novática
Revista de la Asociación de Técnicos de Informática

Novática, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de **ATI** (Asociación de Técnicos de Informática), organización que edita también la revista **REICIS** (Revista Española de Innovación, Calidad e Ingeniería del Software).

<http://www.ati.es/novatica/>
<http://www.ati.es/reicis/>

ATI es miembro fundador de **CEPIS** *(Council of European Professional Informatics Societies)* y es representante de España en **IFIP** *(International Federation for Information Processing)*; tiene un acuerdo de colaboración con **ACM** *(Association for Computing Machinery)*, así como acuerdos de vinculación o colaboración con **AdaSpain**, **AI2**, **ASTIC**, **RITSI** e **Hispalinux**, junto a la que participa en **ProInnova**.

Coordinación Editorial, Redacción Central y Redacción ATI Madrid
Padilla 66, 3º, dcha., 28006 Madrid
Tlfn.914029391; fax.913093685 <novatica@ati.es>
Composición, Edición y Redacción ATI Valencia
Av. del Reino de Valencia 23, 46005 Valencia
Tlfn. 963740173 <novatica_prod@ati.es>
Administración y Redacción ATI Cataluña
Via Laietana 46, ppal. 1ª, 08003 Barcelona
Tlfn.934125235; fax 934127713 <secregen@ati.es>
Redacción ATI Aragón
Lagasca 9, 3-B, 50006 Zaragoza.
Tlfn./fax 976235181 <secreara@ati.es>
Redacción ATI Andalucía <secreand@ati.es>
Redacción ATI Galicia <secregal@ati.es>
Suscripción y Ventas <novatica.subscripciones@atinet.es>
Publicidad Padilla 66, 3º, dcha., 28006 Madrid.
Tlnf.914029391; fax.913093685 <novatica@ati.es>
Imprenta: Derra S.A., Juan de Austria 66, 08005 Barcelona.
Depósito legal: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Portada: Corredor de hierba - Concha Arias Pérez / © ATI
Diseño: Fernando Agresta / © ATI 2003

sumario

Nº 220, noviembre-diciembre 2012, año XXXVIII

Tema del próximo número: "Modularidad en el diseño de software"

Hasta el infinito y más allá

Cuando los de nuestra generación empezaron en Internet, los ordenadores eran caros. Excepto tal vez las personas y familias más pudientes que podían permitirse la adquisición de un portátil (que por entonces podía llegar a costar fácilmente el doble que un sobremesa con la misma configuración), el resto vivíamos con un solo ordenador para toda la familia, generalmente un sobremesa en algún rincón de la casa que compartíamos.

No queremos ponernos en plan "batallita" ni "cualquier tiempo pasado fue mejor", como reza el tópico, pero lo cierto es que las cosas han cambiado y mucho.

Actualmente, cualquier usuario medio en muchos rincones del mundo fácilmente puede disponer de teléfono inteligente (*smartphone*), tableta, portátil y sobremesa. El Internet de las cosas está llevando la conectividad mucho más allá: *Smart TV's*, relojes, coches ¡e incluso neveras y lavadoras!

Esto es lo que se ve, pero lo mejor está detrás de todos estos nuevos dispositivos. Hagamos un recuento: si antes podíamos repartir un solo aparato "en línea" entre tres, cuatro, o cinco personas, ahora estamos hablando de un potencial de tres dispositivos por persona más uno o dos compartidos por cada unidad familiar. La "logística" del asunto debe evolucionar.

El IPv6 sea tal vez para el gran público el incomprendido (por oculto) de la historia, mientras que para nosotros [los profesionales] se revela como la herramienta imprescindible que debe hacer posible que cada dispositivo pueda interactuar con la Red como un ente, sin depender de extraños artificios como las redes locales, un misterio insondable para aquellos que carecen de conocimientos técnicos.

El despliegue del IPv6 llega tarde pero aún tenemos tiempo. No es una afirmación incomprensible, nos explicamos: aún queda trabajo por hacer que debería haberse zanjado ya, pero aún disponemos de margen de maniobra para completarlo.

Hasta ahora, las empresas y el sector de las comunicaciones han retrasado al máximo su puesta en funcionamiento, y es trabajo nuestro hacerles ver (a ellos y a la sociedad) la necesidad de ampliar la autopista para que quepan tantos coches. Sin prisa pero sin pausa, como dice la "*vox populi*", dando a conocer en todo momento nuestro trabajo, el porqué de éste, y explicando debidamente qué es y para qué sirve el IPv6 a la sociedad que es, a fin de cuentas, para quien trabajamos.

Como parte de nuestra misión fundamental, desde ATI seguiremos atentamente y contribuiremos en todo lo posible (tanto en nuestro ámbito informático como a nivel general) a que se realice la adecuada difusión de los elementos técnicos, de sus motivaciones y aplicaciones, que, como es el caso patente de IPv6, van a ser protagonistas del presente y del futuro de nuestra sociedad de la información.

Así pues, no solamente se trata de una labor técnica, sino de justificación para que quienes no son tecnólogos nos comprendan y se acerquen a nosotros un poco más.

La Junta Directiva General de ATI

en resumen El futuro ya está aquí y se hace compatible con el presente

Llorenç Pagés Casas
Coordinación Editorial de ***Novática***

El despliegue de IPv6 ya es hoy una realidad y esta vez va en serio. Éste es el mensaje principal contenido en la monografía del presente número de ***Novática*** titulada "*Internet IPv6: una revolución silenciosa*" cuyos editores invitados han sido ***Jordi Domingo Pascual*** (Universitat Politécnica de Catalunya), ***Eduardo Jacob*** (Universidad del País Vasco / Euskal Herriko Unibertsitatea) y ***Carlos Ralli Ucendo*** (Telefónica I+D).

Sin duda, tanto el agotamiento inminente de las posibilidades de seguir con IPv4 como las estadísticas del despliegue contenidas en algunos de los artículos de la monografía así lo señalan.

Estamos convencidos de que el lector de ***Novática*** que leyó con detalle otra monografía, precursora de la presente, que publicamos en 2005 titulada "*IPv6 - Más que un protocolo*", esperaba que el mensaje de hoy lo hubiéramos podido dar hace ya bastante tiempo.

Sin embargo, la realidad es que la inercia del funcionamiento anterior y la necesidad de compatibilizar lo nuevo con lo que ya está en marcha ha hecho posponer el despliegue de IPv6 durante largos años.

Finalmente, las convocatorias de los "días de IPv6" en junio de 2011 y 2012 han resultando decisivas para acabar llamando la atención y poniendo de acuerdo a los distintos actores que debían "mover ficha".

Por otra parte, cabe decir que algo parecido sucede en muy diversos ámbitos de la vida. Evolucionar no es fácil sobre todo cuando venimos de un pasado con una larga y extensa trayectoria. En esos casos, compatibilizar el presente con lo que nos viene en el futuro no suele resultar sencillo.

Precisamente ahora mismo en ***Novática*** estamos inmersos en un proceso de este tipo. Después de muchos años apareciendo como revista impresa, referente en la Informática española e iberoamericana, nos convertimos por mor de los tiempos que corren en revista digital.

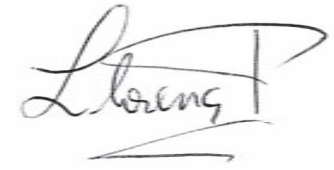
Y estamos adaptando nuestros mecanismos a ello: La revisión de los acuerdos con anunciantes y promotores de eventos patrocinados y la habilitación de una plataforma ágil y sencilla de acceso a los contenidos por parte de nuestros suscriptores son dos de nuestros retos actuales. Por supuesto, confiamos en que esta adaptación sea ya cuestión de unos pocos meses, y dejar a todos plenamente satisfechos.

Esperamos también que a lo largo de estos próximos meses el lector pueda ir apreciando novedades enriquecedoras y atractivas en nuestro nuevo formato digital.

Este número es el primero en el que a la publicación de la revista agregamos un "test de conocimiento previo" que invitamos al lector a realizar, revisando posteriormente las respuestas que proponemos, como un medio sencillo y práctico de que realice una primera toma de contacto con el tema planteado en la monografía y conozca así, a modo general, qué puede esperar de ella.

Esta es una primera muestra del esfuerzo por innovar que estamos realizando en nuestro proceso de adaptación al formato digital.

Confiamos en que os pueda ser útil.



Últimas actividades del IFIP TC13 *Human-Computer Interaction*

Julio Abascal González
Universidad del País Vasco-Euskal Herriko Unibetsitatea; representante de ATI en el IFIP TC13
<julio.abascal@ehu.es>

Reuniones plenarias

Desde mi último informe en ***Novática*** sobre el Comité Técnico TC13 de IFIP, éste ha celebrado dos reuniones plenarias.

La primera, el día 9 de septiembre de 2011 en Lisboa, coincidiendo con INTERACT 2011[2], el congreso auspiciado por el TC13. A esta reunión asistimos representantes de 18 países, cinco directivos de grupos de trabajo del TC13 y un miembro experto.

Los copresidentes de INTERACT 2012, Joaquim Jorge y Philippe Palanque, presentaron su informe provisional, lo que dio lugar a una discusión sobre la necesidad de recoger las experiencias de las sucesivas ediciones del congreso para mantener su continuidad (incluyendo el archivo de los sitios web) y la conveniencia de actualizar el documento de criterios de calidad de INTERACT. Además, se aprobó una plantilla de informe de resultados del congreso y de cuestionario post-congreso.

Por su parte, las copresidentas de INTERACT 2013[3], Paula Kotze y Janet Wesson, presentaron los preparativos del mismo, que se celebrará del 2 al 6 de septiembre en Ciudad del Cabo (Sudáfrica), con el lema "*designing for diversity*". Para este congreso se hará un especial esfuerzo en recuperar subvenciones que permitan becar a investigadores de países en desarrollo para que puedan asistir al congreso (una iniciativa llevada adelante con éxito en INTERACT 2003[4], que facilitó la asistencia de seis personas procedentes de India, Tailandia, Brasil, Sudáfrica, Serbia y Polonia). Además de otros asuntos de rutina, el presidente del TC13, Jan Gulliksen, anunció la convocatoria de propuestas para la sede de INTERACT 2015 que sería resuelta en la siguiente reunión.

Por otro lado, Henry Been-Lim Duh y Nahoum Gershon presentaron una propuesta para crear el grupo de especial interés ""*13.15 SIG: Social Networking and Mobile Interaction"*, cuya aceptación fue pospuesta para permitir ciertas modificaciones solicitadas por los asistentes.

La siguiente reunión se celebró en Singapur el 28 de febrero de 2012. Asistimos representantes de 20 países, 3 directivos de grupos de trabajo del TC13 y 3 miembros expertos. Los respectivos presidentes presentaron los informes definitivo de INTERACT 2011 y de progreso de INTERACT 2013. La selección de la sede para INTERACT 2015 ocupó una gran parte de la reunión debido al gran número de candidaturas recibidas y a la necesidad de aclarar algunos de los criterios de selección que se habían publicado.

Tras la presentación de las seis candidaturas: Bamberg (Alemania), Budapest (Hungría), Limassol (Chipre), Mumbai (India), Paphos (Chipre) y Vienna (Austria), se decidió por votación secreta que INTERACT 2015 se celebre en Bamberg del 14 al 18 de septiembre de 2015, copresidido por Tom Gross (Alemania) y Julio Abascal (España).

Después de tratar los asuntos de rutina, se decidió reestructurar el sitio Web del TC 13 y reactivar la publicación del *TC 13 newsletter*. También se aprobó la creación de un comité *ad hoc* para estudiar la posibilidad de que INTERACT pase de ser bianual a anual y realizar una propuesta en esa línea.

Henry Been-Lirn Duh (Singapur) hizo una presentación sobre el desarrollo de HCI en Asia y planteó la posibilidad de crear capítulos regionales de IFIP TC13. Se pidió a John Karat (USA) que preparara un informe sobre su viabilidad para la próxima reunión.

Como viene siendo habitual en las reuniones no ligadas a INTERACT, la víspera de la reunión se celebró un seminario, *Singapore Human-Computer Interaction Symposium 2012*, organizado por el *Interactive and Digital Media Institute (National University of Singapore)*, en el que participaron investigadores de la comunidad local de HCI, con el objetivo de promover el intercambio de conocimientos y experiencias. El seminario contó con presentaciones de 15 miembros del TC13 y 7 miembros de diferentes universidades de Singapur.

Las próximas reuniones del TC13 se celebrarán en Toulouse (Francia) del 11 al 14 de marzo y en Ciudad del Cabo (Sudáfrica), entre el 2 y el 6 de septiembre, dentro de INTERACT 2013.

Congreso INTERACT 2011

Volviendo al congreso INTERACT 2011, creo interesante analizar algunos datos de la edición de Lisboa, ya que excepcionalmente la participación española fue muy numerosa.

Se recibieron 402 artículos largos (un incremento del 9,5% respecto de 2009) de los que se seleccionaron 112 (índice de aceptación: 28%) y 278 artículos cortos de los que se seleccionaron 60 (índice de aceptación: 22%), con la participación de 800 revisores.

Además se aceptaron 54 *posters*, y se celebraron 14 *workshops* y 6 *tutorials*. Las actas, de unas 2800 páginas, se publicaron en cuatro volúmenes de la serie LNCS de Springer[5]. Respecto de la participación, se inscribió un total de 538 participantes de 40 países, de los cuales 66 eran españoles.

Dado que en anteriores ocasiones la participación española en INTERACT ha sido minoritaria, este crecimiento se puede atribuir a la proximidad geográfica y a la previa celebración del congreso Interacción 2011, que resumiré a continuación. De todas maneras, es de esperar que Lisboa sea el punto de partida de una mayor participación española en INTERACT.

Congreso Interacción 2011

La organización del congreso Interacción 2011 de la *Asociación de Interacción Persona Computador* (AIPO) acordó su celebración en Lisboa, durante la semana anterior a INTERACT 2011, para facilitar el acercamiento entre las comunidades científicas hispana y portuguesa y mejorar la participación española en INTERACT. Se recibieron 55 artículos largos cada uno de los cuales fue revisado por tres expertos del comité de programa internacional. Éste seleccionó 24 de ellos (tasa de aceptación del 43,6%) que fueron

publicados en papel y digitalmente en las actas del congreso[6]. Dada la alta calidad de los trabajos recibidos, el comité de programa de INTERACT propuso su aceptación también como *posters* en dicho congreso[7] para darles una mayor proyección.

Además, siete artículos fueron seleccionados para enviar una versión extendida a la revista *Science of Computer Programming* (SCP). De ellos, se seleccionaron cuatro que serán publicados en un *Special Issue on Methodological Development of Interactive Systems*.

El TC13 valoró muy positivamente la experiencia de organización de eventos regionales ligados a INTERACT y propuso a los organizadores de los futuros congresos INTERACT que lleven a cabo iniciativas similares.

Llamada a la participación

Como en anteriores ocasiones, quisiera finalizar recordando a los interesados en Interacción Persona-Computador la posibilidad de participar en los diversos grupos de trabajo del TC13[8]:

- *WG 13.1: Education in HCI and HCI Curriculum*
- *WG 13.2: Methodologies for User-Centred Systems Design*
- *WG 13.3: Human-Computer Interaction and Disability (HCI and Disability)*
- *WG 2.7(13.4): User Interface Engineering*
- *WG 13.5: Human Error, Safety, and System Development*
- *WG 13.6: Human-Work Interaction Design (HWID)*
- *WG 13.7: HCI and Visualization*

Notas

[1] <interact2011.org/>.

[2] <http://www.interact2013.org/>.

[3] <http://www.idemployee.id.tue.nl/g.w.m.rauterberg/conferences/INTERACT2003/proceedings.html>.

[4] Pueden adquirirse a través del sitio SpringerLink: LNCS 6946, 6947, 6948, 6948 Human-Computer Interaction – INTERACT 2011 13th IFIP TC 13 International Conference, Lisbon, Portugal, September 5-9, 2011, Proceedings, Parts I, II, III, IV.

[5] **N. Garay-Vitoria, J. Abascal (Eds.).** *Actas del XII Congreso Internacional de Interacción Persona-Ordenador – Interacción 2011* (Lisboa, septiembre 2011). Ibergarceta. 2011, ISBN: 987-84-9281-234-9.

[6] **P. Campos et al. (Eds.).** *Human-Computer Interaction - INTERACT 2011 - 13th IFIP TC 13 Int. Conf.*, Lisbon, Portugal, 5-9/9/2011, Proceedings, Part IV. LNCS 6949 Springer 2011, ISBN 978-3-642-23767-6.

[7] *Working Groups of TC13*. <http://csmobile.upe.ac.za/ifip/working-groups-of-tc.13>.

Asamblea General de CLEI

El pasado día 4 de octubre de 2012 se celebró en Medellín (Colombia) la Asamblea General de CLEI (Centro Latinoamericano de Estudios en Informática).
Diversos fueron los principales temas tratados, entre los que, aparte de los consabidos asuntos de trámite sobre la aprobación del presupuesto, la liquidación de las cuentas, los informes del presidente y de la secretaria, confirmación de la aceptación de nuevos miembros, etc., conviene resaltar que se eligió un nuevo comité directivo compuesto por:

- Gabriela Marín de la Universidad de Costa Rica (San José, Costa Rica), como presidenta.
- Ernesto Cuadros de la Universidad de San Pablo (Arequipa, Perú) y de la Sociedad Peruana de Computación, como secretario.
- María Elena García de la Universidad Nacional de Asunción (Asunción, Paraguay), como tesorera.
- Rodrigo Santos de la Universidad del Sur (Bahía Blanca, Argentina) pasa a ser presidente saliente.

Actividad conjunta de IFIP WG6.9 y CLEI para 2013

En el momento de redactar esta nota se puede informar que el *Working Group 6.9, Communication Networks for Developing Countries*, de la IFIP está planteando organizar en colaboración con el CLEI (miembro de IFIP) y dentro de su serie de actividades docentes para países en desarrollo, un conjunto de tutoriales (probablemente en Costa Rica y El Salvador) con colaboración de universidades de esos países.

En estos momentos se está tratando cual sería el programa de mayor interés, buscando los profesores idóneos para el desarrollo de ese programa y ajustando las fechas que convengan a profesores y asistentes.

Ramon Puigjaner Trepat
Vicepresidente de IFIP;
Representante de ATI en IFIP y CLEI

Cambio de presidente en el TC6 de IFIP

Desde el día primero de enero de 2013, Guy Leduc ha dejado de ser el presidente (*Chair*) del TC6 (*Communication Systems*) después de haber cumplido los dos períodos consecutivos de tres años, el máximo permitido por las normas de la IFIP.

Le ha substituido el Profesor Aiko Pras, profesor de la universidad de Twente y representante de los Países Bajos en el TC6. Fue el único miembro del TC6 que se presentó para substituir a Guy Leduc, por lo que no fue necesario proceder a ninguna elección.

Sin embargo, la mayoría de los miembros del TC6 refrendaron su nombramiento.

Reactivación del interés de la *Sociedade Brasilera de Computaçao* en la IFIP

En el pasado mes de julio se celebró en Curitiba (Brasil) dentro del congreso anual de la *Sociedade Brasilera de Computaçao* (SBC) una mesa redonda en la que participaron diversas sociedades científicas (ACM, CLEI, IEEE-CS e IFIP) que expusieron sus planes de colaboración. Por parte de IFIP participó el vicepresidente Ramon Puigjaner. Uno de los resultados de esa mesa redonda ha sido la decisión de la SBC de ampliar su participación en las iniciativas de IFIP.

Como primer paso en esta dirección, se decidió implicar a los comités técnicos de la SBC en un proceso que debe finalizar con la propuesta de representantes en todos los *Technical Committees* (TC) de la IFIP, para cumplir con la norma que haya un representante de cada sociedad miembro en cada TC. En la SBC se tiene el convencimiento que ese es el camino para hacer sostenible la participación de la SBC en las iniciativas de IFIP.

Por su importancia, no solo demográfica sino también por la potencia industrial que representa Brasil, no es necesario comentar que esta iniciativa ha sido muy bien recibida por IFIP.

Ana Pont Sanjuán
Representante de ATI en el TC6

Presentación. IPv6: Un nuevo espacio para la innovación

Jordi Domingo Pascual[1], Eduardo Jacob [2], Carlos Ralli Ucendo[3]

[1]Catedrático de Universidad, Departamento de Arquitectura de Computadores, Universitat Politècnica de Catalunya; [2]Profesor titular de Ingeniería Telemática de la Universidad del País Vasco / Euskal Herriko Unibertsitatea; [3]Telefónica I+D

<jordi.domingo@ac.upc.edu>, <Eduardo.Jacob@ehu.es>, <ralli@tid.es>

Durante los dos últimos años, IPv6, la nueva versión del protocolo IP, ha sido noticia en la prensa tanto especializada como en la prensa diaria. Dos hechos concretos y relacionados fueron los detonantes de las noticias correspondientes: la organización del *World IPv6 Day* en 2011 y del *World IPv6 Launch Day* en 2012, y el anuncio por parte de IANA ("*Internet Assigned Numbers Authority*") del reparto de los últimos bloques de direcciones IPv4 a los RIR ("*Regional Internet Registry*") en febrero de 2011. Este anuncio marca el fin de la disponibilidad de direcciones IPv4. Ante la cada vez más acuciante escasez de direcciones IPv4, ISOC ("*Internet Society*") promovió conjuntamente con los principales proveedores de contenidos los eventos mencionados.

A principios de la década de los 90 ya se detectó el problema de la escasez de direcciones IPv4 en un futuro más o menos próximo y el IETF ("*Internet Engineering Task Force*") empezó a trabajar para proponer diversas soluciones. Unas soluciones iban encaminadas a reducir la demanda de nuevas direcciones IP, como el CIDR ("*Classless InterDomain Routing*"), el desarrollo del NAT ("*Network Address Translation*") y una definición de políticas más restrictivas para asignar bloques de direcciones por parte de los RIR ("*Regional Internet Registry*"). La otra solución fue definir un nuevo protocolo IP con un rango de direcciones más amplio, dando lugar a IPv6.

A finales de los 90 ya estaba definido el conjunto básico de estándares de IPv6 (RFC 2460, diciembre 1998). Ha transcurrido más de una década y el nuevo protocolo todavía no se ha desplegado completamente. Ahora, ante la imposibilidad de disponer de direcciones IPv4 no hay más remedio que utilizar IPv6.

Es por este motivo que hemos propuesto como título de este número monográfico: "Internet IPv6: una revolución silenciosa".

Glosando esta idea podemos considerar que si bien el aspecto negativo es que han transcurrido más de diez años y todavía no está implantado completamente, el aspecto positivo es que durante estos años IPv6 se ha ido introduciendo de forma paulatina en la mayor parte de los sistemas operativos, plataformas, equipos de comunicaciones (equipos de red, incluso muchos dispositivos periféricos como impresoras de menos de cinco años soportan IPv6, a excepción de los *routers* ADSL y cable módems domésticos de gama baja que están empezando a hacerlo ahora), en las distribuciones de navegadores, de gestores de correo y de las aplicaciones básicas más utilizadas (por ejemplo, los servidores de DNS).

Es decir, a lo largo de estos años todas las actualizaciones del software se han ido incluyendo en la pila de protocolos IPv6. El resultado es que ahora estamos mejor preparados para comenzar a abordar la necesaria transición a IPv6 de forma satisfactoria, aunque no exenta de complejidad. De forma silenciosa IPv6 se ha ido haciendo ubicuo y ahora sólo queda que los usuarios entren en ella de forma masiva de la mano de los ISP y operadores. Esta es la parte más costosa en tiempo e inversiones ya que, aunque se han realizado ya los esfuerzos para adaptar el núcleo de la red, se necesita abordar los sistemas de provisión y gestión, así como la capilaridad intrínseca que suponen millones de *routers* en los domicilios o pequeñas empresas conectadas.

IPv6 se diseñó con el objetivo de reemplazar el protocolo IPv4 en un plazo de tiempo más o menos corto. Por este motivo el nuevo pro-

Editores invitados

Jordi Domingo Pascual es Ingeniero Superior de Telecomunicaciones por la *Universitat Politècnica de Catalunya* (ETSETB, UPC), Doctor en Informática (FIB, UPC) y Catedrático de Universidad en el Departamento de Arquitectura de Computadores (DAC, UPC). Es responsable del grupo de investigación *Comunicaciones de Banda Ancha* (CBA) y promotor y co-fundador del Centro de Investigación inter-departamental de la UPC en Comunicaciones Avanzadas de Banda Ancha (CCABA, UPC). Ha participado en proyectos europeos desde 1988 (RACE, ACTS, IST, FP6, FP7). Ha dirigido 11 tesis doctorales y publicado más de 130 artículos en revistas y congresos internacionales. Ha sido Director del Departamento (2005-2011). Actualmente, su actividad de investigación se centra en las nuevas arquitecturas de Internet y "*Network Economics*".

Eduardo Jacob Taquet es Ingeniero Industrial por la Universidad del País Vasco/ *Euskal Herriko Unibertsitatea* y doctor por la misma Universidad. Es profesor Titular de Ingeniería Telemática y en la actualidad dirige el departamento de Ingeniería de Comunicaciones en el que coordina el grupo de investigación I2T de la UPV/EHU. Ha dirigido varias tesis doctorales y ha participado en varios proyectos europeos del sexto y séptimo Programa Marco. En la actualidad su área de trabajo engloba las SDN (*Software Defined Networks*). En este sentido, el grupo de investigación ha desplegado una infraestructura basada en OpenFlow, para soportar tanto la investigación en redes como la operación clásica en su universidad (*EHU OpenFlow Enabled Facility*, EHU-OEF). En esta línea de trabajo se engloban también la participación en los proyectos del séptimo programa marco ALIEN "*Abstraction Layer for Implementation of Extensions in programmable Networks*" en el que se investiga la creación de una capa de abstracción para integración de dispositivos no OpenFlow en redes definidas por software y SECRET "*SECurity of Railways against Electromagnetic aTtacks*".

Carlos Ralli Ucendo es Ingeniero Superior de Telecomunicaciones por la Universidad Politécnica de Madrid. En 1999 realizó la primera conexión a las redes IPv6 de dicha universidad y los laboratorios de Telefónica I+D. Tras liderar Euro6IX (2002-2005), el mayor proyecto IPv6 de operadoras cofinanciado por la UE, ha sido coordinador técnico de la participación de Telefónica en las recientes jornadas mundiales de IPv6. Ha participado en análisis de riesgos *in-situ* de las redes de Telefónica en Brasil, Chile y Colombia y cuenta con una amplia experiencia en proyectos de innovación, asistiendo regularmente a la Comisión Europea como experto independiente en las auditorías técnicas de proyectos cofinanciados. Es un ponente activo, con más de medio centenar de ponencias técnicas, presentaciones relevantes y demostraciones en Asia-Pacífico, Europa y Latinoamérica. Durante el año 2011 desempeñó el papel de jefe de delegación para *Internet Society* (ISOC) y el IETF (*Internet Engineering Task Force*). Actualmente, forma parte del equipo de desarrollo de la plataforma de servicios de "*Future Internet*" FI-WARE (@Fiware) y está abriendo una línea de investigación centrada en las oportunidades e impacto de la llegada masiva de IPv6 en productos y servicios de Internet.

tocolo no es compatible con IPv4 y requiere una serie de mecanismos, denominados "mecanismos de transición", para facilitar la coexistencia entre ambos.

El nuevo diseño recoge toda la experiencia previa adquirida con IPv4. En este sentido mejora la estructura de la cabecera de los paquetes para poder procesarlos de forma mucho más eficiente, define un espacio de direcciones mucho mayor (128 bits), e incluye funcionalidades que en IPv4 se habían implementado como añadidos o parches como el mecanismo de autoconfiguración, el descubrimiento de vecinos ("*Neighbour Discovery*"), el soporte a la movilidad ("*Mobile IPv6*"), seguridad (IPSEC) y *multihoming*.

Además se organiza el espacio de direccionamiento de forma más estructurada de manera que sea más fácil la portabilidad y más eficiente el proceso de los paquetes en los *routers*. En la cabecera de los paquetes también incluye unos campos para dar soporte a las arquitecturas de calidad de servicio en Internet: servicios integrados ("*Integrated Services*") y servicios diferenciados ("*Differentiated Services*").

A pesar de las mejoras técnicas que ofrece el nuevo protocolo su adopción se ha ido relegando mientras se podían desplegar direcciones IPv4 privadas mediante NAT ("*Network Address Translation*") y mientras se disponía de direcciones IPv4. Para muchas organizaciones en Europa y Estados Unidos la escasez de direcciones no es un problema ya que tienen asignadas rangos de direcciones suficientemente grandes.

La proliferación de dispositivos móviles se vio como la gran oportunidad para desplegar IPv6 ya que se suponía que la demanda de direcciones IP aumentaría espectacularmente, sin embargo, la mayoría de los operadores han resuelto la conexión de los dispositivos móviles mediante el uso de NAT.

Otro argumento técnico a favor de IPv6 es que permite recuperar las comunicaciones "extremo-a-extremo" facilitando las comunicaciones P2P ("*Peer-to-Peer*") y la posibilidad de instalar servicios por parte de los usuarios domésticos. Una vez más todo el esfuerzo realizado ampliando las funcionalidades de NAT (por ejemplo, con NAT Traversal) hace que aplicaciones P2P y de VoIP (como Skype) puedan funcionar a través de NAT en la redes de acceso de los interlocutores.

En estos momentos la profusión de NAT y la experiencia adquirida en su utilización constituyen aspectos que han retrasado la adopción de IPv6, pero al mismo tiempo su complejidad y costes va a hacer muy atractivas las soluciones para usuarios IPv6 nativos. Esto provocará que los proveedores de aplicaciones interactivas o P2P se centren en productos (o funcionalidades extra de los mismos) de tipo *IPv6-only*, en tanto en cuanto exista una masa crítica de usuarios potenciales.

En el pasado reciente, la mayoría de las aportaciones del IPv6 no han sido valoradas por la industria y el conjunto de los usuarios como necesarias para optar por el nuevo protocolo. El nuevo protocolo solo se ve como imprescindible cuando se necesita más espacio de direccionamiento tanto público como direccionamiento privado.

Siendo la necesidad de más direccionamiento el principal motivo para su adopción, no hay que desestimar todas las ventajas que traerá consigo de forma intrínseca y que afectarán al modelo de Internet generando oportunidades y riesgos.

Precisamente es en el ámbito de aplicaciones máquina-a-máquina (M2M) donde IPv6 está gozando de una adopción más dinámica a través del estándar IPv6 para redes de sensores (WSN) conocido como 6LowPAN.

Otro motivo que ha frenado la implantación de IPv6 es que, como se ha mencionado, fue diseñado para reemplazar IPv4, con lo que los mecanismos de transición se enfocaron a soportar una transición más que a una coexistencia de las dos versiones.

Como el despliegue y gestión de los distintos mecanismos de transición es complejo y añade ciertas ineficiencias en las comunicaciones, la opción más generalizada es esperar hasta que sea estrictamente necesario desplegar IPv6 y los mecanismos de transición apropiados a cada caso.

La coexistencia indefinida de las dos versiones no es deseable ni desde el punto de vista de costes, ni de gestión ni de eficiencia. Por ello cuanto antes se alcance la masa crítica de servicios y usuarios con IPv6 más rápida será su adopción en modo nativo y se podría eliminar toda la infraestructura de soporte de los mecanismos de transición.

Un fenómeno curioso es que algunos operadores móviles están optando por esquivar esta complejidad dando a los usuarios acceso nativo IPv6 únicamente y traduciendo los accesos (NAT64) hacia la Internet-IPv4. Esto es posible puesto que esos mismos proveedores ya hacían traducción al utilizar direcciones privadas IPv4 (NAT44), por lo que la conexión IPv4 no se degrada más y, al mismo tiempo, la conexión IPv6 es más eficiente.

En 2005, en el número 174 (marzo-abril) de ***Novática***, se abordaron los aspectos tecnológicos del nuevo protocolo IPv6 destacando las aportaciones del mismo como un protocolo diseñado para sustituir a IPv4. En aquel momento la reducción de bloques de direcciones IPv4 disponibles era evidente y se habían publicado diversos estudios con predicciones sobre la fecha en que ya no quedarían disponibles más direcciones IPv4. El tiempo ha demostrado que las acciones que se tomaron sirvieron para prolongar significativamente la disponibilidad de direcciones IPv4 y que hasta el mes de febrero de 2011 no se puede considerar que se haya agotado el espacio de direcciones IPv4.

En aquel número se presentaron las características técnicas del protocolo haciendo énfasis en las opciones de autoconfiguración, soporte a la movilidad y *multihoming*, incorporación de las opciones de seguridad y mejoras en la cabecera del paquete IPv6. Se abordó también el proceso de migración de las aplicaciones a IPv6 y la problemática a resolver en entornos cliente-servidor mixtos IPv4-IPv6 y los mecanismos de transición disponibles. Finalmente, se incluyó la descripción del estado de despliegue de IPv6 en aquel momento y de los desarrollos de servicios en IPv6 pre-comerciales.

Para esta monografía de ***Novática*** hemos escogido un enfoque distinto dando por suficientemente conocido el entorno técnico de IPv6. El conjunto de artículos seleccionados aborda la tecnología y el impacto de IPv6 en los productos y servicios, el estado de despliegue de IPv6 por parte de los operadores, y la perspectiva de los usuarios. Para ello, hemos invitado a varios de los miembros del Observatorio IPv6 a escribir los distintos artículos que componen la presente monografía.

En el primer artículo sobre el "*Estado del IPv6*", ***João Luis Silva Damas*** nos introduce en la situación actual de la mano de los dos acontecimientos que han marcado sendos hitos importantes en el despliegue del nuevo protocolo. Nos referimos al *World IPv6 Day* y al *World IPv6 Launch Day*. El artículo expone los motivos que llevaron a organizar estos eventos, el planteamiento, los participantes y los resultados de los mismos.

El segundo artículo, "*Internet6: Impacto en los Productos y Servicios Digitales*" escrito por ***Carlos Ralli***, se centra en cómo la Internet IPv6 cambia el enfoque de los productos y servicios en la red. El artículo entrelaza los aspectos de la tecnología con los de los de los servicios que se pueden ofrecer a los usuarios haciendo patente a los arquitectos y desarrolladores de productos y servicios este nuevo escenario que traerá consigo nuevas oportunidades y modelos a explotar, pero también riesgos y competidores que habrá que sortear.

La contribución de ***Octavio Alfageme*** "*Ecosistema IPv6: Tecnologías utilizadas*" tiene

como objeto ponernos al día acerca de las tecnologías que se están empleando en la actualidad para desplegar IPv6 y garantizar la conectividad con la Internet IPv4.

El siguiente artículo "*Internet6: Alcanzando la masa crítica de usuarios y tráfico*" es una recopilación de datos de los distintos operadores con la intención de presentar el estado actual de la oferta de servicios IPv6 por parte de los operadores. Este trabajo se ha realizado mediante una encuesta para recoger los datos de dichos operadores.

El segundo conjunto de artículos de este monográfico pretende incluir la visión del despliegue de IPv6 desde el punto de vista de los usuarios. En este sentido, el artículo "*Despliegue en las empresas y redes corporativas. La visión de un integrador*" de ***Miguel González Fernández*** nos plantea el punto de vista de un integrador de productos que debe proponer soluciones concretas a sus clientes analizando el impacto de la introducción de IPv6 en las redes corporativas.

A continuación, ***Josu Aramberri*** con el artículo "*IPv6: Internet Society y la visión de los usuarios*" destaca el papel de ISOC en la dinamización del despliegue de IPv6 y la participación del capítulo español ISOC-ES y de las redes académicas.

Enlazando con este artículo, "*Internet IPv6 en las redes académicas y de investigación: RedIris*" deja testimonio del papel de las redes académicas, y de RedIRIS en particular, en el desarrollo y despliegue de IPv6. Los autores, ***Tomás P. de Miguel***, ***Miguel Ángel Sotos***, ***Francisco Monserrat*** y ***Esther Robles***, dejan constancia de la participación de RedIRIS como red pionera en las fases de prueba y posterior despliegue de IPv6.

Jordi Palet Martínez con su artículo "*Actividades del IETF con respecto a IPv6*" deja constancia del ingente trabajo realizado en los distintos grupos de trabajo para definir los RFC que permiten desplegar IPv6. Asimismo, expone los temas de trabajo actuales para finalizar con la implantación del nuevo protocolo.

Cierra este monográfico el artículo de ***Eduardo Jacob*** titulado "*Redes Definidas por Software e IPv6: Situación actual*", en el que tras una introducción a las Redes Definidas por Software ("*Software Defined Networks*"), se muestra la compatibilidad a medio de plazo de éstas e IPv6.

Para finalizar, queremos agradecer a los autores el esfuerzo que han realizado para elaborar los artículos en el plazo previsto y la paciencia que han mostrado en la fase de revisión para garantizar la coherencia de este monográfico.

No podemos terminar sin agradecer a los editores de ***Novática*** la oportunidad de publicar este número dedicado al protocolo IPv6. Esperamos que el contenido de los artículos sea de interés a los lectores y que finalmente IPv6 sea una realidad.

Referencias útiles sobre "IPv6"

Las referencias que se citan a continuación, junto con las proporcionadas en cada uno de los artículos, tienen como objetivo ayudar a los lectores a profundizar en los temas tratados en esta monografía permitiendo contrastar ideas y obtener información actualizada.

Libros

- **Silvia Hagen.** *Planning for IPv6*. O'Reilly, 2011. ISBN-10: 1449305393.
- **Cricket Liu.** *DNS and BIND on IPv6*. O'Reilly. 2011. ISBN-10: 1449305199.
- **Silvia Hagen.** *IPv6 Essentials*. O'Reilly, 2009. ISBN-10: 0596100582.
- **Niall Richard Murphy, David Malone.** *IPv6 Network Administration*. O'Reilly & Associates, 2005. ISBN-10: 0596009348.
- **Hesham Soliman.** *Mobile IPv6: Mobility in a Wireless Internet*. Pearson Education, 2004. ISBN-10: 0201788977.
- **Christian Huitema.** *IPv6 the New Internet Protocol* (second edition). Prentice Hall, 1997. ISBN-10: 0138505055.

Enlaces web

- *IPv6 para todos*. <http://www.isoc.org.ar/ediciones/ipv6ParaTodos.pdf>.
- *IPv6 nonahi*. IPv6 para todos (Euskera), <http://i2t.ehu.es/publications/resources/>.
- *IPv6 per a tothom*. IPv6 para todos (Catalán),
- <http://www.fundacio.cat/obra-social/publicacions/ipv6peratothom.html>.
- *Edición libre y en Gallego del "IPv6 para Todos"*.
- <http://www.cesga.es/es/ver_nova/idnoticia/4843>.
- **RedIris.** *Observatorio IPv6*. <http://wiki.rediris.es/observatorio_ipv6/Portada>.
- **IPv6 Forum The New Internet**. <http://www.ipv6forum.com/>, <http://www.ipv6forum.org/>.
- **The IPv6 Portal.** <http://www.ipv6tf.org/>
- **IPv6 Cluster.** <http://www.ist-ipv6.org>.
- **IETF IPv6 Working Group.** <http://www.ietf.org/html.charters/ipv6-charter.html>.
- **IETF IPv6 Multihoming Working Group**. <http://www.ietf.org/html.charters/multi6-charter.html>.
- **IETF IPv6 Operations Working Group.** <http://www.ietf.org/html.charters/v6ops-charter.html>

Proyectos europeos

- **Comisión Europea.** *6Deploy*. http://www.6deploy.eu/>.
- *LONG*. <http://long.ccaba.upc.es/>.
- **European IST Program.** *Euro6IX*. <http://www.euro6ix.org/>.
- *6Net*. <http://www.6net.org/>.
- **Unión Europea.** *6Diss*, Sixth Frame work Programme of the European Union. <http://www.6diss.org/>.

Proyectos nacionales

Ministerio de Ciencia y Tecnología. *6SOS*. <http://www.6sos.org/>.

João Luis Silva Damas
Director Técnico de Internet Systems Consortium; Fundador y Director de Bond Internet Systems, SL

<joao@bondis.org>

Estado del IPv6. *World IPv6 Day* (8/6/2011), *IPv6 Launch Day* (6/6/2012)

Resumen: *Tras varios años de desarrollo de los estándares y las primeras implementaciones con el despliegue de IPv6 desde finales de los años 90, el uso real de IPv6 en Internet estaba estancado. En un caso claro del problema del huevo y la gallina, los proveedores de Internet carecían de confianza en las implementaciones de los proveedores de equipos y de los incentivos de negocio para implementar IPv6 mientras los proveedores de contenido y de equipos carecían de los incentivos dada la falta de compradores y consumidores. Tras varios años de falta de progreso y ante el cada vez más cercano fin de la disponibilidad de direcciones IPv4 libres para continuar permitiendo el crecimiento de Internet, una serie de ingenieros de distintas proveniencias se alió con ISOC, la Internet Society, para dar un giro a la situación y desbloquear la situación. Estos esfuerzos culminaron en primer lugar con el IPv6 World Day en 2011 y continuaron con el IPv6 Launch Day en 2012. Aunque el nivel de impacto varía según la geografía, se ha conseguido dar un salto cualitativo que ha abierto las puertas a una vía para el continuo crecimiento de una Internet abierta.*

Palabras clave: *CIDR, despliegue de IPv6, distribución de direcciones IPv6, IETF, IPv6 Launch Day, ISOC, tráfico IPv6, World IPv6 Day.*

Autor

João Luis Silva Damas es Director Técnico (*Chief Technical Officer*, CTO) en *Internet Systems Consortium*, una organización con una larga historia en la creación de software libre para infraestructura de Internet y una de las organizaciones que han proporcionado acceso IPv6 a regiones en vías de desarrollo desde los años 90. Asimismo, João es fundador y director de Bond Internet Systems, SL. a través de la cual desarrolla actividades en nuevas tecnologías básicas de Internet, en particular DNS. Como parte de actividades de apoyo directo a la comunidad de Internet, es co-organizador de ESNOG/GORE y *chairman* del grupo de trabajo de "*routing*" en RIPE.

1. Introducción

A principios de los años 90, cuando el número de usuarios de Internet empezó su tremendo despegue gracias a la aparición de, entre otras, la web y los navegadores gráficos, las direcciones de IPv4 se repartían para uso en un sistema de clases (A,B,C,D y E) que hacía un uso poco eficaz de los bloques de direccionamiento. Se empezó a temer que las direcciones IPv4 disponibles para uso en Internet quedarían agotadas en pocos años. En el IETF (*Internet Engineering Task Force*) se buscó la solución a este problema mediante varias alternativas.

Por un lado se definió la distribución y encaminamiento de direcciones IPv4 sin clases (CIDR[1,2]), una medida encaminada a alargar la vida útil de IPv4 en Internet. Este cambio, ha permitido la enorme explosión de Internet a lo largo de los años 90 y primeros del siglo XXI hasta la fecha de hoy.

Por otro lado, se empezó a trabajar en alternativas para sustituir al IPv4 con el fin de tener una solución a más largo plazo. De este proceso salió lo que ahora conocemos como IPv6. Desafortunadamente, IPv6 resultó ser incompatible con IPv4 y por lo tanto se inició un prolongado proceso de despliegue y transición.

2. Despliegue temprano: El 6Bone

Una vez completado el protocolo llegó la hora de probarlo en la red. Las primeras implementaciones experimentales de IPv6 estuvieron listas casi enseguida, en sistemas operativos como Linux, SunOS, Solaris, etc. Esto permitió probar IPv6 en la red de área local o usando estas máquinas como encaminadores (*routers*). Las implementaciones en equipos de red estándar usados por los ISPs (*Internet Service Providers*), tales como Cisco o Juniper tardaron más en llegar y pocos fueron los administradores de red que se atrevieron a poner este nuevo código *Beta* en sus equipos.

Por ello, y siguiendo el ejemplo del MBone en las pruebas iniciales de IPv4 *multicast*, se creó el 6Bone, una red virtual formada por túneles entre máquinas que transportaba IPv6 sobre la infraestructura de IPv4 existente.

Este paso permitió la familiarización de los ingenieros de red e implementadores más curiosos y atrevidos con el IPv6. Supuso un gran paso para el desarrollo de las tecnologías de infraestructura (red, servidores, etc.) pero no era una red para el gran público.

Con el ánimo de dar el paso a una Internet a gran escala, se decidió en 2002 empezar el camino para poner fin al 6Bone. En 2004 se aprobó por fin el RFC[3] que señalaba la fecha del 6/6/2006 como el fin de las operaciones del 6Bone (algunos se habrán dado cuenta de como la elección de la fecha era un síntoma de que se veía en ese momento al 6Bone ya no como una herramienta de ayuda al despliegue sino como un obstáculo). Al mismo tiempo, los RIRs (*Regional Internet Registries*), que habían estado al margen de la distribución de direcciones IPv6 en el 6Bone, se hacían con el control del espacio de direccionamiento de IPv6, empezando a distribuirlo como parte de sus operaciones normales, tal como hacen con IPv4, enfatizando así el mensaje de "*IPv6 está listo para su uso*" hacia el mundo entero.

3. Problemas en el despliegue de IPv6

Un poco antes de la desaparición del 6Bone, varios sistemas operativos destinados al gran público empezaron a incorporar soporte para comunicaciones utilizando IPv6. Así, Mac OS X incluye soporte para IPv6 desde la versión 10.3 (2003) y Windows Vista desde 2007 (XP tenia soporte opcional a nivel experimental). Linux dejó de considerar el código como experimental en 2005.

En esos momentos la recomendación del IETF era que para máquinas que dispusieran de acceso a la red tanto con IPv4 como con IPv6, el sistema operativo y las aplicaciones deberían intentar primero la conexión utilizando IPv6.

Mientras tanto, el acceso a Internet doméstico, debido a la creciente presión sobre los proveedores de Internet para economizar en el uso de direcciones públicas de IPv4 combinado con un aumento en el número de dispositivos con conexión a Internet en cada residencia, había dado lugar al despliegue masivo de *routers* (para ADSL o cable) con funcionalidades de NAT (*Network Address Translation*) que permiten conectar múltiples dispositivos utilizando una sola dirección IPv4. Estos dispositivos dan un servicio aceptable para la mayoría de los usuarios siempre y cuando los usuarios se dediquen principalmente a consumir información y

> “Dado el escaso acceso a IPv6, los proveedores de servicios tales como sitios web no veían incentivos para dedicar parte de su presupuesto a habilitar IPv6”

servicios, o sea ser clientes de los servicios de Internet proporcionados por otros.

En estos casos la conexión es iniciada por parte de un dispositivo directamente conectado al *router* y esto le permite tener información sobre a donde dirigir las respuestas que vienen del exterior (por ejemplo la página web solicitada por un usuario desde su portátil es enviada a éste y no al equipo de sobremesa, *tablet*, etc.). En los casos en que el usuario quiere ser el origen del servicio, por ejemplo en protocolos *peer-to-peer* como voz sobre IP (VoIP) o un pequeño servidor web en su casa, el *router* no lo puede saber, sin una configuración manual caso por caso por parte del usuario. Aunque se han ideado mecanismos que facilitan este tipo de configuraciones, como uPnP o NAT-PMP, estos suelen requerir que el equipo del usuario residencial sea el que indique al *router* los servicios que quiere mostrar al exterior y en cualquier caso siguen existiendo limitaciones.

Esto hacía imposible el despliegue de acceso a IPv6 en la mayoría de los casos ya que los proveedores de Internet, ISPs, aún hoy no cuentan en su mayoría con este acceso entre sus servicios.

Esta misma situación es la norma en el acceso a Internet para la mayoría de las empresas y organizaciones. Habitualmente la excepción a esta regla la ponen las redes académicas que, por lo general, llevan dando acceso *nativo* a IPv6 a todas las universidades y demás centros educativos y de investigación a los que dan servicio.

Dado el escaso acceso a IPv6, los proveedores de servicios tales como sitios web no veían incentivos para dedicar parte de su presupuesto a habilitar IPv6. Esta falta de servicios era a su vez utilizada por los ISP como justificación para no realizar el gasto que conlleva desplegar un nuevo servicio.

Para intentar romper esta situación de tablas e intentar hacer más fácil el acceso a IPv6 a los usuarios que querían pero que no podían obtenerlo a través de su ISP, el IETF y empresas como Microsoft crearon soluciones para crear túneles automáticamente, tales como 6to4 o TEREDO.

Estas soluciones de túneles automáticos han acabado siendo utilizadas por Apple en su servicio “*Back to My Mac*” y el equivalente de Microsoft.

Estos túneles han resultado tener algunas propiedades que, al incrementarse su uso automático por parte de un creciente número de usuarios, han causado algunos problemas[4]

4. *World IPv6 Day*

Llegados a este punto, con el final de la disponibilidad de nuevas direcciones de IPv4 acercándose vertiginosamente y esta vez sin ninguna nueva idea como CIDR para estirar la situación, algunos ingenieros empezaron a tomarse la situación más en serio y se iniciaron procesos para medir cual seria el impacto real en los servicios de ofrecer acceso via IPv6.

En Google este proceso comenzó como un proyecto “20%” por parte de Lorenzo Colitti al que rápidamente se unieron otros ingenieros como Erik Kline. Al investigar qué habría que hacer en la red y servicios de Google para activar IPv6 y realizar experimentos para medir el comportamiento de una muestra de clientes a los que se les daba acceso por IPv6 además de por IPv4, se toparon con un grave problema.

La combinación de todos los métodos descritos anteriormente (varios tipos de túneles automáticos, preferencia para IPv6, etc.) llevaba a que algunos clientes no pudieran jamás llegar a acceder a las páginas de Google. Se estimó que el 1% de los navegadores de Internet tendrían este problema, lo cuál supone una cantidad inaceptable de clientes perdidos como consecuencia de la habilitación de IPv6 por parte de Google (se estimó que algo similar pasaría en otros proveedores de servicio, como Yahoo, MSN, etc. y esto fue efectivamente confirmado por otros hallazgos más tarde).

Un 1% podría parecer un porcentaje pequeño a primera vista pero ninguna entidad comercial está dispuesta a perder el 1% de sus clientes por la introducción de una nueva tecnología que no sólo no va a suponer ingresos adicionales inmediatamente sino que además conlleva un gasto.

En Google, y después en otros servicios, la opción más a mano fue recurrir al *white-listing*, la creación de una lista de ISPs y redes que, bajo petición previa, pudieran demostrar que su soporte de IPv6 era correcto y que además se comprometieran a apoyar a cualquier usuario de su red que tuviera problemas.

Esta situación se prolongó durante un cierto tiempo pero pronto se vio que este tipo de soluciones no es eficaz a la hora de apoyar un crecimiento significativo. Sin embargo, ningún proveedor estaba dispuesto a dar el primer paso hacia un servicio comercial, no experimental, si eso implicaba una pérdida de clientes hacia proveedores que no dieran ese primer paso.

La solución final provino de nuevo de una iniciativa de Google y era una idea simple. Ya que nadie quiere ir primero, elíjase un día en el que todos activen IPv6 a la vez, evitando así movimientos de transferencia de clientes, proporcionando información a los usuarios que pudieran tener problemas, dando relevancia mediática al evento, y consiguiendo así que IPv6 esté presente en la mente de todos y se pueda obtener información real del verdadero impacto a escala de todo Internet. La duración de esta prueba sería de 24 horas.

Así nació la idea de lo que se llamó el *World IPv6 Day*. La fecha para esta prueba a escala de Internet quedó fijada para el día 8 de junio de 2011 (se estimó que el 6, al ser lunes no daría una vista representativa a escala global).

Para hacer del evento algo efectivo, hacía falta la participación del mayor número de servicios posible. Al anunciar la fecha con una anticipación de casi un año fue posible sumar a la iniciativa a un número importante de participantes. Así, dado que gran parte de las webs de mayor tráfico están alojadas en CDNs (*Content Delivery Networks*, o redes de distribución de contenidos), la participación de Akamai y Limelight contribuyó de manera significativa al aumento de la oferta de contenidos disponibles en IPv6. Asimismo, se sumaron algunos ISPs con pilotos de despliegue IPv6.

El evento se anunció de forma pública varios meses antes de la fecha elegida y eso permitió llevar a cabo no solamente trabajos de difusión sino también trabajos de formación, desarrollo e implementación (tanto a nivel de oferta de servicio como de versiones de código para equipos) lo cual tuvo un gran impacto en la mejora de la situación del acceso a IPv6 durante el *IPv6 World Day*.

Aún así, fueron pocos los ISPs de acceso que se sumaron a este evento de forma significativa. Un análisis del tráfico observado

> “Con el *IPv6 Launch Day* ha quedado patente que toda la infraestructura necesaria se encuentra ya a disposición de los usuarios y los proveedores”

durante el periodo de 24 horas indica que la mayoría del tráfico IPv6 nativo observado provenía de redes académicas y similares que tenían IPv6 habilitado desde hacía tiempo.

Una importante consecuencia de todo el trabajo de preparación fue el notable descenso en el número relativo de problemas para acceder a los servicios sobre IPv6. Esto se debió tanto a la preparación de los proveedores de contenido como a las mejoras llevadas a cabo en los sistemas operativos de fabricantes como Apple o Microsoft, que al ver como IPv6 iba a pasar de ser una nota al margen a un servicio en uso real tomaron iniciativas para mejorar el comportamiento de sus sistemas. Un claro ejemplo de esto fue el proyecto de Happy Eyeballs[5] en el que se analizó y mejoró el comportamiento del sistema operativo y algunas aplicaciones, principalmente navegadores web, para que los usuarios tuvieran una mejor experiencia al navegar en presencia de más de una forma de acceso a Internet, como es el caso de cuando se tiene habilitado tanto IPv4 como IPv6.

El *World IPv6 Day* fue justamente considerado un éxito por todos los participantes y supuso un gran avance en el uso real de IPv6 como tecnología básica de Internet y alternativa al IPv4. Aunque sólo unos pocos servicios mantuvieron el transporte sobre IPv6 una vez pasadas las 24 horas del evento, los demás iniciaron estudios sobre los datos recopilados durante este periodo con vistas a habilitar el transporte IPv6 de forma permanente en fechas posteriores.

5. *IPv6 Launch Day*

El *IPv6 World Day* fue considerado un éxito por todos los participantes ya que demostró que no se produciría ningún cataclismo en Internet. El sólo hecho de que se determinara una fecha fija y se le diera una gran visibilidad al evento hizo que los meses previos supusieran uno de los periodos de mayor avance en cuánto a la disponibilidad efectiva de IPv6 en Internet. No obstante, se hizo también patente que ciertas áreas, no todas tecnológicas como pueden ser los centros de atención a clientes etc., necesitaban más tiempo para poder habilitar el servicio IPv6 de forma permanente.

Con el fin de que todo el esfuerzo anterior no cayera en saco roto y lanzar definitivamente el uso de IPv6 en Internet en igualdad de condiciones que el servicio IPv4, se pensó en repetir el *IPv6 World Day* un año después, el 6 de junio de 2012, pero con el compromiso de que esta vez los participantes dejarían el acceso a IPv6 activado pasada la fecha elegida. De ahí que el lema elegido para este día fuera “*This time it is for real*”.[6]

Con respecto al evento de 2011, una de las diferencias notables fue el incremento en participación por parte de los proveedores de acceso para usuarios. Proveedores como Comcast o Time Warner Cable trabajaron durante el periodo entre eventos para actualizar toda su infraestructura de forma que se diera la posibilidad de acceso a Internet con IPv6 a alrededor del 70% de sus usuarios. Naturalmente el uso efectivo fue bastante menor ya que el hacerlo posible no implica directamente que se vaya a hacer uso de ello. Por ejemplo, la edad media del parque de ordenadores domésticos en EEUU implica que alrededor del 50% de los usuarios domésticos utiliza todavía sistemas operativos que no tienen soporte para IPv6 por ser demasiado antiguos (Windows XP, por ejemplo). De los que tienen equipos suficientemente recientes sólo aquellos con *routers* domésticos capaces de entender IPv6, o en el caso del acceso por cable los directamente conectados al modem de la operadora, pueden hacer uso de esta posibilidad.

Precisamente uno de los avances que tuvo lugar con vistas al *IPv6 Launch Day* fue la participación directa de un número de fabricantes de *routers* domésticos que pusieron a disposición de sus clientes equipos nuevos o versiones de *firmware* nuevas que implementan IPv6.

Los resultados del *IPv6 Launch Day* señalaron un incremento muy notable del tráfico que usa IPv6 para acceder a los servicios en red. Aunque el total sigue siendo un pequeño porcentaje, alrededor del 1%, medidas llevadas a cabo desde junio indican un crecimiento del tráfico de IPv6 superior en más de dos veces al crecimiento del tráfico en IPv4. Esto lleva a extrapolar que en unos 5 años IPv6 podría representar alrededor del 50% del tráfico de Internet.

Por supuesto, hay todavía grandes variaciones en los niveles de tráfico observados en diferentes países pero se espera que con más o menos retraso la tendencia vaya a ser la misma a nivel mundial.

Con el *IPv6 Launch Day* ha quedado patente que toda la infraestructura necesaria se encuentra ya a disposición de los usuarios y los proveedores y que continuando con la voluntad de despliegue pronto podremos contar con IPv6 para seguir haciendo crecer la Red.

Tal como se discutió en el panel organizado por ISOC durante el IETF84 todavía no se ha llegado a un punto en el que se pueda decir que un usuario que sólo tuviera acceso a IPv6 podría considerar que está conectado a la totalidad de Internet, pero sí ha quedado patente que las barreras técnicas son ahora asumibles y que se pueden establecer e implementar modelos de negocio que hagan de IPv6 la nueva base de Internet como forma de sostener el crecimiento.

Internet necesita del nuevo espacio de direccionamiento que proporciona IPv6 ya que de lo contrario, habiéndose agotado ya el espacio de direcciones libre para el crecimiento en las regiones Europea y de Asia Pacífico, el crecimiento de servicios en Internet en el cual se basa una cada vez mayor parte de la economía se hará progresivamente más difícil si los proveedores de servicio (ISPs) empiezan a verse obligados a recurrir a técnicas como NAT444/Carrier Grade NAT que enmascaran el acceso a Internet de los usuarios detrás de gigantescos traductores que impiden la comunicación directa entre dispositivos finales, lo cual ha sido sin duda el factor primordial que ha hecho de Internet lo que es hoy.

Notas

[1] **V. Fuller, T. Li, J. Yu, K. Varadhan.** *RFC 1338, Supernetting: an Address Assignment and Aggregation Strategy*, 1992.
[2] **V. Fuller, T. Li, J. Yu, K. Varadhan.** *RFC 1519, Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*, 1993.
[3] **R. Fink, R. Hinden.** *RFC 3701. 6bone (IPv6 Testing Address Allocation) Phaseout*, 2004.
[4] **G. Huston.** *Flailing IPv6*. <http://www.potaroo.net/ispcol/2010-12/6to4fail.html>, 2010.
[5] *Eyeballs*, o “globos oculares”, es un término empleado frecuentemente en ingeniería de Internet para referirse a los usuarios finales que interaccionan con Internet en gran medida mirando a las pantallas de sus ordenadores para navegar la web.
[6] <http://www.worldipv6launch.org>.

