UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

“TECNOLOGÍAS Y MECANISMOS DE TRANSICIÓN DE IPV4 A IPV6”

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A:

JUAN CARLOS PÉREZ NAVA

ESTEBAN RODOLFO HERRERA GUTIÉRREZ

ASESORA: M.C. CINTIA QUEZADA REYES

AGRADECIMIENTOS

Agradezco a cada profesor que compartió un tiempo invaluable en todo el proceso de enseñanza que con toda su experiencia y conocimientos me ayudaron a fortalecerme como profesionista y humanizarme como persona. A mis compañeros que con nuestros esfuerzos logramos superar cada obstáculo. A mi familia que fueron mi guía gracias a sus consejos y a un apoyo que nunca me hizo falta en toda mi trayectoria como estudiante y por supuesto a la Universidad Nacional Autónoma de México que sin ella no hubiera podido cumplir la primera de muchas metas a lograr y en especial a la facultad de ingeniería que día con día se esmera en la formación de cada una de las personas que la integran engrandeciendo a este país.

PÉREZ NAVA JUAN CARLOS

Este trabajo es el fin de una etapa de aprendizaje en mi vida, indudablemente no se hubiera podido lograr sin mi familia y mis amigos. Quiero agradecer todo el esfuerzo de mi mamá Lourdes por apoyarme incondicionalmente durante tanto tiempo en todos mis estudios, su inmenso cariño y comprensión que me ha ayudado a ser una mejor persona, a mi hermano Alberto que siempre me ha guiado dándome consejos que han mejorado mi vida y que han abierto mi visión sobre el mundo y que siempre se ha preocupado por mí y a mi hermana Ana que siempre me ha cuidado y me ha comprendido cuando he tenido momentos difíciles.

Agradezco a la Universidad Nacional Autónoma de México todos los momentos, enseñanzas, triunfos, derrotas, experiencias, los amigos, los profesores, los lugares para ir a comer, los eventos, los institutos, las bibliotecas, todas las facultades, pero ante todo y sobre todo los valores que representa el ser un universitario y el compromiso hacia mi país.

Le doy gracias a mi escuela la Facultad de Ingeniería por permitirme entender y vivir lo que significa ser ingeniero, enseñarme “aprender a aprender” y por fomentar mi curiosidad para saber cómo funcionan las cosas. También quiero agradecer a mis sinodales por todo el apoyo que me han otorgado y en especial a mi asesora de tesis M.C. Cintia Quezada Reyes que siempre nos apoyó y guió para realizar este trabajo, a su paciencia e interés que demostró durante todo el proceso y sus aportes.

Gracias a todos mis amigos, compañeros y profesores que fueron muchos, por compartir todas mis experiencias en la carrera y todos esos momentos que nunca se olvidan.

ESTEBAN RODOLFO HERRERA GUTIÉRREZ

INDICE GENERAL

Introducción

INTRODUCCIÓN

La humanidad siempre ha tenido la fuerte necesidad de comunicarse no solo para entablar una conversación sino que forma parte del progreso y crecimiento de sociedades con base en cómo ha ido creciendo la extensión de su influencia, ha ideado varias maneras para poder transmitir información donde las capacidades físicas del hombre no son posibles.

Las comunicaciones han ayudado al progreso de las civilizaciones además de acelerar considerablemente el ritmo de crecimiento cultural y tecnológico; originando un sincretismo muy particular en cada una de las regiones del planeta.

Desde el nacimiento de la telefonía ha hecho que el mundo se perciba más pequeño pudiendo hablar con una persona que se encuentre al otro lado del Atlántico de manera tan natural como cuándo se platica con una persona que se encuentre a sólo unos metros de nosotros.

Sin embargo, la posibilidad de establecer una conversación no solo permaneció en el hecho de poder intercambiar palabras mediante la voz, ahora el paradigma de las comunicaciones ha cambiado donde no sólo el audio y texto son las maneras de transmitir información, hoy en día se usa la combinación de imágenes, texto, audio y video; aunque el verdadero impacto de las telecomunicaciones se encuentra en que es posible difundir información que puede ser vista a escala global de manera instantánea.

Esto ha hecho que el mundo se encuentre comunicado prácticamente las 24 horas del día y además de que a cada momento se genera una gran cantidad de información día con día creándose una nueva necesidad de mantenerse enterado.

Las redes han ido más allá que la interacción entre dos o más computadoras, han revolucionado las comunicaciones donde la difusión de la información no es lo único que se puede realizar sino además se han aprovechado de esta tecnología para proveer servicios tales como bancarios, educativos, de telefonía, entretenimiento, un sin fin de posibilidades que existen en el aprovechamiento de esta tecnología y se ha venido adaptando a las nuevas necesidades.

Sin embargo, cada tecnología cuenta con sus limitantes pero por más de 20 años las redes han trabajado mejor de lo que se esperaba aunque jamás se visualizó el crecimiento que tendría, por lo que cada día le cuesta mantener a mas usuarios, el usuario no notará un cambio radical aunque es un cambio importante ya que se refleja la adopción que ha tenido en la sociedad.

Ahora le corresponde la evolución tecnológica al protocolo base del funcionamiento de Internet, el protocolo IP que hoy en día necesita de una actualización para poder soportar no sólo el crecimiento de usuarios, sino el mayor uso de los servicios de red.

IPv4 comienza a verse obsoleto ante las modernas aplicaciones que consumen más y más recursos de procesamiento, información, energía y entretenimiento, pero este cambio debe ser lento y paulatino, debido a que una de las características más importantes del nacimiento de Internet es su capacidad de enviar información a cualquiera sin importar si un nodo deja de funcionar y su fácil adaptabilidad hace que este cambio sea de lo más tardado y complejo.

No sólo los factores tecnológicos intervienen, el cambio en una tecnología tan arraigada a las vidas actuales necesita dinero, dinero que no será gastado hasta que se pueda ver como una inversión, también requiere de acciones de diferentes instituciones gubernamentales y educativas.

Si se tratara de hacer un edificio más alto sería más fácil tirarlo y volverlo a levantar o se intentaría hacer su base más grande para poder incrementar más pisos, pero seguramente no podría elevarse mucho, IPv4 es parecido en el sentido de que no es posible tirar y levantar otro protocolo de inmediato, se debe modificar e ir adaptando a la red poco a poco casi sin percepción al usuario común, por que en la actualidad existen servicios que no pueden ser suspendidos en ningún momento.

Un factor importante son los proveedores de aplicaciones y de hardware que soporten IPv6, pero si no existe una demanda elevada, estos proveedores perderían dinero y no sería un negocio rentable, además que la cantidad de usuarios sería mínima.

También se debe pensar en que la red se encuentra en todo el mundo y por lo tanto existen diferentes gobiernos que tienen diferentes puntos de vista sobre cómo se debería hacer esta transición o peor aún no tienen un punto de vista, y aquí se entra a un factor de desarrollo económico de los países donde la prioridad de los países con pocos recursos se encuentra en actividades básicas como educación, salud y alimentación, aquí lamentablemente no existe una visión de la importancia de tener el control de la información que fluye por sus regiones.

