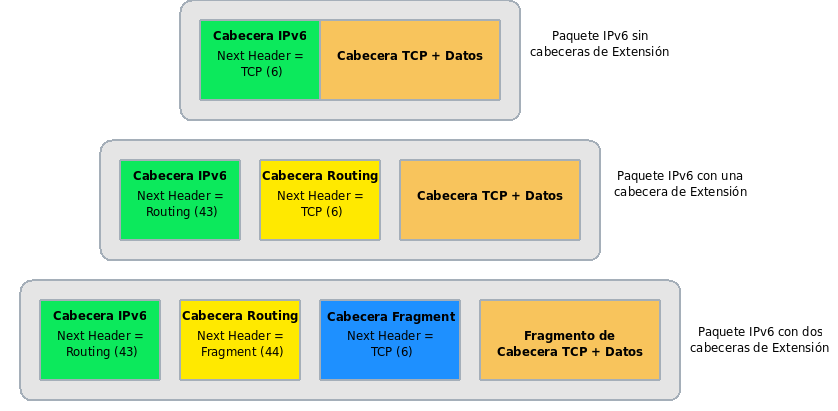
Se usa como relleno entre opciones, para alinear la siguiente opción en un marco de 16 o 32 bits.

•Fin de la lista de opciones.

En este caso se pretende rellenar el final del campo de opción para que el tamaño total sea múltiplo de 32 bits.

En IPv4 no suelen utilizarse estas opciones porque ralentizan la transmisión.

⇨ En IPv6 las opciones se manejan por medio de las llamadas Cabeceras de Extensión (Extension Headers). Estas cabeceras se insertan en el paquete sólo si las opciones son necesarias.



* En el primer paquete hay una única cabecera IPv6 que precede a los datos de la capa superior de transporte.
* En el segundo paquete se ha insertado una tercera cabecera entre las dos anteriores. Ahora, la cabecera IPv6 indica que la siguiente cabecera es una cabecera de Extensión del tipo Routing, cuyo código identificativo es el 43 y que se utiliza para dar una lista de uno o más nodos que deben estar en la ruta seguida por un paquete.
* En el campo Next Header de esa cabecera de Routing se indica ya que a continuación van los datos de TCP.
* En el tercer paquete se ha insertado una cabecera más. En este caso es una cabecera de Extensión de Fragmento, cuyo código es el 44.
* Como se puede ver los campos Next Header de las distintas cabeceras mantienen la lógica explicada.
* Podemos enumerar ya algunas cuestiones generales relativas a las cabeceras de Extensión:
  + En un paquete IPv6 puede haber cero, una o más cabeceras de Extensión.
  + Estas cabeceras se sitúan entre la cabecera IPv6 y la cabecera del protocolo de la capa superior (capa de transporte).
  + Las cabeceras existentes deben ser procesadas en el orden exacto en que aparecen en la cabecera del paquete.
  + Cada cabecera de Extensión es identificada por el campo “Next Header” de la cabecera precedente.
  + Las cabeceras de Extensión son examinadas o procesadas solo por el nodo identificado en el campo dirección de Destino de la cabecera IPv6...
  + ... con una única excepción:
  + Si la cabecera de Extensión es del tipo Opciones Hop-by-Hop, la información que lleva debe ser examinada y procesada por cada uno de los nodos que se encuentran en la ruta del paquete.
  + Este tipo de cabecera debe seguir inmediatamente a la cabecera IPv6 y su valor de "Next Header" es 0.
  + Si en el campo "Dirección de destino" hay una dirección multicast, las cabeceras de Extensión serán examinadas y procesadas por todos los nodos que pertenezcan al grupo multicast.
  + La longitud de cada cabecera de Extensión es un múltiplo de 8 bytes de forma que, independientemente del número de ellas que se utilicen, siempre quedan alineadas.

**Tipos:** Los 6 tipos de cabeceras de Extensión que se definen en la RFC 2460 son:

* + De opción Hop-by-Hop (RFC 2460).

La información de esta cabecera debe ser examinada Salto-a-Salto, es decir, en cada uno de los nodos de la ruta que ha de seguir el paquete.

