MECANISMOS UTILIZADOS EN EL PROCESO DE TRANSICIÓN E INTEROPERABILIDAD DE IPV4 HACIA IPV6

FABIÁN ENRIQUE LEÓN ISAZA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
ESCUELA DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2011

MECANISMOS UTILIZADOS EN EL PROCESO DE TRANSICIÓN E INTEROPERABILIDAD DE IPV4 HACIA IPV6

FABIÁN ENRIQUE LEÓN ISAZA

Monografía para optar por el título de
Especialista en Telecomunicaciones

Director
ÓSCAR GUALDRÓN GONZÁLEZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER
ESCUELA DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2011

A mi hijo Daniel David,

a mi señora Sandra,

a mis padres y a mis hermanos,

por todo el amor y el apoyo

incondicional.

TABLA DE CONTENIDO

pág.

RESUMEN

TÍTULO:
MECANISMOS UTILIZADOS EN EL PROCESO DE TRANSICIÓN E INTEROPERABILIDAD DE IPV4 HACIA IPV6*

AUTOR:
FABIÁN ENRIQUE LEÓN ISAZA**

PALABRAS CLAVE:
IPv4, IPv6, Internet, direcciones privadas, direcciones públicas, mecanismos de transición.

DESCRIPCIÓN:

IPv4 es el principal protocolo de nivel de capa de red utilizado, y es el que permite la comunicación entre dispositivos en una red. Aunque IPv4 puede ofrecer 4.294.967.296 direcciones únicas (2^{32}), ubicadas en direcciones privadas y direcciones púbicas, no son suficientes debido al tamaño que tiene Internet. De hecho, hoy en día ya no quedan direcciones disponibles.

El protocolo IPv6, a diferencia del protocolo IPv4, nos ofrece 340 sextillones de direcciones únicas (2^{128}) sin distinción entre direcciones privadas y direcciones públicas, es decir, todas son asignables a cada equipo de toda la red mundial o para cada persona del planeta si así se quisiera.

Como no se puede detener Internet y las comunicaciones globales por las repercusiones que habrían, ni hacer un proceso macro de cambio de IPv4 a IPv6 y cambiar dispositivos, programas e infraestructura inmediatamente, se está viviendo una etapa de interoperabilidad entre los dos protocolos mientras se hace la transición a IPv6.

Esta monografía expone los mecanismos de transición que existen como alternativas en esta etapa importante de interoperabilidad entre los protocolos de Internet y se organizan de forma clara y explicativa, con el fin de ofrecer a las personas un documento que funcione como referencia en el estudio o de manera informativa sobre los procedimientos que se emplean en el día a día en las redes del mundo entero. La documentación se divide en una parte introductoria y luego tres grandes capítulos, en donde se expone cada mecanismo, sus ventajas y desventajas.

Con esta monografía se busca además que las personas interesadas en este tema, encuentren lo que necesitan saber sobre estos mecanismos en un solo lugar, sin necesidad de buscar desde el principio en fuentes diferentes, por lo menos hasta que se tenga una idea clara de lo que aquí se expone y se decida complementar o indagar aún más.

---

* Monografía.

** Facultad de Ingenierías Físico-Mecánicas. Escuela de Ingeniería Eléctrica, Electrónica y de Telecomunicaciones. Director: Ph.D Óscar Gualdrón González.

ABSTRACT

TITLE:
MECHANISMS USED IN THE INTEROPERABILITY AND TRANSITION PROCESS FROM IPV4 TO IPV6*

AUTHOR:
FABIÁN ENRIQUE LEÓN ISAZA**

KEYWORDS:
IPv4, IPv6, Internet, private addresses, public addresses, transition mechanisms.

DESCRIPTION:

IPv4 is the main network-layer protocol used in the world, and allow the communication between devices in a network. Even though IPv4 can offer 4.294.967.296 unique addresses (2^{32}), all located in public and private addresses, they are not enough because of the size of the Internet. In fact, today there are no longer available addresses.

The IPv6 protocol, contrary to IPv4, can offer up to 340 sextillion unique addresses (2^{128}) with no distinction between private and public addresses, which means that they all could be assigned to each device in the entire worldwide network or to each person in the world if that would be necessary.

As we cannot shut down neither Internet nor the global communications due to the negative repercussions, or to make a sudden change between IPv4 and IPv6, changing devices, programs and infrastructure, we opt for living an interoperability period between the two protocols while the transition to IPv6 is complete.

This monograph presents the transition mechanisms as an alternatives in this important interoperability period and it is organized in an explicative and a clear text to understand, offering to the people a document as a reference for studying or as an informative way about the procedures used in the worldwide network today. This document is divided first into an introductory part, and then into three main chapters, each one describing all the mechanisms along with their advantages and disadvantages.

This monograph is intended to provide to the people interested in this subject a single spot to access to all the mechanisms with a complete documentation, with no need to search in many other documents related to this subject from the beginning, at least until further information or a deep research is necessary.

---

*Monograph.
** Faculty of Physics and Mechanics. School of Electrical, Electronics and Telecommunications Engineering. Director: Ph.D Óscar Gualdrón González.

GLOSARIO

IPV4: Es el protocolo de Internet versión 4, el cual está compuesto de direcciones de 32 bits y que tiene como finalidad de proveer de una dirección única a cada nodo de la red para asegurar su comunicación e identificación.

IPV6: Es el protocolo de Internet versión 6, compuesto de direcciones de 128 bits y que tiene como finalidad de proveer de una dirección única a cada nodo de la red para asegurar su comunicación e identificación. Está destinado a sustituir al protocolo IPv4 debido a las ventajas con las que cuenta.

NAT (*Network Address Translation*): El Traductor de Direcciones de Red es un mecanismo utilizado para asignar un conjunto de direcciones IP a uno o varios nodos estáticamente o dinámicamente.

IETF (*Internet Engineering Task Force*): El Grupo Especial sobre Ingeniería de Internet es una organización de naturaleza abierta enfocada a la ingeniería de Internet y que tiene como objetivo proteger la estructura y los protocolos que conforman el Internet.

IANA (*Internet Assigned Numbers Authority*): La Agencia de Asignación de Números de Internet asignaba anteriormente los registros de Internet, tales como números, puertos opciones.

ICANN (*Internet Corporation For Assigned Names and Numbers*): Sustituyó a la IANA en 1998 y se encarga de las tareas que anteriormente esta realizaba.

RFC (*Request For Comments*): Las Peticiones de Comentarios son una serie de documentos que sirven para referenciar un protocolo, un estándar o un servicio de Internet.

IPSEC (*Internet Protocol Security*): Es un conjunto de protocolos que tienen como objetivo principal brindar protección a los paquetes IP.

QOS (*Quality Of Service*): Son tecnologías que tienen como principal objetivo dar un buen servicio, garantizando la transmisión de información de cierta cantidad de información en un tiempo dado.

ARP (*Address Resolution Protocol*): El Protocolo de Resolución de Direcciones es encargado de encontrar la dirección MAC de un nodo por medio de la dirección IP asignada a este.

IGMP (*Internet Group Management Protocol*): El Protocolo de Administración de Grupos de Internet es utilizado en las redes IP para el intercambio de información y tráfico multicast.

ICMP (*Internet Control Message Protocol*): El Protocolo de Mensajes de Control de Internet es el encargado de la notificación de errores del protocolo IP.

DHCP (*Dynamic Host Configuration Protocol*): El Protocolo de Configuración Dinámica de Host permite entregar a usuarios específicos parámetros de configuración de manera automática.

DNS (*Domain Name System*): El Sistema de Nombres de Dominio es el encargado de asociar una dirección IP con un nombre de dominio específico.

OUI (*Organizationally Unique Identifier*): El Identificador Único Organizacional es un número de 24 bits que identifica a cada empresa u organización a nivel mundial y que reserva un bloque de de las direcciones, identificadores, etc.

HTTP (*Hypertext Transfer Protocol*): El Protocolo de Transferencia de Hipertexto es el protocolo que se utiliza en cada transacción de Internet.

INTRODUCCIÓN

Debido al gran crecimiento de internet y de las comunicaciones globales, el crecimiento de las redes IPv4 se ve cada vez más limitada y su implementación cada vez más reducida. Hoy en día el número de direcciones IPv4 disponibles es 0%, ya que desde el 1 de febrero del 2011 estas están agotadas.

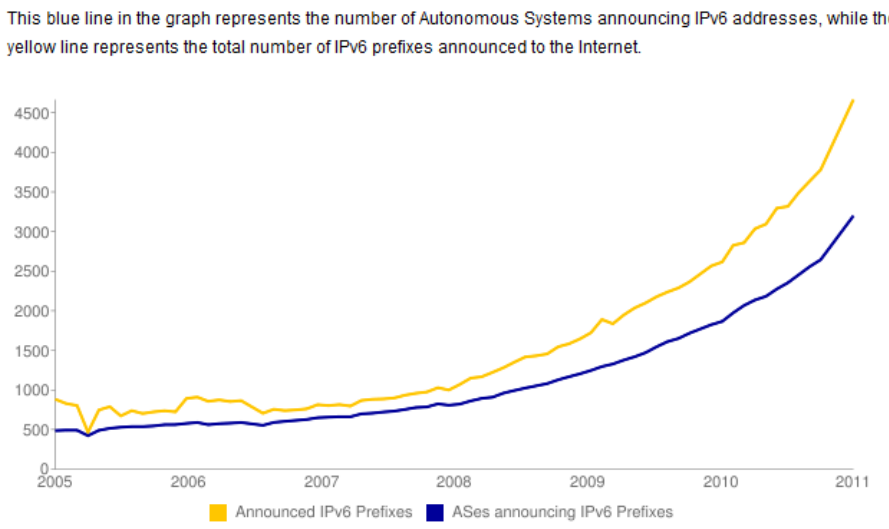
Ante la alarma que se generó hace casi una década atrás cuando se determinó que las direcciones IPv4 asignables se agotarían rápidamente, se optó por implementar mecanismos que de alguna manera le dieran un tiempo extra al consumo total de las direcciones IPv4, tal como la Traducción de Dirección de Red NAT *(Network Address Translation*) que permite que varios nodos de una red interna tengan acceso a internet con una dirección pública.

