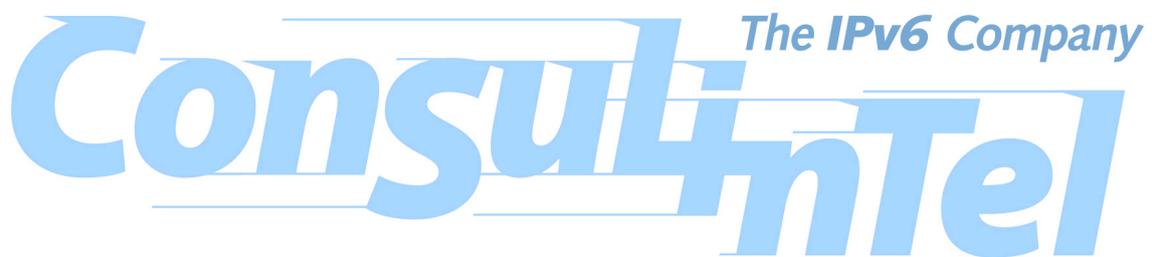


IPv6 para España:

Agotamiento de IPv4 o Transición a tiempo a IPv6 para el adecuado crecimiento de la Banda Ancha



Madrid, Febrero de 2.011

Jordi Palet (Consulintel)

v1.7

1. Resumen Ejecutivo.....	3
2. Estado del Arte	4
2.1. ¿Qué es IPv4?	4
2.2. El Agotamiento de IPv4	5
2.3. ¿Qué es IPv6?	6
2.4. Estado de adopción de IPv6.....	7
2.5. ¿Porqué no se despliega IPv6 con mayor rapidez?.....	12
2.6. Iniciativas en el mundo	14
2.7. Acciones gubernamentales.....	15
3. Oficina Técnica de IPv6 en España	18
4. Innovación y Negocio con IPv6	19
4.1. Sensores y actuadores.....	20
4.2. Gestión de “utilities” (SmartGrids)	20
4.3. Domótica/Inmótica	21
4.4. Intelligent Transport Systems	21
4.5. Monitorización remota y Video-vigilancia	22
4.6. Comunicaciones Máquina-a-Máquina (MxM).....	22
4.7. Redes Móviles 4G (LTE)	22
4.8. “Cloud Computing” y “GRIDS”	23
4.9. Virtualización	23
4.10. Electrodomésticos Inteligentes	23
4.11. Alertas de Catástrofes	24
4.12. Defensa y Orden Público	24
4.13. Servicios de información y publicidad dinámicos.....	25
4.14. Juegos y otras actividades On-line.....	25
5. Anexo I: Detalle de Iniciativas en el Mundo.....	26
5.1. Organizaciones Internacionales	26
5.2. Europa.....	27
5.3. Norteamérica.....	29
5.4. Latinoamérica y Caribe	29
5.5. Asia Pacífico	30
5.6. África	32

1. Resumen Ejecutivo

Internet Protocol es el mecanismo que permite el funcionamiento de Internet, actualmente la versión 4 (IPv4). El agotamiento del mismo es inminente, concretamente el 3 de Febrero de 2011, IANA ha entregado las últimas direcciones IPv4 a cada una de las 5 regiones, previéndose el agotamiento en Europa en torno a final del verano de 2011.

Existe una solución que ha sido estandarizada y comprobada en todo tipo de redes desde hace años, y que está disponible en los equipos de usuarios finales y operadores. Es la nueva versión de IP, concretamente la versión 6 (IPv6), que nos garantiza la continuación del despliegue de Internet de Banda Ancha durante posiblemente los próximos 480 años.

Este protocolo ya está siendo desplegado en operadores de todo el mundo desde el año 2002, y sin embargo, la penetración en España es prácticamente inexistente, que queda muy rezagada, incluso por detrás de países en vías de desarrollo.

Son muchos los gobiernos y entidades internacionales que no sólo han hecho saltar la alarma, sino tomado acciones, incluso hace ya varios años, para garantizar la continuidad y el crecimiento de la economía digital.

Los planes de despliegue de Banda Ancha no podrán cumplirse si no se toman medidas urgentes para garantizar que la administración pública, proveedores de contenidos, ISPs y la industria en general, toma conciencia del problema y se deciden las acciones pertinentes, de tal forma que los usuarios puedan comenzar a utilizar IPv6 de un modo satisfactorio y casi sin apercibirse del cambio, abriendo la puerta al mismo tiempo a nuevas oportunidades de negocio, nuevos tipos de aplicaciones y servicios, que a su vez, harán crecer más la demanda de Banda Ancha y la llegada de "La Internet de las Cosas".

España corre además el riesgo de una nueva "Brecha Digital", si otros países, como ya está ocurriendo, se mueven hacia IPv6 y los proveedores de contenidos continúan con sus planes de despliegue de IPv6 que aunque inicialmente suponen el mantenimiento de IPv4, a medio-largo plazo, supondrán la desaparición de éste último de la Red.

No realizar la transición a IPv6 supone también un retroceso para la industria nacional, de lo que podrían sacar provecho competidores más preparados. En cambio, la transición a IPv6 supone la generación de muchos nuevos puestos de trabajo y un importante crecimiento económico, tanto en el momento de la transición como en los años venideros.

Se propone por tanto la constitución de una Oficina Técnica, al modo de la que ha permitido el despliegue de la TDT en España, para elaborar un plan de acción, las recomendaciones regulatorias, documentación, formación, coordinación del sector, comunicación de todos los aspectos del plan de acción, y seguimiento del mismo.

2. Estado del Arte

2.1. ¿Qué es IPv4?

Internet esta basada en el denominado Protocolo de Internet (IP, Internet Protocol), y desde su inicio comercial, se ha utilizado la versión 4 de dicho protocolo: "Internet Protocol version 4" (IPv4).

Este protocolo se diseño prácticamente como un experimento, sin pensar en un despliegue ni siquiera cercano al actual, utilizando direcciones de 32 bits, con lo cual permite direccionar de forma única un máximo de 2^{32} (4.294.967.296) dispositivos. Estas direcciones son las que se denominan direcciones IPv4 públicas.

Una pequeña parte de este espacio de direcciones esta destinado por IETF (Internet Engineering Task Force, la organización responsable de la estandarización de los protocolos de Internet), para diversos servicios, como funciones de la red (multicast o multidifusión) y direcciones privadas (válidas sólo en el interior de las redes, pero no en Internet).

El despliegue inicial de Internet con IPv4 pasa por una fase inicial en la que se entregaban direcciones a cualquier persona o entidad que las solicitaba, sin mayores justificaciones.

En una segunda fase, se organiza una entidad IANA (Internet Assigned Numbers Authority), actualmente bajo el paraguas de ICANN (Internet Corporation for Assigned Names and Numbers), conjuntamente con los Registros Regionales de Internet (RIRs o Regional Internet Registers), que se ocupan de la asignación de estos recursos de numeración (direcciones IP).

En la actualidad, existen 5 RIRs, para las regiones de Europa y Oriente Medio (RIPE NCC), Norteamérica (ARIN), Asia Pacífico (APNIC), Latinoamérica y Caribe (LACNIC) y África (AfrinIC), que autogobiernan la gestión de los recursos públicos dentro de cada región por medio de políticas regionales establecidas por la propia comunidad (definida como cualquier individuo que desee participar en el proceso de desarrollo de políticas), así como los recursos de forma global (bajo el control de IANA, instruida por IETF), por medio de políticas globales (que han de alcanzar consenso con el mismo texto literal en las 5 regiones, para ser ratificadas por el consejo directivo de ICANN, de tal forma que IANA pueda aplicarlas).

El resultado de este proceso es que en la segunda fase antes indicada, se decide que las direcciones sean repartidas en bloques de 8 bits (los 8 bits superiores de las direcciones IPv4), transferidos a cada uno de los RIRs desde el almacenamiento central en IANA, para su gestión regional, según se vayan agotando los recursos de cada una de dichas regiones. Estos bloques, siguiendo la nomenclatura técnica, se denominan prefijos /8, y utilizables en Internet existen 220.

2.2. El Agotamiento de IPv4

En 1.992, el IETF se apercibe de la necesidad de “ampliar” el número de direcciones, teniendo en cuenta el inesperado crecimiento de Internet, dado que el número de direcciones disponibles no permitían siquiera una única dirección para cada habitante del planeta de aquel momento, y mucho menos direccionar varios dispositivos por cada uno de nosotros.

Ya no se trataba de conectar unos pocos ordenadores, sino cientos, miles o millones de aparatos de todo tipo, incluso no manejados por personas, sino por otras maquinas.

Como solución inmediata y transitoria para permitir el continuado crecimiento de Internet, se crea el mecanismo NAT (Network Address Translation), que en definitiva permite que cada red conectada a Internet (bien sea un usuario residencial o una organización de cualquier tipo), utilice una única dirección IPv4 pública en su punto de conexión a Internet (router o encaminador) y un numero determinado y limitado de direcciones privadas en la parte interna de dicha red. Para ello es necesario realizar una traducción de esas múltiples direcciones privadas a la única dirección pública disponible, lo que conlleva la perdida del paradigma básico de Internet, la conectividad extremo-a-extremo, con graves consecuencias para el desarrollo de la Red.

A pesar de esta solución, el continuado y explosivo crecimiento de Internet a llevado a un agotamiento de dicho espacio de direcciones en el almacenamiento central de IANA, que en el mes de Enero de 2.010 contaba con un 10% de las mismas, reduciéndose a final del verano al 5% y finalmente a tan solo menos del 2.7% a principio de Diciembre (concretamente 7 prefijos /8).

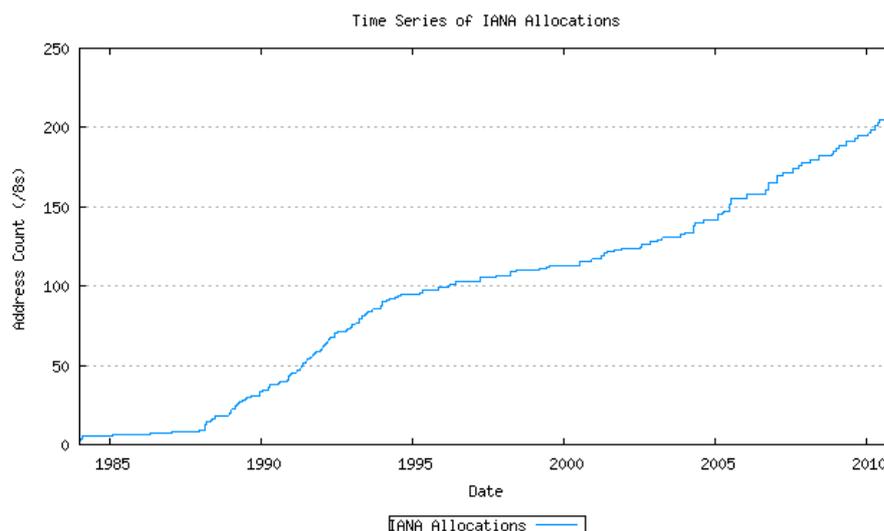


Figura 1: Distribución temporal de asignaciones /8 IPv4 (Fuente: IANA)

El **agotamiento final** de este recurso, se produce por una petición de nuevos bloques por parte de APNIC (concretamente 2 prefijos /8), en **Febrero de 2.011**. En ese momento, se reparten los últimos 5 prefijos /8 (pues así se ha acordado por medio de una política global) entregándose uno de ellos a cada una de las 5 regiones.

