Desplegando IPv6

Deploying IPv6

Jordi Bort

Resumen

De unas necesidades concretas en la Red Telemática Educativa de Catalunya (XTEC) y unas características claramente definidas en el protocolo IPv6, nace el proyecto de despliegue de esta tecnología que irá destinada a 3.000 centros educativos.

Las aplicaciones son básicamente aquellas relacionadas con tecnologías de e-learning, como streaming de audio y vídeo y aplicaciones multimedia, las cuales permiten comunicación extremo a extremo entre las escuelas y los profesores, gracias a IPv6.

En concreto estamos implementando la configuración de advertimiento de prefijos, el plan de direccionamiento, túneles IPv6 en IPv4, HTTP Streaming, 'FFPROXY', Multicast IPv6, multiconferencia con 'ISABEL', DNS IPv6, securización con SSHv6, ACLv6 y finalmente configuración del protocolo BGP IPv6.

Las características de autoconfiguración de IPv6 facilitan el despliegue cuya idea original nace de la necesidad de trabajar con programas de gestión de centros que requieren conexión '*end to end*' y siempre de forma segura por tratarse de transacciones de datos confidenciales tanto de profesorado como de alumnado. Si en este contexto hablamos de la seguridad implícita de las cabeceras IPSec en el formato IPv6, además de la eliminación del NAT y de la '*configuración cero*' por parte de los coordinadores de informática de los centros gracias a la posibilidad de advertimiento y delegación de prefijos, encontramos en esta tecnología la solución perfecta.

Palabras clave: IPv6**,** e-learning, extremo a extremo, advertimiento de prefijos, túneles 6in4, HTTP Streaming, FFPROXY, multicast IPv6, multiconferencia ISABEL, DNS, SSHv6, ACLv6, BGP IPv6, no NAT, configuración cero.

Summary

The project of deploying IPv6 technology (destined to 3.000 educative centers) is born from real necessities in the Catalonian Telematic Educational Network (XTEC) and clearly defined characteristics in the IPv6 protocol.

The applications are mainly those related to eLearning technologies, such as audio and video streaming and multimedia applications, which allow the end-to-end communication among schools and teachers thanks to IPv6.

Now, we are implementing the prefix advertisement configuration, the address planning, tunneling 6in4, HTTP Streaming, '*FFPROXY*', multicast IPv6, multiconference with '*ISABEL*', IPv6-DNS, securing with SSHv6, ACLv6 and finally, configuration the BGP IPv6 protocol.

It is also crucial the ability to easily incorporate end-to-end security, because the network carries not only the student's and teacher's traffic, but administrative information as well, and needs to be protected. IPv6 autoconfiguration features facilitate the deployment.

The necessity of uploading confidential documents, the not-NAT feature, '*zero configuration*', the prefix advertisement and delegation, all these find the perfect solution in this technology.

Keywords: IPv6**,** eLearning, end-to-end, prefix advertisement, tunneling 6in4, HTTP Streaming, FFPROXY, multicast IPv6, ISABEL, DNS, SSHv6, ACLv6, BGP IPv6, no NAT, zero configuration.

De unas necesidades concretas en la Red Telemática Educativa de Catalunya nace el proyecto de despliegue de esta tecnología que irá destinada a 3.000 centros educativos

Las características de autoconfiguración de IPv6 facilitan el despliegue

1.- Introducción

La Red Telemática Educativa de Catalunya, XTEC, gestionada por el Área de Arquitectura Tecnológica del Departament d'Educació de la Genertalitat de Catalunya está apostando por el despliegue del protocolo IPv6 en los centros educativos públicos a nivel de escuelas de Primaria e Institutos de Secundaria en el ámbito de la Comunidad Autónoma.

IPv6 es una actualización de los protocolos de redes de datos e Internet que proporciona espacio de direccionamiento para 2^{128} dispositivos globalmente accesibles en la red.

La XTEC apuntará básicamente a aquellas tecnologías relacionadas con el eLearning, como streaming de audio y video y aplicaciones multimedia, las cuales permiten comunicación extremo a extremo entre las escuelas y los profesores basadas en IPv6.

Esta tecnología en fase de lanzamiento se aplicará también para el envio de transacciones seguras en las tareas de gestión académica de los centros aprovechando la seguridad extremo a extremo implícita en el propio protocolo.

La desaparición progresiva del NAT proporcionará el crecimiento de Internet en nuevas áreas como servicios *'always-on'* y *'peer-to-peer'* que requieren que las conexiones sean establecidas en dispositivos con conexión '*end-to-end*' tanto en redes educativas como en redes domésticas.