Estas prácticas han hecho posible que IPv4 sobreviva mucho más tiempo del previsto y que por consiguiente, la utilización de IPv6 se vea forzada a la espera. Pero, aún cuando NAT ha sido de mucha ayuda, este ha generado un conjunto de desventajas en la utilización de aplicaciones tales como VoIP, P2P, video conferencia, etc. a causa de que NAT no permite el normal funcionamiento de servicios extremo a extremo.

Este tipo de problemas y la falta cada vez mayor de direcciones públicas, han hecho que la implementación de IPv6 sea mayor, sumando a esto las ventajas que implementa este protocolo trae, tales como escalabilidad, accesibilidad, servicio extremo a extremo, QoS, VoIP, IPTV (IP Based TV), triple play networks, movilidad, etc.

Debido a que el tamaño de internet es colosal, hablar de migración de IPv4 a IPv6 es algo que tomaría un tiempo largo en suceder, por lo que hoy en día se vive un ambiente de interoperabilidad y de transición entre estos dos protocolos, en el cual lenta y progresivamente las redes (sistemas autónomos) van adoptando el protocolo IPv6, tal y como se muestra a continuación (Gráfica 1):

Gráfica 1. Relación de las direcciones IPv6 anunciadas por los sistemas autónomos desde el 2005 al 2011.



Fuente: IPv6 Act now http://www.ipv6actnow.org/info/statistics/.

Hoy en día se vive un panorama de transición entre estos dos protocolos, en los cuales se implementan principalmente tres mecanismos, cada una de estas con una serie de mecanismos importantes por destacar y con un conjunto de procedimientos que facilitan la utilización de una o de otra técnica, según las necesidades de la red.

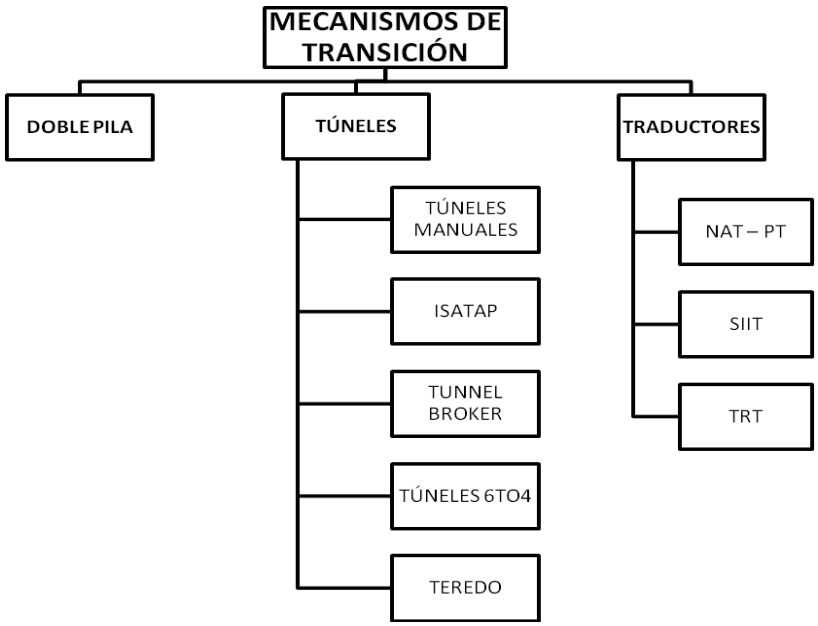
Los principales mecanismos de transición utilizados hoy en día en el proceso de transición de IPv4 a IPv6 y que se exponen aquí son:

- **Mecanismo de doble pila (*Dual stack Mechanism*).**
- **Mecanismo de túneles (*Tunneling Mechanism*).**
- **Mecanismo de traducción de protocolos (*Translation Mechanism*).**

Este documento, en su naturaleza de estudio de caso, busca mostrar la ciencia de cada uno de estos mecanismos, sus características, ventajas y desventajas reunidos en un sólo punto, el cual estará al alcance de todos, que sirva como base para la investigación, lectura, análisis y un espacio para la crítica.

La monografía se expone primero una parte introductoria en la que se habla de las diferencias entre los protocolos IPv4 e IPv6 y se termina hablando de cada mecanismo de la forma más clara y completa posible, describiendo ventajas y desventajas que presentan (Figura 1):

Figura 1. Mecanismos de transición tratados en la monografía.



Conociendo este proceso, podemos ver la realidad que existe detrás de las comunicaciones y de Internet, de esta transformación que se está viviendo y de una serie de debates y de interrogantes que surgen pensando en el futuro. Sería importante llegar a comprender el por qué se implementa una u otra técnica de transición conociendo las características que cada una ofrece y de tener una idea sustentada en el conocimiento.

Para nosotros los que nos desempeñamos en el área de las telecomunicaciones, los apasionados o los interesados en este mundo que continuamente se encuentra en evolución es interesante saber sobre el día a día de este proceso, ya que nos permitiría no sólo ser espectadores o ignorantes, sino jueces o críticos de esta transformación.

1. OBJETIVOS

1.1. OBJETIVO GENERAL

- Exponer los mecanismos de transición de Ipv4 a Ipv6 existentes (Doble pila, túneles y traductores de protocolo), las características de cada uno de estos y además las ventajas y desventajas que estos ofrecen.

1.2. OBJETIVOS ESPECÍFICOS

- Describir los mecanismos que se ofrecen en el proceso de coexistencia y de transición entre los protocolos Ipv4 e Ipv6.

- Describir las ventajas y desventajas que ofrece cada mecanismo de transición, de manera que se conozca a fondo qué pueden ofrecer estos en una red específica, dependiendo de su naturaleza.

- Elaborar una documentación en la que se identifiquen los mecanismos de transición de forma clara, precisa y que se sirva como referencia en el estudio de esta etapa de las redes de comunicaciones.

2. ALCANCE

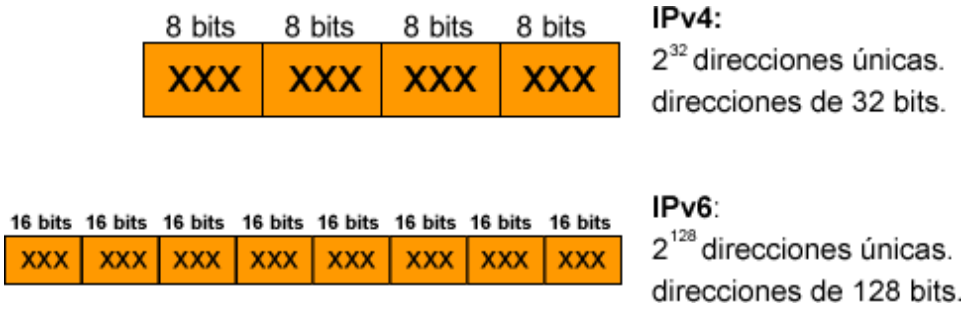
Esta monografía se realizó con el propósito de servir como base en el conocimiento de esta etapa que actualmente se está viviendo en las comunicaciones e Internet y con el fin de que se convierta en un medio en el que se pueda estudiar sobre las características de los mecanismos de transición, todos estos en un solo punto de referencia, estructurado de forma que no resultará imprescindible si se está investigando sobre este tema.

3. IPV4 VS. IPV6

El protocolo IPv6 (RFC 2460) se caracteriza por presentar mejoras, cambios en sus características y por resolver problemas que se presentaban con el protocolo IPv4 (RFC 791), tales como direccionamiento, tamaño de la cabecera, opciones de movilidad, seguridad, etc.

