REDES DE NUEVA GENERACIÓN

TEMA 1

IP de nueva generación: IPv6

1º Introducción a IPv6

– IPv6 es un protocolo de nivel de red cuya principal función consiste en guiar los datagramas desde el equipo origen hasta el destino pasando por los diferentes routers intermedios. Sin embargo, el protocolo clásico IPv4 es más utilizado actualmente, aunque conlleva una serie de problemas:

- **Cantidad de direcciones:** IPv4 utiliza un total de 32 bits para el direccionamiento de todos los equipos en el mismo, sin embargo, peso a que esto se traduce en un total de mas de $4x10^9$ direcciones, con el paso de los años se han vuelto escasas para las demandas actuales.
  - Una de las soluciones actuales es implementar redes privadas mediante el uso del protocolo NAT. Esto hace que un gran números de host puedan estar conectado a través de una misma dirección pública.
  - Sin embargo, el uso de NAT ocasiona cuellos de botella entre las comunicaciones, rompe el esquema cliente-servidor al introducir un elemento intermedio que ejecuta la redirección de datagramas y no es compatible con IPv6 debido a que este tiene una capa de cifrado y el protocolo NAT necesita acceder al interior del datagrama para poder calcular el host destino.
- **Organización en clases:** La organización entre las distintas clases en IPv4 es muy ineficiente y provoca un gran desperdicio de direcciones. Esto se debe a las redes IPv4 de tipo A contienen un total de 16 millones de posibles direcciones host, las cuales no son ocupadas en su totalidad.
  - Para solucionar esto se implemento el estándar CIDR, el cual se basa en que las redes pueden especificar su máscara, permitiendo asignar un rango de direcciones más adecuado.
- **Formato de los datagramas:** El formato de las cabeceras de los datagramas IPv4 es muy complejo y contiene campos que no son utilizados. Por otra parte, la fragmentación de dichos datagramas cuando estos contienen un campo de datos demasiado largo hace que los encaminadores tengan que desarrollar más trabajo, siendo por lo tanto, mas lentos.
- **Seguridad:** IPv4 no fue diseñado para implementar ningún protocolo de seguridad nativo.
  - La solución fue crear e implementar el actual protocolo de seguridad IPSec.
- **Multicast:** Se han desarrollado protocolos multicast opcionales para IPv4, sin embargo, estos no han llegado a usarse de forma eficaz.

– El protocolo IPv6 pone fin a todos los problemas de IPv4 gracias a las siguientes características:

- IPv6 utiliza un total de 128 bits para para el direccionamiento de cada uno de los equipos, lo que significa un total de $3{,}4x10^{38}$ direcciones.
- El formato de las cabeceras es más largo pero mucho más sencillo, lo que conlleva una mayor velocidad de procesamiento en los encaminadores.
- El encaminamiento se produce de forma jerárquica, lo que conlleva que los encaminadores troncales únicamente necesiten conocer las redes pertenecientes a su zona geográfica. Esto hace que las tablas de dichos encaminadores sean mucho más pequeñas y por lo tanto más rápidos.
- Los equipos pueden autoconfigurar sus interfaces red cuando estos arrancan, lo cual hace que no se necesiten implementar protocolos de configuración inicial como DHCP. En el caso de que los parámetros elegidos por el equipo presente algún problema o ya estén en uso, esos serán actualizados a otros nuevos.
- Implementación de un soporte para la transmisión de tráfico en tiempo real (sobre todo pensado para servicios de streaming). En IPv4 existían campos con este fin pero no se han llegado a usar.
- IPv6 implementa medidas nativas de seguridad, como realizar un cifrado extremo a extremo del contenido enviado en el campo de datos de los datagramas.

2º Direccionamiento IPv6

2.1 Representación de las direcciones IPv6

– Las direcciones IPv6 están compuestas por 8 grupos de 16 bits (128 bits) representados en hexadecimal, separados por dos puntos.

8000:0567:0089:0000:0000:0123:4567:89AB

Prefijo Iden. Interfaz

– Para hacer que escribir estas direcciones sea más fácil, se utilizan las siguientes optimizaciones:

- Eliminamos los ceros que se encuentran a la izquierda de los demás números del grupo.

  ej: 8000:567:89:0:0:123:4567:89AB

- Cuando hay múltiples campos llenos de ceros y se encuentran juntos, eliminamos los ceros y los representamos con ::. Esto solo se puede utilizar una vez por cada dirección.

  ej: 8000:567:89::123:4567:89AB

– Para hacer que una dirección IPv4 se corresponda con las nuevas direcciones IPv6, se escriben los 6 primeros grupos (96 bits) a 0 y seguidos de la dirección IPv4. Esto se utiliza cuando un datagrama IPv4 tiene que pasar por una red IPv6.

ej: IPv4 = 5.6.7.8 IPv6 = 0:0:0:0:0:0:0506:0708 = ::506:708

– Los nodos que tienen registradas direcciones IPv4 e IPv6 pueden establecer una correspondencia entre las mismas. Para esto se escriben los 5 primeros grupos (80 bits) a 0, el grupo 6 (16 bits) se pone a 1 y por último se escribe la dirección IPv4:

ej: IPv4 = 5.6.7.8 IPv6 = 0:0:0:0:0:FFFF:0506:0708 = ::FFFF:506:708

2.2 Tipos de direcciones IPv6

– Las direcciones IPv6 son asignadas a las interfaces, aunque una misma interfaz puede tener asignada más de una dirección IPv6. Tipos de direcciones:

- **Unicast:** Identifica una única interfaz y un datagrama enviado a una dirección unicast solo puede entregarse a la interfaz con dicha dirección. Puede usarse como origen o destino.
- **Multicast:** Identifica a un conjunto de interfaces y un datagrama enviado a una dirección multicast se entrega a todas las interfaces con dicha dirección. Pueden ser usadas como destino.
- **Anycast:** Identifica un conjunto de interfaces y los datagramas enviados a una dirección anycast son entregados únicamente a una de todas las interfaces identificadas en dicho conjunto (normalmente se envía a la dirección más cercana desde el emisor, según el protocolo de encaminamiento utilizado). Pueden ser usadas solo como destino.

– Es importante determinar que en IPv6 no existen direcciones de destino broadcast debido a las brechas de seguridad derivadas del uso de las mismas.

2.3 Ámbitos y zona de las direcciones IPv6

– El ámbito de una dirección define donde es válida la misma, es decir, donde puede ser utilizada como dirección unicast o multicast. Las direcciones unicast tienen definidos tres posibles ámbitos:

- **Ámbito de enlace local:** La dirección solo es válida dentro del enlace donde esta conectada la interfaz de red del equipo, es decir, el ámbito no puede sobrepasar las puertas de enlace a las que esta conectada dicha interfaz.
- **Ámbito de sitio local:** La dirección solo es válida dentro de la red delimitada por el sitio. En este caso, el ámbito si puede sobrepasar la puerta de enlace a la que se encuentra conectada la interfaz.
- **Ámbito global:** La dirección es válida en todo internet.

