UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TÍTULO DE LA TESIS:
PROPUESTA PARA LA TRANSICIÓN DE IPv4 A IPv6 EN EL ECUADOR A TRAVÉS DE LA SUPERTEL.

Previa la obtención del Grado Académico de Magíster en Telecomunicaciones

ELABORADO POR:
Ing. José Coellar Solórzano
Ing. Jacob Cedeño Mendoza

Guayaquil, a los 4 días del mes Febrero año 2013

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por los Magísteres José Coellar y Jacob Cedeño Mendoza como requerimiento parcial para la obtención del Grado Académico de Magíster en Telecomunicaciones.

Guayaquil, a los 4 días del mes de Febrero 2013

DIRECTOR DE TESIS

_____

MsC. Edwin Palacios Meléndez

REVISORES:

_____

MsC. Luzmila Ruilova Aguirre.

_____

MsC. Luis Córdova Rivadeneira

DIRECTOR DEL PROGRAMA

_____

MsC. Manuel Romero Paz

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

DECLARACIÓN DE RESPONSABILIDAD

NOSOTROS, José Coellar Solórzano y Jacob Cedeño Mendoza

DECLARAMOS QUE:

La tesis “PROPUESTA PARA LATRANSICIÓN DE IPv4 A IPv6 EN EL ECUADOR A TRAVÉS DE LA SUPERTEL”, previa a la obtención del grado Académico de Magíster, ha sido desarrollada en base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes. Consecuentemente este trabajo es de nuestra total autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico de la tesis del Grado Académico en mención.

Guayaquil, a los 4 días del mes de Febrero 2013

LOS AUTORES

_____

Ing. José Coellar Solórzano

_____

Ing. Jacob Cedeño Mendoza

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

AUTORIZACIÓN

NOSOTROS, José Coellar Solórzano y Jacob Cedeño Mendoza

Autorizamos a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución de la Tesis de Maestría titulada: “PROPUESTA PARA LATRANSICIÓN DE IPv4 A IPv6 EN EL ECUADOR A TRAVÉS DE LA SUPERTEL”, cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y total autoría.

Guayaquil, a los 4 días del mes de Febrero 2013

LOS AUTORES

_____

Ing. José Coellar Solórzano

_____

Ing. Jacob Cedeño Mendoza

Dedicatoria

El presente trabajo va dedicado con todo cariño a mi familia, quienes con su esfuerzo y comprensión me brindaron su apoyo incondicional durante la realización de este trabajo.

Ing. José Coellar Solórzano

El presente trabajo va dedicado con todo cariño a mi familia que siempre me ha apoyado en toda mis decisiones, en especial a mi esposa Silvia por la motivación y paciencia que supo brindarme.

Ing. Jacob Cedeño Mendoza

Agradecimientos

A la Universidad Católica de Santiago de Guayaquil que nos abrió sus puertas, al programa de Maestría en Telecomunicaciones por la colaboración prestada al presente trabajo de intervención, al MsC. Edwin Palacios Meléndez, Director de Tesis y a nuestros maestros que con sus sabias experiencias supieron guiarnos por el camino del saber.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

Capítulo 2: Protocolos de Internet IPv4 e IPv6

Capítulo 3: Propuesta del Mecanismo de Transición a IPv6

Capítulo 4: Simulaciones de mecanismos de transición.

ÍNDICE DE TABLAS

Capítulo 2

Resumen

El nuevo Protocolo de Internet versión 6 (IPv6) actualmente se va a incluir como soporte IP de muchos productos y de los principales sistemas operativos de ordenador. El protocolo de internet IPv6 inicialmente se lo llamó IP de siguiente generación (IPng). En realidad el protocolo de internet IPv6, está formado por especificaciones definidas por la Fuerza de Tarea de Ingeniería de Internet (Internet Engineering Task Force, IETF).

El protocolo de internet IPv6 fue diseñado para mejorar la actual versión IPv4. Donde los hosts y nodos intermedios puedan operar ya sea con IPv4 o IPv6, además de manejar paquetes formateados para cualquier nivel. Tanto los usuarios como los proveedores de servicio de internet pueden actualizarse al IPv6 independientemente, sin tenerse que coordinarse entre sí.

El presente trabajo de investigación consiste en proponer todos los mecanismos existentes y aceptados internacionalmente para ejecutar el proceso de transición de IPv4 a IPv6, todo esto por Decreto Constitucional y regulado por el CONATEL, MINTEL y SUPERTEL para posteriormente realizar una migración total.

Abstract

The new Internet Protocol version 6 (IPv6) will be included as IP support of many products and principal operating systems of computers. IPv6 was initially named Next Generation IP(IPng). Actually, internet protocol IPv6 is formed of specifications defined by the Internet Engineering Task Force (IETF).

IPv6 internet protocol was designed to improve the present version IPv4 in which hosts and intermediate nods can operate with IPv4 or IPv6 in addition to manage packets formatted for any level. Also, users and internet service providers can update to IPv6 independently, without having to coordinate with each other.

The present research consists in proposing every internationally accepted existing mechanism to execute the transition process from IPv4 to IPv6, adhering to Constitutional Decree and following regulations of the CONATEL, MINTEL and SUPERTEL, in order to later carry out a complete migration.

Capítulo 1: Descripción del proyecto de intervención.

1.1. Antecedentes.

El Protocolo de Internet con sus siglas en inglés IP (Internet Protocol), permite el funcionamiento de internet, en la actualidad IPv4 se está agotando inminentemente, la IANA[1] en febrero del 2011 ha entregado las últimas direcciones IPv4 a cada una de las cinco regiones, previéndose el agotamiento en Suramérica para el año 2012.

Actualmente el internet usa el protocolo IPv4 con 4.000 millones de direcciones públicas, con límite práctico de aproximadamente 300 millones, donde cada conexión a internet usa una dirección pública, aunque sea compartida a través de un dispositivo NAT. Hace algunos años atrás se pensó que ocurriría este inconveniente, presentándose una solución estandarizada, la misma que ha sido puesta en evaluación y comprobada para estar disponible en los equipos de usuarios finales y operadores, conocida como la nueva versión del protocolo de internet IPv6, la misma nos garantizaría un despliegue del ancho de banda durante 480 años aproximadamente.

El mencionado protocolo ha comenzado desplegándose en el continente Europeo aproximadamente desde el 2002, pero la penetración en Suramérica es prácticamente inexistente y en países en vía de desarrollo se está quedando rezagado. Los planes de expansión de banda ancha en Ecuador, no podrán cumplirse si no se toman medidas urgentes que garantice a la administración pública, proveedores de contenidos, ISPs y la industria en general, toma conciencia del problema.

Se restringe la asignación de direcciones públicas, es decir, de asignar clases A, B y C se pasó a la asignación de bloques de

[1] **IANA, Internet Assigned Numbers Authority** es la entidad que supervisa la asignación global de direcciones IP, por Jon Postel en el Instituto de Ciencias de la Información (ISI).

direcciones ajustadas a las necesidades, la RIR sugiere el uso de direcciones dinámicas o privadas, y que se restringa el uso de direcciones públicas, salvo los casos en que los servicios cliente-servidor justifique la necesidad. En las eventuales congestiones producidas por el tráfico entre host o terminales de distintas redes, cada paquete de información compite por obtener un poco de ancha de banda disponible para alcanzar su destino.

1.2. Definición del problema

Debido al agotamiento de protocolos de internet IPv4 en Latinoamérica, específicamente en el Ecuador surge la necesidad de realizar la transición de IPV4 a IPV6 a través del Ministerio de Telecomunicaciones mediante la Superintendencia de Telecomunicaciones (SUPERTEL).

1.3. Objetivos

Una vez que se ha definido el problema de investigación procedemos a describir el objetivo general y los objetivos específicos.

1.3.1. Objetivo General:

Proponer los mecanismos de transición de IPV4 a IPV6 para mejorar la interconexión y comunicación de las operadoras de servicios de valor agregado de internet en el Ecuador.

1.3.2. Objetivos específicos:

- ✓ Describir el estado del arte de los protocolos de internet IPv4 e IPv6.
- ✓ Determinar el mecanismo para la migración o transición del protocolo de internet IPv4 a IPv6.
- ✓ Evaluar el funcionamiento de IPv4 versus IPv6 mediante una red donde coexistan ambos protocolos.

1.4. Hipótesis

La presente propuesta de los mecanismos de transición del protocolo de internet IPv4 a IPv6 permitirá un adecuado crecimiento de la banda ancha del internet y mejorar la calidad de transmisión de la información.

1.5. Metodología de investigación.

Alcance:

La presente investigación es de carácter **Exploratorio y Explicativo,** pues se pretende explorar a los protocolos de internet IPv4 e IPv6 a través del estado del arte que originan el fenómeno en cuestión, y pretender una explicación del mismo. También interesa emplear alguna herramienta de simulación para comprobar tal fenómeno.

Paradigma:

Empírico-Analítico con enfoque cuantitativo.

Método:

Ex post facto, puesto que se pretenderá evidenciar las posibles relaciones de causa efecto entre las técnicas o mecanismos de transición para interconexión y comunicación de IPV4 a IPV6.

Diseño de la Investigación:

No experimental Transversal.- Puesto que no se manipularán deliberadamente las variables de estudio, se procederá a la observación directa de los protocolos de internet tal y como se da en su contexto natural, y posteriormente su análisis respectivo.

Capítulo 2: Protocolos de Internet IPv4 e IPv6.

En el presente capítulo se basa en los servicios estandarizados llamados Protocolos de Internet (IP) versiones 4 y 6, presentaremos también el esquema de direccionamiento usado por el IP y explicaremos la división de las clases de direcciones del IP. Adicional detallamos un aspecto del protocolo como TCP e IP brindan las fórmulas para transmisión de mensajes, y lo que es más importante, se discutirán los estándares de comunicación, independientemente de hardware de la red.

2.1. Historia de Internet y protocolo TCP/IP

En realidad Internet es un medio de comunicación que revoluciona el mundo tanto de las telecomunicaciones como de los ordenadores o computadoras. Las bases que permitieron su desarrollo o evolución, inicialmente desde el telégrafo hasta las computadoras personales pasando por el teléfono y la radio[2]. La cantidad de información que maneja en la actualidad Internet es demasiado grande, siendo utilizado como un recurso investigativo cuyo acceso de información mundial se lo realiza en pocos segundos.

Internet inicialmente fue ideada por J. C. R. Licklider, que mediante oficios escritos en Agosto de 1962 en el Instituto Tecnológico de Massachusetts (MIT), describía computadores que se conectaban entre sí, para acceder a la toda la información entre las misma, también denominada por él como una Red Galáctica (Galactic Network). Debido a estas ideas radicales Licklider fue designado Director del Programa DARPA *(Defense Advanced Research Projects Agency)*.

El protocolo TCP/IP fue diseñado a finales de 1960 como el fundamento de la red ARPANET, que conectaba las computadoras de oficinas gubernamentales y universitarias. Funcionaba bajo el concepto

[2]Recuperado de la página web: http://www.iab.org/

de cliente servidor, lo que significa que alguna computadora pide los servicios de otra computadora; la primera es el cliente y la segunda el servidor.(Trejo Ramírez, 2012)

En 1961, Leonard Klienrock introduce el concepto de Conmutación de Paquetes (Packet Switching, en inglés). La idea era que la comunicación entre ordenadores fuese dividida en paquetes. Cada paquete debería contener la dirección de destino y podría encontrar su propio camino a través de la red(Ureña Poirier & Rodríguez Martín, 2012).

En octubre de 1962, Licklider fue nombrado jefe de la oficina de procesado de información de la Agencia de Proyectos de Investigación Avanzada *(Defense Advanced Research Projects Agency o* DARPA), y empezó a formar un grupo informal dentro de DARPA del Departamento de Defensa de los Estados Unidos para investigaciones sobre ordenadores más avanzadas.

Según lo indicado por (Verdejo Alvarez, 2000), la primera WAN *(Wide Area Network, Red de Área Amplia)* documentada fue creada en 1965 por Lawrence G. Roberts y Thomas Merrill, quienes conectaron una TX-2 y un Q-32 desde el MIT en Massachusetts hasta California mediante una línea telefónica. Para 1967 se había avanzado en el diseño de redes de comunicaciones, otros países como Inglaterra investigaban por medios de otros grupos como el RAND y el NPL. Es por esto, que en DARPA se acordó interconectar todos sus centros investigativos por medio de una red a la que fue denominada ARPANET.

Como parte del papel de la oficina de procesado de información, se instalaron tres terminales de redes: una para la *System Development Corporation* en Santa Mónica, otra para el Proyecto *Genie* en la Universidad de California (Berkeley) y otra para el proyecto *Multics* en el Instituto Tecnológico de Massachusetts. La necesidad de Licklider de redes se haría evidente por los problemas que esto causó.(UPF, 2012)

Ya para el año 1969 la Agencia de Proyectos de Investigación Avanzada (*Defense Advanced Research Projects Agency* o DARPA) del Ejército de los EEUU desarrolla la ARPANET(Ureña Poirier & Rodríguez Martín, 2012). La finalidad principal de esta red era la capacidad de resistir un ataque nuclear de la URSS para lo que se pensó en una administración descentralizada. De este modo, si algunos ordenadores eran destruidos, la red seguiría funcionando. Aunque dicha red funcionaba bien, estaba sujeta a algunas caídas periódicas del sistema.

De este modo, la expansión a largo plazo de esta red podría resultar difícil y costosa. Se inició entonces una búsqueda de un conjunto de protocolos más fiables para la misma. Dicha búsqueda finalizó, a mediados de los 70, con el desarrollo de TCP/IP(Ureña Poirier & Rodríguez Martín, 2012). Es por esto, que se inicia la investigación en desarrollar productos de redes de computadoras, y de la tecnología de comunicación, denominada también como conmutación de paquetes, y finalmente surge el protocolo TCP/IP. Entre los objetivos principales se encontraban los siguientes:

- ✓ **Protocolos Comunes:** que permita el protocolo común la comunicación de todas las redes para simplificación de los procesos.
- ✓ **Interoperabilidad:** que funcionen correctamente los equipos de distintos fabricantes y de manera conjunta, permitiendo el desarrollo eficiente y fomentando la competitividad entre los proveedores.
- ✓ **Comunicaciones sólidas:** que los protocolos aporten con conexiones fiables y de alto rendimiento mediante redes de área extensa relativamente primitivas disponibles en aquel momento.
- ✓ **Facilidad de reconfiguración:** que la red permita reconfigurarse, es decir, facilidad para añadir o eliminar computadores sin sufrir interrupciones de comunicaciones.

Tras varias investigaciones realizadas, se asigna roles al protocolo TCP/IP, donde solamente IP se encargaría de enviar paquetes a través

de una red de comunicaciones hacia su destino. Mientras que para controlar el flujo de información o que lleguen los paquetes correctamente al destino se emplean los 2 protocolos, el TCP y el UDP *(User Datagram Protocol)*, en esencia son el mismo, aunque el segundo no permite que todos los paquetes lleguen a su destino, solamente una parte, es decir, no es confiable. Los grupos encargados para desarrollar el nuevo protocolo se encontraban en las Universidades de Stanford y UCLA que incluía a la empresa *Bolt, Beraneck & Newman (BBN)*, cuya designación fue autorizada por la DARPA.(Verdejo Alvarez, 2000)

Los usuarios de Internet por Regiones Geográficas se muestra en la figura 2.1, donde Asia tiene la mayor cantidad de usuarios con el 44,8%; Europa con el 21,5%, América 22,6% (Norte América 12% y Latinoamérica 10,6%), África 7%, Medio Oriente 3,75 y Oceanía el 1,9%. Estos porcentajes se basaron en la información a priori de 2,405,518,376 usuarios de Internet hasta junio 30 del 2012.

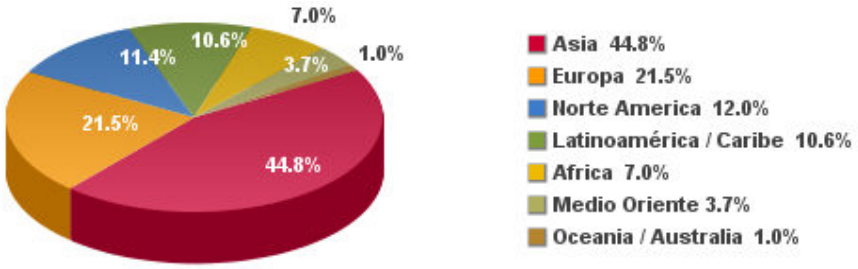

Figura 2. 1: Usuarios de Internet por Regiones Geográficas – 2012.
Fuente: www.exitoexportador.com/stats.htm

En la tabla 2.1 se muestran las Estadísticas de Usuarios Mundiales del Internet que fueron actualizadas a Junio 30, 2012 en la página web www.exitoexportador.com/stats. De donde los datos de población se basan en cifras para 2012 del *US Census Bureau* (http://www.census.gov/) en su mayoría. Asimismo, la información de los datos de los usuarios provienen de las siguientes instituciones: Nielsen Online *(http://www.nielsen-online.com/intlpage.html)*, por la ITU *(www.itu.int/)*, por Internet World Stats *(http://www.internetworldstats.com/)* y algunas fuentes locales. Finalmente

los usuarios o suscriptores de Facebook fueron obtenidos en dicha organización.

Tabla 2. 1:Estadísticas Mundiales del Internet y la Población.

Regiones	Población (2012 Est.)	Usuarios Dic. 31, 2000	Usuarios Junio 30, 2012	% Población (Penetración)	Usuarios % Mundial	Facebook Sept 30, 2012
África	1,073,380,925	4,514,400	**167,335,676**	15.6 %	7.0 %	48,262,820
Asia	3,922,066,987	114,304,000	**1,076,681,059**	27.5 %	44.8 %	235,989,160
Europa	820,918,446	105,096,093	**518,512,109**	63.2 %	21.5 %	243,230,440
Oriente Medio	223,608,203	3,284,800	**90,000,455**	40.2 %	3.7 %	22,793,140
Norte América	348,280,154	108,096,800	**273,785,413**	78.6 %	11.4 %	184,177,220
Latinoamérica / Caribe	593,688,638	18,068,919	**254,915,745**	42.9 %	10.6 %	188,339,620
Oceanía / Australia	35,903,569	7,620,480	**24,287,919**	67.6 %	1.0 %	14,614,780
TOTAL MUNDIAL	**7,017,846,922**	**360,985,492**	**2,405,518,376**	**34.3 %**	**100.0 %**	**937,407,180**

Fuente: www.exitoexportador.com/stats.htm

En Ecuador la población es aproximadamente de 15 millones, los usuarios de internet al año 2000 fue de 180 mil, mientras que en el 2012 superan los 6 millones, cuyo porcentaje de penetración en la población es 43,8% y hay aproximadamente 5 millones de suscriptores en Facebook, esta información se observa detalladamente en la tabla 2.2 de usuarios de internet en América del Sur.

Tabla 2. 2:Usuarios de Internet en América del Sur.

América del Sur	Población (dato 2012)	Usuarios, año 2000	Usuarios Junio 30, 2012	Penetración (% Población)	Usuarios % Tabla	Facebook Sept 30, 2012
Argentina	42,192,494	**2,500,000**	**28,000,000**	**66.4 %**	**14.7 %**	**20,048,100**
Bolivia	10,290,003	**120,000**	**3,087,000**	**30.0 %**	**1.6 %**	**1,753,060**
Brasil	193,946,886	**5,000,000**	**88,494,756**	**45.6 %**	**46.6 %**	**58,565,700**
Chile	17,067,369	**1,757,400**	**10,000,000**	**58.6 %**	**5.3 %**	**9,687,720**
Colombia	45,239,079	**878,000**	**26,936,343**	**59.5 %**	**14.2**	**17,322,000**
Ecuador	15,223,680	**180,000**	**6,663,558**	**43.8 %**	**3.5 %**	**4,970,680**
Islas Malvinas	2,995	-	**2,887**	**96.4 %**	**0.0 %**	**2,020**
Guyana Francesa	249,540	**2,000**	**67,220**	**26.9 %**	**0.0 %**	**67,220**
Guayana	782,105	**3,000**	**250,274**	**32.0 %**	**0.1 %**	**134,800**
Paraguay	6,541,591	**20,000**	**1,563,440**	**23.9 %**	**0.8 %**	**1,214,080**
Perú	29,549,517	**2,500,000**	**10,785,573**	**36.5 %**	**5.7 %**	**9,351,460**
Suriname	560,157	**11,700**	**179,250**	**32.0 %**	**0.1 %**	**99,820**
Uruguay	3,316,328	**370,000**	**1,855,000**	**55.9 %**	**1.0 %**	**1,646,740**
Venezuela	29,497,483	**950,000**	**12,097,156**	**41.0 %**	**6.4 %**	**9,766,540**
TOTALS. América	**394,459,227**	**14,292,100**	**189,982,457**	**48.2 %**	**100.0 %**	**134,629,940**

Fuente: www.exitoexportador.com/stats.htm

De acuerdo a los datos proporcionados por la tabla 2.1, en la figura 2.2 se muestra el diagrama de barras de los usuarios de internet en el mundo por zonas geográficas y en la figura 2.3 se muestra los suscriptores de Facebook.

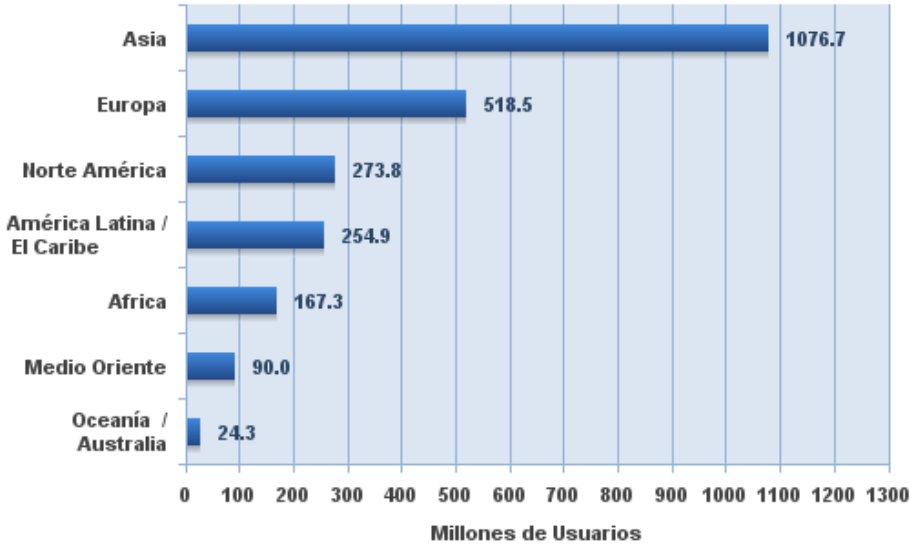

Figura 2. 2: Diagrama de barras de usuarios de Internet por Regiones Geográficas – 2012.
Fuente: www.exitoexportador.com/stats.htm

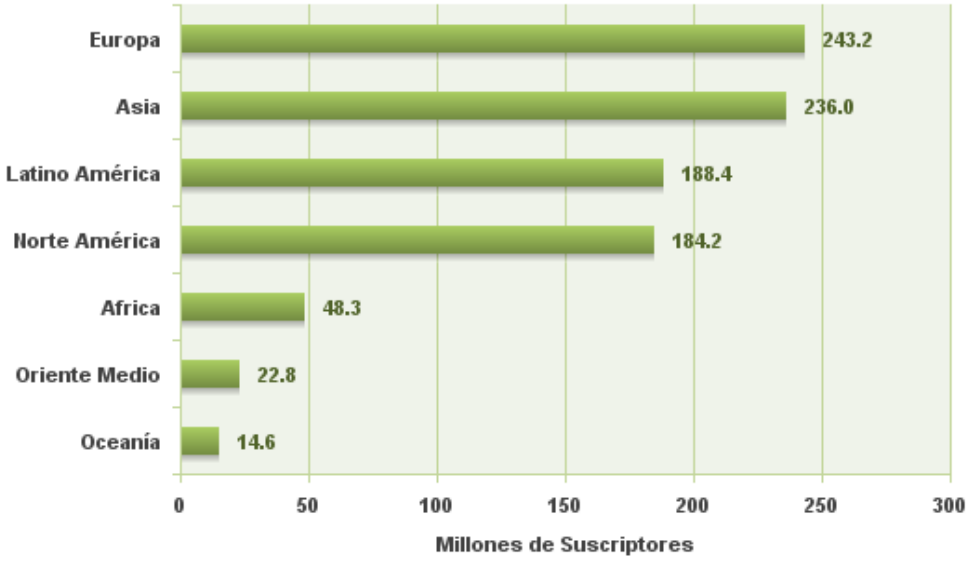

Figura 2. 3: Diagrama de barras de suscriptores de Facebook por Regiones Geográficas – 2012.
Fuente: www.exitoexportador.com/stats.htm

Según los expertos, la Internet como la conocemos, se enfrentará a un grave problema en unos pocos años. Debido a su rápido crecimiento y las limitaciones en su diseño, habrá un momento en que no hay direcciones más libres están disponibles para conectar a nuevos huéspedes. En ese punto, no hay servidores web más nuevas se pueden crear, sin más usuarios pueden inscribirse para las cuentas de los ISP, y no máquinas más nuevas pueden ser configurados para acceder a la web o participar en juegos en línea - algunas personas pueden llamar a este un problema grave.(Feyrer, 2001)

2.2. Protocolo TCP/IP.

Una vez conocida la historia y de cómo se organiza INTERNET, procederemos a describir los protocolos que permiten su funcionamiento universal, independientemente de los computadores, sistemas operativos y/o redes que la conforman. A continuación, definiremos los protocolos TCP/IP extraída de (Richard Stevens, 2011): *"Las familias de protocolos TCP/IP permiten la comunicación entre diferentes tipos de ordenadores con independencia del fabricante, red a la que se encuentren conectados y sistema operativo utilizado."*

El protocolo de Internet, es un protocolo que no se encuentra orientado a la conexión para transmisión de información mediante una red de paquetes de datos conmutados. Se encuentra localizado en la tercer capa del modelo ISO/OSI, el cual permite entregar paquetes de datos desde un nodo de origen a otro nodo destino, basado en la dirección escrita en cada paquete.

La mencionada capa de red de acuerdo al modelo TCP/IP, se emplea los protocolos pertenecientes a la capa de transporte (TCP), permitiendo orientar los datos hacia un destino específico, direccionando los datagrama generados en la capa de red, pero sin poder comprobar la integridad del contenido.

Con lo descrito no se podía distinguir las versiones del IP, aunque con la llegada o aparición de la versión 6, se empezó a diferenciar el IPv6 de la IPv4, ésta versión cuenta con una longitud de 32 bits. Dicha longitud se escribe mediante la forma *dottedquad* (a, b, c, d) que es representado por el número decimal en el intervalo de 0 a 255, es decir, que el rango se escribe desde 0.0.0.0 hasta 255.255.255.255, lo que es una limitante en la actualidad ya que existe combinaciones del tipo $2^{52} = 4.294.967.296$ o sea 4 billones de direcciones.