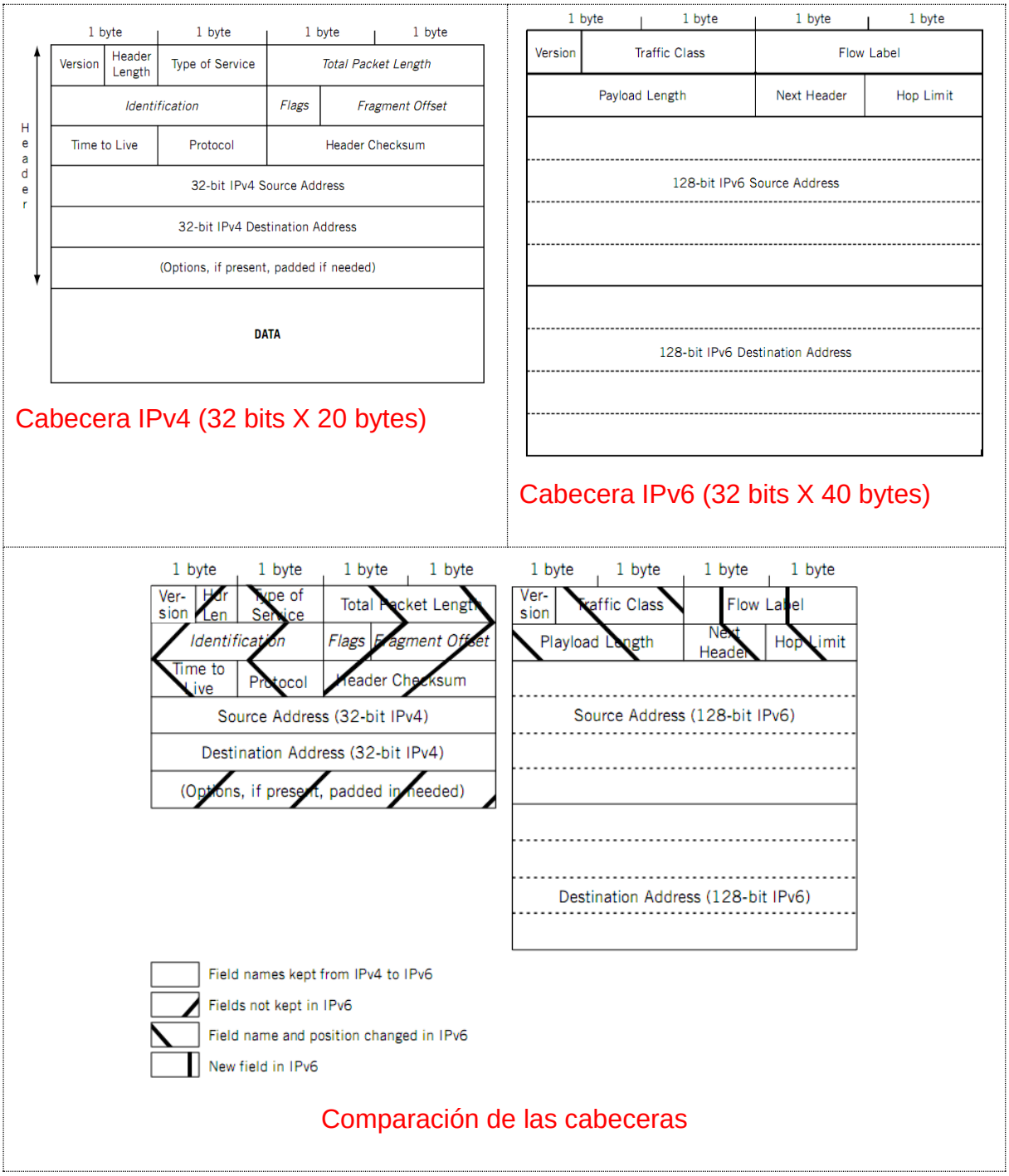
Una de las diferencias principales entre las cabeceras de estos protocolos es la longitud de sus direcciones, ya que IPv4 cuanta con direcciones de 32 bits, mientras que IPv6 cuenta con direcciones de 128 bits (Figura 2).

Figura 2. Comparación entre las direcciones IPv4 e IPv6.



Otra característica de la cabecera de IPv6 es que siempre es de 40 bytes, al contrario de IPv4, que es mínimo de 20 bytes y que se ve modificado según el campo “opciones”, que no es requerido en todos los paquetes. Además, la cabecera IPv6 siempre es de 8 campos, es decir, la mitad de los campos que posee una cabecera IPv4, por lo que se procesa mucho más rápido que la cabecera IPv4 y por ende, más rápido es el paso a la capa superior (Figura 3).

Figura 3. Cabecera IPv4 vs. cabecera Ipv6.



Fuente: GORALSKI, Walter. IPv4 and IPv6 Headers. En: The Illustrated Network. 2009. Elsevier Inc.

Para resumir, las diferencias más relevantes entre el protocolo IPv4 e IPv6 son:

Tabla 1. Diferencias entre IPv4 e IPv6.

IPV4	IPV6
Las direcciones tienen una longitud de 32 bits (4bytes).	Las direcciones tienen una longitud de 128 bit (16 bytes).
La compatibilidad con IPsec es opcional	La compatibilidad con IPsec es obligatoria.
No hay identificación de carga para el control de QoS por parte de los enrutadores en la cabecera de IPv4, pues aunque está el campo tipo de servicio, este no está implementado.	La identificación de carga para el control de QoS por parte de los enrutadores se incluye en la cabecera de IPv6 mediante los campos etiqueta de flujo y clase de tráfico.
La fragmentación es posible en los enrutadores y en el host de envío.	La fragmentación no es posible en los enrutadores. Sólo es posible en el host de envío.
La cabecera incluye una suma de comprobación (*checksum*).	La cabecera no incluye una suma de comprobación (*checksum*) porque otros mecanismos de encapsulado ya realizan esta función.
La cabecera incluye opciones.	Todos los datos opcionales se mueven a extensiones de la cabecera IPv6
El Protocolo de Resolución de Direcciones (ARP) utiliza tramas de solicitud de ARP de difusión para resolver una dirección de IPv4 en una dirección de nivel de enlace.	Las tramas de solicitud de ARP se reemplazan por mensajes “Solicitud de Vecino” *(Neighbor Solicitation)* de multidifusión.
Se utiliza el Protocolo de administración de grupos de Internet (IGMP) para administrar la pertenencia a grupos de subredes locales.	El protocolo IGMP se reemplaza por mensajes de Descubrimiento de Escucha de Multidifusión, MLD *(Multicast Listener Discovery)*.
Para determinar la dirección IPv4 de la mejor puerta de enlace predeterminada se utiliza el descubrimiento de enrutadores de ICMP, que es opcional.	Para determinar la dirección IPv6 de la mejor puerta de enlace predeterminada se utilizan los mensajes Solicitud de Enrutador (*Router Solicitation*) y Anuncio de Enrutador (*Router Advertisement*) ICMPv6, que son necesarios.

Tabla 1. (Continuación)

Las direcciones de difusión se utilizan para enviar tráfico a todos los nodos de una subred.	No hay direcciones de difusión en IPv6. En su lugar, se utiliza una dirección de multidifusión para todos los nodos de ámbito local de enlace.
La configuración debe efectuarse manualmente o a través de DHCP.	La configuración puede ser manual, por DHCPv6, o de forma automática, Descubrimiento Automático.
Utiliza registros A de dirección de host en el Sistema de Nombres de Dominio DNS (*Domain Name System*) para asignar nombres de host a direcciones IPv4.	Utiliza registros AAA de dirección de host en el DNS para asignar nombres de host a direcciones IPv6.

Fuente: NÚÑEZ, Alejandro. Evolución del Protocolo de Internet hacia IPv6. En: Revista Técnica de la Empresa de Telecomunicaciones de Cuba. 2006. Publicación 2.

Adicionalmente a lo expresado en la Tabla 1, es importante resaltar que:

- En Ipv4 el soporte para QoS no es el adecuado, ya que se está destinando para este servicio sólo 3 bits de los 8 bits del campo TOS *Type Of Service* (Figura 3), que permite sólo indicar la prioridad del envío de los paquetes. Este campo nunca fue ampliamente utilizado y en lugar de esto fue redefinido por los Servicios Diferenciales, DS o DiffServ, utilizados en el campo DSCP (Punto de Código de Servicios Diferenciados) (implementado también en IPv6), que no es más que los primeros 6 bits del campo TOS. De esta forma, se permite un poco más de complejidad a la hora de tratar los distintos paquetes, pero debido a que Diffserv no es orientado a reservación, los servicios no están estrictamente garantizados, además la red puede tornarse congestionada debido a que no hay reserva de ancho de banda en cada transmisión, provocando que se pierdan por ejemplo paquetes etiquetados con baja prioridad o mal etiquetados. Aunque en el protocolo IPv6 se busca mejorar las desventajas que en IPv4 se tienen en cuanto a QoS, no ofrece un soporte muy superior en comparación con el de IPv4. Con el campo Etiqueta de flujo se busca identificar de forma única

cada paquete que se genera, con el fin de que los routers puedan diferenciar cada uno de estos más rápidamente.

- La fragmentación es uno de los más grandes problemas de IPv4, y está presente en cada paquete transmitido y cada paquete puede ser fragmentado por cada router de la red si el tamaño de este excede la MTU especificada. De esta forma, un router fragmenta cada paquete y los vuelve a encapsular de manera independiente. Con este proceso se produce mayor congestión en la red, mayor procesamiento de los dispositivos y mayor consumo de ancho de banda de la red. En Ipv6 la fragmentación sólo es realizada por los nodos que transmiten, por lo que se desplaza este alto procesamiento a este punto.

- Con la configuración por descubrimiento automático de Ipv6 se busca que cada nodo de la red obtenga los parámetros automáticamente sin necesidad de que en la red se tenga implementado un protocolo de configuración o de una configuración manual preestablecida, es decir, con sólo conectarse a la red, obtiene su configuración. Esta característica permitirá que la conexión a una red no dependa de parámetros iniciales, dando cabida a aplicaciones como por ejemplo casas o edificios inteligentes, en donde todos los dispositivos electrónicos presentes se encuentren conectados entre sí y además potenciando el uso simple de las redes inalámbricas. La utilización del descubrimiento automático y de DHCPv6 es materia de discusión, ya que, mientras DHCPv6 ofrece una configuración dedicada a los nodos de la red, el descubrimiento automático simplifica el proceso de configuración de una manera radical, haciendo el proceso mucho más simple. La desventaja principal del descubrimiento automático radica en que este no provee de parámetros como servidor DNS, servidor WINS, dominio DNS, etc.

3.1. MECANISMOS DE TRANSICIÓN DE IPV4 A IPV6

El protocolo IPv6 es el protocolo que reemplazará al protocolo IPv4 y tomará en sus manos las riendas de las comunicaciones globales.

El lento proceso de migración entre estos dos protocolos ha causado que se viva en un estado de interoperabilidad y de una etapa de transición que permita su coexistencia. Este proceso de transición debe atravesar un camino lleno de obstáculos y dificultades, los cuales implican cambios y modificaciones en aplicaciones, hardware, equipos y mentalidades, entre otros.