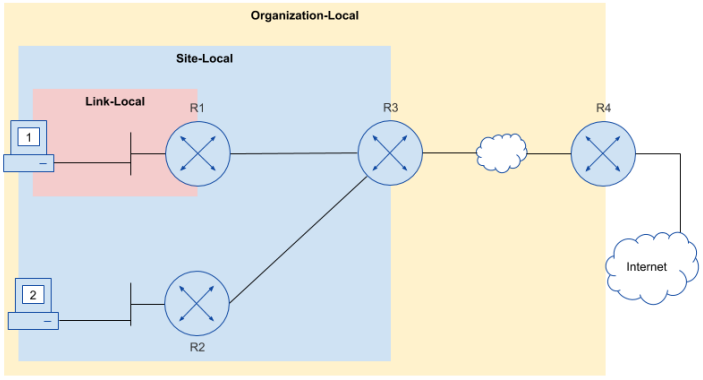
– Las direcciones multicast definen su ámbito mediante un campo de 4 bits situado en su cabecera, lo cual quiere decir que hay un máximo de 16 ámbitos, pero no todos están definidos. Algunos son:

- **2 (0010):** Ámbito de enlace local.
- **5 (0101):** Ámbito de sitio local.
- **E (1110):** Ámbito global.

Def. Se conoce como zona de un determinado ámbito a una región conexa donde la red de computadores que la conforma cumple con los requisitos de dicho ámbito.

– Un datagrama con direcciones origen o destino pertenecientes a un determinado ámbito nunca podrá alcanzar a una zona distinta a la cual fue generado. En el caso de que un datagrama contenga las direcciones de origen y destino pertenecientes a zonas distintas, será descartado en los encaminadores.

– Las zonas pertenecientes a distintos ámbitos están fuertemente ordenadas, es decir, si una interfaz pertenece a dos zonas donde el ámbito de una es mayor que el de la otra, entonces la zona de menor ámbito estará completamente incluida dentro de la zona de mayor ámbito (Sean las zonas X e Y con los correspondientes ámbitos X' e Y'. Si el ámbito X' es mayor que el ámbito Y', entonces $X \subseteq Y$).



– Una dirección IPv6 únicamente se corresponde con una sola zona. Las direcciones de ámbito inferior al global son ambiguas, esto quiere decir que dos máquinas que pertenecen a zonas distintas pueden tener una misma dirección IPv6 correspondiente a dicha zona a la que pertenecen.

– Esto no causa ningún problema por que los datagramas no pueden salir de la zona a la cual pertenece su dirección de origen. Sin embargo, los encaminadores deben saber también la zona a la cual pertenece la dirección destino de los datagramas que reciben.

2.4 Estructura de las direcciones IPv6

– Al contrario que IPv4, el cual únicamente posee dos niveles jerárquicos, el netid y el hostid, IPv6 permite una mayor cantidad de niveles, con el objetivo de facilitar las tareas de encaminamiento. Esto se conoce como Agregado de direcciones.

– Todas las direcciones IPv6, sean del tipo que sean, comienzan con un prefijo que indica el tipo de dirección que es. En la siguiente tabla se encuentran los prefijos que podemos encontrar:

Tipo de dirección	FP (binario)	FP (hexadecimal)
Reservada	0000 0000	00
Unicast Global Agregable	001	2 ó 3
Unicast Enlace Local	1111 1110 10	FE8
Unicast Sitio Local	1111 1110 11	FEC
ULA	1111 1101	FD
Multicast	1111 1111	FF

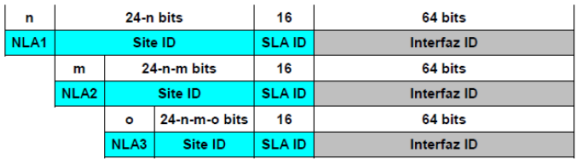
2.4.1 Direcciones Unicast Globales Agregables

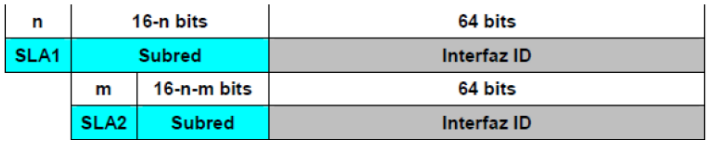
– Las direcciones globales son aquellas que tienen un ámbito sin límites y se utilizan en las máquinas conectadas a internet. Estas direcciones están administradas de forma jerárquica y existen 5 registros de máximo nivel, denominados RIR (Registros Regionales de Internet).

– El sistema de encaminamiento de direcciones IPv6 es jerárquico, de modo que únicamente viendo el prefijo de nuestra dirección IPv6 podemos saber cuales son nuestros proveedores del servicio. La red se encuentra formada por tres tipos de dispositivos:

- Proveedores de nivel superior (TLA).
- Proveedores regionales o similares (NLA).
- Redes de los distintos sitios (SLA)

– Los routers de nivel superior tienen en su tabla de rutas una entrada por cada uno de los TLA activos. Por otra parte, el diseño del espacio para las referencias hacia los NLA dentro de cada TLA es libre para cada router de nivel superior. La identificación de los SLA dentro de cada uno de los NLA ocurre de una manera similar.





– Las direcciones IPv6 son asignadas de manera automática por el proveedor y cuando cambiamos de proveedor únicamente cambia el prefijo de la misma. Esto de debido a que la dirección IPv6 asignada al equipo depende fuertemente de la topología de red.

– Las direcciones Unicast globales Agregables se crean con el objetivo de poder cambiar de proveedor sin tener que cambiar la numeración de una organización, y únicamente necesitar cambiar el prefijo asociado a dicho proveedor. Por este motivo se denominan agregables.

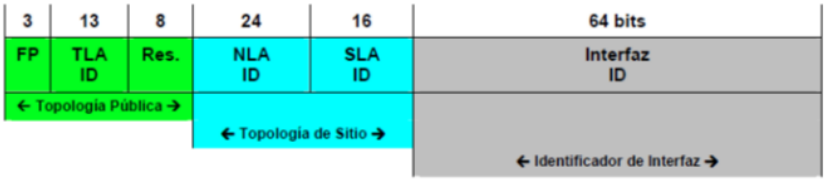
– Las direcciones globales pueden ser autoconfiguradas por el propio equipo, para lo cual, la máquina obtiene la parte del prefijo de red (primeros 64bits) del encaminador de su red, mientras que la parte del identificador de la interfaz (ultimos 64 bits) lo genera a partir de su propia dirección MAC, o bien se encuentra especificado en la configuración de forma permanente.

