Parte I

Protocolo de Internet V6

1. Historia

- 1969 Arpanet, una red de computadoras creadas por encargo del Dpto de Defensa de Estados Unidos para utilizarla como medio de comunicación entre las diferentes instituciones académicas y estatales. El primer nodo fue creado en la Universidad de California en Los Ángeles (UCLA), y fue la espina dorsal de Internet hasta 1990, tras finalizar la transición al protocolo TCP/IP, iniciada en 1983. Se incluian definiciones sobre lo que se conoce como Internet.
    - Red decentarlizadas.
    - Multiples Caminos.
    - División de Mensajes en fragmentos con distintos caminos (fallas)
- 1981 IPv4 surge IPV4 en la RFC 791.
- 1983 ARPANET Adopta los protocoles TCP/IP.
- 1990 1ros estudios sobre Agotmiento de Direcciones. (hace + 20 años).
- 1993 Internet comienza a ser comercial.
- Gobierno de EEUU libera Internet para uso comercial.
- Se intensifica la discusión sobre el agotamiento.
- Creció 2x106 en 1993 a 26x106 para 1997.

Video de NIC

1.1. Agotamiento de IPV4

Las direcciones IPv4 , permite identificar la interfaz de red en todo internet. Estas IP debe ser única, para que funcione.

Sabemos que para IPV4 la cantidad de Direcciones posibles se forman con 32 bits.

Por lo tanto IPv4 = 4.294.967.296 (2^{32}).

Esto a priori parecía una cantidad extremadamente alta, pero no fué así. Algunas desiciones sumadas al gran crecimiento causaron que esta cantidad de direcciones no fuera suficiente.

Los routers de Internet, son los que analizan el camino a seguir para llegar de una IP de origen a otra IP de destinto, siempre hablando de IP Púbicas. Como ya vimos IPv4, tiene 32 bits para generar las IP, sobre este espacio, no se ha asignado con efectividad, lo que perjudicó la falta de Ips.

La IANA, Internet Assigned Numbers Authority es la entidad que supervisa la asignación global de direcciones IP, sistemas autónomos, servidores raíz de nombres de dominio DNS y otros recursos relativos a los protocolos de Internet. Actualmente es un departamento operado por ICANN.

Figura 1: Distintas Regiones de IANA

ICANN , la Corporación de Internet para la Asignación de Nombres y Números, es una organización sin fines de lucro creada el 18 de septiembre de 1998 con objeto de encargarse de cierto número de tareas realizadas con anterioridad a esa fecha por otra organización, la IANA

El organismo que distribuye las IPs. Este organismo distribuye las IPs a los RIRS y estos a su vez a los ISP Internet Service Provider y estos a los usuarios finales.

RIRs es un sistema de Membresía, hay 5 RIRs, cada uno ubicado en una zona georgáfica. Cada RIR tiene sus propias políticas de asiganción de IPs.

Los principales registros son:

1. AfriNIC (African Network Information Centre), región África http://www.afrinic.net
2. APNIC (Asia Pacific Network Information Centre), región Asia/Pacífico http://www.apnic.net
3. ARIN (American Registry for Internet Numbers), región América del Norte http://www.arin.net
4. LACNIC (Regional Latin-American and Caribbean IP Address Registry), América Latina y algunas islas del Caribe http://www.lacnic.net
5. RIPE NCC (Reseaux IP Europeans), Europa, Medio Oriente y Asia Central http://www.ripe.net

El 3 de febrero de 2011 la IANA asignó su último bloque de direcciones IPs a los RIRs.

- APNIC, ultimas IPS 15 de Abril del 2011.
- RIPS NCC, ultimas Ips 14 de Septiembre de 2012
- ARIN, ultimas Ips 23 de Abril del 2014.
- LACNIC ultimas Ips 10 de Junio del 2014.
- AFRINIC , es el único RIR que todavía no entró en face de agotamiento de direcciones IPv4.

1.1.1. Niveles de ISP.

Los ISP se designan mediante una jerarquía basada en su nivel de conectividad al backbone de Internet. Cada nivel inferior obtiene conectividad al backbone por medio de la conexión a un ISP de nivel superior. La Gerarquía o nivel se conoce como Tier y los hay Tier1, Tier2 y Tier3.

Desde los Tier1 hacia Tier3 se van distribuyendo las IPs.

Cuestiones como:

- Mala practica de asignación
- Clases A a IBM, HP, AT&T, etc
- Direcciones reservadas que no se usaron.

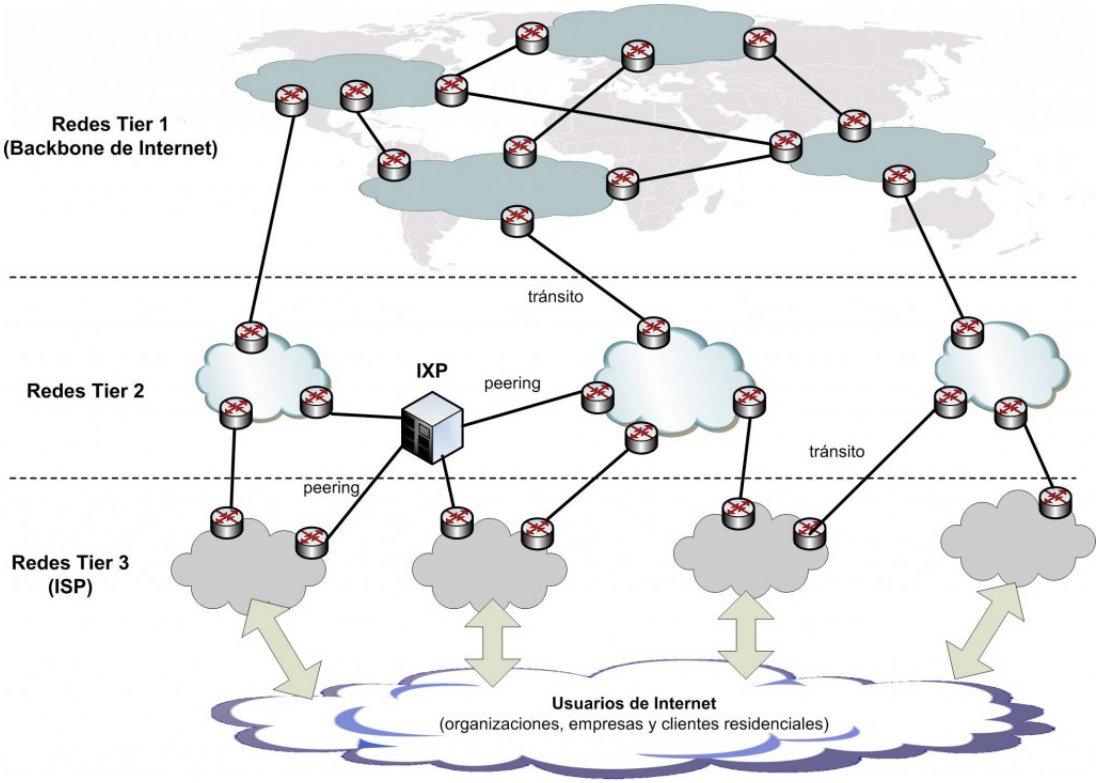


Figura 2: Niveles de ISP

- Crecimiento de Rutas BGP IPV4 (http://www.routeviews.org/dynamics/)

Hicieron que las direcciones de IPv4 que parecían tantas en un primer momento no sean suficientes, esto se vió venir a los pocos años de que se comenzó utilizar IPv4.

Veamos como crecieron las cantidades de desde 1998 al 2003

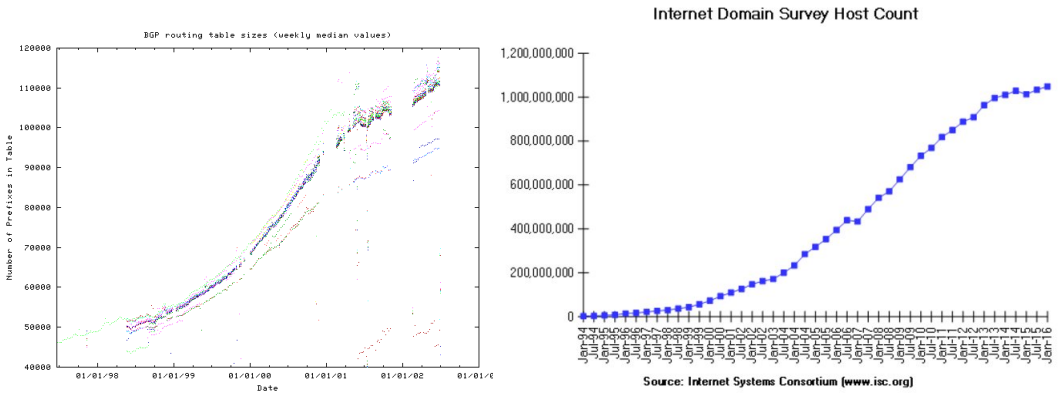


Figura 3: Crecimiento de Rutas y Hosts.

Las gráficas son mas que elocuentes respecto del crecimiento. La gráfica de crecimiento de Host se obtuvo del sitio www.isc.org

El crecimiento se volvería a acelerar, con la aparición de los

- Smartphones,
- Tables, Palmtop (conocidas como Notebooks aquí)
- modems
- 3g o 4g

Todo esto superaría 2,25 billones de equipos y todavía no se incorpora IoT.

El crecimiento en los últimos años fue superior al 400 %. La migración deberá comenzar por los proveedores ISP, que deben adecuar sus equipos, para poder ofrecer a los usuarios nuevos servicios.

1.2. Internet de las cosas: IoT

En la actualidad, Internet es significativamente distinta de como era en las últimas décadas. Hoy en día, Internet es más que correo electrónico, páginas Web y transferencia de archivos entre PC. Internet evoluciona y se está convirtiendo en una Internet de las cosas. Los dispositivos que acceden a Internet ya no serán solamente PC, tablet PC y smartphones. Los dispositivos del futuro preparados para acceder a Internet y equipados con sensores incluirán desde automóviles y dispositivos biomédicos hasta electrodomésticos y ecosistemas naturales. Imagine una reunión en la ubicación de un cliente que se programa en forma automática en la aplicación de calendario para que comience una hora antes de la hora en que normalmente comienza a trabajar. Esto podría ser un problema importante, en especial si olvida revisar el calendario o ajustar el despertador según corresponda. Ahora imagine que la aplicación de calendario comunica esta información directamente al despertador para usted y su automóvil. El automóvil calienta automáticamente para derretir el hielo del limpiaparabrisas antes de que usted ingrese y cambia la ruta hacia el lugar de la reunión. Para este escenario presentado , IPv4 no podría satisfacer las necesidades.

1.3. Soluciones.

Apenas en 1990 , antes de que se comience a explotar comercialmente internet, ya un grupo visionario vió el problema en el horizonte y se comenzaron a trabajar en alternativas. Esttas aparecieron en 1992.

1. En 1992 IETF crea el Grupo ROAD (Routing Addressing) comienza a estudiar posibles soluciones.
2. CIDR (RFC 4632) Dejar de usar Clases.
    a) Bloques de direcciones de tamaño apropiado a las necesidades y usos.
    b) Dirección de red = prefijo/longitud.
3. Agregación de rutas.DHCP.
    a) NAT + RFC 1918 :
    b) En el año 1995 se comienza a usar NAT + CIDR.
        1) Permite usar una Dirección Pública para una Toda una red.
        2) Problema. Acceso y fué insuficiente.