* + De enrutado (RFC 2460).

Se utiliza para dar una lista de uno o más nodos que deben estar en la ruta seguida por un paquete.

* + De fragmento (RFC 2460).

Un host IPv6 que quiere enviar un paquete a un destino IPv6 utiliza el llamado “Path MTU discovery” para determinar el tamaño máximo de paquete que se puede utilizar en el path hasta ese destino. Si el paquete que hay que enviar es más grande que el MTU soportado, el host origen fragmenta el paquete. Gracias a esta forma de actuar, la fragmentación se gestiona de extremo a extremo, liberando a los routers del path de este trabajo.

En caso de que el "Path MTU discovery" falle, se usará el valor mínimo de "Path MTU" en IPv6, 1280 bytes. El valor máximo es de 65536 bytes, en los cuales se incluye la carga o payload del datagrama y los 40 bytes de la cabecera.

* + De opciones de destino (RFC 2460).

Estas cabeceras llevan información que será procesada, exclusivamente, por el nodo de destino.

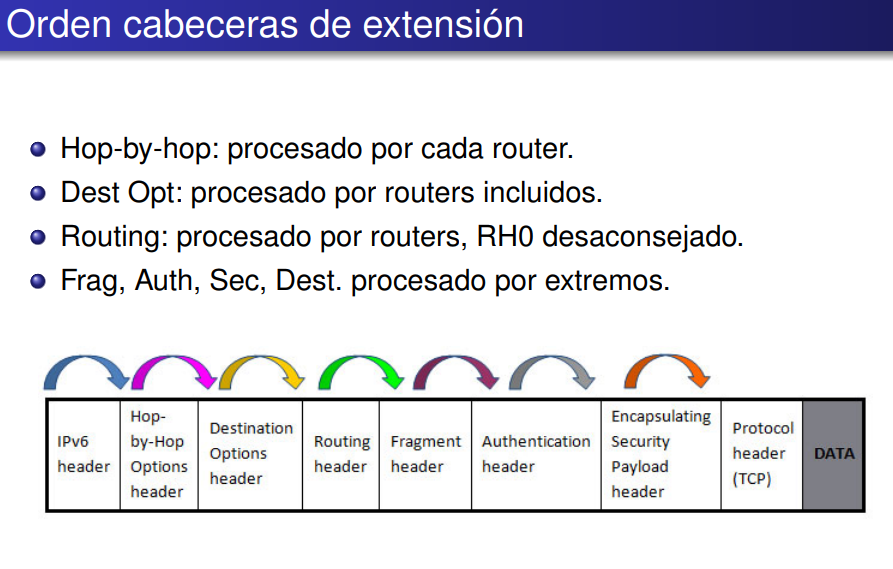
* + De autenticación (AH) (RFC 4302).

Proporciona integridad y autenticación (que no confidencialidad) para todos los paquetes de datos IP. Soporta distintos mecanismos de autenticación.

* + De carga útil de seguridad encriptada (Encrypted Security Payload =ESP) (RFC 4303)

Proporciona integridad, confidencialidad, autenticación de datos y otras funciones para todos los paquetes de datos IP.

⇨ La flexibilidad de esta arquitectura permitirá el desarrollo de nuevas cabeceras de Extensión en el futuro, a medida que sean necesarias. Lo bueno de este sistema es que las nuevas cabeceras de Extensión se pueden definir y usar sin cambiar la cabecera IPv6.



**9. Indique si las siguientes direcciones son de link-local, global-address, multicast, etc.**

Introducción

Las direcciones IPv6 se clasifican según las políticas de direccionamiento y encaminamiento más comunes en redes: direcciones unicast, anycast y multicast.