Los principales mecanismos de transición definidos por el Grupo Especial Sobre Ingeniería de Internet IETF (*Internet Engineering Task Force*) son:

- **Mecanismo de doble pila (*Dual stack Mechanism*).**
- **Mecanismo de túneles (*Tunneling Mechanism*).**
- **Mecanismo de traducción de protocolos (*Translation Mechanism*).**

4. MECANISMO DE DOBLE PILA

Este mecanismo está definido en RFC 4213.

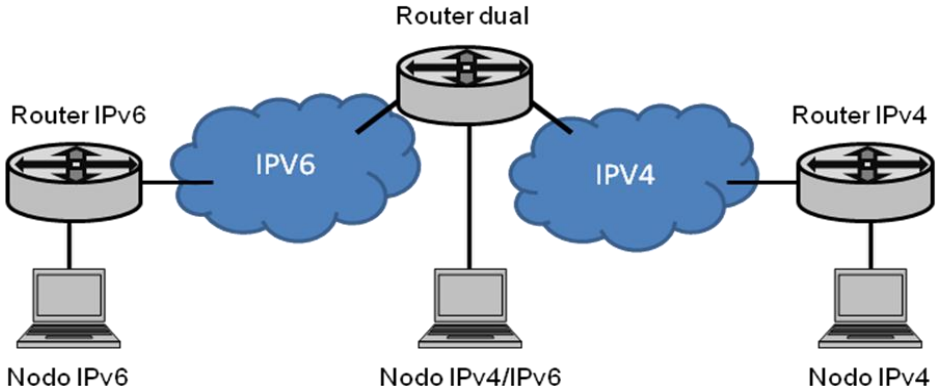
Con este tipo de mecanismo se busca que a lo largo de la red con IPv4 y con IPv6 exista un escenario de interoperabilidad, implementando pilas de IPv4 y de IPv6, funcionando en paralelo en los routers o en los nodos.

De esta manera, cuando un nodo IPv4 necesite comunicarse con un nodo IPv6, utilice datagramas IPv6 y que en el caso contrario también sea posible.

Existen tres tipos de nodos (Figura 4):

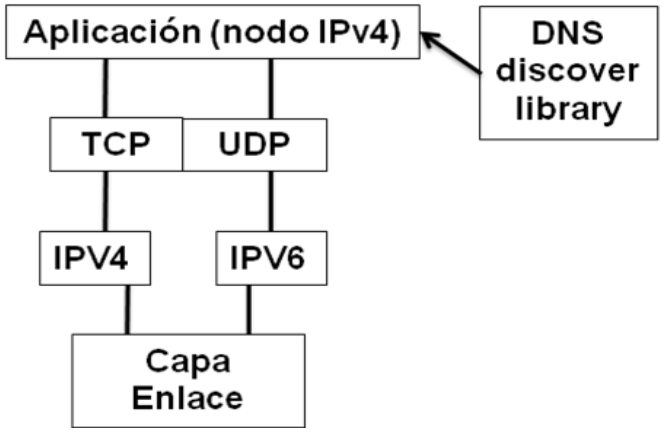
- **Nodos con IPv4 e IPv6 (nodos IPv4/IPv6).**
- **Nodos con sólo IPv4 (nodos IPv4).**
- **Nodos con sólo IPv6 (nodos IPv6).**

Figura 4. Nodos IPv4, IPv6 e IPv4/IPv6.



Cuando se envían paquetes, el tipo de dirección destino recibido de las capas superiores, determina la pila adecuada a utilizar. Las aplicaciones se encargan de escoger la versión IP a utilizar teniendo en cuenta el tipo de dirección que le proporciona el DNS (DNS *Resolver Library*) (Figura 5).

Figura 5. Arquitectura doble pila.



Las respuestas del DNS son de registros A para direcciones Ipv4 y de registros AAAA para IPv6.

Las aplicaciones determinan si están habilitados para recibir registros de IPv4, IPv4 o de ambos.

4.1. VENTAJAS Y DESVENTAJAS DEL MECANISMO DE DOBLE PILA

- Gracias a la implementación del mecanismo de doble pila se permite la coexistencia de los protocolos IPv4 e IPv6 y la migración gradual hacia IPv6.

- Con este mecanismo se tiene la ventaja de que los nodos permanecen con su configuración original.

- Es importante que para la utilización de este mecanismo, los dispositivos tengan implementado o que tengan la posibilidad de implementar las dos pilas, lo que significa un incremento en los costos de las redes.

- Con el mecanismo de doble pila se le adiciona un incremento a la carga de procesamiento de los dispositivos, ya que se están ejecutando dos protocolos de manera paralela, además de hacer más compleja la administración de las redes.

- El mecanismo de doble pila representa la forma más básica de transición de IPv4 a IPv6. Ofrece la ventaja que cuando las configuraciones y los nodos dejen de ser IPv4, sólo habría que deshabilitar las pilas Ipv4 y no afectar la disposición de las redes.

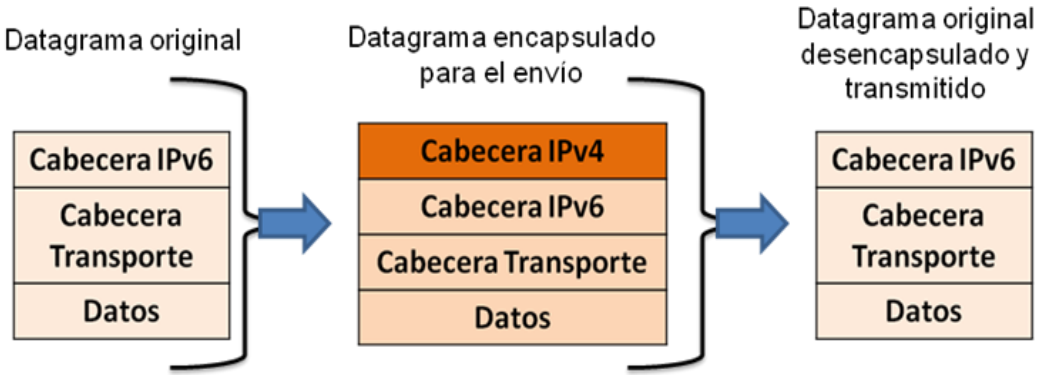
- Es necesario implementar doble seguridad en las redes en las que se utiliza este mecanismo, seguridad para IPv4 y para IPv6, tal y como si existieran dos redes separadas.

5. MECANISMO DE TÚNEL

Este mecanismo está definido en RFC 4213.

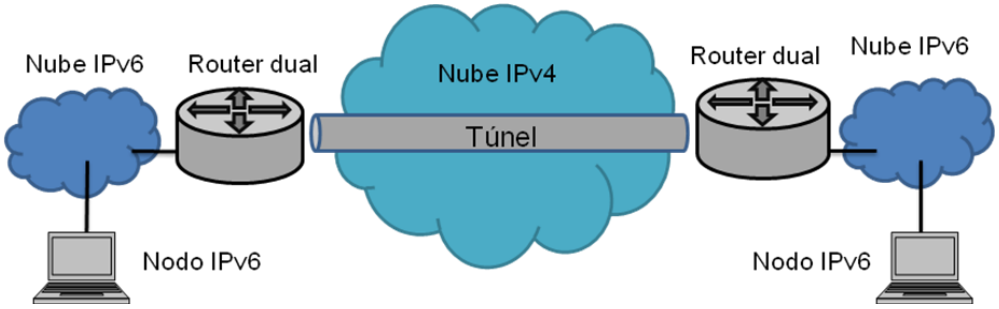
Mediante este tipo de mecanismo es posible la interconexión de extremos en IPv6 por medio de túneles a través de redes o “nubes” de protocolo IPv4. Los túneles se establecen mediante el encapsulamiento de los datagramas en el origen, y de esta forma viajan hasta el destino, en donde son desencapsulados nuevamente (Figura 6).

Figura 6. Proceso de encapsulado y desencapsulado.



De esta forma se logra el transporte de datos IPv6 sobre redes IPv4, utilizando IPv4 como medio de transporte. Los routers de frontera o de extremos deben tener configurado el mecanismo de doble pila con el objetivo de que puedan encapsular en IPv4 y luego desencapsular y leer IPv6 (Figura 7).

Figura 7. Expresión básica del mecanismo de túnel.



Fuente: MORENO, Axel. Ipv6 Interoperabilidad y Robustez. Tesis de maestría. México DF: Instituto Politécnico Nacional, 2004.

En la figura 7 se muestra además que el túnel es de tipo router–router, logrando transmitir datos desde una de las nubes IPv6 hacia la otra nube y en sentido opuesto. Las otras dos posibilidades son host-router y host-host.