Observación: Ver que el problema de falta de Direcciones se comenzó a tratar en 1990, solo apenas 9 años desde su implementación en 1980..

A continuación les dejo un par de videos que hablan sobre este tema:

- Por que debemos implementar IPV6(LACNIC)?
- Desarrollo de IPV6 en la región (LACNIC)

Existen varios protocolos de capa de red; sin embargo, solo los dos que se incluyen a continuación se implementan en Iternet frecuencia, como se muestra en la ilustración:

- Protocolo de Internet versión 4 (IPv4)
- Protocolo de Internet versión 6 (IPv6)

Otros protocolos de capa de red antiguos que no tienen un uso muy difundido incluyen los siguientes:

- Intercambio Novell de paquetes de internetwork (IPX)
- AppleTalk
- Servicio de red sin conexión (CLNS/DECNet)

Podemos decir que de todos estos los que están ampliamente difudidos son IPv4 que está en visperas de desaparecer y IPv6 que está en vísperas de popularizarse.

2. Entendiendo IPV6 Direccionamiento y Subredes

En 1992, el IETF crea el grupo IPng (IP Next Generation) que sería el IP v6. Diseñado por Steve Deering de Xerox PARC y Craig Mudge, IPv6 sujeto a todas las normativas que fuera configurado –está destinado a sustituir a IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India, y otros países asiáticos densamente poblados. El nuevo estándar mejorará el servicio globalmente; por ejemplo, proporcionará a futuras celdas telefónicas y dispositivos móviles sus direcciones propias y permanentes.

El cambio, IPv6 admite 340.282.366.920.938.463.463.374.607.431.768.211.456 (2128 o 340 sextillones de direcciones) —cerca de 6,7 × 1017 (*670 mil billones) de direcciones por cada milímetro cuadrado de la superficie de la Tierra*.

El gobierno de los Estados Unidos ordenó el despliegue de IPv6 por todas sus agencias federales en el año 2008, nuestro país está bastante lejos de esto.

> Tarea para el Alumno.
> 1)Calcular las direcciones posibles para una Oficina de 10 m x 20 m.
> 2)Calcular las direcciones posibles para un Edificio de 10 pisos con oficinas de 10x20.+

Este grupo, tomando como referencia IPv4, debía encontrar respuestas sobre como mejorar en la nueva implementación algunos puntos como ser:

- Escalabilidad
- Seguridad
- Configuración y Administración.
- Soporte QoS
- Movilidad
- Políticas de Ruteo
- Transición (de IPv4 a IPv6)

Las soluciones propuestas cayeron en una terna, las demás se descartaron:

- SIPP
- TUBA
- CATNIP

Ninguna de ellas cubría los deseado, pero si una combinación de dos de ellas.

- SIPP se toman los 128 bit
- TUBA se toma la configuración automática, que luego se llamará autoconfiguración, las cabeceras de extensión, y el CIDR.

CATNIP, fué descartada por considerarse la mas incompleta.

Por lo tanto SIPP + TUBA = IPV6 en RFC 2460 año 1998.

La norma que establecio IP v6 es la RFC 2460
Resumiendo la RFC2460

- 128 bits para Direccionamiento.
- Cabecera base simplificada.
- Cabeceras de extensión.
- Son opcionales y puede haber varias.
  - Proveen información adicional.
  - Hay una cantidad limitada de Extension Headers.
  - Se ubican entre la cabecera IPv6 y la cabecera de la capa superior.
  - Tienen que estar declaradas en la cabecera anterior.
  - Son para el host destino.
  - Se deben procesar en orden
- Identificación de flujo de datos (QoS).
- Mecanismos de IPSEC incorporados al protocolo[1]
- Fragmentación y Re-ensamblado de paquetes solo en origen y destino.
- No requiere el uso de NAT, permitiendo conexiones Punto a Punto.
- Mecanismos que facilitan la configuración de las redes.

Tarea para el Alumno. Comparar el resumen de IPv6/ RFC2460 y comparar con IPv4/RFC791

2.1. UDP IP v6 (Datagrama)

Veamos el formato del Datagrama.
Descripción de cada campo del Datagrama.

- Versión (4 bits): número de la versión del protocolo Internet; el valor es 6.
- Clase de tráfico (8 bits): disponible para su uso por el nodo origen y/o los dispositivos de encaminamiento para identificar y distinguir entre clases o prioridades de paquete IPv6. Este campo se usa actualmente para los campos de ceros y ECN, como se describió para el campo tipo de servicio en IPv4.
- Etiqueta de flujo (20 bits): se puede utilizar por un computador para etiquetar aquellos paquetes para los que requiere un tratamiento especial en los dispositivos de encaminamientodentro de la red; se discute después.
- Longitud de la carga útil (16 bits): longitud del resto del paquete IPv6 excluida la cabecera, en octetos. En otras palabras, representa la longitud de todas las cabeceras de extensión más la PDU de la capa de transporte.

[1] IPsec (abreviatura de Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

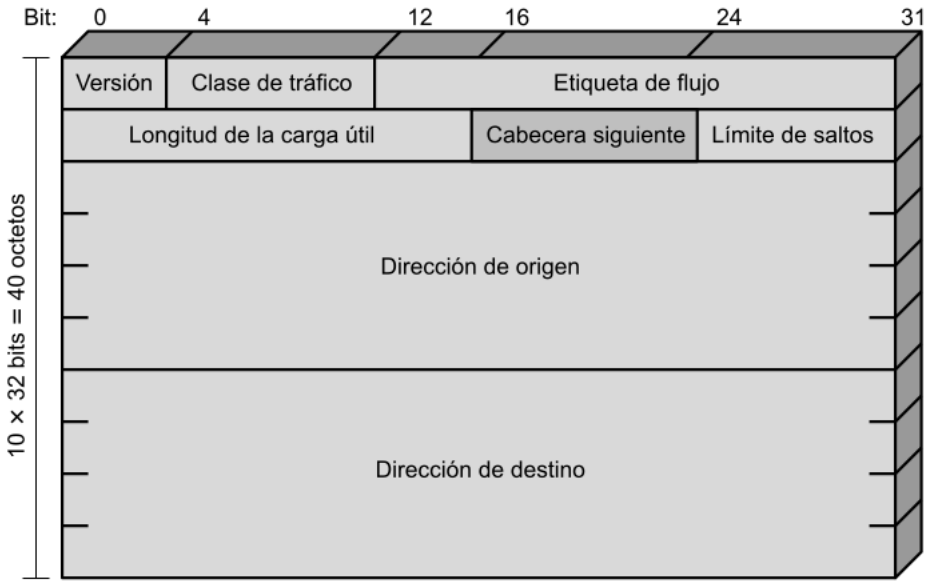


Figura 4: Datagrama IPv6

- Cabecera siguiente (8 bits): identifica el tipo de cabecera que sigue inmediatamente a la cabecera IPv6; se puede tratar tanto de una cabecera de extensión IPv6 como de una cabecera de la capa superior, como TCP o UDP.
- Límite de saltos (8 bits): el número restante de saltos permitidos para este paquete. El límite de saltos se establece por la fuente a algún valor máximo deseado y se decrementa en 1 en cada nodo que reenvía el paquete. El paquete se descarta si el límite de saltos se hace cero. Esto es una simplificación del procesamiento requerido por el campo tiempo de vida de IPv4. El consenso fue que el esfuerzo extra de contabilizar los intervalos de tiempo en IPv4 no añadía un valor significativo al protocolo. De hecho, y como regla general, los dispositivos de encaminamiento IPv4 tratan el campo tiempo de vida como un límite de saltos.
- Dirección origen (128 bits): dirección del productor del paquete.
- Dirección destino (128 bits): dirección de destino deseado del paquete. Puede que éste no sea en realidad el último destino deseado si está presente la cabecera de encaminamiento, como se explicará después.

Extension Headers

- Son opcionales y puede haber varias.
- Proveen información adicional.
- Hay una cantidad limitada de Extension Headers.
- Se ubican entre la cabecera IPv6 y la cabecera de la capa superior.
- Tienen que estar declaradas en la cabecera anterior.
- Son para el host destino.
- Se deben procesar en orden

MTU mínimo de 1280 octetos.

- Se recomienda mín 1500 octetos, para tunelizado.
- IPv6 no soporta fragmentación.

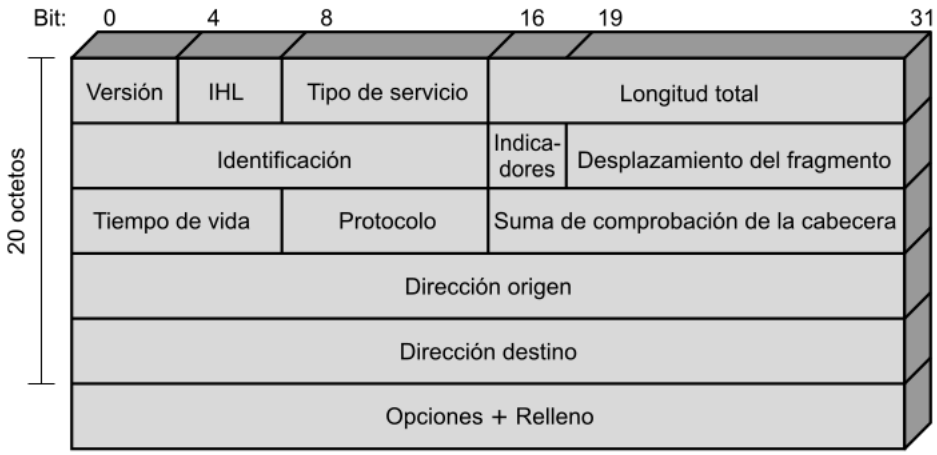


Figura 5: Datagrama IPv4

- Si un enlace no puede transmitir 1280 octetos, debe encargarse de la fragmentación en una capa inferior.
- Carga útil máximo de 64 KB.
- Jumbo Payload option rfc2675: 4 GB.