* Una dirección unicast identifica un único interfaz de red. El protocolo de Internet entrega los paquetes enviados a una dirección unicast al interfaz específico.
* Una dirección anycast es asignada a un grupo de interfaces, normalmente de nodos diferentes. Un paquete enviado a una dirección anycast se entrega únicamente a uno de los miembros, típicamente el host con menos coste, según la definición de métrica del protocolo de encaminamiento. Las direcciones anycast no se identifican fácilmente pues tienen el mismo formato que las unicast, diferenciándose únicamente por estar presente en varios puntos de la red. Casi cualquier dirección unicast puede utilizarse como dirección anycast.
* Una dirección multicast también es usada por múltiples interfaces, que consiguen la dirección multicast participando en el protocolo de multidifusión (multicast) entre los routers de red. Un paquete enviado a una dirección multicast es entregado a todos los interfaces que se hayan unido al grupo multicast correspondiente.

IPv6 no implementa direcciones broadcast. El mismo efecto puede lograrse enviando un paquete al grupo de multicast de enlace-local todos los nodos (all-nodes) ff02::1. Sin embargo, no se recomienda el uso del grupo all-nodes, y la mayoría de protocolos IPv6 usan un grupo multicast de enlace-local exclusivo en lugar de molestar a todos los interfaces de la red.

Una dirección IPv6 está formada por 128 bits.​ Las direcciones se clasifican en diferentes tipos: unicast, multicast y anycast. Cada uno de los tipos define valores específicos para subgrupos de los 128 bits, asociando dicho valor con las características especiales del tipo.

Ahora vamos a estudiar los tipos de direcciones IPv6 que existen dentro de la categoría Unicast:

* Link-Local
* Site-Local
* Global

→ Las direcciones **Link-Local** son el equivalente a las direcciones IP privadas en IPv4. Estas son asignadas a una interfaz de manera automática a partir del momento que activamos el protocolo IPv6 en un nodo.

El prefijo de estas direcciones es FE80::/10. Estas direcciones NO pueden ser encaminadas a través de los Routers fuera del segmento local, de ahí deriva su nombre. El propósito principal es proporcionar direccionamiento IP automático a los nodos en caso que NO exista un servidor DHCP.

Una dirección IPv6 Link-Local comienza con el prefijo FE80::/10 (los primeros 10 bits son los necesarios para formar el nº ff8, 1111 1111 10 | 00 0000 = 15 15 8 0 ), luego los bits del 11 hasta 64 (los siguientes 54 bits) se configuran con valores de ceros (0000). Los 54 ceros siguientes consiguen que el prefijo de red sea el mismo para todas las direcciones locales, y por tanto no enrutable.

De esta manera se forma la porción de red representada por los primeros 64bits.

FE80:0000:0000:0000:0000:0000:0000:0000/10

La porción de nodo, que son los últimos 64 bits, se forma con el formato EUI-64. El formato EUI-64 toma los 48 bits de la dirección MAC de la tarjeta Ethernet y le coloca 16 bits adicionales predefinidos por el protocolo IPv6 (FFFE). A continuación tenemos un ejemplo de una dirección Link-Local.

FE80::211:21FF:FE6C:C86B

→ Las direcciones IPv6 **Site-Local** son también el equivalente a las direcciones IP privadas en IPv4. A diferencias de las direcciones Link-Local, estas pueden ser encaminadas fuera del segmento local, es decir, podemos enviar paquetes entre diferentes segmentos de la red pero NO hacia el Internet.

En las direcciones Site-Local, los primeros 10 bits se establecen con los valores 1111111011, por lo tanto, el prefijo de estás direcciones tendrá un valor en hexadecimal de FEC0 :: /10. Los siguientes 54 bits están compuestos por el ID de red. Los últimos 64 bits son el identificador de la interfaz o nodo, y estos se configuran de la misma forma que las direcciones Link-Local, tomando 48 bits de la dirección MAC y luego agregando 16 bits con los valores FFFE.

A continuación tenemos un ejemplo de una dirección Site-Local.

