Protocolo IP versión 6

1. Introducción

En 1992 el hecho de constatar la escasez de direcciones y el aumento de las tablas de enrutamiento dio lugar al inicio del proyecto IP Siguiente Generación (IP NG).

Se trataba igualmente de implementar de manera nativa las numerosas opciones disponibles con IPv4, trabajando en cuatro temas principales: la autoconfiguración, la movilidad, la implementación de multicast y sobre todo la seguridad (autentificación y confidencialidad).

En diciembre de 1995, se publicó la RFC 1883 «Internet Protocol Version 6».

Esta RFC tardó poco en considerarse obsoleta y se reemplazó por la RFC 2460 en diciembre de 1998 (http://tools.ietf.org/html/rfc2460).

En junio de 1998, nació una red experimental: la **6Bone** (troncal IPv6), para permitir probar IPv6 en condiciones reales. Esta red utilizaba los prefijos 3FFE::/16 (RFC 2471). Esta red se cerró el 6 de junio de 2006 (¡06/06/06!) una vez concluyó el experimento.

2. Principios

IPv6, o IP *Next Generation* (NG), es la nueva versión de IP (*Internet Protocol*), que debe sustituir al protocolo IPv4. Esta migración es progresiva pero se debe realizar rápidamente.

IPv6 mantiene las principales funcionalidades de su predecesor y además cubre sus carencias con la incorporación de nuevas funciones.

En primer lugar, se ha ampliado el espacio de asignación de direcciones de 4 bytes (32 bits) a 16 bytes (128 bits). Desde el principio, este era uno de los objetivos principales de esta nueva versión. De hecho, no se esperaba que IPv4 tuviera tanto éxito, vinculado al de Internet.

Además, IPv6 simplifica los encabezamientos de los paquetes de datos, con solamente 7 campos en lugar de 14. Así, los tratamientos por parte de los routers pueden ser más rápidos aumentando de este modo la velocidad. Las funcionalidades de traducción de direcciones (NAT - *Network Address Translation*) ya no son necesarias, lo que simplifica la arquitectura de red.

A nivel de seguridad, IPv6 incluye de forma nativa IPsec (*IP Security*). Este protocolo de seguridad se explicará más tarde en su totalidad.

Entre las características de esta nueva generación, podemos citar:

- Configuración Plug and Play, gracias a los mecanismos de autoconfiguración de las máquinas.
- Enrutamiento más eficaz, con una reducción de las tablas de transporte.
- Identificación de los flujos para el servicio integrado.
- Mecanismos estándar de seguridad.
- Movilidad.
- Número casi ilimitado de direcciones IP.
- Compatibilidad ascendente mantenida con IPv4, que garantiza una migración progresiva.

3. Estructura de una dirección IP

a. Categorías de direcciones

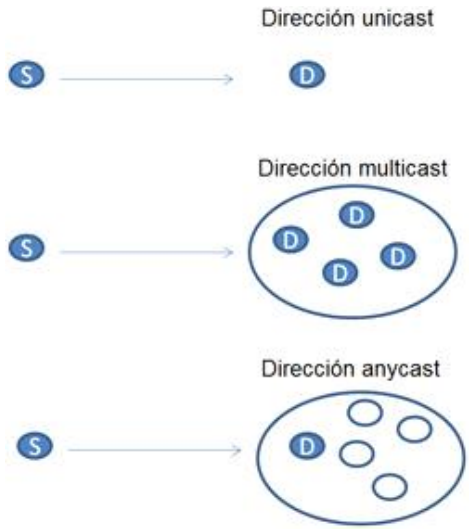
En IPv6, existen tres tipos de direcciones que corresponden a identificadores de 128 bits para interfaces o grupos de interfaces:

- *unicast*,
- *multicast*,
- *anycast*.

Una dirección *unicast* hace referencia a un identificador asociado a una sola interfaz, mientras que una dirección *multicast* hace referencia a un identificador de grupo cuyos miembros son interfaces: se va a asignar el identificador *multicast* a la interfaz.

El concepto de dirección *anycast* designa la interfaz «más cercana», miembro de un grupo, desde un punto de vista de la métrica utilizada (en el sentido de los protocolos de enrutamiento).

No existe el concepto de dirección de difusión (o broadcast) como se daba en IPv4. Las direcciones multicast sustituyen el broadcast definiendo además un ámbito de aplicación de esta dirección.



Tipos de direcciones IPv6

Por lo tanto, un paquete enviado a una dirección *unicast* se entregará únicamente a la interfaz identificada por esta dirección.

Un paquete enviado a una dirección *multicast* se transmitirá a todas las interfases identificadas con esta dirección.

Finalmente, un paquete enviado a una dirección *anycast* se transmitirá solamente a una de las interfaces (la más próxima) identificadas con esta dirección.

b. Ámbito de una dirección

Una dirección dispondrá de un ámbito más o menos importante según su categoría. Al contrario que IPv4, que

separaba las direcciones públicas de las privadas, con IPv6 por una parte las direcciones van a tener una visibilidad mayor o menor y por otra parte una misma interfaz dispondrá de diferentes direcciones IP con una visibilidad diferente.

Una dirección *unicast* o *anycast* podrá disponer de los siguientes ámbitos:

- Ámbito **global** (ámbito mundial, Internet).
- Ámbito **local** (ámbito local, número limitado de sitios interconectados).
- Ámbito de **conexión local** (ámbito limitado a una subred no enrutada).

Teóricamente, una dirección *multicast* se podrá descomponer basándose en los siguientes niveles:

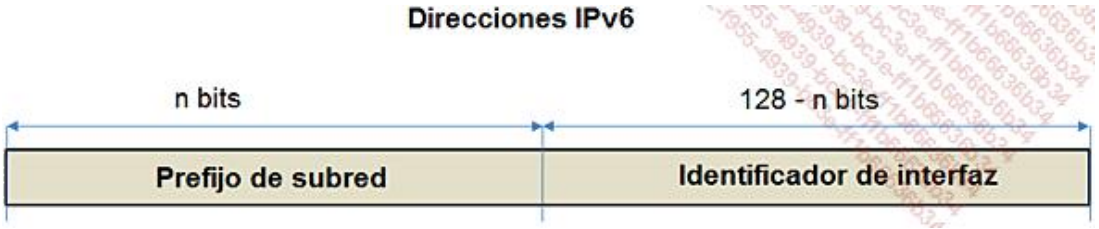
- Ámbito **global** (mundial).
- Ámbito **local en la empresa** (varios sitios de una misma empresa).
- Ámbito **local en el sitio** (sitio único).
- Ámbito **local del administrador** (el ámbito más pequeño que se puede configurar administrativamente con independencia de la topología física).
- Ámbito **local de la subred** (subred).
- Ámbito de **conexión local** (vecinos conectados en una misma conexión).
- Ámbito de **interfaz local** (interfaz).

El ámbito de la dirección se identificará por el prefijo de esta dirección, para las direcciones *unicast* y *anycast*, o por el campo **Ámbito** presente en el prefijo de una dirección *multicast*.

c. Dirección unicast

Las direcciones *unicast* pueden identificar un nodo de manera única (tarjeta de red o interfaz de router).

De manera general, las direcciones IPv6 *unicast* se presentan de la misma manera que las direcciones IPv4 sin clase CIDR (*Classless Inter Domain Routing*).



Hemos visto que estas direcciones pueden ser de ámbito global, de sitio o de conexión local.

También existen direcciones IPv6 que llevan encapsuladas direcciones IPv4.

Veremos un poco más tarde cómo funciona el establecimiento de la dirección en función de su ámbito y de su categoría.

d. Notación

Existen diferentes maneras de representar la direcciones IPv6.

La forma más usual es **xx : xx : xx : xx : xx : xx : xx : xx**.

donde «**xx**» corresponde a la representación hexadecimal de una palabra (2 bytes o 16 bits).