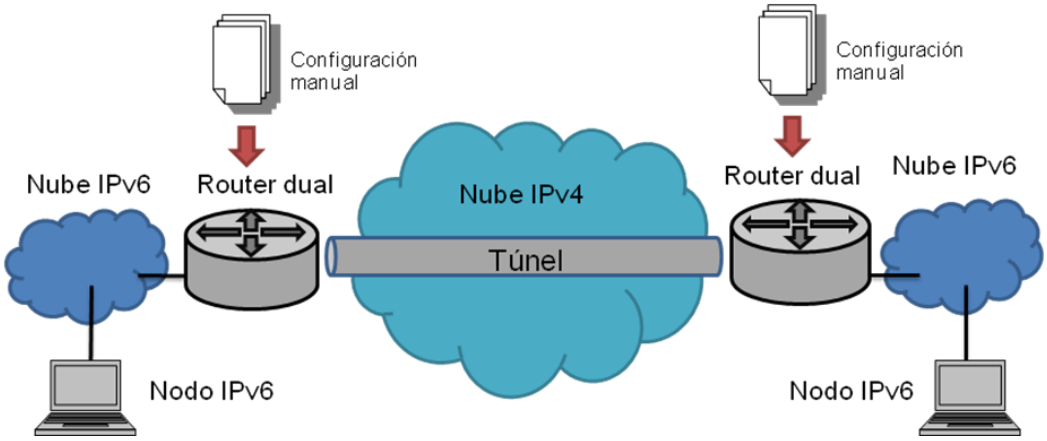
Los mecanismos de túnel definidos son:

- **Túneles manuales.**
- **ISATAP.**
- **Tunnel Broker.**
- **Túneles 6to4.**
- **Teredo.**

5.1. MECANISMO DE TÚNELES MANUALES

Mediante este mecanismo se establecen los túneles de manera permanente entre dos puntos IPv6, configurando manualmente las rutas de origen y destino. Es aconsejable utilizar este tipo de mecanismo de túnel sólo si la red se conoce muy bien y si ésta no es dinámica (Figura 8).

Figura 8. Mecanismo de túnel manual.



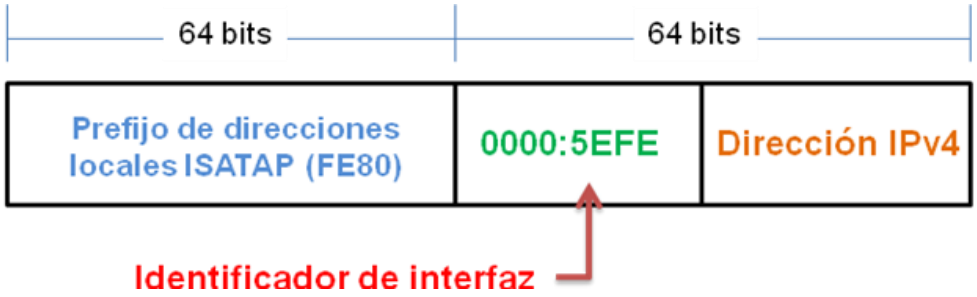
El mecanismo de túnel manual tiene la ventaja de no consumir demasiados recursos, ya que la configuración es siempre la misma (estática).

5.2. MECANISMO ISATAP

Este mecanismo está definido en RFC 5214.

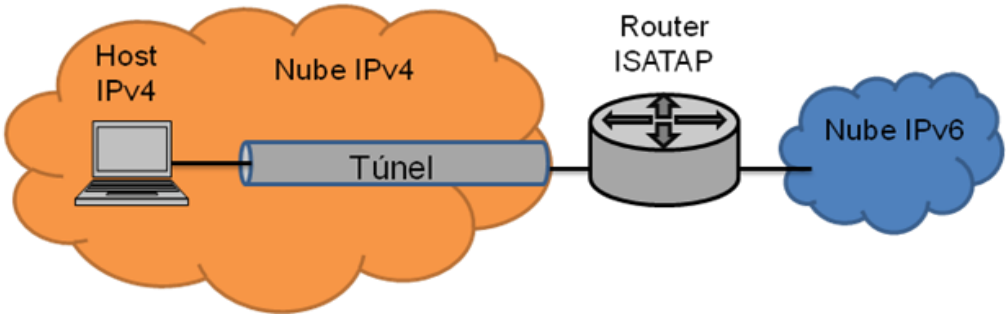
El mecanismo ISATAP (*Intra-Site Automatic Addressing Protocol*) provee de conexión a los nodos IPv4, asignándoles automáticamente una dirección IPv6. Está dirección IPv6 es generada a través de la concatenación de la dirección ISATAP fe80:0000:0000:0000:0000:5efe:0000:0000 (FE80::5EFE:) y la dirección IPv4 del nodo (Figura 9) (Figura 10).

Figura 9. Formato de dirección ISATAP.



Fuente: AMOSS, John y MINOLI, Daniel. Handbook of Ipv4 to Ipv6 Transition. Estados Unidos: Auerbach Publications, 2008.

Figura 10. Mecanismo ISATAP.



El identificador de interfaz (0000:5EFE) consta del "5E" que representa Identificador Único Organizacional OUI (*Organizationally Unique Identifier*) y del "FE", que indica que viene una dirección IPv4 en el formato de dirección.

Entonces, si por ejemplo la dirección origen del host a transmitir es 192.168.5.2, la dirección ISATAP sería:

Dirección origen: 192.168.5.2 → En notación hexadecimal = C0A8:52
Entonces, la dirección origen en IPv6 para ésta dirección origen IPv4 sería: FE80::5EFE: + C0A8:52 → **FE80::5EFE:C0A8:52**.

El mecanismo ISATAP utiliza IPv4 como un nivel de enlace de datos en una red sin multicast, y asumiendo que la red transmisora sólo tiene capacidades en unicast.

ISATAP habilita el mecanismo de túnel sin importar si son direcciones IPv4 privadas o públicas y tiene la capacidad de operar en redes en donde el direccionamiento IPv6 no está disponible. Este mecanismo además permite que los sistemas se actualicen automáticamente y no que cada nodo de la red lo tenga que hacer simultáneamente.

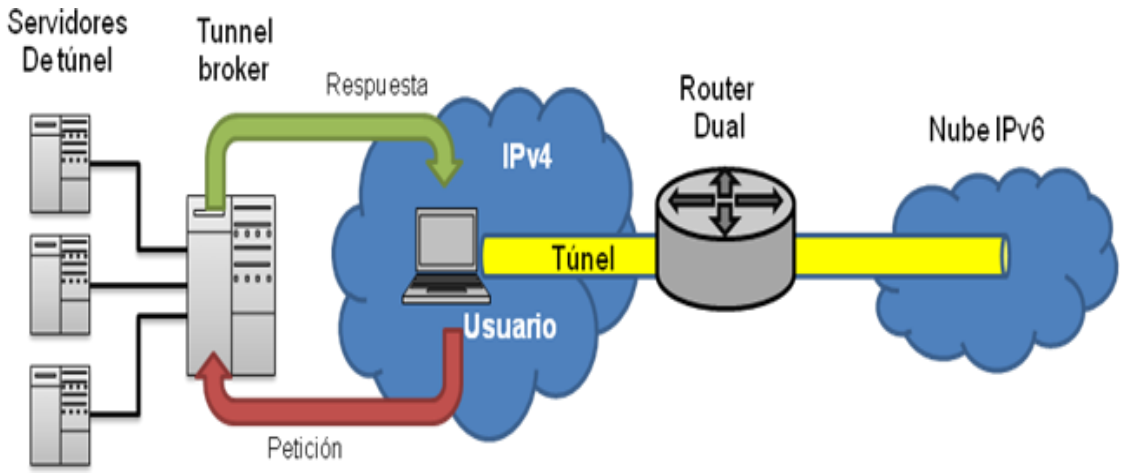
5.3. MECANISMO TUNNEL BROKER

Este mecanismo está definido en RFC 3053.

El mecanismo de Tunnel broker provee de una configuración automática a los usuarios (hosts o routers) sobre redes IPv4. Este mecanismo actúa como un servidor, el cual recibe las peticiones de los clientes y activa un túnel automáticamente, proporcionando la configuración, encapsulando los datos y tunelizándolos a través de IPv4.

Las peticiones son enviadas a través de HTTP por el nodo que desea crear el túnel al tunnel broker. El tunnel broker puede compartir la carga con diferentes servidores de túnel para proporcionar así escalabilidad en el mecanismo. Cabe resaltar que el tunnel broker administra el túnel, es decir, lo crea, lo modifica y lo elimina, según las indicaciones del usuario (Figura 11).

Figura 11. Mecanismo Tunnel broker.



Es importante que tanto el usuario como el tunnel broker puedan interpretar datos IPv4 e IPv6. El usuario debe contar con el mecanismo de doble pila.

Algunas de las empresas que actualmente prestan el servicio de tunnel broker son:

- Hurricane Electric: http://tunnelbroker.net/
- The XS26 Project: http://www.xs26.net/Project/Home.aspx
- Janet IPv6: http://www.broker.ipv6.ac.uk/
- Gogo6: http://gogonet.gogo6.com/
- AARNet IPv6: http://broker.aarnet.net.au/

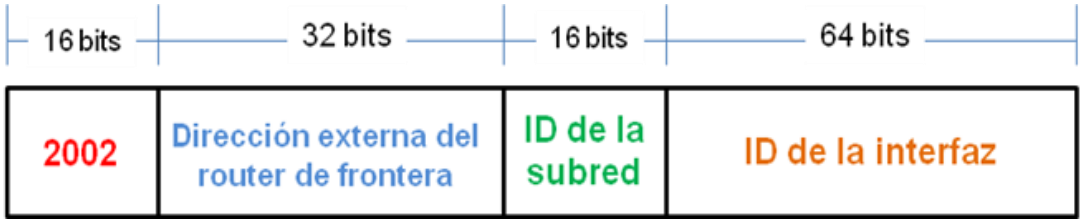
5.4. MECANISMO DE TÚNELES 6TO4

Este mecanismo está definido en RFC 3053.

El mecanismo de túneles 6to4 crea la conexión de routers o de hosts a través de una nube IPv4 y de aquí a otras nubes IPv6 mediante una configuración automática. Permite entonces enviar paquetes IPv6 sobre IPv4 mediante el encapsulamiento de los paquetes IPv6 en IPv4 y utilizando en el campo "protocolo" de la cabecera de IPv4 el protocolo 41, el cual indica que existe un paquete IPv6 dentro del paquete IPv4.