Carlos Ralli Ucendo
Telefónica I+D

<ralli@tid.es>

Internet6: Impacto en los productos y servicios digitales

Resumen: *A día de hoy el despliegue de IPv6 en el mundo de los contenidos es ya un hecho y comienzan además a ser accesibles para millones de usuarios, que están conectándose de la mano de operadores en todo el planeta, pero especialmente en Norteamérica. Sin embargo, muchos arquitectos y desarrolladores de productos digitales y servicios de Internet no conocen cómo esto va a cambiar su entorno de negocio creando nuevas oportunidades y riesgos. El presente artículo trata de explicar los principios generales de este cambio relevante en el ecosistema Internet y, a través de dos casos de estudio concreto (VoIP e IoT), establecer una metodología de análisis para evaluar cómo va a influir la aparición paulatina de la Internet6, una Internet paralela distinta, donde podrán ofrecer sus servicios en un futuro a los usuarios de la Internet tal y como la conocemos hoy.*

Palabras clave: *Aplicaciones, arquitectos de software, innovación, IoT, IPv6, modelos de negocio de Internet, M2M, productos digitales, servicios digitales, software developers, VoIP, 6LowPAN.*

Autor

Carlos Ralli Ucendo es Ingeniero Superior de Telecomunicaciones por la Universidad Politécnica de Madrid. En 1999 realizó la primera conexión a las redes IPv6 de dicha universidad y los laboratorios de Telefónica I+D. Tras liderar Euro6IX (2002-2005), el mayor proyecto IPv6 de operadoras cofinanciado por la UE, ha sido coordinador técnico de la participación de Telefónica en las recientes jornadas mundiales de IPv6. Ha participado en análisis de riesgos in-situ de las redes de Telefónica en Brasil, Chile y Colombia y cuenta con una amplia experiencia en proyectos de innovación, asistiendo regularmente a la Comisión Europea como experto independiente en las auditorías técnicas de proyectos cofinanciados. Es ponente activo, con más de medio centenar de ponencias técnicas, presentaciones relevantes y demostraciones en Asia-Pacífico, Europa y Latinoamérica. Durante el año 2011 desempeñó el papel de jefe de delegación para *Internet Society* (ISOC) y el IETF. Actualmente, forma parte del equipo de desarrollo de la plataforma de servicios de "*Future Internet*" FI-WARE (@Fiware) y está abriendo una línea de investigación centrada en las oportunidades e impacto de la llegada masiva de IPv6 en productos y servicios de Internet.

1. Internet6: Un nuevo hábitat clave en el futuro del ecosistema de servicios

Desde un punto de vista pragmático, Internet se ha convertido en la plaza virtual donde tienen lugar la mayor parte de las comunicaciones personales y sociales, así como el intercambio de información, contenidos digitales, bienes físicos y servicios.

Desde este punto de vista, Internet es el hábitat de un ecosistema de servicios, implementados por productos digitales, que compiten entre sí por unos recursos limitados: los usuarios o clientes.

El sistema evoluciona a un ritmo frenético, debido a la incesante aparición de variaciones de los servicios y a la selección producida por las elecciones de los usuarios. El propio hábitat también varía, aunque lo hace a un ritmo mucho menor que estos debido a su complejidad, pero con gran impacto en el futuro del ecosistema.

Variaciones de este hábitat son, por ejemplo, la superación de un tamaño crítico, ya que al llegar Internet a la mayor parte de nuestros conocidos cobraron mucho más sentido las comunicaciones personales y sociales. Otro ejemplo, es la extensión de Internet al entorno móvil, de la mano de los *smartphones*, transformando algunos servicios existentes y dando lugar a otros nuevos que sólo tienen sentido en movilidad.

Nuestra visión, que intentamos mostrar en este artículo es que la adopción masiva de la Internet6, por parte de servicios y usuarios, es un cambio fundamental del ecosistema que está ocurriendo ya y por tanto es importante que los arquitectos y desarrolladores de productos y servicios digitales se involucren cuanto antes.

Para entender por qué Internet6 es un hábitat distinto del actual hay que conocer que los paquetes IPv4 e IPv6 son como el agua y el aceite, no se mezclan, y por lo tanto dan lugar a dos flujos distintos, aunque sea en las mismas cañerías, creando dos Internet paralelas.

Por lo tanto, no sirve de nada actualizar los equipos y software a IPv6, si no nos conectamos a este circuito nuevo con paquetes IPv6 que es la Internet6 (ver **figura 1**).

Es imprescindible conectarse a esta nueva Internet, para descubrir y experimentar cómo este hábitat elimina algunas barreras e introduce nuevos retos, algunos de los cuales explicamos más adelante.

Se podría argumentar que en realidad existen mecanismos de traducción que nos pueden conectar a ambos dominios desde uno de ellos, pero lo cierto es que introducen los mismos problemas y limitaciones que esta evolución pretende eliminar, por lo que en este artículo solo consideramos el escenario de conexión nativa a Internet6.

Para concluir esta visión evolutiva, recordamos que para Darwin no eran las especies más fuertes, ni las más rápidas o inteligentes las que sobrevivían, sino aquellas que mejor se adaptaban a su entorno y a los cambios del mismo.

Por lo tanto, aquellos que conquisten y se adapten primero a la Internet6 serán los que tengan más posibilidades de supervivencia y éxito ante este cambio.

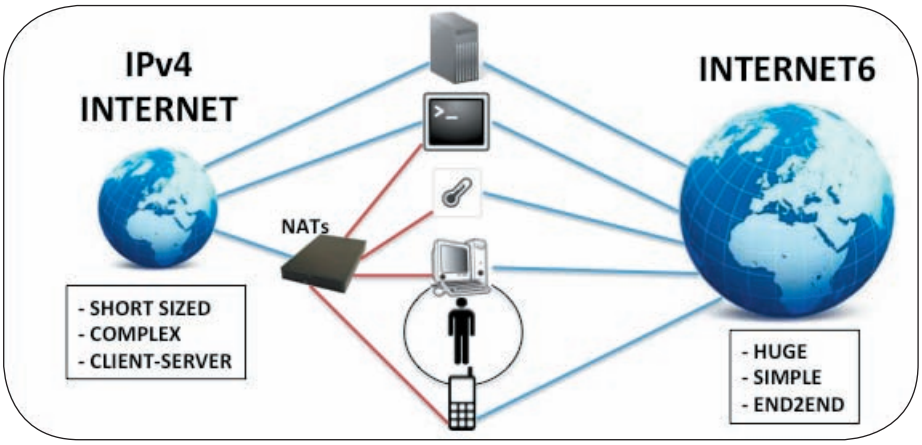


Figura 1. Internet 6: Un nuevo circuito de paquetes IPv6.

> “Para entender por qué Internet6 es un hábitat distinto del actual hay que conocer que los paquetes IPv4 e IPv6 son como el agua y el aceite, no se mezclan”

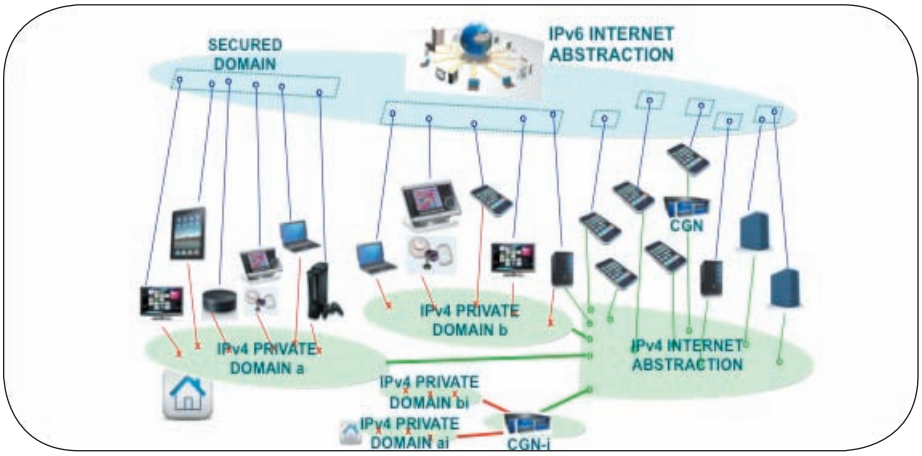


Figura 2. Modelo del funcionamiento actual de Internet.

2. Fases y modelo del nuevo escenario

Las fases y complejidad de la puesta en marcha de la Internet6 se describen a continuación:

- En primer lugar, a finales de los años 90, el IETF (*Internet Engineering Task Force*, organismo que especifica los protocolos de Internet) identificó problemas de escalabilidad por lo que realizó una selección de propuestas para una Internet de nueva generación en la que IPv6 resultó seleccionada.
- En la siguiente década se realizaron las implementaciones en equipos de red, sistemas operativos y redes experimentales.
- En esta década recién comenzada el agotamiento de direcciones y el impulso de *Internet Society* (ISOC) y de gigantes de Internet como Google y Facebook han dado el pistoletazo de salida de la adopción masiva:
  - En junio de 2011, los gigantes de los contenidos hicieron una prueba de adopción en la que sus contenidos se ofrecieron en ambas Internets durante 24 horas.
  - En junio de 2012, el 24% de los contenidos más accedidos a nivel mundial optó por habitar en ambas Internets de forma permanente.
  - Adicionalmente, importantes ISP (*Internet Service Providers*), principalmente norteamericanos y de otras regiones en menor medida, han comenzado una adopción masiva introduciendo millones usuarios nativos en la Internet6.
- Curiosamente, superando cualquier previsión anterior, han empezado a aparecer algunos ISP que han decidido que sus usuarios sólo habiten la Internet6 de forma nativa y tengan un acceso traducido (NAT64) a la Internet tradicional, puesto que en IPv4 los traductores ya son un inconveniente existente. Nacen así los usuarios *IPv6-only*, eso sí por el momento no hay una servicios *IPv6-only* destacados, pero no tardarán en aparecer, cuando las ventajas aportadas superen claramente el inconveniente de que parte de los usuarios no pueda acceder a las mismas.

El modelo actual es muy complejo, los usuarios y servicios que están conectados en la Internet-IPv4 (parte inferior de la **figura 2**) están comenzando a conectarse simultáneamente a la nueva Internet6 (parte superior).

La primera diferencia que observamos en el diagrama es que la Internet4 está fragmentada en dominios privados. Esto se debe a que no hay direcciones públicas únicas para identificar todos los elementos y, por tanto, se numeran con direcciones privadas que se repiten en todos ellos y se conectan a Internet a través de unos elementos traductores de direcciones IP (NAT), que disponen de una o unas pocas direcciones públicas.

Es decir, en realidad los elementos no están conectados a Internet, sino que hay un elemento intermedio que los conecta. Así, por ejemplo, los PCs, tabletas y *smartphones* que utilizan la conexión de nuestro hogar no están realmente presentes en Internet, sino que están intermediados por un NAT instalado en el *router* ADSL, de cable o fibra.

El gran inconveniente de estos dominios privados, típicos en las redes de hogar pero también en redes corporativas y redes móviles (*smartphones*), es que han provocado que la Internet se reduzca a una arquitectura cliente-servidor, que permite servicios centralizados pero dificulta en extremo servicios distribuidos.

Esto es así porque los nodos finales están ocultos rompiendo la conectividad extremo-a-extremo que tanto éxito otorgó a Internet en sus primeros tiempos. Prestar servicios desde nodos privados es muy complicado. No obstante los servidores que prestan servicios masivos están ubicados en la Internet pública, aunque cada vez hay menos espacio para los mismos (direcciones IP).

Además de que prestar servicios desde estos nodos es complicado, el hecho de estar ocultos también interpone una gran barrera para el desarrollo de servicios interactivos y comunicaciones personales en tiempo real, como veremos en el primer caso de estudio de este artículo.

Superar estas barreras ha precisado costosos procesos de definición, estandarización e implementación de tecnologías que aun así siguen presentando dificultades por su coste, complejidad y discutible escalabilidad. Algunos ejemplos son: *NAT-Traversal*, COMET (*long polling*) y los *websockets* actuales, implementados en los navegadores.

Un problema adicional es que los dominios privados tienen también una limitación en el número máximo de direcciones distintas (determinado por la clase A de direcciones IPv4 privadas 10.x.y.z) y, por tanto, para redes con muchos nodos usuarios (distribución de vídeo en un operador, comunicaciones máquina a máquina o M2M) los dominios privados necesitan sub-fragmentarse incrementando la complejidad.

Sin embargo, como puede apreciarse en la **figura 2**, la Internet6 conecta a todos los elementos por igual y por tanto elimina las barreras ya que los elementos están conectados directamente sin intermediarios como los NATs o *proxies*.

Decimos que la Internet6 recupera la conectividad extremo-a-extremo (*end-to-end* ó *end2end*) lo que va a reducir radicalmente las barreras para la innovación y desarrollo de nuevos servicios interactivos, en un escenario más parecido a los orígenes de Internet.

Desde el punto de vista de seguridad los nodos finales no tienen por qué exponerse indefensos en Internet pues existen elementos intermedios o locales (*firewalls*) que filtran total o selectivamente y estática o dinámicamente los puertos de servicio de los mismos. No obstante, el modelo de seguridad cambia y es necesario sumergirse en él.

En resumen, la ausencia de conectividad extremo-a-extremo es capital, puesto que:

- Reduce la innovación en servicios: ya que hay que ceñirse a las limitaciones del modelo cliente-servidor o afrontar una barrera de entrada muy alta desarrollando tecnologías alternativas.
- Incrementa los tiempos de desarrollo (*time2market*) y los costes de despliegue (CAPEX): puesto que hay que diseñar, desarrollar e incluso estandarizar tecnologías que permitan comunicaciones bidireccionales.
- Incrementa los costes de operación (OPEX): porque hay una mayor complejidad y/o nuevos elementos lo que incrementa las posibilidades de fallos y la dificulta en su resolución.

Un riesgo importante para un proveedor de servicios sobre Internet es que sus competidores encuentren y exploten una ventaja competitiva para sus usuarios IPv6 posicionándose claramente en una nueva funcionalidad o servicio.

> “La Internet6 recupera la conectividad extremo-a-extremo lo que va a reducir radicalmente las barreras para la innovación y desarrollo de nuevos servicios interactivos”

3. Estudio del impacto de Internet6 en productos y servicios concretos

Estudiar detalladamente cada uno de los tipos de servicios actuales precisaría seguramente escribir un extenso artículo individual para cada uno de ellos.

Por este motivo, se ha optado por presentar dos casos de estudio relevantes a día de hoy: las comunicaciones personales de voz (VoIP) y las aplicaciones máquina-a-máquina (M2M), también llamadas Internet de las cosas (*Internet of Things*, IoT).

Además de adaptaciones de éstos y otros servicios actuales, este nuevo hábitat hará posibles nuevos paradigmas de servicios impensables con las limitaciones actuales.

Predecir estas evoluciones disruptivas sobre el papel es normalmente un ejercicio complejo y poco efectivo. No obstante, surgirán naturalmente a partir de la creatividad e interacción de todos los actores cuando el hábitat sea ampliamente explotado.

Por lo tanto, como metodología para los arquitectos y desarrolladores de productos y servicios actuales se propone re-diseñar los servicios actuales para la Internet6, poniendo las ideas en práctica cuanto antes para hacer una evaluación correcta de oportunidades y riesgos.

3.1. Caso de Estudio 1: Las comunicaciones personales de voz (VoIP)

El caso de éxito de las conversaciones de voz sobre Internet es sin duda la archiconocida aplicación Skype, desarrollada por un pequeño grupo de estonios en el año 2003.

Skype alcanzó tal relevancia que fue comprada primero por e-Bay y más tarde por Microsoft en el año 2011, por más de 8,5 billones de dólares, cuando ya contaba con más de 600 millones de usuarios.

Pero, ¿cómo surgió esta aplicación y se posicionó frente a sus competidores?

En esta sección, veremos cómo los creadores de Skype[2] comprendieron y convirtieron las barreras de la Internet-IPv4 en su aliado frente a sus competidores y, al mismo tiempo, entenderemos la dificultad y costes de dichas barreras y por qué Internet6 las elimina.

Las aplicaciones de comunicaciones personales y, en particular las comunicaciones de voz, son en esencia entornos extremo-a-extremo (*end-to-end*, e2e, *peer-to-peer* o P2P), puesto que en definitiva suponen establecer una comunicación entre dos usuarios finales para mensajería, voz, vídeo o transferencia de ficheros en tiempo real.

Sin embargo, la arquitectura cliente-servidor de Internet dificulta enormemente las comunicaciones P2P, puesto que muchos usuarios están ocultos en dominios privados y sólo pueden iniciar conexiones, no recibirlas.

Debido a esto, la mayor parte de aplicaciones VoIP eran centralizadas, es decir requerían una inversión notable en servidores intermedios, escalaban con mucha dificultad y eran propensas a fallos.

Los desarrolladores de Skype contaban en cambio con una ventaja competitiva que hicieron valer: conocían y habían experimentado extremadamente bien cómo superar la barrera de entrada para crear entornos P2P, puesto que ya en 2001 habían desarrollado la famosa aplicación Kazaa para el intercambio P2P de ficheros.

Skype emplea técnicas P2P para dos funciones muy importantes: la ubicación de los usuarios y las comunicaciones a y desde redes privadas (*NAT-Traversal*).

Los nodos de Skype están organizados en una red jerárquica superpuesta en la que cada elemento se clasifica en nodos, supernodos y retransmisores (*relays*):

- Nodos: Son los clientes corrientes que emplean los usuarios.
- Supernodos: Son clientes de Skype que están en nodos con dirección IP pública. Almacenan de forma distribuida unas tablas con la información de los usuarios, concretamente un índice a modo de identificador de usuario (asociado al nombre de usuario) y su dirección pública IP y puertos.
- El protocolo de Skype es propietario, por tanto no se conoce cómo están organizadas las asignaciones de índices, aunque es probable que sea similar al de la red Bittorrent con DHT.
- Retransmisores o *relays*: Son un tipo especial de supernodos que permiten cursar comunicaciones a través de los mismos, conectando usuarios inaccesibles por otros medios.

Cuando un usuario arranca Skype, el nodo abre puertos TCP y UDP no estándar (superiores a 1024) y aleatorios para descubrir el tipo de conectividad de red.

Un cliente de Skype precisa conectividad TCP para la señalización y UDP para la transmisión de medios (voz, vídeo o ficheros). Si UDP no está disponible se utiliza TCP aunque es mucho menos eficiente e introduce retardos apreciables debido a las retransmisiones que emplea para garantizar la entrega de todos los mensajes.

Antes de que ocurra cualquier tipo de comunicación, por ejemplo una llamada, el cliente arrancado por el usuario se comunica con la red P2P, es decir con un supernodo. En esta fase, se realiza el proceso de registro, se obtiene el estado de los contactos y se hacen pruebas para descubrir el tipo de conectividad de red. Así, por ejemplo, se verifica si se pueden establecer conexiones UDP salientes, si el usuario está detrás de un NAT y los estándares P2P soportados por este último en caso de existir.

En un escenario ideal donde los clientes están en nodos con direcciones IP públicas, cuando un usuario A lanza una llamada VoIP al usuario B, se hace una búsqueda en la tabla de índices de los supernodos, de tal manera que se obtiene la dirección IP y puerto del usuario B y la comunicación se establece directamente, ya que (tanto A como B) pueden establecer sesiones entrantes y salientes.

Sin embargo, la mayor parte de los usuarios acceden desde terminales en redes domésticas o corporativas con direccionamiento IP privado y conectadas a través de un NAT (traductor de direcciones a Internet). También, muchos proveedores de Internet móvil asignan direcciones privadas a los *smartphones*.

Establecer comunicaciones con usuarios conectados a Internet detrás de NATs y *firewalls* es un reto realmente complicado, ya que el NAT cambia la dirección privada del usuario por otra pública, haciendo que los usuarios no sean fáciles de encontrar y no se puedan establecer conexiones entrantes desde Internet hacia el usuario.

Para resolver este problema, Skype es muy robusto, ya que ofrece tres alternativas, ordenadas de mejor a peor, que se verifican consecutivamente:

1) NAT-traversal nativo en los *NAT/Firewall*, que introduce el menor retardo en las comunicaciones.
2) Servidor *proxy* SOCKS5 ó HTTPS, siendo el mejor el primero puesto que utiliza UDP y por tanto introduce menor retardo.
3) Retransmisores (*relays*) TCP/UDP, que funcionan prácticamente en todas las ocasiones pero introducen mayores retardos, especialmente los retransmisores TCP.

3.1.1. *NAT-traversal* nativo en el *NAT/Firewall*

Skype es capaz de atravesar la mayor parte de los NAT y *firewalls* que soportan la técnica "*UDP hole punching*", definida en los estándares de IETF, entre ellos "RFC 5389 - *Session Traversal Utilities for NAT* (STUN)"[2]. Se calcula que el soporte es de alrededor del 80% de los NATs desplegados actualmente.

Mediante esta técnica, los usuarios que no pueden comunicarse directamente pueden enviar sus parámetros de red (IP y puerto origen del NAT) a través de otros nodos (*relays*) y así tratar de iniciar una conexión IP directa.

El proceso completo es el siguiente:

1) Cuando un usuario A lanza el cliente de Skype se abre una sesión TCP de señalización con un supernodo S_a. En paralelo, se realizan pruebas para determinar la conectividad con el servidor STUN del supernodo[3].
2) En las tablas de ubicación de usuarios distribuidas en los supernodos, el usuario A aparece en realidad ubicado en la dirección IP pública y puerto empleados por el NAT_a. Cuando el usuario A quiere abrir una comunicación, por ejemplo una llamada, con el usuario B que está también detrás de un NAT_b, los supernodos indican a cada cliente que abran conexiones UDP directas contra los NATs (IP pública, puerto) del otro cliente.
3) Al principio, los paquetes que envía A a NAT_b y viceversa (B a NAT_a) son descartados por los NAT puesto que los puertos entrantes no están abiertos. Sin embargo, al cabo de un tiempo, los NATs que cumplen estos estándares son capaces de identificar la otra conexión simétrica y, abrir el puerto entrante correspondiente que se conecta con el cliente final correspondiente.

Veámoslo en detalle:

- Los clientes A (IP_a, $Puerto_a$) y B (IP_b, $Puerto_b$) con direcciones privadas están detrás de sendos NAT: NAT_a (IP_x, $Puerto_x$) y NAT_b (IP_y, $Puerto_y$).
- Los supernodos indican: que A abra una conexión directamente con NAT_b, al que llegarán paquetes de (IP_x, $Puerto_x$) hacia (IP_y, $Puerto_y$). Como NAT_b, está utilizando $Puerto_y$ únicamente como salida y no como entrada, tirará estos paquetes entrantes.
- Sin embargo, al cabo de un tiempo, NAT_b se da cuenta de que además está cursando los paquetes de B a NAT_a, es decir, de (IP_b, $Puerto_b$) a (IP_x, $Puerto_x$) con lo que concluye que B es objeto de una comunicación bidireccional a través de NAT_b y NAT_a. Por tanto, decide abrir $Puerto_y$ como entrante y conectarlo con el $Puerto_b$ de B.
- Una vez abierto este "agujero" de entrada en el NAT (de ahí el nombre "*UDP hole punching*"), los paquetes de A llegan a B.
- Simétricamente, NAT_a realiza un proceso similar, por el cual los paquetes de B llegan a A.
- Para mantener los agujeros abiertos en los NATs es necesario refrescar las sesiones enviando paquetes de forma periódica (mensajes *keep-alive*), aunque no haya información a enviar de la comunicación (silencios en el caso de la llamada).

Para que se pueda emplear este mecanismo, los NATs deben cumplir con el estándar de IETF "*RFC 4787 - NAT Behavioral Requirements*". Concretamente, deben soportar:

- El mapeo de, al menos, unas 100 conexiones por usuario.
- Asignar siempre la misma IP pública para las comunicaciones de una misma dirección privada interna,
- Asignar los puertos de forma consistente mapeando de la misma manera todos los paquetes enviados desde un par dirección y puerto interno a otro externo (*endpoint-independent mapping*)
- Permitir que dos nodos internos se comuniquen entre sí a través de una dirección IP pública externa (*hairpinning*).

3.1.2. Servidores *proxy* SOCKS5 o HTTPs

Este mecanismo se emplea normalmente en redes corporativas de gran tamaño, en las que las que los NAT no cumplen los requisitos para permitir el mecanismo descrito en el punto anterior. Esto puede ocurrir por su diseño, escalabilidad o una política de seguridad concreta de la organización, como por ejemplo, no permitir el uso de los puertos TCP/UDP no estándar (superiores a 1024).

Estas organizaciones cuentan con una alternativa con mejores prestaciones que el mecanismo por defecto descrito en la sección siguiente, que consiste en configurar uno de estos *proxies* para que retransmitan el tráfico de los usuarios de Skype dentro de dicha organización. De hecho, una posibilidad es configurar estos *proxies* como *back-up* principal para alcanzar redes externas para cualquier aplicación, no solo Skype.

Normalmente se prefiere el uso de un *proxy* SOCKS5, dado que soporta UDP, además de TCP, y por tanto introduce menos retardos que los *proxies* HTTPs, que únicamente permiten conectar con clientes remotos a través del puerto TCP 443.

3.1.3. Uso de retransmisores UDP ó TCP

Si no se puede aplicar ninguno de los dos mecanismos anteriores se recurre a éste, en el cual se emplean supernodos y otro tipo de supernodos denominados retransmisores o *relays*.

El mecanismo de registro de usuarios es el siguiente:

1) Para las comunicaciones del un usuario A, se asigna un supernodo S_a que, por definición, tiene dirección pública en Internet.
2) A inicia sesión con S_a, lo cual no supone un problema puesto que es una conexión saliente a través del NAT_a. Por tanto, A puede intercambiar datos con S_a a través de esta conexión, que se mantiene de forma permanente.
3) En las tablas distribuidas de Skype en los supernodos para ubicar usuarios se almacena la dirección IP pública del supernodo S_a, en lugar de la dirección de A, que es privada y por tanto no aporta información.
4) Si B está en una red privada también, como suele suceder, se repiten los pasos (1), (2) y (3) con B, de tal manera que éste puede comunicarse con otro supernodo, S_b.

De esta manera, ambos nodos mantienen sesiones permanentes con sus respectivos supernodos, cuya dirección pública se usa para localizar al cliente de cada usuario. Además, a través de estas sesiones los clientes de los usuarios pueden enviar y recibir información a la red P2P.

Los pasos para la consecución de una llamada son:

5) Cuando A quiere llamar a B, se lo comunica a su supernodo S_a, que busca en las tablas de

> “Skype emplea técnicas P2P para dos funciones muy importantes: la ubicación de los usuarios y las comunicaciones a y desde redes privadas (*NAT-Traversal*)”

usuarios y encuentra la dirección pública S_b. Cuando S_b recibe la petición se la manda a B, con el que está en comunicación permanente.
6) Cuando B recibe la llamada decide si aceptarla o no. Si acepta la comunicación, informa a S_b, que lo transmite a S_a.
7) En este punto, S_a y S_b determinan un tercer supernodo R, también en la Internet pública, que actuará como retransmisor (*relay*) de las comunicaciones. Por tanto, S_a y S_b comunican a A y B, respectivamente, que inicien una nueva sesión con R.
8) Ambos usuarios A y B abren sendas sesiones con el retransmisor R, lo cual de nuevo no es un problema al ser conexiones salientes. Sobre estas sesiones se establece la llamada a cuyo término se liberan finalmente.

Gracias a este mecanismo particular de Skype, las comunicaciones funcionan prácticamente siempre puesto que, si fallan los métodos anteriores, en este no es necesario un NAT o *proxy* con soporte específico ni abrir puertos en el *router* manualmente o dinámicamente con UPnP.

3.1.4. Caso de estudio VoIP: Conclusiones

De todo lo anterior, concluimos que para aplicaciones de este tipo la Internet4 supone una gran barrera en lo que se refiere al tiempo de desarrollo (*time-to-market*) y mayores costes de despliegue (CAPEX) y operación (OPEX), debido a la complejidad que suponen mayores costes aprendizaje y propensión a fallos.

Esta barrera no solo es perjudicial para el que crea y opera estos servicios sino para los usuarios puesto que reduce considerablemente la aparición de más competidores y de mejoras e innovaciones.

En la Internet6 una aplicación como Skype sólo manejaría el escenario de conectividad directa y quizá la apertura dinámica de puertos de *firewalls*, reduciendo enormemente la barrera para su desarrollo y mejoras, sus costes y su tiempo a mercado.

Finalmente, quedan una serie de preguntas abiertas que serían objeto de análisis más allá de este artículo:

- Cómo podría hacerse un servicio VoIP en el escenario de transición?
- Merece la pena afrontar la transición o es mejor diseñar un servicio *IPv6-only*?
- Qué puede aportar la Internet6 de cara a los servicios actuales de VoIP en *smartphones* que están empezando a desbancar a Skype, como Viber, Line, etc.

3.2. Caso de estudio 2: La Internet de las cosas (IoT)

La evolución de Internet no deja de sorprendernos, en origen interconectaba sólo investigadores y centros de I+D civiles y militares, y hoy en día es el principal medio de comunicación telemática para todo tipo de ciudadanos a nivel mundial.

Hoy en día un paradigma nuevo está cobrando una tracción importante, la Internet de las cosas (*Internet-of-Things* o IoT), que pretende que millones de objetos electrónicos estén presentes en Internet.

Los servicios M2M (*machine-to-machine*) existen desde hace un tiempo y actualmente gozan de cierta explosión mediática y de despliegue, que ha traído consigo los paradigmas de hogar inteligente, coche conectado y las ciudades inteligentes (*smartcities*).

En este punto es importante introducir un matiz importante, la mayoría de las propuestas y soluciones actuales conectan a los dispositivos (ya sean sensores o actuadores) mediante plataformas intermedias que son las que realmente están conectadas a Internet.

Los dispositivos se comunican con la plataforma con protocolos no-IP por lo que no podemos decir que realmente sean parte de Internet, si bien es cierto que están accesibles en la manera que establezca la plataforma que puede ser además configurable. Sin embargo, existe otro paradigma que consiste en que los dispositivos sean realmente parte de Internet y alberguen una pequeña aplicación (actualizable) que se comunique con una o varias plataformas, otros dispositivos, *smartphones*, centros de control, etc.

Ambas aproximaciones son válidas y en estos momentos no es posible saber cuál será la cuota del mercado mundial de M2M para cada una, si bien las soluciones no-IP se han desplegado anteriormente y por tanto gozan de cierta ventaja. Sin embargo, para ciertas aplicaciones complejas es ciertamente probable que las redes de sensores y actuadores IP acaben siendo predominantes.

En este caso de estudio nos centramos en este segundo paradigma, un mundo en el que los dispositivos, por ejemplo bombillas de bajo consumo, pueden tener dirección IPv6 y establecer a voluntad cómo, cuándo y quién son las otras entidades para el intercambio de información y comandos de control.

Concretamente nos centramos en dispositivos inalámbricos que se comunican mediante redes radio IEEE802.15.4 (en sus versiones de sub-1Ghz ó 2,4 Ghz) y, muchas veces, son sensores alimentados mediante baterías, a diferencia del ejemplo de las bombillas. Para estudios posteriores quedaría la adaptación a IPv6 de dispositivos que se comunican mediante redes cableadas u otras redes inalámbricas como Bluetooth, 2G, 3G o LTE.

Pudiera parecer muy complejo e ineficiente dotar a pequeños elementos de conectividad IPv6, pero lo cierto es que el ejemplo de la bombilla de bajo coste ya se ha desarrollado y probado con éxito su eficiencia energética. La ventaja de esta aproximación es que repite uno de los elementos fundamentales del éxito

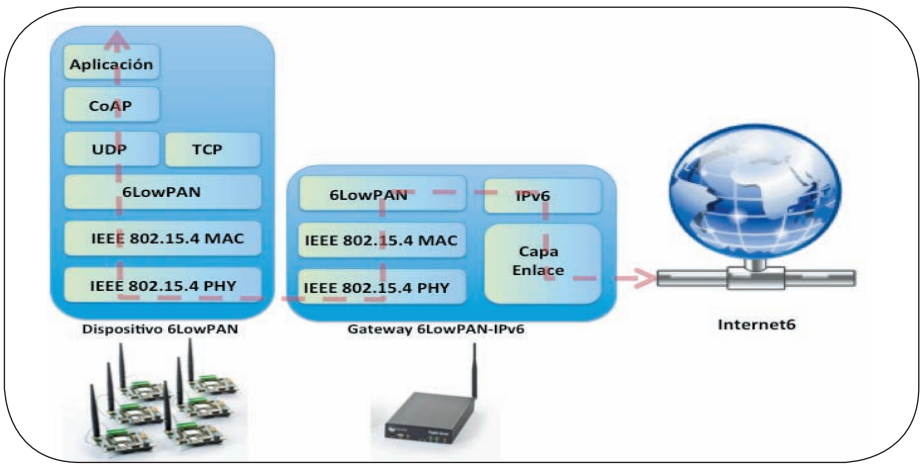


Figura 3. Arquitectura de un servicio 6LowPAN.

> “Pudiera parecer muy complejo e ineficiente dotar a pequeños elementos de conectividad IPv6, pero la bombilla de bajo coste ya se ha desarrollado y probado con éxito su eficiencia energética”

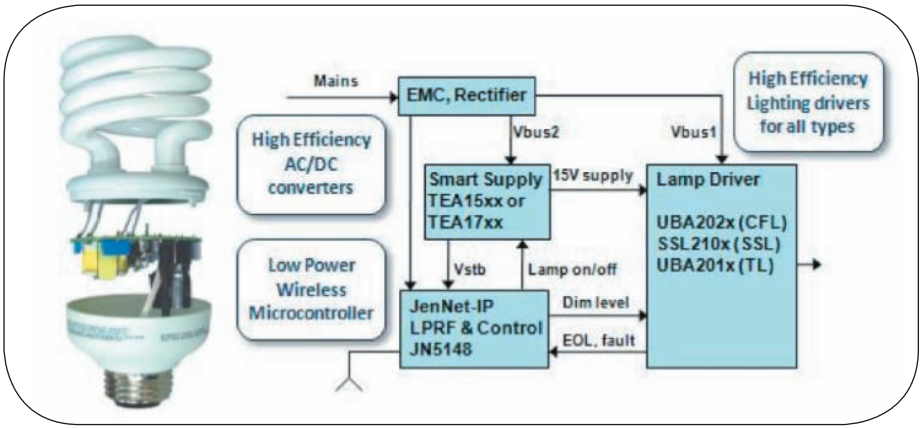


Figura 4. Esquema de funcionamiento de una bombilla con dirección IPv6.

de Internet, que es mover la inteligencia y por tanto la relevancia a los nodos finales.

3.2.1. 6LowPAN: Un protocolo basado en IPv6

No obstante, hablamos de redes de radio inalámbricas de baja potencia (*Wireless Sensor Networks*, WSN) donde los fallos de comunicación son habituales y el ahorro energético impone muchas condiciones como el tamaño de los mensajes a intercambiar y la frecuencia. Por este motivo, el IETF, ha desarrollado un protocolo IP específico para estas redes, llamado 6LowPAN, que se basa en IPv6.

Con 6LowPAN los nodos finales tienen dirección IPv6, pero la compresión de las mismas y la definición de protocolos específicos son compatibles con la eficiencia. Dado que 6LowPAN es una adaptación de IPv6 necesita un elemento intermedio, es decir un *router* 6LowPAN-IPv6, para conectarse a la Internet6. Sin embargo, a diferencia de las soluciones no-IP, este proceso es una mera expansión/compresión de las cabeceras y reenvío que se realizan totalmente en la capa IP. Es decir, los dominios 6LowPAN son a todos los efectos parte de la Internet6.

El estándar 6LowPAN se ha comenzado a implementar de forma masiva (incluso antes de la generalización de la Internet6) gracias a la existencia de dos sistemas operativos libres, Tiny OS y Contiki OS, que funcionan en innumerables plataformas hardware y, entre otros protocolos, soportan 6LowPAN.

La arquitectura de un servicio 6LowPAN se detalla en la **figura 3**, donde además se establece una comparación con otras tecnologías. En el nivel de aplicación, se propone utilizar el estándar IETF CoAP (*Constrained Application Protocol*) que implementa la filosofía REST (*Represesentational State Transfer*), que tanto éxito ha tenido con los *RESTful webservices*, de una manera más ligera y eficiente, sobre el protocolo UDP-IPv6.

Desde el punto de vista del hardware, los elementos necesarios para conectar sensores y actuadores con 6LowPAN se han reducido y miniaturizado sensiblemente. Muchas implementaciones hardware para pruebas, conocidas como “motas”, se basan en un chip microcontrolador dotado de memoria *flash* (1 a 4 Mbytes, generalmente) y un chip de radio conectado a una antena PCB (*Printed Circuit Board Antenna*) o externa, si se desea mayor alcance.

En algunos casos algunos fabricantes han integrado en una sola pastilla (chip) ambos elementos, microcontrolador y circuito de radio. De hecho, el grado de miniaturización es tal, que se ha desarrollado como producto comercial el ejemplo anterior de la bombilla de bajo coste[4,5], basado en el diagrama de la **figura 4**.

Efectivamente, hablamos de una bombilla con dirección IPv6 que, mediante 6LowPAN, puede dialogar con cualquier otro nodo de la Internet6, por ejemplo, otros sensores y actuadores 6LowPAN, *smartphones* y uno o varios sistemas de control de domótica.

Tan real es esta posibilidad desde el punto de vista comercial que Google ha decidido emplear también la tecnología 6LowPAN para su bombilla controlada por Android[6].

3.2.2. Caso de estudio IoT: Conclusiones

Numerosos dispositivos están conectándose a Internet haciendo realidad los paradigmas de casa inteligente, coche conectado, ciudades inteligentes, logística inteligente de personas y objetos y muchos otros nuevos, que irán surgiendo en el futuro. En muchas ocasiones se trata de dispositivos limitados que se conectan con protocolos propietarios a plataformas que los hacen accesibles a Internet. Sin embargo, el avance de la electrónica está permitiendo la aparición de dispositivos que ejecutan pequeñas aplicaciones actualizables remotamente y que están conectados como un nodo más a la Internet6 mediante el uso de la tecnología 6LowPAN.

A día de hoy, son innumerables las empresas en el mundo, en España también, que comercializan soluciones hardware para el prototipado de soluciones 6LowPAN como los que se muestran en la **figura 5**. Este hecho ha sido posible gracias a la aparición de sistemas operativos libres (ContikiOS y TinyOS) que nos permiten programar fácilmente aplicaciones sobre 6LowPAN en este hardware.

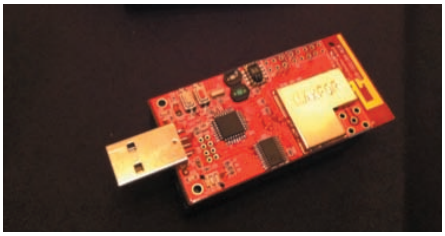


Figura 5. Dispositivos hardware para la implementación de soluciones 6LowPAN.

Notas

[1] *Skype IT Administrators Guide for Windows version 4.2, 2010*. <http://download.skype.com/share/business/guides/skype-it-administrators-guide.pdf>.

[2] **Wikitel.** Problemática NAT: *STUN*. <http://es.wikitel.info/wiki/STUN>.

[3] Siguiendo el algoritmo que se puede consultar desde <http://es.wikitel.info/w/images/6/64/STUN_Algorithm3-spanish.png>. En este esquema, las terminaciones en rojo indican que no es posible aplicar esta técnica, en verde que no es necesario (comunicación directa posible) y en amarillo que es posible y necesario.

[4] **NXP Laboratories UK Ltd.** *Product Brief – JenNet-IP Network Protocol Stack*. <http://www.jennic.com/files/product_briefs/JenNet-IP-PBv1.2docx.pdf>.

[5] **Greentech Media, Inc.** *The IPv6-Addressable Light Bulb Goes On Sale*. <http://www.greentechmedia.com/articles/read/the-ipv6-addressable-light-bulb-goes-on-sale>.

[6] **Greentech Media, Inc.** *Google's Android Bulb to Run on 6LowPAN Standard*. <http://www.greentechmedia.com/articles/read/android-bulb-to-run-on-6lowpan-standard>.

Ecosistema IPv6: Tecnologías utilizadas

Octavio Alfageme
Departamento de Ingeniería de Red y Servicios de Euskaltel

<oalfageme@euskaltel.com>

Resumen: *El soporte de IPv6 en Internet habría sido transparente a los usuarios si la introducción del mismo se hubiese hecho por medio de dual-stack, tal y como los expertos del IETF pensaron al definirlo en 1995. Por el contrario, sólo se ha planteado seriamente la introducción de IPv6 cuando el agotamiento del direccionamiento IPv4 es una realidad, luego el soporte de IPv6 es a día de hoy imprescindible para la continuidad del negocio de todo aquél que ofrece servicios sobre Internet. Esta situación hace necesarias tecnologías de transición (dual-stack, CGNAT, 6RD, NAT64, DS-Lite, MAP, etc.), las cuales posibiliten esa evolución de IPv4 hacia IPv6 y que se adapten a las diferentes situaciones en las que se encuentre cada proveedor de servicio.*

Palabras clave: *CGNAT, DS-Lite, dual-stack, IPv6, MAP, NAT64, 6RD.*

Autor

Octavio Alfageme es Ingeniero de Telecomunicación por la ETSIIyIT de Bilbao (1997) y *MBA Executive* por el Instituto de Empresa de Madrid (2003). Comenzó su carrera en Arthur Andersen MBC (*Management Business Consulting*) como consultor del sector telecomunicaciones, para después integrarse en el departamento de Planificación de Red de Tenaria, hoy parte de Ono, con responsabilidad en la definición del despliegue de red del operador en los ámbitos de red de transmisión, voz, datos y HFC. Finalmente, en el año 1999 se incorporó al departamento de Ingeniería de Red y Servicios de Euskaltel manteniendo responsabilidades tanto en la selección y homologación del equipamiento de la red IP/MPLS, como en la definición de nuevos servicios sobre la misma.

1. Introducción

La evolución de Internet a IPv6 es hoy y seguirá siendo a lo largo de esta década uno de los grandes caballos de batalla a los que nos enfrentaremos todos aquellos que la utilizamos a diario.

Teóricamente esta evolución debería ser transparente para el usuario final y afectar solamente a fabricantes de dispositivos que requieran de conectividad IP, desarrolladores de aplicaciones, operadoras, grandes empresas, etc. Sin embargo, hemos llegado a un punto en que esa transparencia será difícil de mantener en todos los casos.

Nunca pensaron Vinton Cerf y Robert Kahn que sus trabajos de finales de los años 60 y principios de los 70 dentro del proyecto ARPANET del Departamento de Defensa estadounidense derivarían en lo que hoy es Internet. Su trabajo y el de muchos otros fue plasmado por John Postel en la RFC791 de ARPANET [1], la cual definía los fundamentos de lo que hoy conocemos como IPv4.

En la actualidad, Internet cuenta con más de 900 millones de dispositivos conectados a ella de acuerdo al *Internet Systems Consortium* y su crecimiento es imparable, pues Internet forma ya parte de modo indisoluble de la vida de millones de personas (ver **figura 1**).

Durante el tiempo transcurrido, muchas acciones se han tomado para administrar un recurso escaso como son las direcciones IPv4, recurso en otro tiempo considerado prácticamente infinito. Así, podemos citar la especificación en el IETF (*Internet Engineering Task Force*) de mecanismos como *Classless InterDomain Routing* o CIDR [2] para favorecer el uso de subredes de direcciones IPv4, o la creación de los Registros de Internet Regionales o RIRs bajo el auspicio del IANA (*Internet Assigned Numbers Authority*) con objeto de racionalizar el proceso de asignación del direccionamiento IPv4.

Además de las anteriores, otra de las acciones por parte del IETF fue la creación del protocolo IP de nueva generación o IPng, que a la postre conocemos como IPv6 [3], el cual venía a mejorar diferentes aspectos de IPv4 y proporcionaba un espacio de direccionamiento mucho mayor.

La definición inicial de IPv6 llevada a cabo desde el IETF a principios de los 90 llevó asociado un requisito, responsable en gran medida de los problemas que hoy padecemos para llevar a cabo una transición tranquila entre IPv4 e IPv6: ambos protocolos no serían compatibles entre sí. En definitiva, la implantación de IPv6 supondría la existencia de dos Internets, la IPv4 y la IPv6, las cuales no interactuarían entre sí.

Tal vez los expertos técnicos del IETF consideraron una situación de transición en la que las infraestructuras, los contenidos, los dispositivos y las aplicaciones irían soportando progresivamente ambos protocolos. Por este motivo no vieron la necesidad de establecer mecanismos de conexión o traducción entre ambas Internets. Todos los dispositivos tendrían conexión a ambas, luego ellos mismos serían capaces de alcanzar a cualquier otro dispositivo en cualquiera de las dos Internets. Esta configuración es la que conocemos como "*dual-stack*" o mecanismo de doble pila IPv4-IPv6.

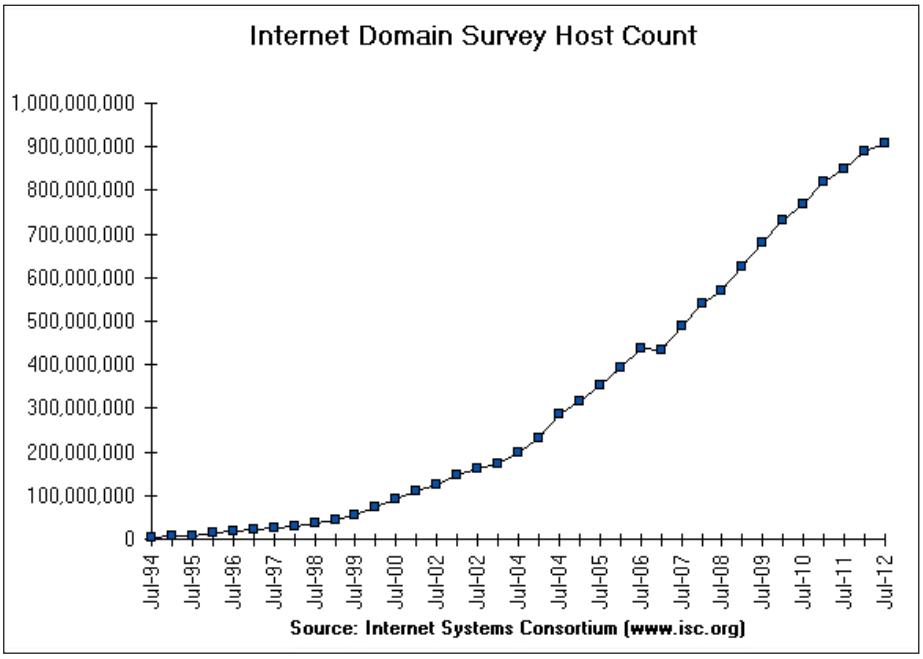


Figura 1. Evolución del número de hosts en Internet (Fuente: Internet Systems Consortium)[1].

> “El caso ideal de evolución para un proveedor de servicio sería tener la capacidad de desplegar extremo a extremo mecanismos de doble pila o “*dual-stack*” IPv4-IPv6 en toda su red, de modo que sean los dispositivos finales los que determinen a cuál de las dos Internets acceder”

Por desgracia, en el IETF pasaron por alto el factor económico. Las actualizaciones ligadas al soporte de IPv6 resultaban y aún hoy resultan, difíciles de justificar por medio de un caso de negocio tradicional en el que surgen preguntas como: “¿por qué fabricar dispositivos con hardware compatibles con IPv6 si esto potencialmente puede aumentar su precio, luego hacerlos menos competitivos?”, o “¿por qué asumir el coste de actualizar mi infraestructura hardware y software para soportar IPv6, si no lo necesito a corto plazo?”. Así, ante la proximidad del fin del direccionamiento IPv4 y el bajo nivel de desarrollo de Internet IPv6, en la última década y especialmente en los últimos cinco años, las iniciativas alrededor de los mecanismos de transición de IPv4 a IPv6 han sido numerosas.

A día de hoy APNIC y RIPE, los registros de Internet regionales de Asia-Pacífico y de Europa, Oriente Medio y parte de Asia central respectivamente, han llegado ya a su última /8 de direccionamiento IPv4 (16,8 millones de direcciones aproximadamente). Esto equivale a un agotamiento tácito del mismo.

Los restantes RIRs lo esperan a lo largo de los próximos años como refleja la **figura 2**. Esta situación ha supuesto un vuelco al “caso de negocio” de IPv6, pues el soporte del protocolo IPv6 se ha convertido en algo indispensable para la continuidad de una Internet abierta tal y como la conocemos en la actualidad [4].

Actualmente Internet IPv6 crece progresivamente, favorecida por la propia escasez de direccionamiento IPv4 y por eventos como el *World IPv6 Launch*. Existen ya expertos como Geoff Huston que vaticinan que Internet será plenamente IPv6 en el año 2022 [5]. Sin embargo, en el camino queda una década en la que los proveedores de acceso a Internet deberán apoyarse en mecanismos de transición entre Internet IPv4 e Internet IPv6.

2. *“Dual-stack”*, la solución ideal

El caso ideal de evolución para un proveedor de servicio sería tener la capacidad de desplegar extremo a extremo mecanismos de doble pila o “*dual-stack*” IPv4-IPv6 en toda su red, de modo que sean los dispositivos finales los que determinen a cuál de las dos Internets acceder. Esto permite además mantener al usuario final ajeno al proceso de migración de los propios contenidos en Internet, los cuales desde el primer momento no estarán disponibles sobre IPv6.

Este modelo es claramente el de menor coste operativo y máxima fiabilidad a la hora de desplegar IPv6. De hecho, “*dual-stack*” está permitiendo un despliegue ágil de IPv6 a grandes cableros norteamericanos como Comcast o TimeWarner Cable, que la han elegido como modelo para proporcionar IPv6 hasta sus usuarios de banda ancha.

“*Dual-stack*” es también el mecanismo tradicional de acceso que los operadores ofrecen en el segmento de grandes empresas tanto para el acceso a Internet como para el acceso a VPNs IP (redes privadas virtuales) cuando requieren de conectividad IPv6.

3. Alternativas ante la escasez de direccionamiento IPv4

Sin embargo, como hemos comentado anteriormente, “*dual-stack*” no es viable en una situación de escasez de direccionamiento IPv4, en la cual el proveedor de servicio ha de buscar mecanismos que le permitan seguir creciendo en número de clientes, a pesar de no poder contar con direcciones IPv4 adicionales. Ante esta situación existen dos tipos de estrategias no necesariamente incompatibles entre sí:

- Preservación de IPv4. Mecanismos que posibiliten ahorrar direccionamiento IPv4 en los que CGN (*Carrier Grade NAT*) es su máximo exponente.
- Transición hacia IPv6. Los mecanismos que favorecen la transición hacia IPv6 contemplando la necesidad de convivencia con IPv4.

3.1. *Carrier Grade NAT* (CGN)

CGN es la estrategia de preservación por antonomasia. Se fundamenta en la compartición de direccionamiento público IPv4 entre múltiples clientes por medio de una función de NAT (*Network Address Translation*) situada en la red del operador. Los clientes pasan a recibir una dirección IPv4 privada en su interfaz de red.

En definitiva, CGN viene a extender a la red el tradicional modelo de NAT de las redes de hogar y es común verlo referenciado como NAT444 por los tres dominios IPv4 en cuyos puntos de conexión existe una función de NAT: Red local – Red de operador – Internet (ver **figura 3**).

Las desventajas de CGN son numerosas y su coste operativo por usuario es creciente en el tiempo, especialmente si lo comparamos con

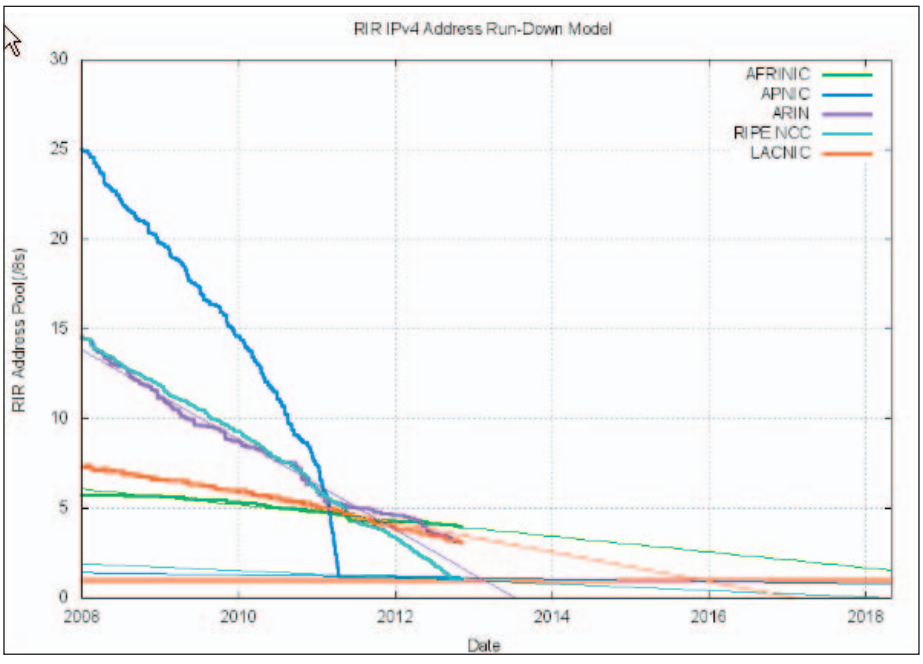


Figura 2. Proyección de consumo de direccionamiento IPv4[2] (Fuente: Geoff Huston).

> “ CGN es la estrategia de preservación por antonomasia. Se fundamenta en la compartición de direccionamiento público IPv4 entre múltiples clientes por medio de una función de NAT situada en la red del operador ”

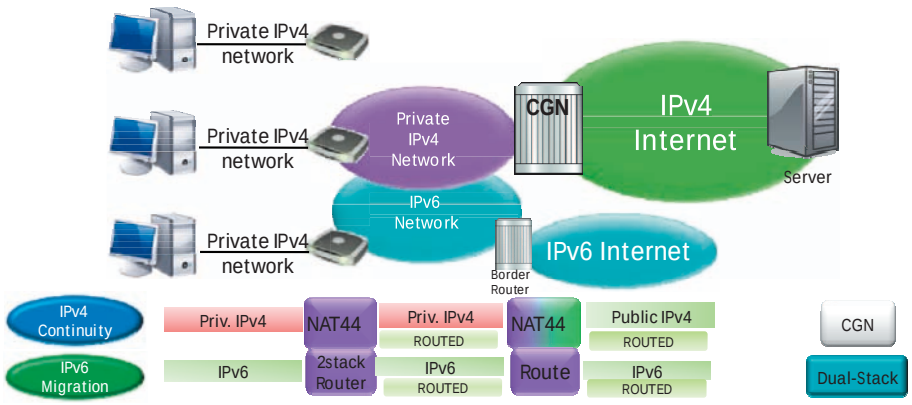


Figura 3. Arquitectura *Carrier Grade NAT*[3]. (Fuente: APRICOT).

el de evolucionar a IPv6. Así, frente a la ventaja de reducir el consumo de direccionamiento IPv4 público, CGN se caracteriza, entre otras cosas, por [6]:

- Número de puertos por usuario limitado al compartirse la IP. Según cuál sea el nivel de concentración de usuarios, algunas aplicaciones podrían no funcionar correctamente.
- Complejo tratamiento de las sesiones entrantes hacia servicios residentes en las redes de los usuarios (*port forwarding*). Protocolos como UPnP o NAT-PMP no son capaces de superar el NAT en el propio *router* de cliente para provocar la apertura automática de puertos en el NAT en la red. Por ello, el IETF ha definido el PCP (*Port Control Protocol*), protocolo orientado a la automatización de la apertura de puertos en CGN.
- Importancia del diseño de la política de creación, mantenimiento y eliminación de los mapeos de NAT en la red.
- Necesidad de contar con ALGs (*Application Layer Gateways*) en la red para el correcto funcionamiento de ciertas aplicaciones y protocolos.
- Gran complejidad de las intercepciones legales y, en general, de todos los procesos de identificación de usuarios, requiriendo un procesado intensivo de información.
- Problemas de geolocalización, pues el punto de NAT en la red puede estar a muchos kilómetros de la ubicación real del usuario.

CGN está muy extendido en entornos de dispositivos de comportamiento controlado como es el caso de los *smartphones* en los operadores móviles. En este escenario, CGN permite hacer frente al enorme crecimiento del número de estos dispositivos, sin pérdida de prestaciones para la mayoría de los usuarios.

Sin embargo, resulta paradójico que aún a día de hoy existan defensores de CGN como solución de infraestructura cuando experiencias, como por ejemplo las del IETF [7], describen los problemas que aplicaciones muy populares como juegos *online* o P2P sufren por el doble NAT que CGN implica. Extender CGN a entornos de dispositivos más abiertos como accesos de banda ancha implicaría indefectiblemente una importante merma de las prestaciones disfrutadas hasta entonces por los usuarios.

3.2. Mecanismos de transición hacia IPv6

Como hemos mencionado, el trabajo del IETF en la definición de mecanismos de transición se ha incrementado enormemente en los últimos cinco años. La **figura 4** muestra los vínculos existentes entre los diferentes mecanismos de transición definidos dentro de “*softwires*”, el grupo de trabajo del IETF responsable de estos protocolos.

Los mecanismos de transición buscan ofrecer alternativas a los proveedores de servicio con el objeto de favorecer la convivencia entre IPv4 e IPv6, adaptándose a cada situación particular en función del tipo de red de acceso considerada (móvil, cable, ADSL…), estado de la misma en cuanto a su capacidad de actualización para soportar IPv6, tipo de equipos de cliente o CPEs (*Customer Premises Equipment*) considerados, etc. De entre todos ellos destacan 6RD, NAT64, DS-Lite y MAP.

3.3. 6RD

6RD (*IPv6 Rapid Deployment*) proporciona conectividad IPv6 a los usuarios conectados a una red de acceso IPv4. Es una evolución de 6to4, un mecanismo histórico de tunelizado de IPv6 sobre IPv4. El operador francés Free es el gran valedor de 6RD en el mundo, pues fue pionero en la conexión de usuarios residenciales a Internet IPv6 por medio de este protocolo.

