IPv6

MANUAL DE DIRECCIONAMIENTO

Por Javier Castillo

IP Services Manager

Índice

Introducción

Propósito de este documento

Las direcciones IPv4 se han agotado, y el 1 de Febrero de 2011, IANA asignó los dos últimos bloques de direccionamiento disponible a APNIC, el registro de internet de la región (RIR) Asia-Pacífico. Por tanto, empresas e instituciones ven ahora la necesidad de estar preparado para la migración IPv6. Las direcciones de IPv6 tienen una longitud de 128bits, es decir, permiten direccionar un espacio equivalente a 2^128, una barbaridad. Las organizaciones, típicamente tendrán asignados espacios de direcciones de 2^80. Por tanto, la escasez de direcciones no volverá a ser un problema, al menos esa es la idea. Lo que si será un problema será el organizar de forma lógica y eficiente, ese inmenso espacio de direcciones, de ahí la necesidad de elaborar un plan de direccionamiento IPv6.

En un plan de direccionamiento IPv6, los rangos de direcciones se agruparán de forma efectiva y lógica, ofreciendo las siguientes ventajas:

- Facilidad de implementación de políticas de seguridad: como las ACL o reglas de los firewalls.
- Trazabilidad de las direcciones: dentro de las propias direcciones, podremos descubrir información como la localización, tipo y/o uso.
- Escalabilidad: a medida que una organización crezca, el plan de direccionamiento permitirá ese crecimiento de forma lógica.
- Una gestión de la red más eficiente

Este manual propondrá cómo elaborar un plan de direccionamiento. En un plan de direccionamiento hay que tomar decisiones importantes, por lo tanto, habrá que pensar con detalle sobre las distintas opciones que se presentarán para asegurar que el plan construido, y que encaje perfectamente con las necesidades de su organización.

¿A quién está dirigido este documento?

Este manual está dirigido a todos los arquitectos de red, managers de red, ingenieros de red, etc., que ya tengan experiencia en el diseño, y gestión de redes IPv4, y que ahora se estén planteando la migración/implementación de IPv6 en su organización.

¿Dónde se puede encontrar más información sobre esquemas de direccionamiento IPv6?

Para la elaboración de este manual, se han seguido y consultados los disguientes documentos, cuya lectura puede ser interesante para aquellos que quieran investigar con más detalle formas de elaborar planes de direccionamiento IPv6 :

- « IP Version 6 Addressing Architecture » : http://tools.ietf.org/html/rfc4291
- « IPv6 Unicast Address Assigment Considerations » : http://tools.ietf.org/html/draft-ietf-v6ops-addcon-10
- « A Flexible Method for Managing the Assigment of Bits of an IPv6 Address Block » : http://tools.ietf.org/html/rfc3531
- « IPv6 Enterprise Network Renumbering Scenarios and Guidelines » : http://tools.ietf.org/html/draft-jiang-6renum-enterprise-01
- « Surfnet.nl : Preparing an IPv6 Addressing Plan » : http://www.surfnet.nl/Documents/handleiding_201012_IPv6_nummerplan_EN.pdf
- « CISCO : IPv6 Addressing White Paper » : http://www.cisco.com/web/strategy/docs/gov/IPv6_WP.pdf

Resumen básico IPv6

En este capítulo se hace un repaso general de distintos conceptos básicos de IPv6. Desde luego, no se pretende dar una repaso completo y detallado a toda la pila de protocolos IPv6, solo aquellos aspectos generales que se consideran importantes comprender, de cara al objetivo final, el poder diseñar un plan de direccionamiento IPv6.

Representación de las direcciones IPv6

Una dirección IPv6 consiste de 128 bits. Como una dirección de 128 unos y/o ceros es del todo ilegible, se ha diseñado un formato de representación, hexadecimal, que permite una visualización mucho más sencilla, y a la vez una relación con la representación binaria.

Cada dígito en el sistema hexadecimal equivale a 4 bits, por tanto, una dirección de 128 bits, se representa como una dirección de 32 dígitos hexadecimales. Por ejemplo:

2a01:7d00:0000:0000:0000:0000:0000:0000

Y como esta representación sigue sin ser especialmente sencilla, los ceros a la izquierda se pueden obviar, obteniendo:

2a01:7d00:0:0:0:0:0:0

Que ya es bastante más legible. El golpe de efecto final se obtiene agrupando la serie de "0:0:0.." con el símbolo "::". De esta forma, la dirección final quedaría como:

2a01:7d00::

Las reglas exactas de representación de las direcciones IPv6 se pueden consultar en el RFC5952.