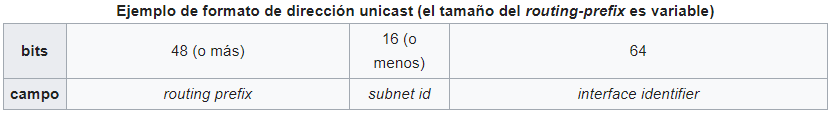
FEC0::CE00:3BFF:FE85:0

→ Las direcciones **Global** en IPv6 son el equivalente de las direcciones IP públicas en IPv4. Estas direcciones pueden ser encaminadas a través de la Internet. Los primeros 3 bits están compuestos por el valor 0010 (en notación binaria), por lo tanto, el prefijo de estás direcciones IP tendrá un valor en hexadecimal de 2xxx con una máscara /3.

Las direcciones Global son el tipo de dirección IPv6 más utilizado

Formato de dirección Unicast y Anycast

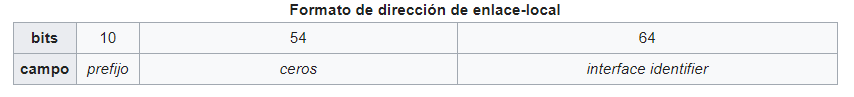
Las direcciones Unicast y anycast generalmente se dividen en dos grupos lógicos: los primeros 64bits identifican el prefijo de red, y son usados para encaminamiento; los últimos 64bits identifican el interface de red del host.



El prefijo de red (network prefix) (prefijo de encaminamiento o (routing prefix) junto con el identificador de subred o (subnet id)) está situado en los 64 bits más significativos de la dirección ipv6. El tamaño del routing prefix puede variar; un prefijo de mayor tamaño significa un tamaño menor para subnet id. El subnet id permite a los administradores de red definir subredes dentro de la red disponible.

Los 64 bits de identificador del interface (interface identifier) son generados automáticamente con la dirección MAC del interface y el algoritmo EUI-64 modificado, obtenidos de un servidor DHCPv6, establecidos aleatoriamente o asignados manualmente.

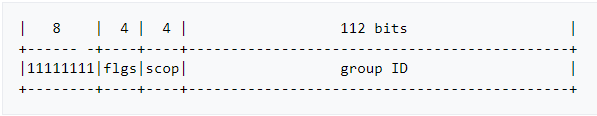
Una dirección de enlace-local es una dirección unicast, pero usando un valor específico para el network prefix.



El campo prefijo contiene el valor binario 1111111010 (fe80::/10).

Formato multicast

Según la RFC4291 en su sección 2.7, una dirección multidifusión en IPV6 es un identificador para un grupo de interfaces, (típicamente en diferentes nodos). Una interfaz puede pertenecer a varios grupos multidifusión. A continuación se muestra el formato de direccionamiento multidifusión para IPV6:



Los primeros dos dígitos hexadecimales son FF, esto es lo que caracteriza a las direcciones multidifusión en IPV6.