Para comparar con IPv4 presentemo el Datagrama IPv4

Podemos observar las siguiente diferencias:

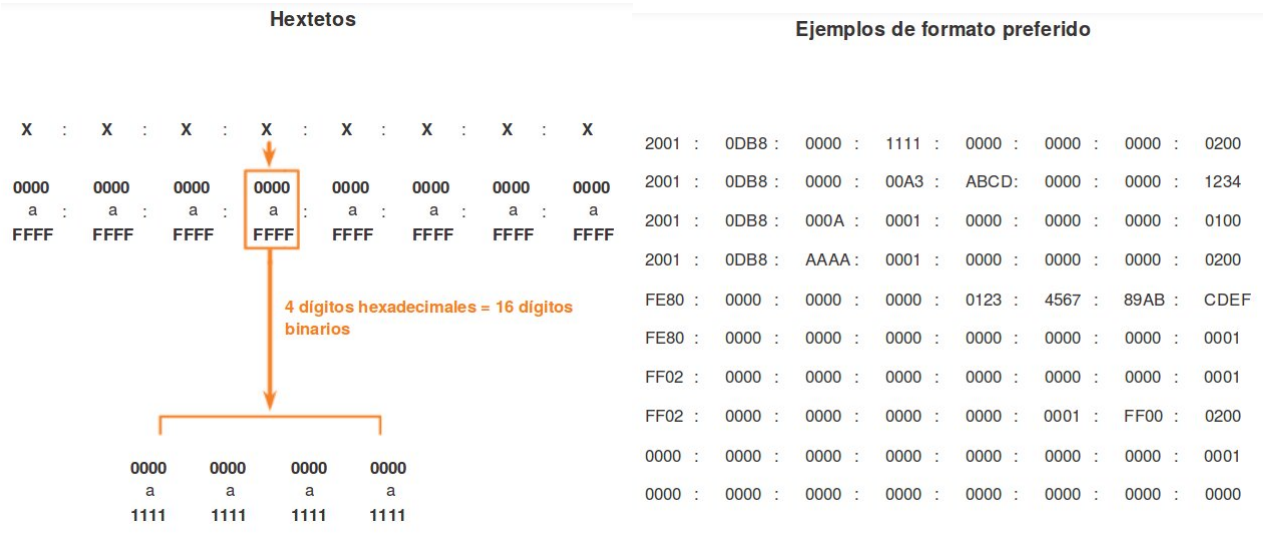
IPv6	IPv4
Largo Minimo del Header del Datagrama 40 bytes (132 bits)	Largo Minimo del Header del Datagrama 20 bytes (32 bits)
Campo de Direcciones 128 Bits (4 x 32)	Campo de Direcciónes 32 bits
1er Campo del Datagrama es la Versión	1er Campo del Datagrama es la Versión
Clase de Tráfico	Tipo de Tráfico, este se utiliza muy poco
Etiqueta de Flujo	
Longitud de la Carga Útil	
Cabecera Siguiente	
Límite de Saltos	Tiempo de Vida

2.2. Notación de direcciones IPV6

Les dejo un link a un Video de sobre la Direcciones de IPv6

En IPv6 no se usa la notación como en IPv4, aqui se usan la base numérica Hexadecimal 0, 1, ...9, A, B, C, D, E, F. (16 en total) .

- Un dígito Hexadecimal está formado por 4 bits. IPv6.
- La dirección IPv6 está formado por 8 Segmentos (partes) de 4 Dígitos Hexadecimales (8*4*4=128 bits)
- A los 16 bits se los llama Hextetos (no es un término formal), hay 8 hextetos.
- Representación recomendada x:x:x:x:x:x:x:x, x es de uno a cuatro dígitos hexadecimales de las ocho partes de 16 bits de la dirección. Ejemplo: ABCD:EF01:2345:6789:ABCD:EF01:2345:6789, 2001:DB8:0:0:8:800:200C:417A
- No es necesario escribir los ceros a la izq.
- Pero debe haber por lo menos un número en cada grupo.



Cuadro 1: Números Hexadecimales

2.2.1. Reglas para Compactar la Dirección IPv6, ya que es muy larga.

2.2.1.1. Regla de los 0 iniciales.

- Los ceros escritos a la izquierda no es necesario escribirlos.
  - Sin son 4 Ceros se debe dejar uno.

Ejemplos:

- 01AB puede representarse como 1AB.
- 09F0 puede representarse como 9F0.
- 0A00 puede representarse como A00.
- 00AB puede representarse como AB.
- 0000 se puede representar como 0.

```
2001:0DB8:0000:1111:0000:0000:0000:0200
2001: DB8:   0:1111:   0:   0:   0: 200
```

Cuadro 2: Regla de los ceros iniciales

2.2.1.2. Regla de dos puntos :: Por una única vez, una secuencia de ceros seguidos, contiguos de uno o mas segmentos pueden reemplazar por ::. Hay que evitar posibles de direcciones comprimidas ambiguas:

2.2.2. Sintaxis especial

- Se puede reemplazar uno o más grupos de 16 bits de ceros por "::"
- "::" solo puede aparecer una vez

Por ejemplo, las siguientes direcciones:

1. 2001:DB8:0:0:8:800:200C:417A a unicast address

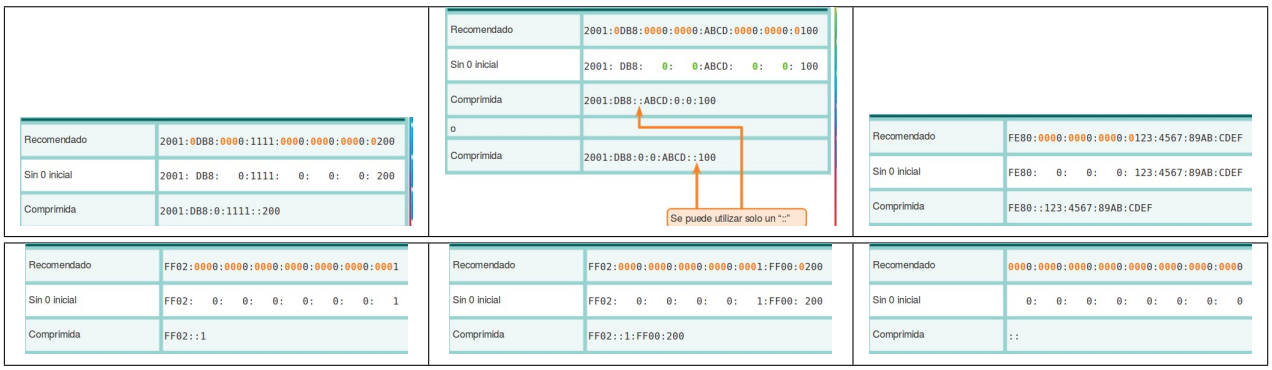


Figura 6: Regla de los dos puntos

2. FF01:0:0:0:0:0:0:101 a multicast address
3. 0:0:0:0:0:0:0:1 the loopback address
4. 0:0:0:0:0:0:0:0 the unspecified address

se pueden representar como:

1. 2001:DB8::8:800:200C:417A a unicast address
2. FF01::101 a multicast address
3. ::1 the loopback address
4. :: the unspecified address

2.2.3. Forma alternativa

Se permite la siguiente forma: x:x:x:x:x:x:d.d.d.d
Por ejemplo:

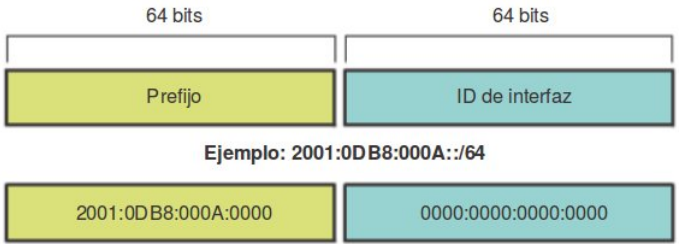
1. 0:0:0:0:0:0:13.1.68.3
2. 0:0:0:0:0:FFFF:129.144.52.38

en su forma comprimida:

1. ::13.1.68.3
2. ::FFFF:129.144.52.38

Tarea para el Alumno: Complete la línea punteada

1. 2001.1111.2222.3333.4444.5555.6666.7777 (esta está mal por. . . . .)
2. 2001:AAAA:BBBB:CCCC:DDDD:EEEE:FFFF:GGGG (esta está mal por. . . ..)
3. 2001:FACA:ACE0:1111:DDDD:EEEE:FFFF:4444:5555 (esta está mal por. . . ..)
4. 2001:FACA:ACE0:11111:DDDD:EEEE:FFFF:44444 (esta está mal por. . . ..)



Cuadro 3: Prefijo de Red

2.3. Representación del prefijo

Les dejo un Video de Representación de prefijo de red para introducir el tema.
La forma de notación es parecida a IPv4, sería: IPv6-address/prefix-length
En IPv4, Formato CIDR para escribir máscara o /x (255.255.255.0 /24) En IPv6 el prefijo se obtiene de la cuenta de bits o longitud del prefijo (/64) /64 me dice que 64 bits pertenecen a la red!!
Por ejemplo, las siguiente son representaciones válidas de 20010DB80000CD3 (hexadecimal):

1. 2001:0DB8:0000:CD30:0000:0000:0000:0000/60
2. 2001:0DB8::CD30:0:0:0:0/60
3. 2001:0DB8:0:CD30::/60
4. 2001::1/80 =>Bits de Red 80, Bits de hosts 48. (80+48=128)
    a) Porción de Red : 2001:0:0:0:0
    b) Porción de host: 0:0:1
5. 2001::1/16=>Bits de Red 16, Bits de host 112 (16+112=128)
    a) Porción de Red: 2001
    b) Porción de Host:0:0:0:0:0:0:1

2.3.1. Identificador de interfaz

Son los 64bits más a la izquierda de una dirección de host.

- Se usa EUI-64 modificado.
- MAC de 48bits se le inserta FF:FE en el medio.
- Se invierte el bit Universal/Local (el séptimo bit más significativo).
- Las direcciones que comiencen con 000, no necesitan respetar el identificador de interfaz

2.3.2. Tipos de Direcciones en IPv6

En IPv6, existen tres tipos de Direcciones:

- Unidifusión (unicast): un identificador para una interfaz individual. Un paquete enviado a una dirección de este tipo se entrega a la interfaz identificada por esa dirección.
- Monodifusión (anycast): un identificador para un conjunto de interfaces (normalmente pertenecientes a diferentes nodos). Un paquete enviado a una dirección monodifusión se entrega a una de las interfaces identificadas por esa dirección (la más cercana, de acuerdo a la medida de distancia de los protocolos de encaminamiento). Se entrega a la interfaz más cercana o de menor “costo”.

- Multidifusión (multicast): un identificador para un conjunto de interfaces (normalmentepertenecientes a diferentes nodos). Un paquete enviado a una dirección multidifusión se entrega a todas las interfaces identificadas por esa dirección. Se entrega a todas las interfaces del identificador

  Observación: NO EXISTE BROADCAST

2.4. Direcciones Unicast

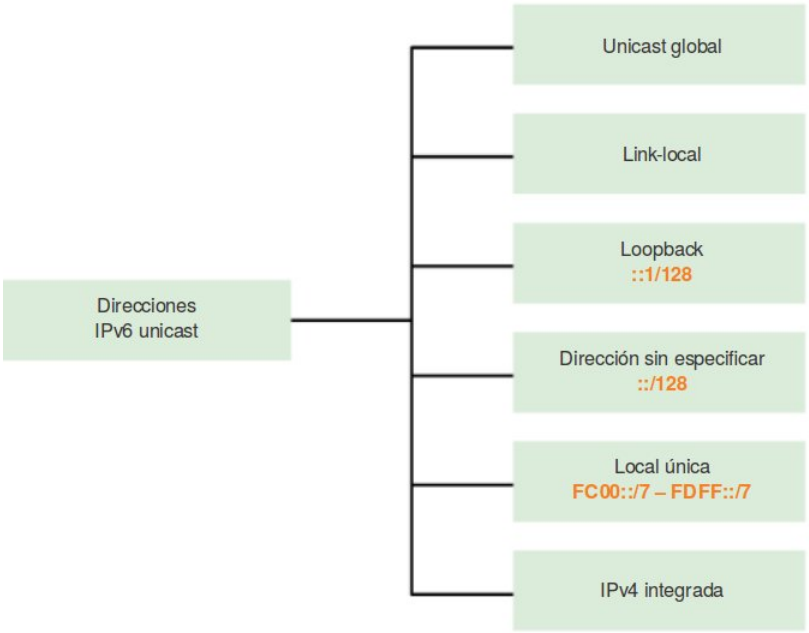


Figura 7: Tipos de Direcciones Unicast

2.4.1. Unicast Global:

Las direcciones unicast globales son similares a las direcciones IPv4 públicas. Estas son direcciones enrutables de Internet globalmente exclusivas. Las direcciones unicast globales pueden configurarse estáticamente o asignarse de forma dinámica. Existen algunas diferencias importantes con respecto a la forma en que un dispositivo recibe su dirección IPv6 dinámicamente en comparación con DHCP para IPv4. Estas direcciones son Unicas y Enrutables.