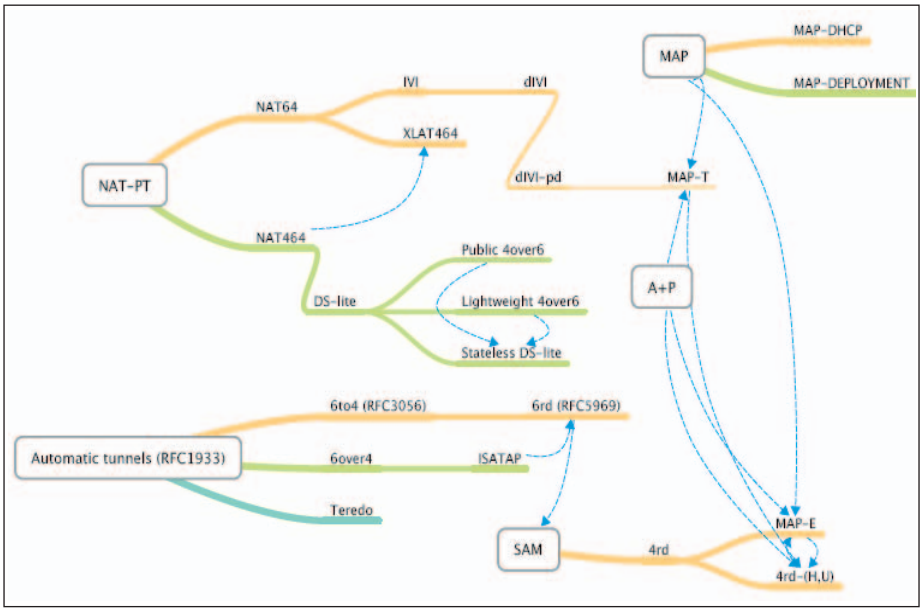


Figura 4. Evolución de los mecanismos de transición hacia IPv6[4] (Fuente: IETF).

> “Los mecanismos de transición buscan ofrecer alternativas a los proveedores de servicio con el objeto de favorecer la convivencia entre IPv4 e IPv6, adaptándose a cada situación particular”

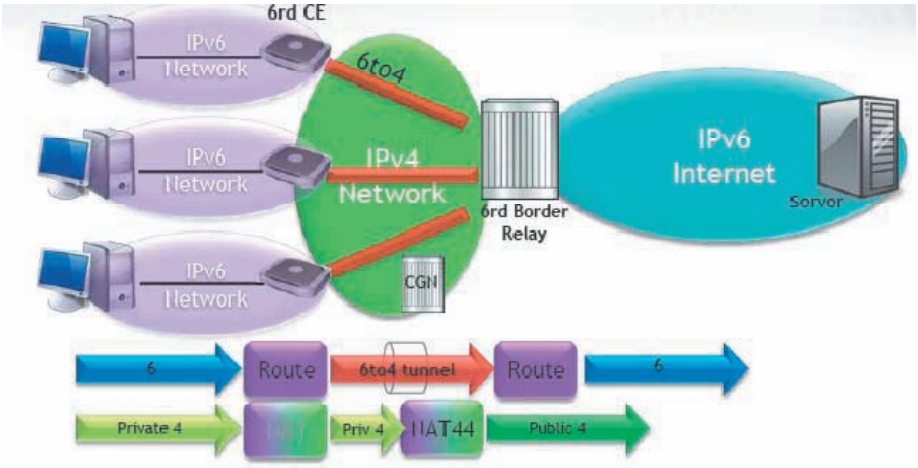


Figura 5. Arquitectura 6RD[5] (Fuente: APRICOT).

6RD define dos componentes específicos dentro de la red: los CPEs de cliente y el *6RD Border Relay*, los cuales son responsables de la encapsulación y desencapsulación del tráfico IPv6 tunelizado dentro de paquetes IPv4. Esta encapsulación es la misma que la de 6to4, pero presenta notables mejoras en cuanto al direccionamiento empleado y las posibilidades de gestión del servicio (ver **figura 5**).

6RD por sí mismo no favorece la evolución a IPv6 de la red de acceso, pues, de hecho, el tráfico IPv4 desde los usuarios sigue siendo cursado de modo nativo sobre IPv4. Por este motivo, en caso de escasez de direccionamiento se hace necesaria una función adicional de CGN en la red.

Otras dos desventajas de 6RD son el hecho de que el tunelizado sobre IPv4 implica tener que controlar el tamaño de los paquetes IPv6 (*Maximum Transfer Unit IPv6*), así como el que 6RD no contempla la posibilidad de que un usuario exclusivamente IPv6 acceda a contenido sólo accesible en IPv4.

3.4. NAT64

NAT64 posibilita que, de modo transparente, dispositivos exclusivamente IPv6 accedan a redes IPv4. NAT64, como su nombre indica, supone una traducción entre direccionamiento IPv6 e IPv4. Para conseguirlo, se apoya en DNS64. Tal y como muestra la **figura 6**, si un destino carece de alcanzabilidad IPv6 (no tiene registro AAAA), el servidor DNS de la red IPv6 es capaz de transformar su registro A de la red IPv4 en un destino IPv6 incorporando el prefijo asociado al correspondiente traductor NAT64 de la red. El traductor NAT64 hará entonces la correspondiente traducción entre el dominio IPv6 y el IPv4.

NAT64 como mecanismo de traducción que es, tiene todas las desventajas que CGN ya presentaba, junto con la desventaja añadida de que los usuarios IPv6 no son accesibles desde el dominio IPv4. Por lo tanto, un usuario IPv4 no podría acceder a un contenido en el dominio IPv6.

Estas desventajas, junto con la ventaja de no implicar requerimientos específicos en el CPE de usuario, han llevado a NAT64 a entornos con dispositivos de comportamiento controlado, como son los *smartphones*.

Así, NAT64 cuenta con numerosas referencias como la de T-Mobile en Estados Unidos o las de operadores móviles asiáticos. Todos ellos han apostado por redes móviles sólo IPv6 ante la escasez de direccionamiento IPv4.

3.5. DS-Lite

DS-Lite (*Dual-Stack Lite*) posibilita seguir ofreciendo conectividad IPv4 tras actualizar la red de acceso a IPv6. Justo a la inversa que 6RD, DS-Lite tuneliza el tráfico IPv4 sobre una red de acceso IPv6 y, para hacer frente a la escasez de direcciones, ofrece un único nivel de NAT (NAT44) en la red (ver **figura 7**).

En la red DS-Lite se distinguen dos elementos: los CPEs de clientes compatibles con DS-Lite y el AFTR o *Address Family Translation Router*. Ambos son responsables de la encapsulación y desencapsulación del tráfico IPv4 transportado sobre IPv6, siendo además el AFTR el punto donde residirá la función de traducción NAT44 de la red.

Frente a la desventaja que implica la necesidad de CPEs compatibles o el hecho de no ser capaz de proporcionar acceso a contenidos IPv4 a un dispositivo con conectividad exclusiva IPv6, DS-Lite ofrece diversas ventajas:

- Proporciona conectividad IPv4 a los *hosts* y/o *routers* domésticos (CPEs) sin necesidad de provisionar direccionamiento IPv4 en su interfaz de red.

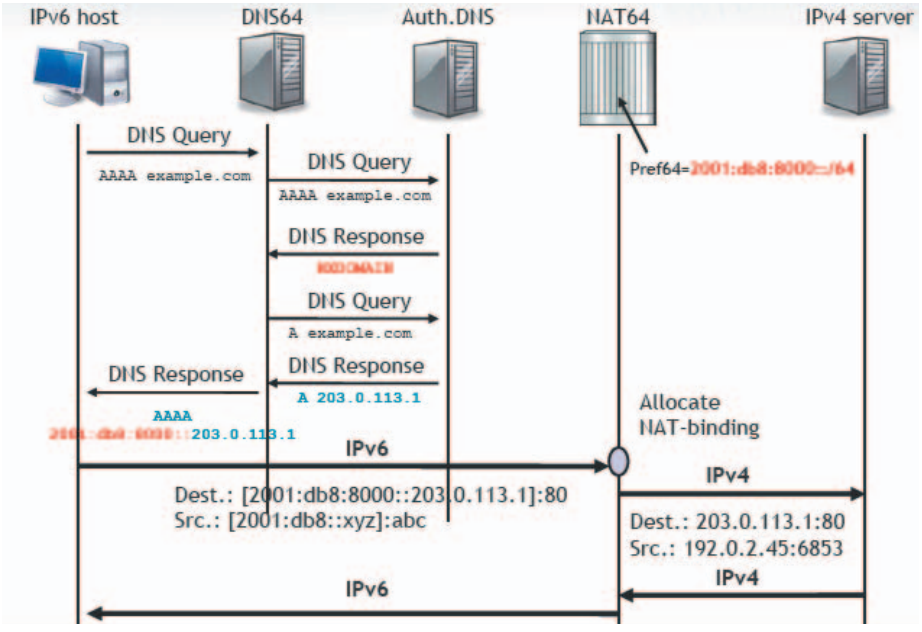


Figura 6. Fundamento de funcionamiento de NAT64[6]. (Fuente APRICOT)

> “A día de hoy, DS-Lite es la tecnología de transición preferida para un operador de banda ancha fija que, por la escasez de direccionamiento IPv4, no puede apostar por *dual-stack* ”

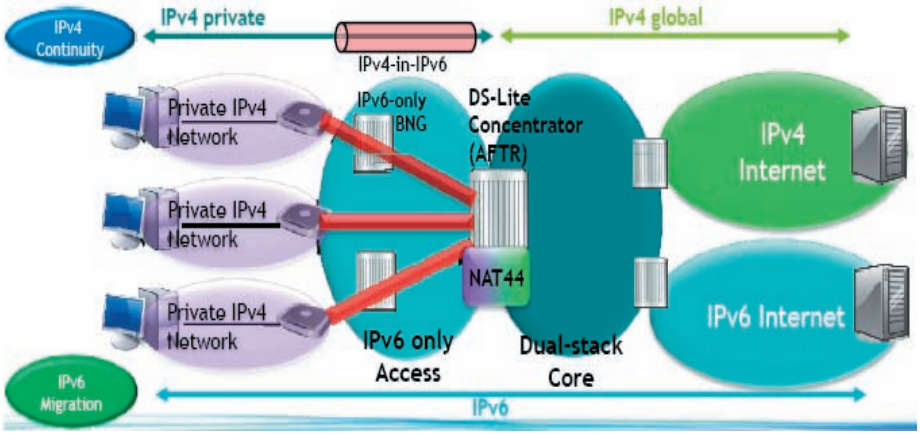


Figura 7. Arquitectura DS-Lite[7] (Fuente: APRICOT).

■ Permite prescindir totalmente de IPv4 en la red de acceso.

Además, el único nivel de NAT aporta ventajas frente a los dos niveles (NAT444) de CGN:

■ No hay necesidad de direcciones privadas IPv4 en la red del operador.
■ El impacto sobre las aplicaciones es menor con uno que con dos niveles de NAT.
■ Es posible el reenvío de puertos o *port forwarding* desde el AFTR con tecnologías propias de la red local del hogar tales como NAT-PMP o UPnP, no requiriendo de protocolos como PCP en el caso de CGN.

A día de hoy, DS-Lite es la tecnología de transición preferida para un operador de banda ancha fija que, por la escasez de direccionamiento IPv4, no puede apostar por “*dual-stack*”. A pesar de ello, las referencias de despliegue de DS-Lite en el mundo no pasan todavía de pruebas piloto.

3.6. MAP

Los mecanismos de transición anteriores comparten la limitación de que las funciones de traducción y de encapsulación/desencapsulación mantienen control de estado, luego el tráfico en ambos sentidos ha de pasar siempre por el mismo dispositivo de red (*Border Relay* en 6RD, traductor en NAT64 y AFTR en DS-Lite), lo cual aumenta su criticidad y afecta de manera importante al proceso de provisión de cada solución

Frente a esto, MAP (*Mapping Address + Port*) ofrece una traducción bidireccional IPv4-IPv6 que no requiere de almacenamiento de estado en el punto de traducción, luego es posible la existencia de tráfico asimétrico que atraviese por diferentes equipos frontera entre los dominios IPv4 e IPv6 (ver **figura 8**).

MAP se postula como la tecnología de transición más prometedora en la que actualmente está trabajando el IETF y sobre la cual comienzan a existir las primeras implementaciones experimentales [8].

La definición principal de MAP es el MAP-E (*Mapping Address + Port Encapsulation*), aunque hay dos ligeras variantes que son MAP-T (*Mapping Address + Port Translation*) y 4rd (*IPv4 Residual Deployments*) que comparten sus características básicas.

En una red MAP existen dos componentes esenciales: los CPEs y los *MAP Border Relays*.

Los CPEs, aparte de cursar nativamente el tráfico IPv6, asumen las tareas de encapsular el tráfico IPv4 sobre IPv6 para enviarlo hacia los *MAP Border Relays*, así como realizar NAT44 sobre el tráfico IPv4 del mismo modo que hoy hacen los CPEs de la mayoría de los usuarios de Internet.

La particularidad de este NAT44 es que múltiples CPEs comparten la misma dirección, luego el CPE recibe en el proceso de provisión los puertos que podrá utilizar y que será lo que diferencie a unos CPEs de otros. Toda esa información viene dada por el prefijo IPv6 recibido por el CPE, ya que en un dominio MAP, dado un prefijo IPv6, se puede deducir de forma unívoca qué dirección pública IPv4 y qué rango de puertos utiliza el CPE. Por su parte, el *MAP Border Relay* se limita a desencapsular el tráfico saliente hacia el dominio IPv4 y a encapsular el tráfico entrante hacia su destino IPv6, pues recordemos que por la dirección y puerto destino IPv4 es posible construir la dirección IPv6.

4. IPv6 es una realidad

El soporte de IPv6 es a día de hoy imprescindible para la continuidad del negocio de todo aquél que ofrezca servicios sobre Internet, luego los proveedores de servicio Internet han de entender esta necesidad y marcar una hoja de ruta para responder a esta demanda.

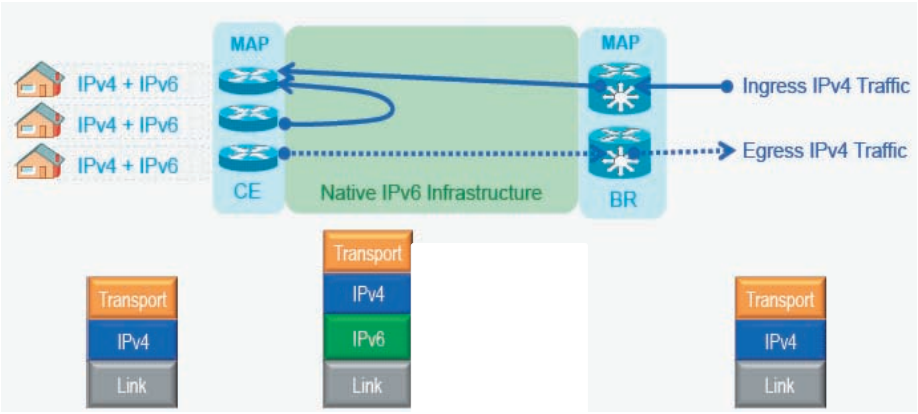


Figura 8. Arquitectura MAP[8] (Fuente: SWINOG).

Red soporta IPv6	Control de CPEs	Escasez de IPv4s	
Sí	Indiferente	No	**Dual-stack**
No	Alto	Indiferente	**6RD**
Sí	Bajo	Sí	**NAT64**
Sí	Alto	Sí	**DS-Lite/MAP**

Figura 9. Idoneidad de los mecanismos de transición frente a la situación de los proveedores de servicio.

Esta hoja de ruta vendrá condicionada por el estado de su red, el control sobre los CPEs desplegados en la misma y sus necesidades de direccionamiento IPv4 a corto y medio plazo (ver **figura 9**).

"*Dual-stack*" es la solución ideal de convivencia IPv4 e IPv6, pero la escasez de direccionamiento IPv4 no la hace siempre viable, por lo que los proveedores de servicio deberán adaptarse a ello por medio de los diferentes mecanismos de transición en cuya definición el IETF trabaja intensamente.

La preservación de IPv4 por medio de CGN ha de ser visto como un último recurso y no como una herramienta desde el punto de vista del proveedor de servicio, pues supone un incremento importante del coste operativo y una degradación del servicio ofrecido a los usuarios finales, luego una pérdida de competitividad.

Agradecimientos
A Fernando Gálvez de Cisco Systems.

Referencias

[1] J. Postel. *IETF RFC791 Internet Protocol*, 1981. <http://www.ietf.org/rfc/rfc791.txt>.
[2] V. Fuller et al. *IETF RFC1338 Supernetting: an Address Assignment and Aggregation Strategy*, 1992. <http://tools.ietf.org/html/rfc1338>.
[3] S. Deering, R. Hinden. *IETF RFC1883 Internet Protocol, Version 6 (IPv6) Specification*, 1995. <http://www.ietf.org/rfc/rfc1883.txt>.
[4] L. Colitti. *Comisión Europea - 2009 IPv6 Meeting*, marzo 2009. <http://ec.europa.eu/information_society/policy/ipv6/docs/ipv6_meeting_march_2009/lorenzo_colitti_en.pdf>.
[5] G. Huston. *LACNIC18*, octubre de 2012. El material ofrecido en estos talleres se encuentra disponible en: <https://www.dropbox.com/sh/8go78duj53630c6/fCd5o3BW0B>.
[6] M. Ford et al. *IETF RFC6269 Issues with IP Address Sharing*, junio 2011. <http://tools.ietf.org/html/rfc6269>.
[7] Z. Li et. al. *IETF draft-li-behave-nat444-test Experience from NAT44 Translation Testing*, julio 2012. <http://tools.ietf.org/html/draft-li-behave-nat444-test-01>.
[8] Shishio Tsuchiya et al. *IETF*, noviembre 2012. <http://www.ietf.org/proceedings/85/slides/slides-85-softwire-2.pptx>.

Notas

[1] <http://www.isc.org/solutions/survey>.
[2] <http://www.potaroo.net/tools/ipv4/index.html>.
[3] <http://www.apricot.net/apricot2011/media/Apricot_IPv6_transition_kashimura_rev3.ppt>.
[4] <http://www.ietf.org/proceedings/83/slides/slides-83-softwire-10.pdf>.
[5] <http://www.apricot.net/apricot2011/media/Apricot_IPv6_transition_kashimura_rev3.ppt>.
[6] Ver nota 5.
[7] Ver nota 5.
[8] <http://www.swinog.ch/meetings/swinog24/p/04_townsley-map-swinog-may-2012-distribution.pdf>.

Internet6: Alcanzando la masa crítica de usuarios y tráfico

Juan Pedro Cerezo Martín[1], Javier Benítez[2], Norberto Ojinaga Goitia[3], Antonio Hernández Armenteros[4], Carlos Ralli Ucendo1[5], Óscar Pantoja García[6]

[1]BT España, [2]Colt, [3]Euskaltel, [4]Jazztel, [5]Telefónica I+D, [6]Vodafone

<benjuan.cerezo@bt.com>, <javier.benitez@colt.net>, <nojinaga@euskaltel.com>, <antonio.hernandez@jazztel.com>, <ralli@tid.es>, <oscar.pantoja@vodafone.com>

Resumen: *En este artículo se describen diversos datos y estadísticas del progreso en el uso de IPv6, tanto en tráfico de datos como en número de usuarios, distinguiendo tanto a nivel de país como en cuanto a la evolución temporal. Los autores, que representan a seis de los principales ISPs (Internet Service Providers) españoles, exponen brevemente las estrategias de sus empresas con vistas a la necesidad de abordar una transición eficaz y eficiente hacia el uso generalizado de IPv6.*

Palabras clave: *BT España, CDN, Colt, estadísticas de transacciones, Euskaltel, implementación de IPv6, ISP, Jazztel, puntos neutros, redes de distribución de contenidos, Telefónica I+D, tráfico IPv6, Vodafone.*

1. Introducción

En otros artículos de esta monografía se ha descrito en detalle el éxito de las iniciativas de Internet Society (ISOC), W6D (*World IPv6 Day*, 6 de junio de 2011) y W6LD (*World IPv6 Launch Day*, 8 de de junio 2012), de cara a poblar la Internet6 de contenidos relevantes.

Efectivamente, como consecuencia de estas iniciativas, más del 24 por ciento de los 500 sitios más visitados están permanentemente disponibles en la Internet6. Esto incluye los más visitados: Google, Youtube, Facebook, Yahoo y Wikipedia, que han impulsado este proceso con la todavía notable ausencia de Twitter.

En este punto, sólo resta que los usuarios también la conquisten y utilicen de forma masiva, convirtiéndose en la Internet de todos. Tras este hecho, tal y como planifica el grupo Sunset4 de IETF, se podría comenzar el lento proceso de apagado progresivo de la Internet IPv4.

Los actores protagonistas en la introducción de usuarios en Internet6 son los proveedores comerciales de Internet (ISPs), que conectan a ciudadanos de todo tipo, y las redes académicas, que traen consigo a investigadores, docentes y estudiantes.

A día de hoy pues, el éxito de Internet6 se debate en los planes de despliegue de estos actores, si bien este artículo se centra en las actividades de los operadores.

Hay dos medidas relevantes a las que prestar atención, por un lado el tráfico (absoluto y relativo a IPv4) y por otro el número de usuarios. En ambos casos se estudian datos agregados sin distinguir si los usuarios son de tipo académico o no, si bien los usuarios académicos tienen menos peso en las estadísticas en general.

El tráfico IPv6 en algunos de los puntos de intercambio más relevantes se ofrece como parte de las estadísticas públicas y el número de usuarios puede conocerse a través de los datos que publican los operadores.

Autores

Juan Pedro Cerezo Martín comenzó su trabajo con redes de datos en 1981, siendo usuario de la red EARN/BITNET, durante sus estudios de grado y postgrado en la Universidad Autónoma de Madrid (UAM). Desde 1984 ha trabajado en proyectos avanzados de implantación de redes como Ingeniero de Sistemas en la UAM, como Investigador Asociado del Centro de Investigación de IBM en la UAM, como consultor independiente en tecnologías asociadas a Internet, y en la actualidad, como Especialista de Redes de BT Innovation & Design. Ha participado en iniciativas como la *IPV6 Task Force* española, Observatorio IPv6 y el Grupo de Operadores de Red españoles (ESNOG/GORE), y lleva promoviendo el despliegue de IPv6 en España desde el año 2001, a través de múltiples pilotos y experiencias de conectividad con operadores nacionales.

Javier Benítez vive en Barcelona y es miembro desde el año 2009 del departamento de Estrategia de Red y Arquitectura responsable de definir la arquitectura de la red de Colt a largo plazo (de 3 a 5 años). Sus áreas de responsabilidad e investigación son la red Óptica, Ethernet, IP, MPLS y SDN (*Software Defined Networking*). En el área de IPv6, Javier es el responsable en Colt del proyecto de implementación a nivel global. Otros proyectos que Javier está liderando en la actualidad son *Network Layer Integration* (integración de las redes Óptica, Ethernet e IP a nivel de conmutación de paquetes) y *Cloud Centric Network* (desarrollo de la arquitectura de nueva generación para los *Data Centre* de Colt y la red que los interconecta). Con anterioridad a su actual posición, Javier trabajó durante casi 10 años en el departamento de ingeniería IP de Colt diseñando tanto las redes IP/MPLS y Carrier Ethernet como los servicios asociados. Javier es Ingeniero Superior de Telecomunicaciones por la UPC (*Universitat Politècnica de Catalunya*, 1996) y tiene un Máster en *Electrical Engineering* por la *Stanford University* (California, USA, 1999).

Norberto Ojinaga Goitia es Ingeniero Técnico Superior de Telecomunicaciones por la ETSIT de Bilbao. Su experiencia profesional anterior se desarrolló en el campo de las telecomunicaciones, principalmente en el sector del transporte en Thales/Thomsom (1992-1999), en proyectos como los metros de Bilbao, Madrid, Paris, Hong Kong, etc. Desde 1999 desarrolla su actividad en Euskaltel, S.A., inicialmente como Coordinador del Centro de Gestión de Redes Corporativas (1999-2001), posteriormente como Gerente de Despliegue Específico de Red (2001-2005), Director de Despliegue de Red (2005-2010) hasta la actualidad como Director de Ingeniería y Planificación Tecnológica de Red. Durante 6 años (2001-2007) fue profesor de Fibra Optica en la Universidad de Deusto en la especialidad de Ingeniería. Es Secretario Técnico del Colegio Oficial de Ingenieros Superiores de Telecomunicación del País Vasco (COITPV), y de la Asociación de Ingenieros Superiores de Telecomunicación del País Vasco (AITPV).

Antonio Hernández Armenteros es Ingeniero Superior de Telecomunicaciones por la Universidad Politécnica de Madrid, diplomado en Ciencias Empresariales por la UNED y *Executive MBA* por el Instituto de Empresa. Ha desarrollado su carrera profesional en Jazztel desde el año 2000 donde se incorporó como Ingeniero de Datos (2000 - 2005), posteriormente como Responsable del grupo de Ingeniería de Datos (2005 - 2006) y actualmente ocupa el puesto de Gerente de Ingeniería de *Core* de Red donde lidera los equipos de Datos, Voz y Transmisión.

Carlos Ralli Ucendo es Ingeniero Superior de Telecomunicaciones por la Universidad Politécnica de Madrid. En 1999 realizó la primera conexión a las redes IPv6 de dicha universidad y los laboratorios de Telefónica I+D. Tras liderar Euro6IX (2002-2005), el mayor proyecto IPv6 de operadoras cofinanciado por la UE, ha sido coordinador técnico de la participación de Telefónica en las recientes

> “ISOC estableció a partir de una encuesta abierta un umbral del 1%, a partir del cual proveedores de todo tipo, incluyendo electrodomésticos, videoconsolas y otros, incluirían soporte nativo IPv6 como parte de su estrategia comercial”

jornadas mundiales de IPv6. Ha participado en análisis de riesgos *in-situ* de las redes de Telefónica en Brasil, Chile y Colombia y cuenta con una amplia experiencia en proyectos de innovación, asistiendo regularmente a la Comisión Europea como experto independiente en las auditorías técnicas de proyectos cofinanciados. Es un ponente activo, con más de medio centenar de ponencias técnicas, presentaciones relevantes y demostraciones en Asia-Pacífico, Europa y Latinoamérica. Durante el año 2011 desempeñó el papel de jefe de delegación para *Internet Society* (ISOC) y el IETF (*Internet Engineering Task Force*). Actualmente, forma parte del equipo de desarrollo de la plataforma de servicios de “*Future Internet*” FI-WARE (@Fiware) y está abriendo una línea de investigación centrada en las oportunidades e impacto de la llegada masiva de IPv6 en productos y servicios de Internet.

Óscar Pantoja García trabaja en Vodafone (Airtel) desde el año 2000. Ha desempeñado diversas funciones de operación y mantenimiento, ingeniería, gestión y coordinación de proyectos a nivel internacional, relacionadas todas ellas con redes IP/MPLS. Actualmente está trabajando en NSU (*Network Service Unit*) de Vodafone. Desde 2009 lidera el programa de IPv6 para Vodafone Grupo en Europa, el cual se encarga de probar la tecnología y definir los estándares para la implementación en las operadoras europeas de Vodafone, así como de coordinar dicha implementación.

Sin embargo, existen datos indirectos que nos permiten conocer el grado de despliegue a nivel mundial, por país o incluso por dominio de *routing*.

Efectivamente, hay unos pocos sitios de Internet que prácticamente todos los usuarios visitan en algún momento y por lo tanto sirven para construir este tipo de estadísticas. Uno de ellos es Google, que proporciona unos datos sobre accesos IPv6 que pueden darnos una idea muy aproximada del número y crecimiento de usuarios de la Internet6.

Podemos preguntarnos cuál es el umbral de tráfico a partir del cual podríamos esperar un rápido crecimiento exponencial típico del modelo Internet. En este sentido, ISOC estableció a partir de una encuesta abierta un umbral del 1%, a partir del cual proveedores de todo tipo, incluyendo electrodomésticos, videoconsolas y otros, incluirían soporte nativo IPv6 como parte de su estrategia comercial.

Para ilustrar la utilidad y sensibilidad de estas medidas, en la **figura 1** mostramos un gráfico que compara los accesos a Google por IPv6 en Estados Unidos, Japón, Alemania e India.

A nivel global, el diagrama de la **figura 2**, elaborado y publicado recientemente por Cisco, muestra mediante un mapa interactivo los datos por país en relación al porcentaje de contenidos accesibles y usuarios.

Podemos ver que el país líder en Europa es Rumanía, debido a un despliegue relevante realizado por RCS-RDS, el mayor ISP de acceso fijo de banda ancha, que fue anunciado en la prensa y en foros especializados, como el “*World IPv6 Congress 2012*” (Bruselas, 28 y 29 de mayo de 2012).

En el caso de España, se percibe un tímido incremento en 2012 aunque todo apunta a que habrá que esperar a despliegues más relevantes para sobrepasar el 1% (ver **figura 3**).

2. Tráfico en los puntos de intercambio

Los puntos neutros (IXs, NAPs) son infraestructuras donde los proveedores de servicios de Internet (ISPs) intercambian el tráfico de Internet entre sus redes. De esta forma, se mejoran los costes de entrega y consumo de información, así como también la eficiencia y la optimización de los algoritmos de encaminamiento.

Actualmente, algunos de los principales puntos de intercambio de tráfico a nivel mundial están en Seúl, Nueva York, Londres, Frankfurt, Amsterdam, y Palo Alto[2].

En España, existen varios puntos de intercambio como Euskonix, Catnix y Espanix, siendo éste último el nodo más importante en cuanto a cantidad de tráfico a nivel nacional y uno de los más relevantes de Europa con una media de más de 180 Gb por segundo.

En este artículo se estudia la evolución del tráfico IPv6 en dos puntos de intercambio que publican datos al respecto: AMS-IX y DE-CIX.

En lo que se refiere a Espanix, situado en Madrid, el nodo neutro dispone de infraestructura y direcciones para el intercambio nativo de tráfico IPv6, que ya está siendo explotado por algunos de sus más de 60 miembros. Sin embargo, no se ofrecen estadísticas de tráfico IPv6 que nos permitan realizar un análisis similar.

2.1. DE-CIX

En el caso de este nodo, el tráfico ascendió a 3Gbps tras el W6LD’12. Mientras que anteriormente era de 1,4Gbps durante el W6D’11 y de menos de 1Gbps antes de este evento. Puede apreciarse también, como actualmente el tráfico ha crecido hasta 4,9 Gbps (ver **figura 4**).

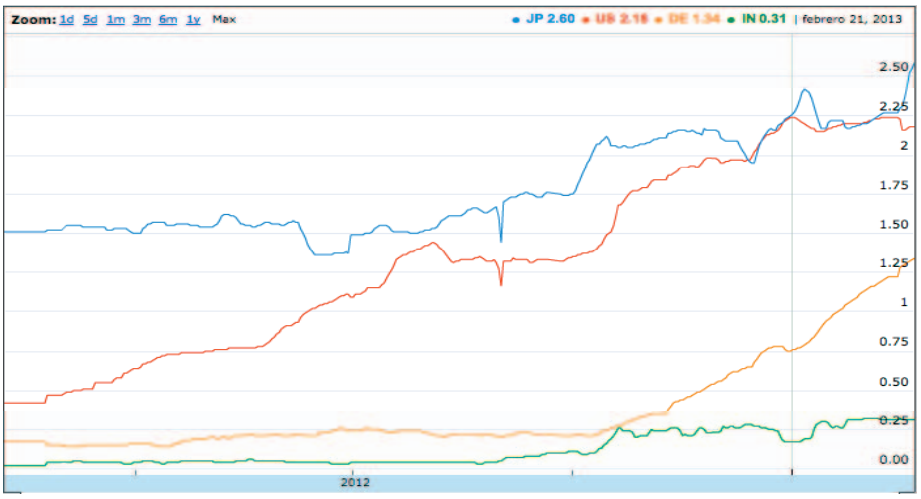


Figura 1. Porcentaje de usuarios que acceden a Google por IPv6 en Japón, Estados Unidos, Alemania e India.

> “En lo que se refiere a Espanix, situado en Madrid, el nodo neutro dispone de infraestructura y direcciones para el intercambio nativo de tráfico IPv6, que ya está siendo explotado por algunos de sus más de 60 miembros”

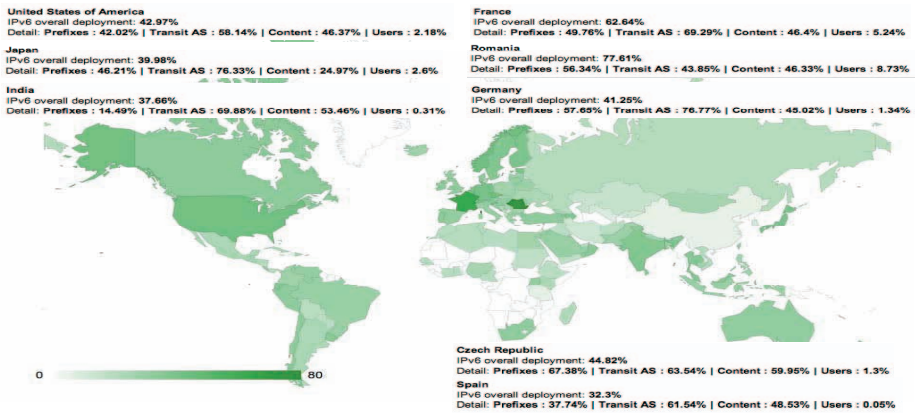


Figura 2. Porcentaje de contenidos, redes y usuarios IPv6 por país. (Fuente: Cisco Systems).

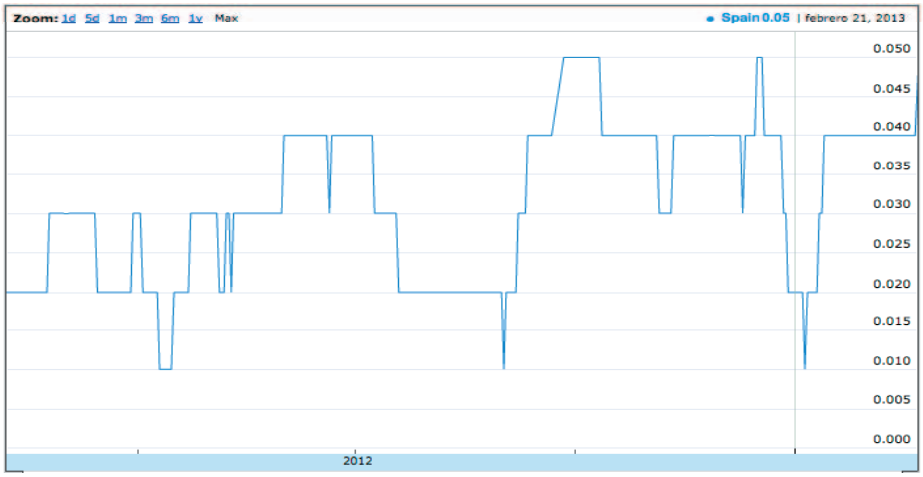


Figura 3. Porcentaje de usuarios IPv6 en España.

2.2 AMS-IX

En el caso de este nodo, mostramos en la **figura 5** la estadística anual respecto de IPv6 en la que puede observarse un fuerte incremento hasta septiembre y a partir de ahí una estabilización entre 3,5 y 4,5 Gbps.

3. Tráfico en las redes de distribución de contenido (CDNs)

Las redes de distribución de contenidos (CDNs) están constituidas por un conjunto de servidores en distintos puntos de Internet e interconectados entre sí que almacenan una serie de contenidos para su distribución eficiente y fiable a los usuarios finales.

En este artículo nos centramos en las estadísticas de tráfico que publica la CDN Akamai[3]. Las estadísticas de transacciones (*hits*) IPv6 de Akamai, de antes, durante y después de las jornadas mundiales de ISOC (junio de 2011 y junio de 2012), nos muestran fuertes crecimientos que se mantienen en el tiempo.

Hasta ahora, estos incrementos se han debido principalmente a la adaptación de contenidos, que han empezado a ser consumidos por los usuarios de ISPs con despliegues anteriores o programados para estas jornadas mundiales.

Sin embargo, a partir de junio de 2012, dado que los contenidos que generan la mayor parte del tráfico se han adaptado ya, el principal factor influyendo estas estadísticas es el crecimiento de usuarios que pueden consumir los contenidos debido a los despliegues de los operadores.

Como puede verse en la **figura 7** y su comparación con la **figura 6**[4], el número de transacciones sigue disparándose, por lo que podemos concluir que está produciéndose ya un incremento notable en el número de usuarios a nivel mundial.

4. Actividades de algunos de los ISP que operan en España

Tal y como se refleja en los diagramas con estadísticas por país que hemos presentado anteriormente, el despliegue de IPv6 en España (en lo que se refiere a usuarios finales) es todavía considerablemente bajo. No obstante, hay ciertas señales, resultantes de actividades concretas, que nos permiten ser optimistas en cuanto al posible crecimiento a medio plazo.

En esta sección, repasamos las actividades de algunos de los ISP (*Internet Service Providers*) que operan en España, expuestas a través de los autores de este artículo, quienes han participado en proyectos de IPv6 en dichos proveedores.

La mayor parte de la información ya ha sido proporcionada anteriormente, a través de notas de prensa u otros artículos técnicos, pero merece la pena presentarla de forma conjunta y actualizada para conocer en detalle el estado del arte.

Asimismo, no están todos los actores que operan en España, pero sí se incluye una muestra suficientemente representativa y variada que permite hacer extrapolaciones al conjunto nacional.

4.1. BT

A través de su filial BT España, BT centra sus operaciones en nuestro país en el segmento corporativo de acceso fijo, en el que ya dispone de oferta comercial IPv6[5]. Se trata de un servicio en el contexto de una oferta disponible en un ámbito mayor, concretamente a nivel EMEA (*Europe, Middle East and Africa*).

Como parte de este servicio, los clientes actuales reciben prefijos estáticos de una longitud comprendida entre 40 y 64 bits. Adicionalmente, se prestan servicios de *hosting* IPv6, similares a los que se ofrecen en IPv4.

Actualmente, BT España es uno de los miembros con interconexión IPv6 nativa (*peerings*) en Espanix.

> “Las estadísticas de transacciones *(hits)* IPv6 de Akamai, de antes, durante y después de las jornadas mundiales de ISOC (junio de 2011 y junio de 2012), nos muestran fuertes crecimientos que se mantienen en el tiempo”

4.2. Colt

Colt Technology Services opera en el ámbito de acceso corporativo fijo, con una cobertura de 13 países en Europa que incluye puntos de presencia en más de 40 ciudades.

En este ámbito, se han realizado proyectos específicos de servicio IPv6 a clientes. No obstante, se ha planificado abrir el servicio a todo tipo de proyectos, como una característica estándar más, durante el año 2013 a nivel europeo, incluyendo ciudades como Madrid, Barcelona y Valencia.

Actualmente, el servicio beta cuenta con más de 20 clientes corporativos en Europa, de los cuales tres están en España. El servicio de acceso a Internet sin *router* gestionado (“*wires-only*”) tiene previsto lanzarse a finales de 2012 o principios de 2013.

Respecto a los detalles de implementación técnica, Colt apuesta por una oferta nativa en modo *dual-stack* mediante los protocolos 6PE (RFC 4798) y 6VPE (RFC 4659), tanto para el acceso a Internet como para el servicio VPN sobre MPLS.

Por último, Colt es miembro de Espanix y dispone de interconexiones nativas en dicho nodo, además de interconexiones nativas en otros intercambiadores relevantes como son AMS-IX, BNIX, DECIX, France-IX, LINX, MIXITA, NYIIX, SFINX, SwissIX y VIX.

4.3. Euskaltel

Euskaltel es un proveedor que opera en el País Vasco tanto en acceso móvil donde cuenta con unos 270.000 usuarios, como en acceso fijo donde alcanza 280.000 usuarios en el área residencial y 90.000 usuarios corporativos, aproximadamente.

Hasta ahora, las pruebas de Euskaltel se han centrado en pruebas de campo en el segmento corporativo de acceso fijo, donde la solución proporcionada es nativa (sin túneles) en modalidad *dual-stack* (IPv4+IPv6). El planteamiento de Euskaltel es el de asignación de prefijos /48 a los clientes corporativos.

En lo que se refiere a los accesos fijos residenciales, se han realizado pruebas sobre accesos DOCSIS 3.0 con modalidades 6RD (*IPv6-Rapid-Deployment*) y *dual-stack*, principalmente en el marco de proyectos de innovación.

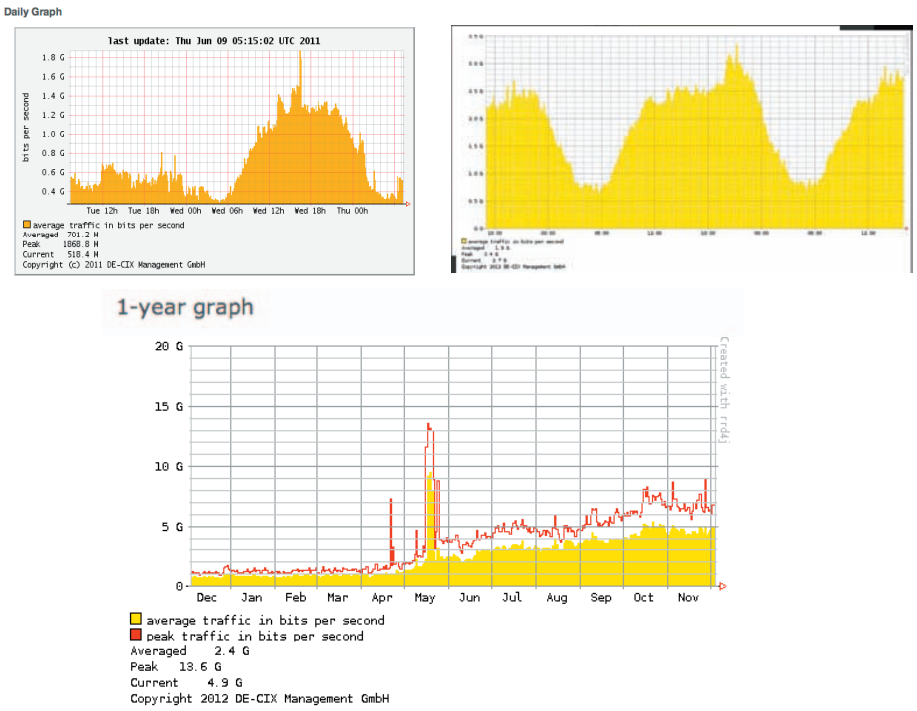


Figura 4. Estadísticas de tráfico IPv6 en DE-CIX.

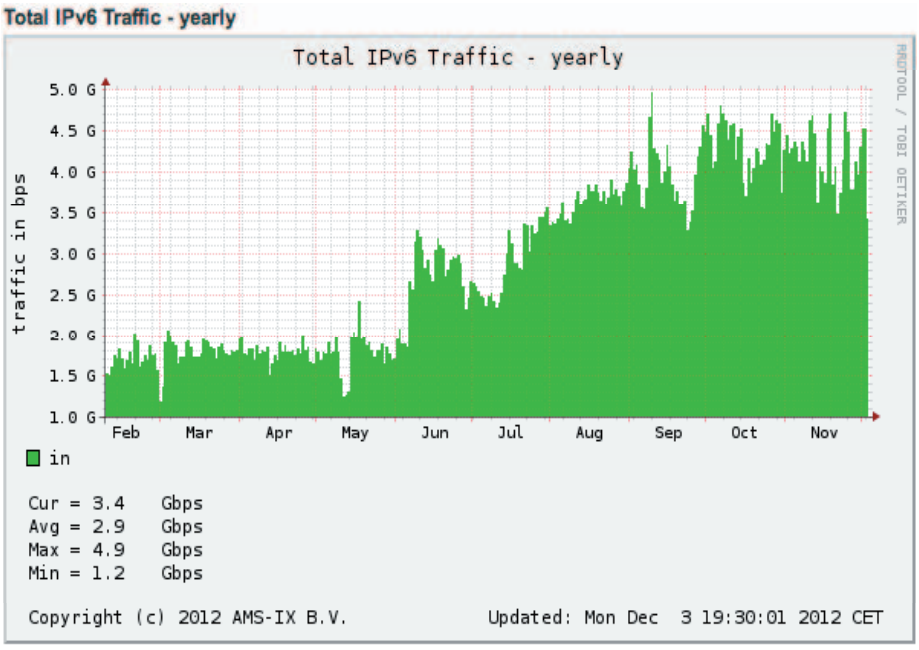


Figura 5. Estadísticas de tráfico IPv6 en AMS-IX.

Adicionalmente, tiene el objetivo de extender estas pruebas a los protocolos DS-Lite y MAP en la medida en que comiencen a estar disponibles versiones de software para cable-módem que soporten los mismos.

Asimismo, se prevé participar en proyectos de investigación que consideren 6LowPAN, el IPv6 de las redes de sensores, para explorar su potencial en las redes de hogar.

> “El despliegue de IPv6 en España (en lo que se refiere a usuarios finales) es todavía considerablemente bajo. No obstante, hay ciertas señales, resultantes de actividades concretas, que nos permiten ser optimistas en cuanto al posible crecimiento a medio plazo”

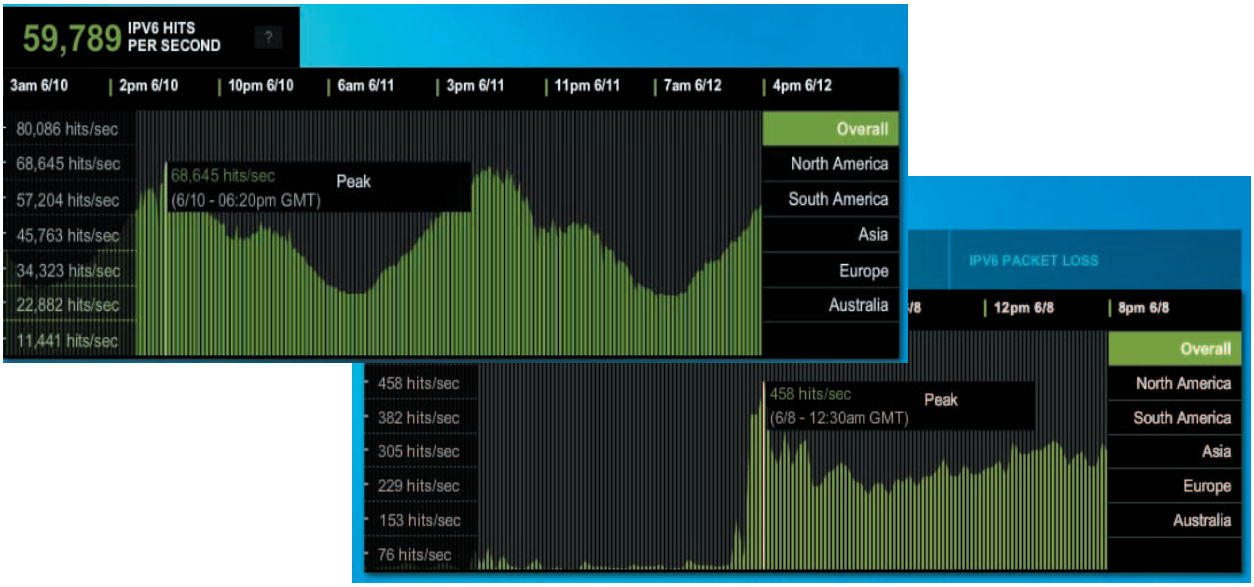


Figura 6. Transacciones IPv6 de Akamai en junio de 2012 (superior) y junio de 2011 (inferior).

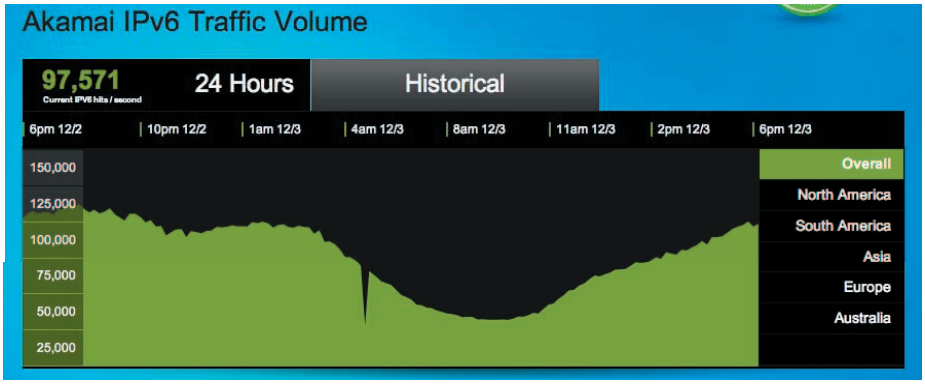


Figura 7. Transacciones IPv6 de Akamai en diciembre de 2012.

4.4. Jazztel

Jazztel es un operador nacional, con infraestructura propia en España, y actualmente emplea tecnología ADSL2+ y VDSL 2 . Ofrece soluciones de banda ancha para el tráfico de voz, datos, Internet y telefonía móvil destinadas al mercado residencial y de empresas. La compañía acaba de anunciar un despliegue de fibra óptica que llegará hasta tres millones de hogares.

Dentro del segmento residencial de acceso fijo, Jazztel ya ha lanzado un piloto reducido de ADSL IPv6 nativo en modo *dual-stack* en el que se delega un prefijo IPv6 de hasta 56 bits por cliente, lo que permitirá abrir hasta 256 subredes de 64 bits en cada hogar. La compañía tiene previsto comenzar a ofrecer el servicio a lo largo de 2013.

La solución adoptada se basa en el protocolo estándar 6VPE y la red se encuentra ya completamente adaptada para ofrecer el servicio.

Además, Jazztel es miembro de Espanix y Catnix donde ofrece conexiones nativas IPv6 a todos sus integrantes, así como en los puntos neutros internacionales de Ámsterdam (AMS-IX) y Londres (LINX).

Dentro del segmento corporativo está previsto tener una oferta de Tránsito BGP IPv6 a comienzos del próximo año.

4.5. Telefónica

En el segmento de acceso residencial fijo en España, se emplea principalmente tecnología ADSL y fibra óptica. En este campo, Telefónica ha lanzado en 2012, con motivo del W6LD, un piloto reducido de ADSL IPv6 nativo, en modo *dual-stack*, con usuarios finales a modo de “*beta-testers*”.

En este piloto se prueba actualmente una configuración en la que se asigna un prefijo IPv6 dinámico de 56 bits. Esta modalidad otorga direccionamiento público suficiente para 256 subredes estándar de 64 bits, que pueden albergar millones de terminales cada una.

En lo que se refiere a IPv4 se prueban dos configuraciones, una dirección pública dinámica por hogar, como en el servicio actual, y otra con dirección privada con traducción a nivel de operador (CG-NAT), anticipando un hipotético escenario de agotamiento total de direcciones IPv4 públicas, que obligaría a direccionar clientes totalmente con numeración privada.

En el segmento de acceso corporativo, Telefónica ha realizado pruebas a través de su filial Telefónica I+D, en sus sedes de Boecillo (Valladolid) y del parque tecnológico de Walqa (Huesca), donde se ha provisto conexión nativa a cada sede, que a su vez se distribuye de forma nativa en modo *dual-stack* a un centenar de puestos de trabajo aproximadamente desde la fecha del W6LD.

En el segmento de acceso móvil, Telefónica ha comunicado a través de la nota de prensa del W6LD'12 las primeras pruebas con terminales móviles en Méjico, con un único contexto PDP dual (IPv4+IPv6), sobre el que se asigna un prefijo dinámico estándar de 64 bits.

Respecto a otros despliegues y pilotos en otros países, Telefónica ha informado, asimismo con motivo del W6LD de este año, pilotos ADSL también en Perú.

4.6. Vodafone

Vodafone ha realizado extensas pruebas de IPv6 en Portugal donde opera tanto en acceso móvil y fijo como en los sectores residencial y corporativo.

En este país se estima lanzar la oferta comercial durante el próximo año 2013, si bien, a día de hoy, en el segmento residencial fijo ya hay usuarios finales que disponen de conexión nativa en modalidad *dual-stack* (IPv4+IPv6) desde hace un año aproximadamente.

En este mismo país, existe también un proyecto piloto en fase de pruebas de segmento corporativo de acceso fijo con características similares al servicio en producción y en el que se proporciona acceso *dual-stack* nativo (sin túneles) asignando prefijos /56.

En España, Vodafone es uno de los miembros de Espanix que intercambia tráfico nativo con otras redes a nivel nacional.

5. Conclusiones

A nivel mundial puede constatarse finalmente una tendencia creciente en la provisión de IPv6 a los usuarios finales, que comenzarán a consumir los contenidos que se han hecho disponibles a partir del W6LD.

El liderazgo de esta tendencia lo ostentan sin duda los operadores norteamericanos que, sin embargo, fueron los últimos en incorporarse activamente a la escena IPv6.

En Europa, países como Francia o Rumania han tomado el liderazgo muchas veces a través de operadores no incumbentes y en países como Alemania, el operador incumbente Deutsch Telekom ha comenzado el despliegue que puede apreciarse ya en las estadísticas de accesos IPv6 de Google.

En España, la mayor parte de los operadores han realizado pruebas y existen proyectos piloto desplegados, a veces directamente en nuestro país y otras veces en otras regiones. Es previsible que la experiencia y resultados en dichas regiones influirá positivamente en los despliegues. Se apunta a 2013 como año clave.

Es importante seguir monitorizando las estadísticas proporcionadas por agentes como Google o en el propio nodo Espanix (a día de hoy no ofrece esta posibilidad) para determinar cuando se supera en España la cota del 1% , hecho que ya ha ocurrido en Estados Unidos, Japón, y otros países europeos como Alemania, Chequia, Francia, Luxemburgo, Rumanía y Suiza.

Notas

[1] Para el lector interesado, en la siguiente referencia se puede obtener la lista y detalles de los mayores puntos de intercambio existentes: <http://en.wikipedia.org/wiki/List_of_Internet_exchange_points_by_size>.

[2] Para el lector interesado, la siguiente referencia describe las principales CDN y su aproximación concreta: <http://www.cdnreviews.com/major-cdns-overview/>.

[3] El lector puede observar cómo en junio de 2012 (figura 6) el número de transacciones IPv6 por segundo oscilaba aproximadamente entre 30.000 y 70.000 según la hora del día, mientras que en diciembre del mismo año (figura 7) la oscilación se producía entre 50.000 y 125.000 transacciones IPv6 por segundo.

[4] Disponible en <http.//ipv6.bt.com>.

Miguel González Fernández
Consultor y Technical Leader en SATEC

<miguel.gonzalez@satec.es>

Despliegue en las empresas y redes corporativas: La visión de un integrador

Resumen: *El agotamiento del direccionamiento IPv4 es una realidad que ha provocado la necesidad de comenzar a implementar IPv6. Las empresas no basan su negocio en IPv4, pero sí que se ven afectados por los problemas que puede suponer una pérdida de conectividad. En este artículo se analiza la necesidad y el impacto de implantar IPv6 en las diferentes infraestructuras de una empresa. También se proporciona una visión sobre cuáles serían las claves para una implantación exitosa de IPv6.*

Palabras clave: *Agotamiento IPv4, claves para la implantación, impacto de la migración, implantación IPv6, servicios en IPv6.*

Autor

Miguel González Fernández es Ingeniero de Telecomunicaciones por la Universidad Politécnica de Madrid (UPM) y CCIE #25851. Ha desarrollado su carrera profesional en la multinacional SATEC, donde lleva trabajando más de doce años. Durante este periodo ha realizado tareas de consultoría, diseño e implantación de redes, tanto en el ámbito corporativo como en el de operadora. Actualmente desempeña las funciones de consultor y *technical leader* en el área de comunicaciones y seguridad de SATEC.

1. Introducción

Aunque se viene hablando desde hace años del problema de agotamiento de las direcciones IPv4, específicamente desde que se empezó a desarrollar el nuevo protocolo IPv6, no ha sido hasta los dos últimos años cuando el problema ha empezado a ser conocido por el gran público en general. Dentro de este público se encuentran gestores y directores de empresas de diverso tamaño, que miran hacia las integradoras y nos realizan las preguntas típicas:

- ¿El agotamiento de IPv4 me afecta a mí o a mi empresa?
- ¿Puedo continuar utilizando IPv4?
- ¿Qué tengo que hacer para implementar IPv6?
- Y por supuesto, la pregunta clave: ¿cuánto me va a costar y qué beneficio voy a obtener de ello?

La primera de las preguntas se puede responder directamente con un rotundo sí. El pasado 14 de septiembre RIPE NCC[1] alcanzó su último /8 [1], entrando en la fase III sus políticas de asignación de direcciones: únicamente asignará un /22 a cada LIR[2] de ese /8, y siempre y cuando haya solicitado previamente un prefijo de IPv6 [2]. El objeto de esos /22 es poder garantizar mecanismos de transición a todos los LIR. Pero evidentemente estos prefijos son insuficientes para que las operadoras asignen direccionamiento a sus usuarios, por lo que tendrán que implementar técnicas de CGN[3] e IPv6.

Así mismo, desde el día 6 de junio de 2012 [3] grandes portales de contenidos habilitaron definitivamente *dual stack*. Entre ellos se encuentran gigantes como Google, Facebook, Yahoo o Microsoft. Lo que viene a significar que el avance de IPv6 es imparable.

Las estadísticas de tráfico cursado mediante IPv6 aumentan día a día, aunque de momento no sean muy elevadas. Como ejemplo en algunos puntos de intercambio de tráfico [4] se puede observar que el tráfico en IPv6 se ha triplicado desde el día 6 de junio de 2012 y cerca del 1% del tráfico que accede a Google ya es IPv6 [5]. Ambos tráficos tienen una clara tendencia alcista.

Con todo esto queremos decir que si Internet se está moviendo hacia IPv6, nuestras empresas no pueden ser ajenas a esta realidad, y tendrán que tomar los pasos necesarios para garantizar que no van a tener problemas de conectividad en el futuro.

Para poder responder al resto de preguntas hay que tener primero en cuenta cual es el núcleo de actividad de una empresa. Una empresa de telecomunicaciones se centra en proporcionar servicios de conectividad, en particular servicios de conectividad de red donde se enmarcan IPv4 e IPv6, mientras que otro tipo de empresas pueden centrar su negocio en cualquier campo que no tenga absolutamente nada que ver con las TIC, aunque utilicen a éstas como un medio de transporte, al igual que podrían usar una flota de camiones para transportar sus mercancías.