Ejemplos:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

2001:0:0:0:8:800:200C:417A

No es necesario escribir los ceros consecutivos de una palabra. Sin embargo, debe haber al menos una cifra por campo, excepto en el caso de utilización de la forma abreviada (ver más adelante).

Teniendo en cuenta los diferentes métodos de obtención de las direcciones, es habitual disponer de direcciones que tengan numerosos ceros consecutivos. Para facilitar la escritura de estas direcciones, una sintaxis especial, **la forma abreviada**, permite comprimir y simplificar esta escritura.

La utilización de «**::**» permite indicar uno o varios grupos de 16 bits de ceros.

Atención, este doble «**:**» solo debe aparecer una vez en una dirección. Se puede utilizar para comprimir los ceros iniciales o finales de la dirección.

La siguiente tabla permite ver las formas abreviadas que se pueden utilizar:

Ejemplo de dirección	Categoría	Forma abreviada
1080:0:0:0:8:800:200C:417A	una dirección *unicast*	1080::8:800:200C:417A
FF01:0:0:0:0:0:0:101	una dirección *multicast*	FF01::101
0:0:0:0:0:0:0:1	la dirección de bucle local	::1
0:0:0:0:0:0:0:0	una dirección no especificada	::

Existe una forma alternativa y a veces más práctica si se trabaja en un entorno mixto (IPv4 y v6):

xx : xx : xx : xx : xx : xx : a . b . c . d donde:

- «**xx**» representa la escritura hexadecimal de seis palabras (12 bytes) más significativas.
- «**a.b.c.d**» representa la dirección IPv4 en notación decimal punteada (4 bytes menos significativos).

A continuación ofrecemos algunos ejemplos:

Ejemplo de dirección	Forma abreviada
0:0:0:0:0:0:192.168.1.1	::192.168.1.1
0:0:0:0:0:FFFF:57.146.31.60	::FFFF:57.146.31.60

Finalmente, la **representación de los prefijos de las direcciones** sigue el mismo principio que la notación CIDR utilizada en IPv4:

Dirección-IP-v6 / longitud del prefijo, donde:

- «**Dirección-IP-v6**» se escribe siguiendo las reglas presentadas anteriormente.
- «**longitud-de-prefijo**» es un valor decimal que indica cuántos bits significativos (a la izquierda) forman parte del prefijo.

Así, el prefijo de 60 bits hexadecimal 200300000000ABC se escribe:

2003:0000:0000:ABC0:0000:0000:0000:0000/60

2003::ABC0:0:0:0:0/60

2003:0:0:ABC0::/60

Igualmente se puede escribir, como en IPv4, la dirección del nodo seguido del prefijo asociado a la red:

2003:0:0:ABC0:123:4567:89AB:CDEF/60

e. Identificador EUI-64

Concepto de identificador

Los identificadores de interfaz para las direcciones *unicast* en IPv6 permiten identificar las interfaces en una conexión dada. Este identificador debe ser único para una subred dada y lo puede ser también para un ámbito mayor, incluso global (Internet).

En algunos casos, el identificador se obtendrá directamente a partir de la dirección MAC (nivel 2) de la interfaz.

Este identificador se puede usar en el mismo nodo siempre que se utilice en interfaces diferentes conectadas en subredes diferentes.

Observe que no hay relación directa entre la singularidad del identificador de interfaz y la singularidad de direcciones IP. Por lo tanto, es posible crear una dirección *unicast* global disponiendo de un identificador de interfaz de ámbito no global, o crear una dirección local de sitio, con un identificador de ámbito global.

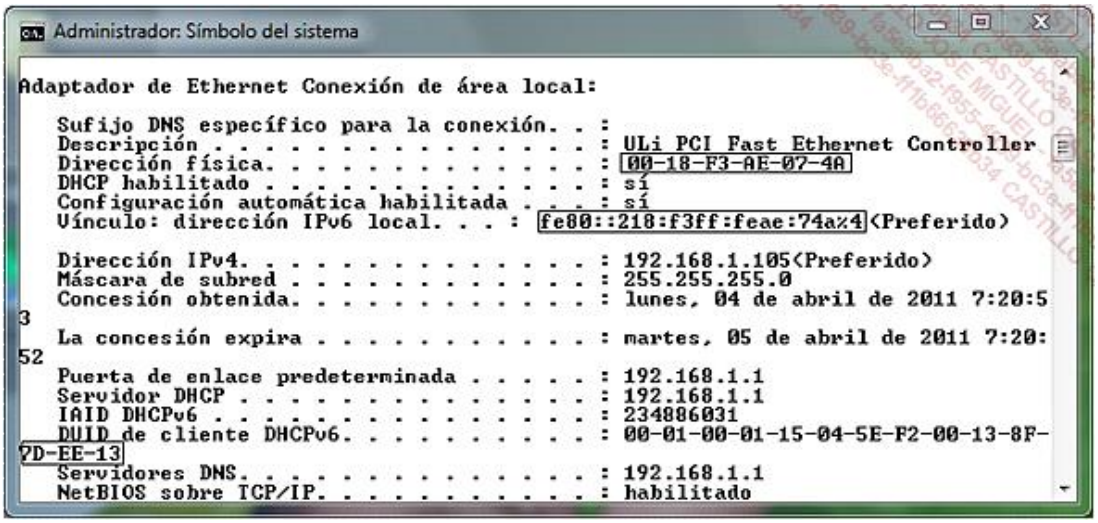
Además, cualquier dirección *unicast*, excepto aquellas que comienzan en binario por «**000**», deben tener un identificador de interfaz:

- de una longitud de 64 bits;
- construido según el formato EUI-64 modificado.

El identificador de interfaz, basado en el formato EUI-64 modificado, es de ámbito global, ya que está construido a partir de la dirección MAC. Por el contrario, el identificador es de ámbito local cuando no tiene ninguna información única o permanente para construir el identificador de interfaz (por ejemplo: conexión serie, terminaciones de túneles).

Construcción de un identificador EUI-64 modificado

Observe a continuación la dirección MAC asignada a la tarjeta de red y la dirección IPv6 correspondiente que se le ha autoasignado:



En este caso, la dirección MAC es 00-18-F3-AE-07-4A.

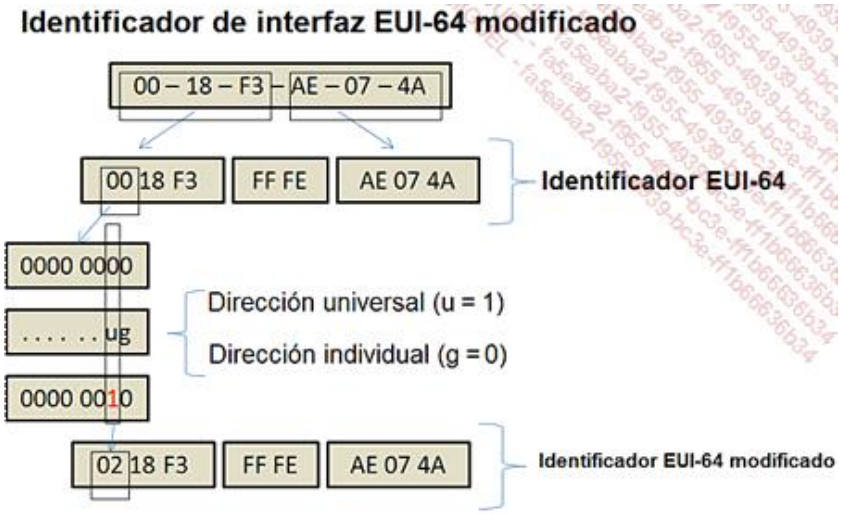
Los tres primeros bytes identifican al fabricante o OUI (*Organizationally Unique Identifier* - http://standards.ieee.org/regauth/oui/oui.txt) y los tres últimos identifican el hardware.

La dirección autoasignada es FE80::218:F3FF:FEAE:74A.

Observe que el "%4" define un índice para esta interfaz y define por tanto la asignación de esta misma dirección en otra interfaz de la misma máquina, a condición que se conecte en otra subred.