Notas HIstóricas

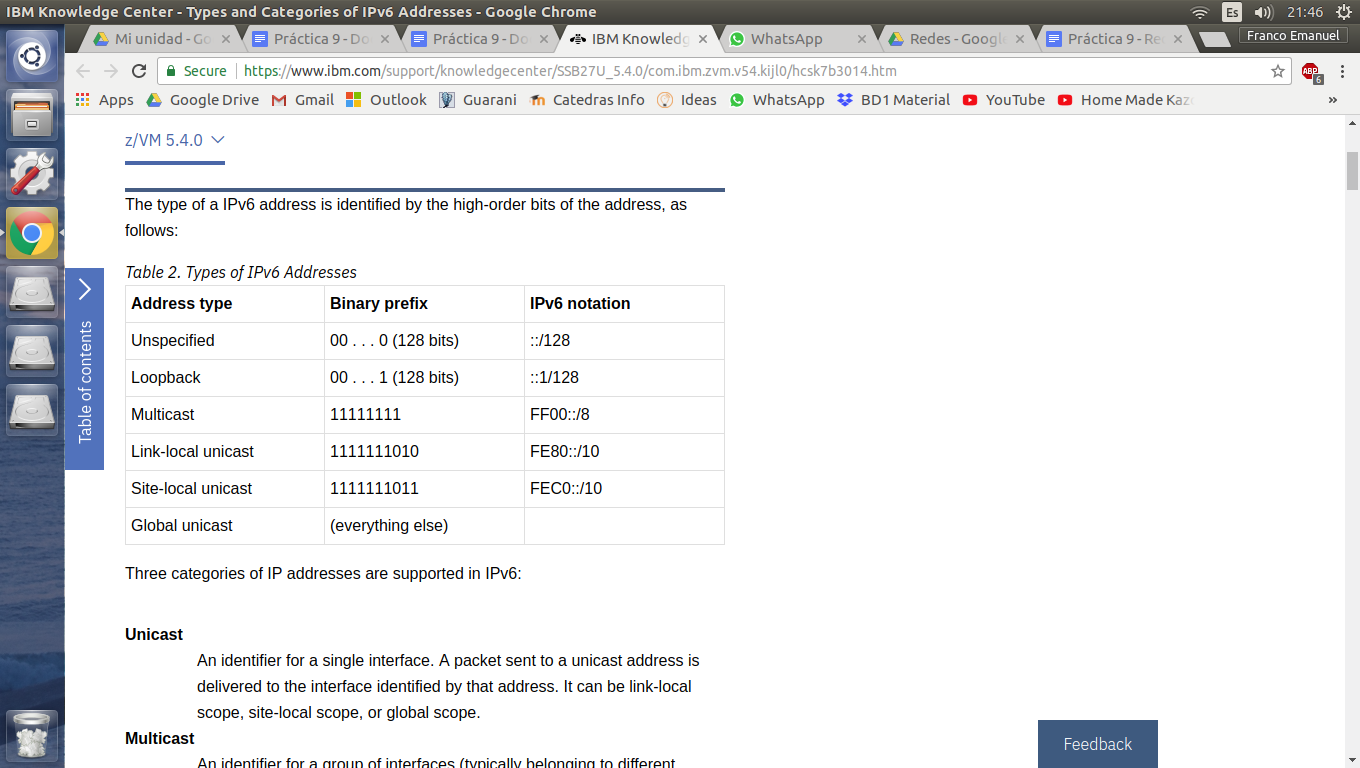
Se reservó el bloque de direcciones 3ffe::/16 para pruebas de la red 6bone en diciembre de 1998. Antes de eso se utilizaba el rango de direcciones 5F00::/8. Ambos rangos fueron liberados en junio de 2006, con la defunción del proyecto 6bone.

La red 6bone era una red IPv6 de carácter experimental creada para ayudar a los vendedores y usuarios a participar en la evolución y transición a IPv6. Su enfoque original fue la prueba de normas e implementaciones. Su objetivo principal era la realización de pruebas de procedimientos interoperacionales y transicionales.