Las regiones de RIPE, ARIN y APNIC, previsiblemente, si mantienen el ritmo de demanda de direcciones IPv4 de los últimos años, agotarían sus remanentes en unos 6 u 8 meses, aunque es difícil de predecir, pues se puede producir cierta situación de “pánico” por parte de los proveedores de Internet (ISPs). LACNIC y AfriNIC, posiblemente tendrían recursos para unos 12 meses adicionales (aunque se podrían producir compras de empresas en dichas regiones por parte de multinacionales para obtener mas direcciones de este modo ciertamente poco ortodoxo, o incluso por medio de un “mercado gris” de direcciones, aún a pesar de estar en contra de las políticas que dicta la comunidad).

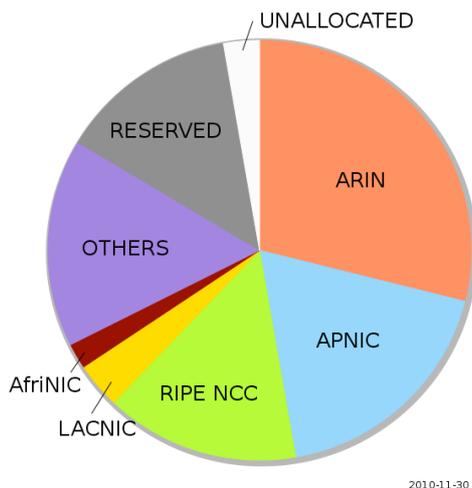


Figura 2: Distribución Actual de Direcciones IPv4 (Fuente: IANA)

2.3. ¿Qué es IPv6?

Casi al mismo tiempo que se produce el desarrollo de NAT, y en paralelo, el IETF inicia los trabajos para buscar una solución a más largo plazo (IPng, IP next generation) que, sin entrar en detalles, se concreta en la versión 6 del protocolo de Internet (Internet Protocol version 6, IPv6).

IPv6 utiliza 128 bits a diferencia de 32 que emplea IPv4, y por tanto permite un total de 2^{128} direcciones únicas, es decir en total 340.282.366.920.938.463.463.374.607.431.768.211.456.

En realidad, técnicamente hablando, esto implica que disponemos de 2^{64} (18.446.744.073.999.983.000) prefijos de 2^{64} direcciones cada uno, dado que cambiamos el paradigma y ya no entregamos a los usuarios direcciones únicas, sino prefijos para cada una de sus posibles subredes. Concretamente, cada usuario final (bien sea residencial o empresarial, de forma indistinta), recibo 65.535 subredes IPv6, es decir, un prefijo de 48 bits (/48).

Por supuesto, con IPv6, se restablece el paradigma de la conectividad extremo-a-extremo, lo que permite pensar entre otras cosas en “La Internet de las Cosas”. La expectativa es que no se agoten las direcciones IPv6 antes de los próximos 480 años, o dicho de otro modo, asumiendo una población de 7 mil millones de habitantes, podríamos abastecer trillones de planetas como la Tierra,

muchos más de los que la órbita solar podría absorber (que solo tiene capacidad para 3.250 planetas como la Tierra).

Es importante añadir que no hay otra solución mas que la transición a IPv6; no hay tiempo para ninguna otra medida. Esto es algo que no admite discusión bajo ningún punto de vista, ni técnico ni económico y así lo han confirmado gobiernos y organizaciones de todo tipo y en todo el mundo.

2.4. Estado de adopción de IPv6

El despliegue de IPv6 se inicio en el año 2.002, momento en el cual ya se podía considerar estandarizado en los aspectos básico que prácticamente lo equiparaban a IPv4.

En ese momento, la mayoría de los fabricantes de Sistemas Operativos ofrecían IPv6 en sus productos, al igual que los fabricantes de equipamiento de redes (encaminadores fundamentalmente), con diferentes grados de madurez y soporte técnico y/o comercial.

En ese mismo año se producen los primeros grandes despliegues en el mundo, siendo el caso mas relevante posiblemente el de NTT, que no sólo ofrecía IPv6 en sus redes “intercontinentales”, sino también decidía que era más viable utilizar IPv6 multicast (multidifusión), aún cuando hubiera que desplegarlo partiendo de cero, que IPv4 multicast para poder lanzar los servicios comerciales de IPTV.

La situación actual es que el 99% de los grandes carriers (los denominados “tier 1”), ofrecen IPv6, muchos de ellos desde hace varios años, en sus redes intercontinentales y en muchos casos regionales, mientras que sólo algunos proveedores de Internet nacionales (aunque es difícil de estimar, quizás un 20% en todo el mundo) proporcionan el servicio, y cuando lo proporcionan, muy pocos lo ofrecen en la “última milla”, salvo para clientes corporativos.

Esto es debido fundamentalmente a que los CPEs (Customer Premises Equipment, encaminador situado en las instalaciones del cliente), han sido los equipos con mayor demora en su introducción comercial, y especialmente los de gama baja, que son los que habitualmente suministran los ISPs a los clientes residenciales. Esta situación ha cambiado radicalmente en los últimos dos años.

Este es por ejemplo el caso Español, en el que el servicio esta disponible por parte de algunos ISPs, para clientes corporativos si solicitan su activación, y se trata de un servicio que no es publicitado y del cual los agentes comerciales suelen incluso desconocer todo tipo de detalles, mientras que por ejemplo hay casos cercanos y recientes (Francia), con despliegues de IPv6 en ISPs que tienen 5 millones de clientes, por no mencionar los casos de Holanda, Alemania, Austria, Suiza, Italia, Suecia, Eslovenia, Portugal, Reino Unido, Bélgica, Estados Unidos, Canadá, Japón, Corea del Sur, China, Australia, Nueva Zelanda, Indonesia, Malasia, Singapur, India, Costa Rica, Chile, Argentina, Brasil, Guatemala, México, Colombia, República Dominicana, Uruguay, Mauricio, Senegal, Sudáfrica y Egipto, entre

otros, que tienen ISPs con servicios comerciales de IPv6, en algunos casos desde hace varios años.

También existen numerosos ISPs realizando pilotos con diferentes números de usuarios, algunos de ellos muy importantes, como Comcast y T-Mobile.

Los proveedores de contenidos iniciaron sus primeros pasos en el año 2.006, anticipándose Google, que desde hace ya 3 años ofrece sus servicios con IPv6, a los que le han seguido FaceBook, Netflix, Yahoo, CNN y eBay entre otros. Del mismo modo diversos prensa online, radios y TV por Internet, por supuesto incluyendo YouTube, soportan IPv6.

Del mismo modo, algunos proveedores de “Content Delivery Networks” (CDNs o Redes Suministradoras de Contenidos), en las que se basan grandes proveedores de contenidos, como Limelight Networks ya ofrecen soporte de IPv6 y otros como Akamai, los han anunciado para los próximos meses. Similar es el caso de grandes proveedores de servicios de “hosting” y “housing”.

Por último, desde el punto de vista de servicios de infraestructura de la Red, el otro servicio que es importante, DNS (Domain Name System, “Sistema de Nombres de Dominio”), está preparado desde hace años en lo que se denomina la Raíz (root), así como en la mayoría de los TLDs (Top Level Domains o Dominios de Nivel Superior), es decir, en los dominios genéricos y mas del 65% de los países del mundo, con la notable excepción (si nos fijamos en los ccTLDs de mayor número de dominios registrados), de España (.es).

IANA, siguiendo indicaciones del IETF y de políticas globales, ha entregado a los RIR’s bloques IPv6 para su distribución a los ISPs de la región. La última entrega de un /12 para cada RIR, se produjo en el 2006, y se espera que esta entrega sea suficiente para muchos años.

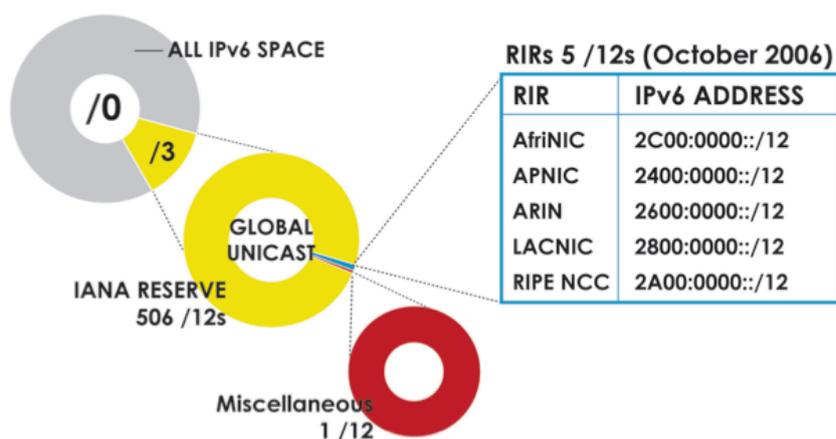


Figura 3: Distribución Actual de Direcciones IPv6 (Fuente: NRO)

A su vez, los RIRs entregan a los ISPs bloques con una longitud de prefijo de 32 bits o menores, según la necesidad justificada por el ISP; dado que los ISPs entregan prefijos de 48 bits a los usuarios, con un bloque /32, un ISP puede direccionar aproximadamente 65.535 clientes, con un /31 el doble, y así

sucesivamente. Para facilitar la uniformidad de las estadísticas, estas se realizan utilizando como base /32.

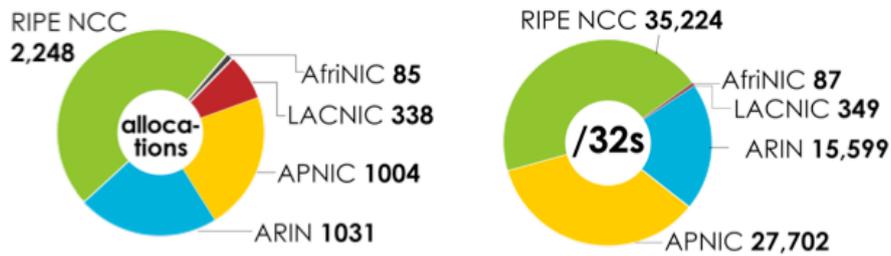


Figura 4: Asignaciones de IPv6 de RIRs a ISPs, Septiembre de 2010 (Fuente: NRO)

Otra cuestión bien distinta es el aspecto de que proporción del tráfico de Internet utiliza IPv6. La problemática estriba en que, por cuestiones técnicas inherentes al diseño del protocolo y su coexistencia con IPv4, cuando la última milla de ambos extremos de una determinada comunicación no tiene IPv6 habilitado, que es la situación mas habitual hoy en día, aunque los ISPs no estén dando servicio IPv6, entran en funcionamiento los denominados mecanismos de transición, algunos de los cuales son automáticos (o bien otros configurados por los usuarios). Es por ello que antes la pregunta a los grandes carriers que ya ofrecen servicio IPv6 de cuanto tráfico IPv6 tienen en sus redes, la respuesta suele estar entre el 3 y el 5%. Sin embargo, algunos estudios (6METER, RIPE55¹) demuestran que si se mide el tráfico IPv6 encapsulado IPv4 (el que se genera con los mecanismos de transición), que por otro lado no es nada fácil de medir, hay niveles de tráfico que llegan a superar el 35%. Este tráfico es fundamentalmente peer-to-peer, pero con la disponibilidad de contenidos en IPv6 (ejemplo, YouTube), también está creciendo de manera muy significativa el tráfico cliente-servidor.