Las clases 'a', 'b' y 'c' han sido divididas en partes fijas, dichas divisiones son muy conocidas en el rango ya mencionado anteriormente. Adicionalmente, existen direcciones del tipo 'd' y 'e' (ver figura 2.4), reservadas para procesos multicast y experimentales. La dirección de clase 'A' tiene 8 y 24 bits, que permite identificar la red y los usuarios respectivamente. (Malone & Niall, 2005)

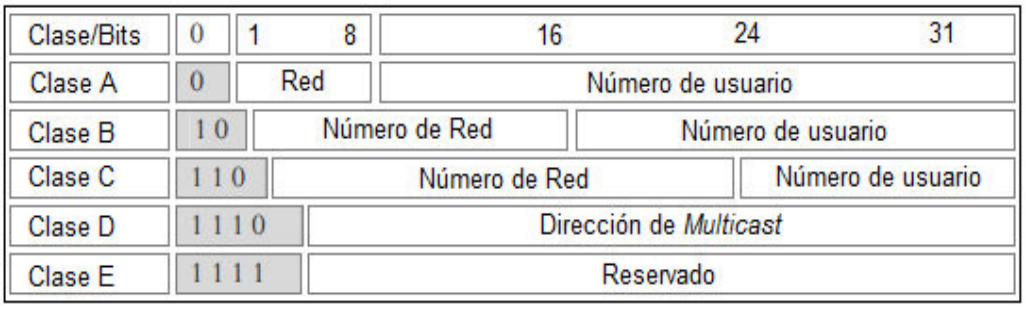

Figura 2. 4: Identificación de las clases de direcciones IP.**(Malone & Niall, 2005)**

Según Roberto Gordo, las clases de dirección se encuentran en una IP determinada, siempre dependerá del rango en él que caiga, según lo mostrado en la tabla 2.3.(Gordo Saez, 1998)

Tabla 2. 3: Rango de direcciones del IPv4

Clase	Rango de dirección	% direcciones disponibles en IPv4
A	0.0.0.0 127.255.255.255	50
B	128.0.0.0 191.255.255.255	25
C	192.0.0.0 223.255.255.255	12.5
D	224.0.0.0 239.255.255.255	6.5
E	240.0.0.0 255.255.255.255	6

Fuente: (Gordo Saez, 1998)

Una vez elegido el tamaño de direcciones IP y la división de cada dirección dada en dos partes, primeramente el prefijo requiere suficientes bits para admitir la concesión de la dirección de red única en Internet. Ahora, para el sufijo se necesitan demasiados bits para cada una de las computadoras que se encuentran conectadas a la red cuyo sufijo es único (Kotal, 2005). No existe la solución integral, ya que al agregar bits a una parte se los disminuía de la otra. Finalmente, se puede decir, que un prefijo grande dirección a muchas redes, aunque limita el tamaño de cada red; mientras que el sufijo grande, indica a la red que puede contar con muchas computadoras, reduciendo así la cantidad total de redes.

En la figura 2.4 se muestran las cinco clases de dirección; los bits de la izquierda identifican las clases y la división el prefijo y el sufijo, siguiendo la convención de los protocolos TCP/IP, debemos numerar los bits de izquierda a derecha y de numerar como cero el primer bit. Las clases A, B y C se denominan clases primarias, porque emplean direcciones de host. La clase D se utiliza para multitransmisión, lo que permite la entrega a un grupo de computadoras. Para pasar multitransmisión IP, un grupo de host debe acordar compartir una dirección multitransmisión. Una vez establecido el grupo multitransmisión, se entrega a los host del grupo copia de los paquetes enviados a esta dirección.

2.3. Protocolo de internet versión 4 (IPv4)

El protocolo de internet IP, es la parte fundamental sustentada por el sistema TCP/IP y de todo el funcionamiento de INTERNET. Su especificación está recogida en la siguiente página web http://www.rfc-es.org/rfc/rfc0791-es.txt.Launidad de datos del IP es el datagrama, cuyo esquema se muestra en la figura 2.5.

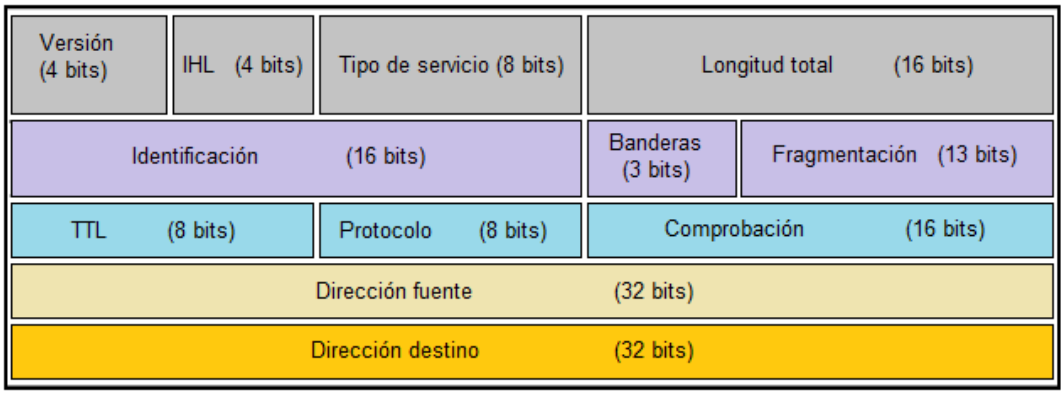

Figura 2. 5: Encabezado del IPv4.
Fuente: http://www.imaginar.org/mdi/docs/ipv6.pdf

En la figura 2.5 se ilustra a un datagrama IP, cuya estructura es en bloques de 32 bits (4 bytes), su transmisión consiste en enviar primero el bit 0, luego el bit 1, 2, 3…hasta finalizar el datagrama. Dicho orden se denomina *network byte order*, el mismo es muy importante, debido a que los diferentes computadores tienen diversos sistemas de almacenamiento de bits en memoria. Otro formato es el *little endian*, que permite almacenar bits en orden inverso al *network byte order*, mientras que la otra posibilidad se denomina *Big endian.*

Según el modelo TCP/IP el protocolo de capa 3 permite direccionar los datagramas en la capa de red, este encabezado se superpone al datagrama manejado, es decir, las características de ruteo y transmisión. En la capa inmediatamente superior a TCP se agrega el encabezado, quedando el datagrama tal y como se muestra en la figura 2.6:

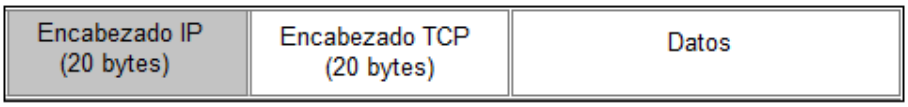

Figura 2. 6: Configuración de un datagrama IPv4. (Richard Stevens, 2011)

La longitud que tiene el encabezado IP en la capa de red es de 170 bits, que aproximadamente es 20 bytes, formada por diversos campos con distintos significados(Gordo Saez, 1998)ilustrada en la figura 2.5.Los campos descritos en la figura 2.5 se describen a continuación:

a. **Versión**, nos indica el número de la versión del protocolo de internet (IP), es decir, que para IPv4 el valor será 4.

b. **Longitud de encabezado (IHL, *Internet Header Length*)**, describe la longitud del encabezado en número de grupos de 32 bits cada uno de 4 bits.

c. **Tipo de servicio**, nos permite saber la importancia de los datos enviados, condicionando la forma en que serán tratados en la transmisión de 8 bits.

d. **Longitud total**, nos indica la longitud completa en bytes del datagrama de 16 bits, incluyendo el encabezado y los datos. En la práctica el datagrama es pequeño (16 bits) y teóricamente no será mayor a 65.535 bytes.

e. **Identificación**, utilizada para el ensamble de los fragmentos de un datagrama de 16 bits.

f. **Banderas**, es un indicador empleado en la fragmentación de 3 bits.

g. **Fragmentación**, permite ensamblar los datagramas previamente fragmentados, cuyo valor es de 64 bits (grupos de 8 bytes), inicializado en 0 para fragmento 1 de 16 bits.

h. **Límite de existencia (TTL, *Time to Live*)**, es aquel número disminuido cada vez que el paquete de datos (8 bits) pasa por un nodo de red, si el valor toma un 0 indica que el paquete se descarta. Por cuestiones de seguridad debemos evadir la

redundancia cíclica, empleado por razones de seguridad siendo improbable que esto ocurra en una red bien diseñada.

i. **Protocolo**, es un número que se emplea para definir el protocolo perteneciente al datagrama (8 bits), de tal manera que sea tratado eficientemente cuando llegue a su destino.

j. **Comprobación**, permite verificar los datos que contienen al encabezado del IP sean correctos, dicha eficiencia no se utiliza para evaluar los datos ya incluidos, sino que los datos de usuario se comprueban posteriormente del encabezado siguiente, correspondiente al nivel de capa de transporte (16 bits). Adicionalmente, si cambiamos la opción de encabezado, dicho campo será calculado nuevamente.

k. **Dirección fuente**, es aquella que contiene la dirección del usuario en la que envía el paquete de datos de 32 bits.

l. **Dirección destino**, es aquella dirección del usuario que recibe la información, es decir, que los routers o gateways (medios intermedios) conocen la dirección para llegar correctamente el paquete de datos de 32 bits.

2.4. Problemas con el protocolo de internet 4 (IPv4)

Como sabemos IPv4, es la cuarta versión del protocolo IP y dominante en Internet, que permite interconectar redes de manera interna y externa. Las principales características son:

a. **Enrutamiento y direccionamiento:** Proporciona únicamente una dirección a cada uno de los dispositivos de redes de paquetes. Es decir, que IPv4 fue principalmente diseñado para proveer el enrutamiento de información (paquetes) mediante redes de diversa complejidad.

b. **Encapsulación:** es una división antigua de TCP *(Transmission Control Protocol)*, localizado en la capa 3 del modelo ISO/OSI y funciona sobre diversos protocolos de nivel inferior.

c. **Mejor esfuerzo:** El protocolo IP provee un servicio de transmisión de paquetes no fiable(o de mejor esfuerzo). No se asegura que los paquetes enviados lleguen correctamente al destino.

IPv4 utiliza un sistema de direcciones de 32 bits $(2^{32} = 4.294.967.296)$subdivididas en cinco clases que fueron descritas en acápites anteriores. Con una simple revisión del crecimiento de INTERNET en los últimos 5 años, podemos observar que las direcciones a este ritmo se agotarán sobre los años 2012/2013 (ver tabla 2.1).

La versión de IPv4 usada actualmente en Internet no ha cambiado sustancialmente desde su publicación inicial en 1981. IPv4 ha demostrado ser un protocolo robusto, fácil de implementar y con la capacidad de operar sobre diversos protocolos de capa 2. Si bien fue diseñado inicialmente para interconectar unos pocos computadores en redes simples, ha sido capaz de soportar el explosivo crecimiento de internet.(Palet, 2007)

En aquel momento tanto el número de ordenadores conectados como las expectativas de crecimiento eran mucho más moderados de lo que han sido realmente, y por tanto la suposición de que un tamaño de 32 bits sería suficiente parecía razonable. De esta manera, podemos justificar la revisión de la versión 4 del protocolo IP desde dos puntos de vista principalmente:

1. **Técnico:** Donde el direccionamiento es insuficiente, debido a la gran demanda y que a futuro incrementa considerablemente. Las tablas de encaminamiento o de direcciones, son las encargadas de almacenar los routers internamente, y empleados para saber hacia dónde deben encaminar un datagrama, son excesivamente grandes debido a la enorme cantidad de direcciones que existen actualmente

y al sistema de encaminamiento utilizado, lo que obligaría a los routers a mantener grandes cantidades de direcciones para conocer hacia dónde deben redireccionar los datagramas.

2. **Social:** Las necesidades de los usuarios de INTERNET han aumentado espectacularmente, exigiendo nuevas capacidades (seguridad, privacidad, comercio electrónico, velocidad...) que la versión 4 no puede proporcionar.

2.5. Historia del Protocolo de Internet versión 6.

La historia de Ipv6 se inició en el año 1990, cuando se reveló que las direcciones IPv4disponibles estaban disminuyendo aceleradamente. Según estudios realizados por profesionales que indicaban que las IPv4 se agotarían alrededor del 2005. Dichos estudios fueron muy cuestionados por toda la comunidad de Internet, y es de ahí que iniciaron la búsqueda de posibles soluciones. Para ese entonces se plantearon dos soluciones:(Dunmore, 2005)

1. ***Mínimo:*** Salvaguardar el protocoloIPv4, es decir, mantenerlo intacto, sólo se debe aumentarla longitud de la dirección. Esto es muy sencillo, lo que ocurriría es tener menos suplicio en la fase de despliegue.
2. ***Máximo:*** Desplegar completamente la nueva versión del protocolo IPv6, cuyo enfoque permitiría incorporar nuevas características y mejoras en IPv4.

Debido a que no existía tanta urgencia en plantear una solución rápida, el desarrollo de un nuevo protocolo fue elegido, es decir, que el nombre original fue IPng (Próxima generación IP, IP *Next Generation*) mismo que fue desplazado por IPv6, siendo este el nombre definitivo, llevados de la mano por Steven Deering y Robert Hinden.

El primer conjunto de protocolos RFCs que rigen al IPv6, fue presentado finalizando el año 1995, dicho protocolo se lo denomino RFC 1883: Protocolo de Internet versión 6 (IPv6). Una vez que se tenía

disponible el RFC 1883 las implementaciones fueron esperadas con entusiasmo, pero nunca ocurrieron.

Para ese entonces (década del año 1990) el auge significativo de Internet en empresas causo incertidumbre entre ellas, donde tenían que resolver un complicado problema de negocio, invertir en IPv6 que traería algunos beneficios a futuro, o invertir en el despliegue de IPv4, ya que cualquiera de los dos protocolos (IPv6 e IPv4) les representarían ganancias. Finalmente la mayoría de las empresas decidieron escoger el retorno rápido y fácil de las inversiones y desarrollaron productos basados en IPv4.

Surgieron otros métodos para mantener el espacio de direcciones, el más importante es el enrutamiento sin clase entre dominios (CIDR, Classless Inter-Domain Routing), como consecuencia, los sitios recién conectados obtuvieron significativamente menos direcciones que en años anteriores. El uso del CIDR retraso la implementación de IPv6 ante los ojos de muchas personas, pero no en todos.

Aquellos sitios nuevos o en expansión desarrollaron métodos para limitar este recurso, uno de estos enfoques ha sido la traducción de dirección de red (NAT, Network Address Translation) que permitió utilizar a las redes de computadoras un número cualquiera de direcciones privadas, y para luego convertirlas en públicas cuando los paquetes dejaran el sitio y viceversa. NAT utiliza el mecanismo de compartir direcciones públicas a través de hosts, así como otros mecanismos tales como PPP (Point to Point Protocol) y DHCP (*Dynamic Host Configuration Protocol*) proporcionan un medio para que hosts alquilen direcciones por un cierto período de tiempo.

2.6. Protocolo de internet versión 6 (IPv6)

El Protocolo de Internet versión 6 (IPv6) ha sido definido por el RFC-2460, cuyo diseño ha sido para sustituir alIPv4 (RFC 791), en la

actualidad se están incorporando en la gran mayoría de dispositivos electrónicos que acceden a Internet tales como: placas de red, switches, routers y todo dispositivo de conectividad.

Steve Deering de Xerox PARC y Craig Mudge fueron los que crearon y diseñaron el protocolo de internet IPv6 destinado a sustituir a IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir e impedir el crecimiento de Internet y su uso en países de gran densidad de población como: China, India, y otros países Asiáticos, en Ecuador hay aproximadamente 7 millones de usuarios a junio 2012.

Dicha versión (IPv6) mejorará el servicio globalmente; por ejemplo, proporcionará a futuras celdas telefónicas y dispositivos móviles sus direcciones propias y permanentes, esto no sería poca cosa. A inicios del 2010 se tenía al menos 10% de IP's disponibles. Es por esto que la IANA (Agencia Internacional de Asignación de Números de Internet, por sus siglas en inglés) entregó en febrero 2011 el último bloque de direcciones disponibles (33 millones) a la organización encargada de asignar IP's en Asia, un mercado que está en auge y no tardará en consumirlas todas, por lo que hemos mencionado anteriormente, su gran crecimiento en población.

Esta nueva revisión del protocolo IP se numerará con la versión 6 y no versión 5 para evitar confusiones, ya que anteriormente se hicieron pruebas añadiendo extensiones a la versión 4. Dichas extensiones experimentales no terminaron de formalizarse con una nueva versión del protocolo, por esto fue preferible evitar posibles conflictos de numeración, razón por la cual el número de versión es 6.

Bajo estas circunstancias, IPv6 conocido también como IPng (IP de próxima generación) ofrece mayor flexibilidad y eficacia para dar soluciones a una amplia gama de nuevos problemas. Los principales objetivos que sigue IPv6 son:

a) Admitir miles de millones de equipos, superando las limitaciones de espacio para las direcciones IPv4 actuales;
b) Reducir el tamaño de las tablas de enrutamiento;
c) Simplificar el protocolo para permitir que los routers enruten datagramas de manera más rápida;
d) Brindar mejor seguridad (autenticación y confidencialidad) que la proporcionada por el protocolo IP actual;
e) Prestar más atención al tipo de servicio y, particularmente, a los servicios asociados con el tráfico en tiempo real;
f) Facilitar la difusión a destinos múltiples, permitiendo especificar el tamaño;
g) Permitir la movilidad de un equipo sin cambiar su dirección;
h) Permitir el futuro desarrollo del protocolo;
i) Posibilitar la coexistencia pacífica del protocolo antiguo con el nuevo.

2.6.1. Características de IPv6.

El protocolo de internet versión (IPv6) conserva muchas de las características que hicieron exitoso a IPv4, dentro de las cuales se puede destacar que opera sin conexiones, es decir, que cada datagrama tiene una dirección de destino y su enrutamiento es independiente. También resaltamos que como IPv4, la cabecera de cada datagrama tiene una cantidad máxima de saltos que deben de hacerse antes de descartarlo. Sin embargo existen otras características que además de ser conservadas, y que IPv6 también se encarga de mejorarlas. (Pinillos, 2003)

Existen características muy interesantes que IPv6 trae consigo, ya que resuelven muchos de los problemas de la versión 4. Las características más importantes de IPv6 se describen a continuación: (Pinillos, 2003)

a. Direccionamiento. (Pinillos, 2003)

El campo para direccionar o identificar dispositivos es de 128 bits (2128), este campo es lo suficientemente grande para manejar el

crecimiento continuo de Internet mundial durante muchas décadas. El número de direcciones IP que ofrece IPv6 es alrededor de 340 sextillones.[3]

b. Rendimiento

Actualmente, las redes LAN y WAN están progresando respecto a la velocidad de transmisión, pudiendo utilizar velocidades de ciento de Megabits por segundo con la tendencia de llegar a varios Gbps (Gigabits por segundo). Esto se debe a que la tecnología mejora día a día y la existencia de la necesidad de ancho de banda por parte de nuevos servicios y aplicaciones, en especial las basadas en gráficos.(Pinillos, 2003)

Por esta razón, los *routers* deben tener la capacidad de reenviar los datagramas IP de manera rápida y así afrontar velocidades inmensas y el incremento de carga lo más rápido y eficiente posible. Para esto es necesario plataformas de hardware robustas, así como también es importante el diseño IP que se tenga. El protocolo de internet versión 6 (IPv6) ofrece tres aspectos de diseño que contribuyen a mejorar el rendimiento de las interredes:

- La simplificación de la cabecera IP. Se reducen los trece campos presentes en IPv4 a sólo ocho campos. Esto permite a los *routers* procesar con mayor rapidez los paquetes y mejorar el rendimiento. (Lázaro & Miralles, 2004)

- Mayor eficiencia en el uso de los campos en la cabecera del paquete. Este cambio fue esencial, ya que algunos capos que antes eran obligatorios ahora son opcionales. Además, la representación de las opciones es diferente, haciendo más sencillo que los routers hagan caso omiso de opciones no dirigidas a ellos, mejorando así el tiempo de procesamiento de paquetes. (Lázaro & Miralles, 2004)

[3] Recuperado el 12 Junio 2012 online http://www.ipv6.es/es-ES/Faqs/Paginas/tecnicas.aspx

- La cabecera del paquete IPv6 es de longitud fija mientras que la cabecera de IPv4 es de longitud variable, simplificando una vez más el proceso.(Lázaro & Miralles, 2004)

- La fragmentación no se permite en lo routers IPv6. Solo puede ser realizada por el origen.(Lázaro & Miralles, 2004)

c. Servicios de red: (Pinillos, 2003)

IPv6, cuenta con un mecanismo que permite a un transmisor y un receptor establecer una trayectoria de alta calidad por la red y asociarle los datagramas, garantizando el alto desempeño a aplicaciones de audio y video en tiempo real. IPv6 permite el etiquetado de los paquetes que pertenecen a un flujo de tráfico en particular para la cual el origen solicita un manejo especial.

d. Capacidad de seguridad: (Pinillos, 2003)

IPv6 proporciona soporte nativo para seguridad basándose en sus cabeceras de extensión. Por medio de las cabeceras de autenticación y la cabecera de encapsulamiento seguro, se logra proveer diferentes niveles de seguridad para diferentes usuarios. Esto es muy importante ya que diferentes comunidades de usuarios tienen diferentes necesidades de seguridad.

e. Calidad de servicio: (Pinillos, 2003)

La calidad de servicio en IPv6, es un servicio más robusto que el provisto por datagrama llamados, Prioridad (*"priority –4 bits-"*) y Etiqueta de Flujo (*"Flow Label –24 bits-"*). Estos, son usados para que un host pueda identificar los paquetes, para el cual se requiere un manejo especial por parte de los routers IPv6. Esta capacidad es importante, para el momento de soportar aplicaciones que requieren el menor grado de retardos, *delay* o alteraciones en el flujo. Estos tipos de aplicaciones son comúnmente descritas como aplicaciones multimedia o de tiempo real.

2.6.2. Arquitectura del Protocolo de Internet versión 6 (IPv6)

La arquitectura de IPv6 es una versión mejorada de IPv4, sin modificar demasiado la estructura ni contenido, pero con cambios sustanciales en seguridad y retirando datos innecesarios o redundantes, dichos cambios se debieron a 20 años de experiencia con IPv4. La arquitectura IPv6 está conformada por una cabecera de 40 bytes fijos, una cabecera de extensión opcional que no es adicionada a la cabecera fija sino que se agrega a la carga útil en caso sea utilizada, tal como se observan en la Figura 2.7.

La nueva estructura de la cabecera del protocolo IP versión 6 se caracteriza principalmente por dos particularidades:

1. Ampliar el campo de dirección IP, es decir, de 32 bits se aumenta a 128 bits cada dirección.
2. Utilizar campos de longitud fija, facilitando así el proceso de cada datagrama en los ruteadores.

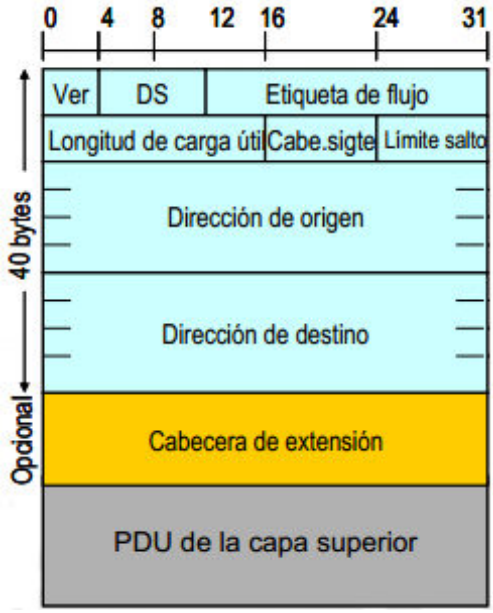

Figura 2. 7:Datagrama del IPv6.
Fuente: http://www.imaginar.org/mdi/docs/ipv6.pdf

Como se indicó anteriormente IPv6 tiene una cabecera del doble de la cabecera IPv4, esto debido al tamaño de los campos “Dirección de

origen" y "Dirección de destino". La cabecera posee los siguientes campos:

a. **Versión**, indica el número de la versión del protocolo de internet (IP), es decir, que para IPv6 el valor será 6.

b. **Longitud de carga útil *(Payload Length*)**, describe la longitud de los propios datos, llegando hasta 65.536 bytes, cuya longitud es de 16 bits, ósea, 2 bytes.

c. **Cabecera siguiente *(next header)***, emplea sucesivas cabeceras encadenadas, de ahí que desapareció el campo de opciones, cuya longitud es de 8 bits (1 byte).

d. **Límite de Saltos *(hop limit)***, cuya longitud es de 8 bits (1 byte).

e. **Clase de tráfico *(traffic class)***, conocido también como prioridad (priority) o clase (class), considerado como equivalente al TOS de IPv4, su longitud es de 8 bits (1 byte).

f. **Etiqueta de flujo *(flow label)***, permite soportar tráficos con requisitos de tiempo real, cuya longitud es de 20 bits.

g. **Dirección de origen**, contiene la dirección del usuario en la que envía el paquete de datos de 128 bits.

h. **Dirección de destino**, recibe toda la información, es decir, que los routers o gateways conocen la dirección para llegar correctamente el paquete de datos de 128 bits.

A continuación en la figura 2.8, se muestra el uso de conceptos de cabeceras de extensión, definidas en el campo siguiente cabecera, cuyo mecanismo en cada cabecera es "encadenada" a la siguiente y anterior en caso de existir:

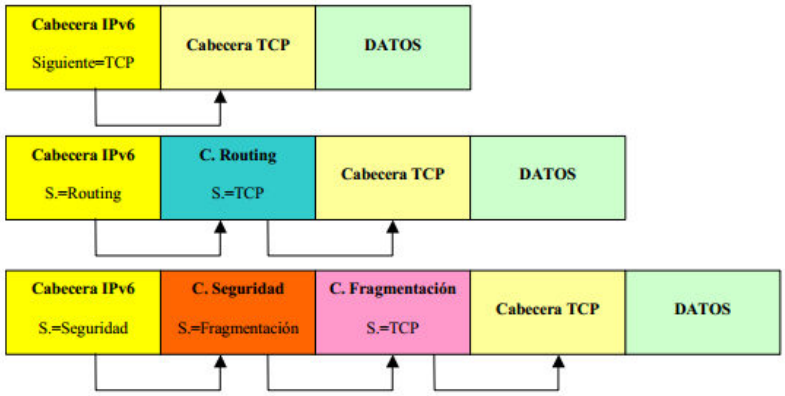

Figura 2. 8: Extensiones de cabeceras de IPv6.
Fuente: http://www.naguissa.com/universidad/wiki-td/ApuntsTema5.html

En la figura 2.9 se pueden apreciar los cambios de la cabecera IPv6 respecto a la cabecera IPv4, donde vemos que la versión no ha cambiado y esto se mantendrá porque durante un buen tiempo convivirán los dos protocolos. Otros campos fueron eliminados, tales como, tamaño de encabezado, tipo de servicio, número de identificación del datagrama, banderas, número de byte del datagrama fragmentado y el checksum se eliminaron, mientras que se refinaron otros campos como longitud del datagrama, tiempo de vida y tipo de protocolo.