Las características de autoconfiguración de IPv6 permite que en los centros educativos con un bajo perfil tecnológico del profesorado, el coordinador de informática pueda implementar el nuevo protocolo

Las características de autoconfiguración de IPv6 por anuncio de prefijo facilitan el despliegue y gestión de los nodos existentes así como de los que se puedan instalar en el futuro, incluyendo ordenadores y otros dispositivos, sin limitaciones del espacio de direccionamiento público.

Este sistema de autoconfiguración permite que en los centros educativos con un bajo perfil tecnológico del profesorado, el coordinador de informática pueda implementar el nuevo protocolo beneficiándose del coste adicional del matenimiento de configuración de red como ocurre con IPv4.

Por medio de la activación de IPv6 en la red de XTEC, se incrementa al máximo el potencial de explotación de la red, dado que se pueden aprovechar las capacidades de banda ancha en 3.000 centros relacionados con el Departament d'Educació de la Generalitat de Catalunya de tal forma que tanto estudiantes como profesores y personal administrativo pueden utilizar nuevos servicios. Las aplicaciones y servicios existentes pueden ser mejorados por medio de la utilización de otras características de IPv6, como movilidad y multidifusión, entre otras.

XTEC es Local Internet Registry (LIR) y desde Diciembre de 2002 se constituye como Autonomous System (AS21193). Si hablamos de cerca de 3.000 centros educativos de ámbito no universitario (desde Educación Infantil a Bachillerato), Oficinas Gestoras en Delegaciones Territoriales, Formación de Adultos, cerca de 100.000 profesores y más de 1.000.000 de alumnos potenciales, podemos entrever que no se trata de una red experimental.

Como toda fase de despliegue lleva implícita una evolución, en el caso de XTEC se habilitó un advertimiento de prefijos con la aplicación 'zebra' en un BSD y extensible sólo a la propia LAN

De hecho la implementación de esta tecnología en comunicaciones es relativamente simple en cuanto se requiere un hardware que soporte el protocolo y enlaces de comunicaciones que proporcione conectividad IPv6 nativa como puede ser la red IPv6 de RedIRIS.

Como toda fase de despliegue lleva implícita una evolución, en el caso de XTEC se habilitó un advertimiento de prefijos con la aplicación '*zebra*' en un BSD y extensible únicamente a la propia LAN. El tema de seguridad se implementó con '*ip6fw*' en el mismo BSD. La evolución ha hecho que el advertimiento de prefijos se centralice en un Catalyst-6500 que comunica con más de una decena de redes virtuales (VLAN) entre distintas tipologías de servidores y perfiles de estaciones de trabajo.

En cada VLAN se procede a su propio advertimiento de prefijos para que los hosts compendien el formato final de su IPv6. Básicamente en ordenadores con SO Linux es automático (en los últimos núcleos ya se presenta de forma no experimental) y en la mayoría de Windows XP nos basta con ejecutar desde símbolo de sistema "ipv6 install".

2.- Desarrollo y actuaciones

A modo de pincelada el ámbito de actuación se está desarrollando en diversos campos.

- **Configuración del Advertimiento de Prefijos:** Como ya se ha anunciado anteriormente está aplicado a cada una de las VLAN sea cual sea su definición en el router (FastEthernet, Gigabit Ethernet en puerto de trunk o la misma interfaz VLAN). En nuestro caso como ejemplo se ha definido una interfaz FastEthernet que conduce el tráfico de distintas VLAN de servidores externos que dan servicio en Internet y a modo de subinterfaz con encapsulación '*dot1.q*' definimos el advertimiento de prefijos para cada una de ellas.

```
ipv6 nd prefix 2001:A50:43::/64 infinite infinite
```

  Hemos de tener en cuenta que la opción 'infinite' es necesaria para que el TTL no caduque nunca y así cualquier reinicio de router o máquinas que se añaden a la LAN puedan configurar su propia IPv6 de forma automática.

Hemos de acostumbrarnos a pensar en 'versión 6' y dejarnos llevar por un estado de derroche en contraposición al de ahorro al que nos tenía acostumbrado el mundo IPv4

- **Plan de direccionamiento:** Si una cosa hay que tener clara en el vasto universo de IPv6, a parte de cambiar la mentalidad y perspectiva de una nueva dimensión de entender las direcciones IP, es cómo vamos a asignar el direccionamiento a nuestros clientes de forma coherente y ordenada para no dejar grandes vacíos sin asignar. De todas maneras hemos de acostumbrarnos a pensar en 'versión 6' y dejarnos llevar por un estado de derroche en contraposición a un estado de ahorro al que nos tenía acostumbrado el mundo IPv4.