Otro indicador del grado de despliegue por países de IPv6 es el denominado "Peering Router Status" (estado de pareado de encaminadores). Un mayor número de "peers" (pares) en un determinado país es indicativo de mayor intercambio de tráfico local entre proveedores de la misma. En la siguiente tabla se refleja el estado organizado por países; obsérvese la deficitaria situación Española.

Peers per Country

TLD	Name	Number	TLD	Name	Number	TLD	Name	Number
DE	Germany	46	DK	Denmark	4	EE	Estonia	1
NL	Netherlands, The	40	HU	Hungary	4	IN	India	1
US	United States	25	SE	Sweden	4	ID	Indonesia	1
GB	United Kingdom (Great Britain)	19	FI	Finland	3	JP	Japan	1
CH	Switzerland	17	PT	Portugal	2	MD	Moldova	1
IE	Ireland	9	RU	Russia	2	NO	Norway	1
IT	Italy	8	AU	Australia	1	PH	Philippines	1
FR	France	7	AT	Austria	1	ES	Spain	1
BE	Belgium	5	CN	China	1	VA	Vatican City	1
PL	Poland	5	HR	Croatia	1			
CA	Canada	4	CZ	Czech Republic	1			

Figura 5: Peering Router Status, Diciembre de 2010 (Fuente: SIXXS)

¹ <http://www.ripe.net/ripe/meetings/ripe-55/presentations/palet-v6.pdf>

Otro indicador del grado de despliegue viene dado por el número de ISPs que han recibido prefijos IPv6 (A de “allocated” en la tabla siguiente), y su comparativa con cuantos de ellos son visibles en la red (V de “visible” en la tabla), es decir cuantos de los ISPs que los han recibido realmente los están “anunciando” (el anuncio de un prefijo no necesariamente indica grado de uso o despliegue, sino tan sólo que se ha configurado el encaminador “principal” con ese prefijo). España ocupa la posición 25, con 54 prefijos, pero sin embargo, queda muy por detrás de otros países si se observa que de ellos sólo se anuncian 19 (y que, insistimos, además no implica que se estén usando) y una participación en el total de Internet de tan sólo el 0,29%.

IPv6 DFP's per country

Total number of countries: 159

Pos	Flag	Country	V	A	VP	Pos	Flag	Country	V	A	VP	Pos	Flag	Country	V	A	VP
1		United States	578	1618	8.70%	55		Asian Pacific	4	18	0.06%	109		Cote d'Ivoire	1	2	0.02%
2		Germany	266	421	4.00%	56		Kenia	3	16	0.05%	110		Morocco	0	2	0.00%
3		United Kingdom (Great Britain)	140	302	2.11%	57		Venezuela	4	16	0.06%	111		International	2	2	0.03%
4		Japan	97	260	1.46%	58		Latvia	7	15	0.11%	112		Georgia	0	2	0.00%
5		Australia	68	254	1.02%	59		Uruguay	8	15	0.12%	113		Kazakhstan	0	2	0.00%
6		Netherlands, The	161	247	2.42%	60		Equador	4	13	0.06%	114		Syria	0	2	0.00%
7		Brazil	66	236	0.99%	61		Colombia	4	13	0.06%	115		Bahamas	0	2	0.00%
8		Russia	94	203	1.42%	62		Lithuania	6	12	0.09%	116		Czechoslovakia	1	2	0.02%
9		France	85	157	1.28%	63		Iceland	7	12	0.11%	117		Sudan	1	2	0.02%
10		Switzerland	77	136	1.16%	64		Nepal	2	10	0.03%	118		Macau	1	2	0.02%
11		China	26	135	0.39%	65		Serbia	5	10	0.08%	119		Monaco	1	2	0.02%
12		Canada	52	132	0.78%	66		Israel	4	10	0.06%	120		Uzbekistan	1	2	0.02%
13		Sweden	64	118	0.96%	67		Sri Lanka	2	9	0.03%	121		Bermuda	0	2	0.00%
14		Italy	50	112	0.75%	68		Bosnia and Herzegovina	6	9	0.09%	122		Bhutan	1	2	0.02%
15		Czech Republic	79	103	1.19%	69		Fiji	3	9	0.05%	123		Algeria	0	2	0.00%
16		Indonesia	38	102	0.57%	70		Armenia	2	9	0.03%	124		Seychelles	0	2	0.00%
17		Poland	59	102	0.89%	71		Croatia	4	9	0.06%	125		Nicaragua	0	2	0.00%
18		Austria	66	98	0.99%	72		Nederlandse Antillen	3	8	0.05%	126		Federated States of Micronesia	0	1	0.00%
19		Norway	45	96	0.68%	73		Peru	1	8	0.02%	127		Mozambique	0	1	0.00%
20		New Zealand	29	94	0.44%	74		Cyprus	2	8	0.03%	128		Cook Islands	0	1	0.00%
21		Korea	9	79	0.14%	75		Mauritius	2	8	0.03%	129		El Salvador	1	1	0.02%
22		India	14	70	0.21%	76		Egypt	2	7	0.03%	130		Namibia	0	1	0.00%
23		Hong Kong	23	62	0.35%	77		Moldova	4	7	0.06%	131		Maldives	1	1	0.02%
24		Denmark	28	59	0.42%	78		Lebanon	2	7	0.03%	132		United States Virgin Islands	1	1	0.02%
25		Spain	19	54	0.29%	79		Nigeria	0	7	0.00%	133		Sierra Leone	0	1	0.00%
26		Singapore	15	54	0.23%	80		Puerto Rico	1	7	0.02%	134		Angola	0	1	0.00%
27		Finland	35	54	0.53%	81		Malta	3	7	0.05%	135		Swaziland	0	1	0.00%
28		Belgium	21	54	0.32%	82		Jordan	2	7	0.03%	136		Palau	0	1	0.00%
29		Malaysia	16	49	0.24%	83		Costa Rica	2	6	0.03%	137		Andorra	0	1	0.00%
30		Ukraine	23	48	0.35%	84		Tanzania	3	6	0.05%	138		Belize	0	1	0.00%
31		Taiwan	16	46	0.24%	85		United Arab Emirates	2	5	0.03%	139		Qatar	1	1	0.02%
32		South Africa	18	40	0.27%	86		Cuba	3	5	0.05%	140		Madagascar	0	1	0.00%
33		Ireland	27	39	0.41%	87		Rwanda	0	5	0.00%	141		Falkland Islands	0	1	0.00%
34		Slovenia	24	38	0.36%	88		Uganda	0	5	0.00%	142		Democratic Republic of the Congo	0	1	0.00%
35		Philippines	7	36	0.11%	89		Trinidad and Tobago	1	5	0.02%	143		Vatican City	1	1	0.02%
36		Mexico	9	35	0.14%	90		Dominican Republic	2	5	0.03%	144		Yemen	0	1	0.00%
37		Thailand	14	35	0.21%	91		Belarus	2	5	0.03%	145		Malawi	0	1	0.00%
38		Argentina	12	34	0.18%	92		Bahrain	0	4	0.00%	146		Gibraltar	0	1	0.00%
39		Vietnam	3	30	0.05%	93		Panama	0	4	0.00%	147		Greenland	0	1	0.00%
40		Turkey	4	29	0.06%	94		Bolivia	0	4	0.00%	148		Republic of Djibouti	0	1	0.00%
41		Iran	11	29	0.17%	95		Kuwait	0	4	0.00%	149		Mali	0	1	0.00%
42		Hungary	13	28	0.20%	96		Guatemala	0	4	0.00%	150		Jamaica	0	1	0.00%
43		Europe	13	28	0.20%	97		Ghana	2	4	0.03%	151		Honduras	1	1	0.02%
44		Portugal	13	27	0.20%	98		Haiti	1	3	0.02%	152		Cameroon	0	1	0.00%
45		Romania	15	25	0.23%	99		Republic of Macedonia	1	3	0.02%	153		Kyrgyzstan	0	1	0.00%
46		Chile	7	22	0.11%	100		Papua New Guinea	0	3	0.00%	154		Senegal	1	1	0.02%
47		Bangladesh	1	21	0.02%	101		Oman	1	3	0.02%	155		Faroe Islands	0	1	0.00%
48		Pakistan	5	21	0.08%	102		Samoa	1	3	0.02%	156		Tonga	0	1	0.00%
49		Slovakia	12	21	0.18%	103		Zambia	1	3	0.02%	157		Solomon Islands	0	1	0.00%
50		Luxembourg	11	20	0.17%	104		Zimbabwe	0	2	0.00%	158		Benin	0	1	0.00%
51		Greece	4	20	0.06%	105		Paraguay	0	2	0.00%	159		Vanuatu	0	1	0.00%
52		Estonia	10	19	0.15%	106		Fuerstentum Liechtenstein	2	2	0.03%						
53		Bulgaria	10	19	0.15%	107		Tunisia	1	2	0.02%						
54		Saudi Arabia	8	18	0.12%	108		Brunei	0	2	0.00%						

V: Visible: Number of Visible Prefixes for this country.
A: Allocated: Number of Allocated Prefixes for this country (excludes returned prefixes).
VP: Visible Percentage: Percentage of visible prefixes against global number of allocated prefixes.

Figura 6: Visibilidad de Prefijos, Diciembre de 2.010 (Fuente: SIXXS)

RIPE elabora desde una clasificación del nivel de penetración de IPv6 en los países de la región, asignando entre 0 y 4 “estrellas” a los ISPs de cada país, según el cual, España estaría aproximadamente en el lugar undécimo empezando por el final (en un total de unos 70 países).