Pero ante este panorama difícil por recorrer en cuanto a esta actualización o cambio de protocolo de IPv4 a IPv6 existe un camino que puede permitir que esta evolución se dé, la solución se encuentra en realizar el cambio paulatinamente y en donde las redes con IPv4 convivan con las redes IPv6 en un mismo conjunto, con el paso del tiempo los protocolos pueden trabajar de una manera conjunta, de esta manera se permitirá que las aplicaciones y los administradores de cualquier tipo de red se acostumbren al cambio y aprendan a utilizar la nuevas aplicaciones que vayan surgiendo.

Con el tiempo, las redes IPv4 llegarán a ser un subconjunto real de una red soportada en IPv6 y después paulatinamente el uso de Ipv4 será desechado y visto como obsoleto a nivel funcional, pero ¿cómo va a pasar esto? Bueno existen mecanismos de transición que permiten utilizar el protocolo IPv6 dentro de redes Ipv4, como existen diferentes casos en

los que una red debe ser utilizada también existen diferentes posibilidades de utilizar estos mecanismos, la intención es utilizarlos más y cada vez más haciendo convivir estos dos protocolos para después dejar de utilizar IPv4.

Con este documento, un administrador de red tendrá una referencia del cómo está constituido el protocolo IPv4 e IPv6, por qué es necesario el cambio y podrá encontrar la manera de adaptar el protocolo Ipv6 a su red, puede que simplemente con la intención de conocer el protocolo, usarlo dentro de su red o incluso probar sus aplicaciones funcionando en IPv6. Para los alumnos que apenas están conociendo cómo funciona Internet y sus protocolos, este trabajo puede funcionar de base para explicarles cómo funcionan y para qué fueron creados y qué mecanismos de transición de IPv4 a IPv6 existen.

Capítulo 1

Surgimiento y Características de IPv4

Desde hace 30 años a la fecha el mundo de las comunicaciones ha evolucionado de manera asombrosa, muchas nuevas aplicaciones y tecnologías se han implementado, pero la que más ha trascendido es Internet. Para poder entender qué es el protocolo IPv4, es necesario hacer una revisión del surgimiento de Internet, captar la necesidad de su creación y entender su evolución.

1.1 Surgimiento de Internet

Dentro de las diferentes épocas de la historia de la humanidad, el hombre se ha visto envuelto en diversas guerras que han permitido el avance acelerado de la tecnología. En este caso interesa la Guerra Fría porque en ese tiempo se crearon las bases de Internet, se le llamó así por el periodo de tensión que existió entre los bloques occidental capitalista y el oriental comunista después de la Segunda Guerra Mundial hasta la caída de la Unión Soviética.

Las dos superpotencias pertenecientes a cada bloque comunista y capitalista se encontraban luchando en una carrera tecnológica de desarrollo nuclear y de interés estratégico por dominar el espacio. Dentro de todas estas investigaciones de carácter militar, la información era vital, de tal forma que se necesitaba un medio que pudiera sobrevivir a cualquier conflicto y pudiera seguir trabajando con la información.

La solución era una red que estuviera compuesta por diferentes dispositivos que tuvieran la misma importancia, al ser destruido uno de estos dispositivos no se afectaría el funcionamiento de la red, cada uno de estos dispositivos se les nombraría nodos y tendrían la capacidad de enviar datos por la ruta que ellos deseasen, estos datos se dividirían en paquetes que podían seguir diferentes rutas pero siempre debían llegar al mismo destino.

Durante los años 60´s la idea de crear una red se encontraba en proceso dentro de varias instituciones de Estados Unidos, tales como el MIT (Massachussetts Institute of Technology - Instituto de Tecnología de Massachussetts) y la corporación RAND (Research ANd Development - Investigación y Desarrollo) creada para apoyar la investigación en las fuerzas armadas. “Leonard Kleinrock del MIT publicó en julio de 1961 el primer trabajo sobre conmutación de paquetes (la tecnología que permitía dividir los datos y que recorrieran rutas distintas)” [A]. El Pentágono por medio de su ARPA (Advanced Research Projects Agency – Agencia de Investigación de Proyectos Avanzados) financió el proyecto para una prueba y para el año de 1969 se abrió el primer nodo de la red ARPANET en la Universidad de California.

En 1972 se realizó la primera demostración pública de ARPANET, que funcionaba de forma distribuida sobre una red telefónica conmutada[1]. Fue un éxito que sirvió para que en 1973, la ARPA iniciara un programa de investigación sobre posibles técnicas para interconectar redes (orientadas al tráfico de paquetes) de distintas clases. Es por eso que desarrollaron nuevos protocolos de comunicaciones que permitiesen el intercambio de información de forma "transparente" para los dispositivos conectados. De este proyecto surgió el nombre de "Internet", que se aplicó al sistema de redes interconectadas mediante los protocolos TCP (Transmission Control Protocol - Protocolo de Control de Transmisión) e IP (Internet Protocol - Protocolo de Internet).

ARPANET utilizaba en sus inicios el protocolo NCP (Network Control Program - Programa de Control de Red) pero en 1983 cambió por TCP/IP, éste es un punto fundamental que marca la importancia y el origen de IP además de su relación con TCP, ya que juntos son la base de Internet. En ese mismo año (1983) TCP/IP se integró a la versión 4.2 del sistema operativo UNIX de la Universidad Berkeley en California y la integración de versiones comerciales pronto llegó.

Para 1986 la NSF (The National Science Foundation - Fundación Nacional de Ciencia), una agencia federal independiente creada por el congreso de los Estado Unidos en 1950 con el fin de promover el avance de la ciencia, inició el desarrollo de su propia red, la NSFN (National Science Foundation's Network - Red de la Fundación Nacional de Ciencia) que junto a otras redes troncales de Europa se convirtió en la red principal de Internet.

La integración del protocolo OSI (Open System Interconnection - Interconexión entre Sistemas Abiertos) en 1989 permitió la interconexión de otras redes de arquitectura distinta a Internet y también facilitó el uso de distintos protocolos de comunicaciones. Al mismo tiempo en el CERN (Conseil Européen pour la Recherche Nucléaire - Consejo Europeo para la Investigación Nuclear de Ginebra), un grupo de físicos encabezado por Tim Berners-Lee, crearon el lenguaje HTML(HyperText Markup Language - Lenguaje de Marcas de Hipertexto), basado en el SGML (Standard Generalized Markup Language - Lenguaje de Marcado Generalizado). En 1990 el mismo equipo construyó el primer cliente web, llamado WWW (World Wide Web - Red Global Mundial) y el primer servidor web.

Internet ha crecido enormemente no sólo en tamaño sino en aplicaciones, protocolos y servicios, es importante entender que la base es TCP/IP, en un principio sólo se buscó transmitir datos de forma segura con fines militares, le siguieron las aplicaciones educativas y científicas, después cuando Internet se volvió comercial su crecimiento se igualó al cambio cultural de la gente y su comportamiento.