2.4.1.1 Estructura según RFC 2374

– La RCF 2374 define la estructura inicial que debían tener las direcciones IPv6 unicast globales. Esta estructura fue concebida para estar fuertemente ligada a la posición geográfica de las redes y facilitar los cambios en los proveedores de la misma con simplemente modificar una parte del prefijo.

– Estas direcciones estaban compuestas por los siguientes campos:

- **Topología pública (24 bits):**
  - **FP (3 bits):** Prefijo de la dirección (001 – 0x 2 o 0x 3).
  - **TLA ID (13 bits):** ID del identificador de agregación de nivel superior.
  - **Res (8 bits):** Campo reservado para un uso futuro que permitirá ampliar los TLA o los NLA.
- **Topología de sitio (40 bits):**
  - **NLA ID (24 bits):** ID del identificador de agregación de siguiente nivel (normalmente el pais).
  - **SLA ID (16 bits):** ID del identificador de agregación del nivel de sitio.
- **Identificador de la interfaz (64 bits):** Puede construirse de forma automática por el propio equipo mediante la dirección MAC o configurarse para que siempre obtenga la misma.

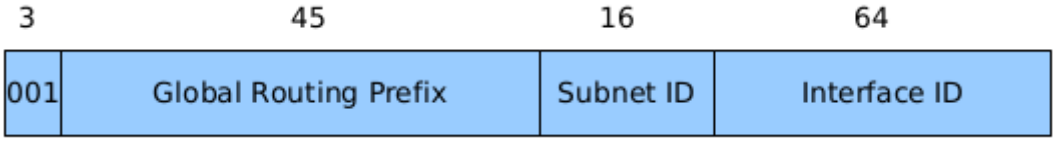


2.4.1.2 Estructura según RFC 3587

– La RFC 3587 fue instaurada en 2003 y reemplaza a la anterior definiendo una nueva estructura para las direcciones IPv6 unicast globales agregables. Este cambio fue debido a las presiones de las grandes compañías e intenta desligar la estructura de las direcciones de la posición geográfica de las mismas, logrando en su lugar que los proveedores puedan disponer de prefijos propios independiente de la posición de la red.

– Estas direcciones contienen la siguiente estructura:

- **Prefijo de red (64 bits):**
  - **FP (3 bits):** Prefijo de la dirección (001 – 0x 2 o 0x 3).
  - **Global Routing Prefix (45 bits):** Prefijo de la red con alcance global.
  - **Subnet ID (16 bits):** Subredes que conforman la red indicada por el campo anterior.
- **Identificador de la interfaz (64 bits):** Puede construirse de forma automática por el propio equipo mediante la dirección MAC o configurarse para que siempre obtenga la misma.



– Se recomienda asignar a los usuarios direcciones con un prefijo /48, de modo que estos puedan utilizar el campo los 16 bits correspondientes al campo *subnet ID* para configurar sus propias subredes.

2.4.2 Direcciones Unicast de Enlace Local

- Las direcciones Unicast de Enlace Local son direcciones privadas que pueden utilizarse en intranets no jerárquicas. Estas direcciones pertenecen a una zona de enlace local, luego nunca serán redirigidas hacia el exterior.

- Estas direcciones permiten realizar funciones de descubrimiento de vecinos y en Linux todas las interfaces de red se configuran de forma automática con una dirección unicast de enlace local.

- La estructura de estas direcciones es la siguiente:
  - **Prefijo de red (64 bits):**
    - **FP (10 bits):** Prefijo de la dirección (1111 1110 10 – 0x fe8).
    - **Prefijo restante (54 bits):** Los restantes 54 bits que componen el prefijo se ponen a 0.
  - **Identificador de la Interfaz (64 bits):** Puede construirse de forma automática por el propio equipo mediante la dirección MAC o configurarse para que siempre obtenga la misma.

ej: fe80:0000:0000:0000:3656:78ff:fe9a:bcde/64 = fe80::3656:78ff:fe9a:bcde/64

- Algunas de las direcciones IPv6 unicast locales reservadas son:
  - **::/128:** dirección no especificada (0.0.0.0 en IPv4).
  - **::1/128:** dirección de loopback (127.0.0.1 en IPv4)

2.4.3 Direcciones Unicast de Sitio Local

– Las direcciones Unicast de Sitio Local son direcciones privadas que pueden utilizarse en intranets no jerárquicas. Estas direcciones pertenecen a una zona de sitio local, luego nunca serán redirigidas hacia el exterior de los márgenes que abarca dicho zona.

– La RCF 2374 define la estructura inicial que debían tener las direcciones IPv6 unicast de enlace local, aunque a día de hoy se encuentran obsoletas debido a que su uso presentaba problemas de duplicidad de direcciones. Están formadas por los siguientes campos:

- **Prefijo de red (64 bits):**
  - **FP (10 bits):** Prefijo de la dirección (1111 1110 11 – 0x fec).
  - **Subned (54 bits):** Identifican las distintas subredes que componen la red local de sitio.
- **Identificador de la Interfaz (64 bits):** Puede construirse de forma automática por el propio equipo mediante la dirección MAC o configurarse para que siempre obtenga la misma.

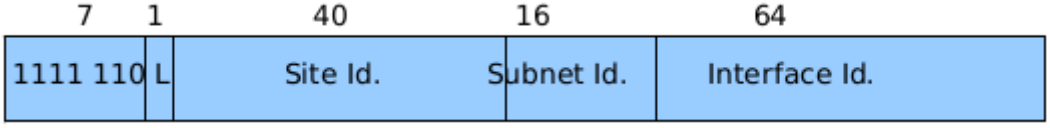
ej: fec0:0050:0016:0000:020f:b0ff:fea5:006e/64 = fec0:50:16::20f:b0ff:fea5:6e/64

2.4.3.1 Direcciones Unique Local IPv6 Unicast Address (ULA)

– Estas direcciones sustituyen a las direcciones Unicast de Sitio Local definidas en la normal RFC 2374, con el objetivo de solucionar los problemas de duplicidad que se daban en las mismas. Así mismo, estas direcciones pasan a denominarse *Unique Local IPv6 Unciast Addresses* (ULA).

– Estas direcciones son definidas en la RFC 3879 y la principal diferencia entre ambos modelos es la estructura de la propia dirección. Estas direcciones contienen la siguiente estructura:

- **Prefijo de red (64 bits):**
  - **FP (7 bits):** Prefijo de la dirección (1111 110L – 0x fc). El bit L indica si la gestión es local o global y su valor debe ser 1.
  - **Site ID (40 bits):** Se genera algoritmicamente para evitar las duplicidades del anterior RFC.
  - **Subnet ID (16 bits):** Identifican las distintas subredes que componen la red local de sitio.
- **Identificador de la Interfaz (64 bits):** Puede construirse de forma automática por el propio equipo mediante la dirección MAC o configurarse para que siempre obtenga la misma.