Agrupamiento de direcciones

Las direcciones IPv6 se agrupan mediante el valor binario de la dirección. Este agrupamiento se lleva a cabo con los prefijos. Los prefijos representan a todas aquellas direcciones que empiezan con la misma serie de bits, y hasta determinada longitud representada por un "/NN". Por ejemplo, el prefijo:

2a01:7d00::/32

contiene todas las direcciones que comienzan en

2a01:7d00:0:0:0:0:0:0

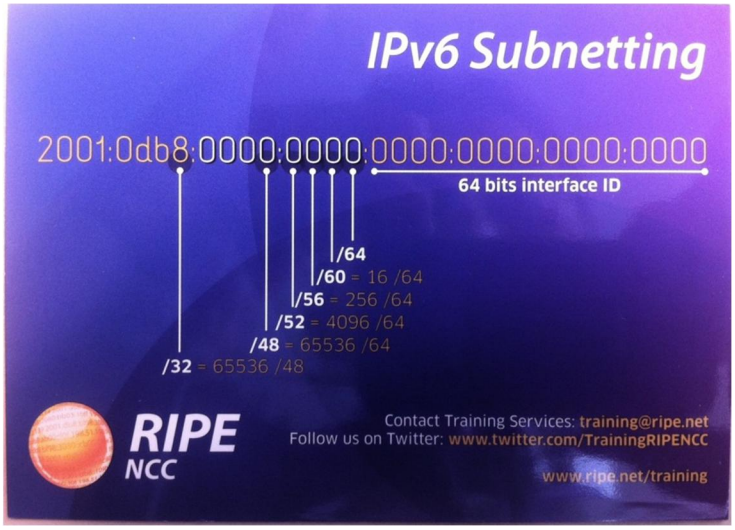
Y terminan en

2a01:7d00:ffff:ffff:ffff:ffff:ffff:ffff

Es decir, los 32 primeros bits son idénticos (representado hexadecimalmente como “2a01:7d00”), y el resto varía.

Puesto que cada dígito hexadecimal agrupa 4 bits, es muy recomendable el usar prefijos cuya longitud sea múltiplo de 4, como por ejemplo /48->/52->/56->/60->64.

Como se puede ver en la siguiente calculadora de RIPE NCC, los prefijos con longitud múltiplo de 4 permiten localizar fácilmente su último dígito hexadecimal dentro de la dirección IPv6:



Dicho esto, nada impide que se usen prefijos con longitudes que no sean múltiplo de 4, lo que hay que tener en cuenta en ese caso, es que la finalización del prefijo estará dentro de un dígito hexadecimal (recordemos que 1 dígito hexadecimal realmente es una serie de 4 bits). Por ejemplo, el prefijo:

2001:0db8::/61

contiene las direcciones que comienzan en:

2001:0db8:0:0:0:0:0:0

y terminan en:

2001:0db8:0:7:ffff:ffff:ffff:ffff

Otro ejemplo, el prefijo:

2001:0db8:0:8::/61

comenzaría en:

2001:0db8:0:8:0:0:0:0

y terminaría en:

2001:0db8:0:f:ffff:ffff:ffff:ffff

Asignación de bloques de direccionamiento

Los bloques de direcciones IPv6, se asignan conforme estás reglas definidas por IANA y los RIR:

/32 -> Estos prefijos, de 2^96 direcciones, son asignados a los *Local Internet Registries* (LIR), para que se repartan entre sus clientes. Los LIR típicamente son los ISP/Carriers.

/48 -> Este prefijo, de 2^80 direcciones, se recomienda que sea el prefijo por defecto para cualquier organización.

/64 -> Este prefijo, de 2^64 direcciones, es el mínimo que se asignará a una subred.

/127 -> Enlaces punto a punto. Aprobado en Febrero de 2012 RFC6547: http://tools.ietf.org/html/rfc6547

/128 -> este prefijo, de una única dirección, se usará para los interfaces *loopback* de routers, servidores, etc.