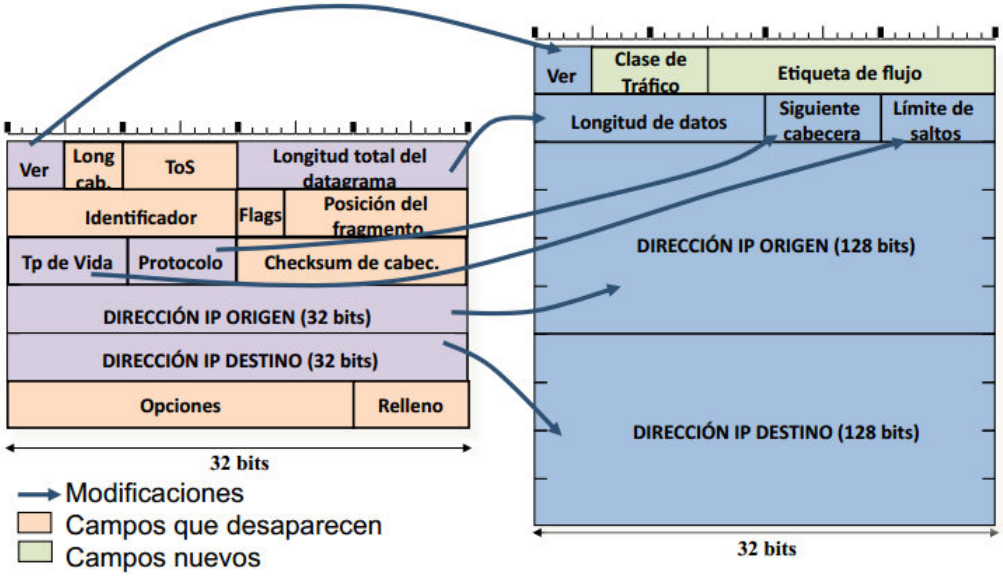

Figura 2. 9: Formato del datagrama IPv4 vs IPv6.
Fuente:

http://rodrigoaguilera.net/sites/rodrigoaguilera.net/files/miscelanea/ipv6.pdf

En la tabla 2.4 se muestran las asignaciones de número y abreviatura para que el switch o ruteador reconozca cada tipo de encabezado. Los datagramas en teoría pueden tener más de un encabezado, que por lo general no deberían tener problemas con los ruteadores, que son los encargados de procesar cada encabezado a medida de que lean al datagrama, pero sin embargo, hay otros encabezados de importancia como el encabezado de autenticación que rechaza al datagrama completamente.

Tabla 2. 4: Valores asignados para encabezados en IPv6.

Valor decimal	Abreviatura (keyword)	Descripción
0	HBH	Opciones entre saltos
4	IP	IP e IP (encapsulación en IPv4)
5	ST	Stream
6	TCP	Transmition Control Protocol
17	UDP	User Datagram Protocol
51	AH	Authentication Header
52	ESP	Encrypted Security Payload
59	NULL	No Next Header
60	DO	Destination Options Header
194	JBGR	Jumbogram

Fuente: (Gordo Saez, 1998)

Como lo indica (Verdejo Alvarez, 2000) el orden de los encabezados dependiendo de su importancia son los siguientes:

a) Encabezado IP versión 6 (IPv6 Header).
b) Encabezado de opciones entre saltos (Hop-by-hop Options Header).
c) Primer encabezado de opciones de destino (Destination Options Header).
d) Encabezado de enrutamiento (Routing Header).
e) Encabezado de fragmentación (Fragment Header).
f) Encabezado de autenticación (Authentication Header).
g) Segundo encabezado de opciones de destino (Destination Options Header).

h) Encabezado de protocolo de nivel superior (TCP, UDP).

2.6.3. Formato de direcciones IPv6.

La arquitectura del formato de direcciones IPv6 se encuentra descrita en RFC4291. Las direcciones IPv6 están compuestas por 8 campos de 16 bytes = 128 bits de largo, agrupados los bytes de 2 en 2 y separados por dos puntos ":", cuya representación es en hexadecimales (0-F), tal como se muestra en la figura 2.10.

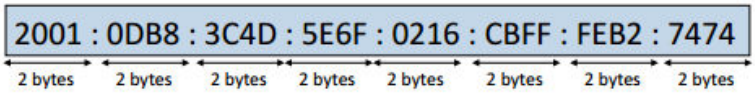

Figura 2. 10: Formato de direcciones IPv6.
Fuente:http://rodrigoaguilera.net/sites/rodrigoaguilera.net/files/miscelanea/ipv6.pdf

También se pueden simplificar el formato de direcciones IPv6 por única vez, dicha simplificación está representada por "::" para uno o varios grupos de 2 bytes a 0, tal como se muestra en la figura 2.11.

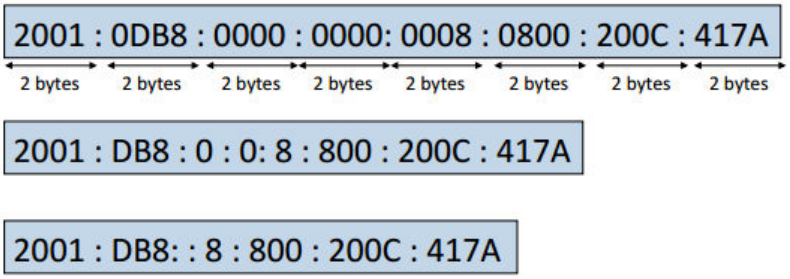

Figura 2. 11: Formato simplificado de direcciones IPv6.
Fuente:http://rodrigoaguilera.net/sites/rodrigoaguilera.net/files/miscelanea/ipv6.pdf

En la figura 2.12 se muestran los 3 campos que dividen el formato de direcciones IPv6, que son el:

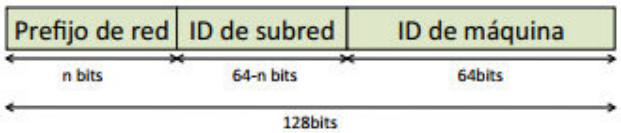

Figura 2. 12: Campos que conforman las direcciones IPv6.
Fuente:http://rodrigoaguilera.net/sites/rodrigoaguilera.net/files/miscelanea/ipv6.pdf

a) **Prefijo de red,** conjunto de direcciones asignadas a una organización, en las ISPs cuentan con prefijos de 32 bits, mientras que las organizaciones tienen 48 bits. (ver figura 2.13)

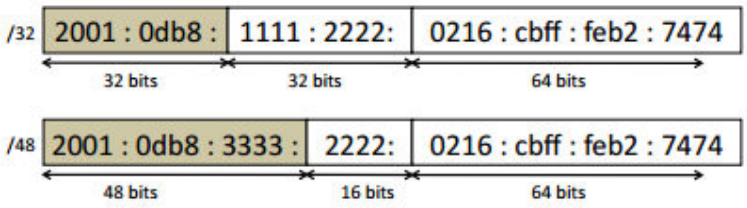

Figura 2. 13: Prefijos de red de 32 y 48 bits.
Fuente:http://rodrigoaguilera.net/sites/rodrigoaguilera.net/files/miscelanea/ipv6.pdf

b) **Identificador de subred,** se encarga de identificar una subred dentro de una organización.

c) **Identificador de máquina,** permite identificar una interfaz de una máquina dentro de una subred.

2.6.4. Direccionamiento IP v6.

Como se ha explicado con anterioridad el cambio de IPv4 a IPv6 es la falta de direcciones IPv4, es decir, que IPv6 ha hecho un esfuerzo grande para que no vuelva a pasar lo mismo, al pasar direcciones de 32 bits a 128 bits. El direccionamiento IPv6 sirve para identificar interfaces de redes (individual o grupos de interfaces) de 128 bits de longitud, por lo tanto, a una interface de nodo se le asignan varias o múltiples direcciones IPv6. Por este motivo IPv6 las clasifica en tres tipos de direcciones: Unicast, Anycast y Multicast.

2.6.4.1. Unicast

Es un identificador para una única interfaz, es decir, que el paquete enviado a una dirección *unicast* se entrega solamente a la interfaz identificada con la dirección mencionada, sin ser encaminados por ningún router.Se configuran automáticamente, tal como muestra la figura 2.14.

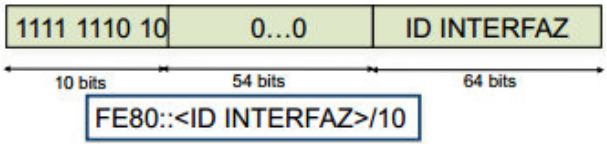

Figura 2. 14:Direccionamiento (Unicast)local de enlace.
Fuente:http://rodrigoaguilera.net/sites/rodrigoaguilera.net/files/miscelanea/ipv6.pdf

Para direcciones locales de enlace en Ethernet, se construye un identificador de interfaces utilizando las direcciones MAC de una tarjeta Ethernet, tal como muestra la figura 2.15.

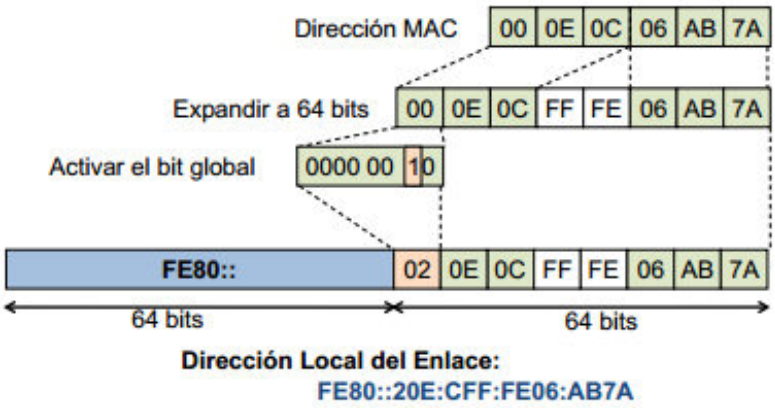

Figura 2. 15: Direccionamiento (Unicast) local de enlace en Ethernet.
Fuente:http://rodrigoaguilera.net/sites/rodrigoaguilera.net/files/miscelanea/ipv6.pdf

En la figura 2.16 se puede apreciar la aplicación de direccionamiento unicast, en la que el equipo transmite uno o varios paquetes a un único destino.

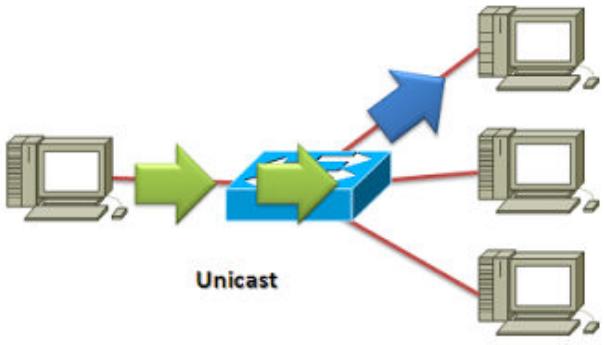

Figura 2. 16: Direccionamiento Unicast.
Fuente: http://blog.capaocho.net/2009/12/introduccion-al-multicast-parte-i.html

En este caso, IPv6 introduce el uso de contextos en las direcciones unicast, los mismo que definen el dominio lógico o físico de una red. De tal manera, reconoceráel contexto al que corresponde una determinada dirección permitiendo realizar un manejo óptimo de los recursos de la red, así optimizando su desempeño.(Jara, 2009)

Existen varios tipos de direcciones IPv6 *Unicast* que pueden pertenecer a uno de los tres contextos existentes: *Link-Local* (Local de enlace)*; Unique-Local* (Locales únicas)*; y Global Unicast* (Globales).

- ***Link-Local:*** Estas direcciones identifican interfaces en un mismo enlace. (Capa 2)[4]
- ***Unique-Local:*** Son direcciones que identifican interfaces en un mismo sitio o área topológica compuesta por varios enlaces o dominios de la capa 2.[5]
- ***Global Unicast:*** Son direcciones que identifica interfaces en toda la Internet.[6]

La figura 2.17 nos muestra la estructura jerárquica de los contextos *Unicast.* En donde el contexto global es el más grande y comprende los dos contextos restantes.

Figura 2. 17: Contextos de direcciones Unicast.
Fuente: http://www.uji.es/bin/docs/projectes/ipv6/ipv6p.pdf

Es importante recalcar que en IPv6 una interfaz puede tener más de una dirección IP.

[4] Recuperado el 12 Junio 2012 online http://www.uji.es/bin/docs/projectes/ipv6/ipv6p.pdf
[5] Recuperado el 12 Junio 2012 online http://www.uji.es/bin/docs/projectes/ipv6/ipv6p.pdf
[6] Recuperado el 12 Junio 2012 online http://www.uji.es/bin/docs/projectes/ipv6/ipv6p.pdf

2.6.4.2. Anycast

Es un identificador de múltiples interfaces (generalmente diferentes nodos), donde los paquetes destinados a una dirección *anycast* se entregan a una sola interfaz, por lo general, la más cercana dentro del grupo de direcciones *anycast*. Ahora, si la dirección multicast define la comunicación <<uno>> a <<muchos>>, una dirección *anycast* se definiría como <<uno>> a <<uno-entre-muchos>>.

Por ejemplo, permite crear ámbitos de redundancia, de tal manera que varias computadoras pueden ocuparse del mismo tráfico de acuerdo a la secuencia determinada por el router, siempre que la primera caiga. Las *anycast* no tienen un espacio propio dentro del direccionamiento IPv6, utilizan el mismo espacio que las direcciones unicast, es decir, si en todas las máquinas a las que se quiere asignar la dirección *anycast* se encuentran en la misma organización, la dirección *anycast* tendrá el mismo prefijo que las direcciones *unicast* de ese sitio, tal como se ilustra en la figura 2.18.

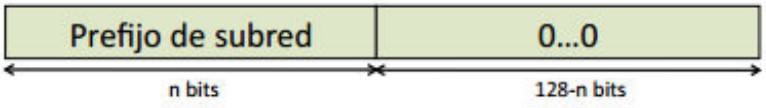

Figura 2. 18: Direccionamiento (Anycast) de los routers.
Fuente:http://rodrigoaguilera.net/sites/rodrigoaguilera.net/files/miscelanea/ipv6.pdf

Para el caso de los routers que pueden soportar direcciones para subredes que se encuentren conectadas (ver figura 2.19). La utilidad de las direcciones *anycast* sirven para implementar mecanismos, tales como:

- Comunicación con el servidor más cercano, donde las direcciones permiten a los usuarios comunicarse con uúnico servidor seleccionado por la red y que sea el más cercano.
- Descubrimiento de servicios, es decir, que si configuramos un nodo con IPv6 no hay necesidad de especificar la dirección del servidor DNS, Proxy, etc..
- Movilidad, son aquellos nodos que se comunican mediante un router de los disponibles en la red.

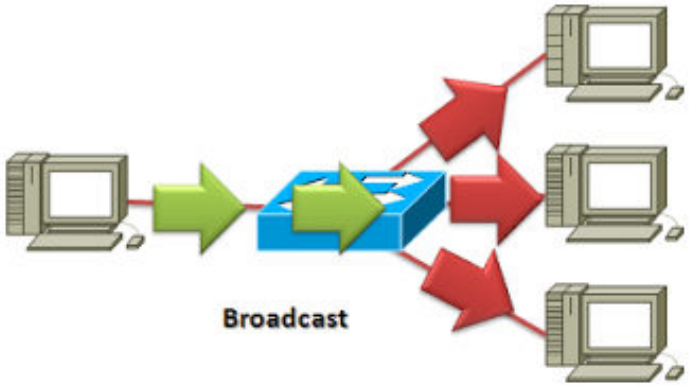

Figura 2. 19: Direccionamiento Anycast.
Fuente:http://blog.capaocho.net/2009/12/introduccion-al-multicast-parte-i.html

2.6.4.3. Multicast

Es un identificador para múltiples interfaces, es decir, que un paquete se envia a una dirección multicast, se entrega a todas las interfaces identificadas por dicha dirección, muy utilizadas para aplicaciones de retransmisión múltiple (broadcast). El direccionamiento *multicast* pertenece a uno o varios grupos, cuyo formato es el mostrado por la figura 2.20.

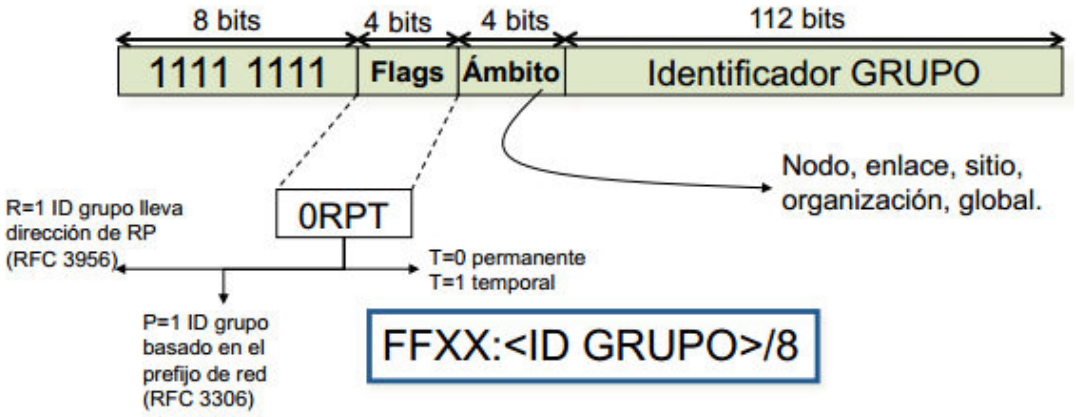

Figura 2. 20: Direccionamiento (Multicast) para retransmisión múltiple.
Fuente:http://rodrigoaguilera.net/sites/rodrigoaguilera.net/files/miscelanea/ipv6.pdf

En IPv6 se requiere que todos los nodos soporten *multicast,* ya que el nuevo protocolo ofrece muchas funcionalidades que usan este tipo de direcciones.(Regis dos Santos, Moreiras, Reis, & Soares da Rocha, 2010)

De la figura 2.20, los primeros 8 bits significa que es una dirección multicast; para los siguientes 4 bits, el bit “T” indica que si T=0 se trata de una dirección permanente y si T=1 nos indica que hay una dirección temporal. En la tabla 2.5 se describe el significado de cada uno de los bits de ámbito. Para el identificador de grupo, permite identificar al grupo multicast referido, ya sea de manera permanente o temporal, dentro de un determinado ámbito.

Las direcciones *multicast* envían un único paquete a varios host, por lo tanto podemos decir que cumplen una función similar a la de *broadcast*, sin embargo, se diferencian solo porque en el caso de las direcciones *multicast* un grupo de *hosts* reciben el paquete, mientras que en las de *broadcast* el paquete se envía a todos los *hosts* de la red sin excepción. (Regis dos Santos, Moreiras, Reis, & Soares da Rocha, 2010)

Esta clase de direcciones no deben ser empleadas como dirección de origen de un paquete. Las direcciones *multicast* proceden del bloque FF00::/8, donde el prefijo FF, que identifica una dirección *multicast*, es precedido por cuatro bits, los mismos que representan cuatro *flags*, y un valor de cuatro bits que definen el alcance del grupo *multicast*. Los 112 bits restantes se utilizan para identificar el grupo *multicast*.(Regis dos Santos, Moreiras, Reis, & Soares da Rocha, 2010)

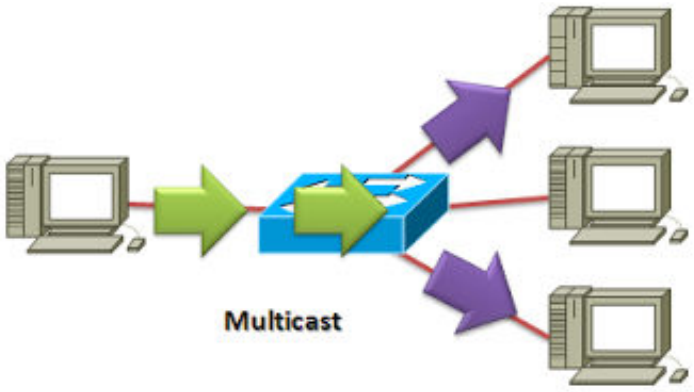

Figura 2. 21: Direccionamiento Multicast.
Fuente:http://blog.capaocho.net/2009/12/introduccion-al-multicast-parte-i.html

En la figura 2.21 se puede apreciar la aplicación del direccionamiento multicast. Si la asignación de direcciones multicast es de manera permanente, el identificador de grupo 101 (en el sistema hexadecimal) hacia el grupo de servidores de tiempo (NTS), entonces:

- ✓ FF01::101, todos los NTS en el mismo nodo que el paquete original.
- ✓ FF02::101, todos los NTS en el mismo enlace que el paquete original.
- ✓ FF05::101, todos los NTS en el mismo sitio que el paquete original.
- ✓ FF0E::101, todos los NTS en internet.

Tabla 2. 5:Significado de los bits de ámbito.

Valor Hexadecimal	Descripción
0	Reservado
1	Ámbito Local de Nodo
2	Ámbito Local de Enlace
3	No asignado
4	No asignado
5	Ámbito Local de Sitio
6	No asignado
7	No asignado
8	Ámbito Local de Organización
9	Jumbogram
A	No asignado
B	No asignado
C	No asignado
D	No asignado
E	Ámbito Global
F	Reservado

Fuente: www.6bone.net

Ahora para el caso de dirección multicast de nodo solicitado, se debe asociar entre las direcciones capa 2 (MAC) y direcciones IPv6, conocido como dirección “multicast” de nodo solicitado. La mencionada

dirección contiene parte de la direcciónIPv6 que deseamos consultar, cuya estructura descrita se asemeja a la figura 2.21.

Un nodo que se configura con direcciones IPv6, permite unirse de manera automática al multicast (grupo)de acuerdo a la dirección de nodo solicitado. Puesto que dicha dirección toma solamente los 24 bits últimos de la dirección IPv6.En la Tabla 2.6se describen algunas direcciones IPv6 y sus correspondientesdirecciones multicast de nodo solicitado.

Tabla 2. 6:Esquema de direcciones multicast de nodo solicitado

Dirección IPv6 solicitado	Dirección multicast de nodo
2800:270:bcd0:3::1	ff02::1:ff00:1
2800:270::1230:1000:a34:9e9a	ff02::1:ff34:9e9a
2800:270::34de:2000:a34:9e9a	ff02::1:ff34:9e9a
fc00:0:0:1::aaaa:a1	ff02::1::ffaa:a1

Fuente: www.6bone.net

2.7. Traductores de direcciones de red (NAT) en IPv6.

Para las NAT es necesario recordar la nomenclatura establecida por la Empresa CISCO, la misma que diferencia entre direcciones IP manejadas internamente en una red y de las que acceden al internet, en otras palabras, se refieren al intranet (direcciones locales) e internet (direcciones globales). Para el caso de las direcciones locales como se vio anteriormente son únicas para cada empresa, aunque esto no impide que otra empresa tengan las mismas direcciones sin ocasionar conflictos en Internet; mientras que las direcciones globales son únicas en la Internet.

Actualmente en muchas empresas ecuatorianas que emplean como red *backbone* de Internet están teniendo problemas, afectando así a los usuarios finales, todo esto ocurría con direccionamiento IPv4, es decir, que la empresa no podía resumir sus direcciones porque las tablas de ruteo se expandían demasiado. Si una empresa no puede acceder a

direcciones globales en la Internet, evidentemente se ve obligada a generar direcciones locales para uso interno de la red (intranet de la empresa).

Capítulo 3: Propuesta del Mecanismo de Transición a IPv6

En el presente capítulo se describen los mecanismos de transición que permiten operar redes cuyas direcciones pertenecen a los protocolos versión 4 (IPv4) y versión 6 (IPv6), dichos mecanismos deben ser implementados por las operadoras del servicio de internet (ISP) debido a la poca disponibilidad de direcciones IPv4. A través de la Superintendencia de Telecomunicaciones (SUPERTEL) y conjuntamente con Ministerio de Telecomunicaciones (MINTEL) se regulará y controlará el cumplimiento de adoptar los mecanismos necesarios para la transición temporal y que a futuro con llevará a una migración total a IPv6.

3.1. La transición de IPv4 a IPv6

Los mecanismos para realizar la transición del protocolo de internet versión 4 (IPv4) al de versión 6 (IPv6) no son tan fáciles como aparentan y peor aún llevar a una migración total a IPv6, por eso es recomendable ejecutar una transición en forma gradual mientras coexistan los protocolos actuales IPv4 e IPv6, debido a que más adelante cambiaran de direcciones de 32 a 128 bits, sin necesidad de suspender servicios.

Los mecanismos de transición de IPv4 a IPv6 que se describirán para la ejecución por parte de las operadoras o proveedoras del servicio de internet, denominadas ISP, no serán posibles de realizar sino adquieren equipos robustos y algunas aplicaciones, que muchas veces dependen de la capacidad de procesamiento de paquetes generados por los dos protocolos IPv4 e IPv6. Dicho proceso de ejecución del mecanismo que junto a los nombres de dominio del sistema (por sus siglas en ingles DNS, Domain Name System) permiten traspasar los dominios actuales para direcciones de 128 bits.

En países desarrollados como los del continente europeo se han evaluado ciertos mecanismos para la coexistencia entre ambos protocolos, lo que permitirá acá en el Ecuador una migración progresiva

de las redes así como los equipos de usuarios. Existen tres mecanismos de transición:

a. Dual Stack.
b. Túneles.
c. Traducción.

Cada una de las empresas proveedoras (ISPs) tienen la mayoría de clientes o usuarios, mismos que necesitan una conectividad para acceder a cuentas de correo electrónico (e-mail), bases de datos y aplicaciones para servidores locales, para algunos lo ideal sería en ejecutar la migración, pero para la mayoría de entendidos en el tema lo ideal en la actualidad es la transición para grupos de trabajo denominados islas y departamentos de redes de computadoras en Ecuador, y a futuro una migración total a medida que los usuarios vayan incrementándose e incluyendo equipos que soporten el protocolo de internet versión 6 (IPv6).

En este contexto de migración a IPv6, surgen nuevos términos con los cuales se designa a ciertos tipos de nodos, los cuales son:

a. **Nodo IPv4 únicamente**, el cual puede ser un host o un enrutador que implementen únicamente IPv4.

b. **Nodo IPv6/IPv4**, el cual es un host o enrutador que implementan los dos protocolos IPv4 e IPv6.

c. **Nodo IPv6 únicamente**, el cual puede ser un host o un enrutador que implemente únicamente IPv6.

d. **Nodo IPv6**, el cual puede ser un host o enrutador que implemente IPv6. Los nodos IPv6/IPv4 y nodos IPv6 únicamente son nodos IPv6.

e. **Nodo IPv4**, el cual puede ser un host o enrutador que implemente IPv4. Los nodos IPv6/IPv4 y nodos IPv4 únicamente son nodos IPv4.

3.2. Tipos de mecanismos de interconexión de IPv4 a IPv6

Más allá de los mecanismos que se utilicen para ser implementados por hosts y routers IPv6, cuya clave de éxito es que deben ser compatibles con IPv4, agilitando la expansión de IPv6 en el Internet, lo que facilita así la transición. Dichos mecanismos son diseñados para ser ejecutados por hosts y routers IPv6 que requieran interactuar con hosts IPv4 y empleen la infraestructura de enrutamiento IPv4.

3.2.1. Dual IP Layer

Conocido también como doble capa IP la cual permite proveer hosts y routers el soporte completo para ambos protocolos IPv4 e IPv6, es decir, que un dispositivo con ambas pilas pueden recibir y enviar tráfico a nodos que soportan uno de los dos protocolos, como se ilustra en la figura 3.1. Se puede configurar de forma manual cuando el usuario conoce la dirección IPv6 del nodo destino.