[1] Es la conexión tradicional analógica por la que circulan las vibraciones de voz, es decir, la que se usa habitualmente para hablar por teléfono. Éstas se traducen en impulsos eléctricos y se transmiten a través de los hilos de cobre de la red telefónica normal.

La red invadió todo terreno social y no sólo unió las formas de comunicación existentes, también está afectando la evolución del hombre al permitirle tener acceso a mucha información de manera simple, los niños de hoy aprenden más rápido y son más despiertos, conviven todo el tiempo con nuevos dispositivos que son compatibles con la red y las distancias geográficas parecen ser cada vez más cortas.

En la actualidad se emplea la versión 4 de IP y es probable que pronto se cambiará a una nueva versión: IPv6. "El 3 de enero de 2006 Internet alcanzó los mil millones de usuarios. Se prevé que en diez años, la cantidad de navegantes de la red aumentará a 2000 millones." [B]

1.2 Importancia de TCP/IP y modelo OSI

En sus primeros momentos de vida, ARPANET estuvo constituida por redes telefónicas comunes, conectaba muchos institutos y universidades. La transferencia de datos no necesitaba de ninguna modificación, pero la red evolucionó y distintos medios de comunicación se le fueron agregando como redes de satélite y radio, es por eso que fue necesario crear un nuevo protocolo que pudiera mantener la comunicación estable, así nació TCP/IP.

También se necesitaba una arquitectura flexible que permitiera la incorporación de nuevas aplicaciones, se había considerado la posibilidad de enviar archivos y sesiones en tiempo real.

La base del funcionamiento de Internet es TCP/IP, es un modelo que explica cómo se transmite la información de un dispositivo a otro, etapa por etapa desglosa el proceso que sufren los datos para poder ser llevados a su destino y lo representa en forma de una pila, en cada nivel de esta pila es en donde se encuentran los diferentes protocolos de Internet.

La pila TCP/IP está compuesta por 5 niveles, éstos se describen a continuación:

1.- Nivel físico: En este nivel se describe el medio por el cual la información es transportada , es decir, las características físicas de la comunicación, existen medios de transmisión terrestres y aéreos, entre los terrestres se encuentran el cable coaxial, el par trenzado, la fibra óptica y algunos aéreos son las microondas, el infrarrojo y los enlaces satelitales.

2.- Nivel de enlace: En esta capa se describe cómo son transportados los paquetes en el nivel físico, la tarea principal es tomar el medio de transmisión en bruto y transformarlo en una línea libre de errores de transmisión, esto sucede al hacer que el emisor divida los datos de entrada en marcos de datos, que transmita los marcos de manera secuencial y procese los marcos de acuse de recibo que devuelve el receptor. La capa física sólo acepta y transmite una línea de bits sin saber qué representan o qué estructura tienen, entonces la capa de

enlace crea y reconoce los límites de los marcos. Esto se logra al añadir ciertos patrones de bits al principio y al final del marco, éstos son delimitadores.

Si le llegase a suceder algún daño a alguno de estos marcos, como una pérdida o que se dupliquen por error, además de que exista un tráfico muy veloz que pueda saturar a un receptor lento o se dé el caso de que el canal sea usado de manera bidireccional, todas estas implicaciones son atendidas por la capa de enlace.

3.- Nivel de Internet: Esta parte de la pila es la pieza fundamental que mantiene unido todo el modelo, el objetivo es permitir que todos los nodos puedan enviar y recibir paquetes en cualquier red y puedan viajar de forma independiente a su destino, además estos paquetes pueden llegar en forma desordenada y corresponde a las capas superiores agruparlos correctamente. Dentro de esta capa se define el formato de los paquetes y también se encuentra el protocolo IP. Las funciones más importantes de este nivel es el ruteo de los paquetes que se encarga de encontrar el mejor camino para el envío y evitar el tráfico.

4.- Nivel de transporte: Para el nivel de transporte se definieron dos protocolos, TCP, este protocolo fragmenta la corriente que entra de bytes en mensajes discretos y pasa cada uno a la capa de red, en el destino, el proceso TCP que recibe reensambla los mensajes recibidos para formar la corriente de salida. TCP también se encarga de manejar el flujo para asegurar que un emisor rápido no pueda abrumar a un receptor lento con más mensajes de los que pueda manejar. UDP (User Datagram Protocol - Protocolo de Datagrama de Usuario), es un protocolo sin conexión, se usa para consultas de petición y respuesta de una sola ocasión, del tipo cliente-servidor y en aplicaciones en donde la velocidad es muy importante como transmisiones de voz y video.

5.- Nivel de Aplicación: Ésta es la parte más alta de la pila y contiene los protocolos de alto nivel, entre los protocolos más viejos están el de terminal virtual TELNET (TELecommunication NETwork - Telecomunicaciones de Red), el de transferencia de archivos FTP (File Transfer Protocol - Protocolo de Transferencia de Archivos), el de correo electrónico SMTP (Simple Mail Transfer Protocol - Protocolo de Simple Transferencia de Correo) y el servicio de nombres de dominio DNS (Domain Name System - Sistema de Nombre de Dominios). En esta capa se utilizan los datos en el formato que cada aplicación requiera y es codificado de acuerdo con un protocolo estándar. [TANENBAUM 1997].

Para tener una mejor referencia del modelo TCP/IP y de la ubicación de los protocolos mencionados se muestra la tabla 1.1. Este modelo de definió por primera vez en los artículos académicos llamados “papers” (Cerf y Kahn, 1974), en (Leiner,et al,1985) se escribió una perspectiva posterior y la metodología del diseño en la que se basa el modelo TPC/IP está en “paper” (Clark, 1988) [TANENBAUM 1997].

Tabla 1.1 Protocolos y modelo TCP/IP mencionados. [TANENBAUM 1997]

Capas del modelo TCP/IP	PROTOCOLOS
Aplicación	TELNET, FTP , SMTP y DNS
Transporte	TCP,UDP
Internet	IP
Enlace	Sin mención
Física	Sin mención

El modelo logró cubrir las necesidades de ese tiempo y sentó la base de las comunicaciones actuales, pero realmente fue diseñado para adaptarse y evolucionar con las ideas que se planearon a futuro, así como también a las ideas que tal vez ni siquiera se pensaron en el momento de su desarrollo. Como en toda evolución tecnológica las ideas se copian cuando tienen éxito, empezaron a surgir nuevos protocolos y la red comenzó a conectar al mundo, entonces la necesidad de una estandarización internacional se veía posible.

Las empresas desarrollaron sus propios mecanismos y aplicaciones, el intercambio de información se volvió complicado y algunas veces incompatible. La gran expansión de internet se enfrentaba al problema de que no había una estandarización internacional que permitiera la compatibilidad de diversas redes. Para este problema se pensó en el modelo OSI propuesto por la Organización Internacional para la Estandarización (ISO) creado para poder establecer comunicaciones bajo un mismo estándar con diferentes redes que están abiertas a la comunicación.