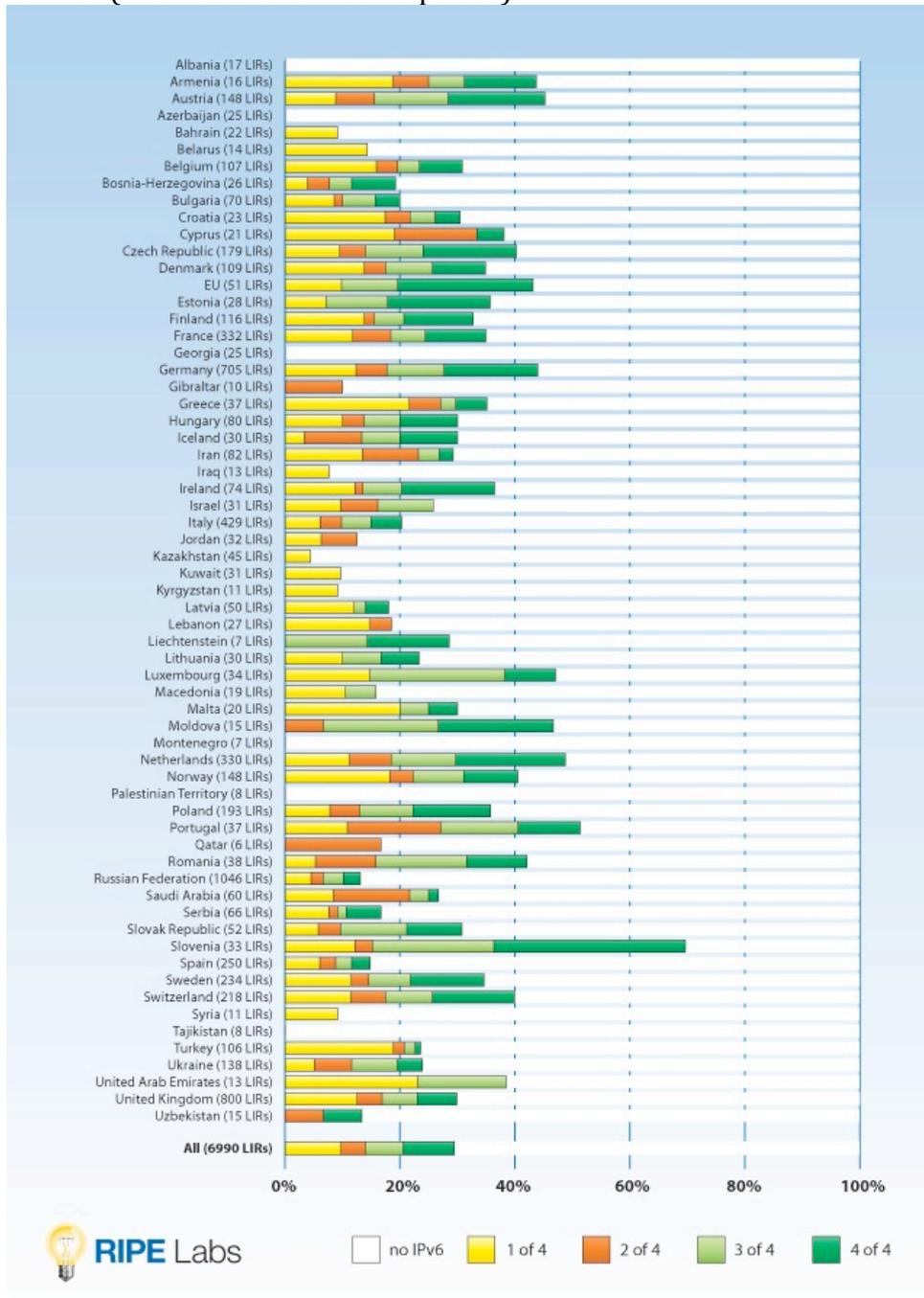


Figura 7: IPv6 Ripeness, Julio de 2.010 (Fuente: RIPE)

Para finalizar, cabe mencionar que existen muchos otros procedimientos para medir el grado de despliegue o penetración de IPv6 y en todos los casos tienen pros y contras, con lo que siempre es preciso ponderar esta información.

2.5. *¿Porqué no se despliega IPv6 con mayor rapidez?*

En las secciones anteriores hemos comprobado que la infraestructura de las grandes redes esta preparada, y que ya se genera tráfico. Hemos de añadir que dicho tráfico se incrementa rápidamente, dado que todos los Sistemas Operativos tienen IPv6 activado por defecto (con la excepción de RIM/BlackBerry), y por definición de los estándares, cuando un servicio (ya sea cliente en caso de peer-to-peer o servidor en caso de cliente-servidor), esta habilitado tanto con IPv4 como con IPv6, tiene preferencia utilizar IPv6. Es decir, el tráfico IPv6 va ganando terreno paulatinamente al tráfico IPv4, en teoría de una forma transparente para los usuarios, aún cuando los ISPs no desplieguen IPv6.

Esto es posible porque los mecanismos de transición cumplen su función, sin embargo, y especialmente los automáticos, no son perfectos y generan problemas a los usuarios y a los proveedores de contenidos. Se generan retardos, pérdida de calidad en los accesos a los contenidos, o incluso en ocasiones la total imposibilidad de acceder a algunos contenidos.

Obviamente la solución no es desactivar IPv6, sino dar los pasos que hace años ya debieran haberse dado, para que se despliegue IPv6 de una forma más rápida. A mayor velocidad del despliegue de IPv6, menos problemas para los proveedores de contenidos y usuarios.

El desconocimiento de IPv6 es precisamente el factor principal por el que no haya sido desplegado con mayor celeridad. Habitualmente se tiene la percepción que desplegar IPv6 supone un coste muy importante, y la realidad es que si se planifica adecuadamente y con anticipación, no es el caso. Por tanto, es obvio que es importante anticiparse y evitar dejarlo para el último momento, pues en ese caso si que pasaría como fue el caso de los “últimos “ que acometieron la actualización de aplicaciones que sufrían del “efecto año 2.000” y al resolverlo de la noche a la mañana, lo pagaron mucho más caro.

Precisamente se ha comparado el caso de la transición a IPv6 con el “efecto año 2.000”, con la gran diferencia que éste tenía desde el primero momento una fecha concreta y la misma para todo el mundo, y no es el caso de IPv6, que depende de muchos factores (ritmo de crecimiento de Internet, situación económica, etc.). De hecho, aunque algunas regiones podrían tener direcciones disponibles durante más tiempo, para dichas regiones puede ser peor, por el riesgo de quedarse ligeramente “desconectadas” del resto del mundo que ya este haciendo la transición a IPv6.

Concretando un poco más, dado que la mayoría de los equipos de las redes de “core” de los ISPs y las organizaciones públicas y privadas tienen antigüedades inferiores a 4-5 años, ya tienen soporte IPv6. En muchos casos es tan sólo cuestión de activarlo y configurarlo. En algunos casos hace falta actualizar el software (lo que puede requerir una licencia).

Y precisamente el mayor coste se refiere a la formación de los ingenieros que gestionan dichas redes y equipamiento. Recientemente se ha evaluado que se requiere formar a unos 20 millones de ingenieros en todo el mundo en los próximos dos años para una correcta transición a IPv6.

Como ya hemos indicado anteriormente, el otro coste importante es la necesidad de reemplazar los CPEs. La disponibilidad de los mismos con un adecuado soporte de IPv6 se ha demorado comparado con el resto de los equipos de la red, precisamente porque los fabricantes no han sido “motivados” por falta de demanda de los mismos por los ISPs.

Sin embargo, en una primera fase, no es estrictamente necesario reemplazar los CPEs, pues si los ISPs despliegan mecanismos de transición en lugar de que los usuarios dependan de los mecanismos de transición automáticos, se alivian los defectos que generan estos últimos. De hecho, se espera que la mayoría de los ISPs suministren CPEs con IPv6 a nuevos usuarios, pero los antiguos sean reemplazados con ocasión de otros cambios tecnológicos (por ejemplo provisión de servicios de IPTV, mayores anchos de banda, otras tecnologías de conexión a Internet, etc.).

Otro de los motivos aducidos para evitar la transición a IPv6 por parte de los ISPs ha sido la falta de contenidos, lo cual ha cambiado rápidamente desde el momento que Google comenzó a ofrecer sus servicios con el nuevo protocolo, y obviamente ello impacta en la competencia que se ve obligada a reaccionar.

Además, los ISPs indican que no hay “caso de negocio”, que IPv6 no es atractivo desde el punto de vista económico. De nuevo es una falsa percepción, por desconocimiento no solo de IPv6, sino de la inevitable situación de agotamiento de IPv4. Más adelante en este documento se estudian algunas de las posibilidades de negocio con IPv6.

Por último, no completar la transición a IPv6 a la mayor brevedad, implicaría la necesidad de utilizar tecnologías de traducción en las redes de banda ancha, lo que se ha dado en llamar “Carrier Grade NAT”, que supondría no sólo grandes costes (en torno a un millón de dólares por cada dispositivo, sin que aún se haya determinado cuantos miles de usuarios podrá atender), sino además perpetuar en la red la existencia de NAT, dificultando el desarrollo de aplicaciones extremo-a-extremo.

No moverse a IPv6 tiene graves consecuencias para la pérdida de negocio para los ISPs. Es obvio que algunos irán por delante, y los rezagados perderán cuota de mercado. Pero es más grave para la Sociedad de la Información, pues los usuarios se ven abocados a una nueva brecha digital, algo así como una “doble Internet” en la que no se puede garantizar a todos los ciudadanos el acceso a todos los contenidos de una forma adecuada, ni siquiera que unos usuarios puedan conectarse con otros, y evitarlo es posible y sin grandes inversiones.

2.6. *Iniciativas en el mundo*

Desde el punto de vista gubernamental, la primera iniciativa surge del Gobierno de Japón, concretamente en Septiembre de 2.000, cuando el Primer Ministro (Mori) identifica públicamente a IPv6 como parte crítica de la iniciativa eJapan 2.005, proporcionando incentivos fiscales a las compañías que integren soporte de IPv6.

La siguiente iniciativa, surge en España en Enero de 2.001 con la convocatoria de un evento internacional para la divulgación de IPv6², con la participación del Ministerio de Ciencia y Tecnología y la Comisión Europea. En parte como resultado de dicho evento, el Comisario Europeo para Empresas y Sociedad de la Información, Erkki Liikanen, convoca la creación del IPv6 Task Force Europeo³ (Grupo de Trabajo de IPv6 Europeo), con el objetivo de preparar la hoja de ruta para la adopción de IPv6 y su despliegue a gran escala en el 2.005.

Como resultado de dichos trabajos, se publican varios documentos, incluyendo, en Febrero de 2.002, el informe final⁴, que la Comisión Europea hace suyo pocos días después, a través de un Comunicado de la Comisión al Consejo y el Parlamento Europeo, marcando las prioridades para la transición a IPv6⁵, refrendado al mes siguiente por las Conclusiones Presidenciales del Consejo Europeo reunido en Barcelona⁶, con el objetivo del despliegue en la Unión Europea hacia el 2.005.

Ante la falta de acción por parte de la mayoría de los Estados Miembros, en Mayo de 2.008, la Comisión Europea lanza un nuevo Comunicado⁷ al Parlamento Europeo, el Consejo, el Comité Europeo Económico y Social y el Comité de las Regiones, para reforzar la importancia de la situación y lograr el objetivo de un despliegue de al menos un 25% para el 2.010.