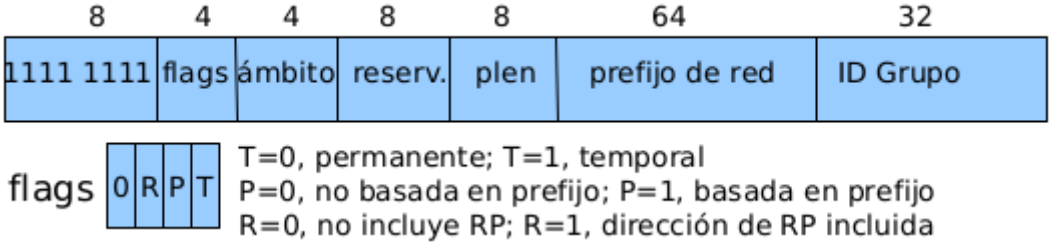


ej: fd12:761f:e8e1:28ea:20f:b0ff:fea5:6e/64

4.3.1 Direcciones Multicast

– Las direcciones Multicast son direcciones asignadas a grupos de máquinas. Su estructura es:

- **Prefijo (96 bits):**
  - **FP (8 bits):** Prefijo de la dirección (1111 1111 – 0x ff).
  - **Flags (4 bits):** Indican información a cerca del grupo Multicast al que pertenece la dirección.
  - **Ámbito (4 bits):** Indica el ámbito al del grupo Multicast al que pertenece la dirección.
  - **Reservado (8 bits):** Campo reservado para usos futuros cuyo valor actual es 0.
  - **Plen (8 bits):** Indica la longitud del prefijo del campo *Prefijo de red*.
  - **Prefijo de red (64 bits):** Identificador de la red.
- **Identificador del grupo Interfaz (32 bits):** Identificador del grupo al cual pertenece la dirección.



– Los posibles valores del campo ámbito son:

- **0001 – 0x 1:** Ámbito de nodo local.
- **0010 – 0x 2:** Ámbito de enlace local.
- **0101 – 0x 5:** Ámbito de sitio local.
- **1000 – 0x 8:** Organización.
- **1110 – 0x E:** Global.

– Los identificadores de grupos están organizados en tres rangos:

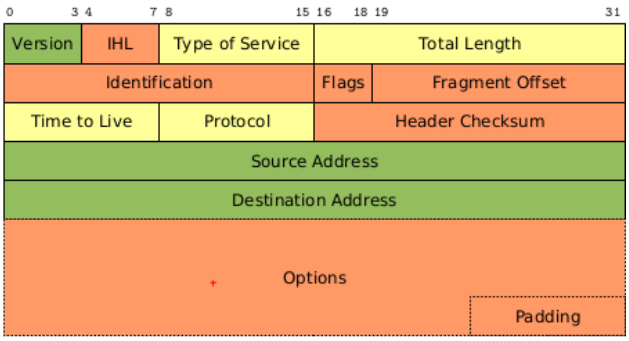
- **0x 00 00 00 01 a 0x 3f ff ff ff:** Identificadores para direcciones multicast permanentes, es decir, las denominadas como direcciones *bien conocidas*. Algunos de los identificadores de las direcciones bien conocidas mas importantes son:
  - **0x 00 00 00 01:** Identificador de todos los computadores.
  - **0x 00 00 00 02:** Identificador de los encaminadores locales.
  - **0x 00 00 00 09:** Identificador de los encaminadores RIP.
- **0x 40 00 00 00 a 0x 7f ff ff ff:** Identificadores para direcciones multicast permanentes basadas en prefijos de red.
- **0x 80 00 00 00 a 0x ff ff ff ff:** Identificadores para direcciones multicast dinámicas.

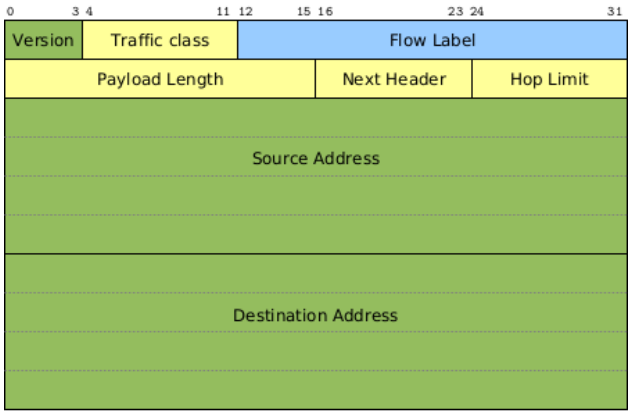
– El protocolo de descubrimiento de vecinos ICMPv6 tiene reservadas las direcciones multicast desde FF02::1:FF00:0000 hasta FF02::1:FFFF:FFFF.

FF01::2 → encaminadores del nodo local.
FF02::2 → encaminadores del enlace local.
FF05::2 → encaminadores del sitio local.
FF02::9 → encaminadores RIP del enlace local.
FF01::1 → computador del nodo local (todos los interfaces del nodo local).
FF02::1 → computadores del enlace local.

3º El datagrama IPv6

– La cabecera de los datagramas IPv6 es una evolución directa de la que utilizan los datagramas IPv4. En las siguientes imágenes podemos ver una comparativa entre ambas, apareciendo en rojo los campos eliminados, en amarillo los modificados, en azul los añadidos y en verde los mantenidos,





– Podemos ver como han desaparecido todos los campos que la cabecera IPv4 tenia en relación con la fragmentación de datagramas. Esto es debido a que en IPv6 la fragmentación se realiza en el origen, es decir, es la propia máquina encargada de transmitir la información la que la fragmenta y envía los datagramas uno a uno con el tamaño válidos para las redes que van a recorrer.