El identificador EUI-64 se construye a partir de la dirección MAC, insertando los dos bytes "**FF FE**" entre la OUI y la parte base de la dirección MAC.

El identificador EUI-64 modificado se obtiene poniendo a "1" el primer bit del byte significativo del OUI.



Finalmente encontramos:

FE80::218:F3FF:FEAE:74A

f. Direcciones reservadas

Existen diversas direcciones reservadas en IPv6.

El bucle local

La dirección de bucle local es

0000:0000:0000:0000:0000:0000:0000:0001

En escritura abreviada ::1

- Esta dirección equivale a 127.0.0.1 en IPv4.

- Cuando no se define ninguna dirección, se utiliza 0000:0000:0000:0000:0000: 0000:0000:0000. También se puede escribir 0:0:0:0:0:0:0:0, o incluso :: (doble «:»).

Las direcciones de transición IPv4 - IPv6

Para asegurar una transición entre las dos versiones, en ciertas circunstancias se pueden utilizar las direcciones IPv6 que se basan en direcciones IPv4.

Se puede utilizar una dirección IPv4 mapeada cuando se trate de comunicar, sea en IPv4, sea en IPv6, a partir de un equipo que disponga de doble pila de protocolo (IPv4/v6).

Esta dirección se puede representar utilizando una mezcla de las notaciones IPv6/v4.

Se escribirá en notación abreviada de la siguiente manera:

::FFFF:<dirección-ipv4-notación-decimal-punteada>

Por ejemplo, ::FFFF:192.168.1.200

Se podrá utilizar también la notación hexadecimal y escribir la dirección así:

::FFFF:C0A8:01C8

Donde 192 en base 10 (d) vale C0 en base 16 (h), o sea 192d = C0h, 168d = A8h, 1d = 1h y 200d = C8h.

En realidad es la dirección 0000:0000:0000:0000:0000:FFFF:C0A8:01C8.

0000	0000	0000	0000	0000	FFFF	C0A8	01C8

Las direcciones IPv4 compatibles sirven para encapsular IPv6 en IPv4 (por medio de un túnel). Estas direcciones se escriben poniendo los 96 bits significativos a 0 antes de cifrar la IPv4:

::<dirección-ipv4-notación-decimal-punteada>.

Ejemplo: **::192.168.1.200**

O **::C0A8 :01C8**

O sea

0000	0000	0000	0000	0000	0000	C0A8	01C8

Tenga en cuenta que la RFC 4291 trata estas direcciones como obsoletas. No se deben utilizar.

g. Descomposición de rangos para la IETF

Introducción

Los rangos de direcciones IPv6 (RFC 4291) se han descompuesto para IETF (*Internet Engineering Task Force*) de la siguiente manera:

Prefijo IPv6	Asignación	Referencia
0000::/8	Reservado	[RFC4291]
0100::/8	Reservado	[RFC4291]
0200::/7	Reservado (ej. NSAP)	[RFC4048]
0400::/6	Reservado (ej. IPX)	[RFC4291]
0800::/5	Reservado	[RFC4291]
1000::/4	Reservado	[RFC4291]
2000::/3	*Unicast* globales	[RFC4291]
4000::/3	Reservado	[RFC4291]
6000::/3	Reservado	[RFC4291]
8000::/3	Reservado	[RFC4291]
A000::/3	Reservado	[RFC4291]
C000::/3	Reservado	[RFC4291]
E000::/4	Reservado	[RFC4291]
F000::/5	Reservado	[RFC4291]
F800::/6	Reservado	[RFC4291]
FC00::/7	*Unicast* locales	[RFC4193]
FE00::/9	Reservado	[RFC4291]
FE80::/10	*Unicast* de conexión local	[RFC4291]
FEC0::/10	Obsoleto (*unicast* de sitio)	[RFC3879]
FF00::/8	*Multicast*	[RFC4291]

Se puede acceder a los documentos oficiales (RFC) en la siguiente URL: http://tools.ietf.org/html/

Así, cuando se retiran las direcciones reservadas, quedan las siguientes categorías:

- Direcciones *unicast* globales.
- Direcciones *unicast* locales.
- Direcciones *unicast* de conexión local.

- Direcciones *multicast*.

Tenga en cuenta que las direcciones *anycast* están incluidas en el rango de direcciones «*unicast* globales».

Explicaciones complementarias

El prefijo IPv6 se debe interpretar de la siguiente manera:

Por ejemplo, «**FC00::/7**» significa que los «7» bits significativos presentes en los 16 bits «FC00» se fijan.

- «**F**» se codifica en 4 bits en binario como «**1111**».
- «**C**» se codifica «**1100**».
- «**0**» se escribe «**0000**» en binario.

Por lo tanto:

- El byte escrito «**FC**» en hexadecimal vale «**1111 1100**» en binario.
- «**00**» en hexadecimal se escribe «**0000 0000**» en binario.

Una vez el prefijo hexadecimal se transcribe en binario, se identifican los n bits significativos (a la izquierda) después de «/» en la escritura del prefijo. Estos bits se deben fijar cuando se enumeran las posibles combinaciones.

FC00::/7	1111 110x.	xxxx xxxx

Así, FC00::/7 quiere decir que los bits significativos se pueden escribir con los valores «mínimo» y «máximo» siguientes:

- **1111 1100.0000 0000**
- y **1111 1101.1111 1111**

Finalmente, FC00::/7 expresa todas las direcciones cuyos prefijos están entre FC00 y FDFF.

Prefijo IPv6	Prefijo	Binario	Rango del prefijo
0000::/8	0000 0000.	xxxx xxxx	0000-00FF
0100::/8	0000 0001.	xxxx xxxx	0100-01FF
0200::/7	0000 001x.	xxxx xxxx	0200-03FF
0400::/6	0000 01xx.	xxxx xxxx	0400-07FF
0800::/5	0000 1xxx.	xxxx xxxx	0800-0FFF
1000::/4	0001 xxxx.	xxxx xxxx	1000-1FFF
2000::/3	001x xxxx.	xxxx xxxx	2000-3FFF
4000::/3	010x xxxx.	xxxx xxxx	4000-5FFF
6000::/3	011x xxxx.	xxxx xxxx	6000-7FFF
8000::/3	100x xxxx.	xxxx xxxx	8000-9FFF

A000::/3	101x xxxx.	xxxx xxxx	A000-BFFF
C000::/3	110x xxxx.	xxxx xxxx	C000-DFFF
E000::/4	1110 xxxx.	xxxx xxxx	E000-EFFF
F000::/5	1111 0xxx.	xxxx xxxx	F000-F7FF
F800::/6	1111 10xx.	xxxx xxxx	F800-FBFF
FC00::/7	1111 110x.	xxxx xxxx	FC00-FDFF
FE00::/9	1111 1110.	0xxx xxxx	FE00-FE7F
FE80::/10	1111 1110.	10xx xxxx	FE80-FEBF
FEC0::/10	1111 1110.	11xx xxxx	FEC0-FEFF
FF00::/8	1111 1111.	xxxx xxxx	FF00-FFFF

En resumen, a continuación se muestra la información que no hay que olvidar para identificar el tipo de una dirección IPv6:

Categoría de dirección	Prefijos	Mínimo	Máximo
Unicast global	2000::/3	2000	3FFF
Unicast local	FC00::/7	FC00	FDFF
Unicast de conexión local	FE80::/10	FE80	FEBF
Multicast	FF00::/8	FF00	FFFF

h. Segmentación de las categorías

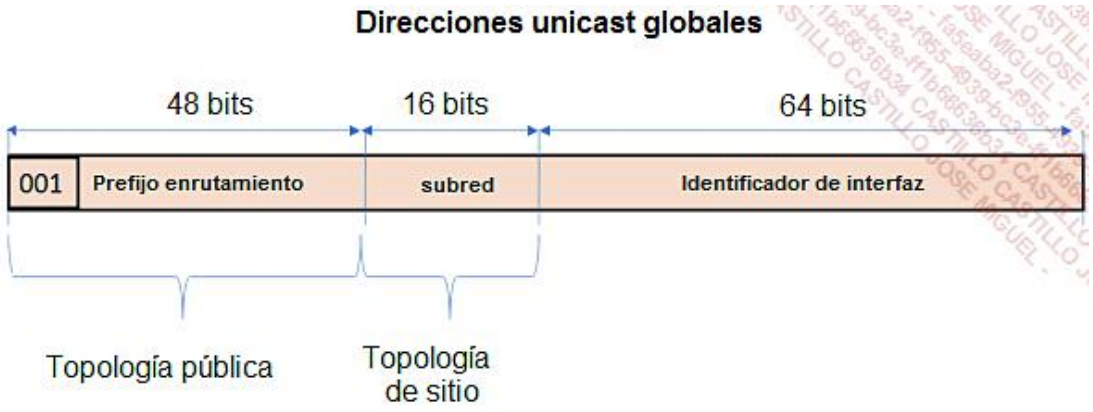
Unicast global

Son las equivalentes de las direcciones públicas en IPv4.