Rango 2000::/3 a 3FFF::/3 (el 4to bit puede ser 0 ó 1)

- 2000 = 0010 0000 0000 0000
- 3FFF = 0011 1111 1111 1111

Figura 8: Unicast Global

Ver que como sería la dirección IPv6 completa. Finalmente esta dirección se podría expresar de forma comprimida.

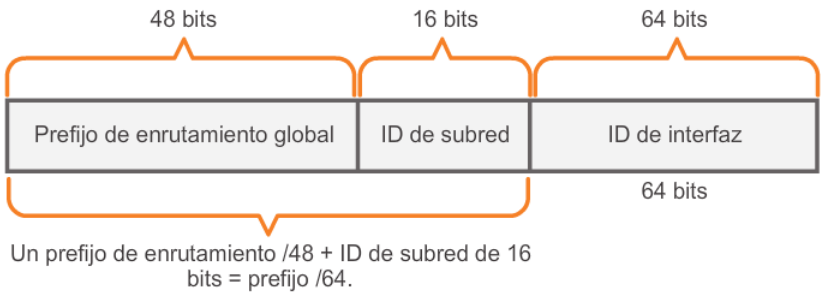


Figura 9: Unicast Global Completa

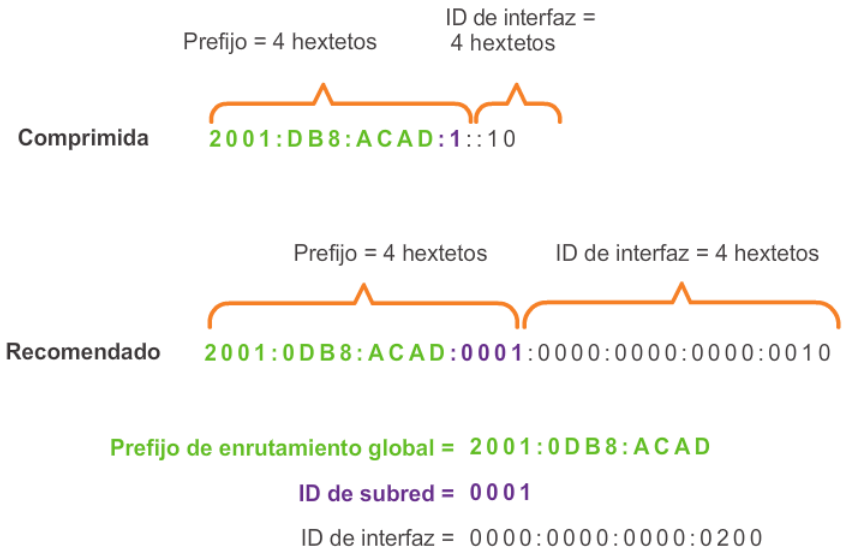


Figura 10: Unicast Gobal comprimidas

La IANA (http://www.iana.org/) dividió todo el rango de direcciones IPv6 en 8 partes. Para ello utilizó los 3 primeros bits, 2 elevado a la 3 da 8.

Por el momento usa 1/8 parte de las Direcciones totales con los tres primeros bits en 001.

=> como los tres primeros bits están en 001

=> 0010 0000 0000 0000 a 0011 1111 1111 1111=> 2000 a 3FFF

El cuarto bit puede ser 0 ó 1 de las direcciones IPv6 actuamente asignadas.

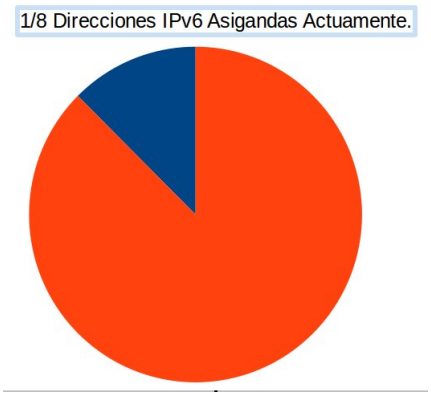


Figura 11: Direcciones Unicast Global en uso

Tarea para el Alumno.

Se pide al alumno calcular:¿Cuantas mas direcciones que IPv4 serían solo la 1/8 parte de IPv6?

El esquema de notación comprimida indicado en figura 2-10 suele conocerce como Regla 3-1-4 por que:

- 3 Segmentos de Red: 2001:0DB8:ACAD
- 1 Segmento de Subred: 0001
- 4 Segmentos de Host: 0000:0000:0000:0010

2.4.2. Link-local

Las direcciones link-local se utilizan para comunicarse con otros dispositivos en el mismo enlace local. Con IPv6, el término “enlace” hace referencia a una subred. Las direcciones link-local se limitan a un único enlace. Su exclusividad se debe confirmar solo para ese enlace, ya que no se pueden enrutar más allá del enlace. En otras palabras, *los routers no reenvían paquetes con una dirección de origen o de destino link-local*.

Las direcciones IPv6 link-local están en el rango de FE80::/10 (en binario 1111 1110 1000 0000) Si lo escribimos de una manera NO Comprimida sería:

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

```
/10 indica que los primeros 10 bits son 1111 1110 10 xx xxxx. El primer hexteto tiene
```

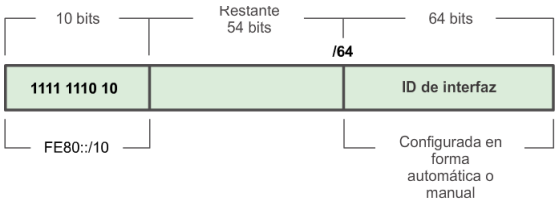


Figura 12: Dirección Link-local

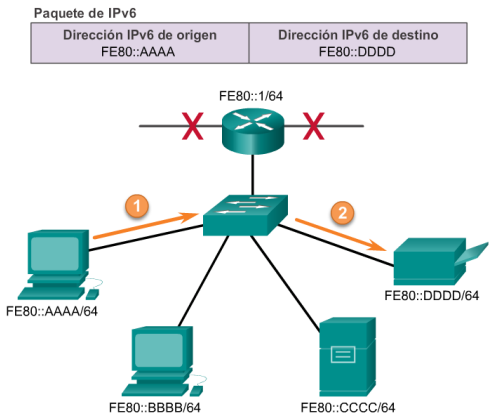


Figura 13: Dirección Link-local NO pasa Router

2.4.3. Loopback

Los hosts utilizan la dirección de loopback para enviarse paquetes a sí mismos, y esta dirección no se puede asignar a una interfaz física. Al igual que en el caso de una dirección IPv4 de loopback, se puede hacer ping a una dirección IPv6 de loopback para probar la configuración de TCP/IP en el host local. La dirección IPv6 de loopback está formada por todos ceros, excepto el último bit, representado en formato comprimido:

- ::1/128 con notación de prefijo.

- ::1 en el formato comprimido.
- 0000:0000:0000:0000:0000:0000:0000:0001 En formato no comprimido.

2.4.4. Dirección sin Especificar:

Una dirección sin especificar es una dirección compuesta solo por ceros representada como ::/128 o, simplemente, :: en formato comprimido. *No puede asignarse a una interfaz* y solo se utiliza como dirección de origen en un paquete IPv6. Las direcciones sin especificar se utilizan como direcciones de origen cuando el dispositivo aún *no tiene una dirección IPv6 permanente* o cuando el origen del paquete es irrelevante para el destino.

2.4.5. Local Única (ULA)

Son direcciones únicas en una red local o intranet, es decir que estas direcciones son el *parecido* al bloque de direcciones privadas en la versión cuatro del protocolo IP (IPv4) este tipo de direcciones estan sobre un bloque que las identifica el cual comienza por fc00::/7 este bloque es el que le da identidad a la dirección, estas direcciones se definen en la RFC 4193.

Las direcciones locales únicas se utilizan para el direccionamiento local dentro de un sitio o entre una cantidad limitada de sitios. *Estas direcciones puede ser enrutables pero no deben ser enrutables en la IPv6 global*. Las direcciones locales únicas están en el rango de FC00::/7 a FDFF::/7.

Con IPv4, las direcciones privadas se combinan con NAT/PAT para proporcionar una traducción de varios a uno de direcciones privadas a públicas. Esto se hace debido a la disponibilidad limitada de espacio de direcciones IPv4. Muchos sitios también utilizan la naturaleza privada de las direcciones definidas en RFC 1918 para ayudar a proteger u ocultar su red de posibles riesgos de seguridad. Sin embargo, este nunca fue el uso que se pretendió dar a estas tecnologías, y el IETF siempre recomendó que los sitios tomen las precauciones de seguridad adecuadas en el router con conexión a Internet.

Como IPv6 proporciona direccionamiento de sitio específico, no tiene por propósito ser utilizado para contribuir a ocultar dispositivos internos con IPv6 habilitado de Internet IPv6. El IETF recomienda que la limitación del acceso a los dispositivos se logre implementando medidas de seguridad adecuadas y recomendadas. Estas direcciones pueden ser enrutadas por los routers internos de una organización, pero cuando llegan al borde de la organización y, pasan a un router del ISP, éstas serán descartadas.

2.4.5.1. ¿Para qué sirven las direcciones ULA? Las direcciones ULA son útiles en el establecimiento de un esquema de direccionamiento propio que no dependa de los bloques asignados por algún ISP; como consecuencia, sólo los nodos de la organización pueden tener acceso los dispositivos internos de la red pero no a internet; para que un host que utilice una dirección ULA pueda acceder a Internet, debe utilizarse NAT en los dispositivos de borde. Siendo así, las direcciones ULA serían perfectas en aquellos equipos o dispositivos que requieren ser accedidos a través de la red local, pero no se espera que tengan visibilidad a nivel de Internet.

Entre los usos de este tipo de direcciones podemos nombrar:

- El direccionamiento para los clientes VPN
- Las redes de gestión fuera de banda
- Las redes de laboratorios
- Las redes de alta seguridad.

2.4.6. IPv4 Integrada.

Se utiliza para facilitar la transición de IPv4 a IPv6.

Observación: Direcciones IPv6 literales en rutas UNC (Uniform Naming Convention).

En sistemas operativos Microsoft Windows, las direcciones IPv4 son identificadores válidos en rutas UNC [2]

Para ubicar una carpeta compartida en la Red haciendo referencia a la dirección IPv4 del host sería:

- \\192.168.0.1\CarpetaCompartida\Recurso

Sin embargo, en IPv6 se usa los ":" como separador y *el carácter dos puntos es ilegal en una ruta UNC*. Por tanto, el uso de direcciones IPv6 es también ilegal en rutas UNC.

Por este motivo, Microsoft ha implementado un algoritmo de sustitución para representar direcciones IPv6 como nombres de dominio, que sí pueden usarse en rutas UNC.

Microsoft registró y reservó el dominio ipv6-literal.net en Internet.