– Funcionamiento de cada uno de los campos de la cabecera IPv6:

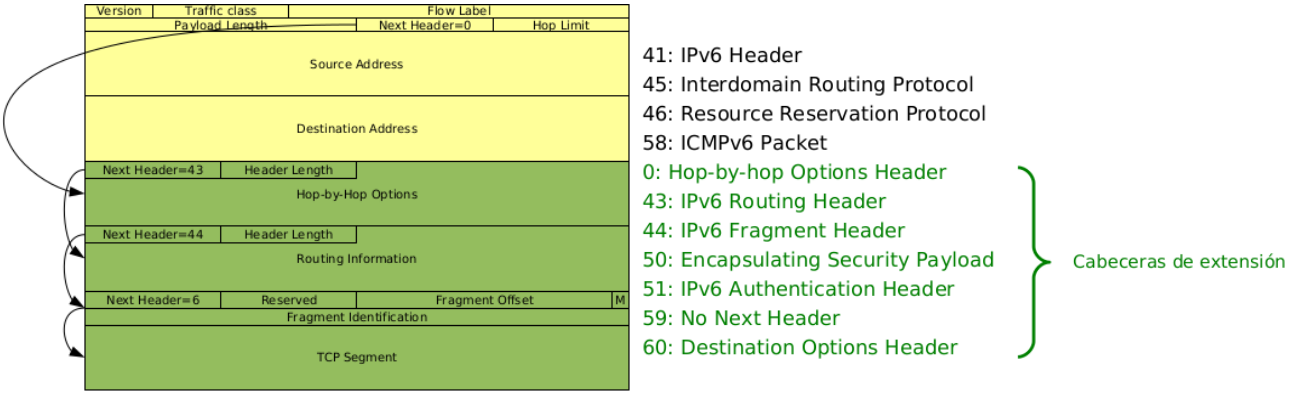
- **Version:** Su función en diferenciar los datagramas de las versiones IPv4 e IPv6.
- **Traffic Class:** Diferencia la clase de tráfico a la que pertenece el datagrama, lo cual sirve para que los encaminadores sepan identificar los datagramas que requieren un envío más urgente (utilizado sobre todo para el tráfico en tiempo real). 0-7: tráfico normal; 8-15: tráfico en tiempo real.
- **Flow Label:** Permite a los encaminadores diferenciar entre los datagramas que pertenecen al mismo flujo de datos, de modo que pueden identificar los recursos asignados a los mismos, sus necesidades y características. Cuando se trata de tráfico normal el valor es 0.
- **Payload Lenght:** Longitud del datagrama excluyendo la cabecera. Esto es debido a que la cabecera en los datagramas IPv6 es de longitud fija.
- **Next Header:** Identifica cual es el tipo de la siguiente cabecera que se encuentra almacenada en el campo de datos. Esta puede ser una cabecera de extensión o una cabecera correspondiente a un protocolo de la capa superior.
- **Hop Limit:** Marca el número de saltos restantes del datagrama. Cuando llegue a cero será descartado en por los encaminadores.
- **Source Address:** Dirección IPv6 de la máquina origen del datagrama.
- **Destination Address:** Dirección IPv6 de la máquina destino del datagrama.

3.1 Las cabeceras de extensión

– Las cabeceras de extensión son cabeceras especiales que se sitúan en el campo de datos, justo después de la cabecera IPv6. Estas cabeceras sirven para transmitir información específica desde al fuente al destino.

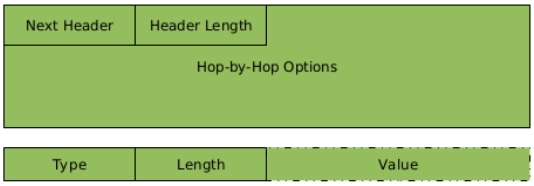
– Cada una de las cabeceras que conforma el datagrama IPv6 contiene un campo (N*ext Header)* en el que de indica el número de identificación de la siguiente cabecera que conforma el datagrama. Debido al tamaño variable de las mismas, dentro de cada una de ellas hay un campo (*Header Length*) que nos indica el tamaño de la propia cabecera.

– Los encaminadores intermedios no leen las cabeceras del campo de datos, ya sean de extensión o de un protocolo de transporte, excepto con las cabeceras *Hop-By-Hop* (código 0).



3.1.1 Hop-By-Hop (código 0)

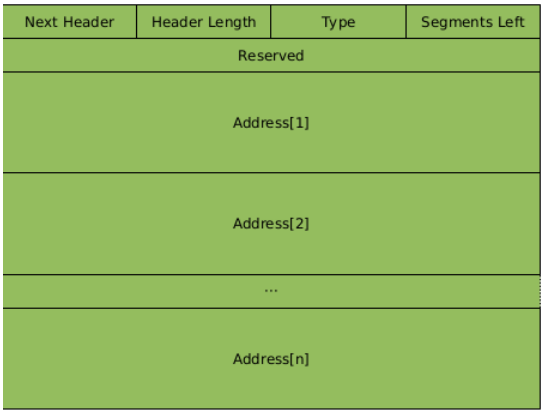
– Esta cabecera sirve para indicar a los examinadores los recursos que deben reservar con el fin de poder llevar a cabo una transmisión en tiempo real. Se trata de la única cabecera que es leída por todos los encaminadores, incluido el destino.



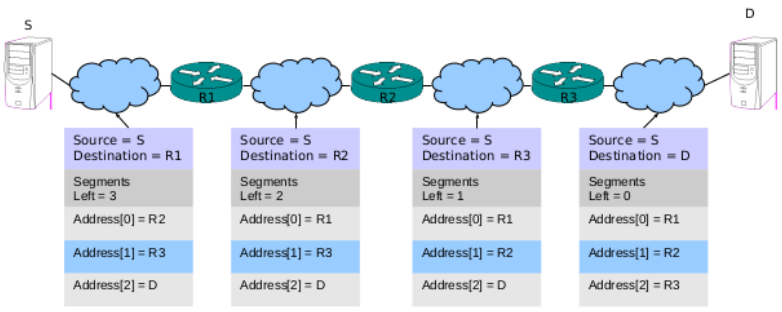
3.1.2 Routing Header (código 43)

– Esta cabecera se utiliza con el fin de forzar al datagrama a recorrer un camino concreto para llegar al destino. Esto se hace mediante la especificación de una lista de direcciones IPv6 que corresponden con los encaminadores que debe recorrer el datagrama.

– Mediante el campo *Segments Left* el encaminador puede saber en que posición de la lista se encuentra, de modo que permuta la dirección de destino del datagrama por la de dicha posición y reenvía el mismo.

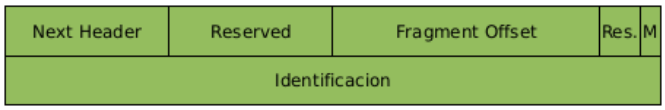


– El uso de esta cabecera de expansión fue desaconsejado en 2007 y posteriormente prohibido, con el fin de evitar ataques de denegación de servicio por saturación de la red.



3.1.3 Fragment Header (código 44)

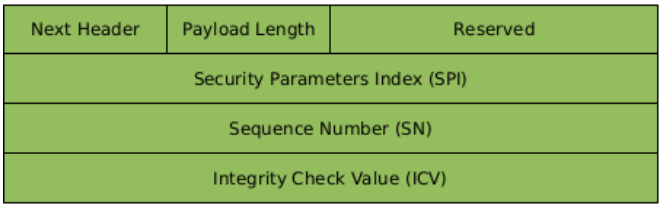
- Estas cabeceras indican al destino cuando un datagrama forma parte de un conjunto de información que ha sido fragmentado. Esta cabecera únicamente es leída por el destino.