**9. Indique si las siguientes direcciones son de link-local, global-address, multicast, etc.**

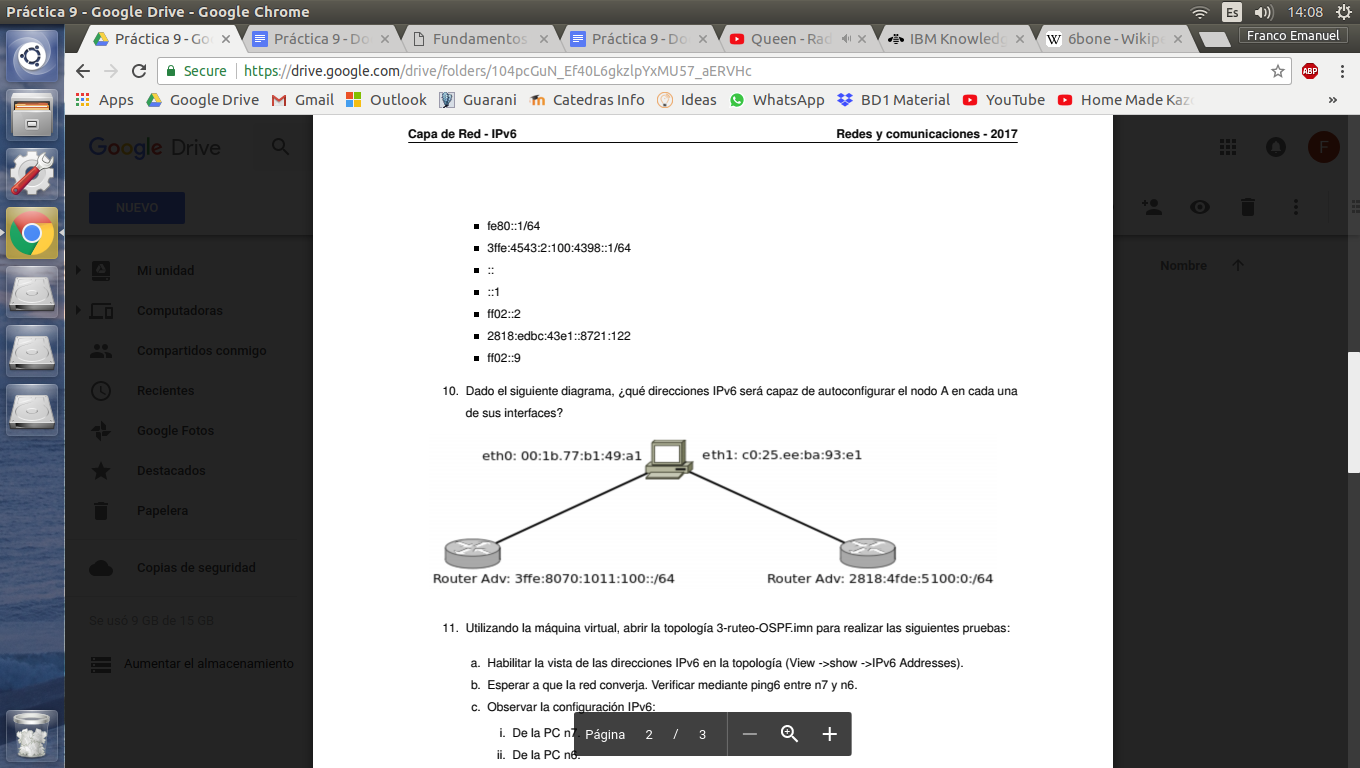
* **fe80::1/64 - Link-Local (fe80)**
* **3ffe:4543:2:100:4398::1/64 - 6bone (3ffe)**
* **:: - Unspecified**
* **::1 - Loopback**
* **ff02::2 - Multicast - link-local**
* **2818:edbc:43e1::8721:122 - Global unicast**
* **ff02::9 - Multicast - link-local**

Todo lo que empieza FF es multicast. El cero indica que es de tipo permanente. El dos indica el alcance de la dirección (LAN).



<https://www.ibm.com/support/knowledgecenter/SSB27U_5.4.0/com.ibm.zvm.v54.kijl0/hcsk7b3014.htm>

**10. Dado el siguiente diagrama, ¿qué direcciones IPv6 será capaz de autoconfigurar el nodo A en cada una de sus interfaces?**



La idea sería que el nodo A genere una dir local usando su MAC con el proceso EUI 64, luego como el router manda cada tanto sus redes (una por cada interfaz, en general son varias, aca manda una sola), concateno el prefijo de red a lo anterior.

* eth0) Primero genera la fe80::21b:77ff:feb1:49a1 /64. Recibe los prefijos de red y arma:

3ffe:8070:1011:100:21b:77ff:feb1:49a1 /64

* eth1) Primero genera la fe80::c225:eeff:feba:93e1 /64. Recibe los prefijos de red y arma:

2818:4fde:5100::c225:eeff:feba:93e1 /64

**NOTA**: CON IPV6 YA PRENDES TU MAQUINA Y TENES UNA DIR IP. CON IP V4 NO PASA ESTO, NECESITAS PEDIR MEDIANTE DHCP, Y BLA BLA BLA. ACA TAMBIEN PODRIAS USAR ACA ESE PROTOCOLO PERO COMO SE SABE COMPLEJO Y TENES ESTO, NI SE USA.

---------------------------------------------

En ipv6 pueden ser publicas. De tipo link local puede haber una sola creo