El modelo OSI propone una pila con siete niveles a diferencia de los cinco de TCP/IP (tabla 1.2), aplicación, presentación, sesión, transporte, red, enlace de datos y físico, aunque estos modelos son muy parecidos, el modelo OSI pone énfasis sobre tres conceptos fundamentales, los servicios, las interfaces y los protocolos. En los servicios especifica claramente qué es lo que cada capa hace, la interfaz de una capa le dice a los procesos que están arriba de la pila la manera de acceder a ella y los protocolos que utilice la capa para trabajar no importan, lo importante es que realice el trabajo adecuadamente.

Los principales principios para desarrollar este modelo fueron [TANENBAUM 1997]:

1.- Siempre se debe crear una nueva capa si se necesita un nuevo nivel de abstracción, esto quiere decir que no se debe dar por sentado que algún proceso que se necesite pueda resolverse entre capas o que cada capa realice una parte.

2.- La función de cada capa debe estar bien especificada y no tiene que relacionarse con los procesos de otras capas.

3.- La función de cada capa debe estar pensada de acuerdo con los protocolos estandarizados internacionalmente.

4.- Los límites de las capas deben ser bien limitados para favorecer el flujo de información entre cada capa.

5.- Las diversas capas deben realizar una sola función y su cantidad debe ser la adecuada para que no se convierta en una arquitectura muy complicada más bien que sea flexible.

Tabla 1.2 Comparación de pilas TCP/IP y OSI

TCP/IP	OSI
Aplicación	Aplicación
	Presentación
	Sesión
Transporte	Transporte
Internet	Red
Enlace	Enlace
Física	Física

Del nivel físico al nivel de transporte los dos modelos no tiene diferencias significativas pero en la parte alta de la pila donde se encuentra el nivel de aplicación de TCP/IP, el modelo OSI presenta un desglose de funciones más claro.

- Nivel de sesión: Permite a usuarios de diferentes dispositivos establecer sesiones entre ellos, las sesiones habilitan el transporte ordinario de datos, de la forma que lo hace el nivel de transporte pero ofrece servicios mejorados útiles para algunas aplicaciones. Otra función es manejar el control de diálogo, dentro de las sesiones puede existir flujo de datos en una sola dirección o ambas. Un servicio dentro del nivel es el manejo de fichas, que es una marca que se otorga a un solo lado de la comunicación para que tenga derecho a efectuar operaciones; para algunos protocolos es importante que ambos lados de la comunicación no realicen la misma operación al mismo momento. Para poder controlar esas operaciones el nivel de sesión proporciona la ficha que se puede intercambiar, el lado de la comunicación que tenga la ficha es el que puede hacer la operación. También proporciona el servicio de sincronización que coloca puntos de verificación en la línea de transmisión y si la comunicación se pierde, al momento de restablecer contacto sólo se deben repetir los datos que se transfirieron desde el último punto de verificación.

- Nivel de Presentación: Esta capa se encarga de la sintaxis y la semántica de la información que se transmite. Las diferentes computadoras tiene códigos distintos para presentar cadenas de caracteres, con el fin de hacer posible la comunicación

entre computadoras con representaciones diferentes, las estructuras de datos por intercambiar se pueden definir en forma abstracta. La capa de presentación maneja estas estructuras de datos abstractas haciendo la traducción para que la representación que el otro lado de la comunicación la entienda y viceversa.

- Nivel de aplicación: Ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico, administrador de bases de datos y servidor de archivos. Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos aumenta sin parar.

El modelo OSI fue diseñado antes de que se inventaran los protocolos, no fue diseñado específicamente para trabajar con cierto tipo de protocolos y esto lo volvió muy general. Al contrario de TCP/IP que fue diseñado para acoplarse a ciertos protocolos y por eso fue de fácil adaptación, pero también esa misma característica lo tornó rígido al no poder trabajar con otras arquitecturas. En ambas arquitecturas el protocolo IP es muy importante puesto que sin él la información nunca llegaría a su destino y si eso ocurriera el principio para el que fue creado Internet (transmitir información de forma segura) no tendría sentido.

1.3 Protocolo IP

El protocolo Internet está diseñado para la comunicación de computadoras mediante el intercambio de paquetes, para esta comunicación el protocolo implementa las funciones de direccionamiento y fragmentación, por lo que debe proporcionar el soporte necesario para que pueda viajar el paquete así como la fragmentación y el reensamble del paquete.

Las funciones básicas que implementa el protocolo IP son los siguientes:

a) Direccionamiento

El direccionamiento básicamente se encarga de proporcionar una dirección única para identificar a un dispositivo dentro de una red, estas direcciones son conocidas como dirección IP.

Existen dos tipos de direccionamiento en Internet y éstos dependen de la longitud del subnet mask - identificador de red[2]:

- Direccionamiento con clase:

  Los identificadores de red tienen una longitud fija y existen cinco clases de red que se clasifican dependiendo del tamaño de la red, las

[2] Subnet mask o máscara de subred, es una serie de 32 bits representado con 4 octetos en binario, su función es identificar en una dirección IP la parte correspondiente al número de red y la parte del host.

más usadas con las clases tipo A, tipo B y tipo C, la clase D es usada para grupos multicast y la clase E son direcciones experimentales que no están disponibles para uso general y se reservan para uso futuro.

- Direccionamiento sin clase:

  Los identificadores de red pueden tener una longitud distinta teniendo 30 identificadores distintos.

b) Enrutamiento

A su vez el protocolo de Internet provee al paquete una serie de lineamientos e identificadores que permitan transmitir correctamente el paquete de un punto de la red a otro en función de su destino, por lo que hay que identificar cada destino de manera única.

La mayor parte de los protocolos de enrutamiento se basan en un formato de direccionamiento que utiliza una red y un número de nodo, con esto se puede identificar cada camino que el paquete puede tomar y existe una inmensidad de éstos, por lo que es necesario buscar el mejor.

Para poder elegir el mejor camino existen los algoritmos de enrutamiento, además de que buscan el camino más óptimo, éstos deben mantener condiciones de equilibrio de todos los componentes de la red para el óptimo desempeño de la misma.

Existen dos clasificaciones principales de los algoritmos de enrutamiento:

1.- Adaptativos o dinámicos

Este tipo de algoritmos se acopla a los cambios que puedan variar su estado final en el momento de su ejecución, por lo que examina las condiciones de tráfico para determinar la ruta más óptima entre todas las posibles, varía en función de los cambios que pueden presentarse en la red.