La dirección IPv6 es generada a través de la concatenación del identificador TLA (*Top-Level Aggregation*) 2002::/16, asignado por La Agencia de Asignación de Números de Internet IANA (*Internet Assigned Numbers Authority*) hoy ICANN (*Internet Corporation For Assigned Names and Numbers*) para identificar una dirección 6to4 y la dirección IPv4 del router 6to4. (Figura 12).

Figura 12. Esquema de direccionamiento 6to4.



Fuente: AMOSS, John y MINOLI, Daniel. Handbook of Ipv4 to Ipv6 Transition. Estados Unidos: Auerbach Publications, 2008.

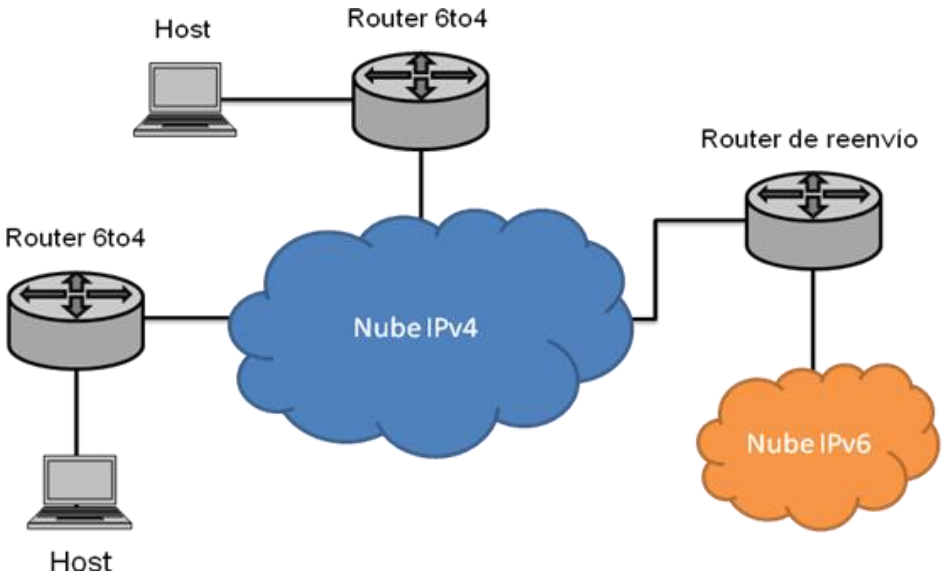
La dirección 6to4 se obtiene de la siguiente manera:

Prefijo 6to4: 2002:: + Dirección IPv4 (hexadecimal) AA.BB.CC.DD → **Dirección 6to4 = 2002:AABB:CCDD::**
Entonces, si por ejemplo la dirección Ipv4 es 192.168.5.3 → Dirección 6to4 es: 2002:C0A8:0503::1.

Es importante resaltar que ya sea para la conectividad entre routers o entre hosts se necesita una dirección IPv4 pública.

El mecanismo 6to4 básico se puede observar en la Figura 13:

Figura 13. Mecanismo 6to4.



El router de reenvío (*Relay router*) es el encargado de transmitir el tráfico 6to4 entre los routers de frontera y los nodos de la nube IPv6.

6to4 es el mecanismo de tunelización más utilizado hoy en día. Para este mecanismo existe la ventaja de que los nodos no requieren de configuración manual y además de que los túneles se crean dinámicamente según las necesidades de direccionamien

5.5. TEREDO

Este mecanismo está definido en RFC 4380.

Este mecanismo tiene la función de crear un túnel automático entre nodos IPv4/IPv6 a través de IPv4 y que se encuentran detrás de Traductores de Direcciones de Red NAT (*Network Address Translation*).

Teredo, a diferencia del mecanismo 6to4, no necesita una dirección IPv4 pública. Esto es una ventaja, ya que para todas las redes no se tiene la facultad de entregar direcciones IPv4 públicas a cada uno de sus nodos. Además de esto, NAT no es capaz de traducir el encapsulamiento 6to4 (sólo traduce TCP y UDP), por lo que un dato proveniente de un túnel 6to4 va hacia una red con dispositivos NAT, este no podría ingresar y alcanzar su destino.

Entonces, para este mecanismo, se encapsulan en caberas IPv4 y UDP los paquetes IPv6 (Figura 14).

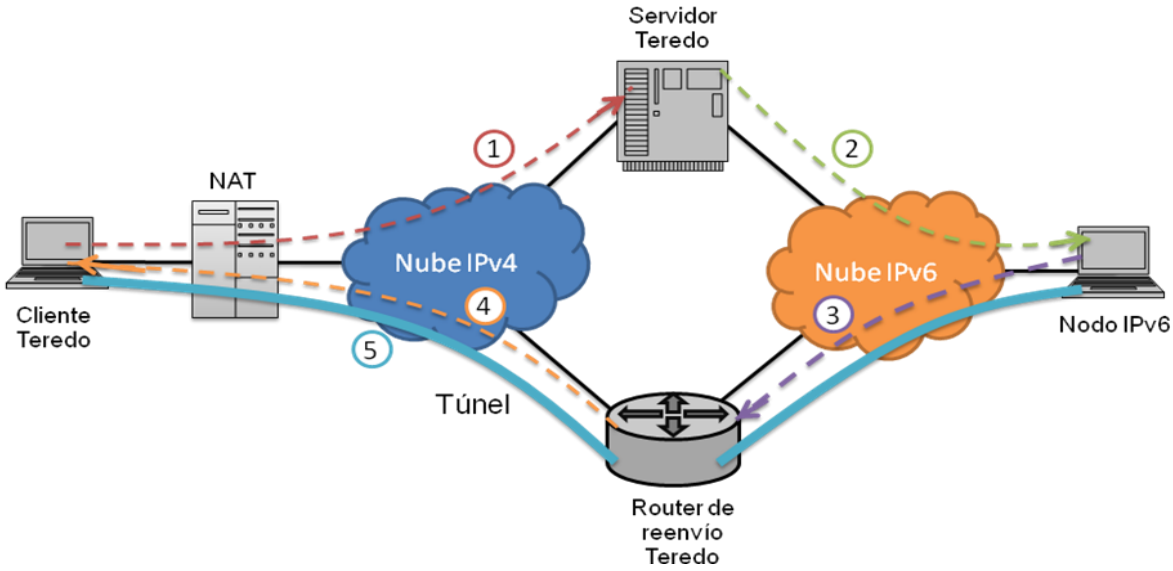
Figura 14. Encapsulamiento Teredo.

Teredo utiliza UDP como medio de transporte, por lo que los paquetes IPv6 son enviados como mensajes UDP. Utilizando una sola dirección IPv4 y mapeos UDP del dispositivo NAT es posible estableces túneles para los hosts con doble pila detrás de un mismo dispositivo NAT.

La dirección Teredo (IPv6) es generada a partir del identificador 2001::/16 y la dirección IPv4, con el mismo principio de concatenación explicado para 6to4.

Entonces, el principio de funcionamiento de Teredo es el siguiente (Figura 15):

Figura 15. Esquema Teredo.



Fuente: AMOSS, John y MINOLI, Daniel. Handbook of Ipv4 to Ipv6 Transition. Estados Unidos: Auerbach Publications, 2008.

En este esquema de ejemplo (Figura 15) se explica el principio de funcionamiento de Teredo:

- En (1), el cliente Teredo envía una petición de eco al nodo IPv6 a través del servidor Teredo. El servidor Teredo reenvía ésta petición al nodo IPv6 (2).
- En (3) el nodo IPv6 envía la respuesta de eco con la dirección destino correspondiente a la dirección del cliente Teredo. Este paquete se envía por medio de la dirección Teredo (2001::/16 + dirección IPv6). Esta respuesta llega al router de reenvío, quien tuneliza hacia el cliente Teredo (4).
- Establecido el túnel el cliente Teredo puede comenzar a enviar datos a través del router de reenvío y desde aquí hasta el nodo IPv6 (5).

5.6. VENTAJAS Y DESVENTAJAS DE LOS MECANISMOS DE TÚNEL

- Ofrece grandes ventajas a la hora de conectar nodos IPv4 e IPv6 en redes extensas.

- La mayoría de los mecanismos de túnel realizan sus procedimientos automáticamente. No necesitan configuración previa.

- La desventaja para este tipo de mecanismos es la carga que recae sobre el router, el cual debe encapsular y desencapsular los paquetes en ambos sentidos.

- Este tipo de mecanismos no requieren complejidad en la configuración de los routers.

- Una de las ventajas del mecanismo 6to4 es que es transparente a las aplicaciones. Además este mecanismo es simple y requiere de poco mantenimiento, además que la configuración en los routers es mínima.

- Con el mecanismo 6to4 permite que los nodos Ipv6 se comuniquen con nodos IPv4 enrutando sus datos entre nubes IPv4 y con los aislados nodos Ipv6 por medio de routers de reenvío.

- Una desventaja del mecanismo 6to4 es que no puede utilizarse en redes en las que se implementa NAT. Es difícil que para cada nodo se le asigne una IP pública.

- Con el mecanismo ISATAP se permite que el protocolo IPv6 cada vez tome más fuerza en las redes con poco esfuerzo. Durante la sesión, sólo es necesario un router ISATAP.

- Una ventaja y a la vez desventaja de mecanismo ISATAP es que no requiere autenticación, es decir, que cualquier nodo que conozca la dirección del router ISATAP puede acceder a sus servicios.

- Una desventaja del mecanismo ISATAP es que no soporta multicast.

- Una ventaja del mecanismo Teredo es la disponibilidad de ser implementado en redes en las que NAT está presente y establecer túneles para varios nodos.