Se puede consultar con más detalle las recomendaciones que ofrece el rfc RFC6177 (IPv6 Address Assignment to End Sites)

Configuración de Equipos

Aunque no es estrictamente necesario saber cómo configurar IPv6 en los equipos de la red, si es conveniente que se tenga una idea aproximada de cómo se hará, de forma que cuando se vaya a elaborar el plan de direccionamiento, se disponga de un background técnico mayor.

Configuración IPv4

En el mundo IPv4, hay dos formas de configurar un equipo de red y asignarle una IP:

- Configuración estática
- Configuración DHCP

Análogamente, la configuración DNS de los equipos, se puede hacer mediante:

- Configuración estática
- Configuración DHCP

La primera opción suele aplicarse en equipos cuya configuración será fija, como servidores o routers. La segunda opción, es la que se suele aplicar a los usuarios y sus equipos.

Configuración IPv6

En el mundo IPv6, existe una tercera opción disponible para asignar la IP a su interfaz:

- Configuración estática
- Configuración con DHCPv6 (un DHCP adaptado a IPv6)
- Configuración automática, *stateless address auto configuration (SLAAC)*

Para la configuración DNS, igualmente existen tres opciones:

- Configuración estática
- Configuración con DHCPv6
- Configuración dinámica con *RDNSS (Recursive DNS Server)*

Estos tres métodos son combinables entre ellos. Por ejemplo, un equipo puede configurar su interfaz de red mediante *SLAAC* y mediante DHCPv6 configurar su información DNS. A continuación se detallan más estas opciones.

Configuración en IPv6

Configuración estática

La configuración estática se usa típicamente en routers y servidores, de forma similar a como se ha hecho con IPv4. Eso si, es una subred IPv6 el prefijo menor a de tener una máscara /64 como se ha visto anteriormente. Si se usan máscaras inferiores, determinados protocolos IPv6, como podría ser el SLAAC, no funcionarían.

Configuración dinámica "*stateless SLAAC*"

En este método de auto configuración, el papel fundamental lo juega el router de la red. El router anunciará a la red el prefijo a usar, mediante "*router advertisements (RA)"*. El equipo final, cuando *escuche* este RA con el prefijo a usar, configurará su interfaz de red.

En las redes Ethernet, que son el 99% de las redes hoy en día, los equipos tienen interfaces de red con direcciones físicas llamadas *MAC*. En IPv6, el SLAAC, hace uso de esta información para construir la dirección IPv6 de un interfaz de red.

Por tanto, SLAAC permite a un equipo construir su dirección IPv6 en base al prefijo anunciado en la red por el router de la misma, y la dirección MAC de su propio interfaz de red.

El RFC4862 detalla el protocolo SLAAC, y el RFC 4941 define opciones de privacidad adicionales, para que no haya una fácil correlación entre la MAC del equipo, y la parte de host de la dirección IPv6 final.

Configuración dinámica con DHCPv6

El protocolo DHCPv6 está definido en el RFC3315. La idea tras DHCPv6 es la misma que la del DHCPv4: un servidor asigna una dirección IPv6 a un equipo. Sin embargo, el router por defecto de la red, que en DHCPv4 se incluía, en DHCPv6 no se incluye. El router por defecto de la red se anunciará por mensajes RA originados por el propio router. Esta es una diferencia importante entre DHCPv6 y DHCPv4.

Configuración DNS IPv6

Configuración estática

De nuevo, como en el anterior caso de configuración estática de direcciones IP, la configuración estática DNS se suele implementar en routers y servidores. No hay diferencia en cómo se hace en IPv4.

Configuración dinámica con RDNSS

Recursive DNS Server está definido en el RFC6106 como un método para anunciar las direcciones de los servidores DNS (*resolvers*). Las direcciones de estos servidores, se añaden dentro de los mensajes del router (*RA*).

Configuración dinámica con DHCPv6

En DHCPv6, como DHCPv4, la información relativa a las direcciones IP de los servidores DNS, se pasa dentro de los datos del servidor DHCP. En el caso de usar DHCPv6, el mensaje del router (*RA*) tiene que llevar el *flag* de "*Other stateful configuration*" activo, para que los hosts sepan que deben usar DHCPv6 para conseguir la información relativa a los servidores DNS.