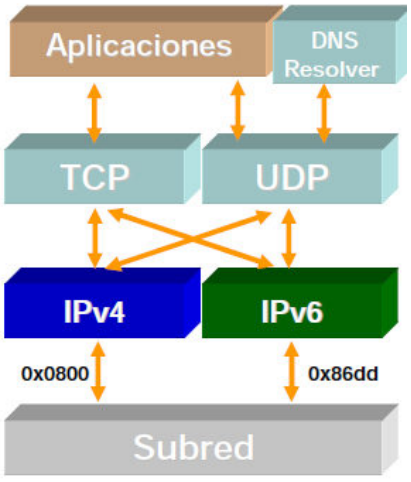

Figura 3. 1: Esquema del mecanismo Dual IP Layer.
Fuente: http://www.redesymas.org/2011/06/mecanismos-de-transicion-basicos-ipv4.html

Una pila habilitada tiene una dirección IP asignada, donde el nodo IPv6/IPv4 puede operar de tres modos distintos:

a. Con la pila IPv4 habilitada pero la pila IPv6 deshabilitada
b. Con la pila IPv6 habilitada pero la pila IPv4 deshabilitada
c. Con las dos pilas habilitadas

Esto es debido a que los nodos soportan tanto IPv4 como IPv6, los mismos que adquieren direcciones con métodos propios, por ejemplo para obtener su dirección IPv4 utiliza DHCP, y el mismo nodo para obtener su dirección IPv6 utiliza DHCPv6.

La otra configuración es utilizando nombre de dominio completamente configurado (FQDN) en un servidor DNS con ambas direcciones IPv4 e IPv6. La desventaja es que hay que tener las tablas de enrutamiento y el soporte para IPv4 e IPv6.

3.2.2. Tunneling IPv6 over IPv4.

Conocido como túneles IPv6 sobre IPv4 la cual permite encapsular paquetes de IPv6 dentro de los encabezados (headers) de IPv4 para ser transportados sobre estructuras de enrutamiento actuales, mediante dos tipos de túneles los configurados y automáticos. En realidad IPv6 es una infraestructura en evolución constante, es decir, que mientras se desarrolla y expande IPv6 va a existir el enrutamiento actual IPv4, que permitirá transportar un tráfico en IPv6, para lo cual el proceso de lograr esto es los túneles (Tunneling) que se muestra en la figura 3.2.

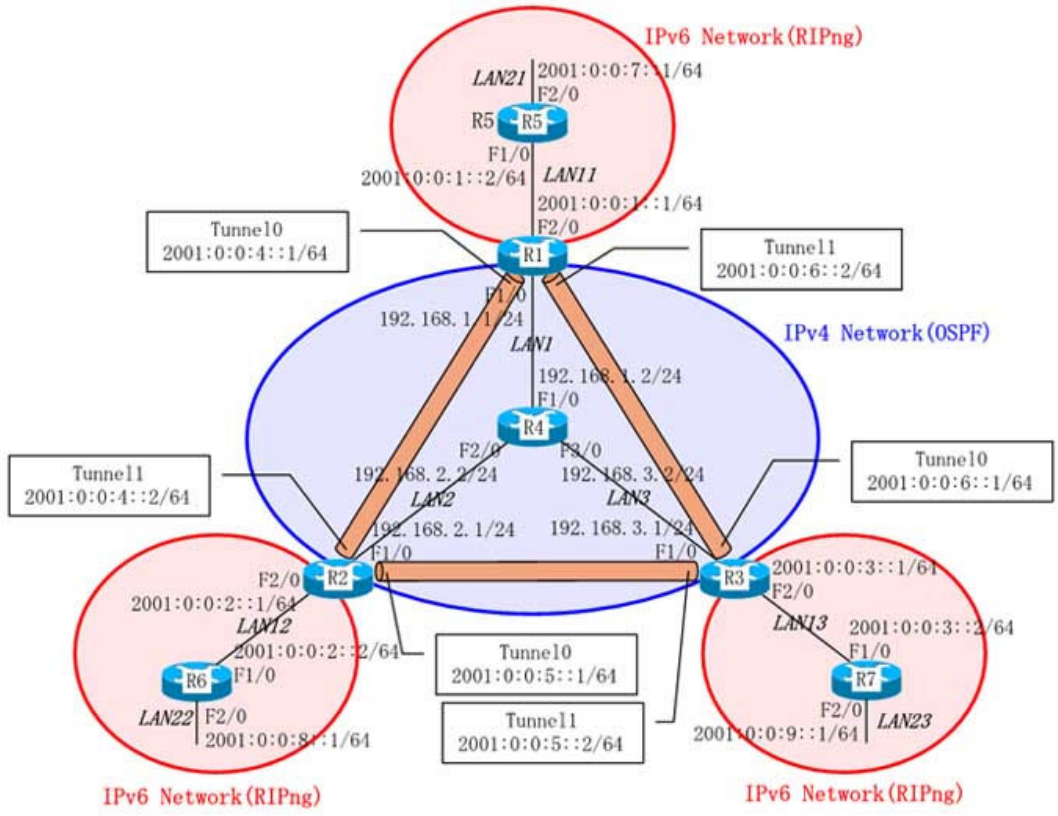

Figura 3. 2: Esquema del mecanismo Tunneling IPv6 over IPv4.
Fuente: http://www.dynalconf.org/30-1_ipv6_ipv6_over_ipv4/index.html

Tanto hosts como routers de IPv6/IPv4 permiten enviar datagramas IPv6 sobre regiones cuya topología de enrutamiento sea IPv4, encapsulándolos dentro de paquetes IPv4. Los túneles (Tunneling) pueden ser empleados en una variedad de formas, que se describen a continuación:

- ***Router to Router***: Los routers IPv6/IPv4 interconectados con una infraestructura IPv4 pueden pasarse entre sí paquetes IPv6. En este caso el túnel abarca un segmento del trayecto que toma el paquete IPv6 tal como se muestra en la figura 3.3.

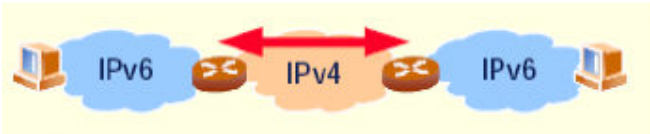

Figura 3. 3: Esquema del mecanismo Router to Router.
Fuente: J. Coellar y J. Cedeño.

- ***Host to Router:*** Los host IPv6/IPv4 pueden pasar paquetes IPv6 por un router IPv6/IPv4 intermediario que sea alcanzable por la infraestructura IPv4. Este tipo de túnel abarca el primer segmento del trayecto del paquete, como se muestra en la figura 3.4.

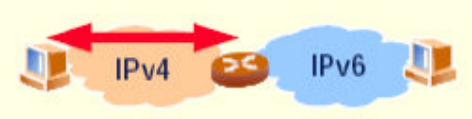

Figura 3. 4: Esquema del mecanismo Host to Router.
Fuente: J. Coellar y J. Cedeño.

- ***Host to Host***: Los hosts IPv6/IPv4 interconectados con una infraestructura IPv4 pueden pasarse paquetes IPv6 entre sí. En este caso el túnel abarca el recorrido completo que toman los paquetes, como se muestra en la figura 3.5.

Figura 3. 5: Esquema del mecanismo Host to Host.
Fuente: J. Coellar y J. Cedeño.

- ***Router to Host***: Los routers IPv6/IPv4 pueden pasar paquetes IPv6 hasta su hostIPv6/IPv4 destinatario (final). Este túnel abarca el último segmento del recorrido, tal como se ilustra en la figura 3.6.

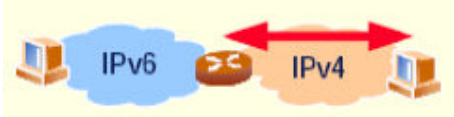

Figura 3. 6: Esquema del mecanismo Host to Host.
Fuente: J. Coellar y J. Cedeño.

En los casos ***Router to Router*** y ***Host to Router*** el paquete IPv6 es pasado mediante el túnel a un router. El punto final (endpoint) para estos tipos de túneles es emplear un router intermediario, el mismo que debe desencapsular el paquete IPv6 y reenviarlo a su destino final. Si enviamos paquetes de datos a un router, el endpoint del túnel es diferente del destino final del paquete que se ha enviado.

Para los dos últimos casos ***Host to Host*** y ***Router to Host***, el endpoint del túnel es el nodo para el cual el paquete IPv6 se ha direccionado. Es decir, que el endpoint se determina por la dirección IPv6 de destino del paquete de datos. En consecuencia, si es una dirección IPv6 compatible con IPv4 entonces los últimos 32 bits describen la dirección del nodo destino y empleado como dirección del endpoint del túnel, por lo tanto esta técnica se denomina ***tunneling automático***.

3.2.2.1. Encapsulamiento.

Para las técnicas de encapsulación normalmente se clasifican dependiendo del mecanismo del nodo encapsulador para determinar la dirección del otro extremo del túnel. Es decir, que si el extremo del túnel resulta ser un router, éste desencapsula el paquete para posteriormente reenviarlo a su destino final. De tal manera, que el extremo del túnel puede no coincidir con el destino del paquete ya encapsulado.

Para el encapsulamiento de datagramas IPv6 sobre una red IPv4 se requiere utilizar el número de protocolo IPv4 41.Tanto el host o router se comportan como un nodo encapsulado y para el proceso inverso, es decir, el desencapsulado puede ser también cualquiera de los dos. El datagrama IPv6 es puesto dentro de la carga útil de un datagrama IPv4, tal y como se muestra en la figura 3.7.

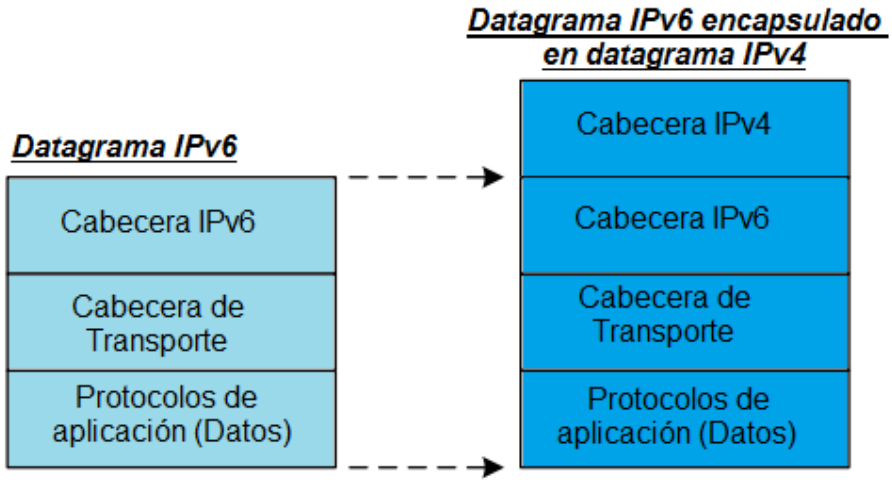

Figura 3. 7: Encapsulamiento del datagrama IPv6.
Fuente: J. Coellar y J. Cedeño.

Tanto la dirección origen y destino del datagrama ambas pertenecientes a IPv4, son aquellas direcciones del nodo encapsulado y desencapsulado, las misma que pueden ser o no las direcciones IPv6 origen y destino del datagrama IPv6. El proceso para el encapsulamiento de un paquete IPv6 son:

a. El punto de entrada del túnel, es decir, el encapsulador decrementa el campo IPv6, límite de saltos, en una unidad, encapsula el paquete IPv6 en la cabecera IPv4, y transmite el paquete encapsulado a través del túnel. Si fuera necesario el paquete IPv4 es fragmentado.
b. El punto de salida del túnel, es decir, el desencapsuladordesencapsula el paquete. Si el paquete fue fragmentado, lo reensambla. Luego el punto de salida remueve la cabecera IPv4 y procesa el paquete IPv6 a su destino original.

El mecanismo de encapsulamiento se clasifica en:

a. Ámbito de aplicación: Global.
b. Requisitos de IPv4: conectividad IPv4 entre los sitios.
c. Requisitos de las direcciones IPv4: >=1 por sitio.
d. Requisitos de IPv6: ninguno.
e. Requisitos de las direcciones IPv6: los nodos finales requieren una dirección IPv6.
f. Requisitos de máquina: pila IPv6 o doble pila.
g. Requisitos de router: doble pila.
h. Impacto del NAT: no realizará actividad en la NAT debido a que ambos extremos del túnel deben ser enrutables, aunque puede operar si dichos extremos se encuentran en el NAT.
i. Otros requisitos: No.

3.2.2.2. Túnel automático.

Los túneles automáticos emplean direcciones IPv6 de destino que son compatibles con IPv4, es decir, que el paquete de datos puede ser enviado sin inconvenientes. Ahora, si la dirección IPv6 de destino resulta

ser una dirección nativa, entonces el paquete no puede ser enviado mediante el túnel automático. Para esto es necesario las tablas de rutas que permiten dirigir el mecanismo, es decir, tener una ruta estática especial como por ejemplo 0:0:0:0:0:0::/96.

Los extremos finales del túnel se determinan por el uso de las interfaces lógicas del túnel, las rutas y las direcciones IPv6 de origen y destino.Este tipo de dirección IPv6 es asignada exclusivamente a los nodos que utilizan túneles automáticos, mismos que permiten a los nodos IPv6/IPv4 comunicarse por medio de la infraestructura IPv4 sin realizar la pre configuración del túnel. Por ejemplo, una dirección cuyo protocolo de internet versión 4 es 10.12.83.119, cuya dirección IPv4 es compatible a la dirección IPv6 ::10.12.83.119, donde el símbolo ':' indica que seagregaron 96 bits cuyo valor son todos ceros.

El mecanismo de túnel automático se clasifica en:

a. Ámbito de aplicación: Global.
b. Requisitos de IPv4: conectividad IPv4 entre los sitios.
c. Requisitos de las direcciones IPv4: 1 por máquina.
d. Requisitos de IPv6: ninguno.
e. Requisitos de las direcciones IPv6: compatibilidad entre direcciones IPv6 e IPv4.
f. Requisitos de máquina: doble pila.
g. Requisitos de router: ninguno.
h. Impacto del NAT: si atraviesa por una NAT no funcionará.
i. Otros requisitos: No.

3.2.2.3. Túnel Manual.

Los túneles manuales también conocidos como estáticos,necesitan ser configurados en ambos puntos finales, es decir, las direcciones origen y destino de ambos protocolos IPv4 e IPv6, adicional a esto los nodos de los puntos finales deben de tener doble pila. Los túneles manuales tienen ciertos requerimientos: **1)** Dos enrutadores deben de ser doble pila, **2)**El

enrutador de entrada debe de contar con una dirección IPv4 con la cual pueda alcanzar al enrutador de salida y viceversa.

Aunque los túneles manuales tienen desventajas, para citar una, si son varios túneles que debemos configurar, resultaría pesado realizarlo, es decir, si las direcciones IP cambian para varios túneles el trabajo también se convierte en pesado. Este tipo de túnel puede ser utilizado cuando se necesitan sólo pocos túneles y cuando no está presente el NAT de IPv4.

El mecanismo de túnel manual se clasifica en:

a. Ámbito de aplicación: Global.
b. Requisitos de IPv4: ninguno.
c. Requisitos de las direcciones IPv4: 1.
d. Requisitos de IPv6: ninguno.
e. Requisitos de las direcciones IPv6: si es un cliente aislado no lo requiere, pero si desea conectarse a una red se debe asignar un prefijo.
f. Requisitos de máquina: doble pila y navegador IPv4.
g. Requisitos de router: ninguno.
h. Impacto del NAT: si atraviesa por una NAT no funcionará, para que pueda operar sin inconvenientes el túnel del cliente debe estar ubicado en el mismo ordenador que el NAT.
i. Otros requisitos: requiere de una base de datos con los túneles actualmente en funcionamiento.

3.2.2.4. Túnel 6to4.

El presente mecanismo 6to4 se configura de maneraautomática, en la cual los extremosdel túnel son determinados por las direcciones IPv4 (ver figura 3.8)encapsuladas dentro de direcciones IPv6 6to4. Éste pertenece al protocolo RFC 3056, para que los sitios de direcciones IPv6 se comuniquen entre sí, a través de una red de direcciones IPv4, sin necesidad de contar con un túnel explícito.(Moore, 2001)

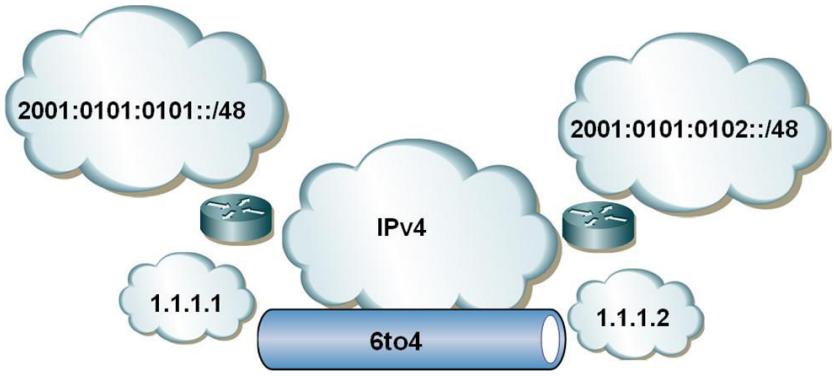

Figura 3. 8: Esquema del túnel 6to4.
Fuente: J. Coellar y J. Cedeño.

A continuación se detallan ciertas definiciones importantes:

- ✓ **Pseudo interface 6to4**. Es aquel punto que es equivalente a la interface de IPv6, donde acontece el encapsulamiento 6to4 de los paquetes IPv6 dentro de paquetes IPv4.

- ✓ **Prefijo 6to4.** Es aquel prefijo diseñado con las mismas características especificadas en el protocolo RFC 3056.

- ✓ **Dirección 6to4.** Es aquella dirección IPv6 diseñada mediante el prefijo 6to4.

- ✓ **Dirección IPv6 nativa.** Es aquella dirección IPv6 diseñada mediante cualquier otro prefijo sin provenir del 6to4.

- ✓ **Enrutador 6to4 o de borde.** Es aquel enrutador capaz de soportar pseudo interfaces del 6to4.

- ✓ **Host 6to4.** Es aquel host IPv6 que tiene por lo menos una dirección 6to4.

- ✓ **Sitio 6to4.** Es un sitio en el cual internamente se está corriendo IPv6 usando direcciones 6to4.

- ✓ **Enrutador relay.** Este es un enrutador configurado para soportar rutas con tráfico de direcciones IPv6 nativa y direcciones 6to4.

El mecanismo 6to4 se clasifica en:

a. Ámbito de aplicación: Global.
b. Requisitos de IPv4: conectividad IPv4.
c. Requisitos de las direcciones IPv4: >=1 por sitio.
d. Requisitos de IPv6: prefijo 6to4 único de forma global.
e. Requisitos de las direcciones IPv6: ninguno.
f. Requisitos de máquina: doble pila y mínimo valor de selección de direcciones fuente.
g. Requisitos de router: implementar reglas de reenvío y desencapsulación especiales.
h. Impacto del NAT: si atraviesa por una NAT no funcionará, para que pueda operar sin inconvenientes el router 6to4 es ubicado donde se encuentre el NAT.
i. Otros requisitos: prefijos de tamaño 48 bits.

El túnel 6to4 es un mecanismo temporal para la transición durante el período de tiempo en que coexistan los dos protocolos IPv4 e Ipv6, no ha sido considerada como una solución permanente. La dirección 6to4 está construida en base al prefijo 6to4 2002::/16 seguido por los 32 bits de la dirección IPv4 externa del enrutador de borde del sitio, dando como resultado un prefijo de /48.

La figura 3.9 nos muestra dos redes 6to4 de manera independientes, el Sitio A y el Sitio B. Cada uno de los sitios tienen configurados enrutadores cuya conexión externa es una red IPv4. El túnel 6to4 de una red IPv4 proporciona una conexión para vincular ubicaciones 6to4.

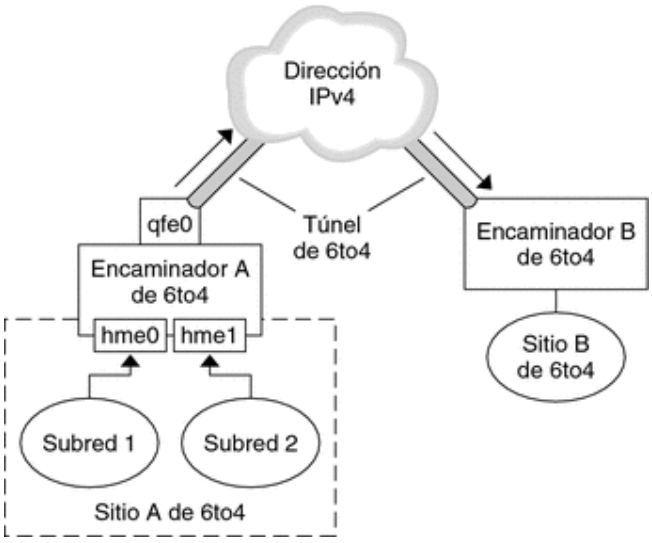

Figura 3. 9: Esquema del túnel entre dos 6to4.
Fuente: J. Coellar y J. Cedeño.

La dirección configurada en ***qfe0*** es única globalmente, donde el enrutador de límite de sistema Router A conecta la ubicación del Sitio A con la red IPv4. La interfaz ***qfe0*** configurada previamente con una dirección IPv4 antes de que sea posible configurar como una pseudointerfaz 6to4.

3.2.2.5. Túnel 6over4

Este mecanismo 6over4 que también se denomina túnel demultidifusión de IPv4, donde 6over4 permite comunicarse entre nodos IPv6 e IPv4a través de unainfraestructura IPv4. El túnel 6over4 como se mencionó utiliza la infraestructura IPv4 con capacidad de multidifusión. Para el correcto funcionamiento de 6over4, la infraestructura IPv4 debe estarhabilitada para multidifusión IPv4 ilustrada en la Figura 3.10.

Para este mecanismo se debe crear un enlace virtual a través de un grupo IPv4 multicast con ámbito local – organizacional, sin olvidarse que el mecanismo multicast en IPv4 es opcional. Mientras que las direcciones IPv6 multicast mapean direcciones IPv4 multicast para ejecutar. Para el encaminamiento entre IPv6 y el dominio 6over4 es suficiente configurar un router al menos en una de sus interfaces.

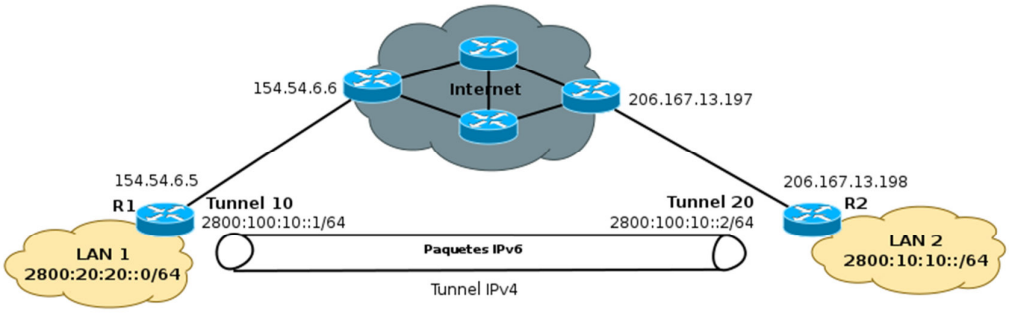

Figura 3. 10: Esquema del túnel 6over4.
Fuente: J. Coellar y J. Cedeño.

El mecanismo 6over4 se clasifica en:

a. Ámbito de aplicación: dominio.
b. Requisitos de IPv4: conectividad IPv4 multicast entre hosts.
c. Requisitos de las direcciones IPv4: 1 por host.
d. Requisitos de IPv6: ninguno.
e. Requisitos de las direcciones IPv6: doble pila.
f. Requisitos de router: configurar mecanismo 6over4 para encaminamiento entre enlaces virtuales e IPv6.
g. Impacto del NAT: mayor esfuerzo para su funcionamiento debido a que primero tendrá que habilitar el multicast IPv4 a traves de las NATs.
h. Otros requisitos: para conectar máquinas IPv6 cuyos enlaces físicos son diferentes.

3.2.2.6. Túnel Teredo

El túnel Teredo fue diseñado para garantizar las conectividades IPv6 de los nodos dual stack, localizados detrás de los dispositivos NAT sobre dominios IPv4, es decir, que define el encapsulamiento de paquetes IPv6 en datagramas UDP[7]-IPv4 para ser dirigidas a través de dispositivos NAT y en internet IPv4. El esquema que se muestra en la figura 3.11indica que

[7]UDP,(Protocolo de Datagramas de Usuario)es un protocolo que permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación, ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco sabemos si ha llegado correctamente, ya que no hay confirmación de entrega o de recepción.

un cliente se comunica a través de un túnel Teredo con hosts IPv6nativos.(Olvera, Palet, & Vives, 2008)

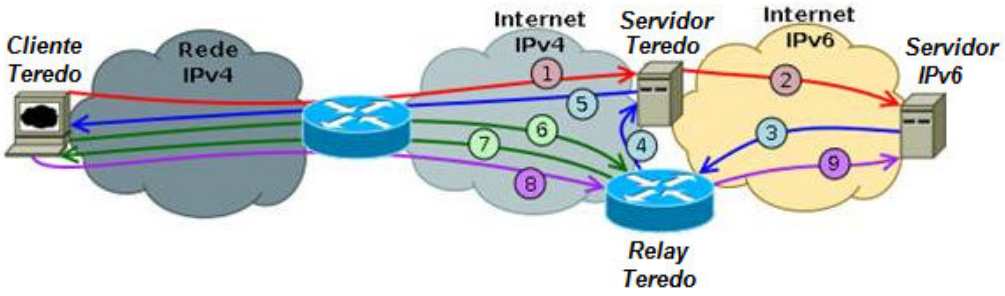

Figura 3. 11: Esquema del túnel Teredo.
Fuente: http://ipv6.br/entenda/transicao/#tecnicas-teredo

El mecanismo Teredo requieren de servidores y relays Teredo, donde los servidores por lo general no redireccionan paquetes de datos, si no que su función principal es facilitar el direccionamiento entre clientes y relays Teredo. De acuerdo al esquema de la figura 3.11, el túnel teredo consta de los siguientes elementos:

a. Cliente Teredo: se trata de un ordenador ubicado detrás de la NAT, adquiriendo la dirección IPv6 mediante el servidor Teredo, encapsulando los paquetes IPv6 en paquetes UDP para ser enviados hasta el servidor Teredo más cercano.
b. Relay Teredo: es en realidad un router, que se encarga de anunciar el prefijo IPv6 de servicio Teredo hacia la red IPv6, siendo capaz de enviar paquetes UDP sobre el protocolo IPv4 empleando como fuente la dirección IPv4 Anycast reservada para el servicio Teredo.
c. Servidor Teredo: asigna un prefijo del protocolo IPv6 para el servicio Teredo, mediante el envío de bajo demanda. Localizan direcciones del protocolo IPv4 Anycast reservada para el servicio Teredo, sin guardar estado. El servidor Teredo puede convertirse en un Relay Teredo, siendo capaz de advertir el prefijo del protocolo IPv6 de servicio Teredo en la zona del protocolo IPv6.

El mecanismo Teredo se clasifica en:

a. Ámbito de aplicación: global o de dominio.

b. Requisitos de IPv4: direcciones IPv4 Anycast deben ser topologicamente correctas, para mantener la compatibilidad con el filtro de entrada.
c. Requisitos de las direcciones IPv4: 1 dirección IPv4 Anycast para los servidores incluido el relay.
d. Requisitos de IPv6: ninguno.
e. Requisitos de las direcciones IPv6: 1 prefijo para el servidor Teredo.
f. Requisitos de máquina: ninguno.
g. Requisitos de router: ninguno.
h. Impacto del NAT: correcta funcionalidad a través de las NATs.
i. Otros requisitos: ser compatible con el filtrado de entrada de los routers.