Como consecuencia de la importante acción de la Comisión Europea en el año 2.002, se convoca la creación de IPv6 Task Forces no sólo en cada país de Europa, sino en el resto del mundo. Concretamente en España se crea el primer Task Force nacional el 16 de Mayo de 2.002, auspiciado por el Ministerio de Ciencia y Tecnología. Igualmente la mayoría de los Task Forces de otros países e incluso regiones del mundo, cuentan con la participación de los respectivos gobiernos.

Sin embargo, en pocos casos estos Grupos de Trabajo han tenido resultados importantes que impliquen el avance del despliegue de IPv6 en sus respectivos territorios, que era su objetivo fundamental, salvo en países concretos donde la implicación gubernamental era suficientemente fuerte que ha

² <http://www.consulintel.es/Html/ForoIPv6/madridgishome.htm>

³ <http://www.eu.ipv6tf.org/in/i-index.php>

⁴ <http://www.eu.ipv6tf.org/PublicDocuments/IPv6TF-Report.pdf>

⁵ ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/ipv6-communication_en.pdf

⁶ http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/71025.pdf

⁷ http://ec.europa.eu/information_society/policy/ipv6/docs/european_day/communication_final_27052008_en.pdf

conllevado la organización de entidades o grupos de trabajo específicos dentro del propio gobierno, organizados a modo de Oficinas Técnicas (comparables al caso del desarrollo de la TDT en España), que han desarrollado incluso legislaciones y/o reglamentaciones para garantizar el avance del despliegue y su seguimiento.

Algunos ejemplos concretos de países donde dichas “Oficinas Técnicas de IPv6” han obtenido resultados concretos son: Japón, Corea del Sur, Taiwán, China, India, Indonesia, Malasia, Singapur, Australia, Tailandia, Vietnam, Pakistán, Francia, Austria, Alemania, República Checa, Irlanda, Reino Unido, Luxemburgo, Eslovenia, Estados Unidos de América, Canadá, Cuba, Chile, Egipto y Kenia.

Son muy relevantes las decisiones acerca de IPv6 de la CEPAL (Comisión Económica para América Latina), concretamente por medio de eLAC2010 y eLAC2015, y de forma similar en Asia Pacífico, APEC (Asia Pacific Economic Cooperation), en ambos casos con resoluciones de Noviembre de 2.010.

Importante también el informe elaborado por la OCDE, de Junio de 2.008, Encuentro Ministerial acerca del Futuro de la Economía de Internet: “Consideraciones Económicas en la Gestión de IPv4 y el Despliegue de IPv6”⁸.

Igualmente relevantes la adjudicación en el mes de Diciembre de 2.010 del contrato de despliegue de IPv6 en Andorra y la promulgación en Colombia de una resolución en Enero de 2.011 para regular el régimen de adopción de IPv6.

Véase el Anexo I, para información más detallada de iniciativas en todo el mundo.

2.7. Acciones gubernamentales

En general, los gobiernos no están imponiendo a las empresas privadas la adopción de IPv6. Sin embargo, es obvio que dado que las entidades públicas tienen la obligación de gestionar adecuadamente los recursos públicos, ello implica no invertir en adquisiciones (tanto de hardware, software, servicios, comunicaciones, etc.), de forma innecesaria. Es decir, las entidades públicas no deberían de estar adquiriendo, desde hace años, nada que no garantice el soporte completo de IPv6, pues en caso contrario, habría que repetir dichas inversiones en plazos muy inferiores al de sus amortizaciones.

Ello implica que si hay que obligar a la industria que desee participar en concursos públicos, que ofrezca sus productos con soporte IPv6, y por tanto, indirectamente, es difícil pensar que dicha industria tenga una oferta diferente para clientes corporativos y residenciales que no sean entidades públicas. Por tanto, indirectamente se fuerza a la industria a la transición de todos sus productos y servicios a IPv6.

⁸ <http://www.oecd.org/dataoecd/7/1/40605942.pdf>

Se presupone que los gobiernos han de ser agnósticos a las tecnologías, sin embargo, no pueden ser indiferentes al devenir del resto del mundo y por ende de Internet, para el continuado desarrollo de la Banda Ancha y la Sociedad de la Información y los altísimos costes económicos y otras muchas implicaciones que ello conllevaría para el país en cuestión, como el incremento de la Brecha Digital que se produciría en caso de ignorar esta situación.

Además, los reguladores tienen que contemplar en algunos casos aspectos tecnológicos. Por ejemplo, un regulador tiene que decidir si la habilitación de servicios, por ejemplo en el caso de los telefónicos, como Voz sobre IP, tiene que realizarse tanto con protocolo IPv4 (al menos por el momento), como con IPv6, garantizando así la interconexión no sólo nacional, sino regional e internacional. Igualmente se podrían contemplar otros servicios que requieren asegurar aspectos de conexión a Internet, como podría ser la Televisión Digital Terrestre (TDT), telefonía celular, enlaces satelitales, etc.

Los gobiernos también tienen una misión de protección de los consumidores que no hay que menospreciar, y dado que el ciudadano, en general, utiliza Internet, sin conocer los detalles técnicos, es preciso que se regulen los mecanismos para su defensa.

Hay que destacar que la consideración de “soporte de IPv6” es muy relativa. Si bien se puede acudir a las especificaciones del IETF, es preciso de cara a la preparación de los concursos y contratos públicos, al igual que sería el caso para, por ejemplo, el suministro de servicios de acceso a Internet, el adecuado estudio caso a caso, en función de que servicios se pretenden facilitar para determinar “que es el soporte de IPv6” en cada uno de esos casos.

Podríamos estudiar algunos ejemplos concretos de lo que se ha hecho en determinados países a modo de “casos de estudio”, sin embargo, dado que en la mayoría de ellos se han llevado a cabo aproximadamente las mismas acciones, mencionaremos los más comunes:

- 2.7.1. Incentivos fiscales para la adopción de IPv6.
- 2.7.2. Regulaciones para garantizar la importación de equipos, software, servicios que soporten IPv6.
- 2.7.3. Las licitaciones públicas de todo tipo de productos, bien sean aplicaciones, equipos o servicios tienen que soportar IPv6. Por ejemplo:
 - a. Los sitios web, servidores de correo electrónico, y cualesquiera otros servicios de la administración pública visibles desde Internet, tienen que soportar IPv6.
 - b. Las líneas de comunicaciones de la administración pública han de soportar IPv6.
 - c. Los sistemas operativos de clientes y servidores utilizados por las entidades públicas y funcionarios, han de soportar IPv6.

- d. El equipamiento (encaminadores, conmutadores, otros) de las redes de las entidades públicas, ha de soportar IPv6, incluyendo los sistemas de gestión.
 - e. Si se utiliza IP para sistemas de automatización de edificios (domótica), video-vigilancia, gestión remota, control de acceso/horarios de personal, etc., es preciso que soporten IPv6.
 - f. Igualmente en el caso de infraestructuras similares no situadas en edificios, sino carreteras, vías férreas, tráfico marítimo y aéreo, etc.
 - g. Todo lo mencionado anteriormente es también válido para las escuelas, universidades y redes académicas, tanto si son públicas como privadas o concertadas, dado que generalmente existen redes que las interconectan entre sí y con las redes académicas y de investigación de otros países (NRENs).
 - h. Cualesquiera desarrollos e inversiones que se produzcan tendentes al desarrollo de la Sociedad de la Información y Tecnologías de la Información y las Telecomunicaciones, tienen que contemplar el despliegue y uso de IPv6.
 - i. Los programas de subvenciones y otros tipos de financiación pública de Investigación, Desarrollo, Innovación y similares, han de exigir el uso de IPv6.
 - j. Etc.
- 2.7.4. Los planes de educación tienen que incorporar los aspectos relacionados con la enseñanza de IPv6.
- 2.7.5. Aspectos relacionados con el regulador, y no solo de Telecomunicaciones (interconexiones de VoIP, TDT), sino posiblemente aquellos que se ocupan de la regulación con “utilities”, dado que la gestión de los recursos como energía, gas, agua, etc., es cada vez más crítica y requiere que los sistemas de control estén sujetos a medidas mas granulares, y por tanto se hace preciso el uso de millones de sensores y actuadores que utilizan IPv6.
- 2.7.6. Para garantizar el desarrollo de la Sociedad de la Información y reducir la Brecha Digital, en los servicios de banda ancha (tanto fija como celular) se entregaran prefijos de direcciones estáticas a los usuarios finales (tanto residenciales como corporativos), con una longitud máxima de 48 bits (/48), aunque se podrán entregar prefijos mas cortos (es decir un mayor número de subredes/direcciones) si así lo justificara el usuario, y por tanto, se evitará el uso de NAT con IPv6.
- 2.7.7. Las agencias relacionadas con la seguridad en Internet, tendrán en cuenta los aspectos relativos a IPv6.
- 2.7.8. Campañas de concienciación ciudadana. Los usuarios deben exigir a sus proveedores de productos y servicios, el soporte de IPv6, para garantizar que no adquieren productos obsoletos.

3. Oficina Técnica de IPv6 en España

Teniendo en cuenta el estado del arte y la situación de IPv6 en España, así como las acciones llevadas a cabo por organizaciones internacionales y Gobiernos de otros países, se hace necesaria la creación de una Oficina Técnica, en la que participen representantes de los diversos Ministerios implicados en la transición a IPv6, un experto en los diversos aspectos relacionados con la transición (estandarización, formación, regulación, consultoría, despliegue), así como algunos representantes de los diferentes sectores privados implicados.

Esta Oficina Técnica sería la responsable de elaborar un plan de acción, incluyendo al menos los siguientes aspectos:

- Recomendaciones de regulación.
- Seguimiento de la estandarización.
- Documentación precisa para los diversos implicados.
- Planes y aplicaciones de formación.
- Campaña de Comunicación/divulgación.
- Colaboración internacional.
- Coordinación del sector y agentes implicados.
- Seguimiento de los resultados del plan de acción.
- Página web que contenga todos los aspectos del plan de acción, reglamentos, documentos, enlaces, campaña de comunicación, resultados del plan de acción, etc.

Los detalles de la Oficina Técnica se documentan en un informe separado.

4. Innovación y Negocio con IPv6

IPv6 no es tan diferente de IPv4. De hecho, lo más importante es el número casi ilimitado de direcciones.

Sin embargo, este pequeño detalle, permite que no sea preciso el uso de NAT, y por tanto se permiten las comunicaciones reales extremo a extremo, e incluso la seguridad en las mismas, es decir, seguridad extremo-a-extremo.

Por otro lado, el elevado número de direcciones que se entregan a los usuarios (incluso usuarios residenciales), permite que estas sean estáticas, y por tanto que la comunicación desde el exterior de las redes hasta el interior de las mismas también sea factible.

No realizar la transición a IPv6 supone importantes trabas para el crecimiento de la Sociedad de la Información y el despliegue de la Banda Ancha, y sobretodo, una importante limitación a la innovación en Internet, debido al uso extensivo de NAT, que se acrecentaría incluso a varios niveles e implicaría también la disminución de la seguridad en la red, y el incremento de la dificultad de su gestión y monitorización.