Comparativa RA, RDNSS, DHCPv6

La siguiente tabla, muestra un resumen de los SSOO que soportan las distintas opciones:

SSOO	Version	SLAAC	RDNSS	DHCPv6	Privary Extension	Manual	Doble Pila
MS Windows	7	Si	No	Si	Si	Si	Si
Apple Mac OS X	10.7	Si	Si	No	Si	Si	No
Apple iOS	4.2.1	Si	No	Si	No	No	Si
Google Android	2.2	Si	No	No	No	No	No
Linux	>=2.6.35	Si	Si	Si	Si	Si	Si
Cisco IOS	15.x	Si	No	Si	No	Si	Si

Seguridad de redes IPv6

Igual que en IPv4, las redes IPv6 son susceptibles de ataques. Los problemas de seguridad, desde un punto de vista del origen, pueden ser externos (venir desde Internet) o internos (originados en la propia LAN).

A continuación se ven algunos aspectos relacionados con la seguridad en entornos LAN

Descubrimiento de vecinos

En IPv6, el protocolo de *Neighbor Discovery* (ND) es el equivalente al ARP de IPv4. Hay varios tipos de paquetes ND, como por ejemplo: *Router Advertisements* (RA), *Duplicate Address Detection* (DAD), etc. Cuando IPv6 se diseñó, los potenciales problemas de seguridad en el entorno (teóricamente) seguro como el entorno LAN, no se consideraron. Posteriormente, los RFC 4861 y 3756 fueron liberados para enfocar este problema.

De entre todos los ataques en este entorno, destaca el conocido como “Hombre en el Medio” o en inglés *Man in the Middle* (MITM), para interceptar el tráfico. En IPv6, mensajes RA “no autorizados” podrían fácilmente ser el medio elegido por un hacker para realizar este ataque.

Para mitigar este potencial problema de seguridad se han propuesto varias alternativas, entre las que destacan:

- El uso de switches L2 capaces de identificar y controlar, mediante el uso de ACL, qué dispositivos de la red pueden enviar mensajes RA al resto de la red. Cisco tiene equipamiento capaz de implementar esto, véase "Cisco IPv6 First Hop Security": http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/whitepaper_c11-602135.html
- *SeND* (Secure ND) emplea el uso de certificados digitales para firmar los mensajes. Este protocolo está definido en el RFC3971 y RFC 3972. Actualmente, solo Cisco tiene implementada una primera solución conforme a este protocolo.

DHCPv6

Igual que en DHCPv4, en IPv6 un atacante pueden conectar a una red su propio servidor DHCPv6 para realizar un ataque *Man in the Middle.*

Actualmente, la mejor solución aportada hasta el momento consiste en apoyarse en la inteligencia del switch L2, como en "Cisco IPv6 First Hop Security".

En las redes Wifi, la comunicación directa entre el servidor DHCP y los clientes, hay que bloquearla y hacer que el AP aísle la red.

Servidores y equipos

A nivel de PC's y servidores, en IPv6 se recomienda el uso de *Firewalls* locales. En Linux, el uso de las "*ip6tablesk"* y en Windows el firewall que viene por defecto instalado en Windows7/2008.

Preparación de un plan de direccionamiento

Introducción

Cuando se prepara una plan de direccionamiento, lo primero en lo que hay que pensar es en el método o sistema que se usará para asignar el direccionamiento a las redes de las organización. A continuación se verán varios métodos, todos ellos válidos, que se pueden ajustar mejor o peor a su organización, dependiendo de las singularidades de la misma.

Estructura básica

Como se ha visto, el espacio de direcciones IPv6 es tan grande, que se pueden crear todas las subredes que se necesiten. Y las subredes, se pueden asignar en función de distintos criterios, como por ejemplo: localización, tipo de uso, o una combinación de ambos.

Por ejemplo, si una organización recibe un prefijo 2001:db8:1233::/48 (lo recomendado), para la dirección:

2001:db8:1234:LLLLGGGGBBBBBBBB::/64

vemos que desde el bit 49 hasta el bit 64 (16 bits) hay:

- 4 bits para definir localizaciones (L) (Madrid, Barcelona, sedeA, sedeB, etc.)
- 4 bits para definir el tipo de uso (G) (backbone, servidores, redes invitados, etc)
- 8 bits para uso alternativo (B).