- En IPv6 la fragmentación se hace en el origen, de esta manera, si un encaminador recibe un datagrama que no puede enviar por que supera el tamaño máximo permitido por la red, este se lo comunicará al emisor con el fin de que lo reenvié fragmentado

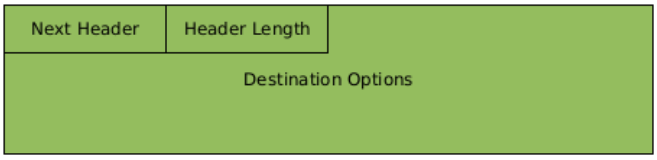
3.1.4 Autentication Header (código 51)

- Esta cabecera se utiliza para garantizar que el datagrama no ha sido alterado en el tránsito y que la dirección del emisor coincide con la que aparece en el campo de dirección de origen.



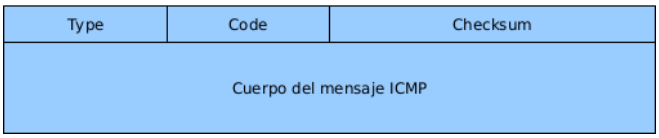
3.1.5 Destination Option Header (código 60)

- Esta cabecera únicamente debe ser examinada por el destino, excepto si precede a una cabecera del tipo Routing Header, en cuyo caso deberá ser examinada por todos los nodos cuya dirección se encuentre dentro de la lista de nodos intermedios en dicha cabecera.



4º El protocolo ICMPv6

- ICMPv6 continua realizando todas las funciones de ICMPv4 y todos los mensajes tienen un formato genérico. Además de esto, ICMPv6 asume las siguientes funcionalidades:



  - Trasmite la información sobre la pertenencia a los grupos multicast (en IPv4 lo realiza IGMP).
  - Se encarga del descubrimiento de direcciones (en IPv4 se utiliza ARP).
  - Autoconfiguración en los equipos. Esto también permite descubrir encaminadores presentes en el enlace. (en IPv4 lo realiza DHCP, aunque en IPv6 existe DHCPv6, pero este no es necesario).

4.1 Descubrimiento de vecinos (Neighbour Discovery)

- El descubrimiento de vecinos en IPv4 se realiza mediante el protocolo ARP, el cual sirve para asociar direcciones IPv4 con las direcciones MAC de sus respectivos equipos. Una trama ARP viaja por difusión y es aceptadas por todas las interfaces a las que llega, las cuales copian la pregunta en el Kernel del equipo y únicamente la máquina por la que se esta preguntando responde.

- Esto trae consigo dos problemas: Estamos aumentando el tráfico broadcast y todas las máquinas que reciben la petición deben de parar de hacer lo que están haciendo para respondernos.

– Para solventar estos problemas se utiliza la función *Neighbour Discovery* del protocolo ICMPv6, el cual centra su funcionalidad en el uso de direcciones Multicast para realizar las preguntas con el fin de obtener la MAC de los equipos.

– La dirección IPv6 a la que enviaremos la trama ICMPv6 con la pregunta será de la siguiente forma: **FF02 : 0000 : 0000 : 0000 : 0000 : 0001 : FFXX : XXXX,** donde X serán los últimos 24 bits de la dirección IPv6 a la que queremos preguntarle la MAC. En el interior de la trama ICMPv6 se contendrá información sobre la solicitud y la dirección IPv6 entera del destino al cual preguntamos.

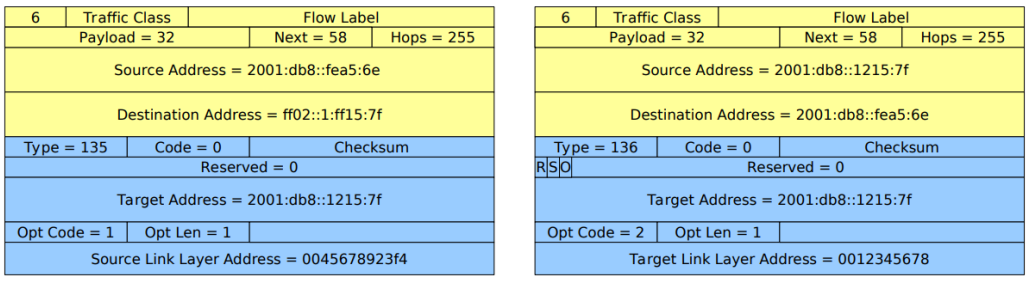
– Esta trama debe estar encapsulada dentro de una trama Ethernet, lo que hacemos es utilizar como dirección de destino de la misma una dirección multicast de la forma **33 : 33 : XX : XX : XX : XX**, donde X serán los últimos 32 bits de la dirección multicast a la que enviamos la trama ICMPv6.

IPv6	2001:0db8:0100:0103:020f:b0ff:fea5:006e
Solicited-node prefix	FF02:0000:0000:0000:0000:0001:ff00:0000/104
Solicited-node	FF02:0000:0000:0000:0000:0001:ffa5:006e
ethernet	33:33:ff:a5:00:6e

– Como la dirección de destino de las tramas ICMPv6 depende de la dirección IPv6 del equipo destino, todas las maquinas que reciban dichas tramas pueden saber de antemano si esta dirigidas a ellas o no. En caso negativo, la tarjeta de red desecha la trama sin la necesidad de hacer que el equipo tenga que atender a la solicitud. Únicamente responde el equipo al que va dirigida la trama.

-- Para realizar el descubrimiento de vecinos, ICMPv6 utiliza un total de dos tipos de mensajes

1. Un nodo envía un mensaje *ICMPv6 Neighbor Solicitation* pidiendo la dirección MAC asociada a una determinada dirección IPv6 indicada en el mensaje. La solicitud se envía a la dirección multicast calculada de la forma indicada anteriormente y a su vez encapsulada en la correspondiente dirección Ethernet asociada a dicha dirección IPv6 multicast
2. El nodo correspondiente a dicha dirección IPv6 responde con un mensaje *ICMPv6 Neighbor Advertisement*, en el cual proporciona su dirección MAC. Este mensaje es enviado a la dirección indicada como origen en el mensaje *ICMPv6 Neighbor Solicitation* al cual está respondiendo



Neighbour Solicitation Neighbour Advertisement

-- El mensaje *ICMPv6 Neighbor* Solicitation es enviado, normalmente, con la dirección local de enlace del equipo solicitante. Si la fuente aún no ha realizado el proceso automático de configuración de sus dirección IPv6 de Enlace Local, esta trama se enviará con dirección origen ::.