3.2.2.7. ISATAP

El túnel ISATAP[8]permite crear túneles IPv6-in-IPv4 automáticamente dentro de un sitio IPv4. Cada host solicita a un enrutador dentro del sitio IPv4 una dirección IPv6 para obtener información de enrutamiento, de tal manera, los paquetes enviados por el protocolo IPv6 son enrutados a través del enrutador ISATAP y los paquetes destinados hacia otros hosts dentro del mismo sitio son entregados directamente mediante túneles ISATAP. (Olvera, Palet, & Vives, 2008)

Las direcciones IPv6 se configuran automáticamente mediante el protocolo “descubrimiento de enrutador” ISATAP, aunque también pueden ser configuradas de manera manual. En la figura3.12 se muestra el esquema de funcionamiento de los túneles ISATAP.

[8]ISATAP, por sus siglas en inglés IntraSiteAutomaticTunnelAddresingProtocol

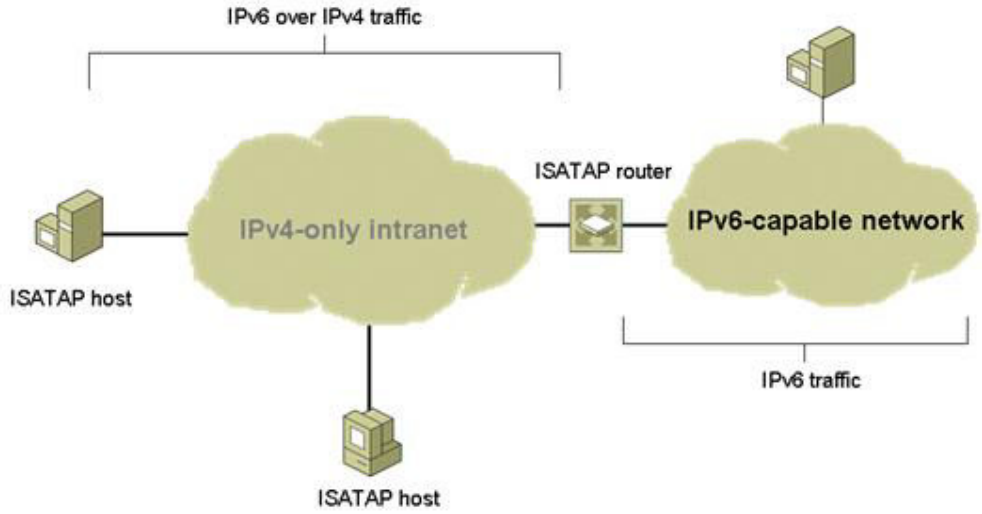

Figura 3. 12: Esquema del túnel ISATAP.
Fuente: http://www.1ask2.com/Windows7/IPv6Trans.htm

Para el mecanismo ISATAP, la comunicación se ejecuta encapsulando automáticamente los paquetes IPv6 en IPv4, es decir, que las cabeceras IPv4 son extraídas por las propias direcciones ISATAP. Los ordenadores cuyo soporte es ISATAP utilizan la estructura de datos <<*lista de routers potenciales*>>. Dicha lista aporta el descubrimiento de vecinos y valida routers existentes en los enlaces ISATAP.

En general si está habilitado un enlace ISATAP, este debe mostrar una lista de routers potenciales que se describen a continuación:

a. El administrador de dominios mantiene registros DNS para diferentes interfaces ISATAP de los routers, para lo cual se recomienda usar el dominio <<*isatap.domain-name*>>.

b. Los nodos buscan una o más direcciones de la lista, preguntando a los DNS por registros anteriores.

c. Posterior a la inicialización de la lista de routers potenciales, los nodos revisan periódicamente los registros anteriores, para poder actualizar la lista de routers.

El mecanismo ISATAP se clasifica en:

a. Ámbito de aplicación: dominio.
b. Requisitos de IPv4: ninguno.
c. Requisitos de las direcciones IPv4: 1 por máquina.
d. Requisitos de IPv6: ninguno.
e. Requisitos de las direcciones IPv6: ninguno.
f. Requisitos de máquinas: doble pila.
g. Requisitos de routers: ninguno.
h. Impacto del NAT: no hay operatividad directa de las NATs, aunque puede operar de manera privada dentro de la red gestionada por el posible NAT, es decir, que ISATAP se emplea como un mecanismo complementario.
i. Otros requisitos: el descubrimiento de vecinos implica que los nodos confían en los <<*routers advertisements*>> recibidos por los routers del mismo enlace. En otras palabras, solo son confiables los <<*routers advertisements*>> pertenecientes a la lista de routers potenciales.

3.3. Tipos de mecanismos de comunicación entre IPv4 a IPv6

Para la interconexión de islas IPv6 se pueden emplear cualquiera de los mecanismos presentados en el inciso anterior, habilitando la comunicación entre nodos IPv6, pero es necesario establecer una mejor comunicación tanto para nodos IPv6 como IPv4. Estos mecanismos se pueden realizar de algunas maneras, empleando la traducción a nivel de red e incluso mediante asignación temporal de direcciones IPv4 en una máquina u ordenador IPv6.

Los traductores de protocolos o traducción, mapean los protocolos a nivel de campos semejantes de otro protocolo. Recordemos que IPv4 tiene aplicaciones que requieren de información de la capa de red, conocida como <<*ftp*>>, es decir, que la traducción no solamente a nivel de red sino también a nivel de aplicación. La mayoría de mecanismos de comunicación entre nodos IPv4 a IPv6 que se proponen, requieren implementaciones de ambas pilas de los protocolos de red, denominadas también como <<*dual stack*>>cuyas características son:

a. Evaden túneles, ya que los routers no necesitan direcciones IPv4 sino <<*dual stack*>>.
b. Evaden traducciones, siempre que se tenga una aplicación con soporte IPv4 e IPv6.

3.3.1. Mecanismo DSTM.

DSTM por sus siglas en inglés <<*Dual StackTransitionMechanism*>>, es un mecanismo que permite a nodos <<*dual stack*>> comunicarse con otras aplicaciones solamente IPv4, aunque la pila IPv4 está habilitada pero debe configurarse para lograr dicha comunicación. En consecuencia, un nodo IPv4 e IPv6 requieren direcciones IPv4, la cual es solicitada al servidor DSTM, mientras que la comunicación entre el nodo y servidor DSTM es a través de IPv6.

En ausencia de encapsulamiento IPv4 en redes IPv6, la máquina <<*dual stack*>> encapsula paquetes IPv4 dentro de paquetes IPv6 hasta el extremo del túnel, el mismo que lo desencapsula y enviado a infraestructura IPv4. El encapsulamiento se lo realiza virtualmente, para lo cual DSTM describe la arquitectura (ver figura 3.13) siguiente:

a. Servidor DSTM, encargada de asignar direcciones IPv4 a clientes que lo soliciten.

b. Router DSTM, se encarga de realizar la encapsulación y desencapsulación de paquetes asegurando el envío de paquetes.

c. Cliente DSTM, son capaces de configurar dinámicamente su pila IPv4 y son capaces de establecer túneles IPv4 sobre IPv6.

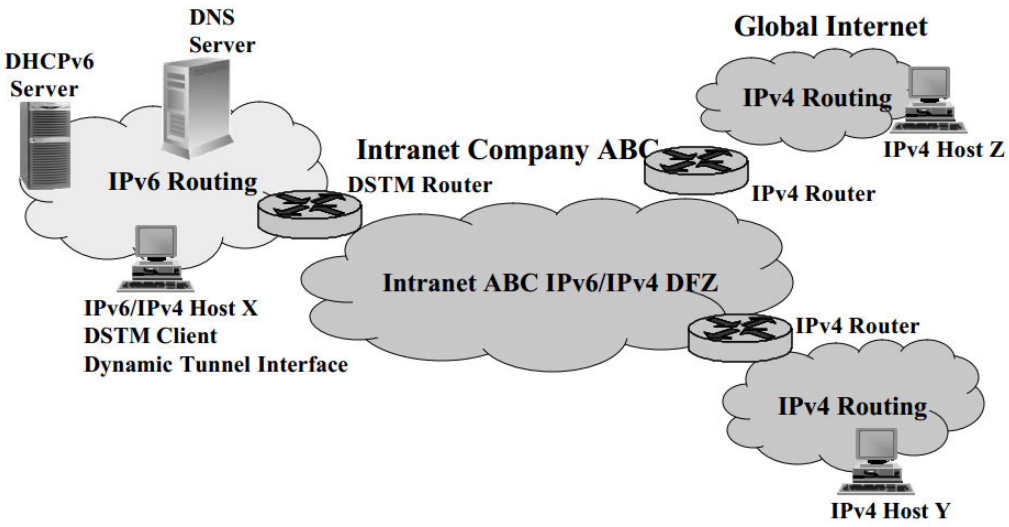

Figura 3. 13: Arquitectura DSTM.
Fuente: http://www.ietf.org/proceedings/54/slides/ngtrans-7.pdf

En la figura 3.14 se muestra el esquema del funcionamiento del mecanismo DSTM, para el cual una máquina envía paquetes IPv4 previo contacto con un servidor DSTM. Dicho servidor emplea una dirección IPv4 temporal en forma conjunta con la dirección IPv6 del TEP (Tunnel end Point), el mismo que actúa como extremo remoto del túnel. Con esto se configura la interfaz túnel del cliente origen y el encapsulamiento se produce cuando el paquete IPv4 se introduce dentro de un paquete IPv6, que ya se trata básicamente del túnel 4over6, al contrario del funcionamiento del túnel 6over4.

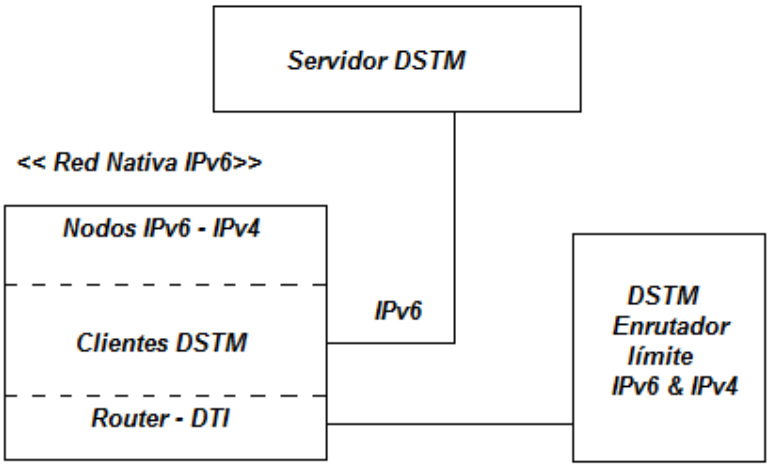

Figura 3. 14: Implementación esquemática DSTM.
Fuente: http://www.ietf.org/proceedings/54/slides/ngtrans-7.pdf

El mecanismo DSTM se clasifica en:

a. Ámbito de aplicación: dominio.
b. Requisitos de IPv4: ninguno.
c. Requisitos de las direcciones IPv4: >=1 por sitio.
d. Requisitos de IPv6: extensiones para DHCPv6.
e. Requisitos de las direcciones IPv6: ninguno.
f. Requisitos de máquinas: pila IPv4 e IPv6 con extensiones.
g. Requisitos de routers: ninguno.
h. Impacto del NAT: se comunican utilizando IPv4 aunque pueden ser penalizadas por NATs que encuentren en el camino.
i. Otros requisitos: infraestructura de encaminamiento de IPv4.

3.3.2. Mecanismo SIIT.

El mecanismo SIIT (Stateless IP/ICMP Translation Algorithm) se encarga básicamente de traducir los paquetes a nivel de red entre los nodos IPv4 e IPv6, dicha traducción se limita a la cabecera IP, es decir, que la traducción debe realizarse para cada paquete. Adicional a las direcciones IPv6 el mecanismo SIIT emplean direcciones IPv4 traducidas, haciendo uso de dos tipos de direcciones que se describen a continuación:(Nordmark, 2000)

a. Direcciones IPv4 mapeadas, del tipo **<<::ffff:a.b.c.d>>** que permiten identificar una máquina IPv4.
b. Direcciones IPv4 traducidas, del tipo <<::ffff:0:a.b.c.d>> que permiten identificar una máquina IPv6.

En el método SIIT, el nodo IPv6 obtiene direcciones temporales IPv4 y sirve como medio de enrutamiento para los paquetes. En consecuencia, las direcciones para SIIT suelen ser de tres tipos: IPv4, IPv4-traducidas o IPv4-mapeadas.El método SIIT no específica como obtiene direcciones temporales IPv4, y mucho menos como se registre su DNS. La figura 3.15 se ilustra el método SIIT empleado para la comunicación entre redes IPv6 (pequeñas) o hosts IPv6 y hosts IPv4.

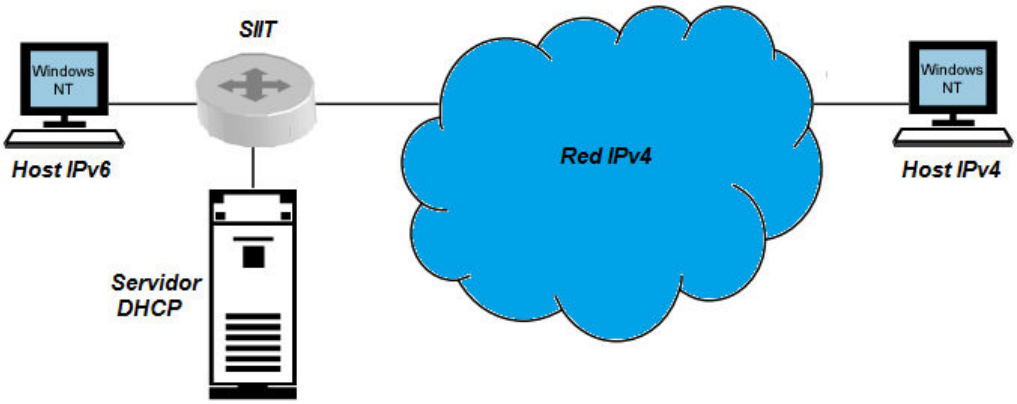

Figura 3. 15: Esquema SIIT para redes IPv6.
Fuente: http://www.faqs.org/rfcs/rfc2765.html

La figura 3.16 se ilustra el método SIIT empleado para sitios que tiene únicamente IPv6 en una red <<*dual stack*>>.

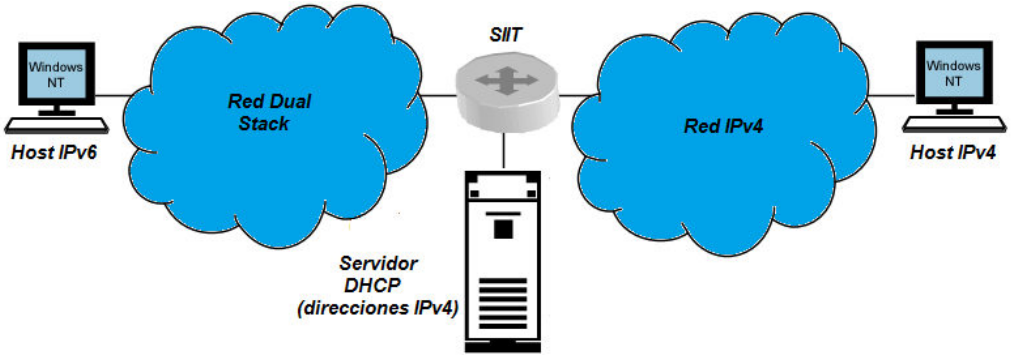

Figura 3. 16: Esquema SIIT para redes <<*dual stack*>>.
Fuente: http://www.faqs.org/rfcs/rfc2765.html

Los ordenadores que no hagan uso de los traductores SIIT, deben de modificar ciertos aspectos para implementar el protocolo IPv6, que son capaces de:

a. Permitir la transmisión y recepción de paquetes IPv6 con direcciones mapeadas IPv4.
b. Determinar si las direcciones IPv4 traducidas, deben ser asignadas o refrescadas.
c. Asegurar que el mecanismo de selección de la dirección IPv4 traducidas sólo se utilizan conjuntamente con direcciones IPv4 mapeadas.

El mecanismo SIIT se clasifica en:

a. Ámbito de aplicación: dominio.
b. Requisitos de IPv4: ninguno.
c. Requisitos de las direcciones IPv4: 1 dirección temporal por cada máquina IPv6.
d. Requisitos de IPv6: ninguno.
e. Requisitos de las direcciones IPv6: direcciones IPv4 mapeadas y traducidas que permitan identificar nodos IPv4 e IPv6.
f. Requisitos de máquinas: pila IPv6.
g. Requisitos de routers: ninguno.
h. Impacto del NAT: son traducidos los paquetes más de una vez.
i. Otros requisitos: algún mecanismo de asignación de direcciones como por ejemplo <<*dual stack*>>.

3.3.3. Mecanismo NAT-PT.

El mecanismo NAP-PT *(Network Address Translator – Protocol Translator)* es aquel que permite la comunicación entre nodos IPv6 e IPv4 (ambas son únicas y no privadas). NAP-PT es similar al método NAT que se utiliza en IPv4 pero no es idéntico, el mismo consiste en traducir una dirección IPv4 a otra dirección IPv4. Mientras que los enrutadores NAT-PT pasan todos los paquetes de una misma sesión.

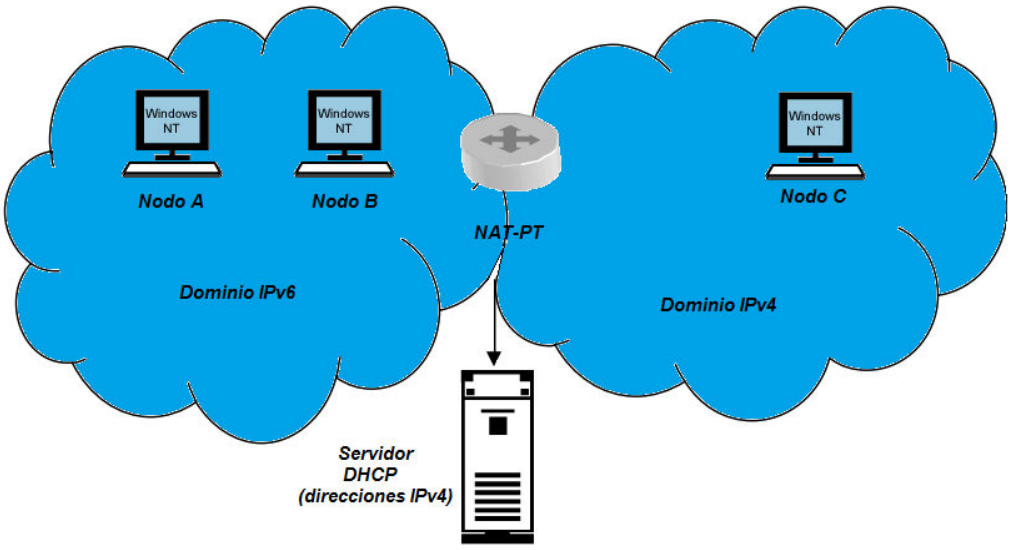

Figura 3. 17: Esquema NAT-PT.
Fuente: http://www.faqs.org/rfcs/rfc2765.html

En la figura 3.17 se ilustra el esquema básico NAT-PT, donde los Nodos A y B tienen direcciones IPv6 **(FADC:AC23::2345:1130 y FADC:AC23::2345:1131 respectivamente)**, el Nodo C tiene una dirección IPv4 (192.68.40.10) y el router NAT-PT tiene asignado un grupo de direcciones de la subred 168.130.36/34.(Tsirtsis & Srisuresh, 2000)

El funcionamiento del mecanismo NAT-PT consiste en:

a. Las direcciones IPv6 a IPv4definen direcciones falsas IPv6 empleando una dirección IPv4 de destino y anteponiendo el prefijo NAT, para poder establecer comunicaciones de datos se debe configurar en el NAT-PT con un prefijo de 96 bits. En consecuencia, el NAT-PT examina los paquetes para identificar direcciones falsas, y finalmente traduciendo el paquete a IPv4.

b. Las direcciones IPv4 a IPv6 funcionan como un NAT bidireccional, donde la traducción es semejante al inciso a), generando un paquete IPv6 con dirección origen, mientras que la dirección falsa IPv6 contiene internamente una dirección IPv4 de tal manera se inicia la comunicación.

El mecanismo NAT-PT se clasifica en:

a. Ámbito de aplicación: dominio.
b. Requisitos de IPv4: ninguno.
c. Requisitos de las direcciones IPv4: >=1 por sitio.
d. Requisitos de IPv6: ninguno.
e. Requisitos de las direcciones IPv6: ninguno.
f. Requisitos de máquinas: pila IPv6.
g. Requisitos de routers: ninguno, aunque el router puede ser NAT-PT.
h. Impacto del NAT: requieren dos o más niveles de traducción.
i. Otros requisitos: DNS dentro de una red IPv6.

3.3.4. Mecanismo BIS.

El mecanismo BIS (Bump in theStack) permite a hosts <<*Dual Stack*>>comunicarse con hosts IPv6 utilizando aplicaciones IPv4. Puede resultar muy útil para aquellas aplicaciones que no han migrado (por no tener el código fuente) a IPv6 para así establecer comunicación entre hosts IPv6. En consecuencia, cuando las aplicaciones IPv4 buscan comunicarse con aplicaciones IPv6, éste realiza el mapeo entre una dirección IPv6 y una dirección IPv4.(Tsuchiya, Higuchi, & Atarashi, 2000)

El mecanismo BIS se encarga de traducir aplicaciones IPV4 y redes situadas por debajo de IPV6, en otras palabras, nos referimos al controlador de interfaz de red. Básicamente el diseño del stack consta de una pila <<*dual stack*>>, en el cual añade tres módulos, un traductor, un nombre de laextensión de la resolución y la dirección de un mapeado, tal y como se muestra en la figura 3.18.

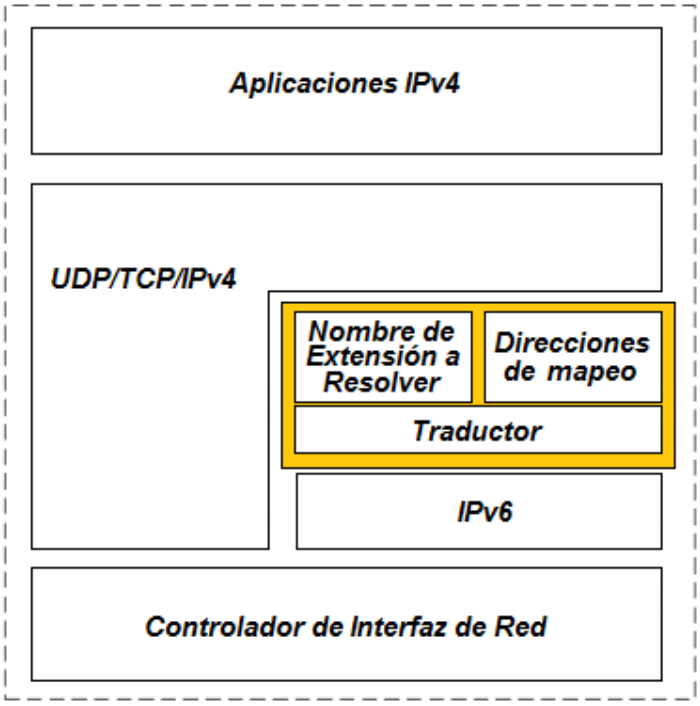

Figura 3. 18: Esquema del mecanismo BIS.(Dunmore, 2005)

El mecanismo BIS admite que hosts se conviertan en traductores autónomos, para lo cual ya no es necesario un traductor externo. El mecanismo BIS está ubicado en el área de seguridad del protocolo de

internet (IP), y posteriormente encargado de verificar datos que pasan entre TCP/IPv4 y una interface de red, además de traducirlos a IPv6 y viceversa.

El mecanismo BIS permite la comunicación de hosts IPv4 al IPv6 pero no existe comunicación IPv6 al IPv4. Imposible de enviar o recibir algún paquete IPv4 para la red, por lo que una aplicación IPv4 pretende comunicar con otra aplicación IPv4 a través del BIS, el cual produce un error si no hay mecanismos de traducción adicionales en algún lugar de la ruta de comunicación.

Al igual como ocurre con los mecanismos NAT-PT, SIIT y BPI no pueden funcionar comunicaciones multicast, ni para aplicaciones que incorporen direcciones IP en sus cargas. Una ALG (Application LayerGateway) es necesaria para cualquier aplicación que tiene este comportamiento.

Por ejemplo, una máquina implementa el mecanismo BIS actuando como originadora de la comunicación y a la vez como receptora. Se va a comentar paso a paso cuando la aplicación IPv4 intenta enviar paquetes a una aplicación en una máquina IPv6:

1. La aplicación IPv4 consulta al DNS si inicia o no la comunicación con el extremos remoto.
2. Resuelve la consulta de tipo <<*AAAA*>> procesada por el módulo <<*resolver*>>, el cual solicita al módulo de mapeo establecer la correspondencia entre direcciones IPv6 (destino) e IPv4 disponibles.
3. El nombre de extensión resolver, crea un paquete de respuesta para la aplicación de tipo A con la dirección IPv4 recién creada.
4. La aplicación detecta el destino como una dirección IPv4 y empieza el envío de paquetes.
5. El traductor captura los paquetes IPv4 a través del mapeador logrando convertir al IPv4 destino en IPv4 fuente.

6. El traductor envía el paquete IPv6 creado por el controlador de interfaz de red.
7. El paquete llega hasta la dirección IPv6 destino, el mismo que se encarga de enviar un paquete IPv6 hacia el nodo origen de la comunicación.
8. El paquete IPv6 llega hasta el nodo origen.
9. Finalmente se traduce el paquete IPv6 a través de la tabla de asignaciones del mapeador, entregando el paquete IPv4 así construido a la aplicación final.

Cuando entra en funcionamiento el mecanismo BIS se comporta como un receptor, dicha comunicación se explica paso a paso:

1. Un paquete IPv6 adquiere al nodo implementado por el mecanismo BIS.
2. La traducción obtiene el paquete y lo traduce, a través del módulo de mapeo para conseguir la correspondencia entre las direcciones IPv6 (destino) e IPv4.
3. La traducción entrega un paquete IPv4 creado en las aplicaciones IPv4.
4. Las aplicaciones IPv4 como respuesta envía un paquete IPv4 al nodo inicial de la comunicación.
5. Para el presente paso hay que seguir los pasos del ejemplo anterior.

El mecanismo BIS se clasifica en:

a. Ámbito de aplicación: host.
b. Requisitos de IPv4: ninguno.
c. Requisitos de las direcciones IPv4: espacio privado de direcciones por máquina.
d. Requisitos de IPv6: ninguno.
e. Requisitos de las direcciones IPv6: ninguno.
f. Requisitos de hosts: doble pila más extensiones.
g. Requisitos de routers: ninguno.

h. Impacto del NAT: hay presencia de una NAT aunque no hay efecto en el tráfico IPv6 debido a que las direcciones IPv4 son usadas internamente.
i. Otros requisitos: direcciones de una forma literal.

3.3.5. Mecanismo TRT.

El mecanismo TRT *(Transport Relay Translator)* especificado por el requisito RFC3142, establece que los hosts IPv6 intercambien el tráfico TCP o UDP con hosts IPv4. Es decir, que permite comunicarse directamente entre aplicaciones IPv6 e IPv4. A diferencia del mecanismo NAT-PT, el TRT actúa a nivel de la capa de transporte, y a diferencia del BIS, actúa como una pasarela entre ambos protocolos, estableciendo una conexión para IPv6 y otra para IPv4 permitiendo el reenvío de paquetes entre ambas direcciones.(Hagino & Yamamoto, 2001)

Ninguna modificación de los host es necesaria, el sistema TRT puede ser muy fácil de instalar en las redes con capacidades de IPv6.El mecanismo TRT es traducido y ejecutado en un nodo <<*dual stack*>> para así establecer la comunicación con un host (cliente) o con el servidor. Al implementar una red IPv6 es necesario mantener el acceso a todos los recursos IPv4 de redes externas, tales como servidores web IPv4 y es por este motivo que emplearemos el mecanismo de pasarela de traducción a nivel de transporte (TRT).