Con este sencillo esquema, se puede direccionar de forma sencilla una organización 16 emplazamientos distintos, cada una con 16 tipos de usos, y 256 subredes por tipo de uso.

Definición de la subred principal

Lo primero de todo, es elegir el direccionamiento de las subredes principales, y elegir la localización o el tipo de uso, como discriminador de dichas subredes.

Localización

Cuando la localización se elige como discriminador, el objetivo es que todas las subredes de una misma localización puedan ser agregadas de forma que la tabla de rutas se mantenga compacta y reducida.

Tipo de uso

Si el discriminador elegido es el tipo de uso, en este caso la optimización de la tabla de rutas no podrá ser conseguida como en el caso anterior. Sin embargo, esta opción permitirá una implementación de una política de seguridad mucho más sencilla, y alineada con las configuraciones de los firewalls, que suelen implementar reglas por cada tipo de uso.

Además, el problema del tamaño de la tabla de rutas, a no ser que estemos ante una organización muy extensa, no debiera ser un problema para la mayoría de los routers modernos.

Recomendación

En general, la recomendación es intentar usar el tipo de uso como discriminador de las subredes principales, porque es la mejor forma de integrar el direccionamiento con los procedimientos y políticas de seguridad que tiene una organización.

El uso de la localización como discriminador estaría justificado en casos como:

- Cada localización quiere tener su propio plan de direccionamiento
- Los routers que hay no pueden procesar una gran tabla de rutas, por lo que hay que optimizar el tamaño de esta.

Calcular el espacio de direcciones necesario

Como se ha visto en el ejemplo anterior, normalmente una organización tiene 16bits para jugar con el plan de direccionamiento, y definir localizaciones y tipos de uso, y agruparlas en grupos. Se pueden definir los grupos de la siguiente forma:

- Primero determinar localizaciones o tipos de uso en la organización. Cada localización, o cada tipo de uso, cuenta como un grupo.
- Añada un grupo adicional para su backbone o infraestructura propia.
- Si se elige usar la localización como discriminador de las subredes principales, hay que añadir otro grupo adicional para reflejar las redes que no tengan una localización fija (VPNs por ejemplo)
- Para futuro crecimiento, añada uno o dos grupos más.
- Redondee el número de grupos a un número que sea potencia de 2 para que sea fácilmente representable por la notación binaria (1 bit = 2 grupos)

Con estas consideraciones, se pueden calcular fácilmente el número de bits necesarios para cubrir todos los grupos calculados, tanto si su plan de direccionamiento se basa en la localización, o en el tipo de uso. Más adelante, se ven unos ejemplos.

Uso opcional de direccionamiento secundario

Como se ha visto en el punto anterior de estructura básica, la dirección

2001:db8:1234:LLLLGGGGBBBBBBBB::/64

ofrece 16 bits con los que jugar. Los bits B permiten definir las subredes secundarias. Si el discriminador de subredes principales es la localización, en cada localización se tendrán X subredes secundarias. Si el discriminador de la red principal es el tipo de uso, se tendrán entonces X subredes secundarias para cada tipo de uso.

Por ejemplo:

2001:db8:1234:GGGGLLLBBBBBBBB::/64

define un esquema de subredes principales basadas en el tipo de uso. Cada tipo de uso, tiene varias localizaciones(L), y estas a su vez, varias subredes(B). Este esquema, como se ha comentado anteriormente, suele ser el esquema que mejor se adapta a las políticas de seguridad existentes en una organización.

Control y flexibilidad

Una vez definido el esquema de direccionamiento, se puede comprobar fácilmente si el número de bits disponibles para las redes secundarias (B) es suficiente para las necesidades de la organización. En el ejemplo del punto anterior, hay 9 bits B, es decir 2^9 = 512 subredes secundarias.