En cambio, el despliegue de IPv6 es el habilitador de la innovación que se requiere en la red, dado que permite recuperar su paradigma inicial de comunicación segura extremo-a-extremo.

IPv6 disminuye drásticamente el coste del desarrollo de aplicaciones, tanto por el hecho de no utilizarse NAT, como por otras características como la autoconfiguración y la extensibilidad del protocolo. Tal como ha sido indicado en varias ocasiones por los creadores de Skype, NAT supone importantes costes de gestión y complica y encarece el desarrollo de aplicaciones, de hecho el 80% de los costes de la creación y mantenimiento de Skype son a causa de NAT, no de la aplicación en si misma.

Por si esto no fuera suficiente, el despliegue de IPv6 genera nuevos puestos de trabajo, dado que se requieren más ingenieros cualificados e indirectamente programadores con la capacidad de crear nuevas aplicaciones y servicios en la red, que también conllevan nuevos puestos de trabajo y el crecimiento económico.

No se trata de un crecimiento económico tan solo a corto plazo, sino también a medio/largo, pues el número de direcciones permite esa innovación durante decenas de años.

Se trata de un círculo: El despliegue de Banda Ancha requiere IPv6. El despliegue de IPv6 permite nuevos servicios y aplicaciones. Nuevos servicios y aplicaciones requieren el crecimiento de la Banda Ancha a usuarios existentes y hacen atractiva la conexión a Internet de Banda Ancha no sólo para nuevos usuarios, sino también para todo tipo de dispositivos que hasta ahora ni habíamos pensado conectar a la Red. Es la "Internet de las Cosas".

Puede parecer que todo esto es posible hacerse con IPv4, y ello es innegable desde un punto de vista técnico, pero lograr el crecimiento de las redes de Banda Ancha y el continuado desarrollo de nuevas aplicaciones y servicios sería tan costoso y complejo, una vez agotado dicho protocolo, que lo haría inviable (múltiples niveles de NAT, casi-imposibilidad de gestión de las redes, etc.).

Veamos algunos ejemplos.

4.1. Sensores y actuadores

Los sensores y actuadores son dispositivos que se han incorporado recientemente al mundo IP, pues anteriormente utilizaban protocolos propietarios.

IETF ha desarrollado un protocolo, que tan sólo utiliza IPv6 (no IPv4), por el ahorro energético que supone, denominado 6LOWPAN, que permite que diminutos sensores y actuadores, sin conexión a red eléctrica, utilicen comunicaciones inalámbricas, mediante IPv6, con un consumo tan reducido que las baterías pueden durar varios años, o incluso recargarse automáticamente con la luz ambiente por medio de pequeñas micro-células solares (inferiores al tamaño de una uña), por medio del movimiento, etc.

Obviamente el uso de IPv6 no sólo es debido al menor consumo eléctrico, sino también a las características de autoconfiguración, que evitan la necesidad que estos sensores y actuadores tengan que ser configurados manualmente o por medio de servidores, por el número de direcciones, y por supuesto por la posibilidad de utilizar seguridad extremo-a-extremo.

Sin pecar de ficción se puede llegar a pensar que en un futuro próximo todos los “objetos” de nuestro alrededor, desde ropa, hasta edificios, tengan un sensor en cada uno de sus elementos (termostatos, ladrillos, grifos, válvulas de gas, etc.), por cuestiones de seguridad, control energético y otras muchas que ni cabe imaginar aún.

4.2. Gestión de “utilities” (SmartGrids)

Uno de los graves problemas a los que nos enfrentamos es no sólo el ahorro energético, sino el adecuado aprovechamiento de todas las fuentes de energía, y especialmente las renovables.

Fuentes renovables como la solar y eólica, aportan energía a la red eléctrica de un modo no “constante” y ello puede suponer picos en la red, que en algunos casos pueden incluso llegar a dañarla.

Cuando las fuentes de energía en lugar de provenir de unas pocas centrales de producción proviene de miles de puntos de la red, se hace indispensable un control muy granular y totalmente automatizado.

Además, se hace preciso también monitorizar continuamente los consumos en cada punto de la red, por lo que la tendencia es a sustituir los contadores por dispositivos totalmente automatizados, que bien con tecnologías inalámbricas o bien a través de la propia red eléctrica, o bien utilizando la Banda Ancha, envían datos a la red, que también pueden ser utilizados por los usuarios y dispositivos de, por ejemplo el hogar o la industria, para facilitar los ahorros energéticos, consumir cuando la energía es mas barata, etc.

Ya se están produciendo despliegues de IPv6 en varias redes eléctricas del mundo para obtener estos beneficios.

Esto también es aplicable en gran medida a otros tipos de redes no sólo de energía eléctrica, sino de aprovisionamiento de gas, agua, etc.

4.3. Domótica/Inmótica

La domótica y tecnologías afines o asociadas han estado presentes desde hace años, aunque no han logrado una buena implantación comercial.

Una de las razones por las que esto no ha ocurrido ha sido sin duda que estas tecnologías no han estado fuertemente ligadas a Internet, sino que se utilizaban otros medios de conexión, como módems, enlaces de radio telefonía celular, etc. El caso de las centrales de alarmas es un buen ejemplo.

La causa por la que no se ha producido dicha integración con Internet de éstas tecnologías ha sido precisamente la falta de conectividad extremo-a-extremo, es decir la existencia de NAT en Internet.

Dado que IPv6 no utiliza NAT, al disponer de un número casi ilimitado de direcciones, se convierte en la oportunidad para integrar estas tecnologías con Internet.

Entre los campos en los que la domótica puede aplicarse con IPv6 podemos mencionar como ejemplos su uso en viviendas, oficinas, industrias, salud/telemedicina, cuidado de enfermos y ancianos y seguridad.

4.4. Intelligent Transport Systems

Desde hace varios años, los fabricantes de automóviles han apostado por unificar los centenares de protocolos de comunicación entre los diferentes dispositivos del interior de los vehículos.

Una de las acciones que se realizaron en Europa fue la creación de un proyecto en el que participaba Renault, en el que se decidió utilizar IPv6 para dicha unificación de protocolos y no sólo en el interior del vehículo, sino también para la comunicación con el exterior y vehículo a vehículo. Ello permite tal y como se demostró en este proyecto, no sólo servicios de información y entretenimiento, sino también incrementar la seguridad vial y por tanto salvar vidas, gestión automática de accidentes, supervisión del tráfico y del estado de las carreteras, etc.

Hay otros ejemplos similares en Japón. Es lo que se denomina ITS (Intelligent Transport Systems) y se creó una asociación “Car-to-Car Communications Consortium”, en la que participan prácticamente todos los fabricantes de vehículos del mundo, que adoptó IPv6 como el protocolo unificado para todo este tipo de servicios.

4.5. Monitorización remota y Video-vigilancia

Del mismo modo que antes hablábamos de domótica, los sistemas de monitorización remota y video-vigilancia de edificios, viviendas, vías férreas, carreteras, etc., son cada vez más necesarios.

Piénsese por ejemplo en el número de sensores que se sitúan en una vía del AVE, o el número de sensores y actuadores en cualquiera de los telescopios que generalmente están en lugares “fácilmente” accesibles y sin embargo tienen que ser utilizados por científicos de todo el mundo.

4.6. Comunicaciones Máquina-a-Máquina (MxM)

Internet conecta cada vez más máquinas que personas.

Desde hace algunos años, existen numerosos dispositivos en el mercado que permiten que aquellos antiguos puertos serie, por ejemplo en centralitas telefónicas, balanzas de supermercados, centrales de detección de incendios o alarmas, de forma transparente obtengan conectividad IP, bien Ethernet o bien Wireless.

Esta tendencia, que inicialmente eran “dispositivos añadidos” se está convirtiendo en una realidad para los fabricantes de todos estos dispositivos y cada vez es más habitual que quienes se conectan no sean personas a esas centralitas telefónicas para su gestión, sino otras máquinas para realizar una tarea que puede ser perfectamente automatizada.

De nuevo, es imperiosa la necesidad de direcciones suficientes y éstas sólo pueden ser proporcionadas por IPv6.

4.7. Redes Móviles 4G (LTE)

La nueva generación de telefonía celular, LTE (“Long Term Evolution”, frecuentemente denominada 4G) se basa exclusivamente en IPv6.

Aunque ya lo hemos mencionado anteriormente, el desarrollo de aplicaciones que funcionen a través de NAT es muy complejo y caro, al igual que la gestión de las redes donde existe NAT.

Pero además, NAT tiene otro gran inconveniente que es muy dañino para las redes móviles. El uso de NAT implica que se tengan que enviar cada 30 segundos unos paquetes de denominados “keepalive”, para indicar a los NAT que se están utilizando recursos (puertos) en dicha conexión, para evitar que se cierre. Esto implica no sólo un mayor consumo energético, sino también mayor

uso del ancho de banda disponible en los enlaces de radio. Esto es perjudicial para los operadores, pero también para los fabricantes de teléfonos celulares, dado que cada vez se requiere que sean más pequeños y con mayor tiempo de vida de la batería.

Además, aunque utilizar IPv4 e IPv6 no sea una “carga” para un dispositivo tipo ordenador, portátil, etc., para dispositivos como teléfonos celulares (también válido para sensores, PDA’s, etc.), si que lo es, pues puede encarecer de forma apreciable el coste de estos dispositivos (hablamos de ordenes de magnitud de 10 Euros al llegar al consumidor), por lo que diversos fabricantes (por ejemplo Nokia), han afirmado que retirarán IPv4 de los mismos a la mayor brevedad.

Es obvio que el crecimiento de estas redes y por tanto la gran necesidad de direcciones es también una razón mas que suficiente para la necesidad de IPv6.

De nuevo es importante el factor de la seguridad extremo-a-extremo.

4.8. “Cloud Computing” y “GRIDs”

No es necesario explicar los conceptos de “Cloud Computing” y “GRIDs”. En ambos casos básicamente se trata de compartir recursos situados en diferentes redes. Estos recursos están ubicados en diferentes clientes (o servidores), en dichas redes.

Con IPv4, es muy difícil que este tipo de servicios se reproduzca a gran escala debido a la falta de direcciones y el uso de NAT impide la seguridad extremo a extremo. Con IPv6, no sólo disponemos de direcciones más que suficientes, sino que además no existe NAT y sin embargo, se permiten comunicaciones extremo-a-extremo seguras.

De hecho en Francia e Italia ya existen proveedores que, por medio de IPv6, permiten a los usuarios “alquilar” los tiempos muertos de sus ordenadores, en sus hogares y oficinas a modo de GRIDs, para financiar los costes de sus propias conexiones, lo que a su vez genera una mayor demanda de Banda Ancha, y negocio para todos los implicados.