Una empresa o corporación apoyará su negocio en los servicios de red que le sirvan para transportar las aplicaciones que utiliza (ERPs - *Enterprise Resource Planning* -, portales de comercio electrónico, servicios de directorio, desarrollos a medida, correo electrónico, portales web, etc.). Se puede decir que la capa de la torre OSI (*Open Systems Interconnection*) que le importa principalmente a la empresa es la 7 ó capa de aplicación. Y para que esta capa funcione correctamente el resto de capas inferiores deben hacerlo igualmente.

En la **figura 1** se muestra la torre OSI ampliada, incluyendo los niveles no oficiales de *staff* y gestión. En ella se pretende mostrar que el impacto de implantar IPv6 es mayor a medida que se sube en ella:

- IPv6 es completamente transparente a la capa 1.
- En la capa 2 es prácticamente transparente, aunque hay algunas funcionalidades que tienen interacción entre capa 2 y capa 3 (tales como *IGMP snooping* o *MLD snooping*)
- En la capa 3 y 4 el impacto es moderado. Es en estas capas donde se sustituye IPv4 por IPv6. Pero hay que tener en cuenta que IPv6 no es más que otro protocolo de red, como en su día fueron CLNS, IPX o Appletalk.

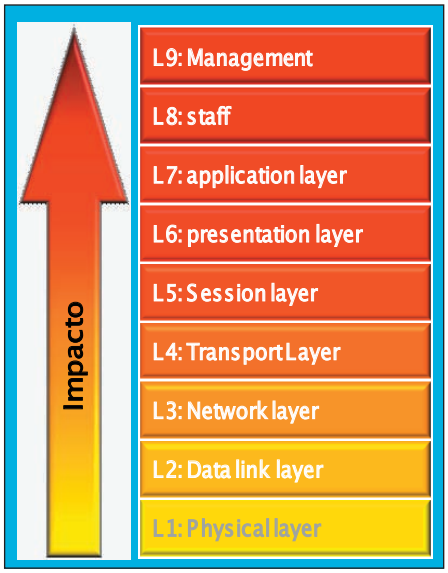


Figura 1. Torre OSI ampliada.

> “Si Internet se está moviendo hacia IPv6, nuestras empresas no pueden ser ajenas a esta realidad, y tendrán que tomar los pasos necesarios para garantizar que no van a tener problemas de conectividad en el futuro”

- De la capa 4 a la capa 7 el impacto ya es muy alto, sobre todo en aquellas aplicaciones que embeban direcciones dentro de su funcionamiento, como *web services* o telefonía IP.
- El impacto en las capas no oficiales es el más alto:
  - En la capa de staff es habitual encontrar una gran resistencia al cambio, que puede imposibilitar la transición de tecnología
  - En la capa de gestión es donde se toman las decisiones económicas, y puesto que IPv6 no presenta en un principio ningún retorno de inversión directo es complicado convencer a un gestor de que realice ninguna inversión en IPv6.

2. Estructura de servicios habitual en una empresa

Puesto que el foco de una empresa o corporación se basa en los servicios que proporciona, es conveniente realizar primero una catalogación de éstos. A continuación, realizaremos un análisis de las infraestructuras de comunicaciones, seguridad y sistemas que se utilizan en una empresa. A partir de estos análisis verificaremos cuál es el impacto de la migración de servicios a IPv6 en las diferentes infraestructuras y cuál es la necesidad real de migración para cada uno de los servicios catalogados.

Una posible catalogación podría estar basada en el tipo de cliente, su ubicación y la del recurso al que precisa acceder:

- Servicios a clientes internos que no precisan acceso a Internet:
  - Se presta a clientes internos de la organización.
  - La conectividad es interna a la organización.
  - No precisa acceso a Internet.
  - Ejemplos: ERP, CRM, portal interno, etc.
- Servicios a clientes internos que precisan acceso a Internet:
  - Son ofrecidos a clientes internos a la organización.
  - Precisan conectividad con Internet.
  - Ejemplos: Correo electrónico, navegación web, acceso remoto (SSL o IPSec), DNS, etc.
- Servicios externos a la organización:
  - Ofrecidos a clientes externos a la organización.
  - Precisan conectividad con Internet.
- Servicios de gestión:
  - Servicio interno a la organización
  - Son sistemas de apoyo a la producción: Gestionan la infraestructura de red y sistemas, y gestionan el puesto de trabajo.

El diagrama de la **figura 2** muestra una división en bloques de las diferentes infraestructuras involucradas en la prestación de los servicios anteriores, indicando cuáles de ellos son internos o externos a la empresa.

La descripción de cada uno de los bloques y el impacto de IPv6 en cada uno de ellos se describen a continuación.

2.1. Clientes internos

Empezando por abajo vemos que tenemos los clientes internos. Estos clientes pueden ser de cualquier tipo, desde un PC a un sensor, pasando por una impresora o un TPV (Terminal Punto de Venta). Son los dispositivos finales que van a hacer uso de un servicio como clientes.

El impacto en estos clientes vendrá determinado por:

- El sistema operativo, *middleware* o *firmware* que utilicen.
- Aplicativo usado.
- El volumen de clientes que exista.

Los dispositivos tipo PC normalmente no van a tener muchos problemas con el soporte de IPv6 en el sistema operativo. Si están basados en Windows, desde Windows XP está soportado IPv6, aunque en esa versión viene deshabilitado por defecto. A partir de Windows 7 IPv6, el sistema operativo preferirá siempre utilizar IPv6 antes que IPv4 en caso de disponer de conectividad utilizando las dos opciones.

Los sistemas de Linux tienen soporte de IPv6 desde versiones bastante antiguas de su *kernel*, aunque dependiendo de la distribución particular el módulo de IPv6 estará cargado en el sistema o habrá que hacerlo explícitamente.

El problema aparece en otros dispositivos, que generalmente no estarán pensados para trabajar en IPv6.

Aparte, aunque un dispositivo se pueda actualizar a IPv6, habrá que tener en cuenta su número. Si éste es muy elevado y la actualización no se puede realizar por medios automáticos el coste puede ser muy grande.

Adicionalmente, hay que tener en cuenta el riesgo que conlleva cambiar de protocolo, porque pueden aparecer errores en el software del dispositivo que no existían cuando se utilizaba el que sólo soportaba IPv4.

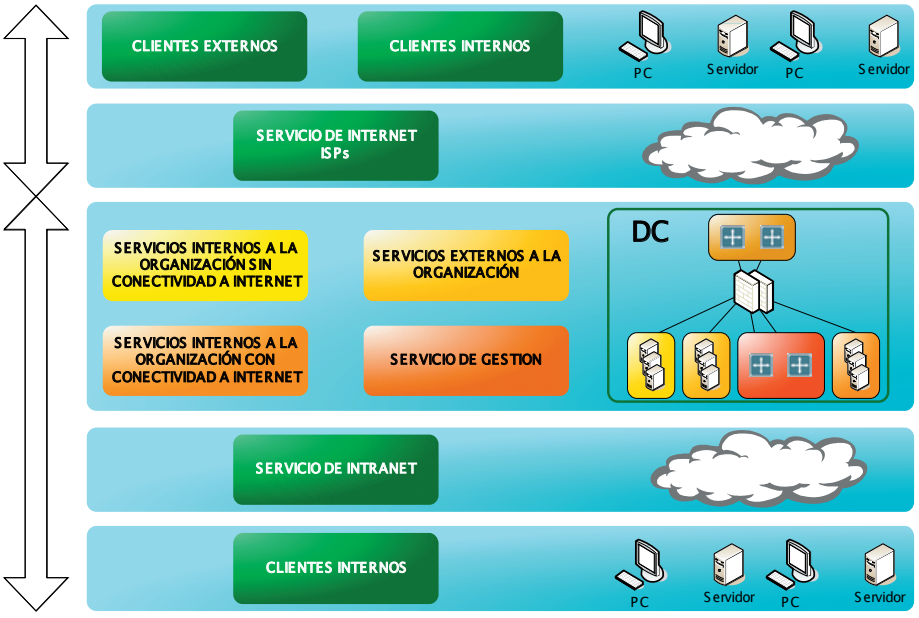


Figura 2. Infraestructuras involucradas en la prestación de los distintos servicios.

> “Conectarse a un operador que tenga soporte IPv6, no garantiza que se tenga conectividad IPv6 con los posibles clientes externos. Para que esto ocurra, éstos deben tener acceso también al servicio de Internet IPv6”

2.2. Servicio de Internet

En una corporación que dispone de varias sedes se utiliza un servicio de Intranet para poder establecer comunicación entre ellas. Las formas habituales de construir esta Intranet se muestran en la **figura 3**.

La responsabilidad de proporcionar IPv6 en el servicio de Intranet dependerá en mayor medida del operador o de la propia empresa dependiendo del modelo que se utilice.

Así, si la Intranet está completamente externalizada será el operador el que se encargue de proporcionar el servicio, siendo transparente para la empresa ese proceso de migración.

Si la empresa tiene un punto de demarcación de nivel 3, entonces estará obligada a actualizar sus elementos de comunicaciones fronteras a IPv6. Si el operador no soporta IPv6, deberá utilizar tecnologías *overlay* (GRE, IPv6oIP, 6rd, etc…) para transportar el tráfico IPv6 sobre la red IPv4. Otra alternativa que siempre existe es utilizar otro operador que sí proporcione soporte IPv6.

Si el operador únicamente proporciona servicios de niveles 1ó 2, la responsabilidad completa de la implantación de IPv6 en la Intranet recae en la empresa, que se tendrá que encargar de actualizar sus dispositivos a IPv6. La red del operador debiera ser transparente al protocolo de red que la empresa utilice.

2.3. Servicios de *Data Center*

En los *Data Center* hay que tener en cuenta por un lado las infraestructuras de comunicaciones y seguridad, y por otro lado las infraestructuras de sistemas.

Dependiendo del grado de actualización del software de las infraestructuras de comunicaciones y seguridad, éstas tendrán más o menos funcionalidades de IPv6.

Actualmente, si el hardware no es obsoleto, la probabilidad de que estas infraestructuras tengan soporte de IPv6 es muy alta.

En cuanto a las infraestructuras de sistemas, los sistemas operativos que se utilizan frecuentemente en los servidores tienen soporte de IPv6 (Windows 2008, Red Hat, Solaris, etc.). Pero que el sistema operativo soporte IPv6 no implica que los aplicativos que se estén utilizando sí proporcionen dicho soporte.

2.4. Servicio de Internet

La principal limitación para que este servicio soporte IPv6 es que el ISP soporte IPv6.

Aunque pueda parecer que el grado de implantación de IPv6 actual en las operadoras es bajo, porque no se publicite abiertamente, muchas de ellas ya disponen de conectividad IPv6 con *carriers*, y aunque sus redes no estén adaptadas para proporcionar el mismo catálogo de servicios en IPv6 que en IPv4, es posible que puedan ofertar sin problemas el servicio de conectividad IPv6 con Internet.

Pero conectarse a un operador que tenga soporte IPv6, no garantiza que se tenga conectividad IPv6 con los posibles clientes externos. Para que esto ocurra, éstos deben tener acceso también al servicio de Internet IPv6. Y esta circunstancia ya no depende en absoluto de la empresa. Éste es uno de los motivos por los que se recomienda no proporcionar servicios únicamente en IPv6, ya que clientes potenciales pueden no tener acceso a ellos y la empresa no dispondría de ninguna capacidad para solventar esa falta de conectividad.

2.5. Clientes externos

Otro grado de incertidumbre se centra en los dispositivos que utilicen los clientes externos para conectarse a los servicios ofrecidos por la empresa. Al igual que con los clientes internos, esos dispositivos deberán tener versiones de sistemas operativos que permitan la utilización de IPv6. La empresa en teoría tiene el control de los dispositivos que actúan como clientes internos, pudiendo forzar su actualización. En el caso de los clientes externos, la empresa no tiene ninguna clase de control sobre ellos, por lo que no va a poder garantizar en ningún caso que todos tengan acceso a los servicios de la empresa por IPv6. Este es otro motivo para proporcionar estos servicios con *dual stack*.

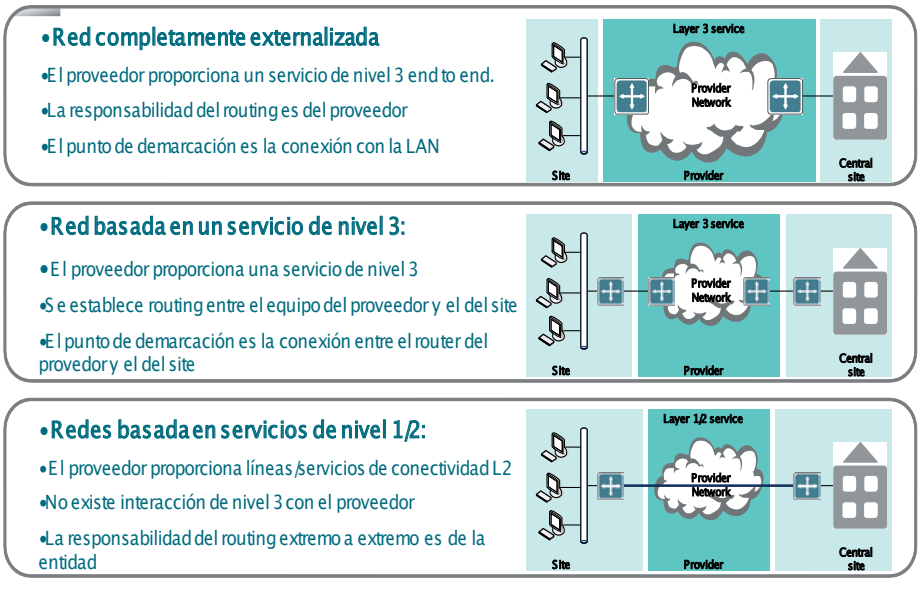


Figura 3. Distintos modelos para proporcionar el servicio de Intranet en una empresa.

3. Análisis de impacto

Una vez definidos los diferentes servicios y las infraestructuras necesarias para prestarlas analizaremos el impacto de migrar cada servicio a IPv6 y la necesidad real de hacerlo.

3.1. Servicios internos a la organización sin conectividad a Internet

Es raro encontrar una organización que utilice direccionamiento público IPv4 en los dispositivos finales. Uno de los motivos es un factor de coste: o bien la empresa se convierte en LIR o *Direct Assignment User* y abona anualmente una cuota [6], o bien le pide ese direccionamiento a un ISP, que se lo facturará de forma correspondiente.

Si un servicio es interno a la organización, implica que no tiene necesidad de conectarse a Internet. Consecuentemente no se verá afectado por el problema de agotamiento de

direcciones IPv4, que es el principal motivo de migración a IPv6. Entonces, únicamente en casos excepcionales sería necesaria esta migración a IPv6. Además, los aplicativos en los que se basan la mayoría de estos servicios suelen o bien ser desarrollos a medida, o desarrollos estándar personalizados para la propia empresa. Esto conlleva una dificultad inherente para su migración a IPv6, ya que lo más probable es que cuando se desarrollaran no tuvieran en cuenta este protocolo.

Dentro de los casos excepcionales estaría la implantación de *smart grids*. Según la normativa española, todos los contadores eléctricos de los abonados podrán ser consultados en tiempo real en el 2018 [7]. Aunque se podría pensar en proporcionar este servicio utilizando direccionamiento privado IPv4, el número de estas direcciones es aproximadamente 17 millones, lo que puede resultar insuficiente para implementar una red de estas características. Por ello, una de las alternativas para la construcción de *smart grids* es la utilización de IPv6 como protocolo de transporte.

Pero en el caso de *smart grids* no estaríamos hablando de migración de infraestructuras y aplicaciones ya existentes, sino de implementación de un nuevo servicio con nuevas infraestructuras. Por lo tanto, lo habitual sería que el diseño se haya realizado teniendo en cuenta ya IPv6.

Resaltar finalmente, en referencia a los servicios internos, que aunque su evolución a corto plazo no se contemple, el desarrollo de nuevos servicios debería tener en cuenta obligatoriamente IPv6 dentro de sus requisitos de conectividad. Estos nuevos servicios deberían funcionar en los tres entornos posibles:

- Clientes IPv4 only.
- Clientes dual-stack.
- Clientes IPv6 only.

3.2. Servicios externos a la organización

Estos serían los servicios que se proporcionan a los clientes externos, yendo desde una simple página web corporativa, a webs de venta de productos, etc.

Para poder proporcionar este servicio primero la organización deberá ser accesible vía IPv6, por lo que el ISP debe ser capaz de proporcionar este servicio.

Las infraestructuras de comunicaciones del *Data Center* deben ser capaces también de soportar este protocolo. Entre otros:

- Routers de *peering*.
- *Firewalls*.
- IPS.
- Balanceadores.

Y la parte más importante, las aplicaciones utilizadas por los clientes externos deben ser accesibles por IPv6.

Normalmente las aplicaciones no son *stand-alone* (ver **figura 4**), sino que suelen estar basadas en interrelaciones de aplicaciones (bases de datos, servidores de presentación y aplicación, almacenamiento, etc.).

Migrar estas interrelaciones a IPv6 no es trivial, ya que no sólo afectan a la comunicación entre los diferentes servidores, sino que pueden impactar en el modelo de datos que utilizan: en algunos casos se almacenan o se utilizan direcciones IPv4. Pasar a utilizar indistintamente direcciones IPv4 o IPv6 puede suponer cambios en el código sustanciales.

Por lo tanto, la recomendación en estos servicios sería hacer visible por IPv6 al servidor *front-end*. Esto se podría lograr de dos formas:

- Implantando IPv6 en el servidor *front-end* para la comunicación con clientes externos, que hablaría en IPv4 ó IPv6 con los clientes y en IPv4 con el resto de servidores internos
- Utilizando un *proxy* inverso de aplicación, al que le llegarían las peticiones por IPv6 y las transformaría en IPv4.

El camino más sencillo, siempre que la aplicación lo permita, es la utilización de *proxies* inversos. En algunos casos ya se estarían utilizando, como en el de una granja de servidores que se encuentran detrás de un balanceador de aplicaciones. Éste presenta una dirección IPv4 virtual contra la que se conectan los clientes, y cuando uno de ellos quiere establecer una transacción decide contra qué servidor real se establece la sesión. Estos balanceadores podrían presentar también una dirección IPv6 virtual a los clientes externos, y seguir estableciendo la conectividad con los servidores físicos utilizando IPv4.

Al igual que con los servicios internos, cualquier nuevo servicio externo que se plantee debe contemplar IPv6 desde el principio para evitar problemas de compatibilidad en un futuro.

3.3. Servicios a clientes internos con conectividad a Internet

Anteriormente, hemos visto que no tiene mucho sentido migrar a IPv6 la Intranet en un primer momento. Pero si no se realiza esta migración es necesario proporcionar una solución para que los clientes internos se puedan conectar a Internet.

Actualmente la conectividad de los clientes internos con Internet se suele realizar de dos formas:

- Utilizando NAT.
- Mediante servidores intermedios (como el del correo electrónico) o *proxies*.

La primera opción no es una alternativa, puesto que la traducción de IPv4 a IPv6 no está plenamente desarrollada.

La segunda opción es la más sencilla y la que más se utiliza en las empresas, ya que proporciona un mayor control y seguridad sobre la navegación de los usuarios.

Al utilizar un servidor intermedio o un *proxy dual-stack*, los clientes internos van a realizar siempre la navegación por IPv4, y será el *proxy* el que navegue utilizando IPv4 o IPv6 dependiendo de la resolución DNS del *host* destino.

Los elementos afectados en este caso serían:

- El servicio de Internet.
- Equipamiento externo del *Data Center*:
  - Firewalls.
  - IPS.
  - Proxy.
  - etc.

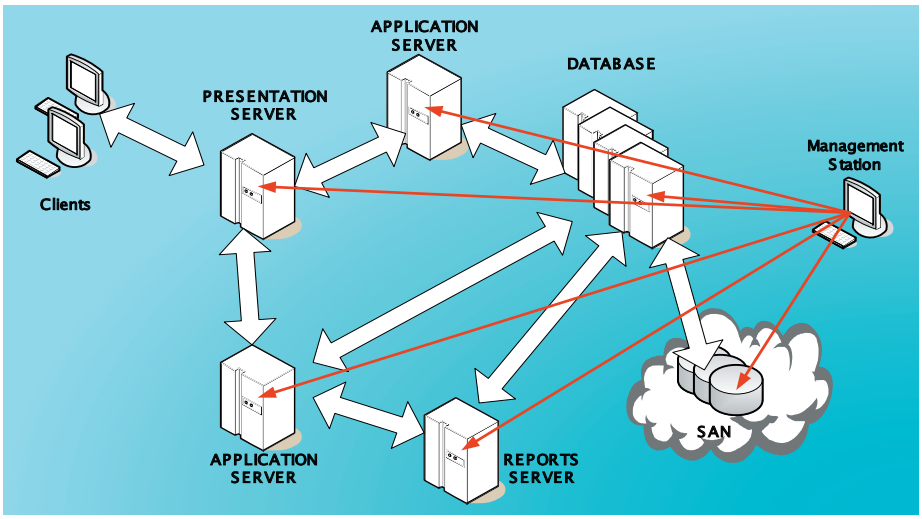


Figura 4. Esquema de las interrelaciones habituales entre componentes de las aplicaciones ofrecidas a clientes externos.

> “ IPv6 no es ni más ni menos seguro que IPv4: para casi todos los ataques basados en IPv4 existe un ataque similar en IPv6. Aunque sí que se puede decir que hay un ataque que ha desaparecido en IPv6 que es el escaneo de direcciones ”

- Proxy de navegación.
- Servidores intermedios.
- DNS.

3.4. Servicios de gestión

En este punto se pueden distinguir dos ámbitos de gestión, el del puesto de trabajo y el de las infraestructuras de comunicaciones y sistemas.

Ambos tipos de gestión son servicios internos a la empresa, y como tales no debieran tener acceso a Internet. Esta situación les excluiría en un primer momento de la necesidad de realizarse mediante IPv6.

La necesidad real de gestionar dispositivos mediante IPv6 no vendrá marcada por si éstos utilizan este protocolo, sino más bien por si no utilizan IPv4. Si un dispositivo utiliza IPv4 podrá ser interrogado utilizando este protocolo para obtener parámetros de IPv6.

Por lo tanto, inicialmente no sería necesario contemplar la migración de los servicios de gestión a IPv6. Si bien habrá que vigilar que todos los elementos gestionados con capacidades IPv6 sean capaces de enviar información acerca del uso de este protocolo.

3.5. Implicaciones de seguridad

IPv6 no es ni más ni menos seguro que IPv4: para casi todos los ataques basados en IPv4 existe un ataque similar en IPv6. Aunque sí que se puede decir que hay un ataque que ha desaparecido en IPv6 que es el escaneo de direcciones, puesto que el direccionamiento de *host* en redes LAN se basa en 64 bits y es virtualmente imposible escanear una red.

La diferencia entre unos ataques y otros estriba en la disponibilidad de formas de mitigar o bloquear esos ataques, sobre todo en redes de nivel 2. En IPv4 estas técnicas llevan disponibles desde hace mucho tiempo, mientras en IPv6 las técnicas similares únicamente están disponibles en las últimas versiones de software de los últimos modelos (recomendamos consultar la presentación de Eric Vincke sobre seguridad de IPv6 en entornos de nivel 2 [8] que realizó en RIPE 65 [9]).

Aunque estos ataques se vean lejanos en una empresa que no tiene implantado oficialmente IPv6, es muy importante tener en cuenta que es muy probable que esa empresa ya esté utilizando IPv6, aunque sea de forma inadvertida.

Windows 7 tiene habilitado IPv6 *out-of-the-box*. Esto no es en sí un problema, pero sí que implemente túneles IPv6 sobre IPv4 por defecto, como son ISATAP, 6to4 y Teredo. Este tipo de túneles pueden proporcionar conectividad con Internet IPv6 saltándose reglas de los *firewalls*, y lo que es peor, permitir que un atacante desde Internet tenga acceso a un dispositivo interno de la empresa sin ningún tipo de medidas de seguridad. Solucionar este problema es muy sencillo, siempre y cuando se sea consciente del mismo.

Adicionalmente, existen otros tipos de túneles IPv6 sobre IPv4 que proporcionan algunos organismos que pueden permitir a un usuario interno tener conectividad con Internet IPv6 sin ser controlado por los administradores de la seguridad de la empresa. Un ejemplo de este tipo de túneles es AYIYA[4] (*Anything in Anything*), que la organización SIXXS [10] proporciona para promocionar el uso de IPv6.

Por lo tanto, aunque se pueda pensar que IPv6 no afecta en nuestra empresa, es muy probable que ya lo esté haciendo. Aunque no se esté planteando su implantación, es obligatorio implementar las medidas de seguridad necesarias para controlar el uso inadvertido del mismo que puedan conllevar fallas de seguridad.

4. Conclusiones

La implantación de IPv6 en una empresa no viene motivada por factores de ingreso, ya que en estos momentos no existe ninguna aplicación que por estar basada en IPv6 vaya a aumentarlos. Todo lo contrario, implantar IPv6 supone básicamente un coste en el que se pueden contemplar los siguientes factores:

- Consultoría para definir el diseño y la estrategia de implantación. Esta tarea se puede realizar con servicios profesionales o con recursos propios, pero en ambos casos representa un coste.
- Renovación de hardware y software.
- Incorporación de nuevos elementos necesarios para la prestación de servicios en IPv6
- Costes de operación
  - Hay que adaptar los procesos de operación y mantenimiento para que contemplen el nuevo protocolo.
  - Es necesario adquirir conocimiento para dominar el nuevo protocolo.

Aunque IPv6 representa fundamentalmente un gasto, se pueden realizar algunas acciones para mitigar el impacto económico, como realizar una migración a largo plazo, minimizando riesgos y espaciando inversiones, o tratar de hacer coincidir renovaciones hardware y software con actualizaciones tecnológicas.

Por lo tanto, se impone definir una estrategia global para la implantación gradual de IPv6.

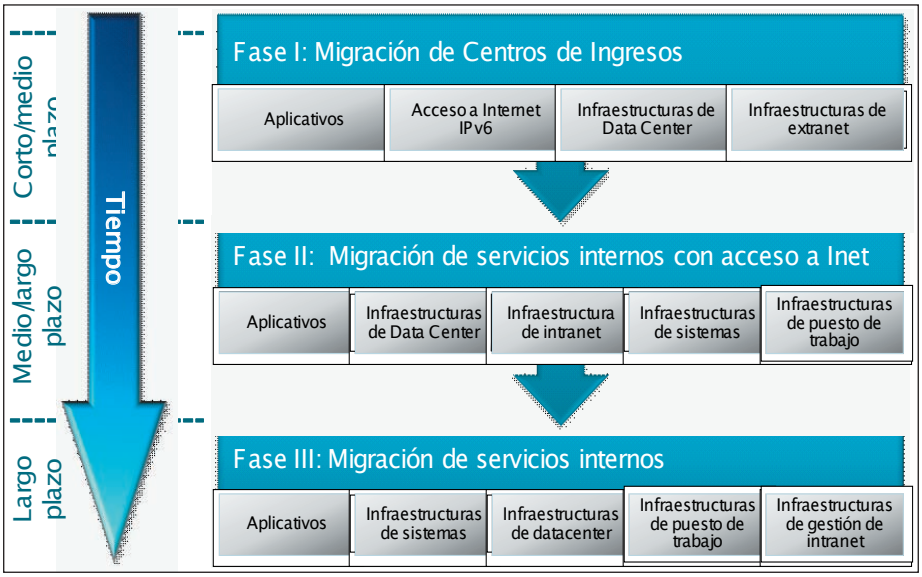


Figura 5. Estrategia para la implantación gradual de IPv6 en una organización.

> “El proyecto de implantación de IPv6 presenta muchas similitudes con el Y2K. Ambos tienen una problemática muy bien definida, el grado de impacto es inicialmente desconocido y es necesario un proceso de verificación de que las aplicaciones están adaptadas a la problemática”

En esta estrategia se definirían tres fases:

- Fase I: En la que se migrarían a IPv6 los centros de ingresos de la compañía, es decir los servicios externos que proporciona.
- Fase II: En la que se migrarían los servicios internos que precisan acceso a Internet.
- Fase III: Donde se migrarían los servicios internos que no precisan acceso a Internet.

La **figura 5** muestra los elementos que serían afectados en cada una de las fases, y los plazos que se contemplarían para cada uno de ellos.

Las claves para que este proceso de implantación se realice con éxito serían:

- Definir la estrategia global antes mencionada.
- Realización de un análisis exhaustivo de las capacidades de todos los elementos involucrados para el soporte de las diferentes funcionalidades IPv6.
- Definición de un plan de direccionamiento global orientado a la optimización de la información de *routing*, así como los procesos de operación y resolución de fallos.
- Realización de diseños orientados a una total implantación de IPv6, aunque ésta no vaya a ser inmediata, para evitar así costes innecesarios de adaptación en un futuro.
- Establecimiento de métricas y mecanismos para medir el grado de implantación de IPv6, tanto de forma interna como por parte de todas las entidades o clientes externos que se conecten a la empresa
- Establecimiento de un proceso formativo gradual para el personal de operación de sistemas y de red, con el objetivo de minimizar los tiempos de gestión y operación de la red.

El proyecto de implantación de IPv6 presenta muchas similitudes con el Y2K. Ambos tienen una problemática muy bien definida, el grado de impacto es inicialmente desconocido y es necesario un proceso de verificación de que las aplicaciones están adaptadas a la problemática. La diferencia entre los dos estriba en que en el caso del Y2K la fecha límite estaba muy clara, y en el caso de IPv6 esa fecha es más bien difusa. Pero que sea difusa no quiere decir que nos podamos a relajar y pensar que nunca va a llegar. IPv6 ya está funcionando y es fundamental que las empresas vayan pensando en la estrategia para su implantación.

Referencias

[1] RIPE Network Coordination Center. *IPv4 Exhaustion*. <http://www.ripe.net/internet-coordination/ipv4-exhaustion>.

[2] RIPE Network Coordination Center. *IPv4 Address Allocation and Assignment Policies for the RIPE NCC Service Region (Use of last /8 Allocations)*. <http://www.ripe.net/ripe/docs/ripe-553#-----use-of-last-8-for-pa-allocations.com>.

[3] World IPv6 Launch. <http://www.worldipv6launch.org/participants/?q=1>.

[4] Amsterdam Internet Exchange (AMS-IX). IPv6 Traffic. <https://www.ams-ix.net/technical/statistics/sflow-stats/ipv6-traffic>.

[5] Google. *IPv6 Adoption*. <http://www.google.com/ipv6/statistics.html>.

[6] RIPE Network Coordination Center. *RIPE NCC Billing Procedure and Fee Schedule for LIRs 2012*. <http://www.ripe.net/lir-services/member-support/info/billing/billing-procedure-and-fee-schedule-for-lirs-2012/ripe-ncc-billing-procedure-and-fee-schedule-for-lirs-2012>.

[7] BOE. ORDEN ITC/3860/2007, de 28 de diciembre. *Disposición adicional primera. Plan de sustitución de equipos de medida*. <http://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-22458>.

[8] Eric Vyncke. *The Layer-2 Security Issues and the Mitigation Techniques*. <https://ripe65.ripe.net/archives/video/179/>.

[9] RIPE Meeting 65. <https://ripe65.ripe.net/>.

[10] SixXS. *IPv6 Deployment & Tunnel Broker*. <http://www.sixxs.net/>.

Notas

[1] *Reseaux IP Europeens Network Coordination Center*.

[2] *Local Internet Registry.*

[3] El NAT masivo, conocido también como NAT a gran escala (*large-scale NAT*, o LSN) o *Carrier-grade NAT* (CGN), es una herramienta de diseño de redes IPv4 donde los extremos de la comunicación, en concreto, las redes residenciales, se configuran con direcciones de red privadas, que se traducen a direcciones públicas mediante equipos de traducción que se interponen dentro de la red del proveedor entre el usuario e Internet. Estos dispositivos permiten compartir conjuntos pequeños de direcciones públicas entre muchos puntos finales. <http://es.wikipedia.org/wiki/Carrier_Grade_NAT>.

[4] <http://en.wikipedia.org/wiki/Anything_In_Anything>.

IPv6: Internet Society y la visión de los usuarios

Josu Aramberri
Vicepresidente del Capítulo Español de Internet Society (ISOC-ES)

<jaramberri@i2basque.es>

Resumen: *Internet Society (ISOC) es uno de los principales promotores de la transición a IPv6. Se inquieta por el lento despliegue del nuevo protocolo, y por el efecto que esto puede tener en la sociedad y los usuarios. Y actúa con la organización de eventos para dinamizar el cambio: World IPv6 Day en 2011 y World IPv6 Launch en 2012. También mantiene una campaña contínua de formación y asesoramiento con el programa Deploy360. El capítulo español ISOC-ES y las redes académicas han tomado ese testigo en nuestro país. Este artículo muestra los avances y las experiencias en los dos últimos años.*

Palabras clave: *Carrier Grade NAT, Content Delivery Networks, Deploy 360, DNSSEC, Internet Society, IPv6, ISPs, RedIRIS, World IPv6 Day, World IPv6 Launch.*

Autor

Josu Aramberri es Licenciado en Ciencias Físicas y Doctor en Informática. Es profesor de la Universidad del País Vasco/*Euskal Herriko Unibertsitatea* y coordinador de la Red Académica I2BASQUE <http://www.i2basque.es> que impulsa la existencia de infraestructuras regionales y el despliegue de servicios para los agentes de I+D+i en el País Vasco: redes de banda ancha sobre fibra óptica, IPv6, cálculo intensivo (GRIDs), multimedia (videoconferencia IP, *streamings* de video por Internet…), *eLearning,* y gestión de contenidos colaborativos basados en wikis. Es también patrono de la Fundación EuskoMEDIA de *Eusko Ikaskuntza* <http://www.euskomedia.org>, y vicepresidente del Capítulo español de la *Internet Society* - ISOC-ES <http://www.isoc-es.org>. Ocupó el puesto de Director de Política Científica en el Gobierno Vasco de 1985 a 1987. Entre otros cargos universitarios en la UPV/EHU ha sido Vicerrector de Profesorado, Decano de la Facultad de Informática, y Director del Departamento de Informática.

1. Introducción

Internet Society (ISOC) adoptó hace ya más de 10 años el lema "*Internet is for everyone*", dejándolo reflejado por escrito en una RFC informativa redactada por Vinton Cerf [1].

Siempre una de las principales preocupaciones en ISOC han sido las personas, que encuentran en la Red una ventana de comunicación con inmensas posibilidades para el acceso al conocimiento, la comunicación, el crecimiento personal y la participación ciudadana.

La transición a IPv6 es un episodio más, meramente tecnológico, cuyas bases ya estaban establecidas en 1998 en la RFC 2460 [2]. Sin citarlo expresamente, Vinton Cerf escribía lo siguiente el año 2002:

Internet is for everyone - but it won't be if it cannot keep up with the explosive demand for its services, so we must dedicate ourselves to continuing its technological evolution and development of the technical standards the lie at the heart of the Internet revolution.

Las personas son lo más valioso de la Red, pero es necesario contar también con infraestructuras que proporcionen la conectividad global y local, y así poder llegar a los contenidos y servicios de Internet. En la primera Internet esta conectividad se encontraba en las redes académicas pero, desde que en 1992 apareciese la Internet comercial, son las empresas de telecomunicaciones las que proporcionan el acceso a la Red.

La transición a IPv6 obliga a movilizar muchos agentes: fabricantes de equipos, contenidos y servicios de Internet, redes corporativas de empresas e instituciones, y proveedores de acceso a la Red (mayoristas o minoristas).

Para ***Novática*** este tema no es nuevo: Ya fue objeto de un número monográfico en el año 2005 [3]. Pero entonces el foco del análisis estaba en la tecnología, aún quedaban suficientes direcciones IPv4, y el planteamiento era todavía bastante académico. Hoy la situación ha cambiado y existe una cierta sensación de alarma.

Es en este escenario en donde la *Internet Society* y sus capítulos locales se han comprometido con el despliegue de IPv6, coordinando sus actividades para conseguir un mejor efecto. También en nuestro país el capítulo ISOC-ES ha organizado diversos actos de difusión y formación, siempre contando con la participación de Jordi Palet, destacado *evangelista* de IPv6, y en colaboración con i2basque, CESGA y CESCA.

El despliegue de IPv6 es una necesidad cada vez más acuciante. Las direcciones IPv4 se van agotando. Mantener los protocolos actuales es poner un freno al crecimiento de la Red, como lo era para las ciudades europeas a mediados del siglo XIX la existencia de las murallas que bloqueaban su desarrollo. La solución diseñada para este nuevo "ensanche" ordenado y racional está planteada y probada desde hace más de 10 años.

Como queda reflejado en el título de este artículo, los ciudadanos nos vemos convertidos en "usuarios", sometidos al mercado y al negocio de los proveedores de acceso a Internet. El usuario es quien menos información tiene, desconociendo qué diferencias existen en los servicios que va a recibir de su proveedor de acceso si sólo le proporciona IPv4, o incluye también IPv6. Unas diferencias que no serán notables hasta que proliferen productos y aplicaciones para domótica como las bombillas 6LoWPAN recientemente anunciadas[2], o contenidos y servicios "sólo IPv6".

Internet Society se pone en el papel del usuario y trata de movilizar a los agentes implicados: los proveedores de Internet y las redes corporativas, que son quienes tienen en su mano la llave para el despliegue definitivo de IPv6.

Desde ISOC-ES también interpretamos que IPv6 puede contribuir positivamente a nivel local a mejorar un objetivo de primer nivel, como es el crecimiento económico. El protocolo IPv6 es un elemento de innovación que desde un segundo nivel actúa como "palanca" para propiciar la actividad de empresas locales, especializadas en comunicaciones y software libre, nuevos productos y servicios generados a nivel local destinados a un mercado global, aportando un intangible que beneficia a la economía regional.

2. Iniciativas de *Internet Society* sobre IPv6

ISOC ha incluido IPv6 entre las "tecnologías que importan", dedicándole un conjunto muy amplio de actividades. También ha entendido siempre que las barreras de entrada para conseguir una implantación efectiva de IPv6 no las pone el usuario.

Como fruto de este esfuerzo de concienciación, desde hace varios años los equipos personales están preparados para la transición. Los fabricantes se han preocupado por incluir esa facilidad en los sistemas operativos más extendidos, ya sean ordenadores de sobremesa, portátiles, tabletas o teléfonos inteligentes.

> “Mantener los protocolos actuales es poner un freno al crecimiento de la Red, como lo era para las ciudades europeas a mediados del siglo XIX la existencia de las murallas que bloqueaban su desarrollo. La solución diseñada (…) está planteada y probada desde hace más de 10 años”

La oferta de contenidos también se ve afectada por la dificultad en conseguir de los ISPs (*Internet Service Providers*) conexiones con IPv6, hecho que sólo puede resolverse utilizando los servicios de “Redes de entrega de contenidos” (*Content Delivery Networks* - CDN) con servidores en IPv6.

La barrera principal se localiza en los proveedores de la conexión a Internet, ya sea en el acceso doméstico, en las conexiones de las redes corporativas (empresas, administraciones, instituciones), y en las redes troncales de las empresas de telecomunicaciones.

Por esta razón los esfuerzos de ISOC se concentran en dinamizar la oferta de contenidos y la oferta de conectividad IPv6. La estrategia se puede resumir en tres conceptos: informar, comprometer, y ayudar.

- *Informar* con los anuncios sobre el agotamiento de IPv4 y las ventajas asociadas a IPv6.
- *Comprometer* con eventos como los “Días IPv6” celebrados en 2011 y 2012.
- *Ayudar* con programas permanentes como Deploy360.

3. Actividades de *Internet Society* sobre IPv6

Para muchos agentes, IPv6 es aún un territorio lleno de incógnitas. Con un despliegue poco significativo, es necesario despejar las dudas del efecto que puede producir en servidores de contenidos y redes troncales.

Por este motivo. *Internet Society* se planteó avanzar hacia un uso habitual de IPv6 con una estrategia con dos ejes:

- Eventos con fecha y metas definidas. Comenzaron en 2011 con la celebración de una prueba global significativa, implicando a los principales agentes y analizando los resultados: “*World IPv6 Day*”. Superada la prueba con éxito, se estableció otro objetivo, un compromiso de permanencia en IPv6 de contenidos y servicios.
- Información y formación para facilitar el despliegue de IPv6 con el programa Deploy360.

3.1. *World IPv6 Day*

El evento “*World IPv6 Day*”, celebrado el 8 de junio de 2011, fue un test de 24 horas. Los sitios web más visitados ofrecerían sus contenidos en IPv6, con objeto de observar el comportamiento de la red y los servidores durante esas 24 horas (ver **figura 1**).

El objetivo de este experimento era motivar a las organizaciones a preparar sus servicios, para que el cambio a IPv6 se haga sin problemas cuando las direcciones IPv4 se agoten, y esta transición sea obligada. Para certificar este hecho, el 3 de febrero de 2011 la Agencia de Asignación de Números de Internet (IANA) entregó simbólicamente, en un acto celebrado en Miami, las últimas direcciones IPv4 disponibles en el mundo.

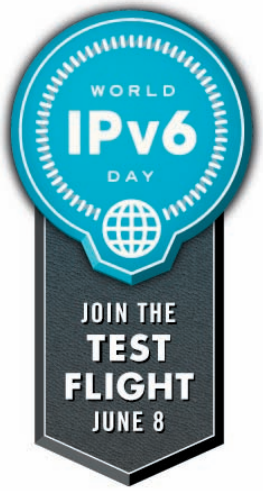


Figura 1. Logotipo de *World IPv6 Day.*

Internet Society convocó el evento con la colaboración de los sitios web más visitados (Google, Youtube, Facebook, Yahoo), y varias CDNs (Akamai, LimeLight Networks). La fecha podía haber sido más simbólica (6-6-2011, lunes) pero no se consideró adecuado realizar el test un lunes, al solaparse en algunos husos horarios con un día festivo.

A la iniciativa se adhieren un total de 858 sitios web, 20 de ellos en el dominio “.es”[3]. Aunque el compromiso se limitaba a la disponibilidad de los sitios web en IPv6, también se buscó la complicidad de ISPs, redes corporativas y fabricantes de hardware (*routers* domésticos).

Los resultados fueron un éxito. Los operadores de red observaron que los tráficos de IPv6 aumentaron un 65%, aunque los porcentajes globales respecto a IPv4 eran sólo de un 0,3 %. Según Cisco, sólo 3 petabytes de un tráfico global diario de 1 hexabyte utilizaron IPv6.

No se detectaron problemas especiales durante la jornada, aunque se observaron algunas ineficiencias que pueden ser corregidas, debidas a la coexistencia de IPv4 e IPv6. Dado que la transición a IPv6 llevará un tiempo, estas informaciones son muy valiosas para evitar situaciones complicadas cuando se vayan incrementando los tráficos del nuevo protocolo, hasta llegar a desplazar a la versión anterior.

En el número de conexiones con sitios web destacó Google, aunque por volumen de tráfico fue Youtube quien acaparó casi todos los paquetes que circularon por la Red. También se pudo comprobar que muy pocos ISPs soportan el protocolo IPv6 nativo en las conexiones de los usuarios.

Otro resultado indirecto es la permanencia en IPv6 después del test de 24 horas de numerosos sitios web, una vez comprobado que esta permanencia no les generaba problemas de ningún tipo.

Las Redes Académicas de País Vasco, Galicia y Cataluña también organizaron jornadas dedicadas a IPv6 en colaboración con ISOC-ES[4]. Estas jornadas tenían como objetivo sensibilizar a los agentes locales, tanto empresas como administraciones, para que se planteasen la transición a IPv6.

3.2. *World IPv6 Lauch*

“*World IPv6 Launch*” ha tenido lugar el miércoles 6 de junio de 2012. En este caso no se trataba de un test, sino de un compromiso de permanencia en IPv6 a partir de una fecha señalada (ver **figura 2**).

World IPv6 Launch[5] ha contado con el apoyo explícito de numerosas empresas y personalidades, que han dejado sus testimonios como por ejemplo videos en Youtube[6]. En esta ocasión han participado los principales proveedores de Internet (ISPs), fabricantes de equipos domésticos (*routers*) y sitios web de todo el mundo, habilitando IPv6 de forma permanente en sus productos y servicios.

Los “*operadores de redes*” adquirieron el compromiso de habilitar por defecto IPv6 a

> “Este programa se complementa con una serie de presentaciones locales denominadas Conferencias ION (*Internet ON*), con la participación de expertos en estas dos tecnologías emergentes (IPv6 y DNSSEC)”

Figura 2. Logotipo de *World IPv6 Lauch*.

los nuevos clientes a partir del 6 de junio de 2012. “Habilitado por defecto” significa que el servicio no necesita una configuración específica por el usuario final para utilizar el protocolo IPv6 en su conexión. También se comprometieron a que al menos el 1% de sus clientes podrían utilizar IPv6 al visitar sitios web. En esta categoría de soporte se inscribieron 77 operadores de red, con una destacada participación de las Redes Académicas (RedIRIS, RENATER, Janet, GARR, SURFnet…). En nuestro país figuran tres redes académicas (RedIRIS, CESCA, CICA), y una red de iniciativa ciudadana (guifi.net).

Sólo cinco “*fabricantes de routers*” domésticos se han sumado a la iniciativa, obligándose a incorporar IPv6 en sus productos de gama “baja” y “media”: Cisco, D-Link, NEC, Yamaha y ZyXEL. Todos los routers fabricados a partir del 6 de junio de 2012 han de tener IPv6 activado por defecto, y superar un test que certifique esas capacidades[7].

El número de “*sitios web*” en IPv6 superó los 3.000 participantes. Entre ellos destacan cinco de los seis primeros según el rango de Alexa (Facebook, Google, Youtube, Yahoo y Wikipedia), y numerosos sitios web gubernamentales. Un 4% de los participantes (121) están localizados en España, siendo los sitios web más populares los que corresponden a prensa y administración.

3.3. IPv6 y Deploy360

Los “*Días IPv6*” son sólo hitos o etapas en un largo camino iniciado hace casi 15 años. Entre las herramientas más útiles para conseguir los objetivos de despliegue global destaca un repositorio de información puesto en marcha por *Internet Society* el año 2011 con el nombre de “*Deploy360*”[8].

Pero esta tarea, coordinada y apoyada por *Internet Society*, tiene ya antecedentes en el año 2009: el Capítulo ISOC-Argentina, junto con el proyecto 6DEPLOY[9] de la UE, publicó el libro “*IPv6 para todos: Guía de uso y aplicación para diversos entornos*” [10]. La versión original en castellano ha sido traducida a diversos idiomas (inglés, catalán, euskera, gallego), coincidiendo con diversos actos y presentaciones del “*World IPv6 Day*” en Galicia, País Vasco y Cataluña.

“*Deploy360*” de *Internet Society* está dedicado a dos de las “tecnologías que importan”: el despliegue de IPv6, y DNSSEC (extensiones de seguridad para los DNS). El objetivo es llenar la brecha entre los estándares desarrollados en el seno de IETF (*Internet Engineering Task Force*) y la comunidad global de Internet que tiene que adoptarlos y desplegarlos. Por esta razón, Deploy360 proporciona recursos seleccionados para que sean inteligibles y fáciles de aplicar a los responsables del despliegue de estas tecnologías: operadores de redes, desarrolladores, proveedores de contenidos, fabricantes de equipos, y redes corporativas.

Entre los recursos que ofrece este repositorio encontraremos información básica (incluye el libro antes citado), “casos de estudio”, recursos de formación (cursos, tutoriales, videos), estadísticas, y referencias a otros sitios dedicados a IPv6.

Este programa se complementa con una serie de presentaciones locales denominadas Conferencias ION (*Internet ON*), con la participación de expertos en estas dos tecnologías emergentes (IPv6 y DNSSEC), que intercambian informaciones y experiencias sobre los despliegues tempranos, y debaten sobre su futuro. Más que jornadas de formación, son talleres de casos prácticos con profesionales, donde los operadores de redes públicas y los responsables de redes corporativas reciben respuestas para realizar el despliegue de estos nuevos estándares y tecnologías. Las últimas Conferencias ION se han realizado en Buenos Aires y Toronto.

4. Situación actual de IPv6

Como ya hemos mencionado antes, el usuario final depende de otros agentes. En lo que se refiere a la conexión, de la cadena de operadores de red que le proporcionan la conexión a Internet, y en el caso doméstico, de los fabricantes de *routers* que instalará en su casa. Los contenidos y servicios son competencia de sus proveedores. Los sitios más visitados ya están en IPv6 desde 2011 o 2012 (Facebook, Goggle, Youtube, etc.), aunque algunas empresas y administraciones no han hecho el esfuerzo de conectar sus servidores en IPv6.

Los fabricantes de equipamiento, junto con los operadores de red, proponen soluciones globales basadas en CGN (*Carrier Grade NAT*) para efectuar la transición. Esta alternativa al despliegue de IPv6 nativo está siendo objeto de una fuerte controversia [4].

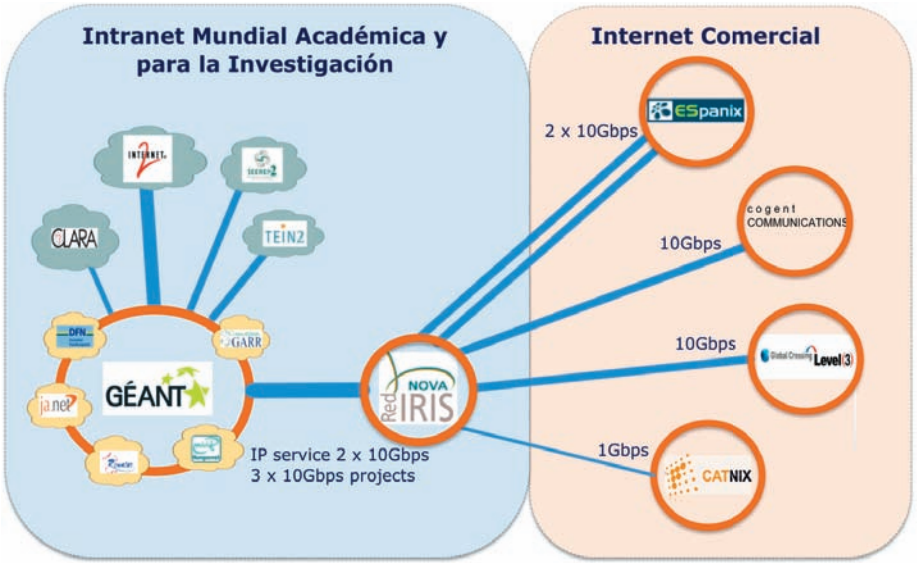


Figura 3. Conexiones de RedIRIS (© RedIRIS).

> “Los fabricantes de equipamiento, junto con los operadores de red, proponen soluciones globales basadas en CGN *(Carrier Grade NAT)* para efectuar la transición. Esta alternativa al despliegue de IPv6 nativo está siendo objeto de una fuerte controversia”

Los ISPs tienen inversiones significativas en equipamiento y aplicaciones que necesariamente han de actualizar para soportar IPv6. Plantean una solución que extiende el ciclo de vida de IPv4, y argumentan que en su opinión no va a haber retrasos para que IPv6 alcance una masa crítica en breve. Pero hay quienes tienen muchas dudas sobre esta alternativa. Sabiendo que implantar CGN tiene un coste significativo, suponen que este “artificio” seguirá tiempo en uso hasta que se amortice la inversión, demorando un despliegue global de IPv6 nativo.

Las redes académicas, que en su conjunto se pueden asimilar a un operador de red global, son un ejemplo de buenas prácticas. Sus redes troncales ya tienen desplegado IPv6 nativo desde hace años, pues siempre han sido más sensibles a los estándares y a la incorporación de nuevos protocolos. En las reuniones nacionales e internacionales es habitual contar con conexiones IPv6 (*TERENA Networking Conference*, 2012).

En el mundo académico la barrera se encuentra en las redes corporativas de las entidades afiliadas. El caso de RedIRIS es significativo (ver **figura 3**). Como Registrador Local de Internet (LIR) en RIPE[11], proporciona direcciones IPv6 a las entidades afiliadas (universidades, centros de investigación, etc.). Pero en estas redes corporativas el despliegue de IPv6 es aún incipiente, como se puede ver en un “cuadro de honor”[12] de IPv6 que mantiene RedIRIS. De las más de 400 entidades afiliadas, en octubre de 2012 sólo 41 tienen asignadas direcciones IPv6, y de éstas sólo 4 tienen todos los servicios operativos con este protocolo (web, e-mail, dns y ntp).

Las redes corporativas de administraciones y empresas por lo general van al mismo ritmo que les marcan sus proveedores de Internet. Si se trata de proveedores comerciales, han hecho pocos avances. Cuando por su naturaleza, contenidos o servicios tienen acceso a las redes académicas, pueden ser muy activas en la incorporación de IPv6. Es el caso en RedIRIS de MINECO (*Ministerio de Economía y Competitividad*), MINETUR (*Ministerio de Industria, Energía y Turismo*) y la RAE (*Real Academia Española*), recientemente incorporados al “cuadro de honor IPv6”.

Las actividades de ICANN (*Internet Corporation for Assigned Names and Numbers*) y de ISOC con sus anuncios del agotamiento de IPv4, y la promoción del nuevo protocolo IPv6, han sensibilizado a las administraciones. Éstos son algunos ejemplos:

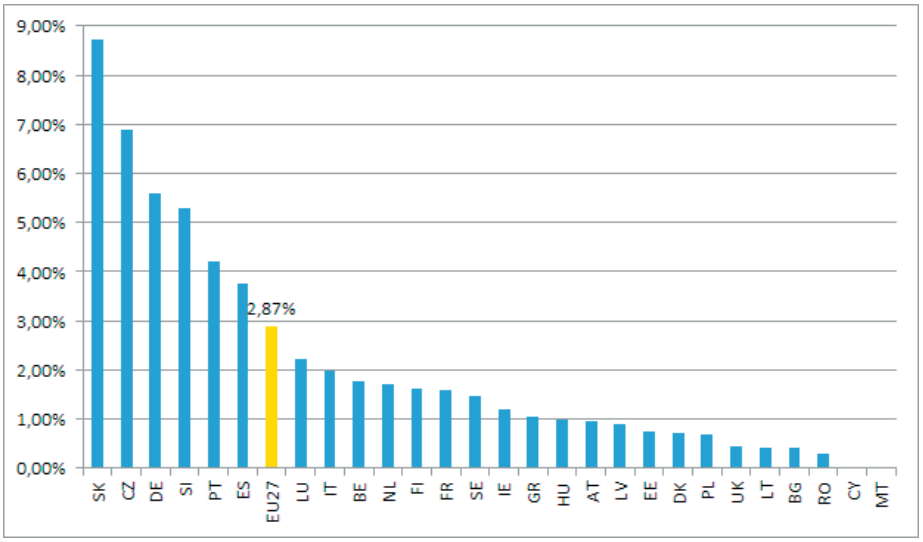


Figura 4. Porcentaje de sitios web accesibles por IPv6 en los países europeos (Fuente: Comisión Europea).

- La Casa Blanca anunció hace dos años que antes de finalizar septiembre de 2012 todos sitios web y servicios gubernamentales USA tenían que ofrecer conectividad IPv6[13]. El mandato especificaba que las agencias gubernamentales debían de utilizar IPv6 nativo, en lugar de mecanismos de transición basados en IPv4 (túneles, etc.).
- La Agenda Digital Europea incluye desde junio de 2012 un nuevo indicador: porcentaje de sitios web accesibles por IPv6 en cada país (ver **figura 4**). La muestra se obtiene del primer millón de sitios web más visitados según Alexa[14].
- La propuesta de Agenda Digital para España[15], que ha estado sometida a consulta pública hasta el 30 de septiembre de 2012, propone en el apartado de conectividad “*impulsar la implantación de la nueva versión del Protocolo de Internet IPv6*”. Con anterioridad se había aprobado el 29/04/2011 un “*Plan de Fomento para la Incorporación de IPv6 en España*”[16].

5. Conclusiones

La transición a IPv6 es un proceso similar al que siguieron las ciudades y las villas para desprenderse de las murallas medievales, que eran los límites a su crecimiento. Fue la revolución industrial, a mediados del siglo XIX la que propició la eliminación de estas barreras, y la aparición de los “ensanches”. El comienzo del derribo de la “primera piedra” era motivo de júbilo y celebración. Con Internet toda va más rápido. Pasaron siglos antes de que las murallas fueran un problema, pero aunque la red tiene menos de medio siglo, ya ha llegado a consumir el espacio disponible.

Desde *Internet Society* y sus capítulos hemos querido festejar también el comienzo de una nueva etapa. No sabemos hasta donde pueden llegar los desarrollos que contemplaremos en los próximos años. Pero aunque la “Internet de las cosas” y los “”ambientes inteligentes” nos puedan sorprender, deberán ser siempre las personas, los ciudadanos, los protagonistas de la nueva sociedad.

La transición a IPv6 es un camino que hay que recorrer obligadamente. Especialmente los grandes operadores de red y los ISPs. Hoy el recurso principal que consume este proceso es “tiempo”, como lo hemos podido comprobar en i2basque. Tiempo para formación, planificación, despliegues piloto con prueba y error, etc. Quizás más adelante, cuando sea imperativo y a fecha fija, el costo sea más importante en inversiones y servicios de ingeniería.

El papel de los gobiernos es fundamental. Puede y debe de seguirse el modelo establecido por *Internet Society* con el *World Internet Launch*: conseguir compromisos de los principales

agentes. Fijar una fecha, de forma dialogada, a partir de la cual los operadores de redes e ISPs han de incluir IPv6 nativo en todas las conexiones de nuevos clientes, y dar un plazo para que las conexiones anteriores tengan esa funcionalidad.

No debemos ignorar el papel pionero de las redes académicas en el despliegue de IPv6. RedIRIS y las Redes Autonómicas son un ejemplo de buenas prácticas, en el que puede y debe de apoyarse la administración para trasladar las experiencias a sus redes corporativas.

Superados los retos tecnológicos, en *Internet Society* no sólo entendemos que "Internet es para todos", también defendemos que "Internet es de todos", o que "Internet somos todos". Internet no debería de tener dueños, ni los operadores de redes, ni las empresas proveedoras de contenidos y servicios. Por eso, ISOC hace oír su voz también en organizaciones y conferencias donde trata de seguir defendiendo aspectos fundamentales, como la neutralidad de la red.

Referencias

[1] V. Cerf. *RFC 3271: The Internet is for Everyone*. IETF, abril 2002. <http://www.ietf.org/rfc/rfc3271> (consultado: octubre 2012).

[2] S. Deering, R. Hinden. *RFC 2460: Internet Protocol, Version 6 (IPv6) Specification*. IETF, diciembre 1998. <http://www.ietf.org/rfc/rfc2460> (consultado: octubre 2012).