La categoría *unicast* global se define de la siguiente manera:

2000::/3	001x xxxx.	xxxx xxxx	2000-3FFF

Se descompone así:

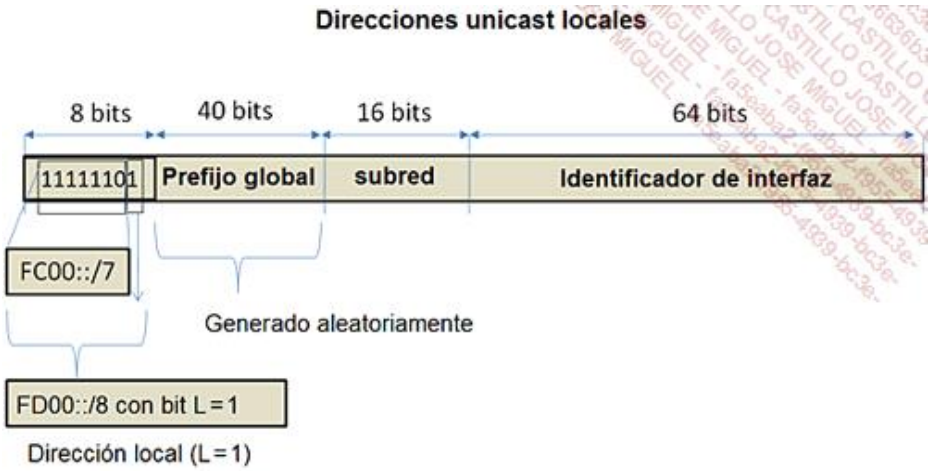


El identificador de interfaz se construye según EUI-64 modificado.

Dirección unicast local

Se trata del equivalente de las direcciones IP privadas en IPv4 (RFC 1918).

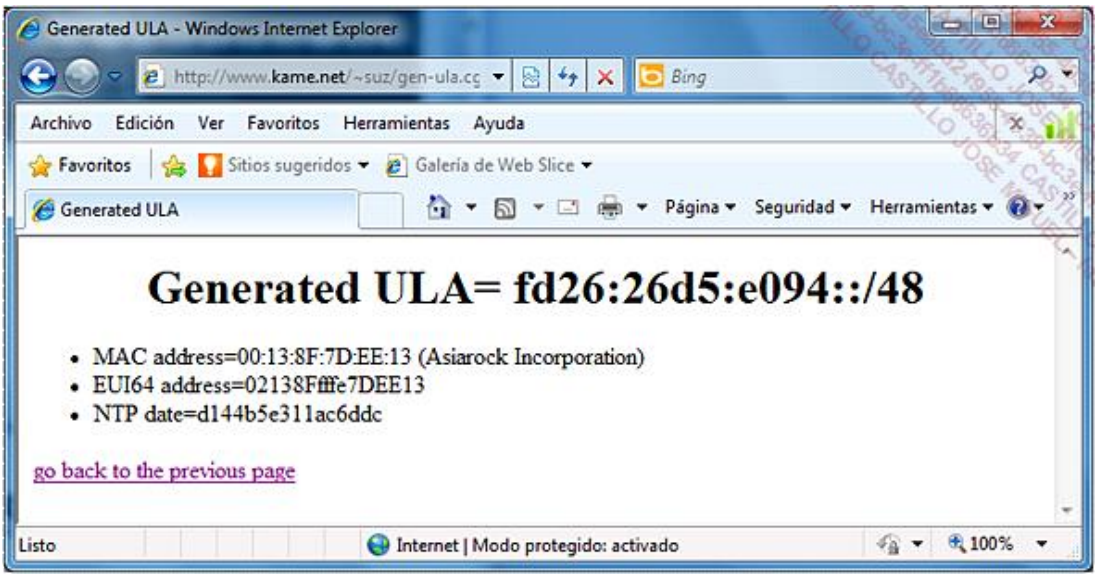
El prefijo de base que designa este tipo de direcciones es FC00-FDFF (FC::/7).



Estas direcciones no se pueden utilizar más que en un ámbito restringido. Sin embargo, dado el número de combinaciones y el algoritmo utilizado para generar aleatoriamente el prefijo global, es poco probable que en la interconexión de dos redes privadas haya un problema de rango de direcciones ya existentes.

De hecho, el algoritmo utilizado se basa en la dirección MAC de la interfaz y en la hora actual para generar este identificador.

Algunos sitios ofrecen generar identificadores a partir de la dirección MAC para ilustrar este algoritmo:



ULA hace referencia al acrónimo *Unicast Local Address*, una dirección unicast local.

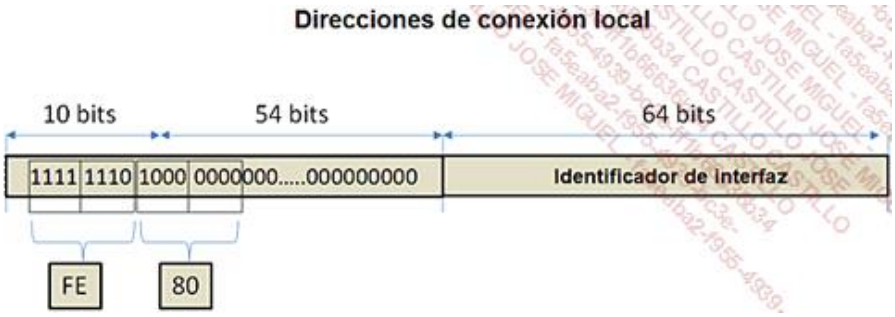
Unicast de conexión local

El concepto de conexión local permite a una interfaz tener una identidad en el envío de tramas iniciales de descubrimiento de red. Esta dirección se conservará incluso cuando más adelante se asigne una dirección global. Esto permite comunicar con una identidad real, al contrario que IPv4, en que la dirección tiene el valor 0.0.0.0 hasta que las fases iniciales de obtención IP hayan finalizado.

Esta dirección servirá principalmente para encontrar equipos vecinos o routers.

Esta dirección no pasará de los routers y solo servirá dentro de la subred.

La estructura de esta dirección es la siguiente:



Multicast

La dirección *multicast* se define con un ámbito con el que puede tener una cierta visibilidad en la red, y dispone de un estado que le permite ser reconocida como permanente (oficialmente asignada por IANA) o temporal.

El prefijo asociado a las direcciones *multicast* es FF::/8 y el rango de direcciones, de FF00 a FFFF.

El campo **Estado** define un estado asociado a la dirección *multicast* de 4 bits:

0 R P T

El bit T o Transitorio indica si la dirección es temporal o permanente.

Si T = 0, la dirección *multicast* constituye una dirección conocida, asignada de manera permanente por IANA. Por el contrario, T = 1 indica que la dirección se ha asignado por un tiempo (Temporal) limitado y, en este caso, esta dirección solo tiene sentido en su ámbito.

El bit P, «Prefijo», indica si la dirección multicast se basa en el prefijo de red (P = 1) o no (P = 0).