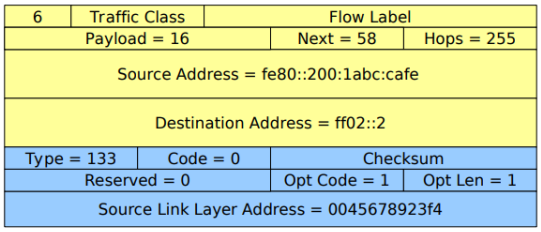
-- Estos mensajes cuentan con tres bit de flag que indican lo siguiente:

- **Flag R:** Si vale 1 quiere decir que el equipo fuente del mensaje es un router.
- **Flag S:** Si vale 1, el mensaje es una respuesta a un *ICMPv6 Neighbor Solicitation* previo.
- **Flag O:** Si vale 1, el contenido debe actualizar a las entrada en caché correspondientes.

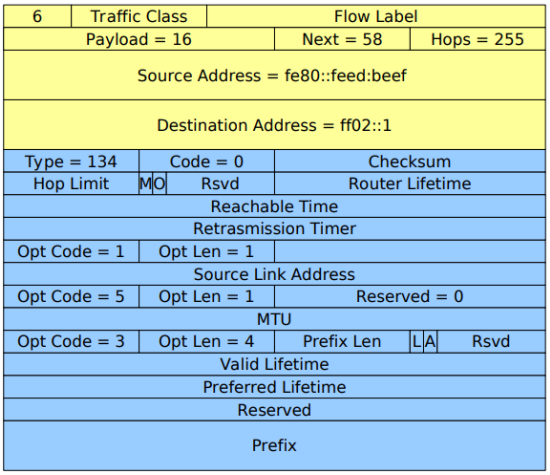
4.2 Descubrimiento de encaminadores

– Cuando un equipo se activa, este intenta configurar sus interfaces IPv6 de forma automática, para lo cual debe realizar un proceso de descubrimiento de encaminadores. Esto se realiza mediante el envío de un mensaje *ICMPv6 Router Solicitation* por parte del equipo.

-- En el caso de que existe algún encaminador configurado en el enlace, este recibirá el mensaje enviado y responderá al equipo con un mensaje del tipo *ICMPv6 Router Advertisement*, en el cual incluirá la información necesaria para que este realice la configuración de sus direcciones IPv6 de forma automática.



Router Solicitation



Router Advertisement

-- En el caso de que el equipo solicitante no reciba una respuesta a su mensaje *ICMPv6 Router Solicitation* dentro de un tiempo estipulado, este lo reenviará hasta un máximo de tres veces. En el caso de que ninguno de dichos mensajes sea respondido, el equipo asumirá que no existen encaminadores operativos y procederá a autoconfigurar su dirección de Enlace Local.

-- Los routers envían los mensajes *ICMPv6 Router Advertisement* de forma periódica, sin la necesidad de haber recibido previamente una solicitud. De esta manera se consigue que los equipos identifiquen a los encaminadores incluso cuando estos empezaron a operar posteriormente.

-- Los routers envían un mensaje *ICMPv6 Router Advertisement* por cada uno de los prefijos que dicho router debe anunciar según su configuración. De esta manera, los equipos pueden ir configurando una dirección IPv6 distinta para cada una de las redes anunciadas por los routers.

4.3 Autoconfiguración del equipo

-- En IPv4, la configuración de las direcciones IP se realizan mediante el protocolo DHCP, en el caso de IPv6 esto no es necesario, ya que basta con que los encaminadores anuncien prefijos mediante los mensajes *ICMPv6 Router Advertisement*.

-- Cuando una máquina recibe un mensaje *ICMPv6 Router Advertisement*, esta autoconfigura una nueva dirección IPv6, para lo cual necesita 2 datos:

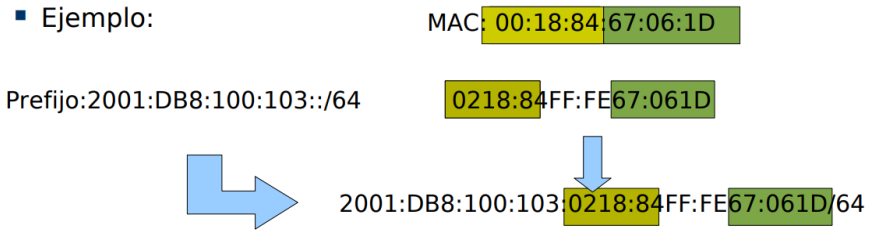
- **Prefijo de red (primeros 64 bits):** Indicado por los encaminadores mediante los mensajes *ICMPv6 Neighbor Advertisement.*
- **Interfaz de la máquina (últimos 64 bits):** Creado por la máquina a partir de la dirección MAC perteneciente a la tarjeta de red a la cual va a asignar la nueva dirección IPv6.

4.3.1 Creación de dirección IPv6 según RFC 4862 (SLAAC)

-- Se trata de la forma clásica para la creación de direcciones IPv6 a partir de la dirección MAC de la tarjeta de red a la cual se asociará dicha dirección.

-- Una dirección MAC está formada por 6 octetos (48 bits) mientras que el campo de identificación de la interfaz son 8 octetos (64 bits), lo cual nos lleva a tener que realizar los siguientes pasos para poner una dirección MAC en formato EUI-64:

1. Ponemos el penúltimo bit del primer octeto a 1.
2. Introducimos los dos campos :FF:FE: entre el tercer y cuarto octeto.
3. Ensamblamos los 8 campos resultantes en lo que conformará el identificación de la interfaz.
4. Ensamblamos el identificación de la interfaz con el prefijo de red indicado por el encaminador.



-- Esta forma de generar las direcciones IPv6 tiene un serio problema de privacidad. Esto se debe a que la dirección MAC utilizada para la generación del identificador de la interfaz esta ligada a la tarjeta de red, lo que hace que este asociada al equipo que utiliza dicha tarjeta y en segunda instancia, al individuo al cual pertenece dicho equipo.

4.3.2 Creación de dirección IPv6 según RFC 4941

-- Esta forma de generación de dirección IPv6 surge con el fin de solventar los problemas de confidencialidad utilizados por la forma clásica. El identificador se genera de forma pseudoaleatoria mediante el uso de varios parámetros: La dirección MAC, una semilla y un algoritmo Hash.

-- Esto hace que cada vez que el usuario se conecta a red obtenga una dirección IPv6 diferente. Sin embargo, provoca que las direcciones de los usuarios en la red sean cambiantes, de modo que la gestión de los sucesos sea mucho más complicada y los servidores difíciles de administrar.

4.3.3 Creación de dirección IPv6 según RFC 7217

-- Debido a los problemas asociados a las dos anteriores formas de generar los identificadores de la interfaz, se llega a la conclusión de que es conveniente tener direcciones estables pero que no produzcan problemas de privacidad ni ofrezcan información sobre el hardware del equipo.