[3] ATI. IPv6 - Más que un protocolo. Monografía de *Novática, nº 174, marzo-abril, 2005*. <http://www.ati.es/novatica/2005/174/nv174sum.html> (consultado: octubre 2012).

[4] Wesley George. Shared Transition Space: Is it necessary? *The Internet Protocol Journal. Vol. 15, núm. 2*, junio 2012. <http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_15-2/152_transition.html> (consultado: octubre 2012).

Notas

[1] **Greenwave Reality.** Connected Lighting Solution for Smart Home Platform, octubre 2012. <http://www.greenwavereality.com/solutions/led-lighting/> (consultado: octubre 2012)

[2] **Internet Society.** Sitios web participantes en el *World IPv6 Day* <http://www.worldipv6day.org/ipv6-enabled-websites/index.html> (consultado: octubre 2012).

[3] **ISOC-ES.** Memoria de Actividades 2011, <http://www.isoc-es.org/files/downloads/MA11.pdf> (consultado: octubre 2012)

[4] **World IPv6 Launch.** <http://www.worldipv6launch.org> (consultado: octubre 2012).

[5] **Youtube.** Videos sobre *World IPv6 Launch*, <http://www.youtube.com/playlist?list=PL934BCF00AAC2EDD4&feature=view_all> (consultado: octubre 2012).

[6] **IPv6 Ready.** *CE Router (CPE) Interoperability Test Scenario*, Technical Document, Revision 1.0.0b8, <http://www.ipv6ready.org/docs/CE_Router_Interoperability_Latest.pdf> (consultado: octubre 2012)

[7] **Internet Society.** *Deploy360 Programme*, <http://www.internetsociety.org/deploy360/>.

[8] **Seventh Framework Programme of the European Union.** Proyecto 6DEPLOY, <http://www.6deploy.eu> (consultado: octubre 2012)

[9] **The IPV6 Portal.** IPv6 para todos <http://www.ipv6tf.org/index.php?page=news/newsroom&id=8281&lan=sp> (consultado: octubre 2012)

[10] **RIPE Network Coordination Centre.** *REDIRIS - Entidad Publica Empresarial Red.es, Resource Overview*, <https://stat.ripe.net/AS766#tabId=at-a-glance> (consultado: octubre 2012)

[11] **RedIRIS**. *Cuadro de honor de Instituciones Afiliadas*, <http://www.rediris.es/actividades/ipv6day/cuadro_de_honor.html> (consultado: octubre 2012)

[12] **Executive Office of the President**. *Memorandum for Chief Information Officers of Executive Departments and Agencies: Transition to IPv6*, <https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf> (consultado: octubre 2012).

[13] **Comisión Europea.** *Digital Agenda for Europa: IPv6 readiness of most visited websites*, <http://alturl.com/2q44j> (consultado: octubre 2012).

[14] **Gobierno de España.** *Presentada la Agenda Digital para España a los Grupos Parlamentarios*, <https://agendadigital.gob.es> (consultado: octubre 2012).

[15] **Gobierno de España.** *Plan de Fomento para la Incorporación de IPv6 en España*, <http://www.ipv6.es/es-ES/transicion/Paginas/Fomento.aspx> (consultado: octubre 2012).

Internet IPv6 en las redes académicas y de investigación: RedIRIS - Géant

Tomás P. de Miguel, Miguel Angel Sotos, Francisco Monserrat, Esther Robles
Red Académica y de Investigación Española RedIRIS

<{tomas.demiguel, miguel.sotos, francisco.monserrat, esther.robles} @rediris.es>

Resumen: *Desde que en los años 90 se decidió abordar el diseño de un nuevo protocolo para resolver problemas como el direccionamiento y otros aspectos técnicos de IP, las redes académicas han servido de laboratorio para probar la nueva tecnología y ser los primeros en desplegarla. Aunque su uso en el entorno académico ha sido muy prematuro, la penetración real del nuevo protocolo es muy baja. Las redes troncales académicas y de los operadores comerciales están preparadas, pero todavía queda mucho camino por recorrer para que se alcance una penetración similar a nivel doméstico y de transición de los servicios principales de las instituciones.*

Palabras clave: *IETF, IP, túnel IP, 6bone.*

Autores

Tomás P. de Miguel es Doctor Ingeniero de Telecomunicación de la Universidad Politécnica de Madrid (1987) y director de la Red Académica y de Investigación Española RedIRIS desde 2005. Es colaborador de la Agencia Nacional de Evaluación y Prospectiva, miembro de numerosos asociaciones y comités de programa de congresos científicos, miembro del Comité Español de e-Ciencia y del *European Academic Network Policy Group*. Ha dirigido numerosos proyectos relacionados con tecnologías para la nueva generación de Internet, en especial tecnologías avanzadas de colaboración, el protocolo IPv6 o redes móviles de tercera generación, siendo autor de numerosos artículos en revistas especializadas. Ha gestionado numerosas licitaciones públicas de equipamiento informático e infraestructuras de comunicaciones, entre las que destaca RedIRIS-NOVA con un presupuesto de 130 millones de Euros. Hasta su incorporación a RedIRIS fue profesor titular en la E.T.S.I. de Telecomunicación y Subdirector de Infraestructuras y Recursos Humanos de la Universidad Politécnica de Madrid, contribuyendo al despliegue de la red de alta velocidad en dicha universidad.

Miguel Ángel Sotos es Licenciado en Informática por la Universidad Politécnica de Madrid y trabaja en RedIRIS desde el año 1999 como ingeniero de red, centrando su labor en la operación, diseño e ingeniería de la infraestructura de comunicaciones. Ha participado en numerosos proyectos de investigación a nivel nacional e internacional (principalmente de la Comisión Europea) centrados en la investigación, prueba y aplicación de protocolos como IPv6 y tecnologías de virtualización. Desde el año 2009 ha trabajado en el diseño, despliegue e implementación de la red de fibra oscura del proyecto RedIRIS-NOVA.

Francisco Monserrat es Licenciado en informática por la Universidad de Murcia y trabaja en RedIRIS desde 1999 como técnico senior de seguridad. Es miembro del IRIS-CERT (CSIRT) y miembro de FIRST desde 2007. Ha impartido numerosos cursos sobre seguridad informática y participa en proyectos internacionales como ingeniero de sistemas y experto en seguridad informática.

Esther Robles es Ingeniero superior en Informática por la Universidad de Valladolid. Su actividad profesional se ha desarrollado desde 1998 en RedIRIS, la red académica y de investigación española que ofrece servicios de comunicaciones a universidades y centros públicos de investigación y que fue pionera en suministrar servicios de Internet en España, donde ocupa el puesto de Jefa de Área de Red. Es Master Ejecutivo en Dirección de Proyectos por la Escuela de Organización Industrial. Ha participado en decenas de proyectos internacionales. Colabora con la Agencia Nacional de Evaluación y Propectiva y otros comités de evaluación de redes. Es miembro de numerosos comités técnicos internacionales como el *Terena Technical Committee* y ha participado en congresos internacionales formando parte del comité de programa.

1. Introducción

Desde hace casi dos décadas, Internet se ha venido enfrentando al problema de cómo responder al problema del agotamiento de sus recursos básicos de direccionamiento, debido al increíble crecimiento de la red. El protocolo IPv4 [1] no ha cambiado desde su definición inicial y se ha demostrado eficaz y robusto para trabajar en redes globales, pero no puede adaptarse a las exigencias actuales.

Internet se ha expandido por todo el mundo y el número de dispositivos conectados a la red es gigantesco. Sin embargo, las necesidades en vez de disminuir siguen aumentando y previsiblemente van a crecer aun más rápidamente en el futuro debido a la introducción de las nuevas tecnologías de la Internet de las cosas y las nuevas generaciones de dispositivos móviles. El previsible agotamiento de las direcciones y otras cuestiones desfavorables para el despliegue de una nueva generación de aplicaciones más seguras o de tiempo real, llevó a los diseñadores a pensar en una restructuración de IP.

Por éstas y otras razones, a finales de los 90 se impulsó desde IETF un grupo de trabajo (*Address Lifetime Expectations WG*) para desarrollar una nueva versión del protocolo IP que resolviera todas las pegas detectadas. El fruto de esos trabajos fue la especificación de Internet versión 6 (IPv6) (RFC2460 [3]). La especificación resultante es incompatible con IPv4, de manera que, una vez concluida la definición, muchos grupos empezaron a abordar el estudio de cómo evolucionar Internet hacia el nuevo protocolo, ya que la opción de parar Internet para sustituir todos los sistemas al mismo tiempo quedó descartada inmediatamente. En consecuencia se empezarían desplegando islas IPv6 conectadas entre sí a través de túneles sobre IPv4 y con pasarelas que permitieran conectar los sistemas IPv6 con los IPv4 y viceversa, durante todo el proceso de transición. Todo este proceso se ha desarrollado en el ámbito de las redes académicas. De ahí que las redes académicas europeas y RedIRIS en particular hayan participado en el proceso desde un primer momento.

6bone [4] se creó como un banco de pruebas informal del protocolo IPv6 en marzo de 1996. Su misión era establecer una red para fomentar el desarrollo, prueba y despliegue de IPv6 mediante un modelo que se basaba en las experiencias del Mbone, de ahí el nombre. RedIRIS se adhirió pronto a 6bone en mayo de 1997 [5] como resultado de la participación en los primeros grupos de trabajo europeos sobre el tema (TEN y CHOC). Como paso previo a la conexión al 6bone, RedIRIS participó en el piloto de IPv6 creado entre varias Redes Académicas y de Investigación Europeas, estableciendo un túnel con la red Holandesa SURFNET. Esta conexión, pionera en España, se realizó en 1995, y sentó la base para la creación de una red Europea, al amparo del proyecto TF-TANT (*Task Force – Testing of Advance Networking Technologies*). Esta red, al igual que el mencionado 6bone, se

> “En 2002, RedIRIS participó en colaboración con otras redes académicas, en un reto donde se consiguió un record de transmisión de datos con IPv6”

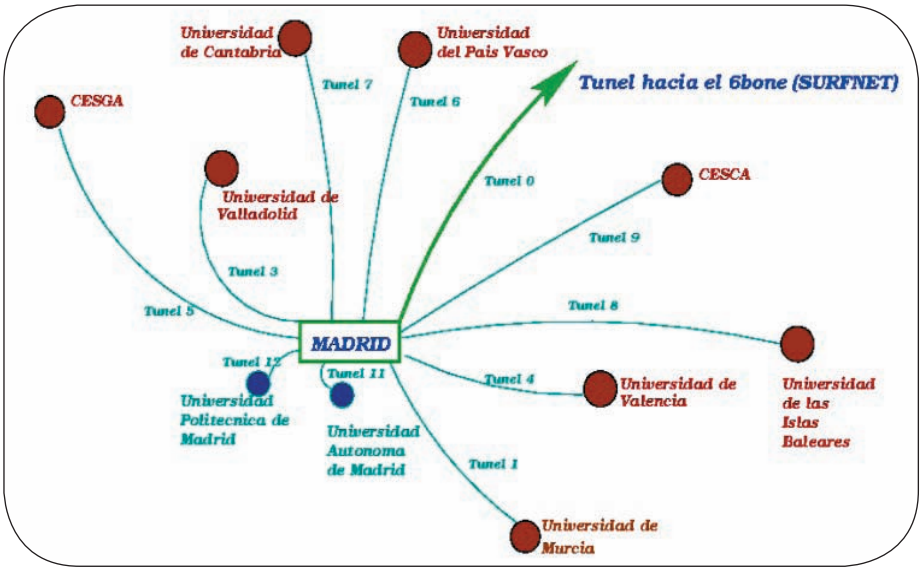


Figura 1. Conexión de los centros españoles más activos al 6bone a finales de los años 90.

sustentaba en túneles, por ser el modelo mas sencillo y flexible para empezar a construir la infraestructura, sin comprometer los demás servicios en producción, en esta etapa en la que la adopción e implantación del IPv6 no estaba todavía madura.

La red resultante consistía en la conexión de islas IPv6 a través del encapsulado del tráfico IPv6 sobre IPv4. RedIRIS conectó a los 10 centros que trabajaban más activamente en este tema en España (ver **figura 1**). Aunque el enfoque inicial de 6bone era la realización de pruebas de estándares e implementaciones, los principales esfuerzos se centraron más en la realización de pruebas de numerosos procedimientos de transición, así como el uso real de la red IPv6.

El modelo de conexión de islas a través de túneles no es adecuado cuando el número de islas a conectar aumenta mucho. Por ejemplo, un paquete de datos IPv6 podía dar la vuelta al mundo para conectar dos sitios próximos geográficamente, pero lejanos respecto a su situación en la red, lo que supone un modelo de encaminamiento muy ineficiente. De ahí que con el tiempo 6bone evolucionara hacia un despliegue en forma nativa de IPv6.

Para ello RedIRIS quiso asegurarse primero de que el rendimiento de sus equipos de comunicaciones era adecuado para desplegar IPv6 nativo. Por eso, en 2002, RedIRIS participó en colaboración con otras redes académicas, en un reto donde se consiguió un record de transmisión de datos con IPv6. RedIRIS en colaboración con otras redes académicas transmitió 675 MB entre Eslovenia y Madrid, separados 2.500 Km, en 11,53 segundos utilizando las redes académicas con IPv6 en modo nativo. En vista del éxito, desde 2003 se puso en producción en RedIRIS el soporte nativo IPv6 en su red troncal para todas las instituciones que lo demandaran.

2. Evolución de IPv6 en los últimos años

Desde la puesta en servicio en RedIRIS de IPv6 en modo nativo hasta el año pasado con ocasión del Dia Mundial de IPv6 [6], la evolución del servicio ha sido prácticamente nula. Las instituciones donde trabajan los grupos de investigación que han participado en los proyectos de investigación a lo largo de los años 90 han mantenido las conexiones con la red, pero solo para los proyectos de investigación. El número de servicios nativos IPv6 hasta el año pasado era escasísimo. La infraestructura de comunicaciones está preparada para el acceso a la red académica como a la Internet comercial, pero tanto en un ámbito como en el otro en número de servicios nativos es todavía muy reducido.

El tema dejó de ser tema de investigación a comienzos de siglo y, en teoría, desde entonces debería venir desarrollándose el proceso de transición al nuevo protocolo. Sin embargo, este proceso no ha ocurrido así, porque en el entorno académico no ha habido, al menos hasta ahora, escasez de direccionamiento y ha primado mucho más la evolución en capacidad de las redes de campus o el desarrollo de nuevas aplicaciones, que la transición hacia un protocolo que no tenía un uso masivo ni dentro ni fuera del entorno académico. Esta tendencia ha empezado a cambiar tras el anuncio de ISOC de que las posibilidades de asignación de nuevo direccionamiento IPv4 prácticamente han desaparecido.

El proceso de transición se ha demostrado que es sencillo en algunos aspectos, pero complicado en otros. Los usuarios en general no están familiarizados con la tecnología y ésta todavía, hablando también en términos generales no está disponible a nivel doméstico. Por otra parte, hay aplicaciones que utilizan la dirección IP como parte de los datos de configuración, lo que puede obligar a desarrollar una nueva versión para soportar las largas direcciones IPv6. Las instituciones de investigación no han visto la necesidad de destinar parte de sus escasos recursos a este fin.

No obstante la transición masiva se va a producir más pronto que tarde y por eso desde RedIRIS se ha animado a las instituciones a realizar el proceso de transición suavemente, de manera que no sea necesario consumir muchos recursos, pero al mismo tiempo se evite tener que hacer una transición acelerada en el último momento.

Para ello, RedIRIS propone desplegar en las redes locales de las instituciones el “doble *stack*”, al igual que en la red troncal de RedIRIS. De esa manera la mayoría de sus usuarios accederán automáticamente a todos los servicios disponibles por IPv6. Otro paso consiste en migrar poco a poco los servicios principales de la institución como los servidores web, el DNS o el correo.

Los servicios compartidos que presta RedIRIS para sus instituciones ya están operativos en IPv6, como por ejemplo el Servicio Centralizado Antispam (popularmente conocido como *lavadora*) y por eso todas las instituciones adheridas disponen del servicio. En el caso de *lavadora* el uso de IPv6 es muy reducido en proporción a IPv4 ya que está en torno a un 1,5%, tanto para el tráfico entrante como saliente.

Para impulsar el despliegue de IPv6 entre sus instituciones, RedIRIS ha trabajado en iniciativas como la transmisión de Opera mediante la tecnología *multicast* usando IPv6 de forma nativa. Con estas actuaciones se ha demostrado a las instituciones la madurez de

> “Los servicios compartidos que presta RedIRIS para sus instituciones ya están operativos en IPv6, como por ejemplo el Servicio Centralizado Antispam (popularmente conocido como *lavadora*) y por eso todas las instituciones adheridas disponen del servicio”

la tecnología y se las ha animado a desplegar los primeros servicios con usuarios reales.

Se observa que aunque la penetración de IPv6 entre las instituciones académicas es muy reducida, lo es aun más entre los servicios que ofrecen las instituciones. Esto se puede deducir de las estadísticas de tráfico externo que indican que la proporción de tráfico entrante a RedIRIS IPv6 frente a IPv4 por término medio está en torno a un 2,8%. El tráfico entrante es el de usuarios de RedIRIS que acceden a servicios en instituciones fuera de RedIRIS y que disponen de servicios que operan en IPv6. Por el contrario, la proporción de tráfico saliente, que es el de usuarios externos que intentan acceder a servicios de instituciones de RedIRIS en IPv6, es de solo un 0,6%.

Está suposición ha quedado ratificada al desplegar en RedIRIS una aplicación de análisis de servicios que resume el estado de despliegue en las instituciones que ya han solicitado direccionamiento IPv6. El Cuadro de Honor de IPv6 de RedIRIS [8] muestra las instituciones que han solicitado direccionamiento IPv6 y muestra cuales de los servicios más generales, como DNS, web, correo o ntp, se prestan ya a través de IPv6. De las 450 instituciones afiliadas, solo 41 han solicitado hasta ahora direccionamiento, y de ellas solo 6 ofrecen los servicios de DNS, web y correo a través de IPv6.

Esto se debe a que la situación en las redes locales de campus es muy desigual. Los centros más tecnológicos que han participado en el desarrollo de IPv6 tienen desplegado total o parcialmente el protocolo, aunque en la mayoría de los casos, los servicios principales siguen operando únicamente en IPv4.

Entre las redes autonómicas la situación es similar. Las redes que han participado desde hace años en el desarrollo de IPv6, ofrecen ese servicio a sus usuarios, mientras que el resto no lo tiene incluido en su cartera de servicios.

El 8 de junio del 2011 se produce un hito importante en lo que respecta al impulso de IPv6 que fue el *IPv6 Day*. Los principales proveedores de Internet activaron sus servicios en IPv6 durante todo el día. Multitud de empresas y organismos participaron activamente en la iniciativa (RedIRIS actuando como representante europeo), resultando éste todo un éxito. Lo importante es que no se registró ninguna incidencia o problema grave de acceso a los servicios, de forma que ni siquiera los usuarios finales percibieron que estaban usando un protocolo distinto. Se produjo un incremento notable del tráfico IPv6 en la red, llegando en momentos puntuales a incrementos de más del 50%. También aumentaron de manera notable el número de visitas a la web de RedIRIS a través de IPv6; pasando de una media de 65.000 accesos IPv6 a más de 76.000 accesos en ese día.

Este evento sirvió para que se tomara conciencia del problema del agotamiento de direcciones y para que en muchas instituciones empezara a considerarse un plan activo de transición suave hacia IPv6. Esto ha supuesto mayor interés por parte de instituciones que todavía no disponían de direccionamiento y desarrollo de pruebas y revisión de los primeros servicios por parte de otras, que ya disponían de direccionamiento, pero no lo habían utilizado efectivamente hasta ese momento. Todos estos avances son los que pretende reflejar el Cuadro de Honor de RedIRIS [8].

Debido al éxito del *IPv6 Day*, el 6 de junio de 2012 se promovió el *World IPv6 Launch*. A partir de esa fecha, los principales proveedores de contenidos y servicios activan IPv6 de forma nativa y permanente. La Internet comercial se une así a las iniciativas que comenzaron las redes académicas hace años, probando que el protocolo es maduro y está listo para usarse sin problemas. RedIRIS participa activamente en la iniciativa, como uno de los miembros con sus servicios completamente activos con IPv6.

Este hecho también se ratifica analizando los datos estadísticos de *IPv6 Test* [9], donde se puede comprobar que el despliegue real de servicios IPv6 es muy bajo, porque todavía hay proveedores que no ofrecen el servicio a sus usuarios. Un ejemplo significativo es HE (*Hurricane Network*), que no da servicio en España y que, al igual que gogo6, solo ofrecen túneles 4to6 en nodo remoto y donde RedIRIS ocupa uno de los lugares mas destacados. Esto es especialmente relevante cuando tomamos en consideración la estadística de ancho de banda de bajada [9] donde la proporción de tráfico IPv6 es muy baja, pero además RedIRIS aparece como el proveedor que ofrece la tasa de tráfico más alta (ver **figura 2**). Esto se debe a que las conexiones de RedIRIS son simétricas y las de los operadores comerciales no.

En otras redes académicas de nuestro entorno la situación es muy similar. El protocolo se ha desplegado de forma nativa desde hace años, pero el uso es muy limitado entre las instituciones conectadas, debido a que no se ha detectado todavía una necesidad urgente de nuevo direccionamiento.

3. Conclusiones

La utilización masiva de tecnología móvil o el desarrollo inminente de la Internet de las cosas parece que están siendo el detonante que está ayudando, más activamente incluso que la escasez de direcciones, a la transición a IPv6. En general las redes académicas nacionales están preparadas desde hace años. RedIRIS ha participado desde las primeras etapas (año 1995) en la investigación y posterior despliegue del protocolo en producción como un

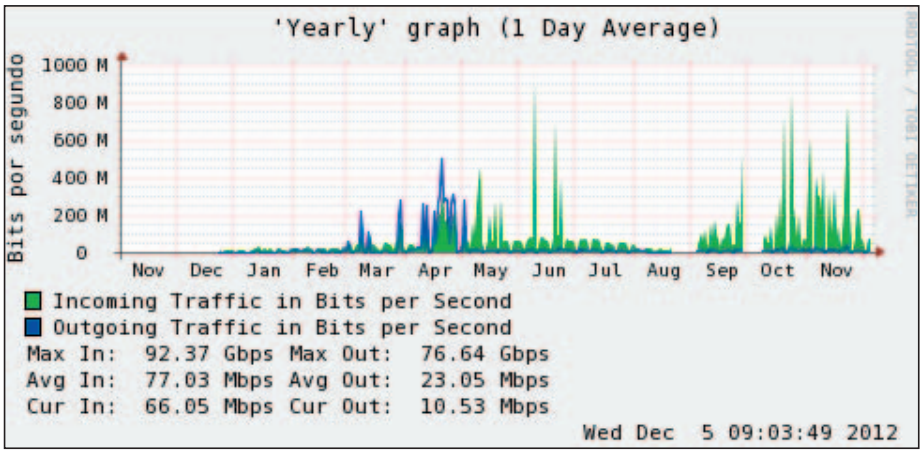


Figura 2. Tráfico nativo IPv6 entre RedIRIS y la Internet global.

> “Todavía hay muchos dispositivos (tabletas o *smartphones*) que no están preparados para operar con IPv6 en algunas redes (como 3G) aunque la mayoría sí lo están para WiFi”

servicio más a sus usuarios [10]. Esto ha sido posible porque las redes troncales internacionales como GÉANT también han desplegado el protocolo IPv6 como una opción más de servicio para todas las NRENs europeas. Los operadores comerciales también están preparados, pero sin embargo falta mucho camino por recorrer.

A nivel doméstico los operadores todavía no han desplegado un plan masivo de transición y por tanto el mundo comercial no ha dado un vuelco todavía, aunque a través de iniciativas como el Día Mundial de IPv6 se ha puesto de manifiesto el interés de los grandes proveedores de contenidos por ofrecer ya de forma estándar todos sus servicios a través del nuevo protocolo.

Sin embargo, todavía hay muchos dispositivos (tabletas o *smartphones*) que no están preparados para operar con IPv6 en algunas redes (como 3G) aunque la mayoría sí lo están para WiFi. Aunque la solución no es muy difícil, no existe una gran presión por hacerlo ya que, aunque IPv6 ofrece mejoras a las aplicaciones en muchos aspectos, no se ha detectado ninguna aplicación que mejore sensiblemente con su utilización y preocupa que el proceso de transición sea complicado para el usuario final.

A todo esto hay que añadir la situación de crisis económica que vivimos y que ha truncado en muchos casos los planes de transición previstos en muchas instituciones. En este momento es difícil para las instituciones de investigación abordar inversiones que no sean muy urgentes. Por eso aunque en buena medida las redes troncales están ya operativas desde hace tiempo, los terminales de los usuarios y sobre todo los servicios no están todavía preparados para operar plenamente en el nuevo escenario.

La estrategia que se presenta como más atractiva en este momento es la de buscar servicios compartidos. A través de la compartición de recursos y agregando demanda es posible mejorar y evolucionar los servicios y al mismo tiempo identificar ahorros. Esta estrategia puede conseguir que, sin recursos adicionales, muchas instituciones puedan evolucionar en muy poco tiempo todos sus servicios esenciales a IPv6.

Referencias

[1] DARPA. *RFC 791, Internet Protocolo version 4*, 1981. <http://www.rfc-es.org/rfc/rfc0791-es.txt>.

[2] Frank Solensky. Resumen de minutas del ALE WG, 1994. <ftp://ftp.ietf.cnri.reston.va.us/ietfonlineproceedings/94dec/area.and.wg.reports/ipng/ale/aleminutes94dec.txt>.

[3] S. Deering, R. Hinden. *RFC 2460, Internet Protocol, Version 6 [IPv6] Specification*, diciembre 1998. <http://rfc.net/rfc2460.html>.

[4] R. Fink, R. Hinden. *RFC 3701 6bone (IPv6 Testing Address Allocation)*, marzo 2004. <http://www.ietf.org/rfc/rfc3701.txt>.

[5] Natalia Benito, Josu Aramberri. *Red piloto IPv6 y conectividad a 6bone*. <http://www.rediris.es/difusion/publicaciones/boletin/50-51/ponencia10.html>.

[6] ISOC. *World IPV6 Day*, 2011. <http://www.internetsociety.org/ipv6/archive-2011-world-ipv6-day>.

[7] IPv6 ACT NOW. *World IPv6 Launch*, 2012. <http://www.ipv6actnow.org/info/world-ipv6-launch/>.

[8] RedIRIS. *Cuadro de Honor de Instituciones Afiliadas - IPv6*. <http://www.rediris.es/actividades/ipv6day/cuadro_de_honor.html>.

[9] IPv6 Test. <http://ipv6-test.com/stats/country/ES>.

[10] RedIRIS. *IPv6 en RedIRIS*. <http://www.rediris.es/actividades/ipv6day/cronograma.html>.

Jordi Palet Martínez
CEO/CTO, Consulintel, S.L.

<jordi.palet@consulintel.es>

Actividades del IETF al respecto de IPv6

Resumen: *El IETF (Internet Engineering Task Force) es la entidad que se ocupa de la estandarización de Internet y obviamente la responsable tanto del desarrollo de IPv4 como de IPv6. La actividad de esta organización, formada por voluntarios, es ingente, y especialmente en los últimos años ha sido muy relevante para el desarrollo de IPv6, y continúa siéndolo según avanza su despliegue. Más aún desde 2011, cuando IPv4 se fue agotando. Este artículo da un breve repaso a las actividades de los diversos grupos de trabajo, especialmente a los más relevantes respecto de IPv6 y sus desarrollos.*

Palabras clave: *Áreas de actividad, grupos de trabajo, IETF, Internet, IPv6, RFCs, seguridad, softwires, transición.*

Autor

Jordi Palet Martínez ha trabajado en informática y comunicaciones desde hace más de 30 años y tiene experiencia en diversos lenguajes de programación, *porting* de sistemas operativos, electrónica y diseño de circuitos, consultoría, diseño e implementación de redes, formación, marketing y desarrollo de productos. Actualmente es CEO/CTO de Consulintel, una empresa española experta en IPv6, con negocios en este campo en todo el mundo. Frecuentemente escribe artículos, fundamentalmente al respecto de IPv6, y ha participado en IETF desde el 2001, siendo autor y/o co-autor de numerosos documentos. Esta también involucrado en las actividades de desarrollo de políticas de los Registros Regionales de Internet (RIRs), habiendo contribuido muy activamente en todos ellos. Ha desarrollado y participado numerosos proyectos de I+D+i de la Comisión Europea y del Gobierno Español, habiendo contribuido al despliegue de Internet en numerosos organismos públicos y privados y proporcionado consultoría estratégica en este campo a numerosos gobiernos de todo el mundo.

1. Introducción

El IETF (*Internet Engineering Task Force*)[2] es la entidad responsable de la estandarización de los protocolos de Internet. Se trata de estándares abiertos y no sujetos a ningún tipo de canon, derechos de propiedad, patentes, etc.

Tal y como lo define la propia organización, la misión del IETF es lograr que Internet funcione mejor, mediante la producción de documentos técnicos de alta calidad (los denominados RFC's, *Request For Comments*, algunos de los cuales son normativos mientras que otros son recomendaciones o meramente informativos) que influencien la forma en la que se diseña, utiliza y gestiona Internet[3].

Es importante entender que se trata de una labor voluntaria, sin membresía formal ni cuotas por participar, sino que los propios participantes cubren sus gastos de participación en las reuniones anuales (tres, en diferentes partes del mundo para facilitar una participación global, y en ocasiones reuniones específicas de uno o varios grupos de trabajo) y su tiempo, a menudo financiados ambos por las entidades para las que trabajan. El trabajo y las decisiones, basadas en consenso, se realiza a través de las listas de correo, no en las reuniones presenciales.

El trabajo del IETF se organiza en diversas áreas de actividad, de las cuales, las que más afectan al desarrollo de los estándares relacionados con IPv6 son:

- Internet
- Operaciones y Gestión
- Transporte

De forma tangencial, siendo IPv6 junto con IPv4 los protocolos básicos, siempre han de ser tenidos en cuenta los trabajos realizados en las áreas de Encaminamiento, Seguridad, Aplicaciones e Infraestructura de Tiempo Real y Aplicaciones, ya que desde hace varios años se exige que cualquier desarrollo en IETF contemple por igual el soporte de IPv6 e IPv4, salvo que se demuestre explícitamente que no es preciso tener en cuenta alguno de los dos.

Dentro de cada área de trabajo, se configuran tantos grupos de trabajo como sean precisos, en función de la definición del capítulo de acción y objetivos que se vayan configurando, siempre por un tiempo definido por la consecución de los propios objetivos, aunque éstos pueden ser ampliados si es preciso[4].

En las siguientes secciones describimos la actividad actual y perspectivas futuras más destacadas de los diversos grupos de trabajo, organizados en las áreas de actividad antes mencionadas.

2. Internet

2.1. 6LOWPAN

Este grupo de trabajo busca resolver los problemas de utilización de IP sobre redes inalámbricas en pequeños dispositivos como sensores, con reducidas capacidades de batería y computación, y especialmente bajo coste, para lo cual se utiliza IEEE802.15.4[5].

El trabajo esta prácticamente concluido, exceptuando la compresión genérica de cabeceras, una guía de hoja de ruta e implementación, y la definición de los objetos para la gestión.

2.2. 6MAN

Dado que el trabajo de definición de los estándares básicos de IPv6 se concluyó hace años, se estableció el grupo de trabajo de mantenimiento de IPv6 con el objetivo de mantener el protocolo y solucionar problemas que se descubran durante su despliegue y operación[6].

El objetivo no es desarrollar grandes cambios o novedades del protocolo, para los cuales se establecerán los adecuados grupos de trabajo o se incluirán en el capítulo de otros ya existentes, si fuera apropiado.

En este momento, se trabaja en una veintena de documentos, entre los cuales los más destacados son la mejora del protocolo DAD (detección de direcciones duplicadas), la distribución de políticas de selección de direcciones, implicaciones de seguridad en el caso de fragmentación de ND (descubrimiento de vecindario) y en el caso de largas cadenas de cabeceras de extensión, generación de direcciones de privacidad estables.

2.3. CSI *(Cga & Send maIntenance)*

El protocolo SEND (descubrimiento de vecindario seguro) permite la protección de las funciones de resolución de direcciones y detección de no-alcanzabilidad, por medio de la verificación de la propiedad de las direcciones IPv6 y la protección de los mensajes, por medio de firmas digitales RSA y CGAs (direcciones generadas criptográficamente).

La labor del grupo de trabajo consistía en ultimar detalles relacionados con el uso de *proxies* y análisis de amenazas entre otros, y se puede considerar que prácticamente el trabajo se ha concluido[7].

2.4. DHC

Este grupo de trabajo ha desarrollado el protocolo DHCP (*Dynamic Host Configuration Protocol*), tanto para IPv4 como para IPv6, y su trabajo actual es el continuado desarrollo de protocolos adicionales como el registro de direcciones, CGAs, uso de DHCPv4 con

> “ Desde hace varios años se exige que cualquier desarrollo en IETF contemple por igual el soporte de IPv6 e IPv4, salvo que se demuestre explícitamente que no es preciso tener en cuenta alguno de los dos ”

transporte IPv6, opciones de redundancia de fallos, opciones de conjuntos de prefijos y soporte de RADIUS en equipamiento de banda ancha, reconfiguración y mejoras de seguridad.

Es un grupo de trabajo muy activo y es probable, que aún cuando se concluyan los múltiples trabajos actuales, sigan apareciendo otros muchos, dado el uso extendido de DHCP tanto en redes corporativas, como de ISPs y domésticas[8].

2.5. DMM *(Distributed Mobility Management)*

Este grupo de trabajo especifica soluciones de movilidad IP, redes de acceso y encaminamiento que permiten la configuración de las redes de tal forma que se facilite la distribución eficaz del tráfico, sin depender de puntos de anclaje centrales para la gestión de la sesiones de movilidad[9].

Casi todo su trabajo está pendiente de aprobación como RFC, aunque éste está bastante avanzado, con documentos que cubren prácticamente todos los aspectos indicados en su capítulo.

2.6. *Home Networking (homenet)*

Este es uno de los grupos de trabajo de más reciente creación con una misión muy interesante e importante, ya que se trata de resolver los problemas de las redes domésticas, cuyo crecimiento (número de dispositivos, subredes, extensión, etc.), plantea nuevos problemas como múltiples segmentos con tecnologías menos complejas que las de nivel 3, cambios en las redes debidos al despliegue de IPv6 (asignación de direcciones públicas, no-existencia de NAT) y comunicaciones extremo-a-extremo (facilitan nuevos servicios pero pueden exponer la seguridad)[10].

Hasta el momento solo ha sido aprobado como borrador del grupo de trabajo el documento de arquitectura para IPv6, y se esta trabajando en aspectos como la asignación de prefijos, el arranque de la red, soporte de *multi-homing*, DNS *multicast* extendido, arquitectura de delegación de nombres así como en el descubrimiento de nombres y servicios.

2.7. *Multicast Mobility (multimob)*

Este grupo de trabajo tiene como objetivo proporcionar guías para el soporte de multicast en entornos de movilidad. Para ello se centra especialmente en extensiones para movilidad IPv6, estando el trabajo bastante avanzado[11].

2.8. *Network-based mobility extensions (netext)*

El RFC5213 especifica el *proxy* de movilidad para IPv6. Se trata de un protocolo de movilidad basada en redes y ha sido incorporado en numerosos productos. Dado que su despliegue está ocasionando numerosas dudas y nuevas necesidades, este grupo de trabajo se ocupa de las mismas, complementando el trabajo que se viene realizando en otros grupos de trabajo[12].

2.9. *Port Control Protocol (pcp)*

Las “cajas intermedias” como NATs (*Network Address Translation*) y cortafuegos han tenido un despliegue muy significativo en todo tipo de redes durante muchos años y las aplicaciones han sido adaptadas para dichos entornos, con diversas soluciones que trabajan tanto directamente como indirectamente comunicando con dichas cajas.

El agotamiento de las direcciones IPv4 está obligando a los ISPs a desplegar en sus redes los denominados *Carrier Grade NATs* (CGN), incluso con configuraciones de doble NAT. Estos despliegues romperán esquemas actualmente contemplados por los protocolos existentes antes mencionados, y por lo tanto múltiples servicios y aplicaciones podrían dejar de funcionar.

Este grupo de trabajo tiene como objetivo estandarizar un protocolo de control de puertos cliente-servidor que permita un diálogo explícito con dichas cajas para la apertura y reenvío de tráfico a/desde puertos TCP (*Transmission Control Protocol*) o UDP (*User Datagram Protocol*) independientemente de la localización de dicha caja[13].

2.10. *Source Address Validation Improvements (savi)*

El propósito de este grupo de trabajo es el de estandarizar mecanismos que prevengan que nodos conectados en el mismo enlace IP utilicen de forma inapropiada las direcciones IP de otros nodos. De esta forma se mejoran las capacidades de filtrado de un modo más controlado[14].

El trabajo está bastante avanzado aunque numerosos documentos están pendientes de aprobación como RFCs.

2.11. *Softwires (softwire)*

Este grupo de trabajo especifica la estandarización de métodos de descubrimiento, control y encapsulado para conectar redes IPv4 a través de redes IPv6, así como redes IPv6 a través de redes IPv4, de tal modo que se faciliten múltiples e interoperables implementaciones, tanto en topologías “*hubs and spokes*” como “*mesh*”, y siempre que sea posible reutilizando tecnologías existentes. Así, por ejemplo, la mayoría de los mecanismos de túneles de *softwires* se basan en L2TP (*Layer 2 Tunneling Protocol*)[15].

Se trata de un grupo de trabajo que ha estado muy activo y que a través de numerosas reuniones específicas, una de ellas incluso hospedada por la *Universitat Politècnica de Catalunya* (UPC) en Barcelona, ha logrado avanzar en su trabajo de forma mucho más rápida de lo habitual en comparación con otros trabajos del IETF.

El trabajo de *softwires* es fundamental en la transición a IPv6, pues es la fuente principal de mecanismos que facilitan, aún a pesar del agotamiento de IPv4, continuar con dicha transición, evitando en la medida de lo posible perjudicar a usuarios, servicios y aplicaciones ya existentes.

La cantidad de trabajo realizada es ingente, tanto como ingente es el trabajo aún pendiente, y es por ello que su capítulo ha sido modificado en varias ocasiones por la necesidad de acoger otros trabajos relacionados y necesarios para finalizar la transición a IPv6.

2.12. *Sunsetting IPv4 (sunset4)*

Este grupo de trabajo tiene como objetivo la estandarización de tecnologías que faciliten el “apagado” ordenado de IPv4 en el contexto de su agotamiento mientras IPv6 está siendo desplegado[16].

Por ejemplo, los trabajos actuales consisten en revisar las tecnologías CGN (*Carrier Grade NAT*), documentar los problemas y requerimientos para su estandarización y determinar si es una tecnología apropiada para el apagado de IPv4.

Obviamente, se trata de un conjunto de trabajos de suma importancia.

3. Operaciones y Gestión

3.1. *IPv6 site renumbering (6renum)*

A pesar de que uno de los objetivos iniciales de IPv6 era facilitar el renumerado de las redes, sigue siendo una tarea relativamente complicada, tal como se describe en el RFC5887.

> “ Home Networking (homenet) es uno de los grupos de trabajo de más reciente creación con una misión muy interesante e importante, ya que se trata de resolver los problemas de las redes domésticas, cuyo crecimiento plantea nuevos problemas ”

Ello implica que, especialmente las redes empresariales, pueden verse abocadas a utilizar direccionamiento independiente del proveedor (PI), lo que a la larga tendría nefastas consecuencias para el continuado crecimiento de Internet por su impacto en las tablas de encaminamiento.

El objetivo de este grupo de trabajo, por lo tanto, es analizar y documentar las posibles prácticas para el renumerado de IPv6, identificar problemas, y consecuentemente facilitar el trabajo futuro para idear soluciones en otros grupos de trabajo si fuera preciso[17].

3.2. *IPv6 operations (v6ops)*

El despliegue de IPv6 tiene evidentes implicaciones en la operación de las redes, tanto IPv4 como IPv6, motivo por el cual este grupo de trabajo se ocupa de desarrollar guías para la operación de Internet IPv4/IPv6 y proporciona detalles operacionales para el correcto despliegue de IPv6 en redes IPv4 ya existentes, así como en nuevas instalaciones[18].

El objetivo más inmediato son las fases actuales de despliegue más que etapas más avanzadas, que por tanto tienen menos prioridad en el trabajo a realizar.

Los documentos que resultan de este grupo de trabajo no son normativos, pues su objetivo no es capturar las necesidades de nuevas soluciones sino tan sólo describir qué aproximaciones son correctas y cuales no y, por lo tanto, tampoco se pretende crear nuevos protocolos.

Obviamente éste es otro de los grupos que tiene una ingente cantidad de trabajo ya realizado, y al mismo tiempo le queda todavía mucho trabajo pendiente, que irá creciendo con el despliegue de IPv6 según se vaya adquiriendo experiencia en el mismo.

4. Transporte

4.1. *Behavior engineering for hindrance avoidance (behave)*

El objetivo de este grupo de trabajo es la generación de documentos para permitir que NAT IPv4-IPv4 y la traducción IPv6-IPv4 funcionen de forma lo más determinística posible[19].

Se contemplan los escenarios: red IPv6 a Internet IPv4, Internet IPv6 a red IPv4, red IPv6 a red IPv4 y red IPv4 a red IPv6.

Gran parte del trabajo de este grupo ya se ha realizado, pero sigue habiendo necesidad de progresar en nuevos campos, según otros grupos de trabajo, como *softwires* o *v6ops*, van avanzando en sus propios trabajos.

Notas

[1] <https://www.ietf.org/>.
[2] *Getting Started in the IETF*. <https://www.ietf.org/newcomers.html>.
[3] *Active IETF Working Groups*. <http://datatracker.ietf.org/wg/>.
[4] <http://datatracker.ietf.org/wg/6lowpan/charter/>.
[5] <http://tools.ietf.org/wg/6man/>.
[6] <http://datatracker.ietf.org/wg/csi/charter/>.
[7] <http://datatracker.ietf.org/wg/dhc/charter/>.
[8] <http://datatracker.ietf.org/wg/dmm/charter/>.
[9] <http://datatracker.ietf.org/wg/homenet/charter/>.
[10] <http://datatracker.ietf.org/wg/multimob/charter/>.
[11] <http://datatracker.ietf.org/wg/netext/charter/>.
[12] <http://datatracker.ietf.org/wg/pcp/charter/>.
[13] <http://datatracker.ietf.org/wg/savi/charter/>.
[14] <http://datatracker.ietf.org/wg/softwire/charter/>.
[15] <http://datatracker.ietf.org/wg/sunset4/charter/>.
[16] <http://datatracker.ietf.org/wg/6renum/charter/>.
[17] <http://datatracker.ietf.org/wg/v6ops/charter/>.
[18] <http://datatracker.ietf.org/wg/behave/charter/>.

Redes Definidas por Software e IPv6: Situación actual

Eduardo Jacob
Profesor titular de Ingeniería Telemática de la Universidad del País Vasco / Euskal Herriko Unibertsitatea

<eduardo.jacob@ehu.es>

Resumen: *Una de las tecnologías que con más fuerza ha surgido en los últimos tiempos, es la asociada a las SDN, acrónimo de "Software Defined Networks" o en castellano "Redes Definidas por Software", que se materializan en el protocolo OpenFlow. En sus momentos iniciales, los detractores de OpenFlow argumentaban que no soportaba IPv6. El presente artículo busca dos objetivos, el primero realizar una breve presentación, limitada por definición, de los conceptos de SDN y OpenFlow, y por otro, analizar la veracidad de ese argumento. Como se verá, esto aun siendo cierto en su momento, va a dejar de ser un problema a medio plazo.*

Palabras clave: *Compatibilidad IPv6, OpenFlow, redes definidas por software, SDN, Software Defined Networks.*

Autor

Eduardo Jacob Taquet es Ingeniero Industrial por la Universidad del País Vasco/ *Euskal Herriko Unibertsitatea* y doctor por la misma Universidad. Es profesor Titular de Ingeniería Telemática y en la actualidad dirige el departamento de Ingeniería de Comunicaciones en el que coordina el grupo de investigación I2T de la UPV/EHU. Ha dirigido varias tesis doctorales y ha participado en varios proyectos europeos del sexto y séptimo Programa Marco. En la actualidad su área de trabajo engloba las SDN (*Software Defined Networks*). En este sentido, el grupo de investigación ha desplegado una infraestructura basada en OpenFlow, para soportar tanto la investigación en redes como la operación clásica en su universidad (*EHU OpenFlow Enabled Facility*, EHU-OEF). En esta línea de trabajo se engloban también la participación en los proyectos del séptimo programa marco ALIEN "*Abstraction Layer for Implementation of Extensions in programmable Networks*" en el que se investiga la creación de una capa de abstracción para integración de dispositivos no OpenFlow en redes definidas por software y SECRET "*SECurity of Railways against Electromagnetic aTtacks*".

1. Introducción

Dentro de los "*buzzwords*" que los expertos en redes y tecnologías de la información manejan estos últimos tiempos sin duda destaca el de SDN, acrónimo de "*Software Defined Networks*" o en castellano "Redes Definidas por Software". Probablemente bastantes lectores habrán oído hablar de este término, o tal vez, incluso con más frecuencia de OpenFlow, el estándar que se considera como la actual encarnación de esta tecnología.

El objeto de este artículo es tratar de revisar la relación de IPv6 con OpenFlow, dado que en sus primeras versiones, en los tiempos en los que era un proyecto del "*Clean Slate Program*" de la Universidad de Stanford, se le achacaba como fallo o limitación su incompatibilidad con IPv6.

2. Redes Definidas por Software

Antes de empezar a hablar de este tema, conviene hacer una breve descripción de la tecnología. De manera muy simplificada y sin entrar en mucho detalle, podemos decir que las Redes Definidas por Software preconizan una separación clara entre el plano de control y el de datos, así como la definición de un protocolo que intercomunica estos dos planos.

De manera generalizada (aun cuando no es totalmente cierto) también se suele adjudicar a esta tecnología un control centralizado sobre todos los elementos de comunicación de la red. Ha habido otras iniciativas con fines similares, siendo la más cercana en el tiempo la llevada a cabo por el IETF (*Internet Engineering Task Force*) con el grupo de trabajo FORCES [1]. Sin embargo, en la actualidad, la implementación más usada, la que más soporte industrial y mediático tiene es OpenFlow [2]. Este protocolo es una evolución de la versión original diseñada por Stanford, gestionado por una organización sin ánimo de lucro [3] dedicada al despliegue de las SDN y a la estandarización del protocolo.

Analicemos estas características que hemos mencionado. La primera, la referente a la separación del plano de control del de datos, de hecho, convierte a los dispositivos de comunicaciones clásicos como enrutadores o conmutadores o incluso dispositivos de mayor "inteligencia" como cortafuegos, en equipos muy similares a nivel de hardware.

En realidad, dicho hardware proporciona siempre puertos interconectados por un *backplane* que deja pasar, o no, paquetes de un puerto a otro, modificando en caso necesario alguno de sus campos (por ejemplo: insertar o retirar etiquetas VLAN o MPLS, cambiar direcciones MAC, modificar direcciones de origen y destino, etc.).

En OpenFlow, el paradigma empleado para realizar estas acciones es el flujo. En la versión 1.0 (la que hoy en día está más desplegada), el flujo se puede definir en base a un patrón que se compara con las cabeceras de los paquetes que entran por un puerto como se muestra en la **figura 1**.

En el caso de que se detecte el patrón establecido, se llevará a cabo una de las acciones definidas: enviar al controlador el paquete, reenviarlo por otro puerto, eliminarlo, o incluso modificarlo. El protocolo OpenFlow, define cómo insertar o retirar estas reglas de la tabla de flujos de un equipo (por definición, un conmutador OpenFlow), como detectar funcionalidades o tratar la información que le llega del mismo.

La segunda característica tiene unas implicaciones mucho más sutiles.

Por un lado, la existencia de un protocolo promueve el diseño y la producción de un equipamiento estandarizado para todas las aplicaciones. La implementación interna

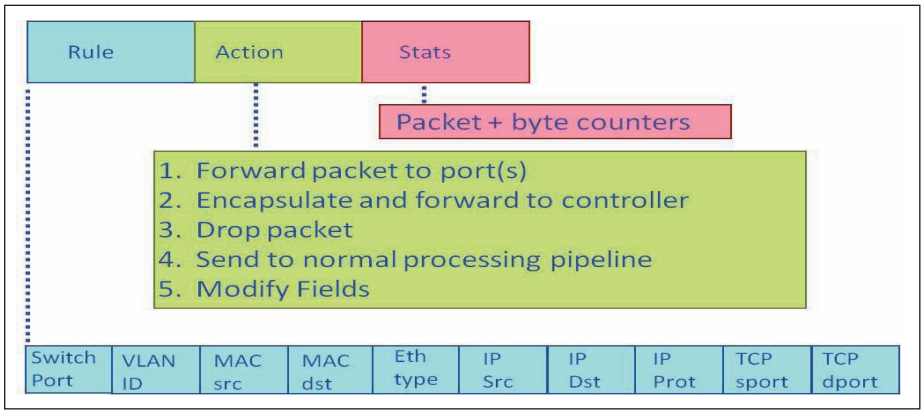


Figura 1. Definición de un flujo en la tabla de flujos, version 1.0 (Stanford).

> “Podemos decir que las Redes Definidas por Software preconizan una separación clara entre el plano de control y el de datos, así como la definición de un protocolo que intercomunica estos dos planos”

puede variar, con el grado de maniobra que permite la utilización de *chipsets* de un pequeño número de fabricantes, permitiendo la aparición de equipamiento compatible con gran variedad de densidad de puertos, rendimientos y costes.

En segundo lugar, aparece un mercado de ecosistemas completos para la programación (de ahí el término de redes definidas por software), gestión y administración de dichos equipamientos para implementar las funcionalidades que las modernas redes de hoy en día necesitan.

Afortunadamente, estos ecosistemas no son monolíticos. Constan por un lado de sistemas operativos que van a arropar las funcionalidades que el protocolo ofrece y a ofertar llamadas al sistema (una API) que serán empleadas por el segundo componente, las aplicaciones, para implementar las funcionalidades de la red.

Es necesario destacar que, en este contexto, una aplicación puede ser desde la lógica de un conmutador con aprendizaje, pasando por la implementación de un protocolo de enrutamiento hasta una aplicación que optimiza la distribución de video. Véase en la **figura 2** el esquema de este ecosistema.

En este momento existen varios sistemas operativos de red de código abierto y están empezando a aparecer sistemas comerciales. Esto promoverá la aparición de aplicaciones que se ejecutarán sobre todos ellos. Finalmente, queda por comentar que los grandes clásicos del equipamiento de red han abrazado esta iniciativa en diverso grado, desde un soporte claro hasta una reorientación de los productos actuales para ofertar soluciones que incluyen algunas de estas funcionalidades.

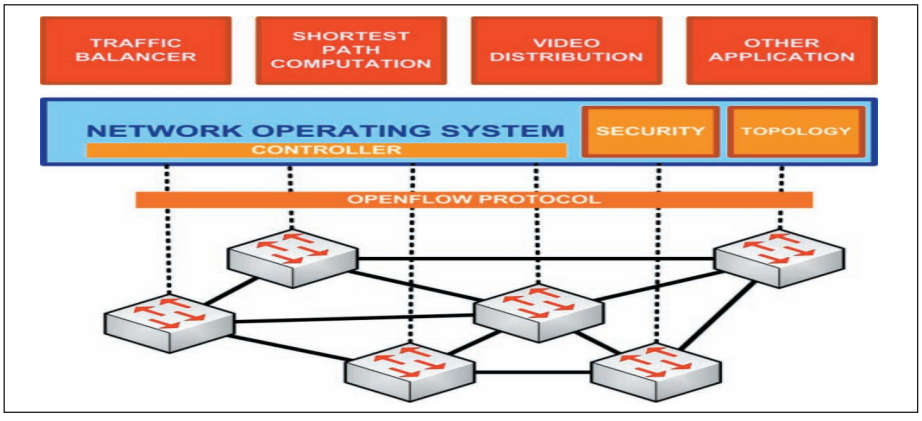


Figura 2. Ecosistema OpenFlow.

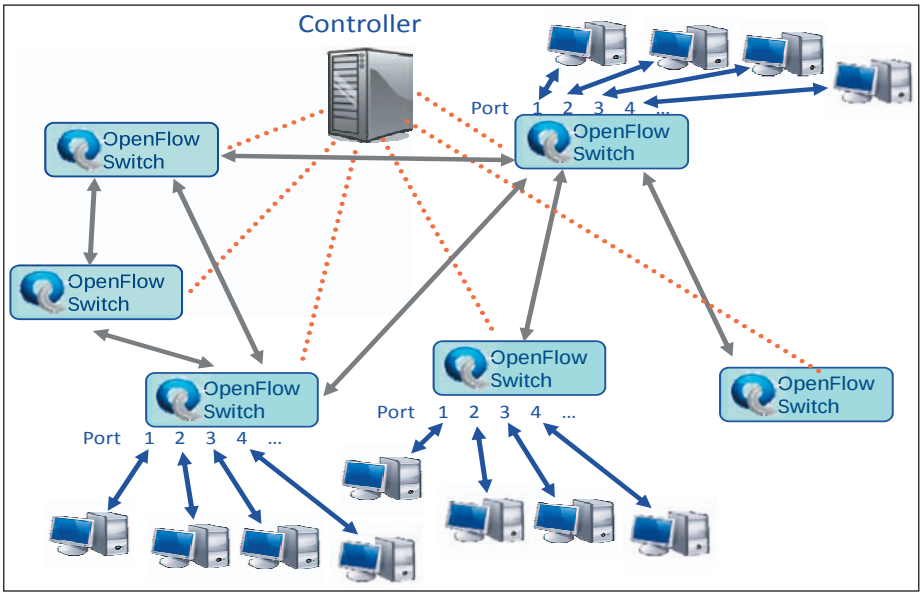


Figura 3. Red basada en OpenFlow.

Una característica adicional, aun cuando como hemos comentado no es imprescindible, sí es percibida por muchos como la mayor ventaja. Con una visión global de la red, podemos transformar soluciones que tradicionalmente se han llevado a cabo por medio de procesos colaborativos que convergen iterativamente en una solución estable, a una reprogramación directa del comportamiento de una red. Por ejemplo, ante una caída de un enlace podemos reorganizar en milisegundos los flujos que constituyen nuestro tráfico.

La solución puede ser precalculada y simulada por adelantado. En este sentido, es un clásico de la literatura de OpenFlow la charla impartida por Urs Hoelzle de Google [4] en la que se explica cómo implementan esta tecnología en su propia red. Una red basada en OpenFlow pasa a tener el aspecto que se muestra en la **figura 3**, en la que el comportamiento del equipamiento no lo define su posición en el esquema, sino su programación.

3. Compatibilidad de OpenFlow con IPv6

Después de esta introducción, en la que quedan infinidad de aspectos sin tocar, podemos pasar a estudiar y comprender la compatibilidad de IPv6 y de OpenFlow.

En la definición de flujo de la **figura 1** y que corresponde a la versión 1.0 (2009), los campos de direcciones IP que se pueden emplear para definir el patrón a buscar corresponden exclusivamente a la versión IPv4. Lo mismo sucede con el resto de los campos. Es decir no podemos definir flujos que empleen el campo de dirección IP origen o destino de tipo IPv6, ni otros aspectos de la cabecera IPv6. Si fuera necesario segregar el tráfico IPv6 podremos crear un flujo que recoja todos los paquetes de IPv6, sin más que aplicar la máscara sobre el campo *Ethertype,* que para IPv6 es 0x86dd, pero no podremos realizar ningún tratamiento adicional sobre el resto de campos. Podemos decir que es una estrategia del tipo “vive y deja vivir”.

Desde el punto de vista operativo, esto no quiere decir que no se pueda transitar IPv6 sobre la infraestructura, sino simplemente que no vamos a poder implementar aplicaciones que requieran acceso a los campos de dicha cabecera, por ejemplo crear un enrutador IPv6, con un conmutador OpenFlow.

> “Aun cuando la disponibilidad actual de equipamiento OpenFlow emplea casi exclusivamente el protocolo 1.0, la próxima generación de conmutadores compatibles sí soportará IPv6 de manera completa”

Esta limitación fue claramente detectada y denunciada por los detractores de OpenFlow. La *Open Networking Foundation* produjo en 2011 la versión 1.2 que proporcionaba no sólo soporte para la versión IPv6, sino un mecanismo de definición generalizado de máscaras. Poco después, en 2012, la versión 1.3 implementó además el soporte para la definición de máscaras que implican a las cabeceras de extensión IPv6. La versión actual es la 1.3.1

4. Conclusiones

Aun cuando la disponibilidad actual de equipamiento OpenFlow implementa casi exclusivamente el protocolo 1.0, la próxima generación de conmutadores compatibles sí soportará IPv6 de manera completa, permitiendo aplicaciones que trabajen con IPv6 de la misma manera que en la actualidad lo hacen con IPv4.

La evolución de esta tecnología presenta muchas incógnitas. Es bastante razonable pensar que desde el punto de vista del equipamiento, la evolución será (por motivo de los costes de inversión) bastante más lenta que en el área del software.

Por otra parte, estas tecnologías pueden representar una nueva manera de enfocar el negocio de las redes y esto hace que se puedan esperar movimientos para frenar o al menos modificar el escenario. Un ejemplo de esto es el recientemente anunciado controlador *open source* Daylight [5] promovido por un consorcio liderado por Cisco e IBM y en el que otros “grandes” de esta industria, como HP, Citrix, and NEC participan.

Esto plantea un escenario en el que la función estandarizadora de la *Open Networking Foundation* puede quedar en entredicho y en el que el actual ecosistema puede verse afectado, en principio a medio plazo favorablemente.

A modo de resumen, podemos decir que las redes definidas por software están arrancando con gran empuje, que lo mejor está por venir y que este escenario global e imparable de IPv6 que por medio de este especial de ***Novática*** tratamos de promover se verá igualmente beneficiado.

Referencias

[1] IETF. FORCES: *Forwarding and Control Element Separation*. <https://datatracker.ietf.org/wg/forces/charter/>.

[2] Open Networking Foundation. *ONF White Paper: “Software-Defined Networking: The New Norm for Networks”*, 13 de abril de 2012. <https://www.opennetworking.org/images/stories/downloads/white-papers/wp-sdn-newnorm.pdf>.

[3] Open Networking Foundation. <https://www.opennetworking.org/>.