P = 1 indica que la dirección se construye a partir del prefijo de red y, en este caso, se trata de una dirección asignada de manera temporal (T = 1).

La principal funcionalidad del *multicast* es permitir crear grupos en las comunicaciones que puedan tener lugar. Se hablará de **punto de encuentro** para designar el router o el servidor alrededor del cual el grupo se tendrá que registrar para acceder a cualquier servicio (RFC 3956).

El bit R indica si la dirección *multicast* se construye (R = 1) o no (R = 0) a partir de la dirección de red de un punto de encuentro.

Si R = 1, P = 1 y T = 1, el prefijo de la dirección multicast es FF7::/12.

La RFC 3956 indica el contenido del campo **Identificador de grupo** en este caso.

El campo **Ámbito** permite especificar el ámbito de la dirección *multicast*:

Ámbito	Valor hexadecimal	Valor binario
Interfaz	1	0001
Conexión	2	0010
Sitio	5	0101
Organización	8	1000
Global	E	1111

Las direcciones multicast entre FF01:: y FF0F:: son direcciones reservadas.

Ejemplos:

FF02::2 identifica a todos los routers de conexión local.

FF05::1:3 identifica a todos los servidores DHCP del sitio local.

FF0E::101 corresponde a todos los servidores NTP en Internet (E = Global).

Las direcciones reservadas están disponibles en la siguiente dirección: http://www.iana.org/assignments/ipv6-multicast-addresses/

i. Autoconfiguración de las direcciones IPv6

Tipos

Existen dos tipos de autoconfiguración:

- Con estado.
- Sin estado.

Configuración con estado

Desde que un equipo IPv6 detecta la presencia de un router, examina los mensajes enviados por este para saber si hay algún servicio DHCPv6 configurado. Si el router responde que puede haber un servicio DHCPv6 implementado o si no se recibe ningún mensaje, el equipo IPv6 enviará un mensaje para intentar encontrar un servidor DHCPv6. Este mensaje se envía utilizando una dirección multicast específica que emplea el ámbito de conexión local, para garantizar que el mensaje no se dirija más allá del router.

Configuración sin estado

Se trata de una extensión del funcionamiento de DHCPv6. El equipo IPv6 se basa en la información recibida por el router para configurar una dirección en su interfaz. Simplemente va a recuperar los 64 primeros bits de la dirección origen del router enviando un mensaje y completando su identificador de interfaz (EUI-64).

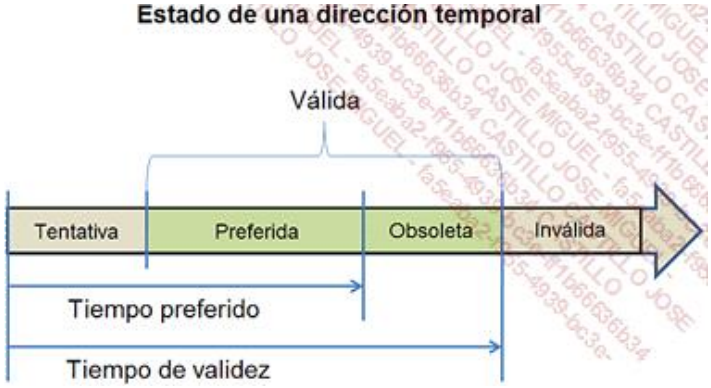
Por lo tanto, tan pronto como se hayan configurado manualmente las direcciones IPv6 de los routers, se les asignará un número de red correcto a todos los equipos «sin estado» (el recibido del router).

Originalmente, este tipo de configuración se concibió que para los teléfonos móviles, PDA y otros dispositivos pudieran obtener direcciones automáticamente, sin necesidad de implementar un servidor DHCPv6.

Estados de direcciones autoasignadas

Las direcciones autoconfiguradas pueden tener uno de los siguientes estados:

- Tentativa.
- Válida (Preferida, Obsoleta).
- Inválida.



Tentativa

La dirección está en proceso de verificación. Esta prueba permitirá asegurar que no existen direcciones duplicadas. No se puede recibir ningún tráfico unicast por una dirección «tentativa». En contraposición, se pueden enviar o recibir mensajes *multicast* durante la fase de detección de direcciones duplicadas (algoritmo *Duplicate Address Detection* (DaD), basado en el protocolo *Neighbor Discovery Protocol* (NDP)).

Válida

La dirección se puede utilizar para la emisión o recepción de tráfico *unicast*. El estado «válida» engloba también los estados «Preferida» y «Obsoleta».

El mensaje del router incluye el campo «Tiempo de validez», que corresponde a la suma de los tiempos asociados a los estados «Tentativa», «Preferida» y «Obsoleta».

Preferida

La dirección es válida, se ha comprobado que es única y se puede utilizar sin limitación.

El tiempo de vida preferido enviado por un mensaje de un router define la suma de los tiempos asociados a los estados «Tentativa» y «Preferida».

Por ejemplo, un router CISCO ofrece por defecto un Tiempo de validez de 30 días y un Tiempo de vida de 7 días.

Obsoleta

La dirección es válida, se ha comprobado que es única, pero se desaconseja su utilización para nuevas comunicaciones. Las sesiones en curso pueden continuar utilizando estas direcciones obsoletas.

Inválida

Una vez que ha pasado el Tiempo de validez, la dirección pasa al estado «Inválida». La dirección ya no se puede utilizar para la emisión/recepción de tráfico *unicast*.

4. Túneles

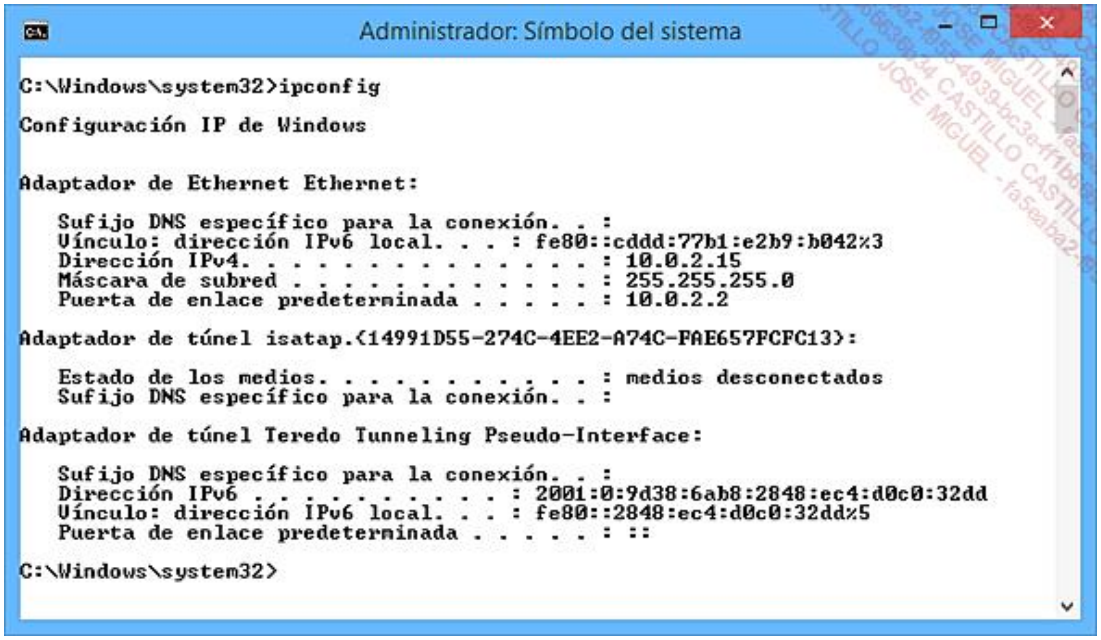
a. Introducción

En IPv6, el concepto de túneles es muy importante. Sobre todo va a permitir la implementación de IPv6 en redes distantes incluso cuando la conectividad IPv6 no sea total.