Las direcciones IPv6 se transcriben como subdominio dentro de ese espacio de nombres, del siguiente modo:

- 2001:db8:85a3:8d3:1319:8a2e:370:7348

es traducido a:

- 2001-db8-85a3-8d3-1319-8a2e-370-7348.ipv6-literal.net

lo que daría lugar a una ruta UNC del tipo:

- \\2001-db8-85a3-8d3-1319-8a2e-370-7348.ipv6-literal.net\CarpetaCompartida\Recurso

Esta notación es resuelta automática por el software de Microsoft sin hacer peticiones a servidores DNS.

2.5. Direcciones Multicast

Las direcciones IPv6 multicast son similares a las direcciones IPv4 multicast. Recuerde que las direcciones multicast se utilizan para enviar un único paquete a uno o más destinos (grupo multicast). Las direcciones IPv6 multicast tienen el prefijo FF00::/8.

Nota: las direcciones multicast solo pueden ser direcciones de destino, no de origen.

Existen dos tipos de direcciones IPv6 multicast:

- Dirección multicast asignada
- Dirección multicast de nodo solicitado

2.5.1. Dirección multicast asignada

Las direcciones multicast asignadas son direcciones multicast reservadas para grupos predefinidos de dispositivos. Una dirección multicast asignada es una única dirección que se utiliza para llegar a un grupo de dispositivos que ejecutan un protocolo o servicio común. Las direcciones multicast asignadas se utilizan en contexto con protocolos específicos, como DHCPv6.

Dos grupos comunes de direcciones multicast IPv6 asignadas incluyen los siguientes:

Grupo multicast de todos los nodos FF02::1: grupo multicast al que se unen todos los dispositivos con IPv6 habilitado. Los paquetes que se envían a este grupo son recibidos y procesados por todas las interfaces IPv6 en el enlace o en la red. Esto tiene el mismo efecto que una dirección de broadcast en IPv4. En la ilustración, se muestra un ejemplo de comunicación mediante la dirección multicast de todos los nodos. Un router IPv6 envía mensajes de RA de protocolo de mensajes de control de Internet versión 6 (ICMPv6) al grupo multicast de todos los nodos. El mensaje de RA proporciona a todos los dispositivos en la red con IPv6 habilitado la información de direccionamiento, como el prefijo, la duración de prefijo y el gateway predeterminado.

Grupo multicast de todos los routers FF02::2: grupo multicast al que se unen todos los routers con IPv6 habilitado. Un router se convierte en un miembro de este grupo cuando se habilita como

[2] Uniform Naming Convention: Direcciones IPv6 literales en rutas UNC (Uniform Naming Convention)

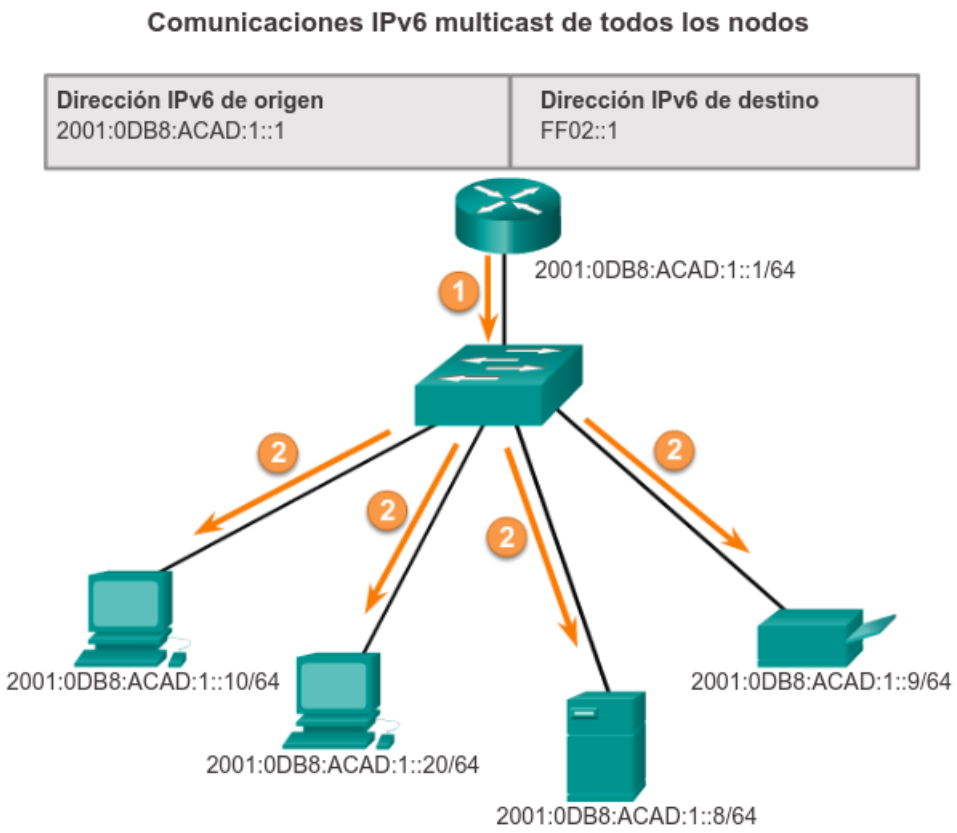


Figura 14: Multicast de Nodo Solicitado

router IPv6 mediante el comando de configuración global ipv6 unicast-routing. Los paquetes que se envían a este grupo son recibidos y procesados por todos los routers IPv6 en el enlace o en la red.

Los dispositivos con IPv6 habilitado envían mensajes de solicitud de router (RS) de ICMPv6 a la dirección multicast de todos los routers. El mensaje de RS solicita un mensaje de RA del router IPv6 para contribuir a la configuración de direcciones del dispositivo.

2.5.2. Multicast de Nodo Solicitado

Las direcciones multicast de nodo solicitado son similares a las direcciones multicast de todos los nodos. Recuerde que la dirección multicast de todos los nodos es esencialmente lo mismo que una dirección IPv4 de broadcast.

Todos los dispositivos en la red deben procesar el tráfico enviado a la dirección de todos los nodos. Para reducir el número de dispositivos que deben procesar tráfico, utilice una dirección *multicast de nodo solicitado*.

Una dirección multicast de nodo solicitado es una dirección que coincide solo con los últimos 24 bits de la dirección IPv6 unicast global de un dispositivo. Los únicos dispositivos que deben procesar estos paquetes son aquellos que tienen estos mismos 24 bits en la porción menos significativa que se encuentra más hacia la derecha de la ID de interfaz.

Una dirección IPv6 multicast de nodo solicitado se crea de forma automática cuando se asigna la dirección unicast global o la dirección unicast link-local. La dirección IPv6 multicast de nodo solicitado se crea combinando un prefijo especial FF02:0:0:0:0:1:FF00::/104 con los 24 bits de su dirección unicast que se encuentran en el extremo derecho.

La dirección multicast de nodo solicitado consta de *dos partes*:

- Prefijo multicast FF02:0:0:0:0:1:FF00::/104: los primeros 104 bits de la dirección multicast de todos los nodos solicitados.

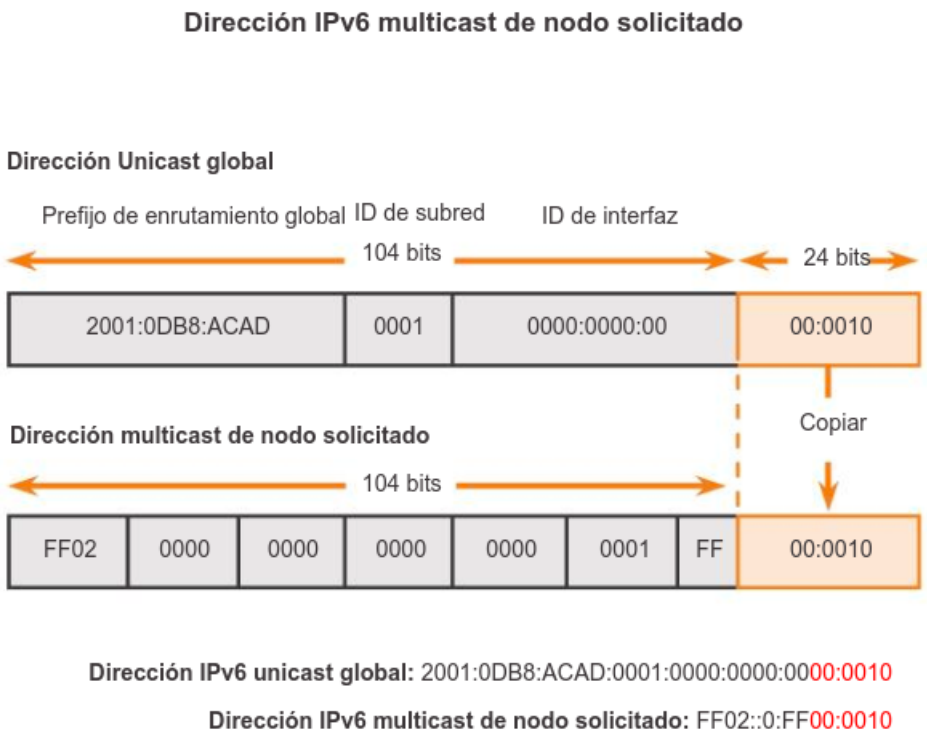


Figura 15: Multicast de Nodo Solicitado

- 24 bits menos significativos: los 24 bits finales o que se encuentran más hacia la derecha de la dirección multicast de nodo solicitado. Estos bits se copian de los 24 bits del extremo derecho de la dirección unicast global o unicast link-local del dispositivo.

Es posible que varios dispositivos tengan la misma dirección multicast de nodo solicitado. Si bien es poco común, esto puede suceder cuando los dispositivos tienen los mismos 24 bits que se encuentran más hacia la derecha en sus ID de interfaz. Esto no genera ningún problema, ya que el dispositivo aún procesa el mensaje encapsulado, el cual incluye la dirección IPv6 completa del dispositivo en cuestión.

2.6. Métodos para asignar las IPv6 Globales

Al igual que con IPv4, la configuración de direcciones estáticas en clientes no se extiende a entornos más grandes. Por este motivo, la mayoría de los administradores de red en una red IPv6 habilitan la asignación dinámica de direcciones IPv6.

Los dispositivos pueden obtener automáticamente una dirección IPv6 unicast global de dos maneras:

- Configuración automática de dirección sin estado (SLAAC)
- DHCPv6

Veamos cada uno de ellos.

2.6.1. Configuración automática de dirección sin estado (SLAAC)

La configuración automática de dirección sin estado (SLAAC) es un método que permite que un dispositivo obtenga su prefijo, duración de prefijo e información de la dirección de gateway predeterminado de un router IPv6 *sin utilizar un servidor de DHCPv6*. Mediante SLAAC, los dispositivos dependen de los mensajes de *anuncio de router (RA)* de ICMPv6 del router local para obtener la información necesaria.