[4] Urs Hoelzle. *“OpenFlow@Google”*, Open Networking Summit 2012, Santa Clara.

[5] Matthew Palmer. “*Exclusive: Shining the Spotlight on Daylight-What you MUST know about the new open-source SDN Controller*”. SDNCentral, 8 de febrero de 2013. <http://www.sdncentral.com/companies/spotlight-on-daylight-sdn-consortium-open-source-controller/2013/02/>.

Sebastià Justicia Pérez
Diputació de Barcelona; socio sénior de ATI

<sjusticia@ati.es>

Interoperabilidad en los sistemas de información públicos

***Resumen**: La coyuntura socio económica condiciona fuertemente la dinámica actual evolutiva de los sistemas de información. Desde los primigenios esfuerzos de la interconexión de redes de comunicaciones a la generación de middleware que facilitara la amortización de los proyectos software, hemos llegado a la necesidad de interoperabilidad de los datos, de la información o del conocimiento generados corporativamente. La interoperabilidad emerge como elemento necesario para transitar hacia el objetivo de la maximización de prestaciones y funcionalidades de los servicios basados en las Tecnologías de la Información (TI) con un aporte drásticamente menor de recursos al efecto. Describimos así los precedentes, la fase actual a nivel tecnológico, la voluntad política y la consiguiente plasmación legislativa y reglamentaria. Trazamos esquemáticamente el tránsito hacia nuevas etapas a recorrer para la asunción de la interoperabilidad en la prestación de servicios digitales y la consiguiente obtención de valor público.*

***Palabras clave**: Gobernanza TI, interoperabilidad, legislación tecnológica, middleware, servicios digitales.*

1. Introducción

El sector público se ha visto sometido a un requerimiento ineludible de racionalización de los recursos que utiliza para dar satisfacción a los deberes inherentes emanados del marco jurídico e institucional.

Las pasadas décadas han estado caracterizadas en materia de construcción de sistemas de información en la administración por una relativa bonanza económica que permitía un gasto auditado de forma laxa y, en consecuencia, un crecimiento inercial de la informatización motivado por la tecnificación *per se* de sus ámbitos productivos. No ha prevalecido un ejercicio sistematizado y riguroso de evaluación de rentabilidad, de compromiso de retorno de valor de los ingentes recursos destinados a tales proyectos.

Este interregno en la fiscalización del gasto ha concluido. El ambiente recesivo obliga a justificar las inversiones y los mantenimientos en los servicios de las tecnologías de la información (TI), a evaluar las obsolescencias y a comprometerse en los retornos de valor agregado. Nuestra interlocución, como profesionales de los sistemas de información, ha de ser, en referencia a las instancias directivas de las corporaciones, relevante en términos de suministro de valor, de riesgo asumido y de recursos implicados.

La interoperabilidad de los sistemas de información y de todo aquello por ellos generado, datos, información, conocimiento y valor, trascienden a la elicitación de requisitos funcionales de las aplicaciones, constituyendo un planteamiento estratégico sin cuya presencia un proyecto informático en el ámbito público y en el momento actual, no debería ser acometido.

¿Qué debería exigirse en el abordaje de un ejercicio inversor emanado del erario público?

Consideramos entre otros los siguientes criterios: el menor coste total de propiedad posible, la mayor aportación de servicios a la ciudadanía, la observancia ejemplarizante de la legislación y reglamentación en materia tecnológica promulgada, la sostenibilidad y evolución en el tiempo del sistema tecnificado, la accesibilidad asegurada a toda la ciudadanía, el uso de estándares públicos de los formatos producidos y la extensión de su utilidad a todos los segmentos sociales susceptibles de ser receptores del valor generado y no únicamente de los sectores poblacionales subsidiarios. Es por ello que la interoperabilidad ha de trascender al mero desiderátum de aprovechamiento del producto suministrado por el servicio digital sea, en el estadio que sea (dato, información, conocimiento o valor), para formar parte de la genética de los sistemas de información desde su concepción.

> “La interoperabilidad de los sistemas de información y de todo aquello por ellos generado… (constituye)… un planteamiento estratégico sin cuya presencia un proyecto informático en el ámbito público y en el momento actual, no debería ser acometido”

Se ha publicado una profusa literatura para el ordenamiento de este ámbito. Se ha superado el simple hecho discursivo bienintencionado, para normativizar sin encorsetamientos pero sin ambigüedades generadoras de incertidumbres que pudieran paralizar las iniciativas que cada vez con más impulso se acometen en aras de la interoperabilidad [1].

El Esquema Nacional de Interoperabilidad (ENI), regulado por el Real Decreto 4/2010, está inspirado y recoge las recomendaciones de las instituciones europeas en materia de e-gobierno. Ha sido elaborado de forma idiosincrásica por las instancias competentes en el ámbito tecnológico del gobierno estatal.

Las normas técnicas que progresivamente se van publicando ayudarán a definir los marcos de interoperabilidad institucionales. La asunción de la interoperabilidad no es sino un paso más en la consecución de la madurez de lo que algún día habrá de constituir el corpus consolidado de la ingeniería informática en el sector público con los necesarios elementos de estandarización, de racionalización, de minimización del gasto así como de optimización de los servicios digitales útiles al ciudadano.

2. Precedentes de la conectividad de los sistemas

Desde que el primer bit generó el primer *output* en informática, compartir, hacer extensiva una información generada ha sido objetivo deseado en los ámbitos cibernéticos. Podríamos datar el origen significativo por relevante de esta necesidad, en la iniciativa de la oficina de proyectos de la administración norteamericana DARPA (*Defense Advanced Research Projects Agency*) para la interconexión de sus ordenadores como mecanismo de contingencia frente a un desencadenamiento de hostilidades de gran calado en plena Guerra Fría. Afortunadamente para todos, el sistema no tuvo que ser puesto a prueba. Quedó sin embargo como prototipo tecnológico de comunicación. In-

> “El espíritu del ENI pretende, con el fomento de políticas de estandarización, liberación de código y compartición de activos, potenciar el armado de la citada sociedad del conocimiento”

corporándose además la implementación del futuro y exitoso protocolo de comunicaciones *IP*.

La eclosión de tecnologías software y hardware en los ochenta de la pasada centuria permitió unos patrones arquitectónicos particularizados a necesidad. Sistemas operativos abiertos, desarrollo del protocolo *TCP/IP*, capacidad de cálculo descentralizada (*PC*, estaciones de trabajos, miniordenadores), sistemas gestores de bases de datos, herramientas de productividad en la generación de código tipo *CASE*, interfaces de usuario gráficas, originaron un nuevo escenario en cuanto a expectativas de aprovechamiento de la informática. El incremento geométrico de la generación de datos que todo esto supuso, trajo consigo de forma inherente la necesidad de construir interfaces para las aplicaciones. Nacieron así las primeras especificaciones de software de intercambio, los llamados *middleware,* precedentes en el ámbito tecnológico de lo que hoy convenimos en llamar interoperabilidad.

El estándar abierto más importante por pretencioso en el objetivo de la interconexión podríamos decir que fue *CORBA*. Este prolijo *middleware* surgido en el foro OMG (*Object Management Group*) constituyó sin duda elemento de referencia tecnológica durante muchos años para los ingenieros de interfaces. La relativa complejidad de su implementación sin embargo, limitó su extensión a modo de estándar universal de software base de conexión.

Se promueve posteriormente la filosofía SOA (*Service Oriented Architecture*), que pretende justificar la demanda de recursos de la profesión informática a las instancias directivas y financieras cada vez más reticentes en la liberación no justificada de los mismos para la generación de proyectos de TI.

A modo ilustrativo esbozamos la situación que muchos y muchas profesionales de la informática hemos presenciado. En la reunión de un consejo directivo de la corporación, el director de sistemas tecnológicos comunicó: “*Ahora si seremos productivos, basaremos nuestros sistemas de información en una arquitectura tecnológica orientada a servicio*” a lo que el responsable financiero con cierto escepticismo y la tesorería exhausta por proyectos tecnológicos pretéritos fracasados espetó: “*¿pues así, a qué estaba orientada hasta ahora la arquitectura?*”.

Los sistemas de información en la división productiva socioeconómica se encuadran en el sector servicios. La profesión informática imbuida de cierta introspección y de virtuosismo autocomplaciente no era enteramente consciente de que constituía una pieza más del entramado productivo, que formaba parte de empresas en las cuales se identificaba la informática más a gasto que a retorno de valor.

Enmarcado en este contexto tecno-empresarial junto a la extensión ubicua de la red Internet, su estándar más relevante, el *Web*, y un formateado de datos más transparente a precio de sobrecarga de *markup* como es el esquema *XML*, se desarrolla el marco tecnológico Servicios Web.

Este estándar relajaba en parte la complejidad de *CORBA* con una estructura aparentemente más liviana. Los datos se empaquetan, se envían, se anuncian, se descubren y se recepcionan en la dialéctica proveedor, usuario con protocolos XML en buses de conectividad [2].

Este *middleware* sería a fecha de hoy el estándar imperante mayoritario. Emergen asimismo ámbitos particularizados como los microelementos interconectados basados en el Internet de las Cosas (*Internet of Things*, *IoT*) que supondrán una segunda oleada de necesidad de interoperabilidad ya abordada por las respectivas instancias europeas competentes en materia de nuevas tecnologías [3].

3. Significado de la interoperabilidad en la sociedad del conocimiento

Define el Esquema Nacional de Interoperabilidad de forma plausible tal concepto como la capacidad de los sistemas de información, y por ende de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos.

Así en el ámbito público, los datos generados por los respectivos sistemas de información y dentro de la tipificación de privacidad y seguridad correspondiente, se han de publicitar de forma transparente y se han de poder obtener sin restricciones tecnológicas.

Nos encontramos delante de un cambio copernicano en la e-administración. Deja de ponerse en valor la patrimonialización por restricción del acceso a la información de origen público para, en sentido diametralmente opuesto, poder valorizar el quehacer corporativo en la maximización de la difusión de datos generados que permita alinear las administraciones al paradigma productivo de la sociedad informacional. Estamos presenciando cada día nuevas iniciativas de las administraciones públicas de liberación de información, de *open data*.

La sociedad informacional se ha modelado en el siguiente esquema de círculo virtuoso:

1) Los sistemas de información tecnificados digitalmente generan **datos** con herramientas transaccionales como las *Data WareHouse, ERP, CA computing aided, CRM …*
2) Los datos en un entorno asistido de mayor complejidad producen **información** significativa en el negocio en cuestión: *Data Mining, Business Intelligence*, sistema de ayuda a la toma de decisiones, *OLAP*, bases de datos *NoSQL*, bases de datos multidimensionales …
3) Tal información es tratada de forma relevante según su objetivo finalista para la obtención de **conocimiento**. Aquí juegan todavía un papel importante las habilidades del factor humano profesionalizado, con la ayuda de paradigmas tecnológicos como la inteligencia artificial entre otros.
4) El conocimiento no es más que el *input* cognitivo, cuya aplicación en el entramado socio productivo conveniente genera **valor** material, plusvalía y/o valor inmaterial, prestación o satisfacción a modo de servicios.

El sistema se retroalimenta tomando como entrada del primer paso, de los sistemas de información transaccionales, el resultado del cuarto, el conocimiento, una vez recorrido su ciclo de vida de amortización.

Este mecanismo emerge como el generador de crecimiento socio-económico ya sea por la provisión de servicios avanzados en el tercer sector o por mejora de rendimientos en el primero, provisor de materias primas y en el segundo, manufacturero e industrial.

No parece factible un tránsito efectivo a la sociedad del conocimiento sin el despliegue de la interoperabilidad. Cualquier óbice al libre acceso al conocimiento generado por los sistemas de información, frustraría este paradigma socio-productivo.

La interoperabilidad no es más que un elemento facilitador, un factor necesario en

dicho encaje. Son los servicios fundamentados en el conocimiento los que generan plusvalía. Coartar el acceso al conocimiento deprimiría los sectores restringidos en su acceso, pero posteriormente a toda la sociedad provocando un quebranto estructural del modelo reproductor de valor. El espíritu del ENI pretende, con el fomento de políticas de estandarización, liberación de código y compartición de activos, potenciar el armado de la citada sociedad del conocimiento vertebrando en el plano social, económico y político nuestra sociedad en el presente siglo [4].

4. Alineamiento con la gobernanza TI

A diferencia del sector privado, con una extendida traslación a su modo organizativo, en las administraciones no se ha aplicado todavía con la extensión que merece la gobernanza de las tecnologías de la información (TI).

Difícilmente podemos publicitar con credibilidad y solidez a la ciudadanía una propuesta de e-gobierno (*front office*) si no regimos nuestros sistemas de información corporativos con un esquema de eficacia en la consecución de objetivos y de eficiencia en el uso de los recursos basados en marcos de gobernanza TI (*back office*). Las administraciones han generado especificaciones, normas y reglamentos en diferentes ámbitos de los sistemas de información: protección de datos personales, seguridad operativa, ingeniería del software, gestión de riesgos, contratación de activos y servicios.

Sin embargo, hay una ausencia clamorosa de directrices de gobierno TI específicas del entorno público. Con la meritoria excepción del estándar *KING III* de *e-governance* del gobierno sudafricano, no hemos encontrado otra especificación pública en la materia.

El remedo aplicado con imaginación y pericia por profesionales responsables en la materia ha sido aplicar el estándar *CobiT* a la cosa pública. Con las necesarias equivalencias de los conceptos del ámbito privado como son ganancia, accionistas, mercado, clientes, etc., la versión *CobiT 5* recientemente publicada contempla en sus especificaciones las organizaciones sin ánimo de lucro y las administraciones públicas.

Sin entrar de forma exhaustiva en una propuesta de implementación del estándar en toda su extensión, haremos algunas consideraciones por lo que respecta al concepto de interoperabilidad que es recogido en un proceso del documento de tal especificación *Identificar y construir soluciones BAI03* del dominio "*Construir, adquirir e implementar*" del área de Gestión.

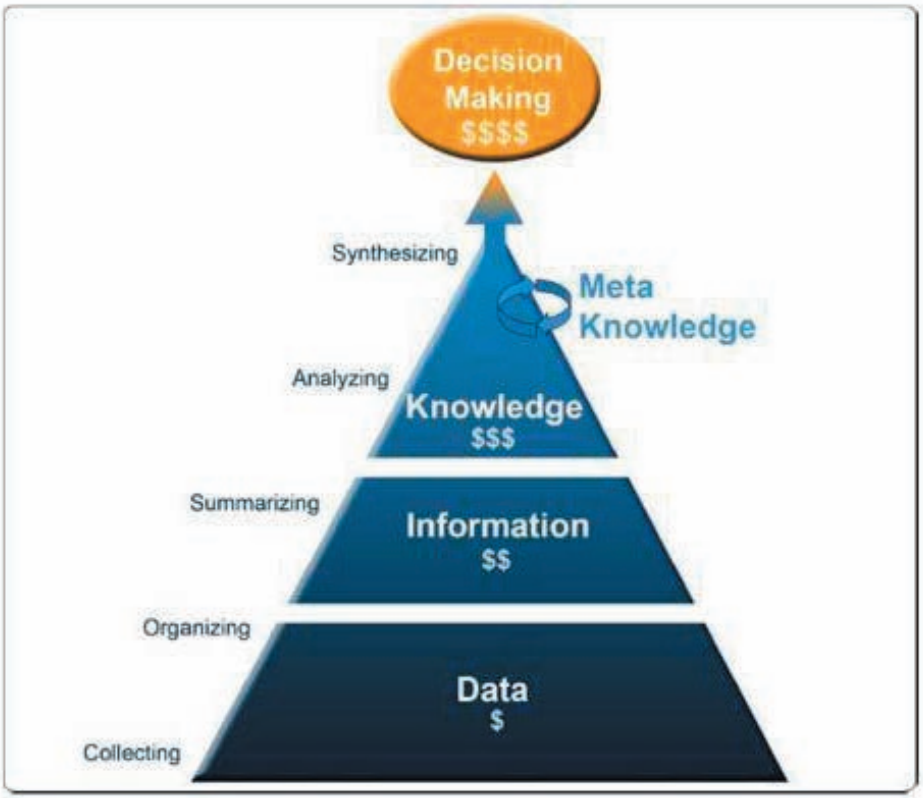


Figura 1. Ciclo de la información corporativa en el esquema COBIT 5 (Fuente: ISACA).

El primer requerimiento es asegurar la interoperabilidad de los componentes de la solución informática.

El segundo es el precepto de testar los requisitos no estrictamente funcionales de la solución, entre ellos la interoperabilidad. Sin embargo la verdadera plasmación de la interoperabilidad reside en uno de los facilitadores (*enablers*) de la gobernanza IT según *COBIT 5*, la información, a la cual se dedica un completo modelo de atributos y requerimientos (*IM Information Model*).

La **figura 1** representa el ciclo virtuoso de la información en los procesos TI corporativos tal como se remarcaba en la **sección 3** y coincidente con la formulación *CobiT 5*.

Esta arquitectura posee aspectos relevantes en cuanto a los elementos facilitadores de la gobernanza TI.

Focalizaremos en particular en la información desde la perspectiva de la interoperabilidad. La información ha de poseer unas expectativas de logro a modo de dimensiones evaluables de objetivos. Se plantean quince dimensiones en el *IM* de las cuales en la focalización de la interoperabilidad significamos las siete siguientes:

1) **Relevancia** como el grado en que la información es aplicable y útil para la tarea a realizar.
2) **Representación concisa** como medida en que la información se representa de forma compacta.
3) **Representación consistente** como el grado en que la información es presentada en el mismo formato.
4) **Interpretabilidad** como el grado en que la información está expresada en los idiomas apropiados, símbolos y unidades y donde las definiciones son claras.
5) **Comprensibilidad** como el grado en que la información sea fácil de asimilar.
6) **Facilidad de manipulación,** ductilidad, como el grado en que la información es fácil de tratar y se aplica a diferentes posibles tareas
7) **Disponibilidad** como la cualidad en que la información está accesible cuando se requiera y de forma fácil y rápida.

Éstos serían según la especificación de gobernanza TI los objetivos deseables a conseguir con la información obtenida, tratada y generada para una óptima interoperabilidad.
La información según el estándar citado, posee un ciclo de vida de seis fases, desde la **planificación,** la **obtención,** el **almacenamiento,** la **compartición** y el **uso** hasta su **eliminación** final.

La interoperabilidad entendida en un sentido global abarcaría todas estas fases. Haremos sin embargo énfasis en la de compartición, objetivo actualmente prioritario y candente para las administraciones públicas.

> “El Esquema Nacional de Interoperabilidad es una guía suficiente para este proyecto estratégico de racionalización de los recursos públicos. Nos propone una vectorización del concepto identificando tres dimensiones, organizativa, semántica y técnica”

La compartición la entenderemos como la fase en la que la información está disponible para su uso a través de un método de distribución. Las actividades en esta fase pueden referirse a los procesos involucrados en obtener la información en los repositorios donde ésta puede ser accedida y utilizada.

Finalmente y contemplando diferentes conceptos y estadios evolutivos que por el contexto se posea del concepto “información”, el estándar propone la segmentación en seis capas a las cuales otorga varios atributos. Se pretende así objetivar el uso del concepto para unificar expectativas respecto del mismo.

Tal estructuración en capas pretende abarcar todas las perspectivas, todas las acometidas con las que se desee abordar un proyecto de sistemas de información. Cobra plenitud así la asunción del negocio TI como elemento esencial en la consolidación de la sociedad informacional. Al desarrollar una nueva aplicación, el *IM* modelo de información de *CobiT 5* se puede utilizar para definir las especificaciones de la aplicación y la información asociada, así como los modelos de datos.

Los atributos de la información del *IM* se pueden utilizar para orquestar los procesos de negocio. En el diseño y las especificaciones del nuevo sistema tecnificado digitalmente es necesario esquematizar:

1) Capa **física**, ¿Dónde se almacena la información? ¿Qué medios de transmisión se utilizarán?
2) Capa **empírica**, ¿Cómo puede la información ser accedida?
3) Capa **sintáctica**, ¿Cómo se estructurará la información y cómo se interroga el repositorio codificado?
4) Capa **semántica**, ¿Qué tipo de información se genera? ¿Cuál es el nivel de información conseguido?
5) Capa **pragmática**, ¿Cuáles son los requisitos de conservación? ¿Qué otra información es necesaria para que esta información sea útil y usable?
6) Capa **social**, ¿Qué valor añadido se obtiene de su utilización?

Hemos visto así elementos significativos a tener en cuenta en nuestra planificación de la interoperabilidad en los sistemas de información desde la perspectiva de un esquema de gobernanza TI.

Al margen de la sucinta referencia explícita del estándar *CobiT 5* a la interoperabilidad, podemos no obstante hacer una traslación operativa de todo aquello pautado en el *IM* Modelo de Información.

5. Aplicabilidad del ENI

El Esquema Nacional de Interoperabilidad es una guía suficiente para este proyecto estratégico de racionalización de los recursos públicos. Nos propone una vectorización del concepto identificando tres dimensiones, organizativa, semántica y técnica (ver **figura 2**).

La **organizativa** se dirige tanto a la interlocución interna correspondiente a los órganos en las diferentes administraciones para asumir la interoperabilidad en su realidad operativa cotidiana como a un llamado a todas las instituciones para que conciban los sistemas de información, y por ende los productos y servicios por ellos obtenidos, como patrimonio común tan accesible como el marco garantista de derechos de privacidad y seguridad lo permita.

La **semántica** tiene por objeto asegurar una estructuración de la información asumible por todos los sistemas, humanos y cibernéticos, que soliciten acceso. Ello obliga a una estandarización de la información, a un formateado del significado de todo aquello puesto en común.

Las normas técnicas previstas en el RD 4/2010 en su disposición adicional primera son un compromiso explícito de marco semántico para el soporte al despliegue de la interoperabilidad.

Su promulgación es progresiva a medida que se consensúan las diferentes especificaciones. En la Web del Gobierno estatal podemos ya obtener las directrices para el documento electrónico, la digitalización de documentos, el expediente electrónico, la política de firma electrónica y certificados de la Administración, los requisitos de conexión a la Red de comunicaciones de las Administraciones Públicas españolas, los procedimientos de copiado auténtico y conversión entre documentos electrónicos, así como desde papel u otros medios físicos a formatos electrónicos y el modelo de datos para el intercambio de asientos entre las Entidades Registrales. Completan la lista, con reciente promulgación, el esperado catálogo

Figura 2. Estructura de dimensiones del ENI (Fuente: Ministerio de Administraciones Públicas).

de estándares y protocolos de intermediación de datos y la política de gestión de documentos electrónicos.

Por último, la dimensión **técnica**, la concreción de la cual vendrá en gran parte cumplimentada por las normas técnicas citadas, será la que concretará las interfaces de conexión entre sistemas.

El ENI está fuertemente imbuido de espíritu socializador no sólo del conocimiento generado, sino más allá, de las herramientas habilitadoras para conseguirlo.

Yendo un paso más allá, que sobrepasaría una expectativa parca reguladora de la interoperabilidad, el Capítulo VIII, *Reutilización y transferencia de tecnología*, nos induce a poner en valor el acervo procedimental en forma de software de las administraciones durante estas últimas décadas de tecnificación digital intensiva en repositorios de libre acceso y utilización no restringida. Los artículos 16 y 17 que componen dicho Capítulo, pretenden poner fin a esta destrucción de valor público, ofreciendo el libre licenciamiento de tipología europea LPUE y un repositorio centralizado para su obtención.

Un sistema *ERP*, un sistema *CRM,* en el ámbito administrativo no solamente han de dar satisfacción a unos requisitos transaccionales de operatoria normada, pago de un impuesto, liquidación de una tasa, obtención de una prestación, concesión de una licencia de actividades… Ha de poseer elementos software iniciales para el tratamiento en profundidad de la información recogida y elaborada de cara a la posibilidad de ofrecer servicios particularizados con criterios definidos de política concreta, que redunde en una aportación a la ciudadanía de valor añadido en su interrelación A2C (Administración-Ciudadano) .

Aspecto asimismo fundamental en un entramado de interoperabilidad lo constituye el cumplimiento de los criterios de seguridad. No puede haber interoperabilidad que vulnere atributos clave de la seguridad de la información.

La seguridad según el Esquema Nacional de Seguridad RD 3/2010 viene vectorizada en cinco dimensiones, autenticidad, confidencialidad, integridad y disponibilidad y el añadido de la trazabilidad como cualidad de la auditoría de tránsito de la información.

Para dar cumplimiento a tales preceptos, así como a consideraciones de sello temporal o aseguramiento del no repudio, se implementan los mecanismos de firma electrónica y certificados contemplados en el ENI y estructurados profusamente en el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

Este ejercicio garantista en ciertos ámbitos del transaccionado público absolutamente ineludible, introduce aspectos de complejidad añadida al hecho de la interoperabilidad.

Tal requisito sin embargo viene perfectamente reglado en cuanto a sus exigencias funcionales y connotaciones semánticas para las diferentes implementaciones tecnológicas en base a las infraestructuras de clave pública homologadas de los diferentes prestadores de servicios de certificación. El valor para las administraciones públicas ya no es sólo el cumplimiento de obligaciones administrativas globales para con sus ciudadanos, sino el ofrecimiento de servicios particularizados.

Este valor únicamente es posible con un tratamiento intensivo y altamente tecnificado de la información recabada. Y esta operativa solamente es posible en un escenario tecnológico interoperable [5].

6. Esquema tecnológico

La interoperabilidad legislada pretende ser neutra. Se incide exclusivamente en los objetivos finales de aseguramiento del intercambio de información y más someramente con sugerencias de uso de herramientas de libre licenciamiento. No es poco teniendo en cuenta un panorama mundial del mercado tecnológico donde hasta hace bien poco tiempo prevalecía el criterio de las corporaciones que detentaban la posesión del software propietario [6].

Todo esto está cambiando. Hemos contemplado en la anterior década como multinacionales insignia de la producción de hardware migraron su volumen de negocio principal hacia la generación de software de licenciamiento libre en una primera fase y fundamentan su mayor parte de actividad en una segunda fase en la división de consultoría con soluciones que gravitan en la personalización y diseño de software de fuentes abiertas.

Una propuesta posibilista de *framework* tecnológico que modele la interoperabilidad a día de hoy en las administraciones públicas tendría los siguientes componentes:

1) Redes de comunicaciones de uso exclusivo público y/o mecanismos de securización confiables en la red Internet. Una red que ha de asumir sin dilación el protocolo *IPv6* por las prestaciones de infinitud de direccionado, aseguramiento de todas las dimensiones de la seguridad de la información transmitida, y por la incorporación de los criterios de calidad de servicio que ya de forma intrínseca asumen las cabeceras de los paquetes IP.
2) Formatos para la información estandarizados, sin patentes ni regalías asociadas, que aseguren sin hipotecas, la sostenibilidad de las soluciones informáticas. Tarea ardua que conoce todo participante en los foros de estandarización, pero asimismo necesaria.
3) Catálogo unificado de software de libre licenciamiento que dé respuesta óptima a cada competencia asignada a la correspondiente administración.
4) Orquestación definida de procesos asociados a las diferentes fases de la generación y tratamiento de la información *BPM*.
5) Arquitecturas y patronazgo de software fuertemente orientados a la prestación de servicios al usuario final proporcionando valor público a partir de las prestaciones de servicios digitales.
6) Buses lógicos de conectividad que aseguren la mensajería, la publicación, el descubrimiento y el recepcionado de los servicios ofrecidos por los diferentes sistemas de información públicos.
7) Middleware de conectividad que dé cobertura al bus de conexión de la arquitectura interoperable.

Todo este entramado tecnológico ha de ser modular y el máximo de desacoplado que permita una auditoría constante de funcionamiento. Posibilitando además un mantenimiento evolutivo que asegure la transición a nuevos paradigmas tecnológicos y nuevos requerimientos sociales de satisfacción de necesidades asumidas por las administraciones públicas.

7. Conclusiones

No somos ajenos a la tesitura actual en la que concurren una situación de crisis económica que dibujará un nuevo escenario en el marco competencial de las administraciones junto a una eclosión de nuevas tecnologías digitales que permiten la creación de servicios de alto valor añadido.

Así, independientemente de cómo quede perfilado el marco institucional de las administraciones en el futuro inmediato, el ejercicio de gobernanza TI de las mismas es ineludible. Esta gobernanza se basa fundamentalmente en la satisfacción de los requerimientos de los agentes interesados que podríamos resumir en la creación de valor público, la minimización del riesgo asumido en su desempeño y la optimización de los recursos aportados a los proyectos tecnificadores.

La interoperabilidad se proyecta transversalmente sobre los tres objetivos convirtiéndose en factor imprescindible en su consecución. El valor público será la maximiza-

> “Una gobernanza TI asumida en nuestras corporaciones públicas propiciará grandemente un e-gobierno satisfactorio para la ciudadanía”

ción de servicios, en cantidad y calidad, que preste la administración. Los servicios tendrán una fuerte impronta digital ya sea en su elaboración, ya sea en su prestación final.

La compartición de conocimiento fruto del ejercicio de interoperabilidad entre administraciones será elemento sinérgico. El valor lo genera actualmente quien tiene más capacidad de prestar servicios. Confinar conocimiento carece de sentido por la efímera vida que tiene éste y por lo tanto el corto lapso de posibilidad para valorizarlo. El valor reside en su reproducción constante en un mercado o en un espacio público interesado en recibirlo y con capacidad adquisitiva, en tanto cliente, y derechos de ciudadanía como contribuyente, suficientes como para ser posibles receptores.

El riesgo de fracaso en los proyectos de tecnificación se ve minimizado cuanta mayor es la posibilidad de acceso a la información, cuanto más grande es el acervo público compartido.

Si los recursos son escasos y la interoperabilidad implica de forma natural la compartición, la relación es directa entre la optimización de los recursos y la extensión de la interoperabilidad.

Por lo tanto, una gobernanza TI bien entendida en el entorno público conlleva de manera ineluctable la asunción de la interoperabilidad de forma integral. Es misión de la alta decisión política no sólo la aquiescencia, liderar el patrocinio de los proyectos de despliegue de dicho criterio.

Una gobernanza TI asumida en nuestras corporaciones públicas propiciará grandemente un e-gobierno satisfactorio para la ciudadanía.

Referencias

[1] Miguel Ángel Amutio. Esquema Nacional de Interoperabilidad – Iniciativas legales y tecnológicas. *Tecnimap, 2010*, Zaragoza. <http://www.slideshare.net/MiguelAmutio/20100202-tecnimap-comunicacioneni> (accedido: 30 de diciembre de 2012).

[2] Andy Carvin, Tim Berners-Lee. *Weaving a Semantic Web*. Digital divide network papers, 2005.

[3] Jean-Baptiste Waldner. Nanocomputers and Swarm Intelligence. London: *ISTE, 2008*, pp. 227-231. ISBN: 1847040020.

[4] John F. Sowa. *Knowledge Representation: Logical, Philosophical, and Computational Foundations*. Pacific Grove, CA: Brooks Cole Publishing Co, 2000.

[5] Mila Gascó, Carlos E. Jiménez. Interoperability in the justice field: variables that affect implementation. *11th European Conference on eGovernment*. Slovenia, 2011.

[6] BOE. *Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica*. <http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1331.pdf> (accedido: 30 de diciembre de 2012).

Guías para el modelado de procesos de negocio

Laura Sánchez-González, Francisco Ruiz González, Félix García Rubio
Instituto de Tecnologías y Sistemas de Información, Universidad de Castilla la Mancha

<laurasnchezglez@gmail.com>, <francisco.ruizg, felix.garcia}@uclm.es>

1. Introducción

Las organizaciones prestan cada vez más atención a la mejora de sus procesos de negocio, ya que cuanto más eficiente es una organización, más competente será en el mercado [1].

Un proceso de negocio puede ser visto como una entidad compleja que pasa por diversas etapas, que conforman un ciclo de vida completo.

La primera de dichas etapas es el diseño, cuyo principal valor es disponer de modelos explícitos de los procesos. Aunque no se encuentra entre las fases más costosas en esfuerzos, recursos o costes, puede tener un alto impacto en los beneficios y eficiencia durante la implementación de los procesos [2]. Además, las mejoras incorporadas en los modelos de proceso evitan la propagación de los errores o deficiencias a etapas posteriores, en las cuales la solución suele ser más difícil y costosa [3].

Por estas razones, los modelos de procesos de negocio deben ser diseñados con niveles adecuados de calidad. Sin embargo, al tratarse de una actividad del ámbito de modelado del negocio, es frecuente, al contrario que en diseño de software, que participen actores con poca experiencia en técnicas de modelado, por ejemplo, analistas organizacionales u otros '*stakeholders*' de los procesos. Esta situación supone un riesgo alto de obtener modelos con niveles de calidad no adecuados.

Una buena opción es aplicar una serie de guías, consejos o buenas prácticas de modelado. En la bibliografía existen algunas propuestas en este sentido, pero suelen ser demasiado abstractas o genéricas, perdiendo efectividad práctica, o careciendo de fundamentación empírica.

Un paso necesario para mejorar la calidad de cualquier artefacto es la valoración de la misma mediante un adecuado esfuerzo de medición. Así será posible conocer si un modelo satisface un atributo de calidad específico.

Existen medidas enfocadas a la calidad estructural de los modelos de procesos de negocio [4], cuya importancia estriba en la validación empírica de su conexión con los atributos de calidad [5], por ejemplo, la entendibilidad y la modificabilidad.

Este artículo ha sido seleccionado para su publicación en ***Novática*** de entre las mejores ponencias presentadas en las VIII Jornadas de Ciencia e Ingeniería de los Servicios (JCIS2012) celebradas en Almería y de las que ATI ha sido entidad colaboradora.

Resumen. *En la etapa de diseño de los procesos de negocio se genera un modelo conceptual. Estos modelos son un artefacto muy útil para detectar errores tempranos y ayudar en la toma de decisiones sobre qué cambios deben ser aplicados para mejorar la eficiencia del proceso. El modelado de procesos de negocio en una organización puede involucrar a un número significativo de participantes sin experiencia, lo que puede llevar a producir modelos de escasa calidad y, en consecuencia, llevar a esfuerzos ineficientes durante el desarrollo y ejecución del proceso. En este trabajo se presentan unas guías para ayudar al modelador a garantizar unos niveles de calidad adecuados. Las guías han sido obtenidas aplicando una serie de pasos, basados en experimentación y técnicas de validación estadística.*

Palabras clave: *Guías de modelado, mejora de procesos, procesos de negocio.*

La entendibilidad se define como los esfuerzos que los sujetos hacen para reconocer los conceptos lógicos y su aplicabilidad [6], mientras que la modificabilidad se define como el grado con el cual el modelo puede ser efectiva y eficientemente modificado sin introducir defectos o degradar la calidad existente [6]. En procesos de negocio estos atributos de calidad son importantes porque los modelos están continuamente evolucionando para adaptarse a las necesidades cambiantes de las organizaciones.

La medición puede ofrecer información sobre la calidad de los modelos pero, para servir a los modeladores para guiar en la toma de decisiones durante el diseño, es necesario que se exprese en términos comparativos, usando indicadores, respecto de ciertos valores límite o umbrales. Sólo entonces se puede decidir si un modelo es o no adecuado respecto de ciertas propiedades cualitativas.

Determinar valores umbral no es una tarea sencilla y prueba de ello es que la gran mayoría de las propuestas sobre medición, de cualquier tipo de artefactos software, no llegan a conseguirlo. Para el caso que nos ocupa, los modelos de procesos de negocio, en trabajos previos hemos obtenido umbrales usando curvas ROC [7], y hemos estudiado medidas (base, derivadas e indicadores), criterios de decisión y valores umbrales para evaluar la entendibilidad y modificabilidad [8].

El marco conceptual subyacente está basado en la '*Software Measurement Ontology*' [9]. Así, para tomar decisiones de diseño no basta con disponer de medidas, base o derivadas, y de sus valores (por ej. número de actividades = 25), sino que es necesario definir indicadores basados en dichas medidas para tener valores cualitativos (por ej. nivel de complejidad=alto).

Los indicadores vienen expresados como una serie de criterios de decisión que establecen el valor cualitativo que corresponde a cada rango de valores de una cierta medida (por ej. si número de actividades oscila entre 20 y 40 = > nivel de complejidad=alto). Es dentro de los criterios de decisión donde juegan el papel clave los valores umbrales (20 y 40 en el ejemplo anterior).

Para completar la cadena que lleva a la toma de decisiones de diseño, es necesario un último eslabón: asociar a los valores cualitativos de cada indicador las guías de diseño que permiten corregir el modelo mejorando el valor del indicador (por ej. si nivel de complejidad es alto o muy alto, entonces agrupa actividades en forma de subprocesos).

Dichas guías de diseño se pueden capturar consultando a expertos (buenas prácticas, patrones), pero sólo mediante experimentación se pueden validar y, sobre todo, se puede establecer su relación pragmática con ciertos valores de ciertos indicadores.

En este trabajo presentamos el método que hemos ideado y las guías e indicadores asociados que hemos obtenido para modelos expresados con el lenguaje BPMN. Para ello, en la **sección 2** se describen algunos trabajos relacionados con las guías de modelado. En la **sección 3** se explican los pasos que hemos

> “Determinar valores umbral no es una tarea sencilla y prueba de ello es que la gran mayoría de las propuestas sobre medición, de cualquier tipo de artefactos software, no llegan a conseguirlo”

establecido para definir la guías de modelado, mientras que en la **sección 4** se presenta su aplicación a guías para mejorar la entendibilidad y modificabilidad. Por último, en la **sección 5** presentamos las conclusiones y el trabajo futuro de esta investigación.

2. Otras guías para el modelado de procesos

Varios autores han publicado trabajos previos relacionados con guías para el modelado de procesos de negocio. Un ejemplo de guías de modelado se encuentra en [10], con la propuesta llamada “*the Guidelines of Modeling*”.

Este marco está enfocado a diferentes usuarios finales, con diferentes objetivos y la posibilidad de diferentes técnicas de modelado y herramientas para describir los modelos. Revela seis técnicas generales para ajustar los modelos a las distintas perspectivas de los diferentes usuarios y objetivos. Estas técnicas están enfocadas a la correctitud, relevancia, economía, eficiencia, claridad, comparabilidad y diseño sistemático. Sin embargo, esta propuesta es también difícil de aplicar por modeladores noveles y no es usada, realmente, en la práctica.

Algunas guías operacionales de modelado de procesos pueden ser encontradas en libros como el de Sharp and McDermott [11]. Sin embargo, la única guía conocida, que define reglas simples y con fundamentos empíricos es la llamada “*Seven Process Modeling Guidelines* [12]” y consiste en siete guías de ayuda, como por ejemplo “usar etiquetas lingüísticas verbo+complemento” o “modelar de la forma más estructurada posible”.

El presente artículo pretende extender esta línea de investigación a través de los valores umbral derivados de técnicas adaptadas a este contexto y medidas estructurales de modelos conceptuales.

3. Pasos para la definición de guías de modelado

En esta sección se describen un conjunto de pasos para definir guías de modelado de procesos de negocio. Los valores umbral, incluidos como parte de la definición de los indicadores, son usados para detectar los elementos de los modelos que deben ser modificados. Algunas veces, estas modificaciones no son triviales y, por eso, las guías pueden resultar muy útiles.

Frente a las propuestas comentadas en la **sección 2**, nuestro valor añadido o particularidad es que las guías o consejos para el modelado están basados y asociados con los valores umbral incluidos en una lista de indicadores.

De forma resumida, los pasos para definir las guías son: 1) seleccionar un conjunto de medidas base con valores límite asociados, 2) crear una ecuación en la cual la incógnita es la medida (el contador de elementos del modelo) y el resultado el valor límite o umbral, y 3) definir una guía de modelado de acuerdo a ese resultado.

4. Guías para mejorar la entendibilidad y modificabilidad

Como ejemplo del método explicado en la sección anterior, a continuación presentamos su aplicación para mejorar la entendibilidad y modificabilidad.

4.1. Guías para la entendibilidad

Una de las características de calidad más importantes para los modelos conceptuales es la entendibilidad. Por esta razón, es interesante mantener unos niveles de entendibilidad aceptables en los modelos conceptuales. En el caso de procesos de negocio esto es especialmente importante dado que dichos modelos deben poder ser entendidos por ‘*stakeholders*’ con perfiles muy diferentes.

En trabajos previos de nuestro grupo [13], se realizaron varios experimentos para comprobar la correlación existente entre la entendibilidad y ciertas medidas estructurales de modelos de procesos de negocio representados con BPMN [14]. De estos experimentos se obtuvieron resultados del indicador “eficiencia de entendibilidad”.

Trabajos posteriores ampliaron el conjunto de medidas estudiadas [8][15]. Para sacar conclusiones comunes a los diversos experimentos se empleó la técnica de meta-análisis [16], ideada para integrar de forma estructurada y sistemática la información obtenida en diferentes estudios. Los resultados finales sobre correlación de medidas estructurales y entendibilidad se publicaron en [17] y se resumen en la **tabla 1** (parte 1 y 2).

En la literatura se encuentran varias técnicas estadísticas para calcular valores umbral a partir de datos experimentales.

En esta sección comentamos uno de los usados en nuestros trabajos, conocido como método Bender [18], ideado inicialmente para el campo de la medicina. Este método permite asociar probabilidades a ciertos resultados de medición del tipo siguiente: si una medida particular *m* obtiene un valor Y $\in [Y_1, Y_n]$, entonces existe una probabilidad Z% de considerar el modelo como *muy fácil de entender.*

Los resultados de aplicar este método en un conjunto de medidas validadas empíricamente fueron publicados en [8] y [19]. Los umbrales asociados a algunas medidas se muestran en la **tabla 1**. Además, siguiendo las recomendaciones de [20], se eligieron 5 etiquetas lingüísticas (*muy difícil de entender, difícil de entender, moderadamente entendible, fácil de entender, muy fácil de entender*) para dar una valoración más fácil de entender para el ser humano.

A título de ejemplo, supongamos que el número de nodos para un modelo es 70.

Entonces, siguiendo la **tabla 1** (primera fila), sabríamos que ese modelo tiene indicios de ser difícil de entender, y por lo tanto, habría que revisar el número de nodos (el elemento de diseño contado por la medida) del modelo.

Los valores umbral constituyen un complemento fundamental para las guías de modelado, ya que pueden ayudar a un modelador a determinar si su modelo está “bien diseñado” en función de las medidas estructurales. Permiten identificar las circunstancias en que la calidad de un modelo está en peligro. Sin embargo, estos ‘disparadores’ no detallan qué hacer, sólo nos dan el aviso. En la **sección 4.3** se aborda esta cuestión.

4.2. Guías para la modificabilidad

En esta sección se describen un conjunto de medidas estructurales correlacionadas con la modificabilidad y sus umbrales asociados.

La validación empírica de las medidas estructurales y su relación con la modificabilidad se estudió en trabajos previos de manera similar a como se ha comentado con la entendibilidad [13].

Con los experimentos realizados se validaron empíricamente un conjunto de medidas estructurales [8][15] y se hallaron conclusiones globales mediante meta-análisis [17]. Sin embargo, al contrario de lo que ocurrió con la entendibilidad, el número de medidas capaces de predecir la modificabilidad es más reducido, como se muestra en la **tabla 2**.

Medidas	Muy difícil de entender	Difícil de entender	Moderada-mente entendible	Fácil de entender	Muy fácil de entender
Nº nodos	(∞,81.1]	(81.1,58.1]	(58.1,43.7]	(43.7,29.4]	(29.4,6.5]
Diametro	(∞,23.4]	(23.4,16.5]	(16.5,12.2]	(12.2,7.92]	(7.92,1.03]
Densidad	(0,0.06]	(0.06,0.20]	(0.20,0.41]	(0.41, ∞)	-
AGD: nivel medio de nodos de decision	(∞,5.70]	(5.70,3.98]	(3.98,2.90]	(2.90,1.82]	(1.82,0.10]
MGD: nivel máx. de nodos de decisión	(∞ ,8.39]	(8.39,5.3]	(5.3,3.36]	(3.36,1.42]	(1.42,0]
Profundidad	(∞,5.09]	(5.09,3.02]	(3.02,1.72]	(1.72,0.42]	(0.42,0]
GM: Desajuste de los nodos de decisión	(∞,40.9]	(40.9,22.6]	(22.6,11.2]	(11.2,0]	-
GH: heterogeneidad de los nodos de decisión	(∞,1.39]	(1.39,0.71]	(0.71,0.28]	(0.28,0]	-
Secuencialidad	(0,0.25]	(0.25,0.48]	(0.48,0.70]	(0.70,1.07]	(1.07, ∞)
Separabilidad	(0,0.03]	(0.03,0.37]	(0.37,0.71]	(0.71,1.24]	(1.24, ∞)
CNC: coefi. de conectividad	(∞,2.28]	(2.28,1.43]	(1.43,0.90]	(0.90,0.37]	(0.37,0]
TS: token split	(∞,1.36]	(1.36,0.60]	(0.60,0.12]	(0.12,0]	-
CFC: complejidad del flujo de control	(∞,38.2]	(38.2,21.1]	(21.1,10.3]	(10.3,0]	-
NEDDB: nº de join/Split exclusiva basada en datos	(∞,6.02]	(6.02,3.87]	(3.87,2.52]	(2.52,1.17]	(1.17,0]
NEDEB: nº de join/Split exclusiva basada en eventos	(∞,5.76]	(5.76,2.62]	(2.62,0.65]	(0.65,0]	-
NID: nº de join/Split inclusive	(∞,4.63]	(4.63,2.17]	(2.17,0.62]	(0.62,0]	-
NCD: nº de join/Split compleja	(∞,4.56]	(4.56,2.18]	(2.18,0.69]	(0.69,0]	-
NPF: nº de join/Split paralela	(∞,3.36]	(3.36,1.60]	(1.60,0.49]	(0.40,0]	-
NSFG: nº de flujos de secuencia desde nodos de decisión	(∞,42.5]	(42.5,23.2]	(23.2,11.1]	(11.1,0]	-
TNG: nº nodos de decisión	(∞,17.3]	(17.3,9.71]	(9.71,4.89]	(4.89,0.08]	(0.08,0]
NP: nº de participantes	(∞,6.49]	(6.49,4.14]	(4.14,2.66]	(2.66,1.19]	(1.19,0]
PDOPout: proporción de objetos de datos de salida	(∞,1.39]	(1.39,0.79]	(0.79,0.41]	(0.41,0.03]	(0.03,0]
TNE: nº de eventos	(∞,18.2]	(18.2,11.5]	(11.5,7.28]	(7.28,3.04]	(3.04,0]
TNA: nº de actividades	(∞,46.5]	(46.5,31.3]	(31.3,21.8]	(21.8,12.3]	(12.3,0]
TNSF: nº flujos de secuencia	(∞,74.8]	(74.8,50.2]	(50.2,34.8]	(34.8,19.4]	(19.4,0]
CLP: nivel de conectividad entre participantes	(∞,6.32]	(6.32,3.79]	(3.79,2.21]	(2.21,0.62]	(0.62,0]
NDOOut: nº objetos de datos de salida	(∞,19.3]	(19.3,9.60]	(9.60,3.46]	(3.46,0]	-
NDOIn: nº objetos de datos de entrada	(∞, 26.1]	(26.1,12.1]	(12.1,3.38]	(3.38,0]	-
NSFE: nº de flujos de sequencia desde eventos	(∞,16.5]	(16.5,8.74]	(8.74,3.81]	(3.81,0]	-
NMF: nº de mensajes	(∞,22.8]	(22.8,13.2]	(13.2,7.15]	(7.15,1.09]	(1.09,0]

Tabla 1. Medidas para entendibilidad y sus valores umbral.

Medidas	Muy difícil de modificar	Difícil de modificar	Moderadamente modificable	Fácil de modificar	Muy fácil de modificar
AGD: nivel medio de nodos de decisión	(∞,7.65]	(7.65,4.80]	(4.80,3.02]	(3.02,1.23]	(1.23,0]
MGD: nivel máx. de nodos de decisión	(∞,8.95]	(8.95,5.70]	(5.70,3.66]	(3.66,1.63]	(1.63,0]
GH: heterogeneidad de los nodos de decisión	(∞,1.54]	(1.54,0.81]	(0.81,0.35]	(0.35,0]	-
Separabilidad	(0,0.16]	(0.16,0.42]	(0.42,0.68]	(0.68,1.10]	(1.10, ∞)
NSFG: nº de flujos de secuencia desde nodos de decisión	(∞ ,33.1]	(33.1,18.4]	(18.4,9.26]	(9.26,0.05]	(0.05,0]
CFC: complejidad del flujo de control	(∞,50.6]	(50.6,26.9]	(26.9,12.1]	(12.1,5]	(5,0]
GM: desajuste de los conectores	(∞,42]	(42,24]	(24,12]	(12,1]	-
TNG: nº de nodos de decisión	(∞,15.4]	(15.4,8.56]	(8.56,4.23]	(4.23,0]	-
Profundidad	(∞,5.99]	(5.99,3.26]	(3.26,1.56]	(1.56,0]	-

Tabla 2. Medidas para la modificabilidad y sus valores umbral.

Los valores umbral para la modificabilidad también se construyeron, en este caso, mediante el método Bender. Los resultados son los mostrados en la citada **tabla 2**. De esta manera, por ejemplo, si la medida GH recibe un valor de 1, el modelo es considerado como *difícil de modificar*. Las guías para solucionar los niveles bajos de calidad se comentan a continuación.

4.3. Guías de modelado

En esta sección se presentan un grupo de guías que pueden ser usadas para mejorar la entendibilidad y modificabilidad de los modelos.

Estas guías permiten resolver los niveles no adecuados de calidad indicados por ciertas medidas (ver **tablas 1 y 2**) disparadas.

Se describen agrupándolos en forma de guías. Estas guías deben ser usadas cuando los resultados de medición son clasificados como *moderadamente entendible/modificable.* Debemos recordar que los valores umbral son diferentes para cada característica de calidad (entendibilidad o modificabilidad).

Un resumen de toda la propuesta se muestra en la **tabla 3**, donde la columna 'explicación' resume en forma textual las situaciones no deseables, extraídas de la colección de medidas y valores umbral, y la guía a aplicar en su caso.

G1. Modulariza el modelo a través del uso de subprocesos. Elimina actividades obvias o fusiona actividades con un nivel bajo de granularidad. Recoloca actividades desde el modelo principal a los subprocesos o viceversa.

Las medidas implicadas en esta guía son el número de nodos, TNA, diámetro, y TNSF. TNA está relacionada con el elemento más común en un modelo, la actividad, y está directamente afectada cuando se reduce la medida número de nodos.

En esta línea, el diámetro es también afectado, porque la reducción del número de nodos afecta al camino entre el nodo inicial y algún nodo final.

Finalmente, si hay un valor bajo de nodos, los flujos de secuencia también se ven reducidos.

A número grande de nodos es un problema típico en muchos de los casos. Existen varias soluciones a este problema, como es la modularización (tal y como se describió en [12]).

Cuando un modelo tiene un número grande de nodos, es interesante agrupar algunos de ellos y crear un subproceso. Sin embargo, algunos modeladores inexpertos pueden caer en el error de diseñar modelos con un nivel muy bajo de granularidad y poner actividades muy simples u obvias y por tanto, pueden ser eliminadas sin pérdida de información significativa.

Finalmente, algunos subprocesos pueden tener varias actividades en común, lo que significa que éstas deben ser recolocadas en un modelo superior (o padre). Estas soluciones pueden ayudar a mejorar los resultados de ciertas medidas estructurales.

G2. Intentar incluir sólo un nodo de inicio y un nodo de fin por participante.

Las medidas relacionadas con esta guía son TNE y NSFE. El número de eventos (de comienzo, intermedios o finales) en el modelo directamente afecta a la suma de los flujos que parten o surgen de los eventos. Las soluciones propuestas están basadas en [12].

G3. Eliminar los participantes representados como cajas negras cuando no incluyen información relevante.

Las medidas relacionadas con esta guía son NP y CLP, porque ambas están relacionadas con el elemento participante de los modelos. Una solución posible a este problema es eliminar los participantes que están representados como cajas negras en el modelo. La especificación de este tipo de participantes algunas veces implica información redundante. Por ejemplo, cuando una actividad envía un mensaje a un participante representado como caja negra, la información sobre quién recibe el mensaje puede ser especificada en la propia actividad en vez de en el participante.

G4. Intentar dividir un nodo de decisión con un número alto de flujos de salida en varios nodos de decisión anidados cuando sea posible.

Este límite es indicado por las medidas AGD, MGD, y CNC, porque éstas están relacio-

Características	Medidas	Explicación	Guías
Entendibilidad	Nodos, TNA, Diámetro, TNSF	No usar más de 58 nodos en general, y 31 actividades. El camino más largo entre un nodo de comienzo y uno de fin no debe ser mayor a 16 nodos. No usar más de 50 flujos de secuencia.	**G1:** Modulariza el modelo a través del uso de subprocesos. Elimina actividades obvias o fusiona actividades con un nivel bajo de granularidad. Recoloca actividades desde el modelo principal a los subprocesos o vice-versa.
	TNE, NSFE	No usar más de 11 eventos y no más de 9 flujos de secuencia desde un evento.	**G2:** Intentar incluir sólo un nodo de inicio y un nodo de fin por participante
	NP, CLP	No usar más de 4 participantes y un CLP no debe exceder 3.79	**G3:** Eliminar los participantes representados como cajas negras cuando no incluyen información relevante.
	AGD, MGD, CNC	No usar más de 4 flujos de secuencia de entrada o salida desde un nodo de decisión y 2 por nodo, con un máximo de 5.	**G4:** Intentar dividir un nodo de decisión con un número alto de flujos de salida en varios nodos de decisión anidados cuando sea posible.
Modificabilidad	AGD, MGD	Do not use more than 5 input/output sequence flows from each gateway, with a maximum value of 6.	
Entendibilidad	CFC, TNG, GH	No usar más de 10 nodos de decisión, con una heterogeneidad de no más de 0.71. La medida CFC no debe ser mayor a 21.	**G5:** Intentar fusionar varios nodos de decisión cuando las decisiones especificadas en los nodos de decisión están relacionadas. Evitar los nodos OR-split cuando sea posible.
Modificabilidad	TNG, CFC, GH	No usar más de 9 nodos de decisión, con una heterogeneidad de no más de 0.81. La medida CFC no debe ser mayor a 27	
Entendibilidad	GM	GM no debe ser mayor a 23.	**G6:** Usar los patrones de diseño para evitar desajuste en los nodos de decisión.
Modificabilidad	GM	GM no debe ser mayor a 24.	

Tabla 3. Guías para el modelado de procesos de negocio.

nadas con el número de entradas y salidas a los nodos, principalmente, a los de decisión.

Esta solución consiste en separar un nodo de decisión en varios para analizar una pregunta compleja en varios pasos. Esto facilitará el análisis de las tareas, pero puede a su vez incrementar el número de nodos del modelo. El uso de esta guía se restringe, entonces, a las situaciones en las que las medidas relacionadas no se ven perjudicadas en gran medida.

G5. Intentar fusionar varios nodos de decisión cuando las decisiones especificadas en los nodos de decisión están relacionadas. Evitar los nodos *OR-split* cuando sea posible.
Este límite está indicado por las medidas TNG, CFC y GH¨. Todas estas medidas están relacionadas con los nodos de decisión y, por ejemplo, un incremento de la medida TNG puede incrementar la medida CFC y GH.

Esta solución está basada en la idea de reducir el número total de nodos de decisión. El problema es que no es posible eliminar un nodo de decisión en un modelo sin que haya pérdida de información, por eso es mejor fusionar algunos de ellos cuando están relacionados, y por tanto, las preguntas simples se unirán en una pregunta más compleja. Es importante evitar como sea posible, el número de nodos *OR-split* porque incrementa en gran medida el valor de las medidas asociadas.

G6. Usar los patrones de diseño para evitar desajuste en los nodos de decisión.
Esta guía enfatiza la importancia de modelar de forma estructurada, especialmente con los nodos de decisión. Patrones relacionados con acompañar a cada *split* un nodo de decisión de tipo *join* y similares fueron publicados en [21]. Esta guía principalmente ayuda a la sincronización de tareas.

5. Conclusiones y trabajo futuro

En este artículo hemos presentado unas guías para ayudar al modelado de procesos de negocio, construidas a partir de medidas estructurales y sus correspondientes valores umbral. Las medidas fueron previamente validadas empíricamente para comprobar su correlación con la entendibilidad y modificabilidad de los modelos.

Los valores umbral se obtuvieron mediante el método Bender, procedente del campo de la medicina y adaptado a esta investigación. De esta manera, cuando un conjunto de medidas superan determinados valores críticos, los modeladores pueden ser avisados para modificar el modelo de acuerdo a unas guías incluidas también en este artículo.

Estas guías de modelado constituyen un punto de partida para mejorar el modelado de procesos de negocio en una organización. Las guías han sido diseñadas con funda-

mentos empíricos, lo que implica una mayor certidumbre sobre su utilidad práctica.

Sin embargo, no todos los aspectos a mejorar en un modelo conceptual están relacionados con la estructura, y esto constituye la principal limitación del trabajo.

Otros aspectos como las etiquetas asociadas a los elementos en el modelo (por ejemplo, los nombres de las tareas o las cuestiones de los nodos decisión) afectan muy directamente a la entendibilidad y modificabilidad del modelo, y serán estudiados en trabajos futuros.

Finalmente, aunque la entendibilidad y modificabilidad están entre las características de calidad más relevantes para los modelos conceptuales, también serán estudiadas otras en trabajos futuros, para así disponer de unas guías de modelado más completas.

Agradecimientos

Este trabajo ha sido parcialmente financiado por los siguientes proyectos: ALTAMIRA (Junta de Comunidades de Castilla La Mancha, Fondo Social Europeo, PII2I09-0106-2463), INGENIOSO (Junta de Comunidades de Castilla La Mancha, PEII11-0025-9533) y proyecto GEODAS-BC (Ministerio de Economía y Competitividad y Fondo Europeo de Desarrollo Regional FEDER, TIN2012-37493-C03-01)

Referencias

[1] S.L. Pfleeger. Integrating Process and Measurement. En A. Melton (Ed.), *Software Measurement*. International Thomson Computer Press, 1996: pp. 53-74.

[2] M. Rosemann. Potential pitfalls of process modeling: part a. *Business process Management Journal, 2006*, *12(2)*: pp. 249-254.

[3] Y. Wand, C. Weber. Research commentary: Information systems and conceptual modeling–a research agenda. *Info. Sys. Research, 2002. 13(4)*: pp. 363-376.

[4] L. Sánchez-González, F. García, F. Ruiz, M. Piattini. Measurement in Business Processes: a Systematic Review. *Business process Management Journal, 2010, 16(1)*: pp. 114-134.