4.9. Virtualización

Lo indicado en la sección anterior es igualmente válido para la virtualización, dado que la escasez de direcciones IPv4 dificulta incrementar el número de máquinas virtuales disponibles, pues normalmente cada una de ellas requiere una o varias direcciones IP.

4.10. Electrodomésticos Inteligentes

Hoy en día casi cualquier electrodoméstico del hogar tiene software (frigorífico, aspiradores automáticos, hornos, lavadoras, secadoras, lavavajillas, etc.). El software esta sujeto a errores. Además estos electrodomésticos tienen

sensores que permiten indicar que hay una avería (la bomba de agua no funcionar, la presión no es correcta, el compresor no se comporta como debiera, el nivel de agua es bajo, etc.).

Si estos dispositivos estuvieran conectados a Internet, no sólo sería posible actualizar el software para solucionar errores, proporcionar mejoras, sino que además sería posible para los fabricantes de los mismos, los ISPs, o terceras compañías, ofrecer servicios de mantenimiento preventivo, reposición automática de repuestos, y muchos otros.

Tengamos en cuenta que los electrodomésticos son sólo un ejemplo de la gran cantidad de dispositivos que hoy encontramos en nuestras casas, oficinas e industrias, que pueden perfectamente asimilarse a este caso.

4.11. Alertas de Catástrofes

En los últimos años la humanidad ha sufrido diversas catástrofes, como terremotos y tsunamis cuyos daños y número de víctimas podrías haberse aliviado si se hubiera tenido información con cierta anticipación.

Diversas entidades y gobiernos, especialmente en la región de Asia Pacífico, han puesto en marcha proyectos para incrementar las redes de sensores que permitan predecir estos eventos, y obviamente se está utilizando IPv6 como protocolo en el que se produce la comunicación entre los sensores y los puntos colectores de información.

De hecho, en Japón además, esta información se suministra también a los ciudadanos en sus oficinas y viviendas, a través de las redes de Banda Ancha, con servicios que avisan con anticipación de la ocurrencia de, por ejemplo terremotos, a través de ordenadores, pero también se han dispuesto dispositivos autónomos, especialmente para personas que no usan o no pueden usar ordenadores, que consisten en simples luces y sirenas de aviso que se pueden conectar a la red del hogar o de la oficina.

4.12. Defensa y Orden Público

Las ejércitos, fuerzas de orden público y similares, cada vez es más habitual que lleven diversos tipos de armas, sistemas de comunicación, sistemas de posicionamiento, y un sinnúmero de otros dispositivos a modo de PAN ("Personal Area Network", Red de Área Personal), que a su vez se conecta mediante un único sistema de acceso a la red del grupo o incluso mediante Internet, con redes privadas virtuales.

Los inconvenientes de estas redes, con IPv4, son el uso de direcciones privadas y por tanto de NAT, la seguridad, y la configuración de la red PAN, y todos se resuelven con IPv6.

De hecho diferentes cuerpos militares y civiles (ambulancias), de varios países, han avanzado en este sentido, y en este campo es donde se han producido

mayores y mas grandes ejemplos de despliegue públicos con organizaciones como el DOD Norteamericano y la OTAN entre otros.

4.13. Servicios de información y publicidad dinámicos

Cada vez es más importante el número de paneles informativos, de señalización vial en las ciudades y carreteras.

Estos paneles podrían ser más eficaces si pudieran ser direccionados extremo-a-extremo, por medio de IPv6, e incluso podrían ser dinámicos, ya que los sistemas MxM permitirían dotarles de inteligencia, por ejemplo vinculados a sensores o cámaras de tráfico.

Lo dicho, es aplicable también a los paneles publicitarios, que al poder ser direccionados extremo-a-extremo con IPv6, podrían convertirse en paneles inteligentes, con grandes ahorros en su mantenimiento, y al mismo tiempo haciendo que la publicidad pueda ser mucho más dinámica y rica en contenidos y formatos, en definitiva, mucho mas atractiva.

4.14. Juegos y otras actividades On-line

Ya existen algunos fabricantes de consolas de juegos que están trabajando en servicios on-line basados en IPv6, dados los evidentes beneficios.

Microsoft recomienda a los desarrolladores de juegos utilizar las ultimas librerías, que se basan precisamente en IPv6. Microsoft ha desarrollado también una sistema denominado DirectAccess, implementado en los sistemas operativos a partir de Windows Vista y los equivalentes en servidores y consolas de juegos, que permite la configuración automática de seguridad (IPsec), utilizando VPNs con IPv6. Es un paso muy importante para la seguridad en la red, y esta siendo adoptado por otros grandes fabricantes de sistemas y aplicaciones de seguridad.

Consideramos que el crecimiento económico en este sector seguirá en aumento y surgirán nuevos tipos de servicios y aplicaciones al permitir IPv6 la conectividad extremo-a-extremo y el uso de la seguridad también extremo-a-extremo.

5. Anexo I: Detalle de Iniciativas en el Mundo

A continuación detallamos involucración, iniciativas y acciones concretas por parte de algunos gobiernos y organizaciones internacionales.

5.1. Organizaciones Internacionales

5.1.1. IETF. Organización responsable de la estandarización de los protocolos de Internet, y por tanto del diseño de IPv6. No sólo se ha implicado en su desarrollo sino también en el mensaje de su importancia y necesidad.

5.1.2. ISOC. Como organización “paraguas” de IETF, y al que financia parcialmente, se ha ocupado de divulgar entre todos sus miembros y entidades asociadas la gravedad de la “no inmediata adopción” de IPv6.

<http://www.isoc.org/internet/issues/ipv6.shtml>

5.1.3. ICANN/IANA. Se estudia el impacto del despliegue de “glue records” IPv6 en el sistema DNS y se decide agregarlo en “root” en Julio de 2.004. A partir de ahí la mayoría de los TLDs se implican en su despliegue. En Enero de 2.008 se incluyen direcciones IPv6 en los servidores “root”.

5.1.4. RIRs/NRO. Todos los RIRs, y conjuntamente a través del NRO, han indicado en numerosas ocasiones, la necesidad de la inmediata adopción de IPv6.

<http://www.nro.org>

5.1.5. OCDE. Junio de 2.008, Encuentro Ministerial acerca del Futuro de la Economía de Internet: “Consideraciones Económicas en la Gestión de IPv4 y el Despliegue de IPv6”.

<http://www.oecd.org/dataoecd/7/1/40605942.pdf>

5.1.6. Car-2-Car Consortium: Intelligent Transport Systems. Adopta IPv6 como el protocolo de comunicaciones inter e intra-vehiculares.

5.1.7. OTAN. En el año 2.000 se inician los trabajos al respecto de IPv6 y se adopta oficialmente en el año 2.004.

5.1.8. ETSI. Se ha involucrado en el desarrollo, especialmente en pruebas de interoperabilidad de IPv6 desde el año 2.000.

<http://www.etsi.eu/WebSite/Technologies/IPTesting.aspx>

5.1.9. ITU. Tiene establecido un grupo de trabajo específico de IPv6, con recomendaciones a sus miembros para su adopción.

<http://www.itu.int/en/ITU-T/others/ipv6/Pages/default.aspx>

5.1.10. Redes Académicas. La mayoría de ellas en sus versiones internacionales (GEANT, CLARA, Internet2, Canarie, TEIN, EUMED), han desplegado IPv6 desde hace varios años. En algunos casos, los equivalentes nacionales (RedIRIS, Renater, Reaccium, etc.), tienen soporte IPv6 también, así como las universidades y entidades a las que conectan (con diferentes grados de despliegue); esto es cierto más en regiones como Europa, Norteamérica y Canadá, y países concretos como Japón, China y Corea.

5.2. Europa

5.2.1. Comisión Europea. Varios documentos. Los mas relevantes 21/2/2002 (Comunicado al Consejo y Parlamento Europeo: Siguiendo la Generación de Internet – Prioridades para la acción en la transición al Nuevo Protocolo de Internet IPv6), 15/3/2002 (Conclusiones Presidenciales) y 27/5/2008 (Comunicado al Parlamento, el Consejo, los Comités Económicos y Sociales y el Comité de las Regiones: Avanzando Internet – Plan de Acción para el despliegue del Protocolo de Internet versión 6 en Europa). Último documento:

http://ec.europa.eu/information_society/policy/ipv6/docs/european_day/communication_final_27052008_en.pdf

5.2.2. Gobierno Español. El Ministerio de Administraciones Públicas recomienda desde el año 2002 que todas las adquisiciones públicas incorporen IPv6. Igualmente los diversos programas de Investigación y Desarrollo desde dicho año, han contemplado este aspecto.

<http://www.csaemap.es/csi/criterios/normalizacion/index.html>

5.2.3. Gobierno de Francia. Diversos anuncios, desde el 2003 por parte de Claudie Haigneré, Ministra de I+D. Introducción en organismos públicos desde el 2009.

[http://www.fr.ipv6tf.org/DATA/PRESS/Recommandations%20IPv6%20TFF%20\(English\).pdf](http://www.fr.ipv6tf.org/DATA/PRESS/Recommandations%20IPv6%20TFF%20(English).pdf)

5.2.4. Gobierno de Alemania. Iniciado por el departamento de Defensa en el 2006, y continuado por diversos Ministerios, incluyendo el Ministerio Federal del Interior y la Oficina Federal para la Seguridad de la Información en 2009.

<http://www.ipv6council.de/fileadmin/summit09/Aktionsplan.pdf>

5.2.5. Gobierno de Austria. Primer anuncio en Abril de 2004 por parte del Dr. Georg Serentschy (GM – RTR) y el Dr. Hubert Gorbach (Ministro de Infraestructuras y Vicecanciller).

<http://www.ipv6taskforce.at/dokumente/050929/roadmap-fullversion.pdf>

5.2.6. República Checa. En el 2009 se aprobó en dos fases (licitaciones públicas y puesta en marcha), que concluyen el 31 de Diciembre de 2010, y por el momento el cumplimiento es del 100%.

5.2.7. Gobierno de Irlanda. Desde el 2005 se inician los pasos, bajo el auspicio del Departamento de Comunicaciones, Recursos Naturales y

Marinos (ahora Departamento de Comunicaciones, Energía y Recursos Naturales), para la transición nacional a IPv6.