2.- No adaptativos o estáticos

Estos algoritmos no basan sus decisiones en mediciones, estimaciones del tráfico o las topologías, para elegir la mejor ruta, el algoritmo se basa en tablas fijas cargadas en los componentes intermedios, es decir, la ruta que usa se conoce por adelantado.

c) Fragmentación

Cuando un paquete supera el tamaño máximo que puede transmitirse a través de la red ésta no puede descartarlo, a su vez, el protocolo se encarga de dividirlo en varias partes (conocido comúnmente como fragmentar el paquete) hacia la dirección origen, en la dirección destino el protocolo debe ser capaz de reensamblar cada fragmento que se recibe de manera adecuada para obtener el paquete que originalmente fue enviado, el protocolo envía el número de fragmento para que pueda realizar la tarea correctamente.

1.3.1 Características de IPv4

En IPv4 la dirección está conformada por 32 bits, teniendo una limitante de 4,294,967,296 (esto es, 2^{32}) espacios de direccionamiento, la dirección IP divide los 32 bits en cuatro octetos[3], una dirección IP está formada por el identificador del host y el identificador de la red.

El identificador de red permite identificar qué dispositivos están compartiendo una misma red, el identificador del host permite identificar un dispositivo en particular.

Existen distintas notaciones para representar una dirección IP, la más común es usar cuatro números decimales separados por un punto, cada número decimal expresa el valor del correspondiente octeto de la dirección y se encuentra entre 0 y 255, en notación hexadecimal las direcciones se encuentran entre 0 y FF y por último, en notación binaria los valores se encuentran entre 0000 0000 y 1111 1111 por octeto, por ejemplo, las representaciones en las tres formas antes mencionadas de una dirección IP se muestran a continuación:

a) 162.128.2.1 en su notación decimal

b) 10100010.10000000.00000010.00000001 en su notario binaria

c) A2.80.2.1 en su notación hexadecimal

1.3.2 Clases de direcciones

Hay cinco clases de direcciones, cabe destacar que las clases A ,B y C son de uso comercial, la clase D es para multicast y la clase E de tipo experimental.

1. Clase A

[3] Un octeto se refiere a una cantidad formada exclusivamente por ocho bits

La primera clase de red conocida como direcciones de clase A se identifican cuando el bit más significativo en notación binaria tiene un 0, es decir, **0**000 0001 ó 1 en notación decimal, por lo que el identificador de red se encuentra entre 1 y 126, los siguientes 3 octetos identifican al host permitiendo 16,777,214 hosts por red.

2. Clase B

Las direcciones de clase B tienen en los dos primeros bits más significativos un 10 binario es decir **10**00 0000, ó 128 en notación decimal, a diferencia de las direcciones de clase A, las direcciones de clase B utilizan los dos primeros octetos más significativos para el identificador de red donde éste se encuentra entre 128.0 y 191.255, permite 16,384 redes con 65,534 hosts por red.

3. Clase C

Las direcciones de clase C en sus primeros tres bits más significativos tienen un 110 binario, es decir, que en el primer octeto presentan **110**0 0000 ó 192 en decimal, la dirección clase C utiliza los 3 primeros octetos más significativos para el identificador de red y un solo octeto para el identificador de host, así el rango de redes se encuentra entre 192.0.0 y 223.255.255, proporcionando 2,097,152 redes y sólo 254 hosts por red.

4. Clase D

Las direcciones de clase D en sus 4 bits más significativos tienen un 1110 binario o 224 en decimal, esta clase de dirección sirve para realizar funciones de multicast, que es el envío de información a múltiples destinos simultáneamente, el rango de esta clase se encuentra entre las direcciones 224.0.0.0 y 239.255.255.254.

El funcionamiento de multicast es básicamente cuando un emisor envía un único paquete del cual se realizan copias y se envían a varios receptores.

5. Clase E

Las direcciones clase E son de uso experimental, para poder identificarlas se toman en cuenta sus 4 bits más significativos, un 1111 binario o 240 en decimal, por lo que el rango de direcciones se encuentra entre 240.0.0.0 y 255.255.255.254.

Con las clases de direcciones sólo es posible tener una cantidad de máquinas asociadas a cierta clase dependiendo de cuál se esté utilizando, con las clases de red se presenta un desperdicio de direcciones ya que si se cuenta con menos de 100 dispositivos, convendría utilizar una clase de red C, lo que supondría tener 150 direcciones desperdiciadas.

Esto se soluciona si se dividen estas direcciones en otro conjunto de direcciones más pequeñas, de esta manera se generan otro tipo de redes, a éstas se les conoce como classless - sin clase, la primera implementación que se utilizó fue el VLSM [Cb]que divide una red en varias redes pequeñas con una longitud fija.

A estas pequeñas redes que derivan de otra se le conoce como subred, una red puede estar conformada por varias subredes por lo que una subred es un conjunto de direcciones lógicas.

1.3.3 Máscara de red

Una dirección IP acompañada de una máscara de red ayuda a identificar a qué subred pertenece un dispositivo con una operación rápida que consuma pocos recursos, una máscara de red es un número que está formado por cuatro octetos, por lo que tiene una longitud de 32 bits y puede estar representada por números decimales o por números en binario.

Sin embargo, VLSM en todas las subredes utiliza la misma máscara de red, por lo que se tiene un número fijo de hosts, posteriormente se introdujo otra mejora a la planificación de redes, ésta es conocida como CIDR (Classless Inter-Domain Routing o enrutamiento Inter-Dominios sin clase) que permite tener varias subredes cada una con una cantidad de hosts distinto, permitiendo ajustar las subredes según sean las necesidades, para poder identificar la máscara de red que está asociada, se usa una notación que va después de la dirección IP separada por una diagonal, a este número se le conoce como CIDR que indica cuántos bits están activos, es decir, cuántos bits tienen el valor de 1.

Esto es posible ya que existen valores que no están permitidos para una máscara de red, la cual no debe tener valores intermedios distintos en su notación binaria, es decir, dentro de una serie de unos no debe existir un cero entre ellos, con esto se puede elaborar una tabla para identificar todas las máscaras de red que pueden existir en IPv4 la cual se muestra en la tabla 1.3.

Tabla 1.3 Máscara de Red en IPv4

Decimal	Binario	CIDR
255.255.255.255	11111111.11111111.11111111.11111111	/32

255.255.255.254	11111111.11111111.11111111.11111110	/31
255.255.255.252	11111111.11111111.11111111.11111100	/30
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.254.0	11111111.11111111.11111110.00000000	/23
255.255.252.0	11111111.11111111.11111100.00000000	/22
255.255.248.0	11111111.11111111.11111000.00000000	/21
255.255.240.0	11111111.11111111.11110000.00000000	/20
255.255.224.0	11111111.11111111.11100000.00000000	/19
255.255.192.0	11111111.11111111.11000000.00000000	/18
255.255.128.0	11111111.11111111.10000000.00000000	/17
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.254.0.0	11111111.11111110.00000000.00000000	/15
255.252.0.0	11111111.11111100.00000000.00000000	/14
255.248.0.0	11111111.11111000.00000000.00000000	/13
255.240.0.0	11111111.11110000.00000000.00000000	/12
255.224.0.0	11111111.11100000.00000000.00000000	/11
255.192.0.0	11111111.11000000.00000000.00000000	/10
255.128.0.0	11111111.10000000.00000000.00000000	/9
255.0.0.0	11111111.00000000.00000000.00000000	/8