[5] M. Zelkowitz, D. Wallace. Experimental models for validating technology. *IEEE Computer, Computing practices*, 1998.

[6] ISO/IEC. 9126-1, *Software engineering - product quality - Part 1: Quality Model*. 2001.

[7] J. Mendling, L. Sánchez González, F. García, M. La Rosa. Thresholds for Error Probability Measures of Business Process Models. *International Journal of Systems and Software, 2012, 85(5)*: pp. 1188-1197.

[8] L. Sánchez-González, F. García, J. Mendling, F. Ruiz. Quality Assessment of Business Process Models Based on Thresholds. *CoopIS 2010 - 18th International conference on Cooperative Information Systems, 2010*: pp. 78-95.

[9] F. García, M. Bertoa, C. Calero, A. Vallecillo, F. Ruiz, M. Piattini, M. Genero. Towards a Consistent Terminology for Software Measurement. *Information and Software Technology, 2005, 48*: pp. 631-644.

[10] J. Becker, M. Rosemann, C. von Uthmann. Guidelines of Business Process Modeling. En *Business Process Management*, 2000, Springer Berlin / Heidelberg. pp. 241-262.

[11] A. Sharp, P. McDermott. *Workflow Modeling: Tools for Process Improvement and Application Development*. Artech House Publischers, 2001.

[12] J. Mendling, H.A. Reijers, W.M.P. van der Aalst. Seven Process Modeling Guidelines (7PMG). *Information and Software Technology, 2010. 52(2)*: pp. 127-136.

[13] E. Rolón, F. García, F. Ruiz, M. Piattini, C.A. Visaggio, G. Canfora. Evaluation of BPMN Models Quality. A Family of Experiments. *ENASE - International Conference on Evaluation of Novel Approaches to Software Engineering, 2008*.

[14] OMG. *Business Process Model and Notation (BPMN)*, Version 2.0, 2011. <http://www.omg.org/spec/BPMN/2.0/>.

[15] E Rolón, J. Cardoso, F. García, F. Ruiz, M. Piattini. Analysis and Validation of Control-Flow Complexity Measures with BPMN Process Models. *The 10th Workshop on Business Process Modeling, Development, and Support*, 2009.

[16] G.V. Glass, B. McGaw, M.L. Smith. *Meta-Analysis in Social Research*. Sage Publications, 1981.

[17] L. Sánchez-González, F. García, F. Ruiz, M. Piattini. Validación Global de Medidas para Modelos Conceptuales de Procesos de Negocio mediante Meta-Análisis. *Jornadas en Ingeniería del Software y Bases de Datos, 2010*: pp. 293-298.

[18] R. Bender. Quantitative Risk Assessment in Epidemiological Studies. Investigating Threshold Effects. *Biometrical Journal, 1999, 41(3)*: pp. 305-319.

[19] L. Sánchez-González, F. Ruiz, F. García, J. Cardoso. Towards Thresholds of Control Flow Complexity Measures for BPMN Models. *26th Symposium On Applied Computing SAC 10, 2011*: pp. 1445-1450.

[20] G.A. Miller. The magical number seven or minus two: some limits on our capacity of processing information. *Psychological Rev, 1956, 63*: pp. 81-97.

[21] W.M.P. van der Aalst, A.H.M. ter Hofstede, B. Kiepuszewski, A.P. Barros. *Workflow Patterns. Distributed and Parallel Databases, 2003, 14(1)*: pp. 5-51.

José María García, David Ruiz, Antonio Ruiz-Cortés
ETS Ingeniería Informática, Universidad de Sevilla

<{josemgarcia,druiz,aruiz}@us.es>

SOA4All Integrated Ranking: Una herramienta holística basada en preferencias

Este artículo ha sido seleccionado para su publicación en ***Novática*** de entre los mejores trabajos de carácter práctico presentados en las VIII Jornadas de Ciencia e Ingeniería de los Servicios (JCIS2012) celebradas en Almería y de las que ATI ha sido entidad colaboradora.

Resumen: *Los mecanismos existentes para el ranking de servicios proporcionan modelos de preferencias ad hoc que ofrecen diferentes niveles de expresividad. En consecuencia, la aplicación de un único mecanismo en un escenario particular obliga al usuario a definir sus preferencias en función del correspondiente formalismo subyacente. Por otro lado, una serie de preferencias definidas en función a distintos modelos no pueden combinarse en general, debido a problemas de interoperabilidad. En este artículo presentamos SOA4All Integrated Ranking, un mecanismo de ranking integrado que permite la combinación de tres diferentes mecanismos de ranking implementados en el contexto del proyecto europeo SOA4All. Nuestra solución se ha desarrollado utilizando el framework PURI (a Preference-based Universal Ranking Integration), el cual se fundamenta en un modelo de preferencias holístico y común que permite aprovechar sinergias entre los mecanismos de ranking que integra, ofreciendo una interfaz de usuario única para definir preferencias que actúa como fachada al ranking integrado.*

Palabras clave: *Herramientas de ranking, integración de sistemas, modelos de preferencias, servicios web semánticos.*

1. Introducción

En el contexto del proyecto europeo SOA4All[1] se implementaron tres mecanismos de ranking [6], los cuales ofrecen a los usuarios distintas alternativas dependiendo de sus requisitos de expresividad y rendimiento para el proceso de ranking de servicios.

En primer lugar, un mecanismo simple y eficiente de ranking objetivo proporciona una serie de métricas sobre la calidad del servicio y de su descripción.

En segundo lugar, un ranking multi-criterio basado en propiedades no funcionales permite una definición de preferencias más expresivas en función de dichas propiedades.

Por último, un mecanismo de ranking basado en lógicas difusas ofrece una solución altamente expresiva para definir preferencias, aunque el proceso de ranking resulta menos eficiente.

Con el objetivo de aprovechar al máximo estas tres técnicas de ranking desarrolladas, un usuario debería ser capaz de expresar sus preferencias usando al mismo tiempo cualquiera de las herramientas que dichas técnicas proporcionan. Por ello, en la etapa final del proyecto SOA4All se desarrolló una solución integrada de ranking, de forma que un usuario pudiera definir y componer preferencias en base a un modelo genérico y expresivo que integre las definiciones de preferencias utilizadas en los tres mecanismos de ranking.

Esta solución de ranking integrado, presentada en este artículo, puede verse como una fachada para acceder a los mecanismos de ranking disponibles mediante un punto de acceso único y común a todos ellos[2].

2. Modelado de preferencias y mecanismos de ranking

El modelo de preferencias que usamos en esta propuesta es una adaptación del modelo completo descrito en [3].

Básicamente, los usuarios pueden expresar preferencias atómicas usando una serie de términos de preferencias (*PreferenceTerms* en el modelo) que son tratadas internamente por el correspondiente mecanismo de ranking que es capaz de evaluarla. Estos términos pueden ser subsecuentemente combinados usando preferencias compuestas, según la relación que existe entre ellos.

La **figura 1** presenta una representación en UML de este modelo de preferencias.

Esencialmente, cada término de preferencia es tratado por el mecanismo de ranking correspondiente, ya sea el ranking objetivo de métricas, el ranking multi-criterio, o el basado en lógicas difusas, mientras que las preferencias compuestas más genéricas son evaluadas directamente por el *framework* de ranking integrado utilizado en la implementación (véase la **sección 3** de este artículo).

Nótese que la representación de preferencias con lógicas difusas está simplificada en el diagrama (para más información, ver [2]).

La **tabla 1** resume las correspondencias entre términos de preferencia y mecanismos de ranking.

Las preferencias atómicas están relacionadas con conceptos de dominio que normalmente

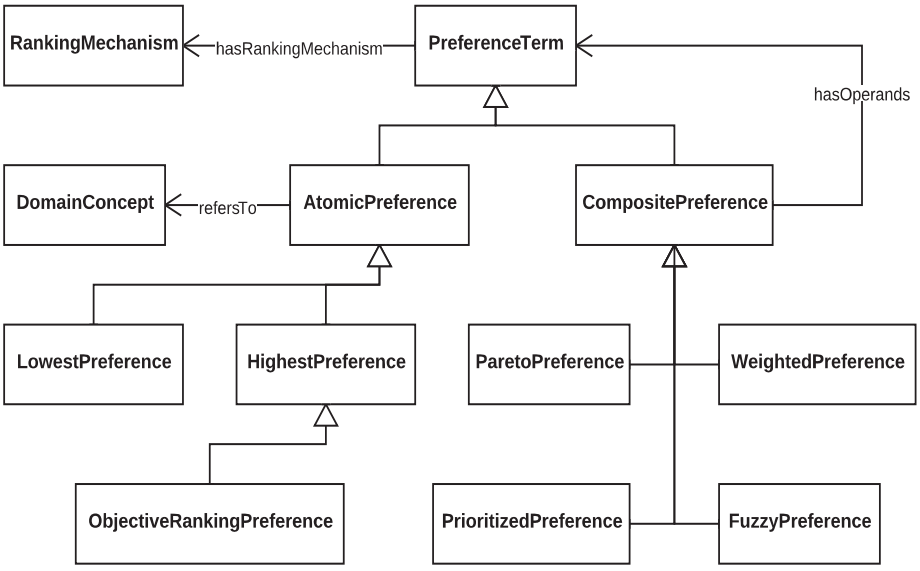


Figura 1. Representación en UML simplificada del modelo de preferencias.

> “Con el objetivo de aprovechar al máximo estas tres técnicas de ranking desarrolladas, un usuario debería ser capaz de expresar sus preferencias usando al mismo tiempo cualquiera de las herramientas que dichas técnicas proporcionan”

Preference Term	Ranking Mechanism
LowestPreference	MultiCriteriaRanking
HighestPreference	MultiCriteriaRanking
ObjectiveRankingPreference	ObjectiveMetricsRanking
ParetoPreference	DefaultParetoRanking
PrioritizedPreference	DefaultPrioritizedRanking
WeightedPreference	MultiCriteriaRanking
FuzzyPreference	FuzzyLogicBasedRanking

Tabla 1. Correspondencias entre mecanismos y preferencias.

representan propiedades no funcionales que deben ser optimizadas para cumplir las preferencias de usuario definidas sobre ellas. Por ejemplo, la instanciación de una preferencia *Lowest* (o *Highest*) significa que el usuario prefiere que el valor de una propiedad no funcional concreta sea cuanto menor (o mayor) mejor.

Estas preferencias se pueden mapear directamente a los órdenes ascendentes o descendentes que define el modelo proporcionado por el mecanismo de ranking multi-criterio, por lo que este mecanismo es el encargado de evaluar dichas preferencias en nuestra implementación. Además, la composición usando preferencias de tipo *Weighted* nos permite definir el peso que indica la importancia para el usuario de cada preferencia atómica que se compone.

Por otro lado, el ranking objetivo realiza una maximización de los valores de las métricas calculadas, por lo que se evalúa de forma similar a una preferencia de tipo *Highest*, donde el concepto de dominio a maximizar al que se refiere es una de las métricas que nos ofrece este mecanismo de ranking.

Finalmente, los usuarios pueden combinar preferencias equilibrando su importancia relativa (mediante preferencias de tipo Pareto) o priorizando algunas frente a otras (caso de las *Prioritized*) [3].

3. Implementación de SOA4All Integrated Ranking

Nuestra solución de ranking integrado es capaz de evaluar las preferencias de usuario definidas en función del modelo presentado para ordenar un conjunto de servicios previamente descubiertos. Como se ha descrito anteriormente, cada término de preferencia es tratado por un mecanismo de ranking concreto.

Con el objeto de instanciar correctamente cada mecanismo, combinar los resultados, y controlar en general el proceso de ranking integrado, nuestra implementación está construida a partir del *framework* PURI[3] [2].

Así, nuestro *framework* proporciona los medios para integrar distintos mecanismos de ranking mediante el uso del modelo de preferencias descrito, el cual también puede ser aprovechado para mejorar el rendimiento del proceso previo de descubrimiento de servicios [4]. La solución de ranking implementada adapta el framework PURI para integrar las tres técnicas de ranking desarrolladas en SOA4All [1].

La implementación, publicada como un servicio web, proporciona un método que recibe un conjunto de servicios a ordenar y la preferencias de usuario definidas con el modelo presentado.

Concretamente, este método analiza en primer lugar los términos de preferencia utilizados, de forma que cada término se delega hacia el mecanismo de ranking correspondiente, según lo descrito en la **tabla 1**.

La adaptación del *framework* PURI que se ha desarrollado en SOA4All Integrated Ranking es la responsable tanto de este mecanismo de delegación como de la composición de los resultados del ranking para cada término de preferencias.

Finalmente, el método devuelve la lista de servicios ordenada como se solicitó.

Adicionalmente, SOA4All Integrated Ranking proporciona una interfaz de usuario para definir preferencias y realizar el proceso de ranking correspondiente.

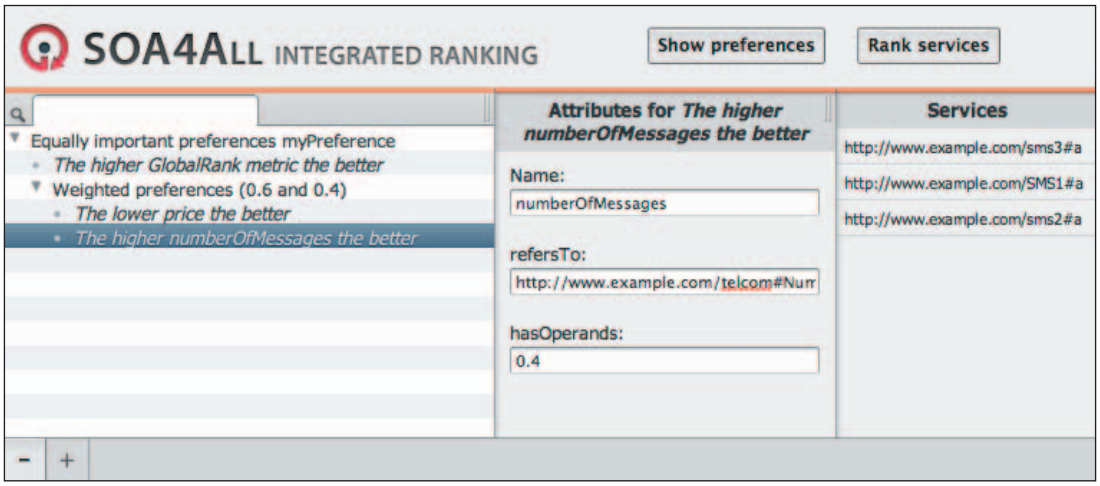


Figura 2. Captura de pantalla de la interfaz de definición de preferencias.

> “ Nuestra solución de ranking integrado es capaz de evaluar las preferencias de usuario definidas en función del modelo presentado para ordenar un conjunto de servicios previamente descubiertos ”

La implementación se realizó basada en Google Web Toolkit y la herramienta de modelado AcME[4]. Esta interfaz permite al usuario definir sus preferencias fácilmente en función del modelo presentado anteriormente. Por ejemplo, en el caso ilustrado por la **figura 2**, un usuario ha definido una preferencia que equilibra la importancia de la preferencia sobre un valor alto para la métrica denominada *GlobalRank* con una preferencia multi-criterio, que a su vez combina el menor precio posible con el mayor número de mensajes enviados posibles tomando como valores relativos de importancia 0.6 y 0.4, respectivamente.

Además, la interfaz también puede usarse para verificar la implementación del ranking integrado, razón por la cual un conjunto de servicios están disponibles para ser ordenados en función de las preferencias que se definan, mediante el uso del botón *Rank services*.

4. Conclusiones

La herramienta que hemos implementado, SOA4All Integrated Ranking, presenta una solución holística para integrar distintos mecanismos de ranking, proporcionando a los usuarios la flexibilidad de elegir y combinar cualquiera de los términos de preferencias ofrecidos por los tres mecanismos de ranking propuestos dentro del proyecto europeo SOA4All, aprovechándolos al máximo y explotando sus sinergias.

Además, una única interfaz de usuario para acceder al proceso completo de ranking simplifica la interacción de los usuarios con la solución de descubrimiento y ranking en SOA4All.

Por último, otros mecanismos de ranking podrían ser a su vez integrados con nuestra actual solución, identificando para ello las correspondencias con nuestro modelo común e implementando un adaptador que sería instanciado automáticamente por nuestro *framework* de integración PURI.

Agradecimientos

Este trabajo ha sido parcialmente financiado por la Comisión Europea (FEDER) y el Gobierno de España mediante el proyecto CICTY SETI (TIN2009-07366), por la Junta de Andalucía mediante los proyectos ISABEL (TIC-2533) y THEOS (TIC-5906), por el proyecto EU FP7 IST 27867 SOA4All, y por EC FP7 Network of Excellence 215483 S-CUBE.

Referencias

[1] Sudhir Agarwal, Martin Junghans, Barry Norton, José María García. *Second service ranking prototype*. Deliverable 5.4.3, SOA4All, 2011.

[2] José María García, Martin Junghans, David Ruiz, Sudhir Agarwal, Antonio Ruiz-Cortés. Integrating semantic web services ranking mechanisms using a common preference model. *Knowledge-Based Systems, Elsevier*, ISSN 0950-7051, 2012, pendiente de publicación.

[3] José María García, David Ruiz, Antonio Ruiz-Cortés. A model of user preferences for semantic services discovery and ranking. ESWC (2), *Lecture Notes in Computer Science, vol. 6089*, pp. 1–14. Springer, 2010.

[4] José María García, David Ruiz, Antonio Ruiz-Cortés. Improving semantic web services discovery using SPARQL-based repository filte ring. *Web Semantics: Science, Services and Agents on the World Wide Web*, *Volume 17*, diciembre de 2012, pp. 12-24. Elsevier, ISSN 1570-8268, <http://dx.doi.org/10.1016/j.websem.2012.07.002>.

[5] José María García, Ioan Toma, David Ruiz, Antonio Ruiz-Cortés. A service ranker based on logic rules evaluation and constraint programming. *NFPSLA-SOC'08. CEUR Workshop Proceedings, vol. 411*, 2008.

[6] Ioan Toma, Natalie Steinmetz, Holger Lausen, Sudhir Agarwal, Martin Junghans. *First Service Ranking Prototype*. Deliverable 5.4.1, SOA4All, 2011.

Notas

[1] <http://www.soa4all.eu>.

[2] SOA4All Integrated Ranking está disponible on line en <http://www.isa.us.es/soa4all-integrated-ranking/>.

[3] Un prototipo inicial, descrito en [5], es encuentra en http://www.isa.us.es/upsranker

[4] <http://www.isa.us.es/acme>.

A continuación presentamos las habituales referencias que desde 1999 nos ofrecen los coordinadores de las Secciones Técnicas de nuestra revista.

Sección Técnica "*Acceso y recuperación de información*" (José María Gómez Hidalgo, Manuel J. Maña López)

Tema: *Conferencia - Workshop on Web Search Click Data 2013*

En su tercera edición, el Taller sobre Datos de Búsqueda Web vuelve a centrarse en cualquier investigación relacionadas con *logs* de búsqueda Web y en cómo mejorar las propiedades de las colecciones públicas de datos de este tipo. Además de un foro ideal para estar al corriente de los últimos avances en investigación sobre la búsqueda Web, pone a disposición de los investigadores una serie de colecciones de datos desarrolladas por Microsoft, Yahoo! y Yandex a partir de búsquedas reales. <http://research.microsoft.com/en-us/um/people/nickcr/wscd2013>.

Estas colecciones permiten la realización de experimentos y pruebas para optimizar las herramientas de búsqueda. Por ejemplo, Yahoo! Proporciona, entre otras, una colección constituida por las 1.000 búsquedas más frecuentes en nueve idiomas, que incluyen el inglés, el francés, el japonés o el español, y que es sumamente útil para los estudios en Acceso a la Información multilingüe. Igualmente, Yandex proporciona una colección útil para la predicción de la relevancia de los resultados de búsqueda constituida por más de 30 millones de consultas, casi 120 millones de URLs distintas, y 44 millones de sesiones de búsqueda. En este último caso, Yandex plantea además diversas competiciones periódicas orientadas a mejorar la calidad de la búsqueda usando los datos que proporcionan.

Tema: *Recurso - Analizador automático de personalidad*

El investigador Fabio Celli de la Universidad de Trento ha desarrollado un programa que es capaz de predecir la personalidad de un usuario en función de los textos que escribe, en función de cinco parámetros clásicos de la personalidad: Extroversión, estabilidad emocional (calmado o neurótico), cooperatividad (amistoso o poco cooperativo), consciencia (organizado, despreocupado), y perspicacia.

El programa consiste en un script en Perl que analiza los textos escritos por una serie de usuarios y clasifica al mismo de acuerdo a sus textos como poseedor o no de las anteriores cualidades. Aunque el sistema ha sido evaluado sobre los idiomas inglés e italiano, es aplicable a otros idiomas también, ya que utiliza atributos del lenguaje independientes del idioma.

Este sistema puede ser interesante para clasificar a los usuarios de acuerdo a su personalidad, y adaptar a la misma los resultados de las búsquedas en un sistema de acceso a la información o en sistemas de recomendación, ya sea sobre un dominio particular (por ej. música, noticias…), como en redes sociales, aumentando potencialmente la satisfacción del usuario con el sistema de recuperación de documentos o con el recomendador.

El sistema está disponible en <http://clic.cimec.unitn.it/fabio/pr2demo.php>.

Tema: *Recurso - CommonCrawl, una colección masiva de páginas Web*

Dado el enorme tamaño actual de la Web, cualquier investigación o desarrollo que pretenda alcanzar resultados efectivos y concluyentes debe efectuarse y evaluarse sobre colecciones de datos masivas. La colección más masiva actualmente es la gestionada por la organización sin ánimo de lucro CommonCrawl, cuyo objetivo es posibilitar una Web más abierta que facilite el acceso libre a la información y la mejora de la investigación, los negocios y la educación.

CommonCrawl ofrece acceso a 6.000 millones de páginas web en forma de un repositorio hospedado en *Amazon Web Services* (concretamente EC2, la "nube elástica" de Amazon), y gestionable a través de tecnologías de manejo de cantidades masivas de datos, como *map-reduce* y su implementación Hadoop. También es posible descargar los datos a un *cluster* local si así se prefiere. Además, la empresa blekko, cuyo objetivo es proporcionar experiencias de búsqueda más efectivas a sus usuarios, va a donar próximamente una colección de 140 millones de websites y 22.000 millones de páginas web a CommonCrawl, <http://commoncrawl.org/>.

En Amazon es posible además encontrar otras colecciones de datos relevantes para el acceso a la información (como la colección de correos del caso Enron, o los ngramas de Google Books, que ya hemos mencionado en ocasiones anteriores), así como colecciones de datos de biología, química, matemáticas, clima, etc., bajo el epígrafe de Colecciones de Datos Públicas, <http://aws.amazon.com/datasets/>.

Sección Técnica *"Auditoría SITIC"* (Marina Touriño Troitiño, Manuel Palao García-Suelto)

Tema: *Auditoría interna y el gobierno de TI*

El gobierno de TI: Este es un aspecto relacionado con las tecnologías de la información que suscita, en los últimos años, cada vez más atención, y aunque el concepto lo encontramos con mucha frecuencia, casi tanta como la que está originando el "*cloud computing*", no en todos los documentos el significado y el alcance de este concepto son análogos.

A través de la *Information Systems Audit and Control Association* (ISACA), se pueden localizar en su *bookstore*, libros sobre el gobierno de TI, así como en otras librerías *online*. En cuanto a normas sobre el gobierno de TI, también hay varias disponibles, entre las más importantes:

- COBIT (ISACA): Tanto en la versión 4.1 como la 5, se define como "*un marco y un grupo de herramientas para el gobierno de TI que permite a la gerencia salvar la brecha entre los requerimientos de control, los aspectos técnicos y los riesgos del negocio*"[1].
- Normas ISO: ISO/IEC 38500:2008 *Corporate governance of information technology*[2].

Pero el problema se presenta para los auditores, especialmente los internos, cuando tienen que auditar y evaluar "el Gobierno de TI". Sobre esta tarea de los auditores internos[3] hay pocas guías o material de referencia específico que realmente ayude a los auditores a planificar este tipo de auditoría de forma adecuada. Este escenario también puede aplicarse a los auditores externos.

ISACA desarrolla estándares, guías y procedimientos para los auditores, en general, pero las relacionadas con el gobierno de TI datan del año 2005, la más reciente.

Por lo tanto, una reciente guía, julio de 2012 del Instituto Global de Auditores Internos (GTAG número 17[4]) provee una significativa y valiosa ayuda para los auditores a la hora de auditar este aspecto de la tecnología de la información, al mismo tiempo que cubrir una cierta carencia de herramientas específicas para auditoría interna, a la hora de auditar el gobierno de TI. Una cuestión es una guía para el gobierno de TI, y otra es cómo planificar la auditoría de esta actividad con un criterio de aporte de valor a la organización.

Esta guía, en primer término sitúa el concepto y el alcance de que se entiende por gobierno de TI:

■ *"El gobierno de TI abarca la gestión (managing) de las operaciones y proyectos de TI para asegurar la alineación entre estas actividades y las necesidades de la organización definidas en el plan estratégico".*
■ "*La alineación de los objetivos de la organización y TI está relacionada altamente con el gobierno y menos relacionada con los aspectos puramente técnicos. El gobierno asegura que las alternativas son evaluadas, que la ejecución es gestionada de forma adecuada, y que el rendimiento es monitorizado, y estos mismos conceptos son aplicables al gobierno de TI".*

La guía define los 5 componentes para un gobierno de TI efectivo:

- Estructuras organizativas y de gobierno.
- Liderazgo y soporte a nivel ejecutivo.
- Planificación estratégica y operacional.
- Entrega y medición del servicio.
- Gestión de TI de la organización y del riesgo.

También incluye una descripción detallada de las áreas clave que el auditor debe considerar con relación al gobierno de TI:

- Las responsabilidades y funciones de los responsables críticos de TI (*Chief Information Officer*; *Chief Technology Officer*; *Chief Information Security Officer*).
- La asignación de responsabilidad y de toma de decisiones.
- La monitorización del rendimiento/comportamiento de TI, y los baremos de medición para el reporte.
- El nivel de entendimiento del nivel de Gerencia y Dirección de la organización sobre como TI soporta y permite el logro de la estrategia y objetivos de ésta.
- La alineación entre TI y la organización.
- El gobierno de los riesgos y controles de TI.

La guía desarrolla los aspectos tanto de los componentes como de las áreas mencionados, indicando en cada caso, las consecuencias o riesgos de una carencia de alineación de esas actividades con las estrategias y objetivos del negocio/organización, y las cautelas que debe considerar el auditor en la planificación y en la auditoría del gobierno de TI.

En un determinado esquema, la guía distingue resumidamente, con criterio acertado, la diferencia entre las actividades de gobierno (*governance*) y gestión (*managing*) de TI, a través de los recursos humanos, los procesos y la tecnología.

Como esta guía está dirigida, fundamentalmente a los auditores internos, también aborda los objetivos de esta función, con relación al gobierno de TI, que debe salvaguardar la preceptiva independencia del auditor interno:

- La responsabilidad primaria del gobierno de TI está en la alta Dirección y/o Consejo de Administración. La actividad de auditoría interna es responsable de evaluar si el gobierno de TI de la organización soporta las estrategias y objetivos de esta.
- Los auditores realizan tanto auditorías de rendimiento/desempeño (*performance*) como de cumplimiento. Mientras que las auditorías de cumplimiento están generalmente enfocadas a la adhesión a requerimientos externos legales o regulatorios, o a políticas y procedimientos internos, en las auditorías de desempeño, para desarrollar un programa de auditoría efectivo, se requiere más análisis y evaluación con relación a qué elementos conducen al desempeño en la organización.

La guía también incluye un anexo con una guía, para la preparación de la auditoría, desde una perspectiva del riesgo.

En resumen, esta guía puede ser de una gran utilidad para los auditores internos, a la hora de planificar la evaluación del gobierno de TI, ya que va orientando, paso a paso, a los auditores sin perder en ningún caso la perspectiva fundamental: que el gobierno de TI está estrechamente ligado y debe servir a los objetivos del negocio o actividad de la organización, y que desde esa perspectiva debe ser auditado.

[1] ISACA gestiona el certificado CGEIT (*Certified in the Governance of Enterprise IT*).
[2] Recientemente AENOR ha publicado un libro muy útil: Modelo para el gobierno de las TIC, basado en un conjunto de normas ISO. La primera edición es de 2012.
[3] La auditoría del Gobierno es mandatoria para los auditores internos según las normas de auditoría interna.
[4] *Global Technology Audit Guide: Auditing IT Governance*.

Sección Técnica "*Derecho y Tecnologías*" (Elena Davara Fernández de Marcos)

Tema: *España a la cabeza en cuanto a penetración de smartphones en toda la UE*

Hace ya varios años que los teléfonos móviles han visto ampliamente superada la vocación de comunicación con la que nacieron, limitada por entonces al envío y recepción de llamadas y mensajes cortos de texto (SMS). Y es que, si tenemos en cuenta que hace algunos días celebramos el 20º cumpleaños del primer SMS, caeremos en la cuenta de que la evolución ha sido mucho más rápida de la esperada y ya no sólo del teléfono móvil en sí, cuya acogida fue, desde un primer momento, muy positiva, sino de los llamados teléfonos inteligentes o "*smartphones*".

Y es que, hoy en día, quien tiene un *smartphone* no tiene únicamente un teléfono sino que puede integrar en él cientos de aplicaciones que le facilitan el día a día, citando, entre otros: La facilidad para hacer la compra, desplazarse por la ciudad, buscar y acceder a información actualizada de los más diversos temas de manera sencilla, el uso de servicios de mensajería instantánea, el acceso a documentos de trabajo, la realización y edición de fotografías y vídeos, la adquisición de descuentos y ofertas en productos y servicios adquiridos a través de Internet o el acceso, actualización y uso de sus perfiles en las redes sociales.

Y precisamente por este motivo no resulta nada sorprendente la enorme penetración de este tipo de dispositivos móviles en todo el territorio europeo. Y es que, aunque su coste es mayor que el de los teléfonos móviles tradicionales, sus amplias funcionalidades parecen haber convencido a los usuarios que no dudan en "rascarse los bolsillos" y adquirir uno de estos terminales.

En este punto, traemos a colación un reciente estudio llevado a cabo por la entidad ComScore quien, tras haber realizado un análisis de la presencia y uso de los *smartphones* a nivel europeo, ha concluido afirmando que España es el Estado Miembro de la UE con una tasa de penetración más alta, habiendo alcanzado el 63,2% de los usuarios del mercado móvil, seguida de cerca por Reino Unido con un 62.3%, y, con un poco más de distancia, Francia, Italia y Alemania.
<http://www.europapress.es/portaltic/sector/noticia-espana-lidera-ranking-europeo-penetracion-crecimiento-smartphones-20121217171637.html>.

Tema: *El E-Commerce B2B aumenta sus ventas en Navidad*

Las Tecnologías de la Información y las Comunicaciones (TIC) están cada vez más presentes en la vida social, política, económica y de ocio tanto de nuestro país como a nivel comunitario e internacional. Y,

en concreto, uno de los sectores que está experimentando un mayor auge en los últimos años es el comercio electrónico.

En este punto, conviene destacar una distinción que, aunque de carácter doctrinal, resulta de utilidad cuando se habla del éxito o fracaso del *e-commerce*, a saber: los diferentes tipos de comercio electrónico que pueden surgir en función del sujeto que vende y el que adquiere, siendo los sujetos posible: una entidad privada, un ente de la Administración Pública o un particular.

En este sentido, pese a que el más conocido es el que se lleva a cabo de empresa a particular, uno de los que más crecimiento ha experimentado en los últimos meses ha sido el conocido como "B2B", esto es, aquel cuyos sujetos protagonistas son dos empresas privadas.

En este punto, traemos a colación un reciente estudio llevado a cabo por el portal de Internet Pixmania-Pro.com en el que se acaban de publicar algunas consideraciones sobre la época navideña en lo que respecta, por un lado, a las previsiones y, por otro, al uso del *e-commerce* en detrimento del comercio tradicional.

Del citado estudio, el primer dato de interés que se desprende es el económico y es que la inversión de las empresas en regalos navideños ascenderá en 2012 a una media de 50 euros.

En esta misma línea, el estudio hace hincapié en la importancia en el uso de las TIC en la adquisición de los productos debido a su comodidad y, en una amplía mayoría de los casos, a su precio competitivo, beneficiándose de sustanciosos descuentos en determinados sitios web. <http://marketing4ecommerce.net/ecommerce-b2b-aumenta-navidad/>.

Tema: *¿El envío de paquetes será servicio universal?*

La Unión Europea ha mostrado en múltiples ocasiones su preocupación por impulsar las TIC en todo el territorio de la Unión, favoreciendo el intercambio de bienes, servicios, productos e información a lo largo y ancho de la Unión.

Y, en los últimos años, los organismos de la UE han mostrado su deseo de favorecer e impulsar el crecimiento y desarrollo del comercio electrónico, venciendo los obstáculos a los que los agentes implicados han de hacer frente, siendo los más comunes: la desconfianza, la falta de seguridad, el desconocimiento de los medios tecnológicos necesarios por parte de los usuarios o el alto coste del envío de los productos de un Estado Miembro a otro.

Y, es que, en multitud de ocasiones, lo que se ha favorecido gracias a las TIC (la interrelación de personas, objetos y servicios con independencia de su localización geográfica y el fácil acceso a productos de calidad y característicos de determinadas zonas) se ve dificultado por cuestiones prácticas del *e-commerce*, siendo una de las más destacadas el elevado coste de los portes cuando el país desde el que se solicita no es el mismo que aquél desde el que se envía.

En este sentido, y teniendo en cuenta que, según un reciente estudio, el 57% de los vendedores señala al coste de las entregas transfronterizas como uno de los principales obstáculos de cara a lograr el pleno desarrollo del comercio electrónico y, en todo caso, con la vista puesta en lograr la consecución de"sistema de entregas (y devoluciones) eficaz" , la Unión Europea acaba de lanzar una consulta pública (cuyo plazo finaliza el 15 de febrero de 2013) cuyo objetivo es conocer de primera mano la opinión de todos los agentes implicados en el sector del comercio electrónico a nivel comunitario sobre cuestiones básicas que afectan a la seguridad jurídica necesaria en la UE en este sentido. En concreto, destacamos la posibilidad que plantea la Comisión Europea en la citada consulta sobre la conveniencia o no de integrar el envío de paquetes en el concepto de servicio universal de cara a que "todos los servicios de reparto de paquetes sean asequibles y de calidad". <http://www.europapress.es/portaltic/sector/noticia-bruselas-plantea-envio-paquetes-sea-servicio-universal-impulsar-comercio-electronico-20121129182325.html>.

Tema: *Crecen las denuncias para retirar contenido de Internet*

En la Sociedad de la Información en la que vivimos, resulta innegable la importancia de tener presencia en Internet, llegando incluso, en algunos casos a convertirse en una necesidad ya que se ha hecho realidad la afirmación de "si no estás en Internet, no existes".

Sin embargo, en los últimos meses, en contraposición a la corriente de opinión en la que la presencia en Internet tiene un elevado valor, lo cierto es que, prácticamente al mismo ritmo con el que se expande la Red, crece la preocupación de los usuarios por el tipo de información accesible en Internet y, en concreto, a través de los motores de búsqueda de la misma.

En este sentido, traemos a colación los datos ofrecidos por la última versión del informe de transparencia que, periódicamente, publica el famoso buscador Google. En concreto, en lo que se refiere a nuestro país, las solicitudes de retirada de contenido por parte de nuestros tribunales e integrantes del Sector Público han experimentado un crecimiento del 60% en comparación con los datos del pasado año. Pese al espectacular aumento en nuestro país, España ocupa el sexto puesto en el ranking respecto al número de solicitud de retirada de contenidos. Así lo indica el citado informe encabezado por Turquía, seguido de Reino Unido, Alemania, Estados Unidos y la India.

Resulta interesante ver cómo el ranking cambia su orden cuando hablamos de órdenes judiciales recibidas para solicitar la retirada de contenido, situándose a la cabeza Estados Unidos, Alemania y Brasil y quedando España en un décimo lugar con tan sólo 17 solicitudes recibidas por las 209 del país americano, por poner tan sólo un ejemplo.

Por último, destacaremos los principales motivos por los que se solicita la retirada de contenidos del buscador, a saber: la privacidad y seguridad es el principal motivo que lleva a las Administraciones y Tribunales a instar al buscador a suprimir el contenido, siendo este motivo el aducido en más de la mitad de los casos. Por lo que se refiere al resto de motivos, baste destacar: la difamación, la promoción de la violencia, la suplantación de identidad o la promoción del odio. <http://www.europapress.es/portaltic/internet/noticia-google-recibio-60-mas-solicitudes-espana-retirar-contenido-20121217132433.html>.

Sección Técnica "*Entorno Digital Personal*" (Diego Gachet Páez, Andrés Marín López)

Tema: *¿Como influirá en nuestras vidas el Internet de las Cosas?*

Partiendo de un concepto básico de que el Internet de las cosas será una red global de objetos identificados por una dirección única en base a protocolos de comunicación estándar, podemos comentar que los objetos del mundo físico podrán interactuar de forma activa decisivamente con el medio ambiente y con nosotros mismos. Por ejemplo, la integración de capacidades de comunicación entre las etiquetas RFID, sensores y actuadores se presenta como una realidad inminente que además se integrará con dispositivos híbridos en el caso de redes de sensores inalámbricos que ya hoy se caracterizan por su modularidad, fiabilidad, flexibilidad, robustez y escalabilidad.

Si bien en la actualidad Internet es una colección de dispositivos bastante uniforme, podemos vislumbrar el Internet de las cosas como

una colección de objetos y dispositivos mucho mas heterogéneo con funcionalidades completamente distintas, así como diferentes en tecnología y aplicabilidad. De esta forma, es fácil imaginar objetos que sean capaces de transportarse a sí mismos, adquiriendo información sobre su posición e instruyendo a las cintas transportadoras hacia donde los deben transportar, siendo capaces asimismo de consultar las bases de datos logísticas y decidir sobre qué ruta seguir.

En los años que vienen veremos con total seguridad el nacimiento de nuevas aplicaciones innovadoras que surgirán de este contexto social y tecnológico de la explotación de la conectividad y la accesibilidad de todo. Algunas las podemos identificar con cierta facilidad. Habrá sistemas de logística mejores y un uso más eficiente de la energía, cambiando muy probablemente el modo de trabajar de la pequeña industria, edificios inteligentes, robots, autos, y ciudades "inteligentes" para facilitar nuestra vida cotidiana.

Aun con una gran dosis de imaginación, es prácticamente imposible predecir el efecto que sobre nuestra vida diaria tendrá el Internet de las cosas.

Sección Técnica *"Informática Gráfica"* (Miguel Chover Sellés , Roberto Vivó Hernando)

Tema: *Conferencias para el año 2013*

La siguiente lista muestra algunas de las conferencias más importantes sobre Informática Gráfica que se celebrarán en 2013. A destacar, el congreso europeo "Eurographics" que se celebrará en Girona y el "Symposium on Rendering" que se celebrará en Zaragoza.

La siguiente lista muestra algunas de las conferencias más importantes sobre Informática Gráfica que se celebrarán el próximo año. A destacar, el congreso europeo "Eurographics" que se celebrará en Girona y el "Symposium on Rendering" que se celebrará en Zaragoza:

- **IEEE 8th Symposium on 3D User Interfaces.** 16–17 de marzo. Orlando, Florida, EUUU. <http://3dui.org/>.
- **ACM SIGGRAPH Symposium on Interactive 3D Graphics and Games.** 21-23 de marzo. Orlando, Florida, EEUU. <http://www.csee.umbc.edu/csee/research/vangogh/I3D2013/>.
- **International Symposium on Biomedical Imaging.** 7-11 de abril. San Francisco, California, EEUU. <http://www.biomedicalimaging.org/2013/>.
- **IEEE International Conference on Computational Photography.** 19-21 de abril. Harvard University Cambridge, EEUU. <http://www.iccp13.org/>.
- **Eurographics 2013.** 6-10 de mayo. Girona, España. <http://eg2013.udg.edu/>.
- **The 26th International Conference on Computer Animation and Social Agents.** 16–18 de mayo. Estambul, Turquía. <http://www.cs.bilkent.edu.tr/~casa2013/>.
- **Computer Graphics International.** 11–14 de junio. Hannover, Alemania. <http://cgi2013.welfenlab.de/>.
- **The Eurographics Conference on Visualization.** 17-21 de junio. Leipzig, Alemania. <http://www.eurovis2013.de/>.
- **24th Symposium on Rendering.** 19-21 de junio. Zaragoza, España. <http://webdiis.unizar.es/EGSR2013/>.
- **Conference on Computer Vision and Pattern Recognition.** 23–28 de junio. Portland, Oregon, EEUU. <http://www.pamitc.org/cvpr13/>.
- **21th International Conference in Central Europe on Computer Graphics, Visualization and Computer Vision.** 24–27 de junio. Pilsen, Czech Republic. <http://www.wscg.eu/>.
- **International Symposium on Non-Photorealistic Animation and Rendering.** 13-21 de julio. Anaheim, California, EEUU. <http://www.cl.cam.ac.uk/conference/expressive-2013/NPAR/Home>.
- **15th International Conference on Human-Computer Interaction.** 21–26 de julio. Las Vegas, Nevada, EEUU. <http://www.hcii2013.org/>.
- **The 40th International Conference on Computer Graphics and Interactive Techniques.** 21–25 de julio. Anaheim, California, EEUU. <http://s2013.siggraph.org/>.

Sección Técnica "*Ingeniería del Software*" (Javier Dolado Cosín, Daniel Rodríguez García)

Tema: *Software tras el bosón de Higgs*

El software está detrás y es la clave de los grandes descubrimientos en física. Este año han tenido una gran repercusión mediática los experimentos de física de partículas realizados en el CERN para la detección del denominado "bosón de Higgs". Detrás de esos experimentos, denominados Atlas y Compact Muon Solenoid, hay un enorme proyecto software que es único en sus objetivos y estructura.

El experimento genera 0.5 Gb/s de datos que se distribuyen a 3.000 físicos en 170 laboratorios. Nos podemos dar una idea del tamaño del proyecto puesto que comprende 4 millones de LOC, repartidas en más de 2.000 paquetes (principalmente C++ y Python). El número de usuarios ronda los 1.500 y el número de desarrolladores es más del millar.

Con respecto al proceso de desarrollo, el proyecto tiene todo el código abierto al resto de desarrolladores, con varios niveles de control. El núcleo de software denominado "*ATLAS Offline*" está organizado en 10 proyectos que se gestionan diariamente para las diferentes configuraciones de sistemas operativos y localizaciones mediante el sistema NICOS (*Nightly Control System*).

ATLAS utiliza diversos *frameworks* para pruebas y validación: ATN (*Atlas Testing Nightly*) para pruebas unitarias; RTT (*Run Time Tester*) para pruebas de funcionalidad y diversas pruebas para el sistema en producción (BCT, *Big Chain Test*) que se ejecutan en GRID con datos simulados.

Según indican sus experiencias, realizar el proceso de construcción y pruebas todas las noches facilita el desarrollo de software e incrementa su calidad.

Podemos encontrar más detalles sobre este apasionante desarrollo software en:

- The Software behind the Higgs Boson Discovery, *IEEE Software, septiembre/octubre 2012*, pp. 11-14.
- **E. Obreshkov.** Software Release Build Process and Components in ATLAS Offline. *Conference on Computing in High Energy and Nuclear Physics 2010*, Taiwan.
- *ATLAS Experiment*. <http://atlas.ch>.
- **T. Colombo, W. Vandelli.** Experience with highly-parallel software for the storage system of the ATLAS Experiment at CERN. *Journal of Physics: Conference Series 396* (2012).

Sección Técnica: "*Lenguajes de Programación*" (Oscar Belmonte Fernández, Inmaculada Coma Tatay)

Tema: *HTML5*

El organismo de estandarización W3C acaba de publicar (17 de diciembre de 2012) la primera versión casi definitiva de HTML5, si bien todavía no se considera un estándar.

Han pasado cuatro años desde que, en 2008, HTML5 comenzara su andadura y la especificación publicada ahora ya tiene todas las funcionalidades desarrolladas. HTML5 da un paso más para convertirse en la plataforma de desarrollo de aplicaciones que puede desplazar a Flash como sistema para aplicaciones multimedia con integración de vídeo, animaciones, gráficos y tipografías. Junto con esta versión se definen también las especificaciones de *Canvas2D*, que proporcionan métodos para crear gráficos bidimensionales sobre un elemento *canvas* HTML.

También ha sido anunciado el primer borrador de la siguiente versión, HTML5.1, así como del *Canvas2D Level 2*, donde se desarrollarán extensiones para accesibilidad, imágenes sensibles o *streaming* adaptativo.

Si bien muchos desarrolladores ya están utilizando actualmente HTML5, todavía es necesario que se avance en la compatibilidad entre navegadores y otras herramientas web, lo cual se prevé que se realizará a finales de 2014.

Tema: *Herramientas para programadores Javascript*

Javascript nació como un lenguaje de *scripting* ligero que se ejecuta, en la mayoría de ocasiones, en el contexto de un navegador web.

La tendencia actual de ofrecer herramientas software como servicios a los que se accede a través de un navegador web ha impulsado el desarrollo de Javascript. Las mejoras continuas en los motores de dibujo de páginas web, y las máquinas virtuales e intérpretes, están alcanzando la demanda de los usuarios de páginas muy dinámicas, con unos tiempos de carga muy reducidos, y respuesta a la interacción comparable al software "tradicional" que instalamos en nuestros ordenadores.

Para los desarrolladores de estos tipos de aplicaciones, tener buenas herramientas de depuración y monitorización de las aplicaciones es fundamental.

Uno de los principales actores dentro de Internet y las aplicaciones web, Google, ha desarrollado un fantástica herramienta para la ayuda al desarrollo de aplicaciones basadas en Javascript, llamada "Chrome Developer Tools", que viene incluida en los navegadores Chrome y en su versión de código abierto Chromium.

Los desarrolladores que usan "Chrome Developer Tools" pueden modificar tanto el DOM como el CSS o el código Javascript usado por la aplicación. Además, cuenta con herramientas que nos permiten conocer con enorme detalle los tiempos de carga y ejecución de los distintos elementos.

Sin duda, una herramienta que todo desarrollador de aplicaciones web debe conocer.

Sección técnica "*Seguridad*" (Javier Areitio Bertolín, Javier López Muñoz)

Tema: *Libros*

- **S.K.S. Gupta, T. Mukheriee, K.K. Venkatasubramanian.** "*Body Area Networks: Safety and Sustainability*". Cambridge University Press. ISBN 1107021022. 2013.
- **R. Chbeir, B. Al Bouna.** "*Security and Privacy Preserving in Social Networks*". Springer. ISBN 3709108934. 2013.
- **M. Mohammed, A-S.K. Pathan.** "*Automatic Defense Against Zero-day Polymorphic Worms in Communication Network*". Auerbach Publications. ISBN 1466557273. 2013.
- **M. Langheinrich.** "*Privacy in Ubiquitous Computing*". Chapman and Hall / CRC. ISBN 1439849773. 2013.
- **B. Applebaum.** "*Cryptography in Constant Parallel Time*". Springer. ISBN 3642173667. 2013.
- **L. Liu.** "*Quantum Techniques and Methods for Security and Policy Driven Computing*". Chapman and Hall / CRC. ISBN 1439866872. 2013.
- **M. Rhodes-Ousley.** „*Information Security: The Complete Reference*". 2nd Edition. McGraw-Hill Osborne Media. ISBN 0071784357. 2013.
- **D. Cowen.** "*Computer Forensics: A Beginner's Guide*". McGraw-Hill Osborne Media. ISBN 007174245X. 2013.

Tema: *Congresos-Conferencias*

- **2013 IEEE 26th Computer Security Foundations Symposium.** Del 26 al 28 de junio 2013. Tulane University. New Orleans. Louisiana. USA.
- **SECURMATICA'2013 (XXIV Congreso Español de Seguridad de la Información).** Del 23 al 25 de abril 2013. Campo de las Naciones. Madrid.
- **20th International Computer Security Symposium and 5th SABSA World Congress.** Del 29 de septiembre al 3 de octubre del 2013. Naas. Irlanda.
- **IT Security Symposium.** Del 24 al 26 de febrero 2013. Dubai. UAE (United Arab Emirates).
- **8th ACM Symposium on Information, Computer and Communications Security 2013.** Del 8 al 10 de mayo de 2013. Hangzhou. China.

Sección Técnica: "*Tecnología de Objetos*" (Jesús García Molina, Gustavo Rossi)

Tema: *Libro*

Marco Brambilla, Jordi Cabot, Manuel Wimmer. *Model-Driven Software Engineering in Practice*. Morgan & Claypool Publishers, 2012**.** ISBN-10: 1608458822.

Un nuevo libro sobre la construcción de software dirigida por modelos está disponible desde el pasado mes de octubre. El título "*Model-Driven Software Engineering in Practice*" llama la atención sobre dos aspectos. Por un lado, que se trata de un libro de "Ingeniería de Software Dirigida por Modelos" (*Model-Driven Software Engineering*, MDSE), la nueva área de la ingeniería del software que aglutina los paradigmas basados en modelos tales como MDA o el desarrollo con lenguajes específicos del dominio (DSL). Por otro lado, subraya la intención de sus autores de un enfoque "práctico".

El libro por lo tanto no tiene por objetivo centrarse en una forma particular de desarrollo basado en modelos sino en los conceptos, técnicas y prácticas que sustentan a cualquier paradigma MDSE. Además, pretende proporcionar la información necesaria para "practicar" con MDSE, aunque no se describen tecnologías concretas. En el capítulo de Introducción, los autores señalan que los posibles destinatarios son: usuarios, desarrolladores, estudiantes y curiosos (CTOs, CIOs, jefes de equipo...), esto es, un libro abierto a todo tipo de lectores.

El libro está organizado en dos partes: "Fundamentos de MDSE" (capítulos 2 al 6) y "Aspectos Técnicos de MDSE" (capítulos 7 al 10).

El capítulo 2 define los principios básicos de MDSE (modelo, metamodelo y transformación), así como otras cuestiones como la terminología, la adopción industrial y algunas críticas que se hacen a MDSE. El capítulo 3 es muy interesante y presenta las principales

aplicaciones de MDSE: automatización del desarrollo de software, interoperabilidad de sistemas y modernización de software. El uso de los modelos para realizar una conexión entre diferentes tecnologías (interoperabilidad) no es muy conocido y se explica de forma clara. El capítulo 4 explica de forma muy breve MDA (la visión más conocida de MDSE que fue propuesta por OMG) e introduce ADM, la propuesta de OMG para modernización de software basada en modelos. El capítulo 5 analiza brevemente la integración de MDSE en procesos de desarrollo de software existentes, en particular en los procesos ágiles, diseño dirigido por el dominio (DDD) y desarrollo dirigido por pruebas (TDD). El espacio dedicado es muy reducido (apenas 6 páginas) y el capítulo se limita a comentar algunas ideas generales sobre el uso de MDSE en los procesos mencionados. La parte de presentación de los fundamentos de MDSE finaliza con el estudio de la noción de "lenguaje de modelado". Se clasifican los lenguajes en dos categorías: lenguajes de modelado de propósito general (GPML) y lenguajes de modelado específicos del dominio (DSML). Como ejemplo de los primeros, se presenta con cierto detalle UML y se defiende el papel que ha jugado y jugará en el desarrollo de software. Luego se muestran ejemplos de VHDL, i* y BPMN como ejemplos de DSMLs. El capítulo acaba con una breve presentación de OCL como lenguaje para completar modelos y metamodelos.

La segunda parte del libro arranca con un capítulo destinado a mostrar cómo aplicar un enfoque basado en el metamodelado para la creación de lenguajes de modelado. Es el capítulo más largo (30 páginas) y resulta muy interesante. Explica cómo se define una sintaxis abstracta como un metamodelo y cómo en torno a él se pueden definir una o más sintaxis concretas, ya sean gráficas o textuales. También se explica de forma clara la noción de "arquitectura de cuatro niveles del metamodelado". Se introduce el ejemplo del lenguaje sWML (*Simple Web Modeling Language*) para ilustrar, en este capítulo y en los dos siguientes, los conceptos introducidos. Se analiza la creación de un metamodelo (con las reglas OCL) para sWML y se muestra cómo se crearía una sintaxis textual con Xtext y una gráfica en EuGENia, todo ello en el contexto de EMF/Eclipse. Este capítulo combina bien la teoría con la práctica, y desarrolla y clarifica algunos conceptos que se habían explicado con anterioridad.

Los siguientes dos capítulos están dedicados a las transformaciones de modelos y comentan bastantes aspectos de ellas. En el capítulo 8 se estudian las transformaciones modelo-a-modelo que se clasifican en dos categorías: exógenas y endógenas. Se utiliza ATL para mostrar un ejemplo muy simple de transformación para un problema extraído del caso de estudio sWML. Incluye un apartado sobre el manejo de transformaciones que no aborda el problema de la composición interna y externa de transformaciones y algunas soluciones existentes. En el capítulo 9 se introduce el problema de la generación de código y se presentan las transformaciones modelo-a-texto, mostrando un ejemplo simple de transformación en el lenguaje Acceleo para generación de código en el caso del ejemplo sWML. Por último, el capítulo 10 introduce de forma muy breve una serie de aspectos de MDSE que son esenciales para su adopción industrial, que hoy son en su mayoría tema de investigación aunque algunas herramientas eficientes y robustas ya empiezan a estar disponibles: intercambio de modelos, repositorios de modelos, versionado de modelos, comparación de modelos, manejo global y desarrollo colaborativo.

Desde esta columna hemos comentado la mayoría de libros publicados sobre ingeniería del software dirigida por modelos y sus diferentes visiones, y en alguna ocasión hemos notado que se echaba en falta un texto que presentase los conceptos y técnicas básicas de MDSE de forma sencilla y didáctica y que, además, mostrase cómo ponerlos en práctica a través de varios ejemplos que ilustrasen diferentes aplicaciones.

El libro de Brambilla, Cabot, y Wimmer supone un paso importante en esa dirección. Es el primero que ofrece una visión global de MDSE como una disciplina de la ingeniería del software, aunque su corta extensión (164 páginas) ha impedido una mayor profundidad que sería deseable en algunos aspectos.

Nuestra principal objeción sería que no alcanza la naturaleza práctica que, a nuestro entender, desean los profesionales o "curiosos" que buscan un libro que les muestre aplicaciones prácticas de las técnicas de MDSE, como serían el tratamiento en profundidad del caso de estudio sWML, y los beneficios obtenidos. Por nuestra experiencia, es un libro más apropiado para estudiantes de un curso de postgrado que para profesionales. Pero, sin duda, se trata de un excelente libro que debe ser leído por aquellos interesados en una introducción a la ingeniería del software dirigida por modelos, y estamos seguros que disfrutarán con su amena lectura y que aprenderán bastante sobre esta nueva disciplina.

Sección Técnica: "*Tecnologías para la Educación*" (Juan Manuel Dodero Beardo, César Pablo Córcoles Briongos)

Tema: *SIIE 2012*

El Simposio Internacional de Informática Educativa (SIIE) celebró su decimocuarta edición en Andorra la Vieja (Andorra) del 29 al 31 de octubre de 2012. Su organización recayó en esta ocasión en La Salle Open University, lo que supone la incorporación de un nuevo país, Andorra, como anfitrión del congreso después de las últimas ediciones celebradas en Salamanca (España), en Coimbra (Portugal), en Santiago de Chile y en Aveiro (Portugal).

El SIIE ha sido un evento tradicionalmente ligado a la comunidad Iberoamericana. En esta edición se ha buscado una mayor presencia internacional para, sin perder ese sello de identidad, permitir la apertura a más grupos de investigación relacionados con la Informática Educativa a lo largo y ancho de todo el mundo.

Las claves de esta apertura internacional se pueden resumir en las siguientes actuaciones principales: 1) incremento del número de miembros del Comité Científico de países fuera del ámbito iberoamericano; 2) organización de sesiones íntegramente en inglés; 3) inclusión del SIIE en la base de datos de conferencias de IEEE (*conference record #21316*); 4) publicación de los artículos presentados en el SIIE y traducidos íntegramente al inglés como *postproceedings* en la biblioteca digital de IEEE (*IEEE Xplore*); y 5) organización de varios números especiales en revistas internacionales, en las que se publicarán versiones extendidas de los mejores artículos de esta edición del SIIE.

Esta edición se ha completado con algunos eventos asociados como son la Segunda Edición de la *Special Session on International Research Projects on Socio-Semantic Technologies Applied to Education*, el Tercer Taller en Ingeniería del Software en *e-Learning* (ISELEAR 2012), y el taller formativo "*De la Idea a la Realidad*".

Otra novedad en esta edición ha sido la concesión del premio "Antonio Vaquero" al mejor artículo del SIIE 2012, en honor del mayor impulsor de la Informática Educativa en el ámbito iberoamericano, que comentamos a continuación.

Tema: *Concesión del premio Antonio Vaquero*

ADIE (Asociación para el Desarrollo de la Informática Educativa, <http://www.adie.es/>) ha creado el Premio Antonio Vaquero para reconocer la calidad de la investigación realizada actualmente por la comunidad hispanoamericana en informática educativa. Es un

premio humilde, consistente en un diploma acreditativo, pero cuyo valor residirá en su prestigio.

Se premia el "mejor" trabajo presentado en el simposio bandera de ADIE, el Simposio Internacional de Informática Educativa (SIIE), habiéndose concedido por primera vez en la XIV edición, celebrada en Andorra entre los días 29 y 31 de octubre.

Se seleccionó el trabajo mejor puntuado por los revisores para su aceptación en el congreso y por el presidente de la sesión donde se presentó, resultando seleccionada la comunicación "*Percepción de la apertura de los LMS en las ramas educativas y tecnológicas*".

En esta primera edición, el premio fue entregado por el propio Antonio Vaquero en el acto de clausura, con asistencia del presidente del Comité de Organización, Lluís Vicent, el presidente del Comité de Programa, Francisco García Peñalvo, y el presidente de ADIE, Ángel Velázquez. El diploma acreditativo fue recogido por el autor que lo había presentado, Miguel Angel Conde, de la Universidad de Salamanca, quien agradeció el premio a los calificadores y revisores, y también dedicó a Antonio Vaquero unas cariñosas y emocionadas palabras.

Sección Técnica: "*TIC y Turismo*" (Andrés Aguayo Maldonado, Antonio Guevara Plaza)

Tema: *"Comparte Iniciativas", plataforma de intercambio de transferencia tecnológica turística*

La Secretaría de Estado de Turismo ha puesto en marcha una plataforma de intercambio de transferencia tecnológica en materia turística entre las comunidades autónomas, que será coordinada por la Sociedad Estatal para la Gestión de la Innovación y las Tecnologías Turísticas (SEGITTUR) <http://www.segittur.es>.