De hecho, con IPv6, aparecen las nuevas interfaces de Tunneling. Se pueden encontrar tarjetas de:

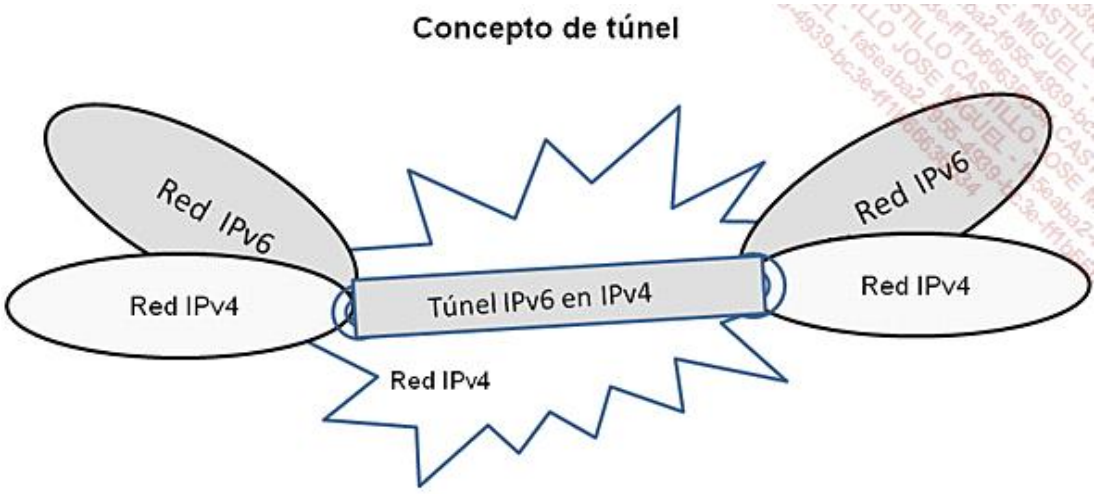
- Túnel 6to4.
- Túnel Teredo.
- Túnel ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*).

En la siguiente imagen se muestran las tarjetas Teredo e ISATAP en un ordenador Windows 8.1 con IPv6 activado (por defecto):



b. Tipos de túneles

Existen diferentes tipos de túneles para permitir que los equipos situados en sitios IPv6 puedan comunicarse a través de redes IPv4:



Se pueden diferenciar dos tipos de túneles, los configurados y los automáticos.

Túneles configurados

Se trata de túneles definidos manualmente por el administrador de red. Cada extremo se configura con la dirección IP del «final del túnel». De este modo, es posible implementar un túnel IPv6 a través de una red IPv4. Los dos extremos tienen que poder tratar tanto IPv4 como v6 para hacer de puerta de enlace.

Túneles automáticos

Se trata de un túnel abierto de forma dinámica, a petición. Como en el caso de los túneles configurados, el objetivo aquí es permitir ampliar la conectividad IPv6 a través de redes IPv4.

Los mecanismos de túneles automáticos más conocidos son los siguientes:

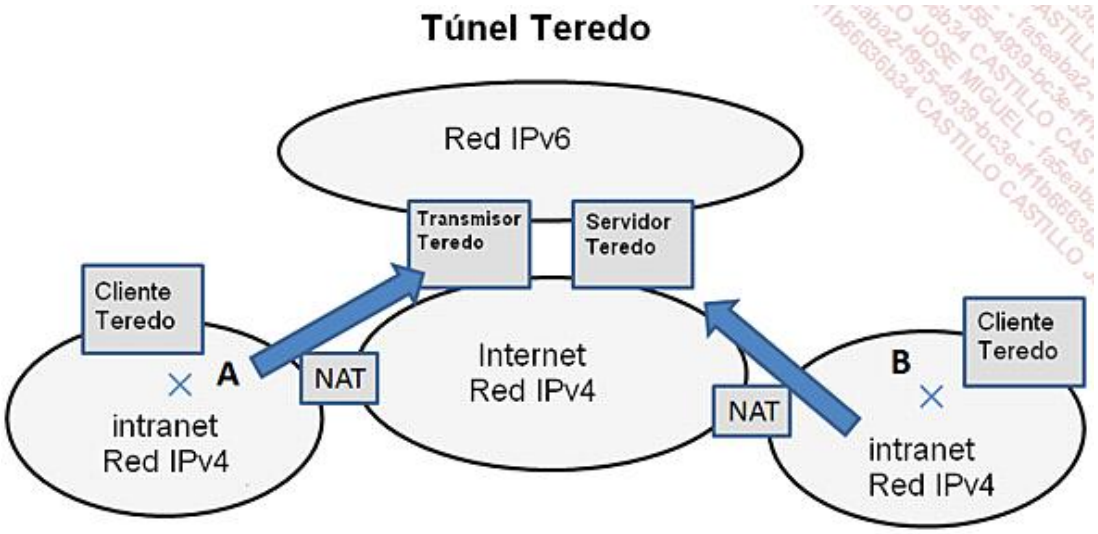
- Túneles Teredo.
- Túneles ISATAP.
- Túneles 6To4.

Túnel Teredo

El Túnel Teredo se describe en la RFC 4380 (febrero de 2006).

Se trata de pasar un túnel IPv6 en la UDP/IPv4 basándose en un mecanismo de traducción de direcciones (NAT - *Network Address Translation*).

Este mecanismo descansa en la existencia de equipos específicos (servidores o routers) que actúan como Servidor o Transmisor Teredo:



En este ejemplo, A y B se sitúan en dos redes privadas y accesibles a través de una traducción de dirección.

A1 es la interfaz pública a la que está asociado el acceso a A.

Lo mismo ocurre con B1, que permite acceder a B.

Se define un puerto específico para A1 y B1 para el acceso a un puerto similar a A y B.

La dificultad de esta configuración reside en la complejidad de la dirección obtenida y sobre todo en su falta de legibilidad.

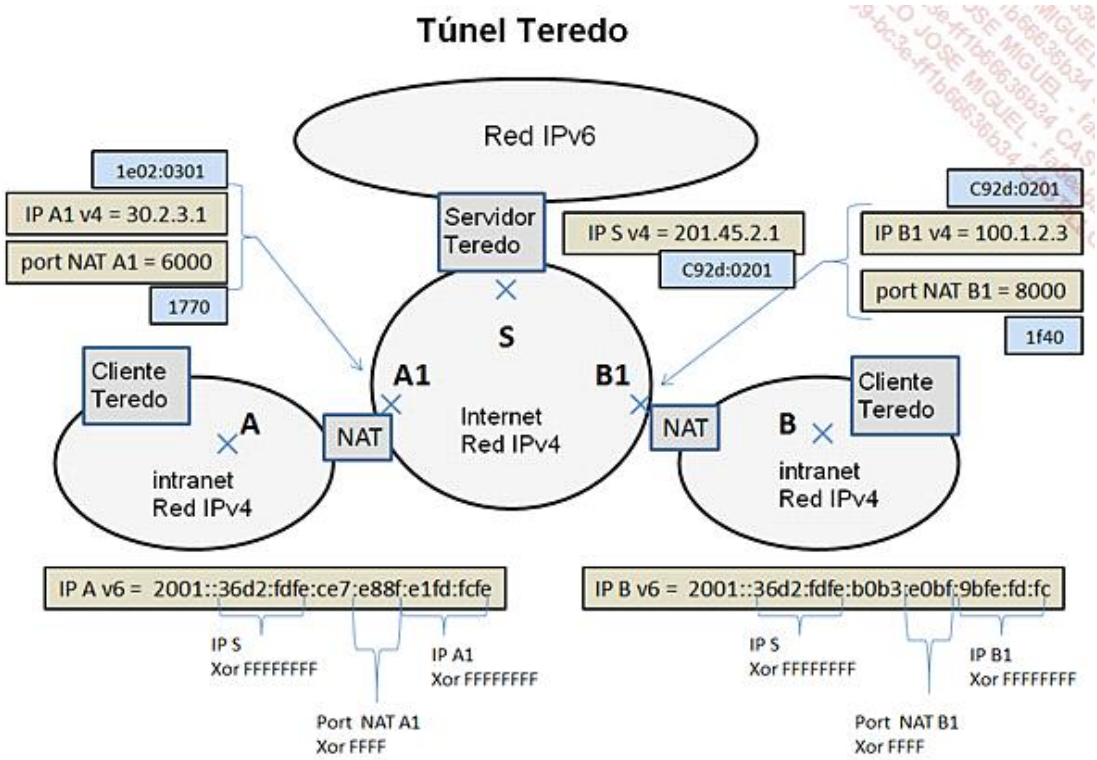
En un principio, la idea es interesante.