- 5.2.8. Gobierno de Reino Unido. Aunque ha habido intentos previos, se conocen acciones no-públicas por parte del Departamento de Defensa, tan sólo recientemente se ha estructurado un plan concreto que busca el despliegue de la “mejor y mas rápida red de banda ancha con IPv6” para final de 2.015.
- 5.2.9. Gobierno de Noruega.
- 5.2.10. Gobierno de Finlandia. Ha estado implicado desde el 2.005, y se han adoptado diversas medidas desde el regulador (FICORA).
- 5.2.11. Gobierno de Polonia.
- 5.2.12. Gobierno de Eslovenia. En Junio de 2.008 se funda el IPv6 Task Force de Eslovenia y como consecuencia el Instituto Zavod go6, bajo el paraguas de los propios ISPs, del Ministerio de Ciencia y Tecnología y la Agencia Reguladora de Comunicaciones, con diversos objetivos como el desarrollo de las recomendaciones para los sectores público y privado, que son finalizadas en Febrero de 2.010. Es de destacar que la colaboración y financiación del instituto go6 por parte de los propios ISPs ha llevado al país a la primera posición del mundo en despliegue de IPv6.
- 5.2.13. Gobierno de Luxemburgo. Se convoca al IPv6 Council que en sus recomendaciones indica que ha de alinearse con las directivas comunitarias y contar con al menos un 25% de despliegue a final de 2.010.
- <http://www.ipv6council.lu/docs/IPv6+Council+Luxembourg+roadmap.pdf>
- 5.2.14. Gobierno de Turquía. Se inician los trabajos en el 2.003, pero el Gobierno se implica a partir del 2.007. En Febrero de 2.009 se diseña el plan nacional de transición con el objetivo de su despliegue en el 2.011.
- 5.2.15. Gobierno de Grecia. IPv6 instalado en las escuelas públicas.
- 5.2.16. Gobierno de Portugal. IPv6 instalado en las escuelas públicas. Portugal Telecom ha iniciado servicios comerciales.
- 5.2.17. Gobierno de Holanda.
- 5.2.18. Gobierno de Albania.
- 5.2.19. Gobierno de Israel.
- 5.2.20. Emiratos Árabes: Diversas acciones desde Febrero de 2.001 con la intervención del Principe de la Corona Shikh Ahmed Bin Saeed Al Maktoum.

- 5.2.21. Gobierno de Arabia Saudí. En Noviembre de 2.008 la Comisión de Tecnologías de Comunicaciones e Información, publica el plan de despliegue, con servicios comerciales previstos a lo largo de 2.010.
- 5.2.22. Gobierno de Líbano. En Octubre de 2.009 se constituye el IPv6 Forum Lebanon, de la mano de la Autoridad Reguladora de Telecomunicaciones, con el objetivo de avanzar el despliegue de IPv6 en el país.
- 5.2.23. ESA. Soporte de IPv6 en tecnologías, productos y servicios satelitales.
- 5.2.24. CENELEC.
- 5.2.25. Eurocontrol. Red de control del tráfico aéreo Europeo, habilitada con soporte de IPv6.

5.3. Norteamérica

- 5.3.1. Gobierno de US. Primeros trabajos a lo largo del 2.002. En Junio de 2.003, el Departamento de Defensa anuncia que todas las adquisiciones publicas desde Octubre de dicho año, requerían el soporte de IPv6. En Junio de 2.005, la Casa Blanca pública una decisión similar para requerir a las agencias federales la utilización de IPv6 desde el año 2.008. Además, se aprueba el plan de e-Government en Septiembre de 2.010, para el despliegue nativo completo de IPv6 como muy tarde en Septiembre de 2.012.

<http://www.defense.gov/releases/release.aspx?releaseid=5457>

<http://www.cio.gov/Documents/IPv6MemoFINAL.pdf>

- 5.3.2. Gobierno de Canadá. En Abril de 2.009 se establece un plan de transición en tres fases, con una fecha máxima para la transición en Diciembre de 2.013.

5.4. Latinoamérica y Caribe

- 5.4.1. Plan de Acción eLAC 2.010: Segunda Conferencia Ministerial sobre la Sociedad de la Información de América Latina y Caribe (8/02/2008), San Salvador.

“Realizar acciones tendientes a la promoción de la adopción del protocolo IPv6 a nivel público y privado con el objeto de lograr que todos los servicios públicos ofrecidos a través del protocolo IP, según sea apropiado, estén disponibles sobre IPv6 y que la infraestructura y aplicaciones más relevantes de los Estados sean compatibles con IPv6. Las medidas que se tomarían incluirán, en la medida de lo posible, la pronta implementación de requerimientos en las compras públicas de equipos y aplicaciones que aseguren su compatibilidad con IPv6.”

eLAC 2.105: Tercera Conferencia Ministerial sobre la Sociedad de la Información en América Latina y Caribe (21/11/2010), Lima.

“Colaborar y trabajar en forma coordinada con todos los actores regionales, incluidos los sectores académico y comercial, la comunidad técnica y las organizaciones que participan en el tema, como el Registro de Direcciones de Internet para América Latina y Caribe (LACNIC) y la Sociedad Internet (ISOC), entre otras, para que la región haya logrado un amplio despliegue del protocolo Internet versión 6 (IPv6) en 2015. Implementar a la mayor brevedad posible planes nacionales para que pueda accederse a los portales de servicios públicos gubernamentales de los países de la región a través del IPv6 y que las redes estatales trabajen de forma nativa con IPv6.”

5.4.2. Gobierno de Cuba. Se inician las pruebas en el 2.005, con reglamentaciones específicas en los años 2.007 y 2.008. La resolución 156 de 2.008 “Establece una Metodología para la introducción en el país del protocolo IPv6 en las redes telemáticas, sistemas informáticos y aplicaciones de software, a través de un cronograma detallado por etapas.”. Primera etapa en Febrero de 2.009, y plazo final Julio de 2.013.

5.4.3. Gobierno de México. En el 2.007 se presenta al senado una propuesta para la adopción de IPv6.

5.4.4. Gobierno de Colombia

<http://www.mintic.gov.co/news.asp?articleId=106>

http://wsp.presidencia.gov.co/Prensa/2010/Diciembre/Paginas/20101203_02.aspx

5.4.5. Gobierno de Argentina.

5.4.6. Gobierno de Chile.

<http://www.ipv6.cl>

5.4.7. Gobierno de Costa Rica.

5.4.8. Gobierno de Brasil.

<http://www.ipv6.br>

5.5. Asia Pacífico

5.5.1. Gobierno de Japón. Septiembre de 2.000, el Primer Ministro (Mori) identifica públicamente a IPv6 como parte crítica de la iniciativa eJapan 2.005, proporcionando incentivos fiscales a las compañías que integren soporte de IPv6. Estos incentivos han superado los 8 billones de yenes. Además hay múltiples iniciativas auspiciadas bajo el paraguas del IPv6 Council, iniciado por el Ministerio de Administración Pública, Asuntos Domésticos, Correos y Telecomunicaciones. U-Japan.

http://www.kantei.go.jp/foreign/it/network/0122full_e.html

http://www.soumu.go.jp/menu_seisaku/ict/u-japan_en/index.html

- 5.5.2. Gobierno de Australia. Anuncio del DoD en Noviembre de 2.005 para el despliegue antes de 2.013. En el 2.007, se desarrollo el plan de transición por parte del Departamento de Finanzas y Desregulación, con 3 fases, Preparación (final de 2.009), Transición (final de 2.011) e Implementación (final de 2.012).
- http://www.finance.gov.au/e-government/infrastructure/docs/Endorsed_Strategy_for_the_Transition_to_IPv6_for_Australian_Government_agencies.pdf
- 5.5.3. Gobierno de China: CNGI. Plataforma de pruebas establecida en 2.003 por 8 ministerios, con resultados en demostraciones y puesta en marcha para los Juegos Olímpicos de 2.008, la EXPO de 2.010 y la Universiada de 2.011, con participación de los 6 principales operadores nacionales, los IXs y la red Académica.
- 5.5.4. Gobierno de India. Diversos anuncios, desde Mayo de 2.004 (Dr. Govind, MCIT; Dr. Maran y Mr. Satyen Gupta, TRAI). En Julio de 2.010 se publica el plan final de transición para que todo el sector publico tenga soporte completo antes de Marzo de 2.012.
- 5.5.5. Gobierno de Corea del Sur. Anuncia el soporte de IPv6 en Febrero de 2.001: u-IT839. En el 2.006 se incorpora como requisito en las adquisiciones públicas y se prevé su incorporación a las redes comerciales antes del año 2.012.
- 5.5.6. Gobierno de Malasia: MyICMS 886. En 2.005 el Ministerio de Energía, Agua y Comunicaciones redacta el plan de transición nacional, incluyendo el requisito de que el país este preparado a final de 2.010.
- 5.5.7. Gobierno de Singapur: Next Gen NII & IN2015. En Junio de 2.006, la Autoridad para el Desarrollo de las Info-Comunicaciones de Singapur, edito el plan de transición nacional, con fecha límite del año 2.010 para el sector público.
- 5.5.8. Gobierno de Indonesia. Desde el 2.006, el Consejo Nacional Indonesio para ICT (DETIKNAS), comenzó sus trabajos con las metas fijadas para el año 2.010.
- 5.5.9. Gobierno de Nueva Zelanda. Esta trabajando en el plan del sector publico (Ministerio de Desarrollo Económico).
- 5.5.10. Gobierno de Tailandia. El segundo Plan Maestro para ICT, creado en el 2.009, para su aplicación del 2.010 al 2.014 (IT2010), implica el despliegue de IPv6 entre los años 2.013 y 2.015.
- 5.5.11. Gobierno de Vietnam. Los trabajos se iniciaron en 2.007, y se publicaron en el 2.009 nuevas recomendaciones para la adopción en el 2.010.

- 5.5.12. Gobierno de Pakistan. Desde el año 2.006 se trabaja a través del IPv6 Task Force, incluyendo pruebas en cooperación entre industria y gobierno.
- 5.5.13. Gobierno de Taiwan: Anuncio oficial por parte del Ministro de Estado Dr. Tsay Ching-Yen en Octubre de 2.001, despliegue hasta el 2.010.
- 5.5.14. Gobierno de Filipinas. En Septiembre de 2.009 se inician los trabajos por parte de la Oficina del Presidente, Comisión de Tecnologías de Información y Comunicaciones, y se constituye el IPv6 Forum, junto con el sector privado. Se incluye una orden gubernamental y política para la promoción del despliegue y uso de IPv6, así como la creación de una agencia Inter-Ministerial para la monitorización de los esfuerzos y actividades al respecto.
- 5.5.15. Gobierno de Afganistán.
- 5.5.16. APEC. En el encuentro de Noviembre de 2.010 (Okinawa, Japón), Ministros de 21 economías de la región de Asia Pacífico, han incrementado el nivel de certeza y soporte a la industria para su movimiento hacia IPv6 “Facilitemos a la Industria y los Gobiernos colaborar juntos para empujar el acelerador del despliegue de IPv6”.

http://www.apec.org/apec/ministerial_statements/sectoral_ministerial/telecommunications/2010.html

<http://www.apnic.net/publications/news/2010/telmin8>

5.6. África

- 5.6.1. Gobierno de Egipto: Primeros pasos en Septiembre de 2.004 por parte del Ministro de Comunicaciones Tarek Kamel.
- 5.6.2. Gobierno de Kenia. En el 2.008 inicia los primeros pasos con la creación del IPv6 Task Force y recomendaciones por parte de la Asociación de ISPs, y diversos departamentos ministeriales.
- 5.6.3. Gobierno de Argelia.
- 5.6.4. Gobierno de Túnez.
- 5.6.5. Gobierno de Sudán.
- 5.6.6. Gobierno de Senegal.
- 5.6.7. Gobierno de Nigeria.