  En el caso de XTEC teníamos que pensar en un plan de direccionamiento de 3000 /48 (200 /48 en una primera fase como especifica RIPE y el resto de forma escalonada). En nuestro caso se optó por designar 16 bits libres a continuación de los 32 de prefijo. Con 16 bits cubríamos con creces todas las tipologías de perfil cliente.

16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

  Así, el bit 16 designaba a 0 una ubicación en la sede central ó con un 1 a un cliente externo. El bit 15 designaba a 0 la tipología de un centro educativo ó a 1 una oficina gestora. Dentro de cada clasificación y dependiendo de cada una de ellas tenemos bits de 14 al 10 para designar VLAN en el caso de oficinas gestoras, del 14 al 3 autonuméricos para cada centro educativo, etc. De todas formas en cada clasificación según los perfiles de cliente hemos dejado 2 bits libres que actúan de comodín para asignar en caso de necesidad.

Mientras la comunicación entre clientes no sea IPv6 nativa, hemos tenido que habilitar túneles IPv6 en IPv4 (6in4)

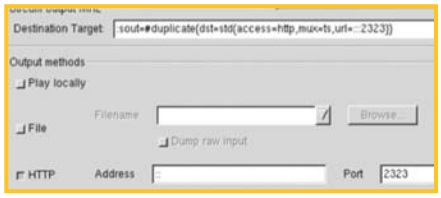
- **Túnel '6in4':** Mientras la comunicación entre clientes (routers ADSL, Punto a punto, satélites unidireccionales y bidireccionales) no sea IPv6 nativa, para poder aprovechar la conectividad IPv6 que nos ofrecen los '*carriers*' (AL-Pi y RedIRIS) hemos tenido que habilitar túneles IPv6 en IPv4 (*6in4*) cuya configuración se muestra a continuación.

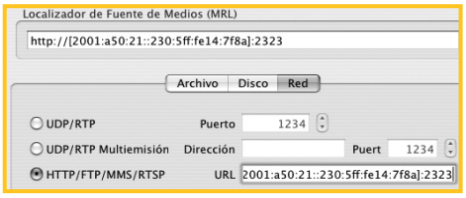
```
!
interface Tunnel1
no ip address
ipv6 address 2001:A50:4:2::2/126
tunnel source FastEthernet0
tunnel destination 213.176.160.1
tunnel mode ipv6ip
!
```

```
!
interface FastEthernet0
ip address 192.168.0.1.255.255.0 secondary
ip address 82.151.214.61.255.255.255.252
no ip redirects
ip nat inside
speed auto
ipv6 address 2001:A50:5::3/64
ipv6 enable
ipv6 nd prefix 2001:A50::/64 infinite infinite
```

- **'ffproxy':** Para poder permitir a hosts con protocolo único IPv6 acceder al mundo IPv4 nativo en cuanto a navegación HTTP y FTP, se montó en un servidor con sistema operativo BSD la aplicación '*ffproxy*' que está diseñada para tal fin.

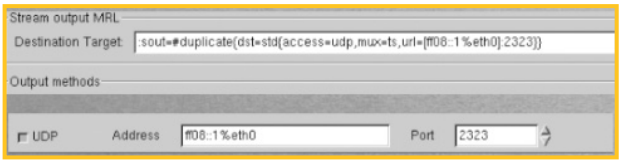
- **HTTP Streaming:** La potente herramienta 'Videolan' con contrastado soporte IPv6 nos permite emitir vídeos de índole educativa adecuados al currículum vigente bajo la concepción de la enseñanza electrónica. La configuración de servidor, en nuestro caso corriendo en Debian aparece en primer lugar y la de cliente (por poner un ejemplo de otro SO, un Mac OS X) en segundo.