254.0.0.0	11111110.00000000.00000000.00000000	/7
252.0.0.0	11111100.00000000.00000000.00000000	/6
248.0.0.0	11111000.00000000.00000000.00000000	/5
240.0.0.0	11110000.00000000.00000000.00000000	/4
224.0.0.0	11100000.00000000.00000000.00000000	/3
192.0.0.0	11000000.00000000.00000000.00000000	/2
128.0.0.0	1000000.00000000.00000000.00000000	/1
0.0.0.0	00000000.00000000.00000000.00000000	/0

La máscara hace una operación lógica AND bit a bit de cada octeto comparando la dirección IP con la máscara de red, del resultado se obtiene el campo de identificador de red.

a) Por ejemplo, considérese la siguiente dirección IP:

105.32.200.20

y su respectiva máscara de red:

255.255.255.240

Al realizar la operación AND bit a bit en su forma binaria:

01101001.00100000.11001000.00010100

•

11111111.11111111.11111111.11110000

––––––––––––––––––––––––––––––––

01101001.00100000.11001000.00010000

El valor que se obtiene en notación decimal es el siguiente:

105.32.200.16

b) Con la misma máscara de red del inciso a), se tiene la siguiente dirección IP:

105.32.200.24

Realizando las mismas operaciones hechas con anterioridad se observa:

01101001.00100000.11001000.00011000

•

11111111.11111111.11111111.11110000

−−−−−−−−−−−−−−−−−−−−−−−−

01101001.00100000.11001000.00010000

Donde se obtiene el mismo identificador de red que es:

105.32.200.16

Esto quiere decir que las dos direcciones anteriores se encuentran dentro de un mismo segmento de red.

c) Por último la siguiente dirección conservando la misma máscara de red:

105.32.200.33

Realizando las mismas operaciones.

01101001.00100000.11001000.00100001

•

11111111.11111111.11111111.11110000

−−−−−−−−−−−−−−−−−−−−−−−−

01101001.00100000.11001000.00100000

El valor que se obtiene en notación decimal es el siguiente

105.32.200.32

En estas tres direcciones IP se tienen dos distintos identificadores de red (105.32.200.16 y 105.32.200.32), al realizar la operación AND de la dirección IP y la máscara de red correspondiente, se obtiene un identificador de red (105.32.200.16), las direcciones que contengan el mismo identificador de red están agrupadas en un segmento de red, con el ejemplo anterior las direcciones 105.32.200.20 y 105.32.200.24 cuentan con el mismo identificador de red por lo que están agrupadas en una misma subred, y la dirección 105.32.200.33 no pertenece a la misma subred de las dos direcciones anteriores al tener otro identificador de red (105.32.200.32), pertenece a otra subred.

1.3.4 Cabecera IPv4

La estructura interna de un paquete de datos en IPv4 está conformada de la siguiente manera:

Todo paquete comienza con una cabecera, ésta cuenta con 13 campos de los cuales 12 son de carácter obligatorio ya que dentro de estos campos se especifican parámetros como el

destino del paquete, longitud, así como información vital para que sea recibido el paquete satisfactoriamente por el destinatario correcto. El último campo es opcional, éste cuenta con un tamaño mínimo de 20 bytes y con un máximo de 60 bytes debido a las limitaciones, las opciones deben tener una longitud múltiplo de 4 bytes.

Tabla 1.4 Cabecera IPv4

<table>
<tr><td colspan="6">0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</td></tr>
<tr><td>versión</td><td>IHL</td><td colspan="2">Tipo Servicio</td><td colspan="2">Longitud Total</td></tr>
<tr><td colspan="3">Identificación</td><td>Flags</td><td colspan="2">Posición</td></tr>
<tr><td colspan="2">Tiempo de vida</td><td>Protocolo</td><td colspan="3">Suma de control de cabecera</td></tr>
<tr><td colspan="6">Dirección de Origen</td></tr>
<tr><td colspan="6">Dirección de Destino</td></tr>
<tr><td colspan="5">Opciones</td><td>Relleno</td></tr>
</table>

En la tabla 1.4 se muestra la cabecera con sus distintos campos, además del tamaño en bits que ocupa cada uno, los cuales son los siguientes:

a) Versión: 4 bits

Este campo describe a versión de la cabecera

b) IHL: 4 bits

Internet Header Length - Longitud de la cabecera Internet, nos indica la longitud de la cabecera en palabras de 32 bits esta puede variar si la cabecera cuenta con los campos opcionales, la longitud de la cabecera debe ser un múltiplo de 32 bits, en caso de no ser se usa el campo de relleno, la longitud mínima es 5 y la máxima es 15.

c) ToS: 8 bits

Type of Service - Tipo de servicio, proporciona una indicación de los parámetros abstractos de la calidad de servicio deseada.

Los campos que son utilizados a nivel de bits se observan en la tabla 1.5

Tabla 1.5 Campos a nivel de bits

Bits	Valor binario 0	Valor binario 1
0 - 2	Prioridad	
3	Demora Normal	Baja Demora
4	Rendimiento Normal	Alto Rendimiento
5	Fiabilidad Normal	Alta Fiabilidad
6 - 7	Reservado para uso futuro	

El campo de prioridad puede tener 8 valores distintos, los cuales corresponden a lo observado en la tabla 1.6.

Tabla 1. 6 Campo de Prioridad

111	Control de red
110	Control entre redes
101	Critical and emergency call processing - Crítico/ECP
100	Flash Override - Muy urgente
011	Flash - Urgente
010	Inmediato
001	Prioridad
000	Rutina

En general el tipo de servicio se usa para especificar el tratamiento del paquete durante su transmisión a través de Internet.

d) Longitud Total: 16 bits

La longitud total es la longitud del paquete medida en octetos, incluyendo la cabecera y los datos, por el tamaño de este campo se permite que la longitud máxima de un paquete sea de 65,535 octetos (esto es, 2^{16}), en todos los hosts se requiere que tengan la capacidad de manejar como mínimo 576 octetos.

e) Identificación: 16 bits

El campo de identificación es usado cuando un paquete es fragmentado, sirve para identificar fragmentos de un único paquete para su correcta recepción.

f) Flags - Indicadores: 3 bits

Los indicadores son usados para el control o la identificación de fragmentos, los valores que puede tener este campo se muestran en la tabla 1.7.

Tabla 1. 7 Indicadores

Bit	Uso	Valor binario 0	Valor binario 1
0	Reservado	Debe ser cero	
1	No fragmentar (DF)	Puede fragmentarse	No fragmentar
2	Más fragmentos (MF)	Último fragmento	Más fragmentos

g) Posición del fragmento: 13 bits

Este campo indica a qué parte del paquete pertenece el fragmento, los fragmentos se miden en unidades de 8 octetos por lo que si un paquete de Internet es demasiado grande para incluir toda su información dentro de un solo paquete, los datos deben ser divididos en múltiplos de 8 octetos.