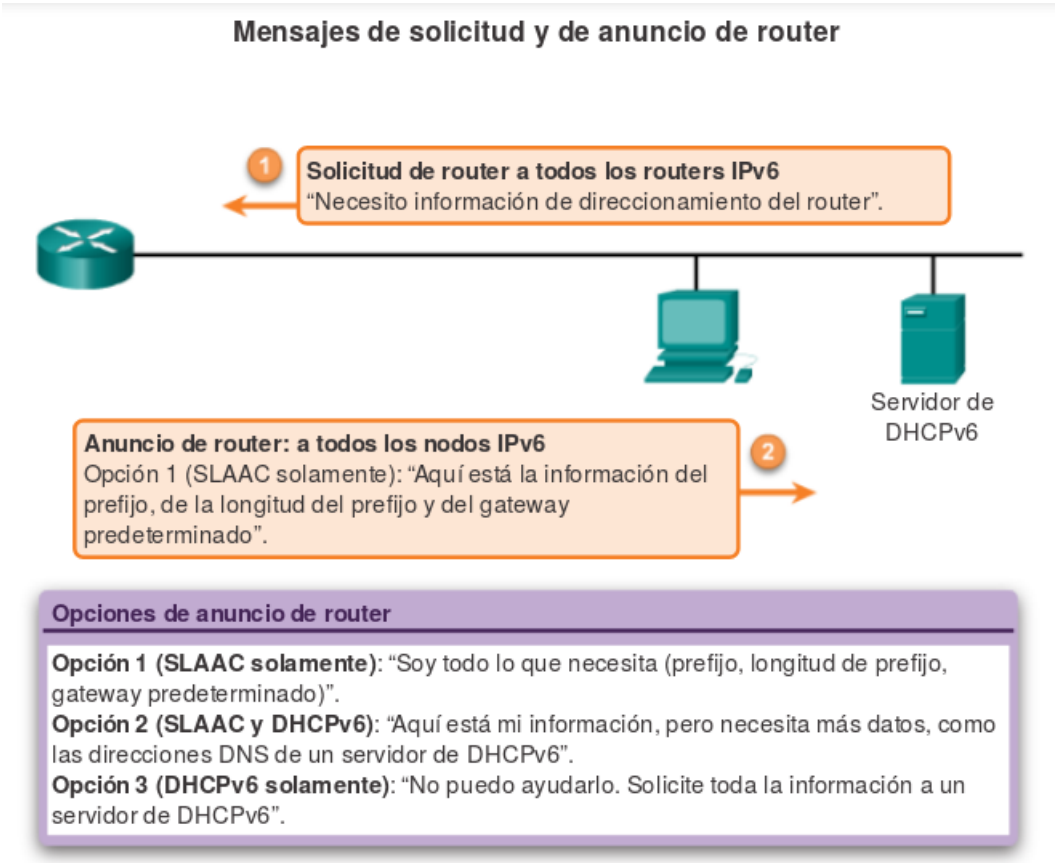


Figura 16: SLACC

Los routers IPv6 envían mensajes de *anuncio de router (RA)* de ICMPv6 a todos los dispositivos en la red con IPv6 habilitado de forma periódica. De manera predeterminada, los routers Cisco envían mensajes de RA cada 200 segundos a la *dirección IPv6 de grupo multicast* (ver que NO ES BROADCAST) de todos los nodos. Los dispositivos IPv6 en la red no tienen que esperar estos mensajes periódicos de RA. Un dispositivo puede enviar un mensaje de *solicitud de router (RS)* utilizando la dirección IPv6 de grupo multicast de todos los routers. Cuando un router IPv6 recibe un mensaje de RS, responde inmediatamente con un anuncio de router (RA).

Si bien es posible configurar una interfaz en un router con una dirección IPv6, esto no lo convierte en un "router IPv6". Un router IPv6 es un router que presenta las siguientes características:

- Reenvía paquetes IPv6 entre redes (=> está conectado a dos redes)
- Puede configurarse con rutas estáticas IPv6 o con un protocolo de enrutamiento dinámico IPv6.
- Envía mensajes RA ICMPv6.

El mensaje de RA de ICMPv6 contiene el prefijo, la duración de prefijo y otra información para el dispositivo IPv6.

El mensaje de RA también informa al dispositivo IPv6 cómo obtener la información de direccionamiento. El mensaje de RA puede contener una de las siguientes tres opciones, como se muestra en la ilustración: nsaje de RA puede contener una de las siguientes tres opciones, como se muestra en la ilustración:

2.6.1.1. • Opción 1, SLAAC solamente: El dispositivo debe utilizar :

- el prefijo
- la duración de prefijo

- la información de la dirección de gateway predeterminado incluida en el mensaje de RA.

No se encuentra disponible ninguna otra información de un servidor de DHCPv6, como podría ser el Servidor de DNS.

2.6.1.2. • Opción 2, SLAAC y DHCPv6 (sin estado): El dispositivo debe utilizar el prefijo, la duración de prefijo y la información de la dirección de gateway predeterminado incluida en el mensaje de RA.

Existe otra información disponible de un servidor de DHCPv6, como la dirección del servidor DNS. El dispositivo obtiene esta información adicional mediante el proceso normal de descubrimiento y consulta a un servidor de DHCPv6.

Esto se conoce como DHCPv6 sin estado, debido a que el servidor de DHCPv6 no necesita asignar ni realizar un seguimiento de ninguna asignación de direcciones IPv6, sino que solo proporciona información adicional, tal como la dirección del servidor DNS.

2.6.1.3. • Opción 3, DHCPv6 solamente: El dispositivo no debe utilizar la información incluida en el mensaje de RA para obtener la información de direccionamiento. En cambio, el dispositivo utiliza el proceso normal de descubrimiento y consulta a un servidor de DHCPv6 para obtener toda la información de direccionamiento, esto incluye

- una dirección IPv6 unicast global
- la duración de prefijo
- la dirección de gateway predeterminado
- las direcciones de los servidores DNS.

En este caso, el servidor de DHCPv6 actúa como un servidor de DHCP con estado, de manera similar a DHCP para IPv4. El servidor de DHCPv6 asigna direcciones IPv6 y realiza un seguimiento de ellas, a fin de no asignar la misma dirección IPv6 a varios dispositivos.

Los routers envían mensajes de RA de ICMPv6 utilizando la dirección link-local como la dirección IPv6 de origen. Los dispositivos que utilizan SLAAC usan la dirección link-local del router como su dirección de gateway predeterminado.

2.6.2. DHCPv6

El protocolo de configuración dinámica de host para IPv6 (DHCPv6) es similar a DHCP para IPv4. Los dispositivos pueden recibir de manera automática la información.

- una dirección IPv6 unicast global
- la duración de prefijo
- la dirección de gateway predeterminado
- las direcciones de los servidores DNS.

Los dispositivos pueden recibir la información de direccionamiento IPv6 en forma total o parcial de un servidor de DHCPv6 en función de si en el mensaje de RA de ICMPv6 se especificó la opción 2 (SLAAC y DHCPv6) o la opción 3 (DHCPv6 solamente). Además, el OS host puede optar por omitir el contenido del mensaje de RA del router y obtener su dirección IPv6 y otra información directamente de un servidor de DHCPv6.

Antes de implementar dispositivos IPv6 en una red, se recomienda primero verificar si el host observa las opciones dentro del mensaje ICMPv6 de RA del router.

Un dispositivo puede obtener la dirección IPv6 unicast global dinámicamente y también estar configurado con varias direcciones IPv6 estáticas en la misma interfaz. IPv6 permite que varias direcciones IPv6 (que pertenecen a la misma red IPv6) se configuren en la misma interfaz.

También se puede configurar un dispositivo con *más de una dirección IPv6 de gateway predeterminado*. Para obtener más información sobre cómo se toma la decisión respecto de cuál es la dirección que se usa como la dirección IPv6 de origen o cuál es la dirección de gateway predeterminado que se utiliza, consulte RFC 6724, Default Address Selection for IPv6 (Selección de direcciones predeterminada para IPv6).

2.6.2.1. Identificadores de interfaz de IPv6 Todas las direcciones que utilizan los prefijos comprendidos entre 001 y 111 deben utilizar también un identificador de interfaz de 64 bits que está derivado de la dirección EUI-64. La dirección EUI-64 de 64 bits fue definida por el Instituto de ingeniería eléctrica y electrónica (IEEE, Institute of Electrical and Electronic Engineers). Las direcciones EUI-64 se asignan a una tarjeta adaptadora de red o se derivan de direcciones IEEE 802.

En este documento se trata la derivación de los identificadores de interfaz de IPv6 según RFC 2373. Para tratar cuestiones relativas a la privacidad, se describe una derivación alternativa del identificador de interfaz de IPv6 que cambia con el tiempo en el borrador para Internet titulado "Privacy Extensions for Stateless Address Autoconfiguration in IPv6" (Extensiones de privacidad para la configuración automática de direcciones sin estado en IPv6).

Uno de los beneficios clave de IPv6 sobre IPv4 es su capacidad para abordar interfaz automática. Al implementar el formato de la IEEE de 64 bits extendido Identificador Único (EUI-64), un host puede asignar automáticamente sí mismo un identificador de interfaz IPv6 de 64 bits única sin necesidad de configuración manual o DHCP. Esto se logra en las interfaces Ethernet haciendo referencia a la dirección de 48 bits ya MAC única, y reformatear ese valor para que coincida con la especificación EUI-64.

RFC 2373 dicta el proceso de conversión, que se puede describir como que tiene dos pasos. El primer paso es convertir la dirección MAC de 48 bits a un valor de 64 bits. Para ello, partimos de la dirección MAC en sus dos mitades de 24 bits: el punto de vista organizativo Unique Identifier (OUI) y la parte específica del NIC. Luego se inserta el 0xFFFE valor hexadecimal de 16 bits entre estas dos mitades para formar una dirección de 64 bits.

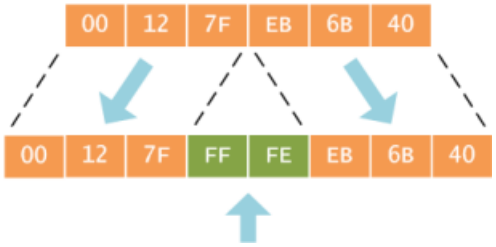


Figura 17: Proceso EUI-64

2.6.2.2. ¿Por 0xFFFE? Como se explica en las Directrices de la IEEE para EUI-64 autoridad de registro, este es un valor reservado que los fabricantes de equipos no pueden incluir en EUI-64 asignaciones de direcciones "reales". En otras palabras, cualquier dirección EUI-64 que tiene 0xFFFE inmediatamente después de su porción OUI puede ser reconocido por haber sido generado a partir de una dirección EUI-48 (o MAC).

El segundo paso es invertir la bandera universales / local (U/L) (bit 7) en la porción OUI de la dirección. Globalmente direcciones únicas asignadas por el IEEE tienen originalmente este bit puesto a cero, lo que indica la singularidad mundial. Del mismo modo, direcciones creadas a nivel local, tales como los utilizados para las interfaces virtuales o una dirección MAC configurada manualmente por un administrador, tendrán este bit puesto a uno. El bit U / L se invierte cuando se utiliza una dirección EUI-64 como una interfaz ID IPv6.

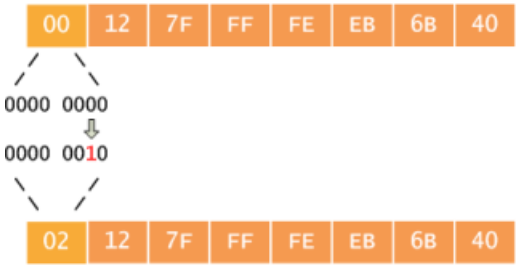


Figura 18: Cambio de bit

Con esto tenemos 64 bits que sumados a los 64 bits que corresponden a la parte de Red de IPV6 forman los 128 bits de Direccionamiento de IPV6.

Veamos en un solo dibujo como es el proceso completo.