La potente herramienta 'Videolan' con contrastado soporte IPv6 nos permite emitir vídeos de índole educativa bajo la concepción de la enseñanza electrónica

- **Multicast IPv6:** Si avanzamos un paso en la optimización de la emisión de vídeo con fines educativos nos encontramos de nuevo con 'Videolan' y la posibilidad del lanzamiento de un canal educativo aprovechando la tecnología 'Multicast'. Esta tecnología permite que a un mismo flujo de emisión puedan contactar distintas audiencias a modo de cliente con el obvio ahorro de ancho de banda frente al 'HTTP Streaming' en el que las emisiones se lanzan en paralelo para cada uno de los clientes. La sentencia de lanzamiento en multicast IPv6 se muestra en la figura siguiente:

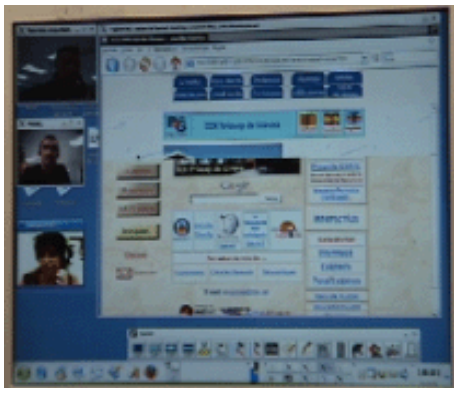


Por supuesto que desde línea de comandos también podemos lanzar la emisión.

```
vlc dvdsimple:/dev/dvd –ipv6 –sout udp:\[ff08::1%eth0\]
```

La tecnología 'Multicast' permite que a un mismo flujo de emisión puedan contactar distintas audiencias a modo de cliente con el obvio ahorro de ancho de banda

- **ISABEL:** Esta aplicación gestada en ETSIT-UPM ha alcanzado la madurez necesaria para ser el referente estrella de multiconferencia en el ámbito educativo. El acceso nativo en IPv6 trabajó de forma estable en las pruebas que se hicieron con distintas universidades, tres centros educativos piloto y nuestra sede central. La finalidad de la utilización de 'ISABEL' es la idea básica de compartir conocimientos (*knowledge sharing*) posibilitando a la vez que centros educativos en zonas geográficas muy dispersas (dada la holografía montañosa de Cataluña) puedan comunicarse desde sus lugares de origen sin la necesidad u obligación de desplazarse para objetivos afines al currículum educativo. Muestra de ello tenemos en la captura de una de la pruebas piloto que se realizaron sobre IPv6 nativo.



- **DNS:** "El tamaño SI importa". Con direcciones de 128 bits se hace imprescindible la declaración de hosts y servidores en todas las LAN de los Servicios Centrales de XTEC para que puedan ser accesibles por nombre. En un segundo estadio se implementarán los centros con DNS propio y tecnología IPv6 enlazándolos con '*forward*' a los DNS Primario y Secundario de XTEC.

Un ejemplo de resolución con '*query AAAA*' y algunas entradas en un fichero de directos utilizando '*Bind 9*' los tenemos en estas capturas

Para la generación de las distintas entradas se partió de una tabla ARP generada a partir de consultas ICMP donde se aíslan con un *script* la IP y la dirección MAC. En base a esta información y a la utilización del binario *ipv6calc*, donde se define también el prefijo que en nuestro caso es 2001:A50::/32, se irán conformando todas la direcciones IPv6.

```
pedregada:~ $ nslookup
Note:  nslookup is deprecated and may be removed from future releases.
Consider using the `dig' or `host' programs instead.  Run nslookup wit
the `-sil[ent]' option to prevent this message from appearing.
> set q=AAAA
> sis47
Server:         213.176.161.13
Address:        213.176.161.13#53

Non-authoritative answer:
sis47.xtec.net  has AAAA address 2001:a50:21::230:5ff:fe14:7f8
```

```
gw-162-1        IN AAAA     2001:a50:0:0:209:12ff:fe11:8202
osiris          IN AAAA     2001:a50:0:0:230:5ff:fe19:647
sis7            IN AAAA     2001:a50:0:0:230:5ff:fe14:65f9
ossamajor       IN AAAA     2001:a50:0:0:20d:61ff:fe2a:6178
oliana          IN AAAA     2001:a50:0:0:203:baff:fe1d:a92f
sis14           IN AAAA     2001:a50:0:0:2c0:26ff:fea1:7c81
sis18           IN AAAA     2001:a50:0:0:230:65ff:fe70:b30a
vitel-poly2     IN AAAA     2001:a50:0:0:2e0:dbff:fe03:92b6
```

- **Securización:** Como en toda inmersión en un mundo desconocido se requiere de esa dosis de cautela aunque te cuenten las mil maravillas del protocolo con sus cabeceras IPSec o el bajo índice de probabilidad de un escaneo de puertos dado lo vasto de la dimensión del direccionamiento IPv6. En nuestro caso se ha abordado desde el punto de vista de acceso remoto con SSHv6 y ACLs en los routers aplicados a cada una de las VLAN. En un principio se habilitó únicamente ICMP para poder constatar la conectividad IPv6 entre máquinas de distintas VLAN. Con el tiempo hemos ido afinando distintas visibilidades por puertos concretos dependiendo de la necesidad y del propio desarrollo de aplicaciones con soporte IPv6. Quizás sea obvio pero la ACL que declaremos la debemos tener aplicada en la interfaz VLAN que corresponda al tráfico IPv6 que queremos filtrar. Un ejemplo de ello queda reflejado en las dos capturas siguientes:

La ACL que declaremos la debemos tener aplicada en la interfaz VLAN que corresponda al tráfico IPv6 que queremos filtrar

Sólo un apunte. Si os queréis ahorrar un 80% de tráfico de intentos de intrusión a través de SSH, cambiad el puerto. ¡Qué alivio!

```
pedregada:~ $ ssh -v -6 -lusuari centreadsl.xtec.net

OpenSSH_3.8.1p1, OpenSSL 0.9.7b 10 Apr 2003
debug1: Reading configuration data /etc/ssh_config
debug1: Connecting to centreadsl.xtec.net [2001:a50:5::230:5ff:fe26:828d] port 22.
debug1: Connection established.
debug1: Next authentication method: keyboard-interactive
Password:
debug1: Authentication succeeded (keyboard-interactive).
debug1: channel 0: new [client-session]
debug1: Entering interactive session.
Linux centrev6 2.4.27-2-686 #1 Fri Mar 25 11:48:59 JST 2005 i686 GNU/Linux
Last login: Fri May 13 14:28:56 2005 from 2001:a50:21:0:20a:27ff:fed7:892e

usuari@centrev6:~$
```

- **BGP IPv6:** La gestión autónoma de las comunicaciones al ser constituidos como '*Autonomous System*' (AS 21193) nos ha permitido acceder al Internet IPv6 en base al protocolo BGP IPv6. La declaración de un vecino (*neighbor*) en nuestro router y el anuncio de prefijo en la '*address-family ipv6*' es como se muestra en la última figura.

La gestión autónoma de las comunicaciones al ser constituidos como 'Autonomous System' nos ha permitido acceder al Internet IPv6 en base al protocolo BGP IPv6

```
ipv6 access-list GLOBAL
 permit icmp FE80::/10 FE80::/10
 permit icmp any FE80::/10
 permit icmp FE80::/10 FF02::/16
 permit ipv6 2001:A50:21::/64 2001:A50:21::/64
 permit ipv6 2001:A50:21::/64 2001:A50:31::/64
 permit ipv6 2001:A50:21::/64 2001:A50:30::/64
 permit ipv6 2001:A50:21::/64 2001:A50:32::/64
 permit ipv6 2001:A50:21::/64 2001:A50:33::/64
 permit ipv6 2001:A50:21::/64 2001:A50:41::/64
 permit ipv6 2001:A50:21::/64 2001:A50:42::/64
 .....
 .....
```

3.- El futuro

Nuestra carta a los Reyes Magos, aun siendo conscientes que las cosas de palacio van despacio y más tratándose de una entidad gubernamental, debe ir en la dirección de:

```
router bgp 21193
 bgp log-neighbor-changes
 neighbor 2001:40B0:1::F001 remote-as 13041
 neighbor 2001:40B0:1::F001 description IPv6-ANELLA/REDIRIS
 neighbor 2001:40B0:1::F001 version 4
 .....
 !
 !
 address-family ipv4
 no neighbor 2001:40B0:1::F001 activate
 .....
 .....
 exit-address-family
 !
 address-family ipv6
 neighbor 2001:40B0:1::F001 activate
 network 2001:A50::/32
 no synchronization
 exit-address-family
!
```

Aún debemos implementar y extrapolar todas las aplicaciones al nuevo protocolo como la Web, Proxy, VoIP, Multiconferencia, Transacciones seguras, e-

- Migrar todo el transporte de red de IPv4 a IPv6
- Implementar y extrapolar todas las aplicaciones al nuevo protocolo como la Web, Proxy, VoIP, Multiconferencia, Transacciones seguras, e-Learning,...
- Disponibilidad de todos los servicios actuales (que superan el centenar) en *dual-stack*
- IPv6 nativo en todo y para todos
- Actualizar el IOS y la memoria RAM de todos los routers ADSL clientes de nuestros centros educativos para que soporten el protocolo IPv6
- Y por supuesto, incluir el prerrequisito IPv6 en todos y cada uno de los nuevos contratos públicos

Jordi Bort
(jbort@xtec.net)
Area de Arquitectura Tecnológica
XTEC - Departament d'Educació
Generalitat de Catalunya