Si el número de bits disponibles no fuera suficiente, se podría hacer un uso más flexible de los bits de localización y tipo de uso. Por ejemplo, en el esquema:

2001:db8:1234:GGGGLLLBBBBBBBB::/64

Se tienen 4 bits (G) para definir primero el tipo de uso, y luego 3 bits (L) para la localización. Supóngase que cada localización, necesita 2048 subredes (por ejemplo, porque hay muchas VPN). En ese caso, las 512 subredes que permiten los 9 bits B no son suficientes. En este caso, lo que se puede hacer es jugar de la siguiente forma con los bits de tipo de uso:

Tipo de Uso (agrupados los 4 bits G en un dígito hex)	Descripción
0	Backbone
1	Servidores
2	Uso futuro
3	Uso futuro
4	Personal
5	Estudiantes
6	Invitados
7	Uso futuro
8	VPNs
9	VPNs
A	VPNs
B	VPNs
C	Uso futuro
D	Uso futuro
E	Uso futuro
F	Uso futuro

Como se ve en la tabla, se definen 4 tipos de uso iguales (VPNs), de forma que en realidad, para VPNs se tienen 4x512 subredes secundarias, y así se cumple con el requisito expuesto en el ejemplo.

En el caso contrario de que los bits disponibles para definir las redes secundarias sean más que suficiente, entonces conviene primar la legibilidad de la dirección, de forma que con un vistazo rápido sobre la misma se obtenga toda la dirección de forma sencilla.

Por ejemplo, el esquema de direccionamiento:

2001:db8:1234:GGGGLLLLBBBBBBB::/64

Tiene 4 bits para el tipo de uso (G), 4 bits para la localización (L), y 8 bits para las subredes secundarias. Como en la direcciones IPv6 los bits se agrupan de cuatro en cuatro para su representación, se podría tener que el esquema en realidad queda como:

2001:db8:1234:GLBB::/64

lo cual hace que su comprensión visual sea muy sencilla.

Uso del VLAN-ID en el direccionamiento

Algunas organización, ya implementan dentro del VLAN-ID un esquema basado en Localización/Tipo de Uso (aunque menos flexible que el IPv6, porque el VLAN-ID son solo 12 bits vs los 16 bits que se tienen disponibles en los ejemplos anteriores). En ese caso, se puede hacer una translación directa de ese esquema al nuevo de IPv6.

En caso de que una organización no implemente ningún esquema, y por tanto, el número de VLAN-ID no tenga un significado especial, también se puede transferir dicho número al esquema de direccionamiento IPv6. Así se podría hacer una relación rápida entre el número de VLAN y la dirección IPv6. Sin embargo, no permitiría hacer un uso óptimo que permitiera una alineación con políticas de seguridad y/o optimizara las tablas de rutas.

La translación del VLAN-ID a la dirección IPv6, se puede hacer de dos formas, como se ve en esta tabla:

VLAN-ID	IPv6 DECIMAL	IPv6 HEX
1	2001:db8:1234:0001::/64	2001:db8:1234:0001::/64
12	2001:db8:1234:0012::/64	2001:db8:1234:000c::/64
4094	2001:db8:1234:4094::/64	2001:db8:1234:0ffe::/64

Como se puede ver, la representación decimal permite que la dirección IPv6 sea muy legible. Sin embargo, supone un desperdicio de direcciones IPv6 muy grande. En organizaciones pequeñas, esta puede ser una opción muy recomendable.

La translación hexadecimal, tiene un grado de legibilidad claramente menor, pero sin embargo, el aprovechamiento que permite de la dirección IPv6 es mayor. Por ejemplo, se podrían tener 15 localizaciones distintas, y en cada localización las VLANs representadas. Para muchas organizaciones de tamaño pequeño-mediano, esta podría ser un esquema de direccionamiento perfectamente válido.

Direccionamiento de enlaces punto a punto

Hasta Febrero de 2012, la recomendación era asignar un prefijo con longitud /64 a los enlaces punto a punto. Sin embargo, desde Febrero de 2012, IETF permite el uso de prefijos /127 en enlaces punto a punto, puede consultarse el RFC6547 en el link http://tools.ietf.org/html/rfc6547

Ejemplos básicos de esquemas de direccionamiento IPv6

Asignación de la red principal basada solo en el Tipo de Uso

Supóngase que universidad ha adoptado un esquema de direccionamiento basado el tipo de uso, de forma que define los siguientes grupos y su número:

Estudiantes /Personal de universidades/Invitados/Servidores -> 4 grupos

Backbone -> 1 grupo

Es decir, en total identifica 5 grupos. Redondeando al número potencia de 2 más próximo (8), se tiene que son necesarios 3 bits (2^3 = 8). Los grupos que sobren, quedan reservados para usos futuros. Por tanto, de los 16 bits disponibles en el plan de direccionamiento, se tienen 3 ya definidos para los tipos de uso, y 13 disponibles (2^13 = 8192!). Puesto que sobran tantos, se intenta mejorar la legibilidad de la siguiente manera: se usarán 4 bits, y no 3, para el tipo de uso, de forma que se permitan agrupar esos 4 bits en un dígito hexadecimal, y ser más legible la dirección. El formato quedará así:

2001:db8:1234:GGGGBBBBBBBBBB::/64

Y ejemplos de direcciones finales quedarían así:

Tipo de Uso(G)	Subred Secundaria(B)	Dirección
Infraestructura(0)	1	2001:db8:1234:0001::/64
Estudiantes(1)	213	2001:db8:1234:10d5::/64
Backbone(5)	12	2001:db8:1234:500c::/64

Asignación de la red principal basada en el Tipo de Uso y Localización

Supóngase que una universidad elige un esquema de direccionamiento basado en el tipo de uso para discriminar la red principal, y la localización como discriminador secundario.

Esta universidad, distingue como en el ejemplo anterior, 5 grupos de usuarios/usos distintos, que redondea a 8, usando 3 bits para representar el tipo de uso.

Esta universidad tiene 35 facultades, por tanto, se necesitan 6 bits (2^5=32 < 35!!) para representar la localización.

Por tanto, se tienen que sobran (16 – 3 – 6 = 7) bits para usar de forma libre en cada localización.

El esquema de direccionamiento quedaría así:

2001:db8:1234:GGGLLLLLLBBBBBBB::/64

Y ejemplos de direcciones concretas serían:

Tipo de Uso(G)	Facultad(L)	Asignación libre	Dirección
Infraestructura(0)	0	0	2001:db8:1234:0000::/64
Infraestructura(0)	0	1	2001:db8:1234:0001::/64
Infraestructura(0)	0	2	2001:db8:1234:0002::/64
Infraestructura(0)	1	0	2001:db8:1234:0080::/64
Infraestructura(0)	35	0	2001:db8:1234:1180::/64
Estudiantes(1)	0	0	2001:db8:1234:2000::/64
Estudiantes(1)	35	1	2001:db8:1234:3181::/64

El direccionamiento es válido, pero, ¿es legible?.

Mejora de la Legibilidad

Se podrían hacer los siguientes cambios:

- 4 bits para el tipo de uso (1 dígito hex)
- 8 bits para las localizaciones/facultaes (2 dígitos hex)
- 4 bits para las subredes de asignación ibre (1 dígito hex)

2001:db8:1234:GLLB::/64

En este caso, la universidad tendría que valorar si 16 subredes de asignación libre por tipo de uso y por localización son suficientes. Si se necesitaran más, se podría intentar una solución como la vista en el punto de “Control y Flexibilidad”

Con este nuevo esquema, ejemplos de direcciones concretas serían:

Tipo de Uso(G)	Facultad(L)	Asignación libre	Dirección
Infraestructura(0)	0	0	2001:db8:1234:0000::/64
Infraestructura(0)	0	1	2001:db8:1234:0001::/64
Infraestructura(0)	0	2	2001:db8:1234:0002::/64
Infraestructura(0)	1	0	2001:db8:1234:0010::/64
Infraestructura(0)	35	0	2001:db8:1234:0230::/64
Estudiantes(1)	0	0	2001:db8:1234:1000::/64
Estudiantes(1)	35	1	2001:db8:1234:1231::/64

De esta forma, la legibilidad de la dirección aumenta considerablemente, y permitirá a los administradores de la red de esta universidad, un trabajo más sencillo, y menos propenso a errores.

Más información:

Alhambra-Eidos
Site: www.alhambra-eidos.com
E-Mail: recepcion-correo@a-e.es
Tel.: +34 902 313 505
Twitter: @AlhambraEidos
Facebook: AlhambraEidos