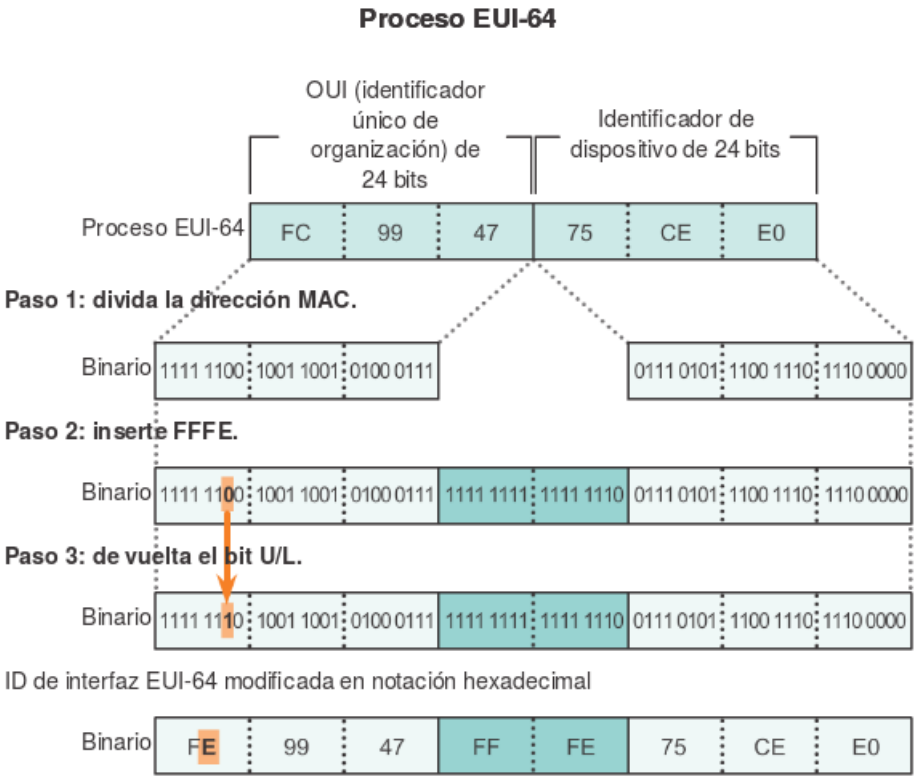


Figura 19: EUI-64

A modo de comentario, este procedimiento de asignación o creación de una dirección IEEE EUI-64, se usa en otros ambitos de manera similar.

Por ejemplo, en Sensores Inalámbricos de Area Personal con IPV6 de poca potencia, denominados 6LoWPAN, los primeros 24 bits de la dirección de capa de enlace lógico se forman de la manera mencionada algunos bits para casos especiales.

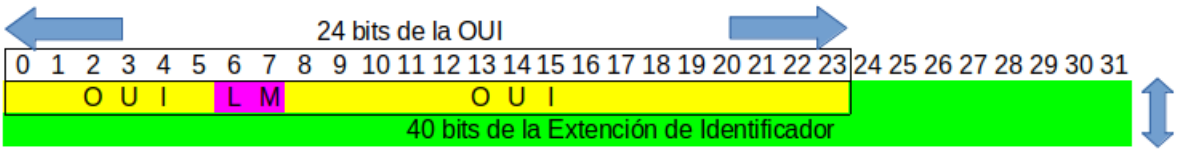


Figura 20: EUI-64 para 6LoWPAN

En el caso de 6LoWPAN, los bits L se usan para diferenciar de dirección Local o Universal al igual que lo visto para IPV6.. y el M para Multicast.

Para el caso de 6LoWPAN, los 40 bits que se agregan son establecidos por el fabricante para cada dispositivo como una especia de nro. de serie, en este caso a diferencia de la implementación para IPV6/Ethernet no se precisa incluir 0xFFFE.

A modo de referencia el precio de los 24 bit de OUI eran de 1650u$ en 2009.

2.6.3. ID de interfaz generadas aleatoriamente

Según el sistema operativo, un dispositivo puede utilizar una ID de interfaz generada aleatoriamente en lugar de utilizar la dirección MAC y el proceso EUI-64. Por ejemplo, comenzando con Windows Vista, Windows utiliza una ID de interfaz generada aleatoriamente en lugar de una ID de interfaz creada mediante EUI-64. Windows XP y sistemas operativos Windows anteriores utilizaban EUI-64.

Una manera sencilla de identificar que una dirección muy probablemente se creó mediante EUI-64 es el valor FFFE ubicado en medio de la ID de interfaz, como se muestra en la figura anterior.

Después de que se establece una ID de interfaz, ya sea mediante el proceso EUI-64 o mediante la generación aleatoria, se puede combinar con un prefijo IPv6 para crear una dirección unicast global o una dirección link-local.

- Dirección unicast global: al utilizar SLAAC, el dispositivo recibe su prefijo del mensaje de RA de ICMPv6 y lo combina con la ID de interfaz.
- Dirección link-local: los prefijos link-local comienzan con FE80::/10. Los dispositivos suelen utilizar FE80::/64 como prefijo o duración de prefijo, seguido de la ID de interfaz.

Al utilizar SLAAC (SLAAC solamente o SLAAC con DHCPV6), los dispositivos reciben el prefijo y la duración de prefijo del mensaje de RA de ICMPv6. Debido a que el mensaje de RA designa el prefijo de la dirección, el dispositivo debe proporcionar únicamente la porción de ID de interfaz de su dirección. Como se indicó anteriormente, la ID de interfaz se puede generar de forma automática mediante el proceso EUI-64, o, según el OS, se puede generar de forma aleatoria.

Con la información del mensaje de RA y la ID de interfaz, el dispositivo puede establecer su dirección unicast global.

Después de que se asigna una dirección unicast global a una interfaz, el dispositivo con IPv6 habilitado genera la dirección link-local automáticamente. Los dispositivos con IPv6 habilitado deben tener, como mínimo, la dirección link-local. Recuerde que una dirección IPv6 link-local permite que un dispositivo se comunique con otros dispositivos con IPv6 habilitado en la misma subred.

Las direcciones IPv6 link-local se utilizan para diversos fines, incluidos los siguientes:

- Los hosts utilizan la dirección link-local del router local para obtener la dirección IPv6 de gateway predeterminado.
- Los routers intercambian mensajes de protocolo de enrutamiento dinámico mediante direcciones link-local.
- Las tablas de enrutamiento de los routers utilizan la dirección link-local para identificar el router del siguiente salto al reenviar paquetes IPv6.

Las direcciones link-local se pueden establecer dinámicamente o se pueden configurar de forma manual como direcciones link-local estáticas.

- Dirección link-local asignada dinámicamente
- La dirección link-local se crea dinámicamente mediante el prefijo FE80::/10 y la ID de interfaz.

De manera predeterminada, los routers en los que se utiliza Cisco IOS utilizan EUI-64 para generar la ID de interfaz para todas las direcciones link-local en las interfaces IPv6. Para las interfaces seriales, el router utiliza la dirección MAC de una interfaz Ethernet. Recuerde que una dirección link-local debe ser única solo en ese enlace o red. Sin embargo, una desventaja de utilizar direcciones link-local asignadas dinámicamente es su longitud, que dificulta identificar y recordar las direcciones asignadas.

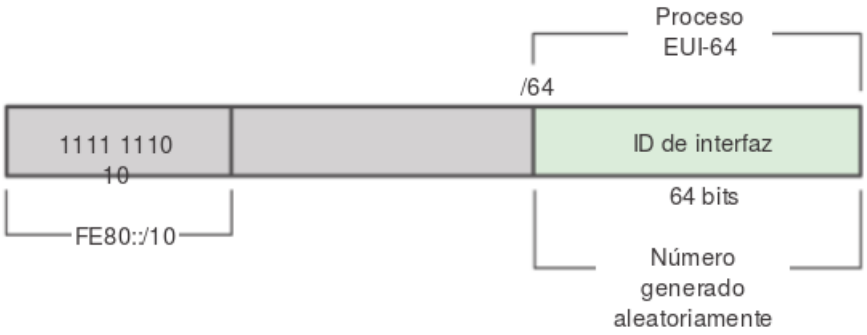


Figura 21: ID de Interfaz generada Aleatoriamente

3. Mecanismos de Transición

Dado que el protocolo predominante en la actualidad en Internet es IPv4, e Internet se ha convertido en algo vital, no es posible su sustitución, es decir, no es posible apagar la Red, ni siquiera por unos minutos y cambiar a IPv6.

Actualmente el protocolo IPv6 está soportado en la mayoría de los sistemas operativos modernos, en algunos casos como una opción de instalación. Linux, Solaris, Mac OS, OpenBSD, FreeBSD, Windows (2k, CE) y Symbian (dispositivos móviles) son sólo algunos de los sistemas operativos que pueden funcionar con IPv6, así que la parte que estaría faltando para la migración definitiva sería mas bien la parte de mayor jerarquía ISP para arriba.

No basta con actualizar unos pocos equipos, es una operación que tendría que involucrar a cualquier organización, sea empresa, administración pública o proveedor de acceso o contenidos de una forma sincronizada, lo cual es imposible.

Precisamente por ello, la organización encargada de la estandarización de los protocolos de Internet (IETF, Internet Engineering Task Force), diseñó junto con el propio IPv6, una serie de mecanismos que llamamos de transición y coexistencia.

Básicamente es importante entender lo que ello implica. No se trata de una migración como erróneamente se indica en muchas ocasiones, sino que ambos protocolos, IPv4 e IPv6, existirán durante algún tiempo, es decir se produce una coexistencia.

Podemos hacer una clasificación general entre los mecanismos de transición de acuerdo al tipo de técnica que se utiliza:

- Dual stack
- Túneles
- Traducción

Veamos un detalle de cada uno de ellos.

3.1. Dual Stack

Es el método propuesto originalmente para tener una transición suave hacia IPv6.

En este caso se necesita contar con suficiente cantidad de direcciones IPv4 para poder desplegar las dos versiones del protocolo en simultáneo en toda la red.

La pila dual o Dual Stack, hace referencia a una solución de nivel IP con pila dual, que implementa l*as pilas de ambos protocolos, IPv4 e IPv6*, en cada nodo de la red. Cada nodo de pila dual en la red tendrá dos direcciones de red, una IPv4 y otra IPv6.

Pros: Fácil de desplegar y extensamente soportado.

Contras: La topología de red requiere dos tablas de encaminamiento y dos procesos de encaminamiento. Cada nodo en la red necesita tener actualizadas las dos pilas.

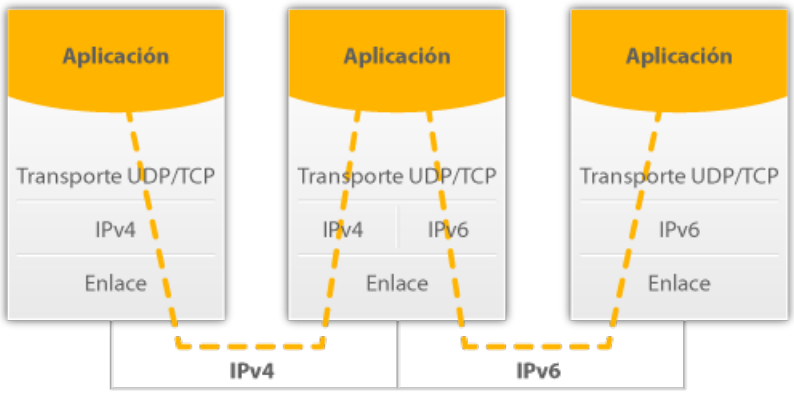


Figura 22: Dual Stack

Viéndolo de otra manera.