- Con el mecanismo Teredo pueden ocurrir cuellos de botella cuando hay gran volumen de tráfico, además de tener problemas por ser un mecanismo complejo, con lo que el desempeño de la red también se ve disminuido.

- Debido a la operación del mecanismo Teredo en redes con NAT, la vulnerabilidad en la seguridad es grande.

- Una ventaja del mecanismo Tunnel Broker es que proporciona el servicio de tunelización en línea. Un nodo puede obtener su dirección IPv6 con sólo contar con su cuenta en una de las empresas que prestan este servicio, que en la mayoría es gratis. De esta forma, un nodo siempre contará con su dirección IPv6 sea cual sea su dirección IPv4.

- Con el mecanismo Tunnel Broker las tareas de administración desaparecen, ya que éstas las provee su ISP virtual.

- La desventaja del mecanismo Tunnel Broker es que no es operativo si el nodo está detrás de NAT.

- Un aspecto importante en el mecanismo Tunnel Broker es la seguridad al compartir información con el ISP virtual y la confiabilidad que estas empresas ofrecen.

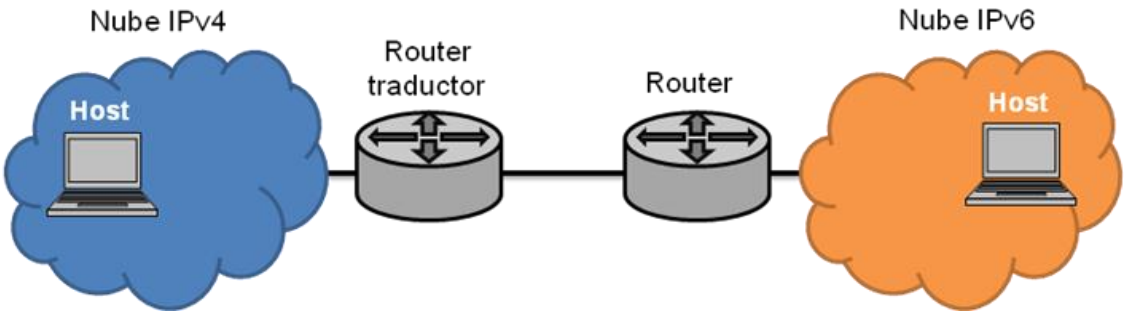
6. MECANISMO DE TRADUCTOR DE PROTOCOLO

Este mecanismo está definido en RFC 4213.

Por medio del mecanismo de traducción se puede lograr la conversión entre protocolos, así como en sus cabeceras, direcciones, etc. Para implementar éstos tipos de mecanismos se deben incluir elementos de traducción a ambos lados de los nodos a comunicar.

Se pueden emplear en los casos en que la comunicación se vaya a realizar entre un nodo IPv6 y un nodo IPv4 o en casos en que un nodo o router sólo tenga habilitado un sólo protocolo IP (Figura 16). De este modo, se traducen los paquetes IPv6 a IPv4.

Figura 16. Mecanismo traductor de protocolo.



Los mecanismos de traducción definidos son:

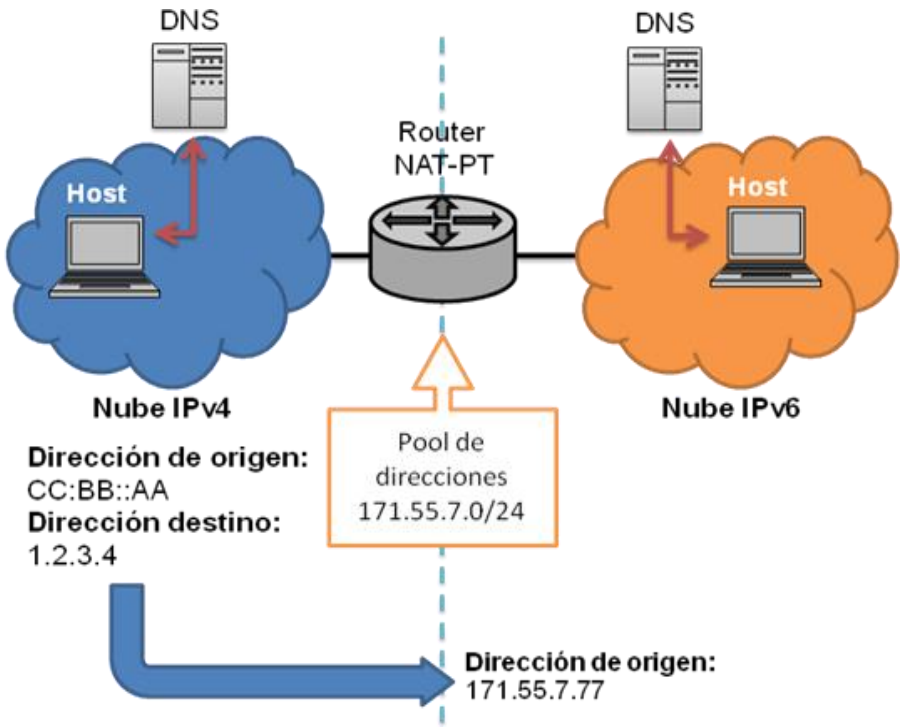
- **NAT - PT.**
- **SIIT.**
- **TRT.**

6.1. MECANISMO DE NAT – PT (Traductor de Dirección de Red –Traductor de Protocolo)

Este mecanismo está definido en RFC 2766.

El Traductor de Dirección de Red – Traductor de Protocolo NAT-PT (*Network Address Translation - Protocol Translation*) funciona de manera similar al traductor de direcciones NAT. Emplea un dispositivo que funciona en la frontera de los dos nodos, IPv4 e Iv6 y que cuenta con un traductor de cabecera IPv4/IPv6. De ésta manera, traduce protocolos y direcciones desde IPv6 hacia IPv4 utilizado un pool de direcciones (Figura 17).

Figura 17. Mecanismo NAT-PT.



En la figura 17 se explica el funcionamiento básico del mecanismo NAT-PT. La sesión es iniciada por el host en la nube IPv6 y es asignada la dirección IPv4 con el primer paquete IPv6 que es enviado. Cuando se inicia la sesión, el router NAT-TP le asigna una dirección al host IPv6 de su pool de direcciones para que sus paquetes puedan ser enrutados en la nube IPv4.

El router NAT-PT se encarga de traducir las búsquedas DNS y de asignar las direcciones IPv4 mediante La Puerta de Enlace de Capa de Aplicación DNS-ALG (*Application Layer Gateway*), la cual traduce los registros A en registros AAAA y permite la comunicación entre los hosts para aplicaciones específicas.

6.2. MECANISMO SIIT (Algoritmo de Traducción IP/ICMP Sin Estado)

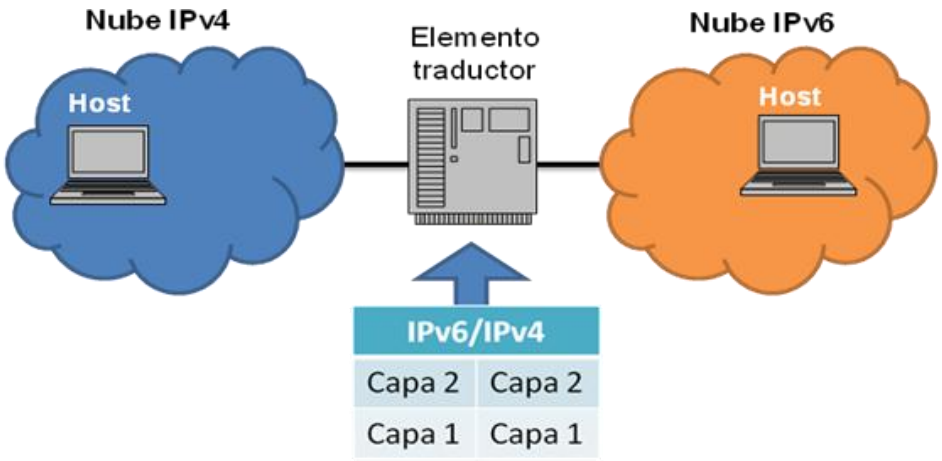
Este mecanismo está definido en RFC 2765.

SIIT es un mecanismo que permite la comunicación entre nodos IPv4 e IPv6.

El mecanismo SIIT utiliza un algoritmo de mapeo sin estado o traducción bidireccional entre cabeceras de paquetes IPv4 e IPv6, así como entre mensajes ICMPv4 e ICMPv6, que permite la traducción de las cabeceras de los paquetes IPv6 a Ipv4.

Con este mecanismo se busca la preservación de las direcciones IPv4, estableciendo la comunicación entre los dos nodos de manera temporal alquilando por el tiempo en el que dura la sesión, una dirección IPv4 al nodo IPv6 (Figura 18).

Figura 18. Mecanismo SIIT.

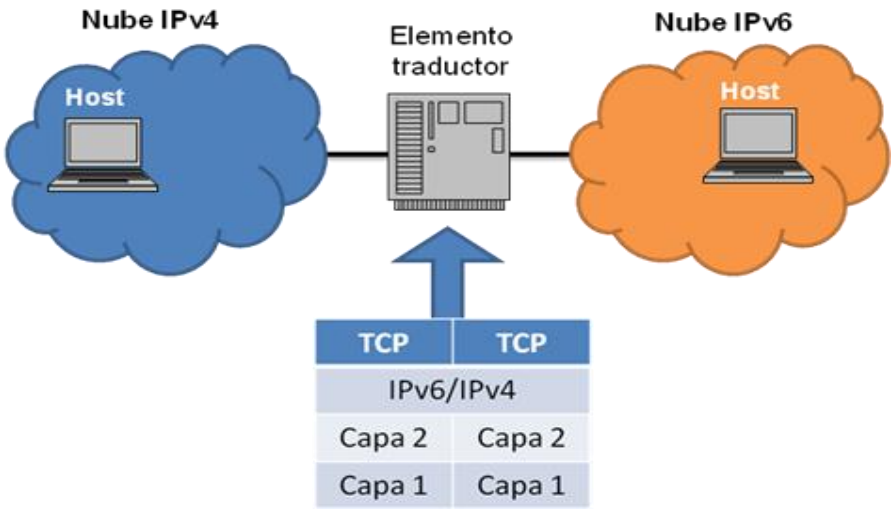


6.3. MECANISMO TRT (Traducción de Retransmisión de Transporte)

Este mecanismo está definido en RFC 3142.