-- La solución se implementa en 2014 mediante la presente RFC (quedando desaconsejado usar SLAAC), donde el identificador de la interfaz se genera mediante la fórmula:

RID = F(Prefix, Net_Iface, Network_ID, DAD_counter, secret_key)

-- De esta manera se consigue que se mantenga la privacidad de los usuarios externos a la red, gracias a que las direcciones son estáticas pero también pseudoaleatorias. Además, el proveedor sabe a quien pertenece cada dirección IPv6 asignada, por lo que facilita la gestión de las redes.

5º Secure Neighbour Discovery (SEND)

-- El empleo del proceso *Neighbour Discovery* para el descubrimiento de vecinos es vulnerables a ataques maliciosos como la denegación de servicios y la suplantación de identidad. Para solventar estos problemas se utiliza el proceso *Secure Neighbour Discovery*, el cual se caracteriza por:

- Las direcciones son generadas de forma criptográfica, de modo que se asegura que máquina que dice tener una determinada dirección IPv6, verdaderamente la posee.
- Se emplean parejas de claves pública-privada.

-- SEND hace uso de PKI (*Public Key Infraestructure*), cuyo funcionamiento se basa en que las máquinas deben confiar en aquellos mensajes que estén firmados mediante el uso de certificados.

-- Los encaminadores deben tener un certificado con el cual firman los mensajes de descubrimiento y anuncios, mientras que cada máquina debe tener una lista de autoridades certificadoras reconocidas. Cuando una máquina recibe un mensaje de un encaminador, verifica si el mismo esta firmado por una de las autoridades que reconoce, en caso negativo, el mensaje es rechazado por la máquina.

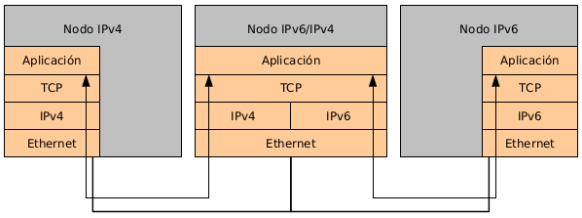
-- La implementación y el despliegue de un sistema SEND es bastante complicado, para lo cual se pueden utilizar los llamados RA-guards. Estos son configurados en los switch de la red y su función es rechazar los mensajes *ICMPv6 Router Advertisement* que provienen de aquellos equipos que no son encaminadores, evitando así que una máquina se haga pasar por un router.

6º Mecanismos de transición

– Hasta que se produzca el despliegue total de IPv6 deberán convivir ambos protocolos, por lo que necesitaremos garantizar que el proceso de migración se realice mediante una transición suave, proporcionando la mayor compatibilidad posible entre Ipv4 e IPv6. Para llevar a cabo esto se han desarrollado diversos mecanismos de transición.

6.1 Dual Stack

– Este mecanismo consiste en que un mismo nodo tiene implementado ambos protocolos. Se trata de la manera más sencilla de garantizar la compatibilidad entre ambos sistemas, pero no resuelve el problema de la escasez de direcciones IPv4.



6.2 Túneles

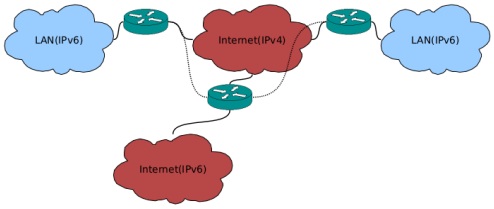
– Los túneles se utilizan para conectar conjuntos aislados de equipos IPv6 entre sí, los cuales necesitan comunicarse a través de redes que únicamente implementan IPv4. Su funcionamiento se basa en encapsular los datagramas IPv6 dentro de datagramas IPv4, permitiendo así que puedan viajar por las redes que únicamente implementan este último protocolo.

– Inicialmente se implementaron túneles automáticos como un medio rápido para facilitar la comunicación entre nodos IPv6 a través de IPv4. Sin embargo, se observo que desempeñaban un bajo rendimiento y sufrían de problemas de seguridad, por lo que se desaconseja su uso.

6.2.1 Túneles manuales 6in4

- Para implementar este tipo de túnel se necesita un *tunnel broker* que permita al equipo conectarse con el resto de redes Ipv6, el cual necesita ser configurado explícitamente por el administrador.

- El encapsulamiento agrega un total de 20 bytes al datagrama IPv6 original, los cuales conforman la cabecera IPv4. Los mensajes IPv4 que encapsulan los datagramas IPv6 siguen el protocolo IP en IP, el cual es identificado por el número de protocolo 41.

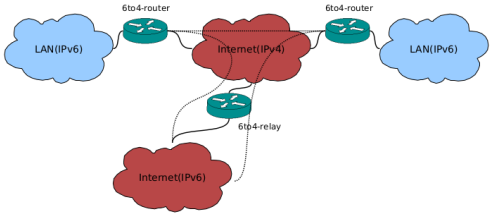



```
# ip tunnel add sit1 [mode sit] remote 194.179.25.50
# ip link set dev sit1 up mtu 1400
# ip addr add 2001:db8:40:261c::2/64 dev sit1
# ip -6 route add default via 2001:db8:40:261c::1
          o bien
# ip -6 route add default dev sit1
```

6.2.2 Túneles automáticos 6to4

- Utilizan el mecanismo *6to4-relay* en los routers, los cuales incorporan ambos protocolos y utilizan la dirección anycast 192.88.99.1 para comunicarse entre sí, de modo que envían los mensajes IPv6 encapsulados dentro de IPv4 a dicha dirección.

- Estos túneles no se pueden utilizar con direcciones IP dinámicas, ya que el router utiliza la técnica de conversión de direcciones IPv4 a IPv6 para redirigir los datagramas hacia la máquina concreta. El rango de direcciones reservadas es 2002::/16 y el prefijo de sitio es 2002:V4ADDR::/48.




```
# ip tunnel add 6to4 mode sit remote 192.88.99.1
# ip link set dev 6to4 up mtu 1400
# ip addr add 2002:c0a8:101:17ce:f3b7:a8f8:d203:7411/128  dev 6to4
# ip -6 route add default dev 6to4
```

7º Despliegue de redes IPv6

- Cuando realizamos un despliegue de una red IPv6, todo enlace debe tener asignado al menos una dirección con prefijo /64, aunque en algunos casos puede bastar con la dirección local de enlace. Por otra parte, el mínimo del prefijo recomendado para un usuario final es el /48, ya que le otorga la posibilidad de crear mas de 6000 redes internas.

- Las subredes deben establecerse en fronteras de 4 bits, de modo que el campo que define dicha subred debe ser múltiplo de 4. No se aconseja el uso de direcciones consecutivas, ya que estas son fácilmente predecibles, por lo que es mejor utilizar direcciones pseudoaleatorias.