El mecanismo TRT posee ciertas ventajas con respecto a los demás mecanismos, como por ejemplo, no tienen problemas en traducción de cabeceras IPv4/IPv6 y de fragmentación. Las desventajas del TRT son:

1. TRT soporta únicamente tráfico bidireccional.
2. TRT requiere de un sistema de almacenamiento de estado entre los nodos IPv4 e IPv6 para poder comunicarse, similar a los sistemas NAT.
3. TRT requiere de un código especial para reenviar protocolos incompatibles con NAT (NAT-*unfriendly)*.

Las redes IPv6 e IPv4 son configuradas de tal manera que tanto los paquetes IPv6 como IPv4 son enviados a direcciones cuyos prefijos de red especiales son enrutados por un nodo remoto TRT. En la figura 3.19 TRT IPv6/IPv4permite interceptar las sesiones de transporte mediante los nodos como punto final de destino de una sesión IPv6 y envía hacia el nodo del servidor como una sesión IPv4, copiando así todos los datos recibidos en cada sesión.(Dunmore, 2005)

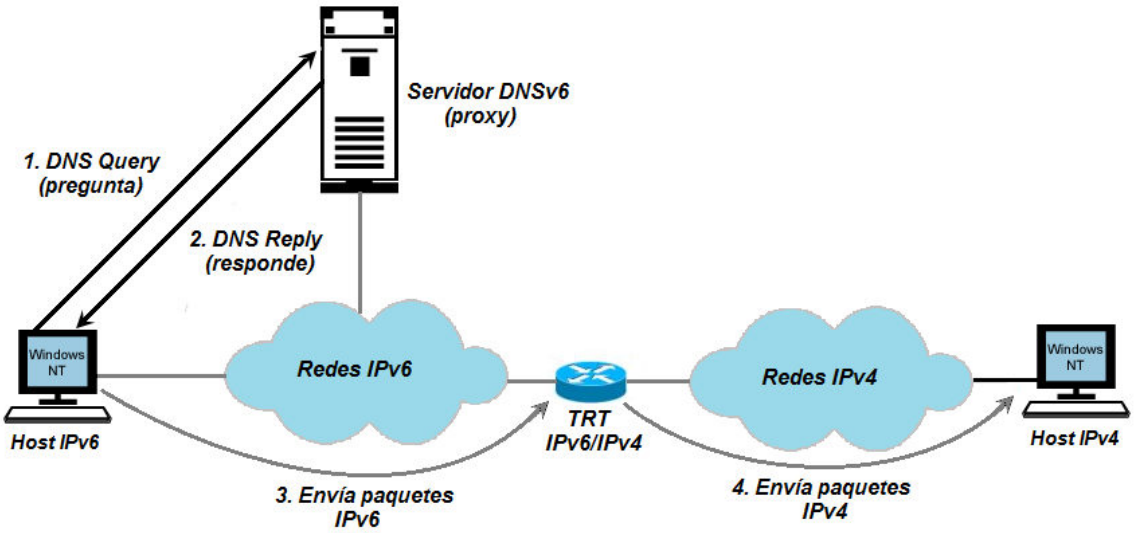

Figura 3. 19: Esquema del mecanismo TRT. (Dunmore, 2005)

El mecanismo TRT se clasifica en:

a. Ámbito de aplicación: dominio.
b. Requisitos de IPv4: ninguno.
c. Requisitos de las direcciones IPv4: 1 por sitio.
d. Requisitos de IPv6: ninguno.
e. Requisitos de las direcciones IPv6: un prefijo para encaminar los paquetes hacia el traductor.
f. Requisitos de máquinas: ninguno.
g. Requisitos de routers: ninguno, pero requiere de una máquina TRT.
h. Impacto del NAT: depende de la aplicación.
i. Otros requisitos: servidor DNS para mapeo de direcciones IPv4 a direcciones IPv6.

3.3.6. Mecanismo Socks64.

El mecanismo Socks64 se basa en el proxy SOCKS convencional, dicho mecanismo está compuesto por una puerta de enlace SOCKS implementado como un host de pila dual IPv4/IPv6 y un cliente de acogida implementado con un software llamado SOCKS LIB entre las capas de aplicación y transporte (ver figura 3.20). Esto intercepta las consultas DNS y responde con falsas direcciones IPv4, de modo que cuando el cliente hace una llamada a la conexión API, donde LIB SOCKS sustituye la dirección falsa original y envía el paquete, llamado SOCKS al proxy que realiza la actual búsqueda de DNS. (Kitamura, 2011)

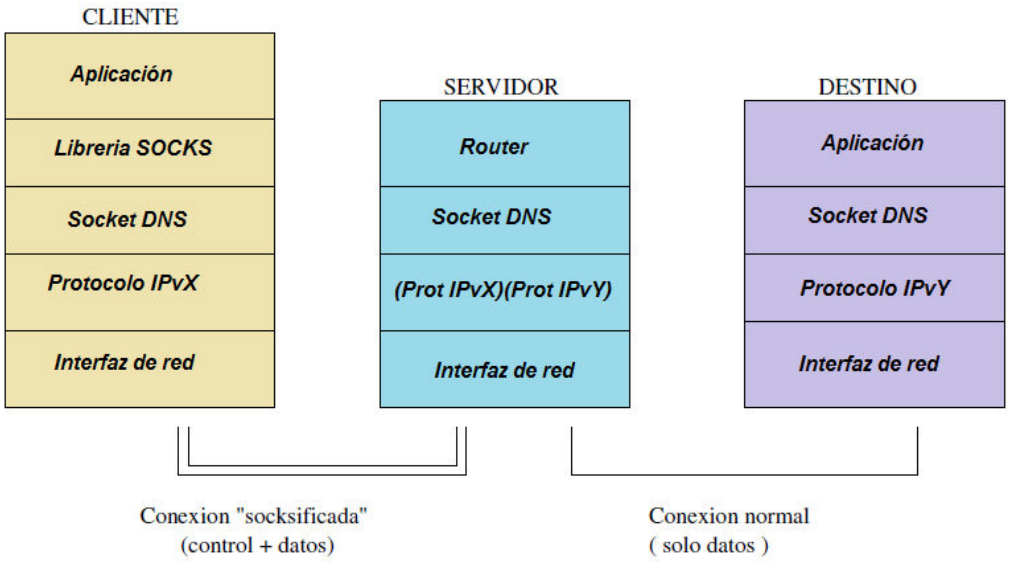

Figura 3. 20: Diagrama del mecanismo Socks. (Dunmore, 2005)

Si el servidor DNS responde con un registro AAAA, el proxy abre un socket IPv6, de lo contrario, se abre un socket IPv4. Definido en el RFC 3089, la solución SOCKS64 es bidireccional, lo que permite anfitriones hosts IPv4 e IPv6 para iniciar sesiones. Sin embargo, es necesario el uso de direcciones IPv4 públicas.

En la figura 3.21 se muestra la configuración del proxy SOCKS, el mismo que se define como un mecanismo de reenvío de la capa de transporte, permitiendo hosts con direcciones privadas o con acceso limitado a través de firewalls que puedan tener libre acceso a los recursos de Internet. Un proxy SOCKS para IPv4 se aloja por lo general en una

gran base dual con una dirección privada y otros públicos. Él recibe conexiones desde hosts internos por su interfaz IP privada y crea conexiones con servidores en Internet a través de su interfaz pública. Del mismo modo, un SOCKS64 proxy está alojado en un servidor de base dual con una dirección IPv6 y otra dirección IPv4 pública. Se puede recibir por sus conexiones de interfaz de IPv6 y redirigirlos por su interfaz IPv4 y viceversa.

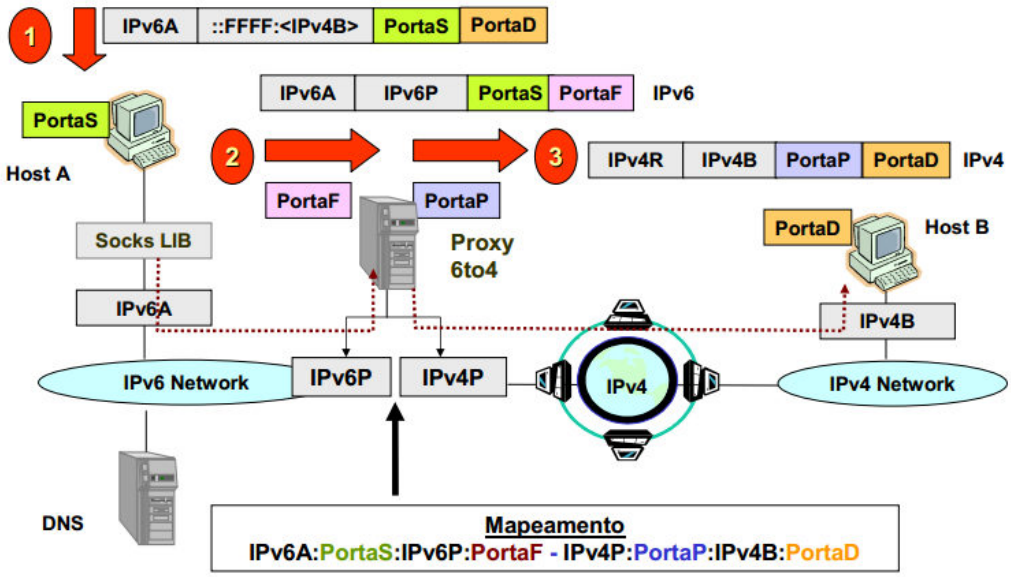

Figura 3. 21: Esquema del proxy Socks64. (Dunmore, 2005)

Esta solución puede llegar a ser la ideal en caso de que el 'sitio' esté utilizando ya SOCKS. Con un gateway de tipo SOCKS64 se puede permitir conectar a los clientes tanto a nodos IPv4 como IPv6, sin los típicos problemas asociados a los túneles (fragmentación y límite de saltos).(Kitamura, 2011)

El mecanismo Socks64 se clasifica en:

a. Ámbito de aplicación: dominio.
b. Requisitos de IPv4: ninguno.
c. Requisitos de las direcciones IPv4: 1 por pasarela o servidor Socks.
d. Requisitos de IPv6: >=1 por sitio.
e. Requisitos de las direcciones IPv6: ninguno.

f. Requisitos de máquinas: los clientes deben ser socksificados.
g. Requisitos de routers: ninguno.
h. Impacto del NAT: operación conjunta entre servidores NAT y Socks.
i. Otros requisitos: servidor Socks emplea el <<*dual stack*>>.

3.3.7. Mecanismo BIA.

El mecanismo BIA *(Bump in the API)* es muy similar al mecanismo BIS, dicho mecanismo agrega una API de traducción entre el API de socket y módulos TPC/hosts IP pila dual, permitiendo aplicaciones de comunicación con anfitriones IPv4 e IPv6, lo que refleja las funciones de la toma en socket IPv4 a IPv6 y viceversa.

El mecanismo BIA está descrito por el RFC 3338, en la cual tres módulos son añadidos (ver figura 3.21):

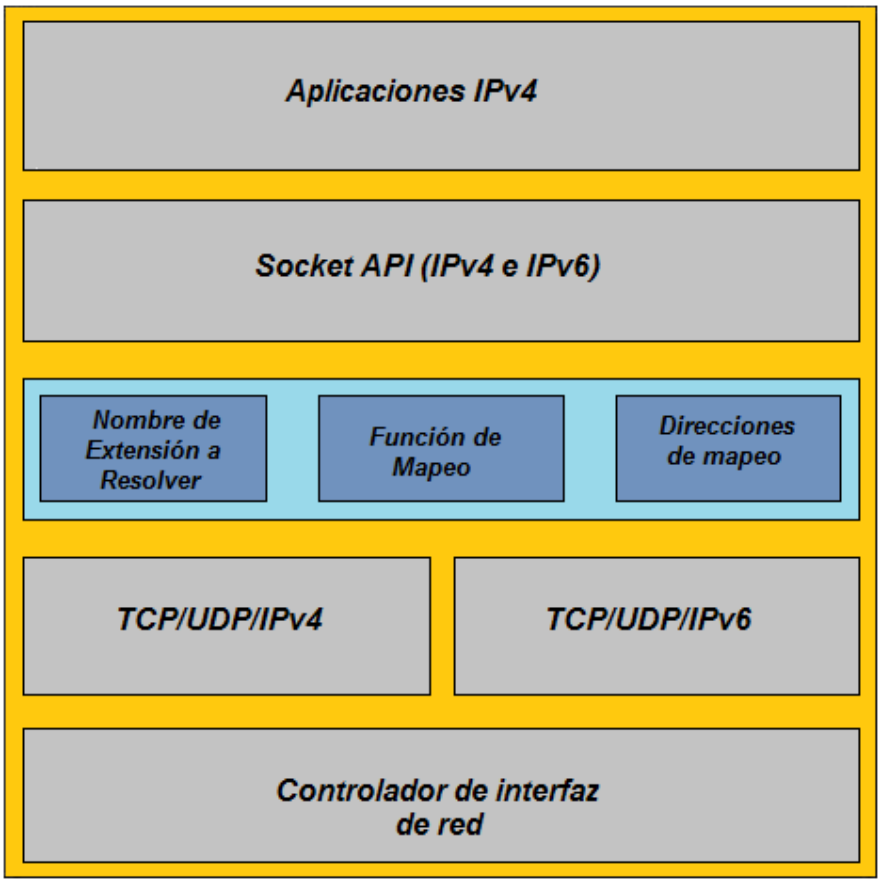

Figura 3. 22: Esquema del mecanismo BIA. (Dunmore, 2005)

a. El nombre de extensión de resolución ***(extensión name resolver)***, y las direcciones de mapeo ***(address mapper)*** funcionan de la misma manera que el BIS.
b. La función de mapeo ***(function mapper)***, detecta las llamadas de las funciones del socket IPv4 e invoca las funciones correspondientes del socket IPv6 y viceversa.

El BIA tiene dos ventajas sobre BIS: no dependen del controlador de interfaz de red y no introducir una sobrecarga en la traducción de los encabezados del paquete. Sin embargo, tampoco es compatible con la comunicación multicast.

El mecanismo Socks64 se clasifica en:

a. Ámbito de aplicación: máquina.
b. Requisitos de IPv4: ninguno.
c. Requisitos de las direcciones IPv4: espacio privado de direcciones por máquina.
d. Requisitos de IPv6: ninguno.
e. Requisitos de las direcciones IPv6: ninguno.
f. Requisitos de máquinas: doble pila más extensiones.
g. Requisitos de routers: ninguno.
h. Impacto del NAT: no resulta afectado por la presencia de NATs.
i. Otros requisitos: aplicaciones que utilizan direcciones de una forma literal.

3.4. Análisis comparativo de los mecanismos de transición IPv4 a IPv6.

Una vez detallado cada uno de los mecanismos propuestos para la transición de IPv4 a IPv6 y que de una u otra manera conllevarán a la migración total de direcciones IPv6. A continuación se presenta el análisis comparativo de los diferentes mecanismos de transición:

3.4.1. Análisis comparativo de los mecanismos de interconexión.

1. Para el caso de los ***túneles configurados*** cuyo mecanismo es el más empleado para obtener conectividad IPv6 de manera estable y sin complicaciones. Sin embargo, dicho túnel requiere de configuración manual en ambos extremos, mediante el subrango de direcciones IPv6 sin afectar la configuración del túnel. Es decir, que para el túnel <<*tunnelbroker*>>solo permite resolver la configuración de un extremo, aunque presenta inconvenientes de escalabilidad.

2. Debido a su simplicidad de configuración el túnel 6to4, permite obtener no sólo una dirección IPv6 sino también la dirección IPv4. Muy útil al momento de conectividad IPv6 mediante los proveedores de servicio que hasta ahora permiten conectividad IPv4.

3. El mecanismo 6over4 es poco empleado, por ser decadente, es decir, obsoleto debido a que requieren del servicio multicast en direcciones IPv4 para que exista interconexión.

4. Por problemas de seguridad los túneles automáticos no son recomendables implementarlos, debido a que los paquetes son transmitidos mediante encapsulación automática sobre IPv4, lo que provocaría un sinnúmero de ataques. Aunque cualquier mecanismo que encapsule de forma automática direcciones IPv4 embebidas dentro de la misma dirección IPv6, tendrían inconvenientes de seguridad (ataques), pero ya existen actualmente distintas soluciones que se relacionan con el uso de direcciones mapeadas.

5. Mientras el mecanismo ISATAP despliega un ámbito de aplicabilidad de dominio, lo que significa que requiere siempre de una dirección IPv4 por cada máquina.

6. En tanto el mecanismo TEREDO es mucho más flexible que los demás mecanismos analizados, es decir, que permite ejecutar la transición a través de las NAT's.

3.4.2. Análisis comparativo de los mecanismosde comunicación.

1. Para el mecanismo TRT que se presenta como muy útil en la transición, aunque el único inconveniente es en aplicaciones no compatibles con las NAT's. Actualmente se conocen implementaciones de TRT bajo TCP, mientras que para UDP son complicadas

2. El mecanismo DSTM requiere tanto del protocolo DHCPv6 y los túneles IPv4/IPv6, permitiendo la comunicación entre un dominio IPv6 y máquinas con dirección IPv4, sin necesidad de emplear el encaminamiento IPv4, es decir, que las máquinas IPv6 no requieren de direcciones IPv4, aunque si deben ser <<*dual stack*>>. Por último DSTM evita utilizar NAT's para comunicaciones solamente entre IPv4 e IPv6.

3. En tanto que los mecanismos Socks64 y BIA manejan un ámbito de aplicabilidad muy reducido debido a las aplicaciones de interoperabilidad evitando una migración a corto plazo. Es decir, que ambos mecanismos permiten la interoperabilidad solo a nivel IP.

4. Mientras el mecanismo BIS casi similar al mecanismo BIA, la diferencia es que deben modificar la pila IP permitiendo así la interoperabilidad de aplicaciones en máquinas IPv4 sobre IPv6. Aunque no es recomendable implantar BIS, por lo expuesto ya que resulta más fácil hacer que una máquina se transforme en un host del tipo <<*dual stack*>> y agregar el mecanismo BIA.

5. El mecanismo SIIT resulta ser más robusto, que al no tener estado, no presenta problemas de escalado en las conexiones. Durante el desarrollo del presente trabajo investigativo se pudo conocer que mediante la implementación del SIIT se han obtenido mejores resultados de interoperabilidad debido a su robustez.

6. Finalmente el mecanismo NAT-PT es muy utilizado en negocios corporativos de ámbito privado y las aplicaciones no requieren de NAT's. Aunque tendría un pequeño inconvenientes si trabaja el mecanismo NAT-PT conjuntamente con el nivel de aplicación DNS-ALG.

3.5. IPv6 en el Ecuador.

Las especificaciones básicas de los protocolos de internet IPv6 fueron establecidas hace aproximadamente 15 años; sin embargo, su utilización estuvo por mucho tiempo circunscrita a unas pocas redes, en su mayoría de carácter universitario o de investigación, pero esto ha comenzado a cambiar con el advenimiento de sistemas operativos que traen IPv6 habilitado por defecto (Windows Vista, 7) y especialmente con la realización del "IPv6 Day", que se desarrolló el 6 de junio de 2011, un evento organizado y coordinado por la Internet Society (ISOC) a través del cual - durante 24 horas - grandes redes y proveedores de contenido (Facebook, Yahoo, Google entre otras) habilitaron acceso por IPv6 a sus páginas principales.

El 6 de junio de 2012, ISOC organizó el "IPv6 Launch", los participantes de este evento dejaron habilitado IPv6 en sus redes ese día y de forma indefinida. A continuación se da un vistazo al estado de la implementación de IPv6 en Ecuador:

- Bloques IPv6 asignados y utilizados (al 8 de abril de 2012):
- 23 bloques IPv6 asignados/distribuidos por LACNIC a organizaciones ecuatorianas.

- 12 bloques utilizados (vistos en el Internet Global)
- 11 organizaciones diferentes utilizan prefijos IPv6

Oferta de servicios consoporte de IPv6:

- ISPs que pueden proveer tránsito IPv6 nativo: 3
- ISPs que proveen servicio HOME con soporte IPv6 nativo:0
- El punto de intercambio de tráfico local de Internet (NAP.EC) tieneIPv6 nativo habilitado
- El dominio .EC tiene un servidor con IPv6 fuera del Ecuador y otro en NAP.EC. NIC.EC acepta registros AAAA para dominios .EC

Páginas locales con soporte IPv6:

- www.aeprovi.org.ec
- www.ipv6tf.ec
- www.cedia.org.ec
- Páginas de algunas universidades ecuatorianas (listado en www.ipv6tf.ec)

3.6. Plan Nacional de Control Técnico a través de SUPERTEL[9] y MINTEL[10].

Como se describió, la transición a IPv6 dentro del territorio ecuatoriano se está iniciando, por lo cual y por iniciativa de AEPROVI[11] se creó la Fuerza de Trabajo de IPv6 de Ecuador (IPv6TF-EC) con los siguientes objetivos:

- Ser fuente de información relacionada con el Protocolo de Internet versión 6 (IPv6).
- Coordinar labores de capacitación y difusión sobre IPv6.

---

[9]SUPERTEL: Superintendencia de Telecomunicaciones del Ecuador.
[10] MINTEL: Ministerio de Telecomunicaciones y de la Sociedad de la Información del Ecuador.
[11]AEPROVI: la Asociación de Empresas Proveedoras de Internet, Valor Agregado, Portadores y Tecnologías de la Información. Aquí podrá encontrar información actualizada acerca de las actividades que realiza la asociación y sobre el sector de las telecomunicaciones y tecnologías de la información en general con ámbito en el Ecuador. http://www.aeprovi.org.ec/

- Coordinar los esfuerzos de los diferentes actores del Internet ecuatoriano para una eficaz y pronta adopción del IPv6.
- Fomentar el uso de IPv6.
- Establecer permanente comunicación e identificar oportunidades de colaboración con los Grupos de Trabajo de otros países y regiones.
- Elaborar un plan de acción para la implementación de IPv6 en el país y propiciar su uso.

El IPv6TF-EC no es una persona jurídica, es simplemente un grupo de trabajo con participación abierta; se busca incentivar la participación de ecuatorianas y ecuatorianos de los siguientes sectores: industria, gobierno, sector educativo, usuarios. El Grupo de Trabajo cuenta con un portal de Internet (www.ipv6tf.ec) con soporte de IPv6 nativo y alojado en Ecuador. La participación se realiza mediante la suscripción a la lista de correo electrónico foro@ipv6tf.ec(la suscripción se realiza a través del portal).

El Art. 313 de la Constitución de la República dispone que el Estado se reserva el derecho de administrar, regular, controlar y gestionar los sectores estratégicos, esto es, aquellos que por su trascendencia y magnitud tienen influencia económica, social, política o ambiental; sectores estratégicos entre los cuales está el sector de las telecomunicaciones, y en representación del estado actuarán la SUPERTEL y MINTEL.

La **SUPERTEL** se encargará de controlar el proceso de transición de IPv4 a IPv6, a través de parámetros técnicos, es decir, que tipo de infraestructura tecnológica (hardware) van a emplear la ISPs para hacer posible el proceso de transición y posterior migración a IPv6. En el Anexo A se detallan los parámetros de calidad para la provisión de servicios de valor agregado de Internet.

El Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) mediante el Acuerdo N° 039-2012, define lo siguiente con respecto a IPv6:

a. Que, dentro del Plan de Acción eLAC 2015, la meta 4 insta a los países miembros a 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, para que la región logre un amplio despliegue del Protocolo de Internet versión 6 (IPv6), así mismo hace un llamado a implementar con brevedad planes nacionales que permitan acceder a los portales de servicios públicos gubernamentales de los países de la región a través de IPv6 y que las redes estatales trabajen de forma nativa con IPv6.
b. Que, en este contexto y mediante Acuerdo N° 0133 del 25 de marzo del 2011 el MINTEL, requirió a las Instituciones y Organismos señalados en el Art. 225 de la Constitución de la República del Ecuador que en los nuevos procedimientos de contratación de equipamiento tecnológico, productos y aplicaciones que utilicen el Protocolo de Internet y que se efectúen a partir de la fecha de publicación en el Registro Oficial del mencionado acuerdo, tengan como exigencia primordial el soporte y compatibilidad con IPv6.
c. Que, con Acuerdo N° 007-2012 del 18 de enero del 2012, el MINTEL emitió lineamientos de política pública vinculados con la incorporación de IPv6 en sitios web y aplicativos del sector público, en el ccTLD.ec y en el curso normal de tráfico IPv6 en las redes de ISPs y Portadores.
d. Que, en la reunión N° XX, el Comité Consultivo Permanente de Telecomunicaciones CCPP CITEL-OEA (ver Anexo B) aprobó las medidas regionales de fomento y adopción de IPv6 en la Región, las cuales fueron presentadas por Ecuador en Buenos Aires, Argentina el 19 de mayo del 2012, mediante documento N° 2608.
e. Que, es necesario que el MINTEL como órgano rector del desarrollo de las Tecnologías de la Información y Comunicación,

dentro de sus competencias, coordine con las entidades del sector público la coexistencia de los protocolos IPv4 e IPv6.

Esto conlleva al MINTEL en ejercicio de sus atribuciones, acordar los siguientes dos artículos.

Artículo 1.- Aprobar las siguientes estrategias de acción para el fomento en la adopción y coexistencia de los protocolos IPv4 e IPv6 en todo el territorio nacional bajo las siguientes estrategias:

1. El proceso de incorporación y adopción del Protocolo de Internet IPv6 en Ecuador, será impulsado por el MINTEL, dentro del programa de Recursos de Banda Ancha, que forma parte del Plan Nacional de Banda Ancha.
2. Las Instituciones y Organismos del Sector Público señalados en el Art. 225 de la Constitución de la República del Ecuador, deberán realizar las gestiones necesarias para que implementen sus sitios web y plataformas de servicios electrónicos, con el soporte y compatibilidad con el protocolo IPv6 de manera coexistente con el protocolo IPv4, en el plazo de un año contado a partir de la entrada en vigencia del presente acuerdo.
3. Las empresas públicas de telecomunicaciones, realizarán las acciones que correspondan, para que en el plazo de 45 días contados a partir de la publicación del presente acuerdo, admitan en sus redes, plataformas y sistemas el curso normal de tráfico de IPv6 nativo en coexistencia con IPv4.
4. Incorporación del protocolo IPv6 de forma coexistente con IPv4 en los sitios Web www.mintel.gob.ec, www.mintel.gob.ec y www.conatel.gob.ec así como en las plataformas de servicios electrónicos asociadas a los portales web tanto del MINTEL, SUPERTEL y CONATEL.
5. El MINTEL organizará talleres, charlas, foros y jornadas teórico-prácticas sobre aspectos técnicos IPv6, de carácter gratuito a los largo del territorio nacional, con participación de expertos internacionales con amplia experiencia en el despliegue real de IPv6.

6. El MINTEL en el plazo de 90 días contados a partir de la publicación del acuerdo N° 039-2012, publicará el “Plan de recursos y adquisiciones de tecnología con soporte IPv6”, el cual servirá como marco de referencia para inclusión del nuevo protocolo en los procesos de adquisición de infraestructura, servicios, y aplicaciones para garantizar el adecuado soporte de IPv6 tanto en el sector público como privado.