Por el tamaño de este campo se permiten hasta 8192 fragmentos (esto es, 2^{13}) de 8 octetos cada uno, de ahí se dice que soporta un total de 65,536 octetos.

h) TTL: 8 bits

Time To Live - Tiempo de vida, este campo ayuda a prevenir que los paquetes se encuentren dentro de un tiempo indefinido en la red por lo que delimita la existencia de un paquete, el tiempo es medido en segundos y es descartado cuando éste llegue a tener el valor cero, su valor va decreciendo conforme va siendo atendido, es decir, cuando es atendido por un módulo éste decrementa como mínimo una unidad de su valor total, independiente de si fue procesado en menos de un segundo.

i) Protocolo: 8 bits

ii) Este campo define el protocolo que va a utilizar el campo de datos, los valores de los protocolos están definidos por la IANA[4].

j) Header Checksum: 16 bits

Suma de control de la cabecera, este campo se utiliza para comprobar errores en la cabecera, en cada salto este número es recalculado ya que hay campos que varían (por ejemplo el TTL), en caso de que no hubiera una concordancia, el paquete es descartado, los errores en los datos del paquete son calculados

k) Dirección Origen: 32 bits

Contiene la dirección desde donde es enviado el paquete

l) Dirección destino: 32 bits

Contiene la dirección hacia donde es enviado el paquete

m) Opciones: variable

Este campo tiene longitud variable ya que no es obligatorio el uso de este campo, la cabecera puede no contar con opciones o a su vez contar con varias opciones, hay dos casos para el formato de una opción:

- Formato simple: un solo octeto de tipo-opción.
- Formato compuesto: un octeto tipo-opción, un octeto longitud-opción y los octetos correspondientes a los datos de opción.

El octeto de tipo-opción es un formato simple constituido por un solo byte, el cual está dividido en 3 campos:

1. Indicador de copiado (1 bit)

El indicador de copiado se usa en caso de fragmentación y sólo se presentan dos casos:

0 - No se copia.

1- Se copia.

2. Clase de opción (2 bits)

En la clase de opción se presentan los siguientes casos:

[4] IANA (Internet Assigned Number Autority - Autoridad de asignación de números en Internet) es la entidad encargada de coordinar algunos elementos de Internet, específicamente almacena códigos y los sistemas de numeración únicos que se utilizan en los estándares técnicos ("protocolos") http://www.iana.org/about/

00 - Control

01 - Reservado para uso futuro.

10 - Depuración y medida.

11 - Reservado para uso futuro

3. Número de opción (5 bits)

Indica una acción específica. Se cuenta con las siguientes opciones de Internet observadas en la tabla 1.8.

Tabla 1. 8 Opciones de Internet

Clase	Número	Longitud	Descripción
0	0	-	Fin de la lista de opciones. Esta opción ocupa un solo octeto. No tiene octeto de longitud
0	1	-	Sin operación. Esta opción ocupa un solo octeto. No tiene octeto longitud.
0	2	11	Seguridad. Usado para seguridad, compartimentación, grupo de usuario (TCC) y códigos de manejo de restricciones compatibles con los requerimientos del Departamento de Defensa
0	3	Var.	Loose Source Routing - Encaminamiento de origen No estricto. Usado para encaminar el datagrama Internet en base de la información suministrada por el origen
0	9	Var.	Strict Source Routing - Encaminamiento de Origen fijo. Usado para encaminar el datagrama Internet con base en la información suministrada por el origen
0	7	Var.	Record Route - Registrar Ruta. Usado para rastrear la ruta que sigue un datagrama Internet
0	8	4	Stream ID - Identificador de Flujo. Usado para transportar el identificador de flujo
2	4	Var	Internet Timestamp - Marca de tiempo Internet

n) Relleno: variable

El valor de relleno se usa para asegurar que la cabecera Internet ocupe un múltiplo de 32 bits, el valor usado es cero.

Capítulo 2

Transición de IPv4 a IPv6

Los temas de investigación relacionados con las Tecnologías de la Información dejan de ser sólo una mención sin importancia cuando los gobiernos ya tienen problemas económicos y necesitan soluciones a futuro. Algunos países se han dado cuenta que el nuevo protocolo IPv6 no sólo es una actualización sino que podría permitirles tomar cierta posición de liderazgo en un futuro cercano. El cambio a IPv6 permitirá mejorar enormemente los servicios y negocios proporcionados por las Tecnologías de la Información y fortalecerá los rezagos con los que IPv4 cuenta.

2.1 La necesidad de la transición de IPv4 a IPv6.

IPv4 no ha cambiado significativamente desde que fue publicado en el RFC (Request For Comments - Petición de comentarios) 791 [Ca.] , en el año de 1981. Al momento de su desarrollo se pensó en que fuera de fácil implementación, robusto (con muchas opciones) y que fuera interoperable. Así se ha mantenido durante más de 20 años, pero como en toda tecnología, con el paso del tiempo surgen nuevas necesidades que posiblemente no fueron pensadas con anterioridad, muchas de estas necesidades se han cubierto con soluciones como el CIDR y el NAT.

A continuación se presentarán ciertos aspectos que en el diseño original de IPv4 no fueron previstos [DAVIES 2008]:

- **El reciente crecimiento exponencial de internet y la escasez de direcciones IPv4.** Los 32 bits de direccionamiento que permiten 4 294 967 296 direcciones podría parecer un número de direcciones lo suficientemente grande como para que las direcciones IP no se terminaran, pero Internet ha crecido tanto que ahora las redes de datos pueden estar formadas por diferentes tipos de dispositivos que no utilizan las mismas subredes, por ejemplo, una persona puede contratar Internet para su computadora, tener contratado su teléfono con conexión a Internet y su televisión de paga con diferentes compañías. Además existe un creciente aumento de servicios para empresas, fábricas y hospitales que necesitan de una asignación de direcciones y la demanda actual de direcciones IP por países asiáticos con grandes poblaciones como China e India han acelerado la escasez.

- **La necesidad de una configuración más simple.** Muchas de las implementaciones actuales deben configurarse manualmente o usan un protocolo de configuración de estado de la dirección como el DHCP (Dynamic Host Configuration Protocol - Protocolo Configuración Dinámica de Anfitrión). Con más computadoras y dispositivos usando direcciones IP, existe una necesidad de implementar una configuración que sea automática y más simple con más opciones que no retrasen la administración de una infraestructura DHCP.
- **La importancia de una capa de seguridad.** Las comunicaciones privadas que viajan a través de un medio público como lo es Internet necesitan de servicios

criptográficos para que protejan los datos evitando que sean vistos o modificados por otras personas, existen protocolos como el IPsec (Internet Protocol security - Seguridad en el Protocolo de Internet) que proporcionan estos servicios pero no son obligatorios lo que hace vulnerable al servicio.