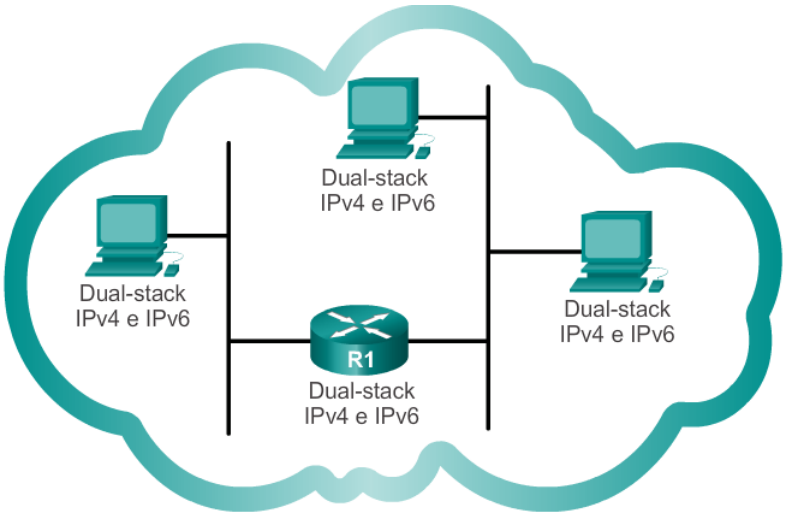


Figura 23: Dual Stack

De esta forma, cuando se establece una conexión hacia un destino sólo IPv4, se utilizará la conectividad IPv4 y si es hacia una dirección IPv6, se utilizará la red IPv6. En caso que el destino tenga ambos protocolos, normalmente se preferirá intentar conectar primero por IPv6 y en segunda instancia por IPv4 (si bien esto se ha ido modificando para solucionar problemas de timeouts, ver "happy eyeballs").

En los equipos se pueden observar esto en las pestañas de configuración de la Red. Veamos para Linux y Windows como se vería.

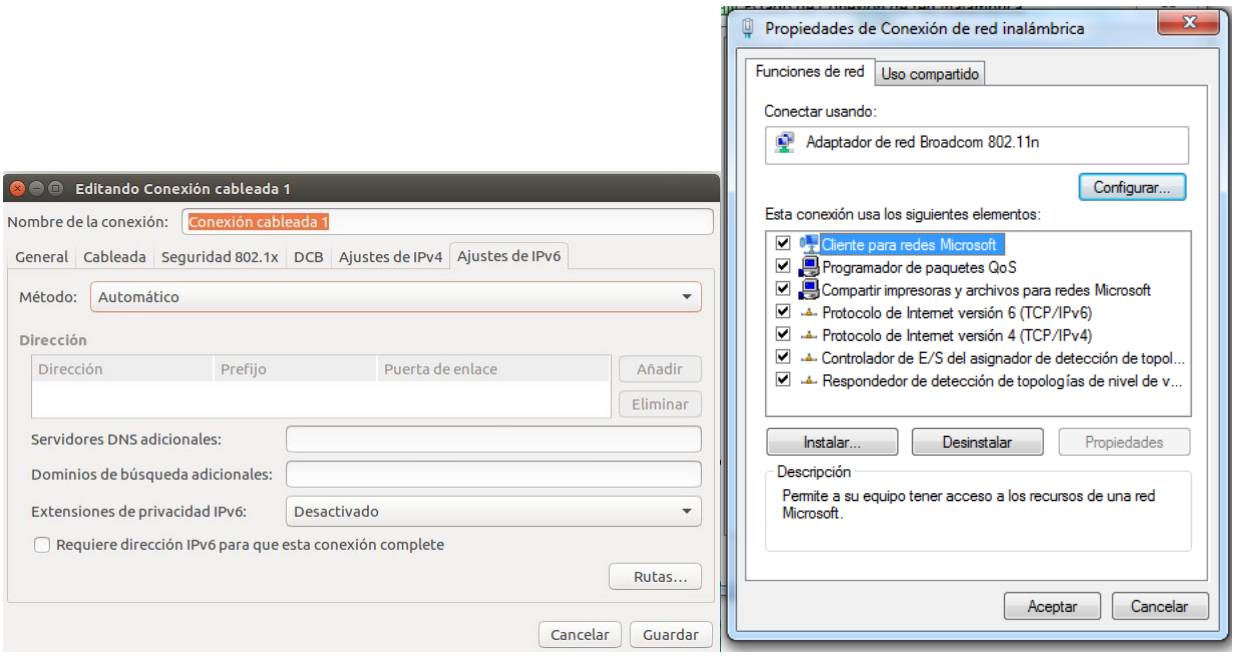


Figura 24: Dual-Stack

3.2. Túneles

Los túneles permiten conectarse a redes IPv6 "saltando" sobre redes IPv4.

Llamado 6in4 o protocolo-41 (es el identificador de protocolo que figura en el encabezado de IPv4) es un mecanismo de transición de protocolo ipv4 a ipv6 definido por el RFC 4213.

Estos túneles trabajan *encapsulando los paquetes IPv6 en paquetes IPv4* teniendo como siguiente capa IP el protocolo número 41. De esta manera, los paquetes IPv6 pueden ser enviados sobre una infraestructura IPv4. Hay muchas tecnologías de túneles disponibles. La principal diferencia está en el método que usan los nodos encapsuladores para determinar la dirección a la salida del túnel.

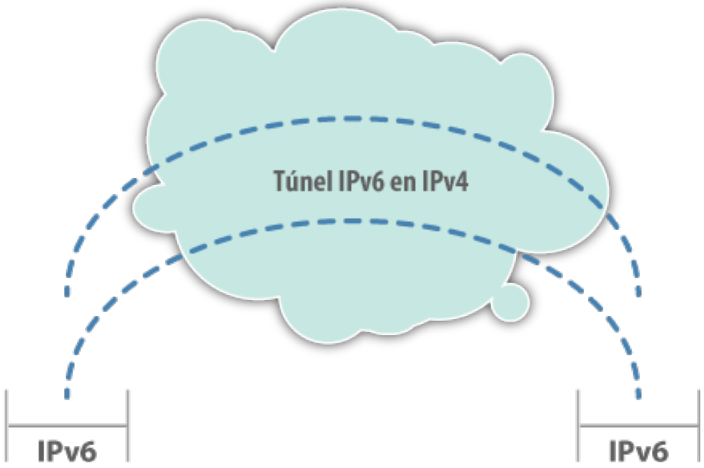


Figura 25: Túneles

Otra forma de verlo.

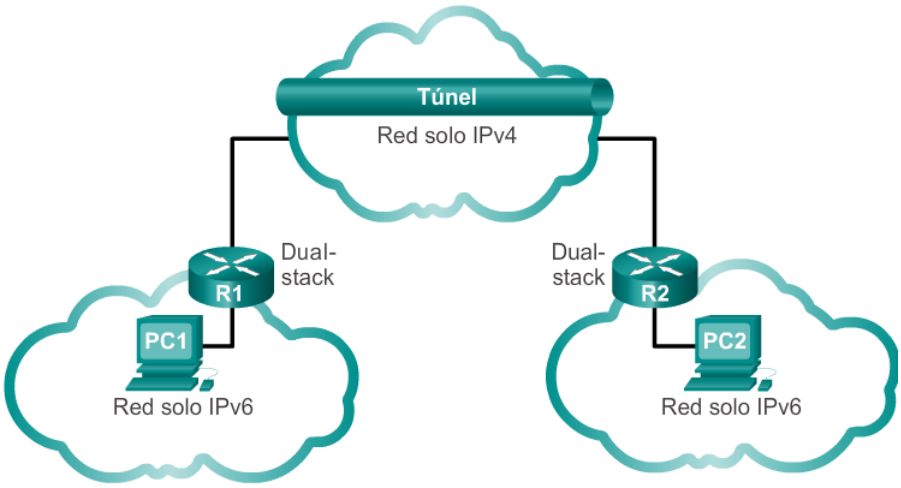


Figura 26: Túneles

3.3. Traducción o Transición IPV4 a IPV6

Les dejo un link a un Video de Lanic sobre el tema.

Esta técnica consiste en utilizar algún dispositivo en la red que convierta los paquetes de IPv4 a IPv6 y viceversa. Ese dispositivo tiene que ser capaz de realizar la *traducción en los dos sentidos* de forma de permitir la comunicación. Dentro de esta clasificación podemos mencionar NAT64/DNS64: la red es IPv6 nativa y para llegar a sitios que son sólo IPv4 se realiza una traducción al estilo NAT, mediante un mapeo entre los paquetes IPv6 e IPv4. Se utiliza un prefijo especial para mapear direcciones IPv4 a IPv6: 64:ff9b::/96. De esta forma, la complejidad de administración se simplifica al sólo tener que administrar una red IPv6-only. Las conexiones IPv6 son nativas, por lo que a medida que el despliegue de IPv6 crece en el mundo, el costo de esta solución no se incrementa.

Es necesario también utilizar una modificación al DNS, llamada DNS64, que permite generar un registro AAAA aún cuando el destino no tenga dirección IPv6 (es decir, el DNS responda sólo con registros de tipo A).

Registros DNS más comunes y a que servicios afectan:

- A record: contiene una dirección IPv4. Afecta al sitio web mostrado (para navegadores que prefieren IPv4).
- AAAA: contiene una dirección IPv6. Afecta al sitio web mostrado (para navegadores que prefieren IPv6).
- CNAME: contiene el nombre de dominio y es solamente para subdominios. Redirige el subdominio al dominio deseado.
- MX: contiene el nombre del servidor de e-mail (por ejemplo mx1.active24.com). Define donde se tienen que entregar los correos electrónicos.

Veamos como se vería gráficamente.

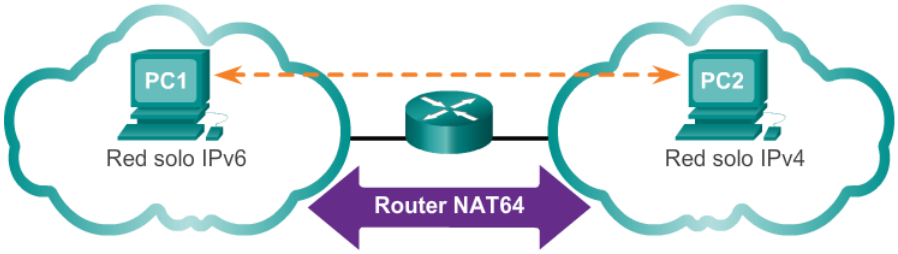


Figura 27: Traducción

3.3.1. 464XLAT

Se basa en la técnica anterior, pero introduce una doble traducción para los casos en que se necesite utilizar una aplicación que no soporta IPv6. Esto soluciona algunos problemas de NAT64 y es una técnica muy adecuada para redes de celulares (móviles) ya que los sistemas Android ya la incorporan. También para montar datacenters IPv6-only.

3.3.2. MAP-E y MAP-T

Son técnicas de transición similares a las anteriores pero que trabajan por compartición de puertos (A+P, ver RFC6346).

MAP-T usa traducción para transportar el tráfico IPv4

MAP-E utiliza encapsulado (túneles).

Índice