Artículo 2.- El MINTEL se encargará del seguimiento y monitoreo respecto al cumplimiento del presente acuerdo, en colaboración con la SUPERTEL.

De acuerdo con lo descrito en el Plan Nacional de Control Técnico el MINTEL, SUPERTEL y CONATEL son los entes públicos que se encargarán de verificar la calidad de los servicios de valor agregado (SVA) de internet.

Capítulo 4: Simulaciones de mecanismos de transición.

4.1. Simulación de los mecanismos Tunnel Broker.

Para la simulación de los mecanismos Broker se emplearán los simuladores virtuales online de freenet6 y hurricane. Estas simulaciones se basan de acuerdo a las propuestas de los diferentes mecanismos de transición expuestos en el capítulo anterior.

4.1.1. Simulación de un Host en WINDOWS 7 mediante Freenet6.

Para la presente prueba de simulación de un túnel Broker, emplearemos una red LAN con protocolo IPv4 detrás de un ADSL con direccionamiento IP público. Inicialmente no se considerará ningún Firewall entre el ADSL y la LAN. Mediante Freenet6 crearemos un túnel con host (Windows) de una red LAN (por detrás de una NAT), que permita obtener conectividad IPv6 para un host con IPv4. Previamente a la simulación debemos considerar lo siguiente:

a. En primer lugar, configuraremos al host en la parte cliente del túnel denominado gogoCLIENT, en la cual el cliente interactuará con el servidor denominado gogoSERVER.

b. En segundo lugar, utilizaremos al protocolo TSP, permitiendo que el túnel de datos se mantenga estático. Es decir, que gogoCLIENT se conecta a gogoSERVER para obtener información relativa al túnel mediante el protocolo TSP. En caso de que el host creará al túnel y se encuentre detrás de un FIREWALL, abriríamos el puerto 3653. **Para este acápite no trabajamos detrás del FIREWALL en consecuencia no abriremos ningún puerto.**

c. En tercer lugar, los códigos fuente deben ser iguales para todas las plataformas cliente.

d. En cuarto lugar, y de manera opcional si deseamos configurar al cliente para conexión a un único gogoSERVER o múltiples SERVIDORES. Esto permite obtener mejor calidad de servicio para

los usuarios al momento de conectarse al servidor más cercano y manteniendo la redundancia, que ante cualquier suceso en el que un servidor no esté disponible el túnel siga funcionando.

e. Y en quinto lugar, emplearemos una interfaz gráfica para Microsoft Windows, permitiendo una fácil configuración del túnel y a la vez ofreciendo un informe del estado de servicio.

Antes de realizar la simulación debemos dirigirnos a la página web: http://www.gogo6.com/freenet6/tunnelbroker, para proceder a descargar el programa gogoCLIENT – Basic Versión. En dicha página deberán registrarse previamente para proceder a descargar el programa en mención. Una vez descargado se procederá a la instalación y configuraciones respectivas del túnel Broker.

El software instalado gogoCLIENT se lo puede visualizar en el botón Iniciar de Windows 7, tal como se muestra en la figura 4.1.

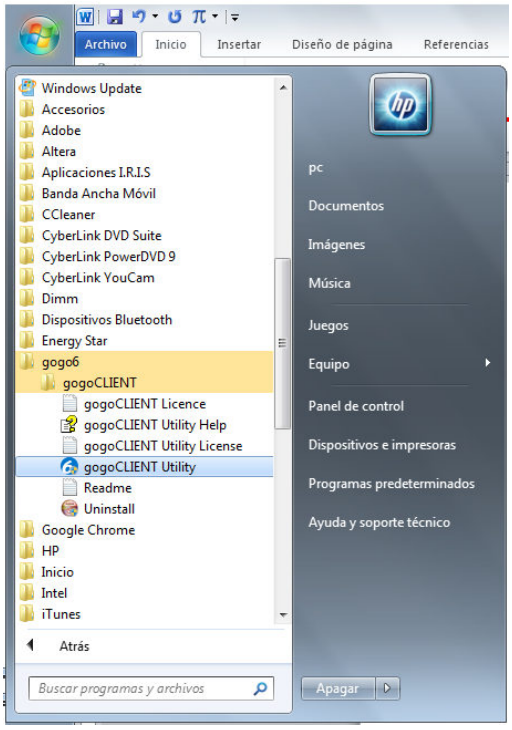

Figura 4. 1: Software gogoCLIENT instalado en Windows 7 de 64 bits.
Fuente: J. Coellar y J. Cedeño.

Al abrir la carpeta gogo6 escogemos la opción gogoCLIENT Utility, la misma debe tener permisos de administrador, permitiendo la conexión mediante identificación o de manera anónima al servidor freenet6, tal como se muestra en la figura 4.2.

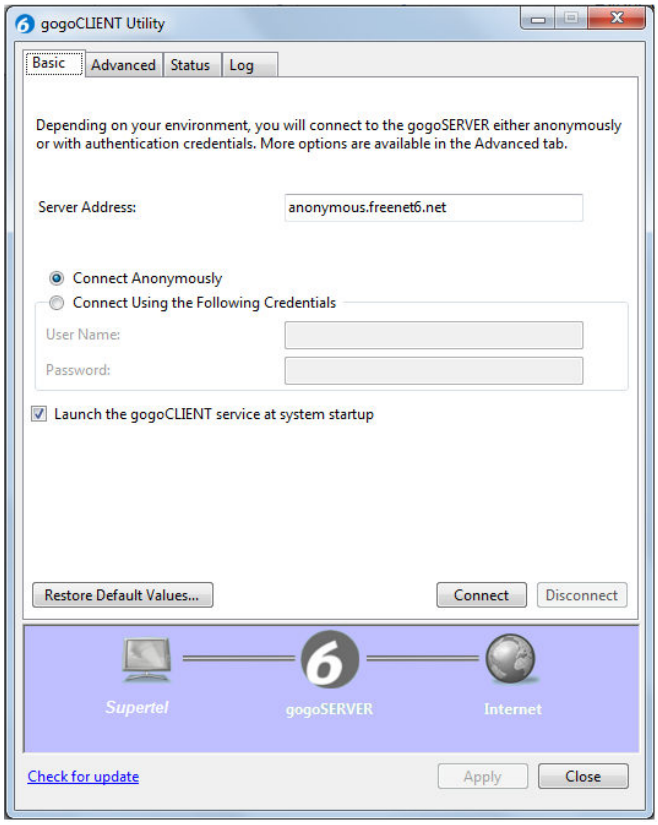

Figura 4. 2: Ventana de gogoCLIENT – Utility.
Fuente: J. Coellar y J. Cedeño.

Hay dos maneras de conectarse al servidor de pruebas:

a. Seleccionamos el tipo de conexión anónima "**Connect anonymously"** mientras que en el "Server Address" escribiremos "**anonymous.freenet6.net"**.Al ser una conexión anónima, nos permitirá navegar con IPv6 en Internet, aunque nadie accedería a páginas Web que tengamos en nuestra máquina. Además, no dará una dirección Ipv6 a ningún host de nuestra LAN.
b. En cambio sí escogemos**"Connect Using the Following Credentials"** y al Server Address"**authenticated.freenet6.net**". Para esta opción es requisito necesario ser usuario y la

contraseña del registro realizado en freenet. En este caso tendremos todas las opciones comentadas si las tenemos activas en la configuración avanzada que se explica más adelante.

No es conveniente activar **"launch de gogoclientservicesystem at startup"** pero al ser activada, pondrá al túnel en marcha cuando encendamos o reiniciemos las computadoras, es decir, que predeterminadamente tenemos una red con IPv6. De la figura 4.2 escogemos la pestaña Status, en la que se puede observar toda la información que freenet6 nos ha asignado.

En la figura 4.3 se muestra el estado status, en la cual nos indica que tenemos una configuración Ipv6-in-UDP-Ipv4 Tunnel (NAT Transversal), es decir, que estamos detrás de una NAT.

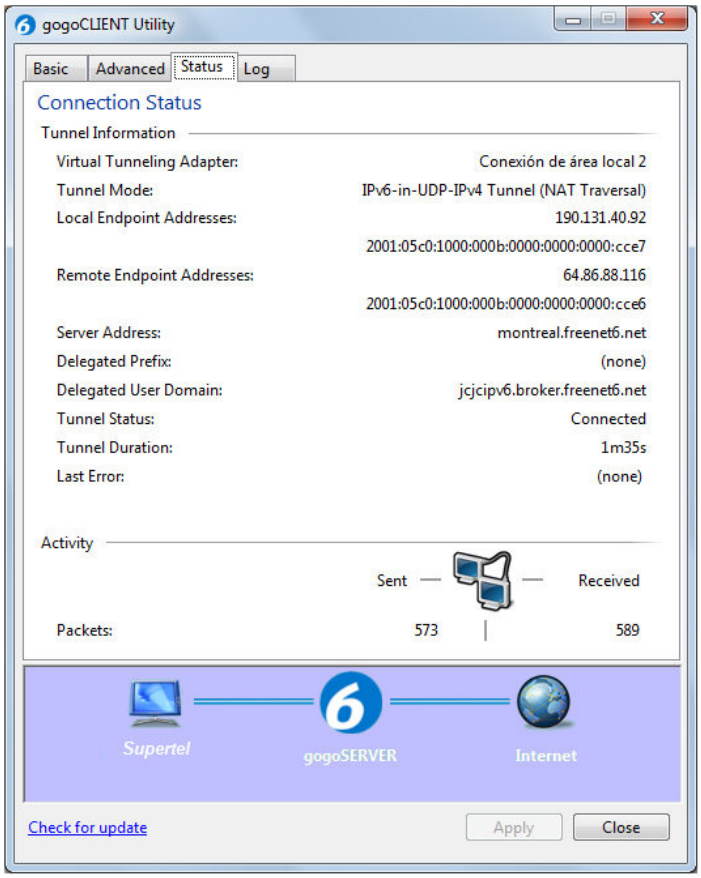

Figura 4. 3: Status de conexión Broker de gogoCLIENT – Utility.
Fuente: J. Coellar y J. Cedeño.

Como podemos observar de la figura 4.3, la longitud del prefijo asignado es de 64 bits. Para esta simulación es importante reconocer cuando los túneles tienen conexión anónima o autenticada, debido a que el prefijo cambia respecto a la conexión. Es decir, que para la conexión anónima, el prefijo tiene la forma 2001:05c0:1000:**a:**: /64 (finaliza con a)la dirección IPv6 viene asociada con cada conexión del túnel mientras que en la conexión autenticada, en donde el segundo prefijo tiene la forma 2001:05c0:1000**:b**:: /64 (acaba con b) y la dirección IPv6 es asignada de forma permanente al usuario sin cambiarse aunque el usuario se desplace a otra IPv4.

Los túneles creados expirarán pocos minutos después de que el cliente se haya desconectado. Mientras tanto, procedemos a comprobar la conexión IPv6 (ver figura 4.4) a través del cmd, dándole un ping a la dirección de google.

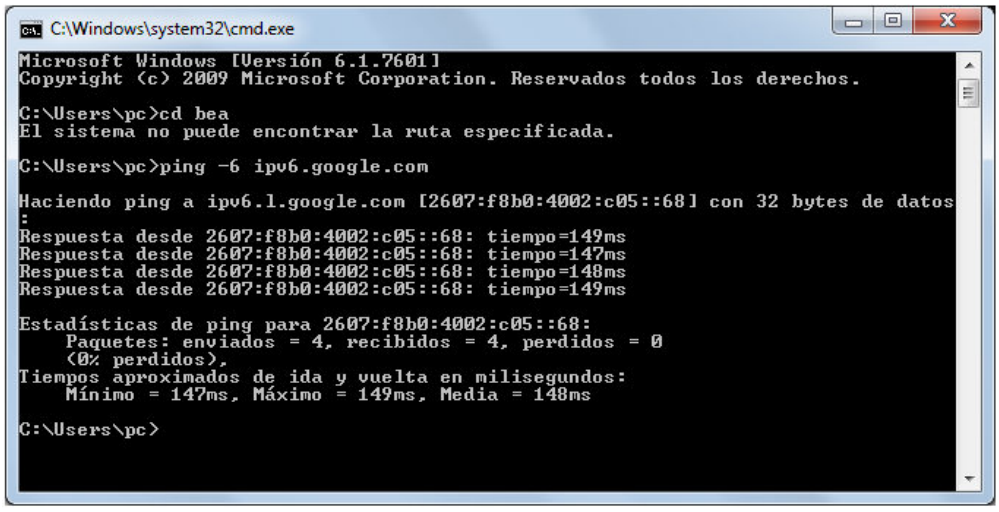

Figura 4. 4: Estado de conexión mediante IPv6.
Fuente: J. Coellar y J. Cedeño.

Este tipo de pruebas se realizaron en los laboratorios de la SUPERTEL para comprobar que la ISPs en este caso Claro (Banda Ancha) trabaje con el mecanismo de transición Tunnel Broker. Este software es libre, servirá para controlar y supervisar por parte de la SUPERTEL a todos y cada uno de las ISPs.

Finalmente cabe recalcar que el programa gogoCLIENT no requiere de programación de alto nivel, sino más bien de una correcta configuración, tener acceso a la red gogoCLIENT. Este software puede ser utilizado en Universidades para el despliegue de otras investigaciones.

4.1.2. Simulación de un túnel de firewall en WINDOWS 7 mediante Hurricane.

Similarmente a la primera simulación, la red disponible es una LAN IPv4 detrás de un Firewall Debian mediante la conexión de un ADSL con IP pública estática. El objetivo de la presente simulación consiste en crear un túnel Broker desde un firewall dotándole de una dirección IPv6 hacia internet y que acceda sin problemas a varias páginas web con direccionamiento IPv6.

Para la simulación de este acápite, se utilizará la página web http://tunnelbroker.net mostrada por la figura 4.5. En dicha página hay que suscribirme y posteriormente recibirán un email para poder acceder a la plataforma Hurricane Electric (Internet Services).

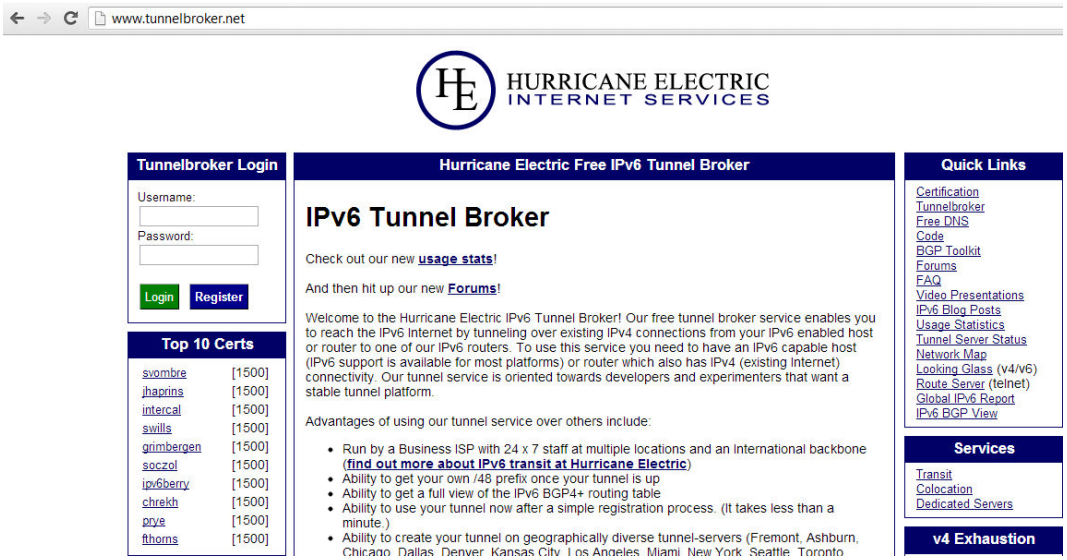

Figura 4. 5: Página web del Tunnel Broker IPv6.
Fuente: J. Coellar y J. Cedeño.

Una vez realizado lo indicado, se procederá a ingresar con el respectivo usuario, posteriormente elegimos **"Create regular tunnel"**la cual permite visualizar una ventana (ver figura 4.6), la misma que solicita una dirección IP pública, que por lo general es la misma de nuestro ADSL.

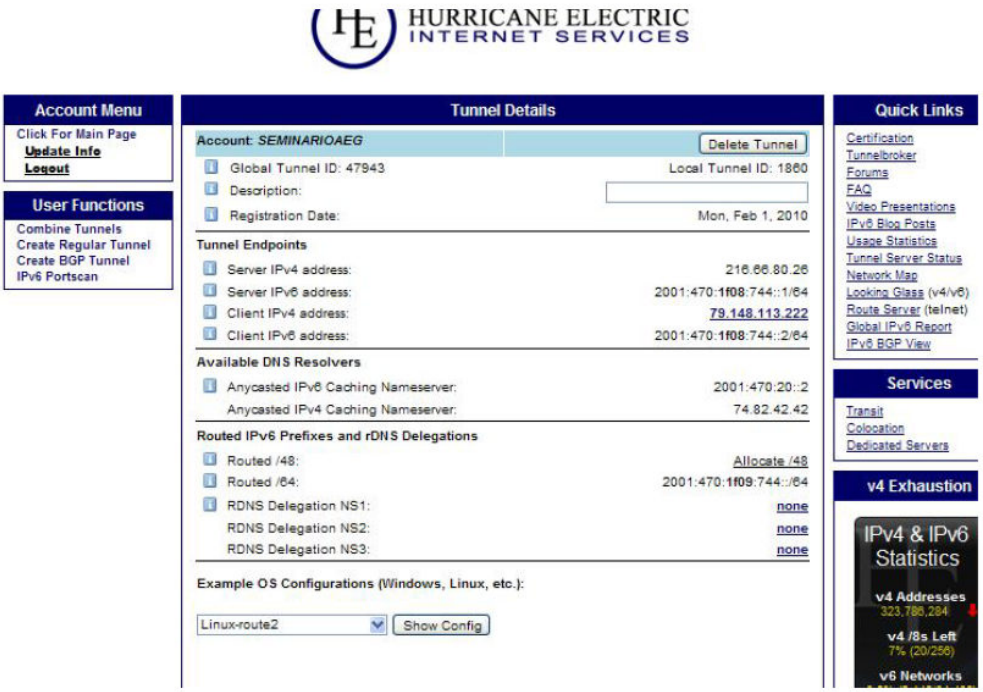

Figura 4. 6: Creación regular de un túnel Broker.
Fuente: J. Coellar y J. Cedeño.

La figura 4.6 nos muestra toda la información, cuyo direccionamiento IPv4 e IPv6 ocurren en ambos extremos del túnel. Adicional, se observa un prefijo IPv6 asignado exclusivamente para dar una dirección IPv6 a cada host de la red LAN localizada por detrás del Firewall.

Posterior a esto procedemos a realizar la instalación del Debian. Provisionalmente el pc u ordenador es un host con distribución Debian, el mismo maneja dos tarjetas de Red, una tarjeta que opera solo para la red LAN (eth1) y la otra a la Red del ADSL (eth0). Adicionalmente, el pc o Host es un Firewall y un servidor Apache.

Para una correcta simulación, la red IPv4 debe cumplir una serie de requisitos:

a. La IPv4 pública del ADSL tiene que ser estática.
b. La dirección IPv4 de cada host de la LAN puede ser estática o dinámica.
c. El túnel diseñado o creado es autenticado, es decir, que no existe anónimos como en Freenet6.

Una limitante del uso de la plataforma web de Hurricane Electric, es que cada usuario puede crear hasta 5 túneles. Primeros pasos:

1. Probar que Kernel de Debían admite IPv6. Este debe ser posterior a la versión 2.6.

#cat /proc/net/if_inet6 &&echo 'IPv6 sistema preparado!' **||** echo 'No se encuentra el soporte IPv6. Compile el Kernel!!'

2. Probar que el módulo IPv6 está cargado:

modprobe IPv6

o

lsmod | grep ipv6

Resultado: ipv6 41142518

Creamos un archivo que tiene las ordenes **iptables** para una correcta configuración del Firewall. Al archivo le damos el nombre de "permitir" y lo almacenamos en la ruta /etc/init.d

```
apacheaeg:/etc/init.d# cat permitir
#!/bin/bash
pt=/sbin/iptables
for TABLE in filter nat
do
$pt -t $TABLE -F
$pt -t $TABLE -X
$pt -t $TABLE -Z
done
echo 1 >/proc/sys/net/ipv4/ip_forward
echo 1 >/proc/sys/net/ipv6/conf/all/forwarding
iptables -t nat -A POSTROUTING --protocol ! 41 -o eth0 -j MASQUERADE
```

Además de poner políticas por defecto **Aceptar,** se da la orden de forwardear entre las tarjetas los paquetes IPv4 e IPv6. También, se da la orden de enmascarar únicamente los paquetes IPv4. Los paquetes IPv6 usan el protocolo 41 y se le está indicando al Firewall que no enmascare estos paquetes. Este archivo tiene un enlace creado en **/etc/rc2.d** para que se ejecute cada vez que se inicia el Host.

/etc/init.d# chmod 777 permitir

/etc/init.d# ln –s /etc/init.d/permitir /etc/rc2.d/S99_permitir

Órdenes para crear el túnel:

ip tunnel add he-ipv6 mode sit remote 216.66.80.26 local 10.10.10.50 ttl 255

Sintaxis:

ip tunnel [add|change|delete] nombre_tunel mode [ipip|sit|gre] remote [direci. Ipv4 b broker] local [la ip de nuestro host] dev [periferico]

Los argumentos posibles son:

- name NOMBRE -- selecciona el nombre del túnel
- mode MODO -- hay 3 modos disponibles: ipip, sit y gre

El modo ipip corresponde a un simple túnel IP sobre IP. Se encapsulan los paquetes sin más. El modo sit se usa para túneles IPv6. El modo gre corresponde a los túneles GRE especificados por la compañía Cisco, que son túneles IP sobre IP cifrados.

- remote DIRECCION -- dirección de 'salida' del túnel
- local DIRECCION -- dirección local de 'entrada' del túnel
- PERIFERICO-- nombre del periférico a través del que se envían los paquetes

ip tun show –

Esta orden muestra los túneles

ip link set he-ipv6 up

Esta orden sirve para levantar el túnel llamado he-ipv6

ipaddr add 2001:470:1f08:744::2/64 dev he-ipv6

Permite asignar una dirección IPv6 al extremo local del túnel

ip route add ::/0 dev he-ipv6

Permite poner una ruta estática. Cualquier paquete que esté destinado a una dirección IPv6 deberá salir por el túnel llamado he-ipv6.

ip -f inet6 addr

El -f significa family, y al poner inet6 hace referencia a la familia IPv6. Si no se pone nada por defecto es IPv4. Esta orden tiene carácter informativo y muestra las direcciones IPv6. Todas las órdenes juntas forman el script para crear el túnel. Se puede usar cualquier editor de texto (nano, vi,..):

apacheaeg:/etc/init.d# nano tunel
ip tunnel add he-ipv6 mode sit remote 216.66.80.26 local 10.10.10.50 ttl 255
ip link set he-ipv6 up
ipaddr add 2001:470:1f08:744::2/64 dev he-ipv6
ip route add ::/0 dev he-ipv6
ip -f
inet6addr /etc/init.d# chmod 777 tunel
/etc/init.d# ln –s /etc/init.d/tunel /etc/rc2.d/S99_tunel

A este archivo se le ha dado permisos de ejecución, se ha creado el enlace a rc2.d para su ejecución en el arranque. La orden **ifconfig**me muestra (ver figura 4.7):

apacheaeg:/home/apacheweb# ifconfig

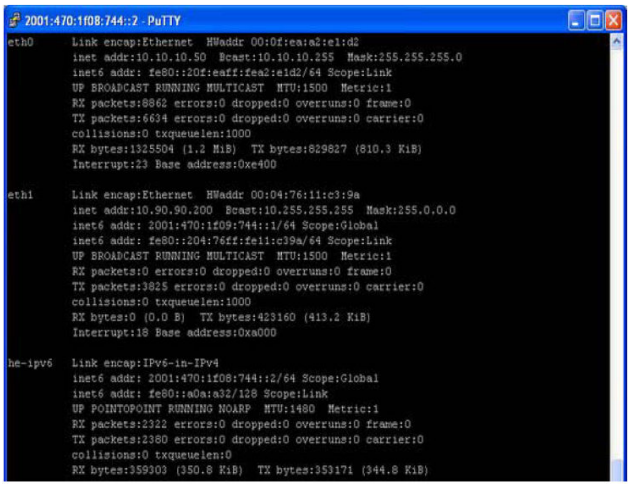

Figura 4. 7: Resultados de la redes LAN.
Fuente: J. Coellar y J. Cedeño.

Para poner el demonio radvd en marcha damos la orden:

apacheaeg:/etc/init.d# /etc/radvdrestart

Stopping radvd: radvd.

Starting radvd: radvd.

Para que se ejecute de forma automática el radvd deberemos en el archivo rc.local que se encuentra en /etc añadir la línea **/etc/radvd.confrestart.** Este archivo tiene un enlace a rc2.d llamado S99rc.local. **/etc# nano rc.local**Añadir la línea: /etc/radvd.confrestart, como se muestra en la figura 4.8

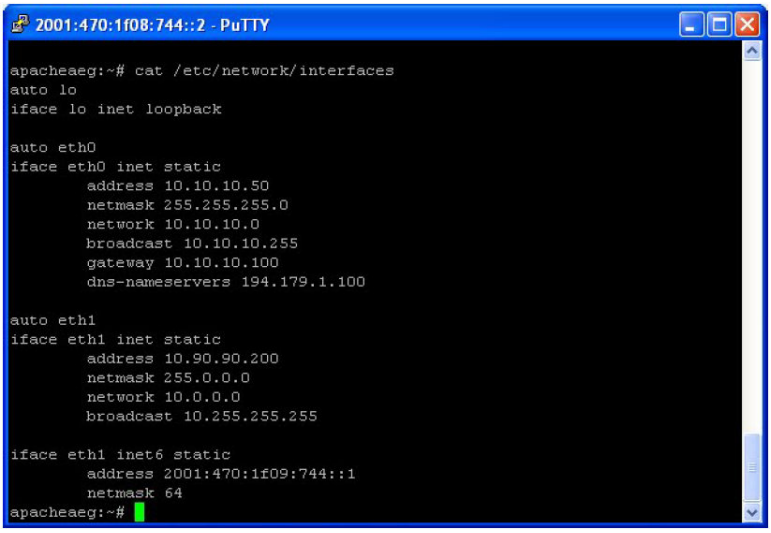

Figura 4. 8: Ejecución automática del túnel Broker.
Fuente: J. Coellar y J. Cedeño.

A partir de ahí y desde cualquier host o máquina de la red LAN tenemos posibilidades de consultar Páginas web IPv6 en Internet. Además, podemos ver nuestra página web en el Firewall desde cualquier host que tenga una dirección IPv6. Consultando la información de la interface del host que está detrás de la LAN observamos en la figura 4.9:

Figura 4. 9: Ipconfig del mecanismo túnel Broker.
Fuente: J. Coellar y J. Cedeño.

El paquete de datos sale a Internet desde un host o máquina de una red LAN, aunque de manera inicial será enviado a la interface del Firewall local (fe80), una vez el paquete ha llegado al router este consulta en su tabla de enrutamiento la dirección Ipv6 por la que debe salir para llegar a internet. En la figura 4.10 se muestra el enrutamiento de direcciones Ipv6.