La dirección IP del servidor (S) se incluye directamente en la parte de red de las direcciones de A y B.

La dirección IP publica así que el puerto que se utiliza para el mapeado en la interfaz pública se integra igualmente en la dirección generada.

Sin embargo, realmente falta legibilidad: hay que establecer la correspondencia de las direcciones IPv4 en

hexadecimal y es necesario realizar un O Exclusivo (XOR) para obtener el valor de destino.



Túnel ISATAP

Se basa en la RFC 5214 (marzo de 2008).

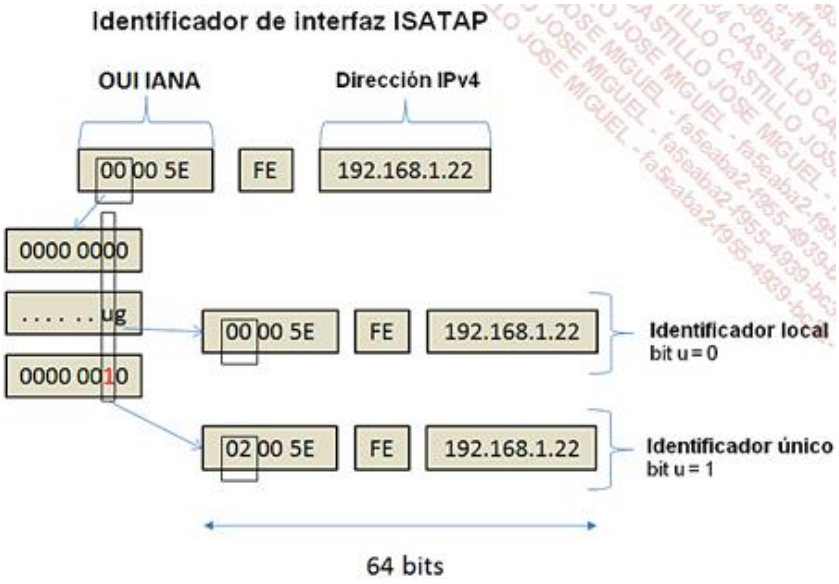
Esto permite a los nodos que disponen de dos pilas de protocolos (IPv4/IPv6) «ver» la red IPv4 como una capa de conexión para IPv6.

El número de red utilizado puede ser un prefijo global, el correspondiente a una dirección de conexión local: **FE80::/64**

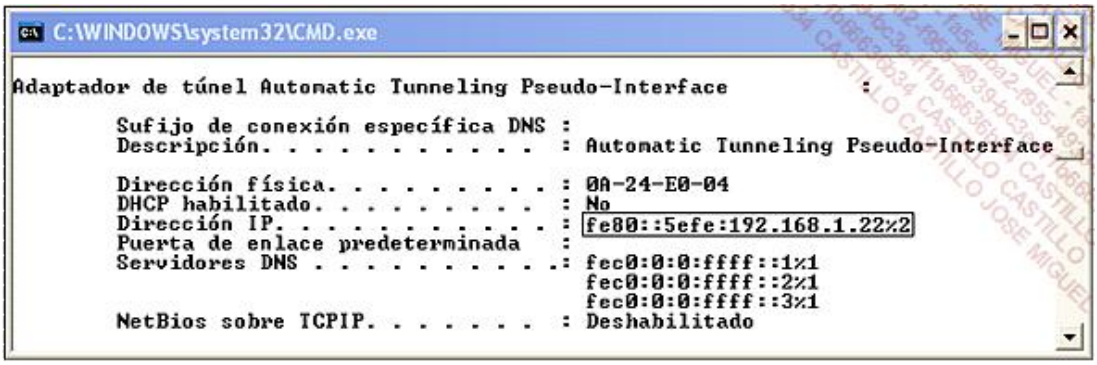
Los identificadores de interfaz se autogeneran utilizando una construcción EUI-64 modificada con un solo byte «FE» en lugar de «FF FE». De hecho, la dirección IPv4 ya utiliza 4 bytes.

La parte «izquierda» del identificador se basa en el identificador IANA «00-00-5E».

Para una dirección IP privada, el bit u se establece a 0 (por defecto):



Observe la notación mixta IPv6/IPv4 provocada:



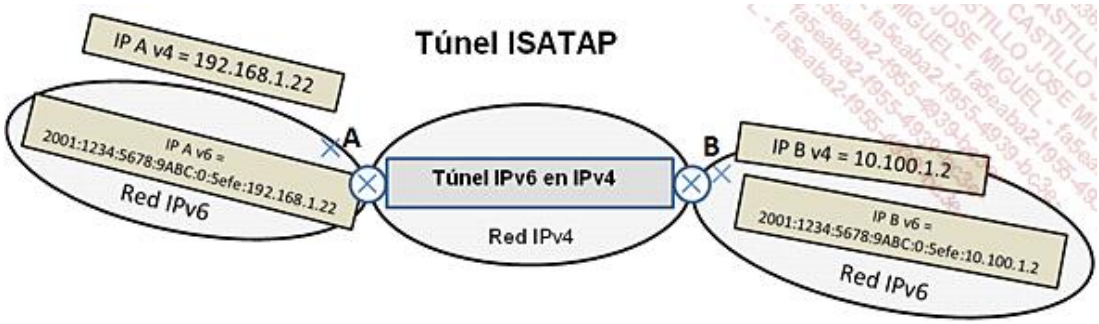
ISATAP está disponible en Windows XP, Windows Vista, Windows 7, Linux (a partir del núcleo 2.6.25), así como a partir de algunas versiones del SO Cisco (12.3T).

Existen dos tipos de configuración para un nodo ISATAP:

- cliente,
- servidor.

El nodo ISATAP cliente hace una consulta sobre una dirección IPv4 (nodo ISATAP servidor) para obtener una dirección IPv6 y así formar el túnel. El nodo servidor puede ser un SO de tipo servidor o incluso un router.

Tenga en cuenta que, al contrario que en los otros túneles, ISATAP no implementa la función NAT. Hay que pasar obligatoriamente por los routers.

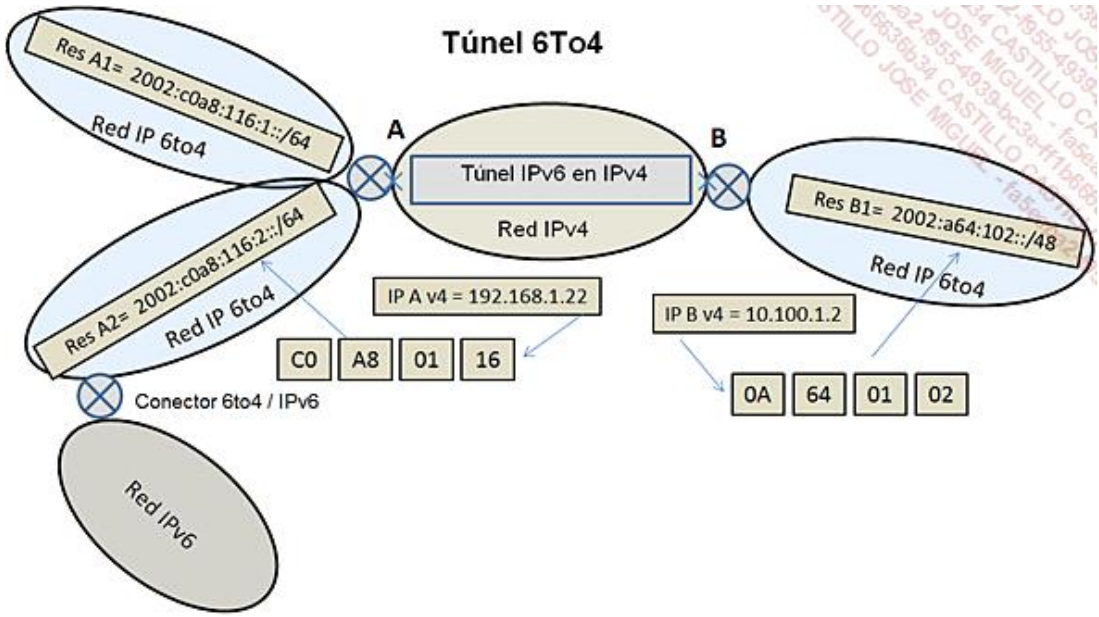


Túnel 6To4

Este tipo de túneles se define en la RFC 3056.