La plataforma, denominada "Comparte Iniciativas", da respuesta al llamado "Espíritu de El Hierro", surgido tras la Conferencia Sectorial, celebrada en la isla en el mes de marzo, y constituye un ejemplo de cooperación y mejora en el uso eficiente de los recursos, gracias a la cooperación interterritorial.

"Comparte Iniciativas", que fue presentado en el mes de junio en San Sebastián, en la Mesa de Directores de Turismo, tiene como objetivo que cada comunidad autónoma ofrezca los desarrollos tecnológicos y de innovación emprendidos en los últimos años para el sector turístico, que en la mayoría de los casos habían quedado limitados a su territorio.

Se trata de una plataforma tecnológica en la que las CC. AA. podrán compartir información, buenas prácticas, conocimiento, desarrollos tecnológicos y producto turístico, a la vez que les permitirá poner en marcha proyectos innovadores de forma conjunta, que contribuyan a la mejora de la competitividad y la sostenibilidad turística de sus territorios.

La plataforma, de uso restringido para la Administración Pública, permitirá a las comunidades reducir los gastos que implica el desarrollo de proyectos participativos al lograr agrupar a los técnicos en espacios virtuales de construcción colectiva. Asimismo, reunirá a todos los técnicos interesados en un tema y fomentará el desarrollo de ideas y proyectos que apoyen los procesos de innovación y gestión dentro del sector turístico.

Constituye un canal a través del cual podrán conocer iniciativas de otras comunidades autónomas que puedan ser de su interés y que resuelvan una problemática común.

En definitiva, "Comparte Iniciativas" permitirá a las CC. AA. avanzar en el desarrollo de sus proyectos, compartiendo su conocimiento y apoyándose en el de otros, lo que sin duda revertirá en el beneficio de todos, tanto desde el punto de vista económico, como del desarrollo del sector turístico español.

La Comunidad Autónoma de la Región de Murcia ha sido la primera en adherirse a "Comparte Iniciativas", al haber cedido gratuitamente la Plataforma de comercialización de productos y servicios turísticos, HERMES, compuesta por cuatro proyectos: ARPA, destinado a la carga de alojamientos ORION, para la carga de producto; ATENEA, gestor de experiencias; y AURIGA, distribución B2B del producto. Murcia también ha cedido los desarrollos relativos a la herramienta "Sabueso" con la que se monitorizan los precios de los establecimientos en las distintas webs comerciales, así como la aplicación "Destino Región Murcia" que recoge un listado de recursos de la Región y la posibilidad de compra.

Además de Murcia, otras Comunidades Autónomas ya han suscrito también este acuerdo de colaboración: La Rioja, Extremadura, Galicia, Castilla y León y Navarra y está previsto que paulatinamente se vaya incorporando el resto.

Wilmer Pereira
Escuela de Ingeniería Informática, Universidad Católica Andrés Bello (UCAB), Caracas (Venezuela)

<wpereira@ucab.edu.ve>

Enseñanza de la Seguridad Computacional como instrumento de la ética profesional

Este artículo fue seleccionado de entre las mejores ponencias presentadas en el Congreso Iberoamericano de Educación Superior en Computación (CIESC 2011) celebrado en Quito (Ecuador) en octubre de 2011.

Resumen: *La Seguridad Computacional como asignatura se basa en la teoría que sustenta las técnicas de cifrado para asegurar, entre otras características: privacidad de los datos (confidencialidad), verificación de identidad (autenticación), evitar rechazo de compromisos (no repudio) y respeto a los derechos de autor (copyright). Así se protege la información de los usuarios en un entorno de red abierto. Sin duda hay aspectos éticos que subyacen y deben orientar el proceso educativo. La perspectiva educativa es importante debido al conocido atractivo que ejerce sobre los estudiantes el conocer las técnicas de ataques a sitios o servidores informáticos, realizados por intrusos o atacantes maliciosos. Los estudiantes centran mucho su atención en como se realizan los ataques más que en conocer lo que el atacante hace, sus efectos y sobre todo como prevenir las consecuencias nefasta de los ataques. En este artículo presentamos una estrategia de enseñanza basada en el hacking blanco o preventivo en contraposición al hacking negro o destructivo. Para ello inducimos al estudiante en el uso de herramientas de prevención, respetando la privacidad, la identidad y las responsabilidades asumidas. Además de la estrategia educativa en el aula, utilizamos una competencia interuniversitaria para reforzar el compromiso ético del estudiante. Este evento sobre delito digital se celebra cada dos años en Venezuela y participan estudiantes de ingeniería, derecho y comunicación social. Tanto en el curso de seguridad computacional como en la competencia, el objetivo es mostrar qué hace el atacante sin necesariamente hacer explícito como lo hace, bajo la perspectiva de la prevención, del compromiso ante los usuarios y, en el caso de la competencia, descubrir los culpables de un delito digital.*

Palabras clave: *Ataques Informáticos, autentificación, confidencialidad, copyleft, ética profesional, no repudio, Seguridad Computacional.*

1. Introducción

La ética profesional es sin ninguna duda uno de los aspectos fundamentales para el buen desempeño de los profesionales egresados de nuestras universidades latinoamericanas públicas y privadas.

Además de graduar ingenieros de calidad debemos formar buenos ciudadanos, íntegros, honestos y responsables de su compromiso con la sociedad. En consecuencia, la enseñanza debe estar reforzada con valores que afiancen los principios éticos dada la importancia del rol que juegan, específicamente los ingenieros, en el aparato productivo de cada país.

En este sentido el docente universitario juega un papel fundamental al impartir principios directivos que orienten los juicios y la ética del profesional. Annie Cohen-Solal, en su libro titulado "*Jean-Paul Sastre*", recoge testimonios de alumnos del conocido filosofo en el liceo de Havre, entre los que resalta el de Pierre Brument: "*Con Sartre se ponían en duda las ideas preconcebidas, se desarrollaba el espíritu crítico, la exigencia de un pensamiento personal y la honestidad intelectual*" [2].

Es decir, creatividad y no seguir al pie de la letra modelos preconcebidos, no implica el rompimiento de normas de respeto al individuo que impone la sociedad. Más aún Nussbaum, también conocida profesora del área de filosofía clásica y ética, cita en un artículo: "*Como dijo Heráclito hace 2.500 años: aprender sobre muchas cosas no da lugar al entendimiento. Marco Aurelio insistía en que, para llegar a ser ciudadanos del mundo, no bastaba con acumular conocimientos; también debíamos cultivar una capacidad de imaginación receptiva que nos permitiera comprender los motivos y opciones de personas diferentes a nosotros, sin verlas como extraños que nos amenazan, sino como seres que comparten con nosotros muchos problemas y oportunidades*" [2].

De estos argumentos se intuye que para el docente, estrechamente ligado al proceso de aprendizaje, no basta con impartir los conocimientos del área, sino, también, debe enseñar principios de comprensión y aceptación para lograr mejores profesionales con amplitud de criterio, aptitud crítica y una posición de compromiso ante la sociedad.

El caso particular de un profesional egresado del área de Ingeniería Informática o Computación, debe manejar información sensible o confidencial de la compañía para la cual trabaja y proteger tanto los datos como el software. Por ejemplo el ingeniero tiene los medios para acceder al sueldo de cada empleado, datos de cualquier computadora de la empresa (sobre todo si trabaja en el servicio de soporte de hardware y software), uso de cualquier recurso, en fin puede conocer mucha información de la empresa. Ante este panorama es vital que el ingeniero muestre integridad y honestidad para poder ser depositario de la confianza de sus empleadores, clientes y personal subalterno.

En la Facultad de Ingeniería de la Universidad Católica Andrés Bello, existe un curso obligatorio de Ética y Ejercicio Profesional (impartida para las ingenierías: informática, civil, industrial y telecomunicaciones) donde los estudiantes toman conciencia de que su bienestar individual descansa sobre su compromiso con el entorno. Allí examinan casos de estudio para reforzar los conceptos éticos desde distintos puntos de vista o teorías.

El curso de Seguridad Computacional ofrece un marco de experimentación ideal para aplicar principios éticos en casos específicos y directamente ligados con el ejercicio profesional. Durante el curso se tienen presente ciertas premisas como la prevención y resguardo de la información ante intrusos y ataques informáticos. El docente enseña las técnicas de protección de los canales de comunicación y la información local de los computadores, siempre tomando en consideración que el ingeniero es el garante de la seguridad en el medio informático donde se desenvuelve.

Así, en esta asignatura, hemos ideado una estrategia para inducir al estudiante sobre la importancia de asegurar cuatros aspectos fundamentales: la confidencialidad, la autentificación, el no repudio y el respeto a los derechos de autor. Con la estrategia propuesta para la enseñanza de estos conceptos, se motiva en el estudiante principios éticos y se desmotivan intenciones de exploración insana, sin la autorización debida, de centros y servidores informáticos. Se induce al estudiante a asumir la responsabilidad que

> “En la Facultad de Ingeniería de la Universidad Católica Andrés Bello, existe un curso obligatorio de Ética y Ejercicio Profesional… donde los estudiantes toman conciencia de que su bienestar individual descansa sobre su compromiso con el entorno”

implican las promesas y los compromisos, siempre respetando los derechos de los demás.

De hecho, intentamos convencerlos de lo inútil que resulta mostrar como se realizan los ataques e incitarlos a asumir una actitud apegada a la ley, que vele por la seguridad e integridad de los datos, personas y recursos de las instituciones para las cuales trabajarán.

Además organizamos, cada dos años, una competencia de simulación de juicio sobre delito informático, donde participan estudiantes de las escuelas de derecho, informática y comunicación social. El objetivo es definir equipos interdisciplinarios donde las habilidades a nivel legal se complementan con la experticia técnica, para conducir una acusación, en el caso del fiscal, o probar la inocencia de un implicado, valiéndose de la evidencia digital, en el caso de la defensa. Todo reseñado por comunicadores sociales que siguen las incidencias del juicio y el comportamiento de sus actores.

2. Motivación y objetivos

Desde hace un buen tiempo hay consenso en el área de informática sobre la importancia de la seguridad de la información. Gradualmente muchos *pensum*[1] de pregrado están incluyendo una asignatura específica aunque en la mayoría de los casos como materia electiva. Por otro lado, en Venezuela, unas pocas universidades tienen muy recientemente ofertas de postgrado cortos en seguridad y hasta una conocida compañía de seguros armó una formación de un año.

Sin embargo, la oferta sigue siendo poca para las exigencias del mercado. Ante esta situación diversas instituciones y compañías privadas, a nivel internacional, están ofreciendo certificaciones. Algunas de las más conocidas son: CISM (*Certified Information Security Manager*) y CISA (*Certified Information System Auditor*) de ISACA, CEH (*Certified Ethical Hacker*) y CHFI (*Certified Hacking Forensic Investigator*) de EC-Council, GSEC (*GIAC Security Essential*) de GIAC, CSSP (*Cisco Certified Security Professional)* de CISCO, entre las más conocidas. Esta situación no sólo se presenta en Venezuela sino en buena parte de Iberoamérica [9].

Este estudio no pretende competir con el nivel de detalle de las certificaciones sino más bien, en una asignatura, reforzar los principios éticos impartidos, mostrando las herramientas de seguridad y sólo considerando la posibilidad de intrusión como punto de partida para definir detalladamente las políticas de defensa.

Durante la materia se siguen los siguientes lineamientos para lograr que el docente obtenga el objetivo general antes enunciado:
1) Presentar las herramientas de prevención y protección ante intrusiones y ataques informáticos.
2) Mostrar como desarrollar políticas de seguridad conociendo las debilidades y cuales son los puntos vulnerables, sin mencionar como se realizan los ataques.
3) Mostrar en clases, generalmente a partir de exposiciones de los estudiantes, casos reales de antiguos intrusos y como se desenvuelven sus actividades y vida una vez descubiertos.
4) Preparar semanalmente talleres cerrados sobre el uso práctico (instalación y configuración) de herramientas de protección y prevención ante ataques.
5) Montar un proyecto de seguridad en computadores, de ser posible individualmente, con fines meramente preventivo, con protección de servidores, y usando herramientas de código abierto. En ese proyecto se debe prevenir o proteger contra:

- Suplantación de identidad.
- Violación de la privacidad de la información.
- Rechazo a los compromisos asumidos.
- Irrespeto a los derechos de autor.

6) Incentivar la participación en el modelo de simulación de delito informático para que el estudiante perciba la importancia de los grupos interdisciplinarios y aplique sus conocimientos y principios éticos.

En esta asignatura, la estrategia se desarrolla a todo lo largo del semestre y se culmina con la presentación del proyecto que utiliza: certificados digitales para la autentificación, cifrado de canales para la confidencialidad, firma digital para evitar el rechazo de los compromisos y código *copyleft* como alternativa para no utilizar herramientas propietarias que irrespeten el *copyrigth*.

3. Marco teórico

Inicialmente en esta sección se presentan los principios básicos de seguridad computacional y posteriormente los fundamentos que rigen la ética en informática.

3.1. Seguridad Computacional

La seguridad, desde el punto de vista técnico, se aboca a los mismos desafíos que debe afrontar la seguridad convencional. De hecho, siempre han existido aspectos vitales para el resguardo de la información entre los que se encuentran: la confidencialidad, la autentificación, el no repudio y el respeto por los derechos de autor.

El primer concepto tiene que ver con la privacidad de los datos, ya sea mientras se transmite información o cuando los datos se colocan en algún medio de almacenamiento del computador. El cifrado normalmente se realiza con algoritmos de clave simétrica dado que son 1.000 veces más rápidos que los algoritmos de clave pública.

Por otro lado, la autentificación se vale de los certificados digitales que contienen la clave pública, única para cada usuario, y acoplada con su clave privada. Justamente es esta última clave la que permite firmar documentos que, en contrapartida, se verifican gracias a la clave pública que contienen los certificados. Por último, el *copyleft*, en contraposición al *copyright*, permite la distribución y uso de software que puede ser usado sin costo, modificado y a su vez redistribuido sin irrespetar ningún derecho de autor.

Un ejemplo práctico donde se combinan todos estos conceptos, en el ámbito digital, es en el comercio electrónico, cuando se cancela mediante el número de la tarjeta de crédito. Ante todo, es necesario entregar el número de la tarjeta de crédito con la previa verificación de la identidad del ente comercial. La autentificación debe preceder al intercambio de información, de ser requerido cifrado, para asegurar que los datos son entregados y recibidos con privacidad para las personas o los entes autorizados.

Una vez llegado a un acuerdo sobre el bien recibido y el descuento de dinero sobre la tarjeta de crédito, el cliente espera una factura firmada para avalar el compromiso de venta del sitio de comercio electrónico (aunque la mayoría de las veces este último paso no se realiza) [7].

3.1.1. Autentificación y certificados digitales

Para lograr verificar la identidad de una persona existen tres métodos importantes [8]:

“ Justamente estas dos vertientes perfilan, según los propios *hackers*, a los primeros como *hackers de sombrero blanco* o simplemente *hackers* y a los segundos como *hackers de sombrero negro o crackers* ”

- Bajo el conocimiento de una secuencia de seguridad o clave.
- Con el porte de un documento o carnet de identificación.
- Verificando características propias del usuario mediante aparatos especializados.

El primer método es el más utilizado y se basa en el conocimiento que tiene el usuario de una secuencia de dígitos y/o caracteres para ser autenticado. Se parte del principio de que sólo el propietario conoce esta clave, lo cual permite asegurar su identidad. Sin embargo, presenta el inconveniente del olvido de la clave o que, bajo coacción o descuido, un usuario no autorizado puede obtener dicha clave.

Debido a estos problemas se ha desarrollado el segundo método, que consiste en exhibir un documento que avala la identidad del portador. Así se logra la autentificación sin que el usuario deba recordar ninguna información. No obstante, se presenta el problema de que sin exhibir el documento el usuario pierde su identidad pues, en realidad, a quien se autoriza es al documento y por ende al portador actual (no necesariamente al propietario). Además, está el problema de la falsificación o clonación de documentos.

Estas deficiencias conducen a un tercer método, más personal, donde el titular no depende ni de una clave que debe recordar ni de un documento que está obligado a exhibir. Aquí se cuenta con un aparato especializado capaz de leer información propia del titular: huella dactilar o palmar, secuencia de ADN, registro del iris, etc. Esta estrategia de autenticación se conoce como *biometría* y, en principio, resuelve algunas de las deficiencias de los dos primeros métodos. Sin embargo, tampoco es infalible: los dispositivos lectores son aún muy costosos y, desafortunadamente, no son capaces de impedir que bajo coacción un titular sea obligado a exhibir alguna parte de su cuerpo para facilitar el acceso a un intruso.

Dado que ninguno de los métodos es infalible, resulta común que se usen combinados para elaborar sistemas de seguridad más robustos y difíciles de violar [7].

El método de portar un documento o prenda también se puede emular con un documento digital, no físico, que avala la identidad de su portador. Así, en una transacción electrónica el propietario exhibe un documento digital que permite al receptor constatar la identidad del emisor. Este tipo de documento se conoce como *certificado digital*, el cual usa técnicas de cifrado conocidas como algoritmos de clave pública o asimétricos comúnmente usados para la autentificación y negociado de las claves simétricas [8].

Dado que este documento digital es público, para evitar suplantación de identidad, algún ente confiable debe avalar los certificados digitales para detectar si son alterados. Estas entidades, también conocidas como *Autoridades de Certificación*, son organismos confiables que avalan la identidad de personas y entes comerciales. Así, la mayor parte de las transacciones bancarias y comercio electrónico se sustenta en esta infraestructura (conocida como PKI: *Private Key Infraestructure*) para validar la identidad de los entes que participan en un intercambio comercial [8].

3.1.2. Firma digital y *copyleft*

Para avalar la autoría de un documento digital, se requiere del uso de la clave privada ya que esa clave está bien resguardada y sólo le pertenece al usuario portador. La verificación de la firma digital es posible gracias a la clave pública ya que con ella se extrae el compendio o *hash* original del mensaje y se compara con el compendio del mensaje recibido. Si son iguales se acepta el documento. En caso contrario, se rechaza el mensaje.

La firma digital tiene múltiples usos. Uno de ellos es el aval que las autoridades de certificación dan al certificado, firmando con su clave privada, las claves públicas de sus clientes. Es decir, el certificado es distribuido con la firma de la autoridad de certificación y la verificación se obtiene usando la clave pública de la propia autoridad.

Por otro lado, el uso de software de libre distribución, en particular con las licencias *copyleft* [13], es útil cuando no se desea o no es posible utilizar el software propietario, protegido por *copyrigth.* El estudiante desarrolla el proyecto sin infringir derechos comerciales de empresas desarrolladoras de software. De hecho el software de libre distribución ha generado todo un movimiento con el patrocinio de licencia *copyleft*, el cual, en contraposición a *copyrigth,* tiene como condición que los códigos fuente son abiertos es decir a disposición de quien lo desee. En la mayoría de los casos se puede comercializar, siempre bajo la condición de que el código debe estar disponible (aunque hay variantes dentro de la filosofía *copyleft* como el caso de las opciones débil o fuerte).

3.1.3. Benefactores e intrusos

Todos estos mecanismos, junto con la confidencialidad o cifrado de la información, se definen para evitar y prevenir los ataques informáticos realizados por personas con alto nivel técnico pero posiciones ideológicas muy cuestionables.

En términos generales, personas con un alto nivel de experticia son conocidas como *hackers*. Ellos encuentran su motivo de vida en alcanzar un nivel técnico alto para, en el mejor de los casos, explorar y diagnosticar fallas en los sistemas. En su peor faceta, son delincuentes que se apropian de información para obtener beneficio personal en detrimento de los auténticos propietarios de la información o bienes.

Justamente estas dos vertientes perfilan, según los propios *hackers*, a los primeros como *hackers de sombrero blanco* o simplemente *hackers* y a los segundos como *hackers de sombrero negro* o *crackers*. La existencia de ambas corrientes justamente antepone principios éticos y permite ver en muchos casos que la frontera es difusa. De hecho hay autores [12] que argumentan que no existen *hackers* éticos pues las típicas posiciones que asumen como benefactores pueden ser fácilmente refutadas.

Por ejemplo, los argumentos más comunes que presentan los *hackers* para justificar sus acciones son:

- Mostrar debilidades de los sistemas para que sean corregidos.
- La información es libre de fluir por Internet sin censura.
- Los estudiantes pueden practicar *hacking* para adquirir habilidades que les permitirán conseguir cierto tipo de empleos.
- Los *hackers* son protectores de la omnipresencia del sector público fuertemente regulador.

Ninguno de estos argumentos supera un examen exhaustivo desde el punto de vista ético por lo que algunos autores aseguran que bajo ninguna circunstancia los *hackers* generan algún beneficio a la sociedad. Para más detalles ver [12].

Por otro lado, a pesar de la comprobada nocividad de las actividades de los *crackers*, aún existen muchos inconvenientes para poder enjuiciarlos y acusarlos de daños a los sistemas informáticos. El problema está en el gran nivel de experticia que debe poseer el

“Por último, está la irresistible atracción que ejercen estos personajes sobre los adolescentes pues se circundan de una ‘aureola heróica’ y contra el sistema que les hace ganar la admiración de adolescentes inconformes”

investigador policial, junto con el fiscal, para poder levantar pruebas y evidencias sobre un medio virtual y bien resguardar la cadena de custodia. Esta cadena es el conjunto de medidas que deben adoptarse a fin de preservar la identidad e integridad de objetos o muestras que pueden ser fuente de prueba de hechos criminales, para su total eficacia procesal [4]. Otro aspecto que influye es que, en general, las leyes sobre delito informática son muy genéricas, lo cual es un factor que dificulta la aplicación de la justicia [1].

Por último, está la irresistible atracción que ejercen estos personajes sobre los adolescentes pues se circundan de una “aureola heróica” y contra el sistema que les hace ganar la admiración de adolescentes inconformes [10]. Justamente éste es el punto sobre el cual se enfoca el curso de Seguridad Computacional para desincentivar actitudes nocivas y destructivas en nuestros estudiantes.

3.2. Ética en Informática

Desde el punto de vista más general la ética define los principios directivos que orientan a las personas en su concepción de vida para lidiar con los juicios, los hechos y la moral. La informática, como su nombre indica, maneja diversos tipos de información y por su potencial de acceso y uso, aunado a las posibilidades que ofrece Internet, genera problemas éticos. Estos se agravan en muchos casos por la ambigüedad de las leyes y regulaciones [6].

Algunos estudios se han abocado a la tarea de definir códigos éticos que llenen los vacíos jurídicos que existen en algunos ámbitos del problema. Algunos trabajos exploran las perspectivas de distintas organizaciones en diferentes países para encontrar puntos coincidentes [3].

Es de notar que las leyes de casi cualquier país, cubren de alguna manera los aspectos más importantes. En particular, la ley sobre delitos informáticos venezolana [1] contempla aspectos como violaciones a la autenticación, privacidad, derechos de autor, etc.

Sin embargo las ambigüedades surgen cuando los delitos traspasan fronteras, algo muy común por el uso de Internet. Otro problema es al levantar pruebas sin que se “contaminen” para que no sean anuladas en los juicios. De hecho en la UCAB hemos dictado cursos a agentes policiales y fiscales donde hemos podido constatar esta dificultad.

La principal dificultad se centra en el resguardo de la cadena de custodia, sobre todo cuando hay evidencia digital. Ésta debe, como mínimo, estar firmada digitalmente por el investigador en presencia de testigos. Esto requiere un conocimiento técnico del investigador policial con el que desafortunadamente no siempre se cuenta.

En otros casos, un investigador contamina la escena digital, es decir, toca el computador antes de hacer el respaldo del disco y firmarlo digitalmente. En consecuencia, en algunos casos, se enturbia la comunicación entre los investigadores y los fiscales. En la competencia justamente interactúan estos dos actores: abogados y especialistas en informática. Antes del evento, el especialista técnico debe levantar la evidencia digital, procesarla y definir la cadena de custodia. A posteriori los abogados, con ese insumo, levantar el caso para la acusación o la defensa.

4. Metodología educativa

Como se mencionó en la introducción y objetivos, la estrategia en la cátedra de Seguridad Computacional es mediante una preparación continua y progresiva con material teórico, talleres prácticos de herramientas de protección/prevención y un proyecto a desarrollar a todo lo largo del semestre. También se realiza un evento, estilo competencia, donde se ejercitan habilidades adquiridas por los estudiantes durante su formación.

4.1. Estrategia docente

Para la asignatura las clases teóricas son en un aula con el apoyo de videoBeam[2] y las clases prácticas en un laboratorio con computadores. En la parte teórica, a grandes rasgos, se cubre en la primera parte del semestre los temas de criptografía simétrica y asimétrica, firma digital y certificación digital.

En la segunda parte se presentan las herramientas de protección clásica: cortafuegos, sistemas de detección de intrusos, redes privadas virtuales, etc. A modo de complemento, en la parte práctica, se hacen 10 talleres en el semestre para reforzar la teoría impartida.

Los temas que abordan los talleres son:

- Seguridad básica (en el sistema operativo Linux).
- Comandos de red seguros (para comandos como ssh, sftp, scp, etc).
- Cifrado simétrico y asimétrico (con GPG).
- Certificación digital (con openSSL).
- Husmeadores y monitoreo de red (con el *sniffer* wireshark y NESSUS).
- Redes privadas virtuales (usando open VPN).
- Cortafuegos (bajo Linux con iptables).
- Sistemas de detección de intrusos (bajo snort).
- Servidores seguros (instalando http+SSL y DNSSec).
- Programación cliente/servidor segura (usando el *security manager* de Java).

Es de notar el fuerte énfasis en el uso de herramientas preventivas, por ejemplo, el preferir NESSUS (práctica 5) en lugar de nmap. Aunque ofrecen las mismas funcionalidades para exploración de vulnerabilidades, NESSUS indica sugerencias de cómo mejorar o cerrar brechas ante “huecos de seguridad”.

Por otro lado está la realización de un proyecto práctico con estrategias de enseñanza controladas, utilizando las herramientas necesarias para la prevención y protección ante ataques e intrusiones informáticas. Éste incluye la instalación conjunta de las herramientas utilizadas en las prácticas, bajo una aplicación cliente/servidor, para proteger tanto el equipo, como los componentes del software y el usuario del sistema. En este proyecto es necesario asegurar los servicios básicos como son la confidencialidad, la autentificación, el no repudio y preservar los derechos de autor.

Entre los proyectos que se han desarrollado están: sitios de comercio electrónico, repositorios seguros de datos y claves, instalación de un segmento de una LAN segura con servidores de red, etc.

4.2. Competencia interuniversitaria

Este evento de simulación de un juicio define el marco para poner en práctica las ideas trabajadas por el estudiante en un ámbito más general, situado dentro del contexto jurídico-técnico-comunicacional.

Inicialmente se le entrega a cada universidad información sobre un fraude o delito del cual se tiene evidencia en documentos físicos y

electrónicos. Las instituciones participantes preparan al menos 5 equipos: defensa y fiscalía conformado por estudiantes de derecho, peritos informáticos para la defensa y la fiscalía, con estudiantes de computación y estudiantes en comunicación social quienes preparan entrevistas y redactan un pequeño instrumento informativo reseñando el juicio.

Cada universidad, un mes antes del evento, debe entregar la acusación para que el resto de las universidades sepan los cargos que se le imputan a cada uno de los acusados.

El día del evento se realiza un sorteo de como se mezclarán los equipos en cada juicio. Evidentemente habrá varios juicios en simultáneo y cada uno presidido por jueces voluntarios, jubilados o aún en ejercicio. Esto para asegurar la completa imparcialidad del personaje cuyo rol conciliador y rector de cada juicio es asegurar un desarrollo satisfactorio de la actividad. Además al momento del cierre del evento, se aprovecha la gran experiencia de los jueces, para mostrar a cada universidad sus fortalezas y debilidades.

Para cada juicio se conforma un grupo de expertos, en cada área del conocimiento, y se les entrega un instrumento de evaluación. Cada miembro de ese grupo, en función a su experticia, evalúa los equipos estudiantiles del juicio que presencia.

Finalmente, al dictarse sentencia en todas las salas, los grupos de expertos se reúnen y, con las puntuaciones, se entregan reconocimientos por área (derecho, informática y comunicación social) y un premio para la universidad con mayor puntuación de todos sus equipos.

5. Discusión

Los aspectos explícitamente trabajados durante el dictado de la asignatura se refieren a: La estrategia educativa, las habilidades técnicas y las consideraciones subjetivas. El rol del profesor, entre otras consideraciones, evita personificarse con el atacante, y siempre asume una posición que respete los derechos de los demás. Esto es de vital importancia para la percepción del estudiante sobre la seguridad informática.

5.1. Estrategia educativa

La interdependencia entre las clases teóricas y los talleres en el laboratorio afianzan y consolidan la relación entre la teoría y la praxis. Cada taller se realiza una vez que el tema es cubierto en clases. Para esta asignatura se exige que el estudiante debe aprobar tanto los exámenes teóricos como el trabajo práctico (talleres + proyecto). A nuestro juicio esta relación vincula estrechamente los conocimientos impartidos con su aplicación en el mundo real.

El material de apoyo se vale de libros de texto, láminas e información en Internet. Entre los medios de difusión de seguridad en el mundo iberoamericano, está la red Criptored, con el patrocinio de la Agencia Española de Cooperación Iberoamericana y coordinado principalmente por la Universidad Politécnica de Madrid. Su principal función es la difusión y enseñanza de la seguridad no sólo en el ámbito universitario sino también empresarial [9].

5.2. Habilidades técnicas

Tanto en los talleres como en el proyecto se deben trabajar y evaluar cuatro aspectos que resumen las pautas que debe seguir cualquier sistema seguro:

- Resguardo de la privacidad y verificación fidedigna de la identidad.
- Evitar ataques e intrusiones en los sistemas informáticos.
- Asumir las responsabilidades y compromisos.
- Protección de la propiedad intelectual de información y bienes.

Para asegurar la autentificación se exige que el proyecto use certificados digitales reforzado con el uso de buenas prácticas de palabras claves seguras al momento de la conexión. Esta última se maneja con palabras claves suficientemente largas, con caracteres diferentes y controlando el número de intentos para evitar ataques de fuerza bruta. Todo esto concientiza al estudiante sobre la importancia de una verificación sólida de la identidad.

El cifrado se trabaja tanto en los talleres como en el proyecto y generalmente se hace montando herramientas que hagan el negociado de la clave simétrica al momento del establecimiento de la conexión, justo después de la autentificación. El resguardo de la privacidad es vital para mantener la confianza del usuario sobre la plataforma y aplicaciones que utiliza. Tener plena certeza que la información no será visible por terceros, aumenta la confianza en los medios digitales.

La firma digital es exigida también para el proyecto pues en principio da tranquilidad al eventual cliente de la aplicación. Así se sabe que si la persona que realizó el intercambio no acepta su compromiso, se dispone de un medio legal para demandarlo ante el incumplimiento de sus obligaciones.

El uso de software *copyleft*, tanto en el proyecto como en los talleres, evita caer en el uso indebido de aplicaciones y programas informáticos privativos, usados sin pago, ya que el *copyleft* es una alternativa para desarrollar aplicaciones económicas con el aval de toda la comunidad GNU.

Todo esto se amalgama con la utilización de una librería (sobre todo en el proyecto) para potenciar servidores y aplicaciones, como lo es SSL (*Secure Sockets Layer*). Esta librería es ampliamente usada para la navegación segura vía Web. También se ofrece al estudiante la posibilidad de usar otras librerías de seguridad de los lenguajes de programación más conocidos, como lo es el caso del *security manager* de Java.

5.3. Posturas éticas del docente

En primer lugar, a todo lo largo del curso de Seguridad Computacional se utiliza un vocabulario donde se habla de *crackers* siempre en tercera persona, evitando cualquier asociación con el docente o algún estudiante. Lo ideal es no asumir roles que inadecuadamente propicien conductas de *crackers*.

También se evita, en lo posible, presentar como se realizan los ataques informáticos. Siempre se indica qué hace el ataque y sólo se explica como se realizan cuando son ataques muy conocidos de los cuales se tienen herramientas de protección. Esto permite que el estudiante se concentre inmediatamente en jugar un rol opuesto al *crackers* para asumir una posición de protector de la seguridad.

Un argumento, que permite justificar al docente en su negativa de explicación de los ataques, es que la rapidez con la que cada ataque es tomado en cuenta, en las herramientas de protección, es tal que puede hacer extremadamente largo y arduo para hacer el seguimiento. Es decir, se puede dedicar mucho tiempo a explicar un ataque que a fin de cuentas cuando se hace público ya no es un ataque que atente contra la integridad de un servidor o computador permanentemente actualizado.

Otro aspecto es convencerlos, con ejemplos de *hackers* famosos, que este camino no siempre lleva al éxito. Ellos mismos constatan que un estudiante a punto de graduarse no se proyecta a futuro realizando *hacking* negro. Este estilo de vida implica vivir en el anonimato, sin poder sacar provecho directo de su gran nivel de experticia a menos que revelen su identidad. Y si mientras el *hacker* está en el proceso de aprendizaje, se ha dedicado a actividades ilícitas, hacer pública su identidad sólo puede traerles múltiples inconvenientes. Con ejemplos de casos reales, los estudiantes verifican que cada es más común el poco reconocimiento que tienen esas personas dada la gran cantidad de profesionales honestos, con buenos niveles de experticias, y que liberan a las empresas de contratar "delincuentes digitales".

Otro aspecto a considerar es mostrar al estudiante los límites entre sus derechos y el de los demás. Un ejemplo claro es el derecho a la privacidad que se contrapone a la libertad

> “También se evita, en lo posible, presentar como se realizan los ataques informáticos. Siempre se indica qué hace el ataque y sólo se explica como se realizan cuando son ataques muy conocidos de los cuales se tienen herramientas de protección”

de información. Es decir la información, en principio, es privada para quien la posee pero debe ser pública en la medida que beneficia a la sociedad y que resultaría inadecuado ocultar. De manera análoga ocurre con el derecho al anonimato que es diametralmente opuesto al deber de la responsabilidad del individuo. Es decir, tengo derecho a no divulgar mi identidad mientras con ello no esté evadiendo responsabilidades. Es de notar que la primera dualidad tiene que ver con la confidencialidad mientras que la segunda está relacionada con la autenticación. Estos son dos conceptos claves en el curso y se afianzan y refuerzan en todo momento.

Es de notar que estos aspectos (confidencialidad, autenticación y ataques) son abordados por la Ley venezolana contra Delitos Informáticos en particular la privacidad en los artículos 11, 20, 21 y 22, autentificación en los artículos 6 y 12 y sanciones contra los ataques informáticos en los artículos 7, 8 ,9 y 10 [1].

Por último en lo que concierne a la competencia, no tenemos ninguna duda que esta actividad fomenta la interdisciplinaridad sobre todo en dos áreas que deben interactuar en busca de un beneficio común durante el ejercicio profesional. Debido a la mala relación que existe entre los investigadores y los fiscales, hemos querido hacer explícita esta dificultad, para incitar al estudiante a esforzarse por la importancia del trabajo en equipo, en la búsqueda de la verdad, cuando se está ante un delito electrónico.

6. Conclusiones y recomendaciones

Estos intentos son los primeros pasos para reforzar aptitudes y actitudes éticas en nuestros estudiantes, en primer lugar, con ejemplos prácticos y desarrollo de un proyecto que inmediatamente aplican en bien de la protección y resguardo de información y bienes. En segundo lugar, la competencia es un ambiente motivante y lleno de retos que implican resolver los enigmas que plantea el caso. De hecho allí constatan como proteger antes de aprender como atacar, lo cual, sitúa al estudiante del bando adecuado.

Durante el curso se genera también la conciencia de que la seguridad no es sólo responsabilidad del ingeniero informático sino también de los usuarios de los sistemas. El ingeniero debe impulsar al usuario o cliente a tomar medidas que resguarden sus datos personales y que definan mecanismos seguros locales, por ejemplo, adoptar claves no ingenuas que puedan ser fácilmente adivinadas por terceros mal intencionados.

A lo largo de nuestra experiencia hemos notado menor interés del estudiante por las técnicas de ataques que típicamente usan los *crackers*. Antes teníamos casos donde, abiertamente en el aula, nos solicitaban que les enseñásemos como atacar, pero ante nuestra clara posición ahora es muy poco frecuente. De hecho en nuestra primera experiencia dictando el curso formamos grupos de ataque y de defensa y, realmente, fue una pésima idea que hasta generó enemistades entre los alumnos. Sin embargo, la experiencia nos concientizó sobre la necesidad de una estrategia ética en la cátedra de Seguridad Computacional.

En trabajos futuros estudiaremos el problema de los sistemas espías (*Spyware*) [5] y troyanos que representan una intromisión a la privacidad y definir estrategias educativas que muestren al estudiante los límites entre el deseo de informar y proteger sin violentar los derechos ciudadanos. También estamos por definir una estrategia educativa para que nuestros estudiantes desarrollen hábitos para el uso de herramientas de compartir recursos (P2P) como kazza, e-mule, limewire, etc, sin violentar los derechos de propiedad.

Por último vale la pena mencionar los esfuerzos recientes que se están haciendo para consolidar un plan de educación para la seguridad en informática [11]. Cuando estas líneas lleguen al lector, se habrá realizando el Primer Taller Latinoamericano de Enseñanza e Innovación Educativa en Seguridad de la Información (TIBETS 2011) que tendrá lugar a finales del año 2011 en Bucaramanga, Colombia. El principal instrumento de trabajo será una encuesta que permitirá emitir un primer informe sobre el estado del arte en enseñanza y formación en Seguridad de la Información en los paises iberoamericanos. Este evento cuenta con el apoyo de Criptored, cuyo coordinador es el Prof. Jorge Ramió de la Universidad Politécnica de Madrid.

Agradecimientos

Este trabajo contó con la participación de los profesores Jorge García y Rafael Andara en la realización de los talleres del laboratorio de seguridad.

Referencias

[1] Asamblea Nacional de Venezuela. Ley Especial contra los Delitos Informáticos, *Gaceta oficial N. 37.313*, 30 de octubre de 2001.

[2] Carlos Berbosa. Elogio de la Docencia Universitaria, periódico *El País, 8/5/2006*, España.

[3] Porfirio Barroso. *Cuatro Principios de la ética*. Disponible en: <http://www.ccee.edu.uy/ensenian/catcomp/material/etica.pdf, 1997>.

[4] Jeimy J. Cano. *Computación Forense: descubriendo los rastros informáticos*. Editorial Alfaomega, 1ra. edición, 2009. ISBN 978-958-682-767-6.

[5] Otorgan Derecho a Instalar Spyware en su PC, *El Diario de Caracas, 18 de noviembre de 2005*.

[6] John Foley, Pierfranco Pastore. *Ética en Internet*. Web del Vaticano <http://www.vatican.va> (última modificación 22 de febrero de 2002).

[7] Luis Gabaldon, Wilmer Pereira. Usurpación de Identidad y Certificación Digital en el Fraude Electrónico. *Revista Sociologias Universidade Federal do Rio Grande do Sul, N. 20*, Dic/2008, pp. 184-190, Porto Alegre, Brasil.

[8] Simson Garfinkel, Gene Spafford. *Seguridad y Comercio en la web*. Mc Graw Hill y O'Reilly, México, 2000.

[9] Jorge Ramió Aguirre, Pino Caballero Gil. Enseñanza de la criptografía y seguridad de la información en España: Primer informe de perfiles de asignaturas. *Revista Seguridad Informática en Comunicaciones (SIC), N.34*, abril de 1999. <http://www.criptored.upm.es/investigacion/informe.htm>.

[10] Manu Rodríguez. *Hackers: aristócratas de la red*. Disponible en <http://www.cibersociedad.net>, 2000.

[11] Miguel Rodríguez. La Seguridad Informática: Una necesidad en la docencia. Universitaria. *Revista PLAC (Publicación Latinoamericana y Caribeña de Educación), nº 1*, enero-abril, 2010.

[12] Eugene Spafford. Are Computer Hacker Breakins Ethical. *Journal of System & Software, January 1992*, Vol. 17, number 1, pp. 41-47.

[13] Richard Stallman. *El Manifiesto GNU*. <http://www.gnu.org/gnu/manifiesto.es.hml>, 1990.

Notas

[1] Nota del editor: “Conceptualmente un pensum es una descripción de algunos de los requerimientos que se aa satisfacer para obtener un grado universitario en un área del saber”, <http://universidadesymasuniversidades.com/producto.php?producto=Pensum+universitario>.

[2] El material de apoyo se encuentra en <http://www.ldc.usb.ve/~wpereira/docencia/seguridad>.

El problema del Buscaminas Cuadrado en 3D

Julio Javier Castillo, Diego Javier Serrano, Marina Elizabeth Cárdenas
Laboratorio de Investigación de Software MsLabs, Dpto. Ing. en Sistemas de Información, Facultad Regional Córdoba - Universidad Tecnológica Nacional (Argentina)

<jotacastillo@gmail.com>,
<diegojserrano@gmail.com>,
<ing.marinacardenas@gmail.com>

Este es el enunciado del problema F de los planteados en la Cuarta Competencia de Programación de la Facultad Regional de Córdoba (Universidad Tecnológica Nacional, Argentina) UTN-FRC celebrada el 23 de octubre de 2012.

Nivel del problema: Medio

El buscaminas Cuadrado es un buscaminas en el cual el objetivo del juego es encontrar dónde están todas las minas dentro de un campo de NxNxN (ver **figura 1**).

Por ejemplo, supongamos el siguiente campo de 3x3x3 con minas (que está representado por un asterisco *), donde cada una de las 3 dimensiones está separada por una línea con numerales.

```
*..
...
.*.
###
...
.*.
.**
###
*.*
...
.*.
```

El campo de las minas representan los ejes X e Y, y el campo de eje Z representa el campo de minas contiguo en el espacio. Entonces el problema nos requiere que calculemos las minas adyacentes en cada unas de las posiciones "." de cada dimensión, por lo cual para el caso de entrada anterior tendríamos:

```
*41
4-4
3*-
###
-4-
6*6
4**
###
*3*
4-5
3*-
```

Notar que en el caso que haya una mina en la misma posición de alguna otra dimensión adyacente, se deberá colocar un "-" en esa posición.

Entrada

La entrada comenzará con un número entero indicando la cantidad de buscaminas 3D a analizar. A continuación en la próxima línea tendremos un número entero indicando el tamaño (2<=n<=5) del buscaminas que vendrá en las próximas líneas, donde cada una de las dimensiones (largo, ancho, profundidad) serán separadas entre sí por una línea de numerales "###".

Las siguientes n líneas contienen los caracteres "*" o "." y representan el campo. Cada lugar seguro es representado por un carácter "." (sin las comillas) y cada cuadro minado es representado por un carácter "*" (también sin las comillas).

Salida

Para cada campo, se deberá imprimir el buscaminas reemplazando en las líneas que contienen el campo con el carácter "." por el número de minas adyacentes. En el caso que haya una mina en la misma posición de alguna otra dimensión adyacente, se deberá colocar un "-" en esa posición. Debe haber una línea con "DDD" (sin las comillas) luego de cada buscaminas que haya sido procesado.

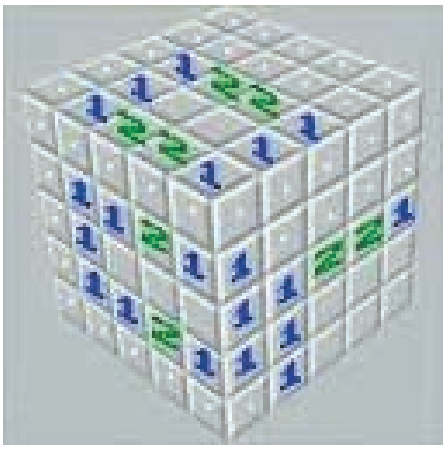


Figura 1. Ejemplo a título ilustrativo.

Ejemplo de entrada

```
2
3
*..
...
.*.
###
...
.*.
.**
###
*.*
...
.*.
2
*.
..
##
..
*.
```

Ejemplo de salida

```
*41
4-4
3*-
###
-4-
6*6
4**
###
*3*
4-5
3*-
DDD
*2
-2
##
-2
*2
DDD
```

El problema de los paréntesis y los corchetes

Julio Javier Castillo, Diego Javier Serrano, Marina Elizabeth Cárdenas
Laboratorio de Investigación de Software MsLabs, Dpto. Ing. en Sistemas de Información, Facultad Regional Córdoba - Universidad Tecnológica Nacional (Argentina)

<jotacastillo@gmail.com>,
<diegojserrano@gmail.com>,
<ing.marinacardenas@gmail.com>

El enunciado de este problema apareció en el número 217 de ***Novática*** (mayo-junio 2012, p.59)

El problema planteado consiste en reconocer expresiones matemáticas que contienen paréntesis y corchetes balanceados. Por ejemplo, la expresión "[(a*b) + (c/2)] *[(3*v)+2]" tiene que ser reconocida por el programa, mientras que la expresión "((y*x]) + z))" no tiene que ser reconocida, pues contiene un corchete de cierre sin su correspondiente corchete de apertura, y falta un paréntesis de apertura.

Ya que el problema consiste en determinar si los paréntesis y corchetes están balanceados, se pueden ignorar los demás caracteres de la expresión y analizar la cadena equivalente "[( ) ( )] [( )]".

Desde el punto de vista de la Teoría Formal de Lenguajes Formales y Autómatas, el problema se puede plantear como "reconocer el lenguaje que genere paréntesis y corchetes balanceados", el cual se corresponde con la siguiente gramática G en BNF (*Backus Naur Form*).

G = ({ (,), [,] } , {S} , S , {S := SS | (S) | [S] | λ}),

donde G es una 4-upla formada por los símbolos terminales, no terminales, el símbolo distinguido(o axioma) y el conjunto de reglas de producción de la gramática G.

Esta gramática produce un conjunto de cadenas, y al tratarse de una gramática independiente de contexto, sabemos que existe un autómata pila que las reconoce.

Una propuesta para el autómata a pila (AP) que reconoce el lenguaje anterior es :

$$AP = (\Sigma_E, \Gamma, Q, q_0, A_0, F, f)$$

$$\Sigma_E = \{(,), [,]\}, \Gamma = \{A_0, (,), [,]\}, Q = \{q_0, q_1, q_2, q_3, q_4, q_f, t\}, q_0 = q_0, A_0 = A_0, F = \{q_f\}$$

Donde Σ_E indica el conjunto de símbolos terminales de entrada, Γ indica el conjunto de símbolos de la pila, Q es el conjunto de estados del autómata, q_0 es el estado inicial del autómata, A_0 es el símbolo base de la pila, y F es el conjunto de estados finales. La función de transición *f* se puede deducir del autómata de la **figura 1**.

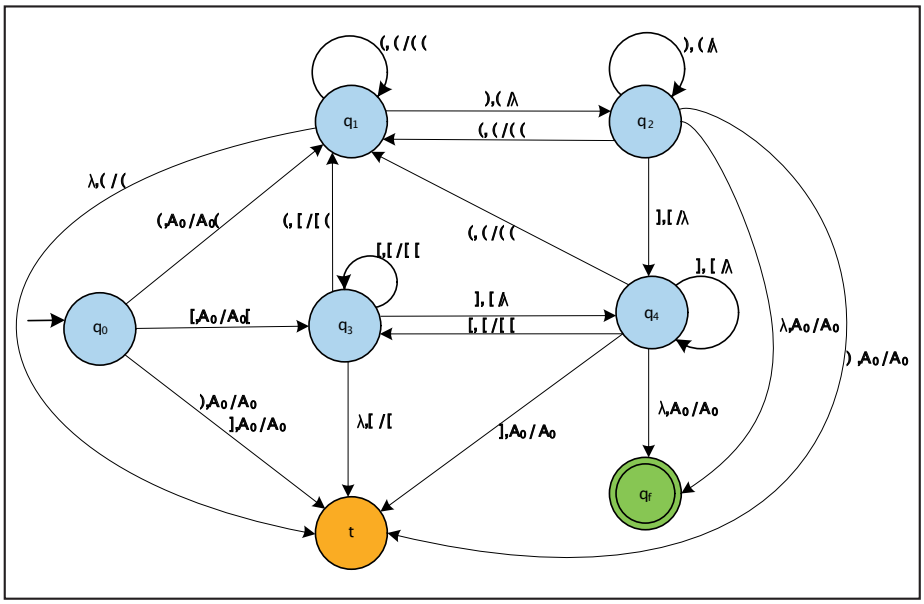


Figura 1. AP que acepta cadenas con paréntesis y corchetes balanceados.

Esta propuesta asume que el AP aceptará cadenas por vaciado de pila y por alcance de estado final.

Asimismo, nótese que el AP incorpora un estado t (estado de trampa), que describe una condición de error de la cual el autómata no puede salir una vez que acontece, es decir que una vez que llega al estado de trampa, esa cadena no será aceptada. Las transiciones representan: "símbolo leído de la cadena de entrada, símbolo leído del tope de la pila / símbolos que se escriben sobre la pila". Por ejemplo, $(,A_1 0\ /A_1 0\ (\ $ significa que se lee un paréntesis de la cinta de entrada, que se lee el símbolo base de la pila A_0, y que se apilan sobre la pila A_0 y (.

El AP comienza apilando paréntesis o corchetes, representados por los estados q_1 y q_3, y desapilando paréntesis o corchetes en los estados q_2 y q_4. Si al desapilar se encuentra que los paréntesis o corchetes no están balanceados se transita del estado q_2 o del estado q_4 al estado trampa t. Por otra parte, si al apilar paréntesis o corchetes se termina de leer la cadena de entrada, esto indica que han faltado paréntesis o corchetes de cierre, por lo cual ante esta situación se transita del estado q_1 o del estado q_3 al estado trampa t. Caso contrario, la cadena estará balanceada y el AP terminará en el estado final q_f y con la pila solamente conteniendo el símbolo de base de la pila (condición de aceptación).

Este modelo formal puede ser fácilmente implementado si se utilizan bibliotecas estándar del lenguaje de programación de su elección. En efecto, la estructura de datos `Stack` (o pila) se encuentra como parte de la biblioteca estándar del lenguaje Java en el paquete `java.util.Stack`.

En otros lenguajes como Python, es posible utilizar los métodos `append()` y `pop()` para apilar y desapilar elementos de una lista. De esta manera, es posible utilizar una pila (estructura de datos de tipo LIFO) implementada con una lista y dos operaciones que trabajan sobre el tope de la pila.

Respecto a la solución en Java, se utiliza la colección `Stack` para apilar los caracteres '(',y '[', y se desapilan los caracteres ')', y ']'. Además, se puede observar que cualquier otro carácter leído de la entrada estándar es ignorado por el programa.

A continuación se exponen dos soluciones a este problema, una planteada en lenguaje Java y la otra en el lenguaje de programación Python.

```
//Solución propuesta en Java
import java.util.Scanner;
import java.util.Stack;

public class Main {
    public static void main(String[] args) {
        Scanner sc = new Scanner(System.in);

        int c = sc.nextInt();
        sc.nextLine();

        for (int i = 0; i < c; i++) {
            String linea = sc.next();
            Stack<Character> abiertos = new Stack<>();
            boolean resultadoOK = true;
            for (int j = 0; resultadoOK && j < linea.length(); j++) {
                switch(linea.charAt(j)) {
                    case '(': abiertos.push('('); break;
                    case '[': abiertos.push('['); break;
                     case ')': if (abiertos.empty() || abiertos.pop() !='(') resultadoOK = false;
break;
                     case ']': if (abiertos.empty() || abiertos.pop() !='[') resultadoOK = false;
break;
                }
            }
            if (resultadoOK) resultadoOK = abiertos.empty();
            System.out.println(resultadoOK ? "SI": "NO");
        }
    }
}

#/Solución propuesta en Python
def balanceada(linea):
  abiertos = []
  for c in linea:
     if c == '(' or c == '[' :
          abiertos.append(c)
     if c == ')' and (len(abiertos) == 0 or abiertos.pop() != '('):
          return False
     if c == ']' and (len(abiertos) == 0 or abiertos.pop() != '['):
          return False
  return len(abiertos) == 0

c = int(input())

for i in range(c):
    if balanceada(input()):
        print('SI')
    else:
        print('NO')
```

Convocatoria para nuevas secciones en Novática 223

Como ya anunciamos en nuestros números anteriores, seguimos apuntando al número 223 de ***Novática*** (mayo-junio de 2013) para publicar artículos de dos nuevas secciones recientemente estrenadas: "Visiones" y "Socios". Ambas secciones aspiran a publicar artículos basados en opiniones y/o experiencias personales relativamente cortos y fáciles de leer.

En el caso de "Visiones" tenemos abierta una convocatoria titulada "*Visiones sobre el mundo de la programación*" que puede consultarse en <http://www.ati.es/spip.php?article2275>.

Por su parte, en "Socios" deseamos publicar artículos basados en *experiencias profesionales de los socios de ATI*, también breves y fáciles de leer. Se establece como una convocatoria permanente que será, no obstante, referida a determinados números para facilitarnos la gestión del espacio disponible en la revista.

Cambios en Secciones Técnicas de Novática

Como suele ser habitual en los principios de año, hemos introducido algunos cambios en los equipos de coordinadores de secciones técnicas de nuestra revista.

En concreto, en la sección "Arquitecturas" ***José Flich Cardo*** (profesor de la Universidad Politécnica de Valencia) sustituye a ***Jordi Tubella***, a quién agradecemos muy sinceramente su excelente contribución a Novática durante largos años. ***José Flich*** formará ahora equipo con ***Enrique Torres*** en la citada sección.

Por otra parte, ***Sebastià Justicia Pérez*** (Diputació de Barcelona) se incorpora a la sección "Administración Pública electrónica" para formar equipo con ***Francisco López Crespo***.

Queremos dar nuestra más cálida bienvenida a José y a Sebastià. Es nuestro deseo que se encuentren muy a gusto colaborando con nosotros.

Programación de Novática

Por acuerdo del Consejo Editorial de ***Novática***, los temas y editores invitados de las monografías de 2013 serán, salvo causas de fuerza mayor o imprevistos, los siguientes:

Nº 221: (enero-febrero 2013): "Modularidad en el diseño de software". Editoras invitadas: ***Lidia Fuentes Fernández*** (Directora del Grupo de investigación en software orientado a aspectos y componentes - CAOSD/GISUM-, Universidad de Málaga), ***Mónica Pinto Alarcón*** y ***Mercedes Amor Pinilla*** (Departamento de Lenguajes y Ciencias de la Computación, Universidad de Málaga).

Nº 222: (marzo-abril 2013): "Lenguajes de programación". Editores invitados: ***Óscar Belmonte Fernández*** y ***Carlos Granell Canut*** (Universitat Jaume I, Castellón).

Nº 223 (mayo-junio 2013): "Eficiencia energética en centros de proceso de datos". Editor invitado principal: ***José Manuel Moya Fernández*** (Universidad Politécnica de Madrid).

Nº 224 (julio-agosto 2013): "Minería de procesos". Editores invitados: ***Antonio Valle Salas*** (Socio Director de G2) y ***Anne Rozinat*** (Cofundadora de Fluxicon, Eindhoven, Países Bajos).

Nº 225 (septiembre-octubre 2013): "Pruebas de software: Nuevos retos". Editores invitados: ***Javier Dolado Cosín*** (Universidad del País Vasco) y ***Daniel Rodríguez García*** (Universidad de Alcalá de Henares).

Nº 226 (noviembre-diciembre 2013): "Empresa 2.0". Editor invitado principal: ***Joaquín Peña Siles*** (Universidad de Sevilla).

Socios institucionales de ati

Según los Estatutos de ATI, pueden ser socios institucionales de nuestra asociación "*las personas jurídicas, públicas y privadas, que lo soliciten a la Junta Directiva General y sean aceptados como tales por la misma*".

Mediante esta figura asociativa, todos los profesionales y directivos informáticos de los socios institucionales pueden gozar de los beneficios de participar en las actividades de ATI, en especial congresos, jornadas, cursos, conferencias, charlas, etc. Asimismo los socios institucionales pueden acceder en condiciones especiales a servicios ofrecidos por la asociación tales como Bolsa de Trabajo, cursos a medida, *mailings*, publicidad en Novática, servicio ATInet, etc.

Para más información dirigirse a <*info@ati.es*> o a cualquiera de las sedes de ATI. En la actualidad son socios institucionales de ATI las siguientes empresas y entidades:

AGENCIA DE INFOR. Y COMUN. COMUNIDAD DE MADRID
AGROSEGURO, S.A.
AIGÜES TER LLOBREGAT
ALC ORGANIZACIÓN Y SISTEMAS,S.L.
ALMIRALL, S.A.
3ASIDE CONSULTORS, S.L.
AVANTTIC, CONSULTORÍA TECNOLOGICA, S.L.
CENTRO DE ESTUDIOS VELAZQUEZ S.A. (C.E. Adams)
CETICSA, CONSULTORIA Y FORMACIÓN
CONSULTORES SAYMA, S.A.
COSTAISA, S.A
DEPARTAMENT D´ENSENYAMENT DE LA GENERALITAT
ELOGOS, S. L.
EPISER, S.L.
ESPECIALIDADES ELÉCTRICAS, S.A. (ESPELSA)
ESTEVE QUÍMICA, S.A.
FUNDACIÓ BARCELONA MEDIA - UNIVERSITAT POMPEU FABRA
FUNDACIÓ CATALANA DE L´ESPLAI
FUNDACIÓ PRIVADA ESCOLES UNIVERSATÀRIES GIMBERNAT
iiR ESPAÑA
IN2
INFORMÁTICA Y COMUNICACIONES AVANZADAS, S.L.
INSTITUT D'ESTUDIS CATALANS
INSTITUT MUNICIPAL D´INFORMÀTICA
INVERGAMING GRUP
KRITER SOFTWARE, S.L.
NETMIND, S.L.
ONDATA INTERNATIONAL, S.L.
PRACTIA CONSULTING, S.L.
QRP MANAGEMENT METHODS INTERNATIONAL
RCM SOFTWARE, S.L.
SADIEL, S.A.
SERVICETONIC, S.L
SISTEMAS TÉCNICOS LOTERIAS ESTADO (STL)
SOCIEDAD DE REDES ELECTRÓNICAS Y SERVICIOS, S.A.
SQS, S.A
TRAINING & ENTERPRISE RESOURCES
T-SYSTEMS ITC Services España S.A.
UNIVERSIDAD ANTONIO DE NEBRIJA
UNIVERSIDAD EUROPEA DE MADRID
UNIVERSITAT DE GIRONA
UNIVERSITAT OBERTA DE CATALUNYA