#route –A inet6

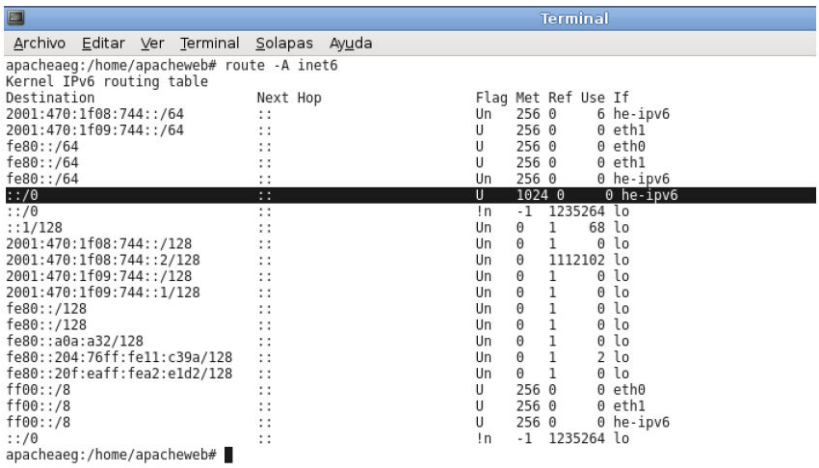

Figura 4. 10: Creación regular de un túnel Broker.
Fuente: J. Coellar y J. Cedeño.

Aunque en relación ala primera simulación del mecanismo túnel Broker, resultaría sencillo trabajar con gogoCLIENT ya que no presenta muchos procesos como programar.

4.2. Simulación del mecanismo Dual Stack.

Una vez conocidas cada una de las interfaces tanto de la Pila IPv4 como la Pila IPv6, procedemos a configurar la asignación del direccionamiento en IPv6ya sea para el Sistema Operativo Windows o Linux. De esta manera tendríamos una dirección válida paraIPv6, ya que si se activa IPv6 inmediatamente se carga una dirección de hostlocal (***fe80*::202:55ff:febf:8991%5**), la cual no nos sirve para tener salida hacia el Internet.

La solución es proceder a la asignación de una dirección válida enIPv6 configurando de manera manual, siendo esta la manera correcta para realizar pruebas de configuración del presente trabajo investigativo, adicional a la asignación manual de direcciones IPv6, existe otra forma dinámica conocida como Dinamic Host Control Protocol versión 6, (DHCPv6).

Establecimiento de Dual Stack en Windows:

En primer lugar se asignará una dirección IPv6 que sea válida para tener una salida directa a Internet, para establecer el transporte de datos en Dual Stack –IPv4 e IPv6, debemos levantar cada una de las dos interfaces de IPv4 e IPv6 (ver figura 4.11),y posteriormente escribimos un comando que permita establecer una dirección válida en IPv6.

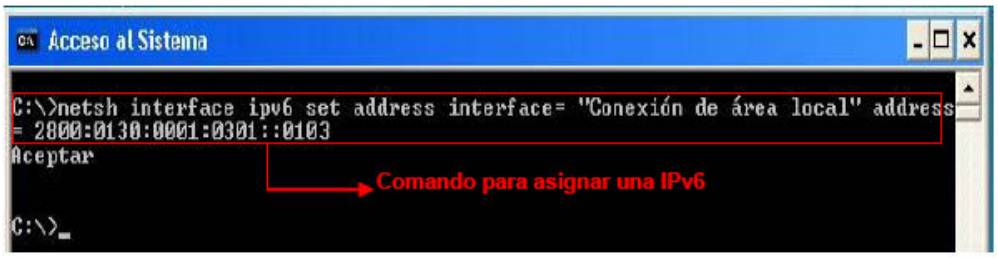

Figura 4. 11: Asignación manual del protocolo de internet versión (IPv6).
Fuente: J. Coellar y J. Cedeño.

La figura 4.12 nos muestra la dirección IPv6 estática asignada manualmente, cuyo direccionamiento en doble pila <<*Dual Stack*>>, permitirá enviar sin inconvenientes el transporte y envío de paquetes en doble pila ya sea para IPv4 e IPv6, así como también la salida hacia el Internet.

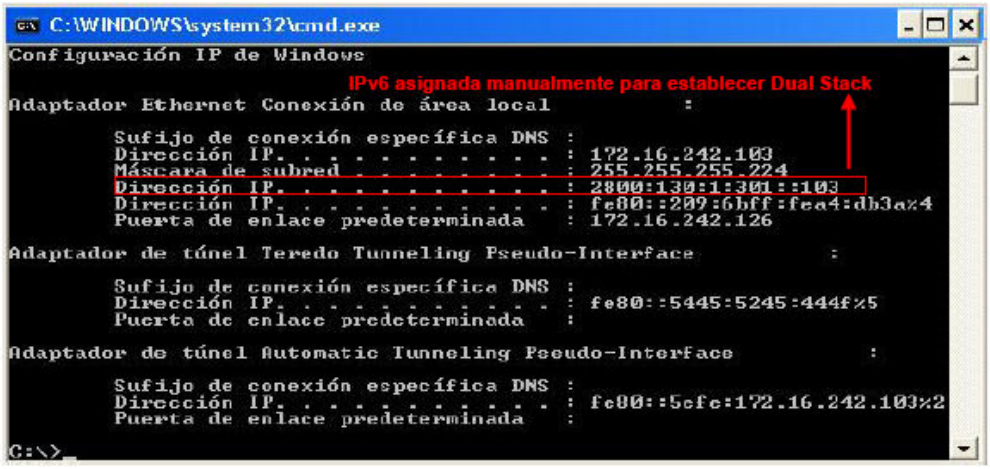

Figura 4. 12: IPv6 asignada manualmente para establecer <<*Dual Stack*>>.
Fuente: J. Coellar y J. Cedeño.

Configuración de Dual Stack en Linux:

Ahora para configurar Dual Stack en el Sistema Operativo Linux, se debe tener activado IPv6, para posteriormente asignarle una dirección IPv6 estática a la interfaz, esto se lo consigue de la siguiente manera:

a. Primeramente debemos editar un fichero que corresponda a una tarjeta de red, pero mediante el siguiente comando:
   vi*/etc/sysconfig/network-scripts/ifcfg-eth0.*

b. Posteriormente se agregan tres variables:
   IPV6INIT = yes (inicializamos con IPv6 en la tarjeta de red).
   IPV6_AUTOCONF = no (desactivamos la generación automática en la tarjeta de red para direcciones IPv6).
   IPV6ADDR = *2800:0130:0001:0301::0102* (asignación estática de una tarjeta de red para direcciones IPv6).

c. Después guardamos los cambios en un fichero, el cual debe editarse tal y como se muestra en la figura 4.13.

DEVICE=eth0	#identificador del dispositivo de red
HWADDR=00:09:6B:A4:19:11	#dirección MAC del dispositivo
ONBOOT=yes	#activar al inicio
TYPE=Ethernet	#tipo del dispositivo
IPV6INIT=yes	#inicializa IPv6 en la Interfase
IPV6_AUTOCONF=no	#deshabilita las técnicas de autoconfiguración
IPV6ADDR=2800:0130:0001:0301::0102	#asigna una dirección IPv6 a la tarjeta

Figura 4. 13: Fichero para <<*Dual Stack*>> en Linux.
Fuente: J. Coellar y J. Cedeño.

d. Finalmente, reiniciamos los servicios de red mediante el comando**<<*service networkrestart*>>** y posteriormente digitamos el comando **ifconfig,** es decir, que la dirección IPv6 se ha configurado, para lo cual se debe reiniciar la máquina o pc y sin desaparecer la dirección, ya que ésta inmediatamente guardará los cambios en los registros del sistema operativo Linux.

Ahora que se han configurado los Sistemas Operativos Windows y Linux respectivamente, a través del <<*Dual Stack*>>donde se tiene el doble direccionamiento, esto gracias a la aplicación del mecanismo de transición <<*Dual Stack*>> descrito en la propuesta del capítulo 3 siendo el objetivo del presente trabajo investigativo.

En las figuras 4.14 y 4.15 se muestran las capturas de los paquetes de una red, esto se logró a través del software ***Ethereal***.

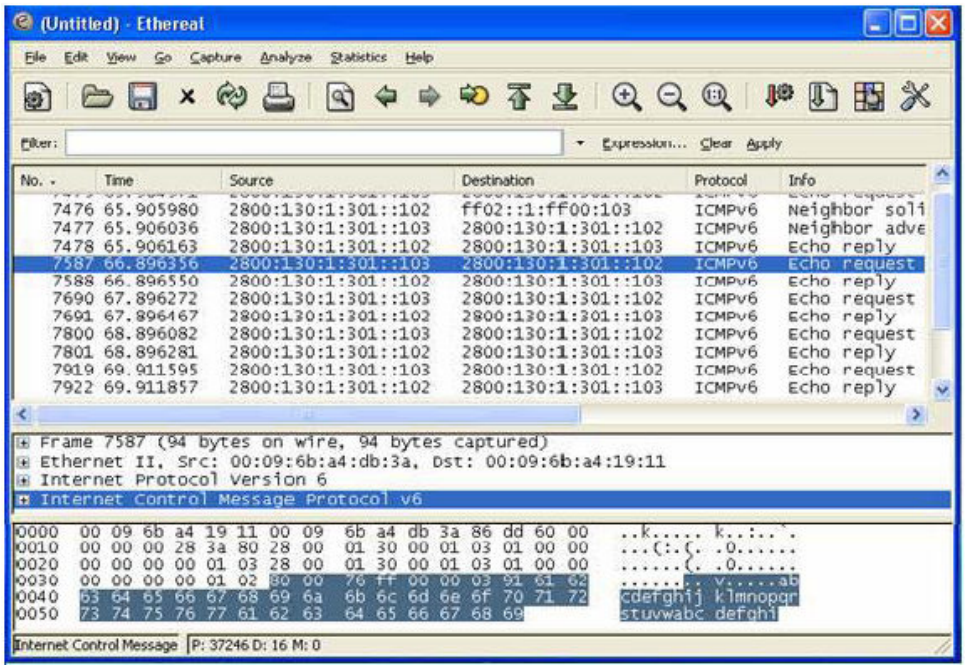

Figura 4. 14: Captura del datagrama IPv6.
Fuente: J. Coellar y J. Cedeño.

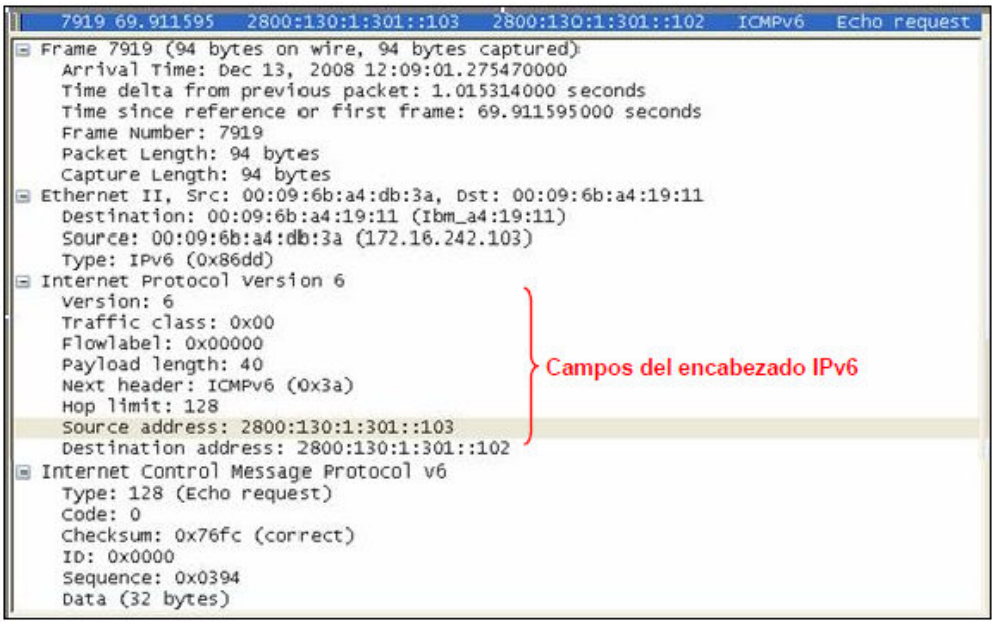

Figura 4. 15: Estructura del encabezado del datagrama IPv6.
Fuente: J. Coellar y J. Cedeño.

Capítulo 5: Conclusiones y Recomendaciones.

5.1. Conclusiones.

1. A través del estado del arte se pudo establecer los fundamentos teóricos necesarios de los protocolos de internet disponibles en la actualidad y los que a futuro continuarán operativos, en consecuencia se pueden crear líneas de investigación acerca de las redes de comunicaciones de datos.

2. Mediante los mecanismos de transición para interconexión y comunicación, propuestos para la transición de IPv4 a IPv6 consiste en que las prestadoras de servicio de internet (ISPs) pongan en práctica cualquiera de los mecanismos, y que los equipos (hardware) sean compatibles con los mismos.

3. A través de las 3 pruebas desarrolladas se pudo constatar que de manera interna existen ISPs que soportan mecanismos de transición de acuerdo a las disposiciones emitidas por el CONATEL y cuyo control lo realizan de manera conjunta el MINTEL y la SUPERTEL.

4. Evidentemente el trabajo es difícil para los administradores de redes o sistemas de las ISPs o compañías que van a emplear los mecanismos de transición, ya que deberán elegir el mecanismo más adecuado, la SUPERTEL tiene previsto para este año 2013 definir guías de implantación de los mecanismos propuestos para determinadas aplicaciones, incluyendo grandes redes corporativas (ISPs), hasta dispositivos móviles y usuarios domésticos.

5. El presente trabajo investigativo ha servido de mucho para el personal del Laboratorio de la SUPERTEL, ya que ahí ponen en

práctica todos los mecanismos de transición para futuros controles a las ISPs.

6. Con el protocolo IPv6 la red de Internet será más rápida, más segura y fiable para todos, para acceder a ciertas aplicaciones en tiempo real. Aunque se puede pensar que la transición a IPv6 sea un proceso largo, complejo y muy costoso, pero las aplicaciones marcarán el ritmo de la transición.

5.2. Recomendaciones.

1. A partir de los mecanismos de transición existe un mundo de posibilidades para experimentar con IPv6 ya sea en movilidad, seguridad a nivel de red, integración con otros dispositivos Ipad's, tablets y celulares smartphones.

2. Que la Universidad Católica de Santiago de Guayaquil a través de la Facultad de Educación Técnica para el Desarrollo y de la Maestría en Telecomunicaciones, que se involucren más a fondo mediante investigaciones que den resultados positivos para la migración total del protocolo IPv6, y que puedan invertir en equipos que permitan desarrollar la parte experimental.

3. Los equipos que se involucran en la transición deben ser previamente analizados, para saber cuál es más flexible y económico de adquirir, dichos equipos deben utilizar el protocolo IPv6 antes de ser actualizados y así poder producir bajas en el rendimiento.

4. Que el MINTEL y SUPERTEL difundan talleres sobre la transición de IPv4 a IPv6 a toda la ciudadanía a través de las Universidades Públicas y Privadas del Ecuador.

Bibliografía

Cisco. (2004). *Implementing IPv6 for Cisco IOS Software*. Obtenido de www.cisco.com

Dunmore, M. (2005). 6net an IPv6 Deployment Guide. En M. Dunmore, *6net an IPv6 Deployment Guide* (págs. 3-4). Javvin Technologies Inc.Distribution .

Feyrer, H. (24 de 05 de 2001). *Onlamp.* Obtenido de Introduction to IPV6. O´Reilly: http://onlamp.com/pub/a/onlamp/2001/05/24/ipv6_tutorial.html

Gordo Saez, R. (1998). *Transmisión de Información en Internet.* España.

Jara, F. (2009). *Estudio e implementación de una red IPv6 en la UTFSM.* Valparaíso-Chile: Universidad Técnica Federico Santa María.

Kotal, V. (2005). *Tesis PhD: Principles, implementation and transistion to IPv6 protocol.* Praga: Universidad de Karlova.

Lázaro, J., & Miralles, M. (2004). *Fundamentos de Telemática.* México, D.F. : Universidad Politécnica de Valencia .

Malone, D., & Niall, M. (2005). *IPv6 Network Administration.* O'Reilly.

Moore, K. (2001). *Draft-Ietf-Ngtrans-6to4-DNS: 6to4 and DNS.*

Nordmark, E. (2000). *RFC 2765: Stateless IP/ICMP Translation Algorithm (SIIT).*

Olvera, C., Palet, J., & Vives, A. (2008). *Herramientas de Transición IPv6.* La Habana: http://www.cuba.ipv6tf.org/talleripv6-2008/5.pdf.

Palet, J. (Abril de 2007). *The Choice: IPv4 Exhaustion or Transition to IPv6*. Obtenido de The IPv6 Portal: http://www.ipv6tf.org/pdf/the_choice_ipv4_exhaustion_or_transition_to_ipv6_v4.4.pdf

Pinillos, E. (2003). IP versión 6: La nueva generación IP. *Télématique* , 51-54.

Regis dos Santos, R., Moreiras, A. M., Reis, E., & Soares da Rocha, A. (2010). *Curso IPv6 básico.* Sâo Paulo: Antônio Marcos Moreiras.

Richard Stevens, W. (2011). *TCP/IP Illustrated Volume 1: The protocols.*Michigan: Addison-Wessley.

Trejo Ramírez, G. (17 de 07 de 2012). *Redes Computacionales*. Obtenido de Slideshare: http://www.slideshare.net/GabyRamirez13/redes-computacionales-13269885

Tsirtsis, G., & Srisuresh, P. (2000). *RFC 2766: Network Address Translation - Protocol Translation (NAT-PT).*

Tsuchiya, K., Higuchi, H., & Atarashi, Y. (2000). *RFC 2767: Dual Hosts using the Bump in the Stack technique (BIS).*

UPF. (17 de 09 de 2012). *Universitat Pompeu Fabra - Barcelona*. Obtenido de http://www.upf.edu/estiu/_pdf/1421t1.pdf

Ureña Poirier, H., & Rodríguez Martín, J. (17 de 09 de 2012). *Gobierno de Canarias*. Obtenido de Consejería de Educación, Universidades y Sostenibilidad: http://www.gobiernodecanarias.org/educacion/conocernos_mejor/paginas/ip.htm

Verdejo Alvarez, G. (2000). *El Protocolo IPv6 y sus extensiones de seguridad IPSec.* Barcelona: UAB.

Anexo A: Parámetros de Calidad para la provisión del Servicio de Valor Agregado (SVA) de Internet.

A continuación se mostrarán el resumen de los parámetros de calidad para el SVA de Internet.

#	Código	Parámetro	Valor Objetivo
1	4.1	Relación con el cliente.	Valor objetivo semestral: $R_c \geq 3$
2	4.2	Porcentaje de reclamos generales procedentes.	Valor objetivo mensual: $\%R_g \leq 2\%$ Para permisionarios con menos de 50 clientes conmutados o con menos de 25 cuentas dedicadas, el valor objeto mensual: $R_c \geq 4\%$
3	4.3	Tiempo máximo de resolución de reclamos generales.	Valor objetivo mensual: máximo 7 días para el 98% de reclamos.
4	4.4	Porcentaje de reclamos de facturación.	Valor objetivo mensual: $\%R_f \leq 2\%$
5	4.5	Tiempo promedio de reparación de averías efectivas.	Valor objetivo mensual: $Tra \leq 24\ horas$
6	4.6	Porcentaje de módems utilizados.	Valor objetivo mensual: $\%M_{utilizados} \leq 100$ (durante el 98% del día).
7	4.7	Porcentaje de reclamos por la capacidad del canal de acceso contratado por el cliente.	Valor objetivo mensual: $\%R_c \leq 2\%$

Anexo B: Políticas Regionales IPv6 – CITEL

ORGANIZACION DE LOS ESTADOS AMERICANOS
ORGANIZATION OF AMERICAN STATES

Comisión Interamericana de Telecomunicaciones
Inter-American TelecommunicationCommission

XX REUNIÓN DEL COMITÉ CONSULTIVO	**OEA/Ser.L/XVII.4.1**
PERMANENTE I: TELECOMUNICACIONES/	**CCP.I-TIC/doc. 2608/12**
TECNOLOGIAS DE LA INFORMACION Y LA	**18 mayo 2012**
COMUNICACION	**Original: español**
Del 16 al 19 de mayo de 2012	
Buenos Aires, Argentina	

POLÍTICAS REGIONALES PARA LA ADOPCIÓN Y COEXISTENCIA IPv4 e IPv6 PARA LOS PAISES MIEMBROS DE CITEL
(Punto del temario: 3.1.2)
(Documento presentado por la delegación de Ecuador)

Introducción

La implantación de normas conjuntas y estandarizadas en el ámbito de la Adopción de IPv6, se vuelve imperiosa debido a la necesidad de unificación de criterios para el acceso a Internet en la región y desarrollo de nuevas tecnologías.

El tratamiento de políticas para el impulso de la nueva versión del protocolo de Internet, será un envión para la generación de la sociedad de la información, aprovechando las capacidades brindadas para el desarrollo de nuevas plataformas o contenidos estables y seguros.

La transición hacia IPv6, será una oportunidad para los Estados de promover nuevas formas de negocios para el sector empresarial, basados en la generación de conocimiento y apropiación de tecnologías disponibles para la comunicación y aprendizaje sobre Internet.

Es necesario el emprendimiento de metas y estrategias conjuntas para la Adopción del nuevo protocolo de Internet (IPv6), de forma que se promueva una correcta coexistencia y transición y se impulse el desarrollo regional de nuevas plataformas y contenidos que originen el adelanto económico y la promoción del conocimiento.

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, tomen conciencia de las importancia de este cambio tecnológico y se ejecuten las acciones pertinentes, de tal forma que los usuarios puedan comenzar a utilizar IPv6 de un modo satisfactorio, sin costos adicionales y de forma transparente, caso contrario la Región corre el riego de una nueva “Brecha Digital”.

En tal sentido se propone el siguiente grupo de medidas a adoptarse con el fin de ir implementando un proceso óptimo de implantación del nuevo protocolo:

PROYECTO DE RECOMENDACION
CCP.I/REC. XXX (XX-12)

POLÍTICAS REGIONALES PARA LA ADOPCIÓN Y COEXISTENCIA IPv4-IPv6 PARA LOS PAISES MIEMBROS DE CITEL

La XX Reunión del Comité Consultivo Permanente I: Telecomunicaciones/Tecnologías de la Información y la Comunicación (CCP.I),

CONSIDERANDO:

a. Que es necesario el diseño e implantación de políticas que permitan la estabilidad y el correcto funcionamiento de la red de Internet;

b. Que dentro del Plan de Acción eLAC 2015, se insta a los países miembros a 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 logre un amplio despliegue del Protocolo de Internet versión 6 (IPv6), así mismo hace un llamado a implementar con brevedad planes nacionales que permitan acceder a los portales de servicios públicos gubernamentales de los países de la región a través de IPv6 y que las redes estatales trabajen de forma nativa con IPv6, en coexistencia con IPv4;

c. Que en febrero de 2011 el Registro de Direcciones de Internet de América Latina y el Caribe, LACNIC, comunicó que el stock central de direcciones IPv4 administrado por la IANA (Internet Assigned Numbers Authority) se agotó definitivamente, pues fueron entregados los últimos bloques disponibles de direcciones IPv4 a cada uno de los cinco Registros Regionales de Internet (RIR) en todo el mundo y a partir de esta fecha únicamente se podrá acceder al stock con el que cuenta LACNIC,

RECONOCIENDO:

a. Que es necesario que los Estados Miembros de CITEL, dentro de sus competencias, coordinen con las entidades del sector público y privado la coexistencia de los protocolos IPv4 e IPv6 así como la transición futura a IPv6;

b. Que la implementación de programas de transición IPv4-IPv6, mantendrá la inclusión y cohesión tecnológica de los diversos actores (Gobierno, Academia, Proveedores, Usuarios, etc.);

c. Que la CITEL, a través del CCP.I recomendó que las administraciones difundan entre los proveedores de servicios, equipamiento, software, aplicaciones y servicios para las redes, instituciones educativas, de investigación, desarrollo tecnológico y usuarias de Internet, la información relacionada con la necesidad de prepararse para la convivencia entre IPv4 e IPv6 y su posterior adopción definitiva,

RECOMIENDA:

1. Que los Estados Miembros de CITEL promuevan la construcción participativa e inclusiva de guías de coexistencia y transición IPv4-IPv6 involucrando a todos los

actores del ecosistema de Internet, .a través de la constitución de fuerzas de trabajo (Task Force).

2. Que los Estados Miembros de CITEL realicen un diagnóstico de la situación actual de adopción de IPv6 en cada país y sobre esa línea base estructuren lineamientos y desarrollo de políticas vinculadas con el nuevo protocolo de Internet IPv6.

3. Que las Instituciones y Organismos del Sector Público de los Estados Miembros, implementen en sus sitios web y plataformas de servicios electrónicos, el soporte y compatibilidad con el protocolo IPv6 de manera coexistente con el protocolo IPv4, con la finalidad de generar tráfico IPv6 a nivel nacional y permitir que dichos recursos públicos sigan siendo visibles desde el resto del mundo, esta medida además propenderá al desarrollo del Gobierno en línea de la nueva era.

4. Que los Estados Miembros de CITEL desarrollen marcos referenciales para compras nacionales de IPv6 considerando aspectos como: Equipamiento, software, servicios-aplicaciones, formación de capital humano y usuarios.

5. Que se implementen los procedimientos administrativos o normativos, para garantizar el correcto funcionamiento del protocolo IPv6 en los ccTLD de cada país miembro de CITEL, sin incremento de costos para los usuarios.

6. Que bajo el esquema de “dar ejemplo”, los Entes de Regulación y Rectoría de Telecomunicaciones implementen proyectos piloto sobre IPv6 en sus sitios Web y plataformas de servicio a fin de incentivar al resto de organismos e instituciones públicas a implementar el nuevo protocolo.

7. Que los Estados Miembros consideren la posibilidad de elaborar Estrategias Nacionales de IPv6, con el fin de garantizar una asignación suficiente y adecuada de direcciones IPv6 a cada Estado por parte de los RIR.

8. Que los Estados Miembros estimulen la implementación IPv6 en el sector privado (necesidad de comunicarse con el gobierno).

9. Que se ejecute las acciones y procedimientos administrativos y normativos necesarios con el fin de que los Proveedores de Servicio de Internet ISPs y Carriers, permitan en sus redes, plataformas y servicios la coexistencia de IPv4 - IPv6.

10. Que los Estados Miembros de CITEL ejecuten las acciones necesarias con el fin de que los Proveedores de Servicios de Internet (ISPs), establezcan sus planes de direccionamiento, y en función de los mismos, inicien los trámites para la solicitud de recursos de direccionamiento (direcciones IP) IPv6.

11. Que los Estados Miembros de CITEL realicen campañas de sensibilización, difusión, capacitación y formación de IPv6.

12. Que los Estados Miembros impulsen y financien proyectos tecnológicos con soporte IPv6.

13. Que se propenda a la adopción de IPv6 en redes de investigación y educación.

ENCARGA:

1. Al Secretario Ejecutivo de la CITEL a comunicar esta Recomendación a las delegaciones de los Estados Miembros de la CITEL con el objeto de lograr que la

mayoría de países adopten las medidas propuestas, lo cual permitirá fomentar la implementación de políticas conjuntas para la adopción de IPv6.

2. Al Secretario Ejecutivo de la CITEL para que transmita al Comité Directivo Permanente de la CITEL (COM/CITEL) esta Recomendación para su conocimiento.