Se basa en un rango de direcciones reservado por la IANA: **2002::/16**

Las interfaces de túnel simplemente tienen necesidad de una dirección de origen, ya que las direcciones de destino se obtienen automáticamente a partir del destino de un paquete: la dirección IPv4 de salida del túnel se utiliza para construir el número de red de destino. Cuando se enrutan varias redes, se utiliza un sufijo complementario para diferenciarlas:



Este tipo de túnel solo permite relacionar redes 6to4. Si se quieren conectar redes IPv6, es necesario utilizar un conector específico (6to4/IPv6).

5. Organismos de asignación de direcciones

Existen cinco organismos repartidos por el mundo que se ocupan del registro para Internet (principalmente los nombres de dominios DNS y las direcciones IPv4 y v6). Se habla de *Regional Internet Registries* (RIR). Su función es proporcionar una implementación global de Internet a traves de:

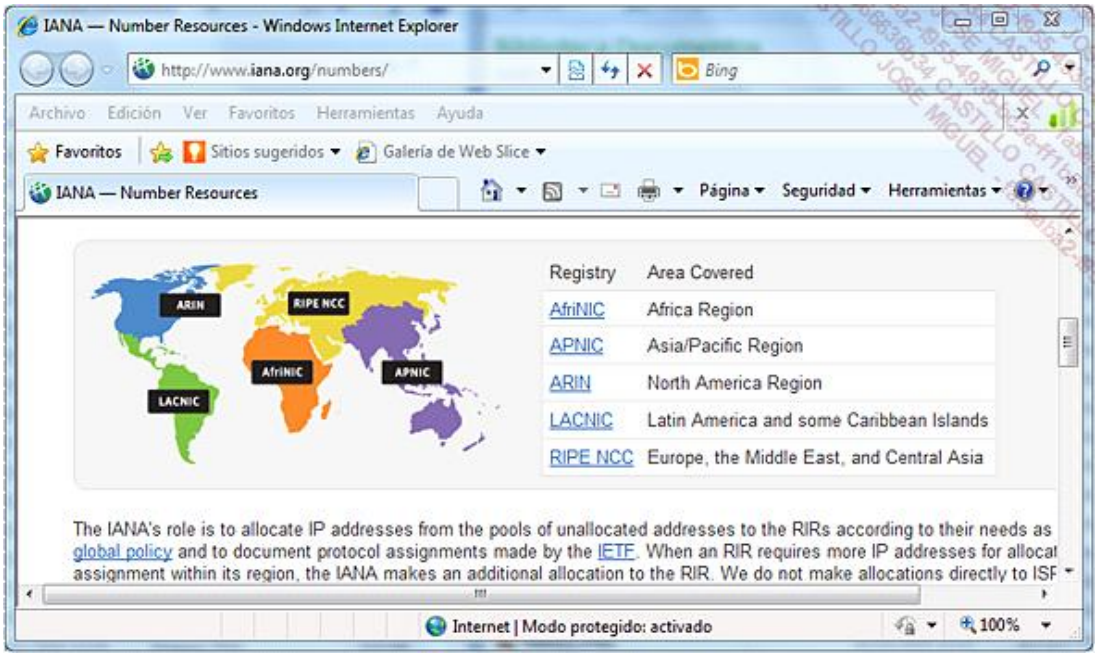
- La asignación de recursos de Internet.
- Servicios de registro.

- Actividades de coordinación.

Estos cinco organismos son:

- ARIN (*American Registry for Internet Numbers*).
- RIPE NCC (*Réseau IP Européens Network Coordination Center*).
- LACNIC (*Latin American and Caribbean Internet Address Registry*).
- AfriNIC (*African Network Information Centre*).
- APNIC (*Asia Pacific Network Information Centre*).

El sitio web www.iana.org detalla esta información:



Como complemento, existen organismos a nivel de cada país, los NIR (*National Internet Registries*), y algunas veces incluso una delegación más localizada, la LIR (*Local Internet Registry*), como un PAI (proveedor de acceso a Internet).

6. Cabecera IPv6

Esta cabecera es mucho más sencilla si se la compara con la de IPv4.

Los 32 primeros bits de la cabecera del paquete se componen de la siguiente forma:

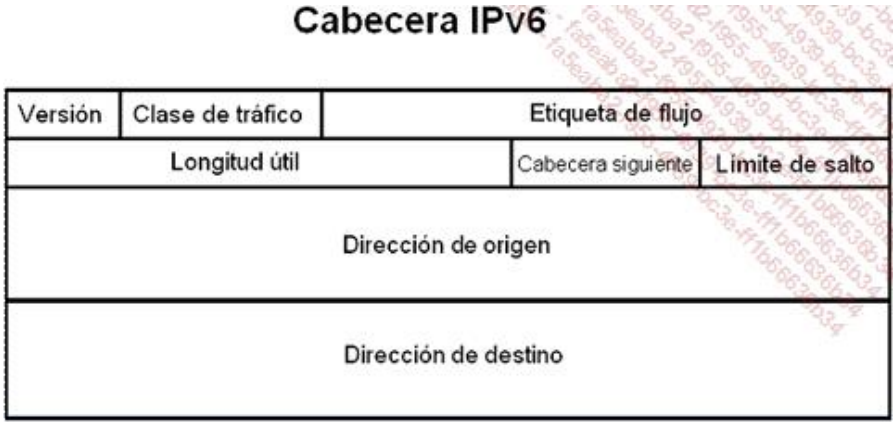
- Un número de versión de 4 bits.
- Un byte para definir la clase de tráfico (prioridad).
- El resto define una etiqueta de flujo (*Flow label*) para el marcado de paquetes especiales.

Los siguientes 32 bits definen:

- La longitud útil de los datos, en 16 bits.
- El tipo de cabecera siguiente de la IPv6 (*Next Header*).

- El límite de salto (*Hop Limit*), indicando el tiempo de vida del paquete en 8 bits.

Los siguientes campos son la dirección de origen y la dirección de destino en 128 bits.



Estos campos de tamaño fijo facilitan un tratamiento más rápido y el alineamiento en 64 bits. En relación con IPv4, hay más tratamientos de tipo *checksum*.

El concepto de TTL (*Time To Live*) se encuentra en el límite de salto. Permite que se elimine un paquete, cuando no se encuentra el destinatario, después de haber pasado por cierto número de elementos activos.

Después de la cabecera IPv6 se pueden insertar otras cabeceras. La información Next Header sirve para indicarlo. De este modo, se marcan los paquetes especiales.

Los tipos pueden ser los siguientes:

- *Routing Header*, para el camino de enrutamiento.
- *Fragment Header*, en caso de fragmentación de paquetes.
- *Authentication Header*, para la seguridad.
- *Hop-by-hop Options Header*, transporte de información encaminada a cada nodo.
- *Privacy Header*, para el cifrado.
- *End-to-end Options Headers*, si el destinatario debe examinar los datos.

El campo **Next Header** de la última cabecera contiene: TCP.