TRT retransmite las conexiones a nivel de capa de transporte (TCP/UDP) entre el origen y el destino entre IPv4 e IPv6 a diferencia de SIIT, que lo realiza en la capa de red (IP/ICMP) (Figura 19). Así como en NAT-PT, mantiene las sesiones y no soporta las direcciones concatenadas.

Figura 19. Mecanismo TRT.



TRT debe configurar dos conexiones TCP/UDP, desde el host IPv6 y desde el host IPv4 para iniciar la sesión. Una vez se establece la sesión, el procesamiento es necesario a medida de que fluyen las retransmisiones entre los dos puntos.

6.4. VENTAJAS Y DESVENTAJAS DE LOS MECANISMOS TRADUCTORES DE PROTOCOLO

- Con los mecanismos de traducción se busca que sólo cuando un nodo IPv4 se vaya a comunicar con un nodo IPv6, se realice traducción de la cabecera y de la dirección. Los mecanismos de traducción proporcionan alto nivel de interoperabilidad en las redes.

- Estos mecanismos pueden llegar a representar en las redes la aparición de cuellos de botellas mientras los paquetes son traducidos, por lo que se experimentan limitaciones en cuanto al rendimiento del proceso.

- Una desventaja grande para los mecanismos de traducción es que tienen un único punto de falla y tienen problema de escalabilidad.

- Una ventaja del mecanismo NAT-PT es que toda la configuración se realiza solamente en el router NAT-PT, lo que significa que la red no se ve afectada ante ésta implementación.

- El mecanismo NAT-PT permite la comunicación transparente entre los nodos IPv4 e IPv6, traduciendo protocolos y direcciones.

- El mecanismo NAT-PT tiene como desventaja que al alquilar todas las direcciones de su pool, no es posible que otros nodos establezcan sesiones, lo cual significa limitación en su servicio.

- Un aspecto a tener en cuenta es que no se recomienda la comunicación entre nodos IPv4 o Ipv6 con nodos IPv4/IPv6 cuando se está implementando el mecanismo NAT-PT.

- El mecanismo SIIT es relativamente sencillo de implementar, pero a medida que crece la red, su administración se vuelve más compleja. Por esto se recomienda su utilización en redes pequeñas.

- El mecanismo SIIT tiene la ventaja de utilizar un traductor sin estado, el cual evita que se cree un único punto de falla en este mecanismo.

- El mecanismo TRT tiene la desventaja que la traducción de los paquetes es más compleja cuando la sesión la inicia el nodo IPv4.

- Para el mecanismo TRT no se necesitan modificaciones ni en los nodos que inician sesión, ni en los nodos destino.

- El mecanismo TRT no tiene problemas en la conversión de las cabeceras IPv4 o IPv6.

- Un problema del mecanismo TRT es que sólo soporta tráfico bidireccional.

- Una desventaja del mecanismo TRT es que tiene un único punto de falla, tal y como sucede con las redes que implementan NAT.

7. CONCLUSIONES

- La transición de IPv4 hacia IPv6 es la solución más viable y menos traumática en este momento, puesto que una migración entre los dos protocolos sin un proceso intermedio traería problemas de operatividad, descoordinación, económicos e incluso legales en las redes globales. Aunque el proceso de transición represente un proceso complejo y costoso, es un proceso que ha demostrado ser muy útil y que ha demostrado las virtudes del protocolo IPv6, el cual ha tomado poco a poco el control.

- Los mecanismos de doble pila y de túneles son los más recomendados y utilizados en las redes actuales, a diferencia de los mecanismos de traducción, debido a la escabilidad, interoperabilidad y a las características que pueden ofrecer a las redes. De estos, los mecanismos 6to4 y Teredo son los más implementados, gracias a la facilidad con la que se pueden crear túneles automáticos en redes con direcciones IPv4 fijas (6to4) y en redes con NAT (Teredo).

- Con esta monografía se busca dar a conocer los mecanismos que actualmente se están utilizando en el proceso de transición e interoperabilidad de IPv4 a IPv6 y llegar a relacionarse con las características que cada uno de estos brindan, de las ventajas que cada uno puede ofrecer y de generar una mente crítica a la hora de analizarlos, entenderlos y de tomar la decisión de cuál mecanismo podría ser el más acertado para implementar en un tipo de red específico si llegara a suceder.

BIBLIOGRAFÍA

1) AMOSS, John y MINOLI, Daniel. Handbook of Ipv4 to Ipv6 Transition. Estados Unidos: Auerbach Publications, 2008.

2) CARPENTER, B. y Moore, K. RFC 3056, Connections of IPv6 Domains Via Clouds. [Sitio en Internet] The Internet Engineering Task Force. Enero, 2001. Disponible en http://tools.ietf.org/html/rfc3056.

3) COOPER, Micah y YEN, David. IPv6: business applications and implementation concerns. En: Computer Standards & Interfaces. Julio, 2005, vol. 28, publicación 1.

4) DURAND, A., *et al*. RFC 3053, IPv6 Tunnel Broker. [Sitio en Internet] The Internet Engineering Task Force. Enero, 2001. Disponible en http://tools.ietf.org/html/rfc3053.

5) DURDAGI, Emre y BULDU, Ali. IPV4/IPV6 security and threat comparisons. En: Procedia - Social and Behavioral Science. 2010, vol. 2, publicación 2.

6) GORALSKI, Walter. IPv4 and IPv6 Headers. En: The Illustrated Network. 2009. Elsevier Inc.

7) HAGINO, J. y YAMAMOTO, K. RFC 3142, An IPv6-to-IPv4 Transport Relay Translator. [Sitio en Internet] The Internet Engineering Task Force. Junio, 2001. Disponible en http://tools.ietf.org/html/rfc3142.

8) HUITEMA, C. RFC 4380, Teredo: Tunneling IPv6 over UDP Network Address Translation (NATs). [Sitio en Internet] The Internet Engineering Task Force. Febrero, 2006. Disponible en http://tools.ietf.org/html/rfc4380.

9) IPv4 Exhaustion. [Sitio en Internet] RIPE Network Coordination Centre. Disponible en http://www.ripe.net/internet-coordination/ipv4-exhaustion.

10) IPv6 Act now. [Sitio en Internet] Disponible en http://www.ipv6actnow.org/info/statistics.

11) MACKAY, Michaels y CHRISTOPER, Edwards. A comparative Performance Study of IPv6 Transitioning Mechanisms – NAT-PT vs. TRT vs. DSTM. En: Networking 2006. Networking Technologies, Services, and Protocols. Mayo, 2006, vol. 3796.

12) MORENO, Axel. Ipv6 Interoperabilidad y Robustez. Tesis de maestría. México DF: Instituto Politécnico Nacional, 2004.

13) NORDMARK, E y GILLIGAN, R. RFC 4213, Basic Transition Mechanisms for IPv6 Hosts and Routers. [Sitio en Internet] The Internet Engineering Task Force. Octubre, 2005. Disponible en http://tools.ietf.org/html/rfc4213.

14) NORDMARK, E. RFC 2765, Stateless IP/ICMP Translation Algorithm (SIIT). [Sitio en Internet] The Internet Engineering Task Force. Febrero, 2000. Disponible en http://tools.ietf.org/html/rfc2765.

15) NÚÑEZ, Alejandro. Evolución del Protocolo de Internet hacia IPv6. En: Revista Técnica de la Empresa de Telecomunicaciones de Cuba. 2006. Publicación 2.

16) PUNITHAVATHANI, Shalini y SANKARANARAYANAN, K. IPv4/IPv6 Transition Mechanisms. En: European Journal of Scientific Research. Julio, 2009, vol. 34, publicación 1.

17) TEMPLIN, F.; GLEESON, T. y THALER, D. RFC 5214, Intra-Site Automatic Addressing Protocol (ISATAP). [Sitio en Internet] The Internet Engineering Task Force. Marzo, 2008. Disponible en http://tools.ietf.org/html/rfc5214.

18) TSIRTSIS, G. y SRISURECH, P. RCF 2766, Network Address Translation – Protocol Translation (NAT-PT). [Sitio en Internet] The Internet Engineering Task Force. Febrero, 2000. Disponible en http://tools.ietf.org/html/rfc2766.

19)TSIRTSIS, G., *et al*. RFC 2694, DNS Extensions to Network Address Translations (DNS-ALG). [Sitio en Internet] The Internet Engineering Task Force. Septiembre, 1999. Disponible en http://tools.ietf.org/html/rfc2694.

20)VAZÃO, Teresa; RAPOSO, Luís y SANTOS, João. Migration to the New Internet – Supporting Inter Operability Between IPv4 and IPv6 Networks. En: Telecommunications and Networking – ICT. Julio, 2004, vol. 3124.

21)XIANHUI, Che y LEWIS, Dylan. Ipv6: Current Deployment and Migration Status. En: International Journal of Research & Reviews in Computer Science. Junio, 2010, vol. 1, publicación 2.