- **La entrega de los datos en tiempo real.** Muchas de las aplicaciones que se utilizan sobre Internet requieren que los datos que sean enviados a su destino lleguen lo suficientemente rápido para que no se entorpezca alguna actividad, por ejemplo, en la actualidad muchos hospitales no pueden dar ciertos tipos de servicios en todas las regiones en donde tienen instalaciones, algunos están especializados en ciertas áreas y si un paciente presenta problemas que sólo pueden ser solucionados en esas instalaciones, entonces el paciente tiene que ser trasladado a esas instalaciones especializadas, pero eso es muy incómodo y el paciente puede sufrir serios daños en el trasladado, ahora existe en algunos lugares la posibilidad de que el paciente sea atendido en su clínica más cercana mediante consultorios o quirófanos donde un doctor es asistido por un especialista para atender el problema del paciente, este tipo de asistencia se hace por medio de Internet y la necesidad de que la consulta sea en tiempo real es sumamente importante. En IPv4 la eficiencia de la entrega del tráfico en tiempo real recae sobre el campo Type of Service y en la identificación del payload. Desafortunadamente los campos ToS han limitado la funcionalidad y a través del tiempo han tenido diferentes interpretaciones locales que han evitado una eficiente entrega de datos.

De los anteriores puntos, la escasez de direcciones IP se considera el más crítico debido a que tiene más consecuencias negativas. En lugares del mundo donde las direcciones IPv4 están escaseando más, existen múltiples niveles de NAT entre el cliente e Internet. A través de la NAT se permite que más clientes estén conectados a Internet, pero también actúan como cuellos de botella y barreras de tráfico de red, además se realizan operaciones para la translación de direcciones que demuestran que NAT es una solución no escalable, provisional y que limita la comunicación end to end (punto a punto).

Al final del 2007, la población del mundo alcanzó aproximadamente los 6.6 mil millones de habitantes [D] y un reporte de las Naciones Unidas pronosticó que para el año 2030 la población alcanzará los 8 mil millones de habitantes, Internet tiene una población de 1.3 mil millones de usuarios, la distribución de estos usuarios es mostrada en la figura 2.1.

El uso de Internet ha visto acelerado su crecimiento alrededor del mundo, particularmente dentro de los mercados emergentes. Por ejemplo, en África, una de las regiones con menos usuarios en el mundo, ha incrementado el uso de Internet aproximadamente un 880 por ciento entre los años 2000 y 2007. Este pronóstico de crecimiento le da una nueva perspectiva a la necesidad de direccionamiento IP.

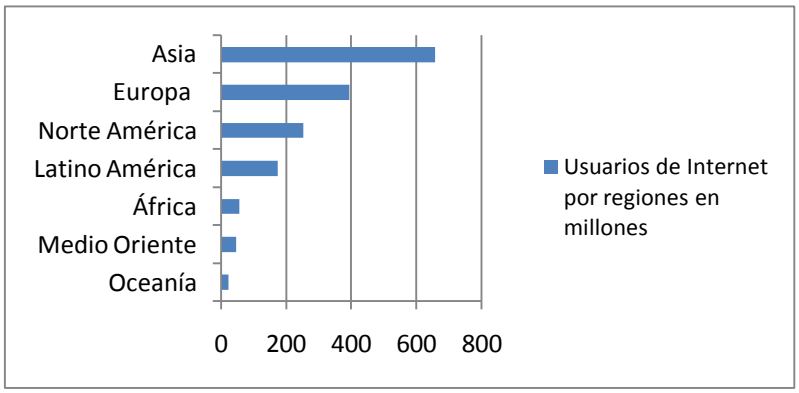

Figura 2.1. Distribución de los usuarios de Internet en el mundo [E].

Por ejemplo, para un negocio pequeño que usa este rango de direcciones privadas 192.168.0.0/24 y que tiene asignada la dirección pública 131.107.47.119 por su ISP (Internet Service Provider – Proveedor de Servicios de Internet) se considera que dentro de esa red un usuario con la dirección 192.168.0.10 utiliza un navegador Web, para conectarse al servidor Web con la dirección 157.60.13.9 el host privado (192.168.0.10) crea un paquete IPv4 con los siguientes datos:

Dirección destino: 157.60.13.9

Dirección origen: 192.168.0.10

TCP Puerto destino: 80

TCP Puerto origen: 1025

Se muestra la configuración en la figura 2.2

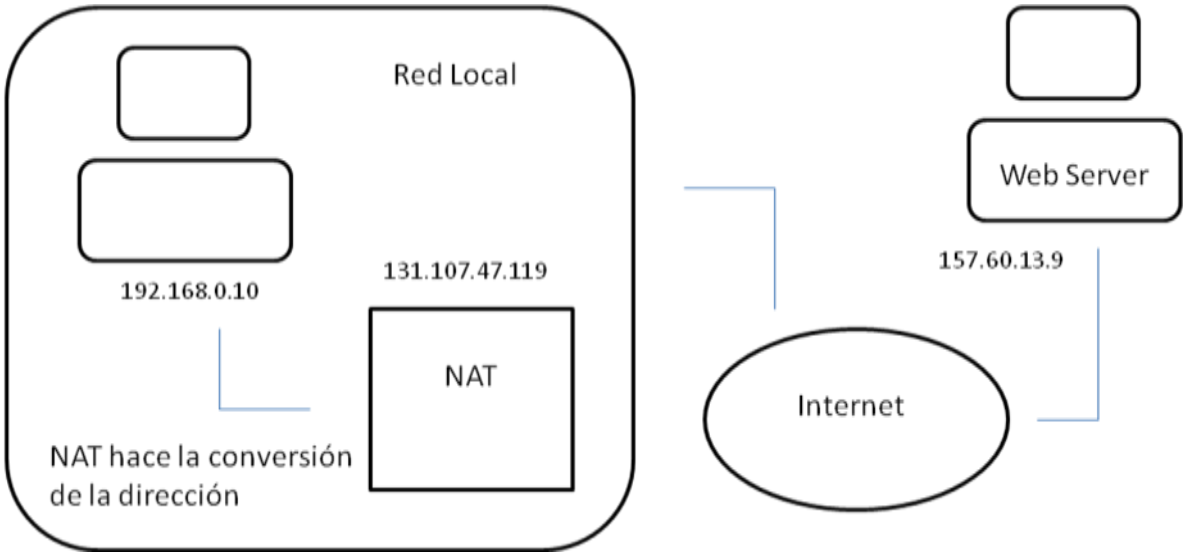

Figura 2.2 Ejemplo de NAT

El paquete IPv4 es trasladado de la dirección y puerto origen al paquete que saldrá de la dirección pública (131.107.47.119).

Dirección destino: 157.60.13.9

***Dirección origen**:* 131.107.47.119

Puerto TCP destino: 80

Puerto TCP origen: 5000

La NAT mantiene los datos de las direcciones y puertos en una tabla local de transición (192.168.0.10 – puerto 1025) y (131.107.47.119 – puerto 5000). El paquete es enviado a través de Internet para esperar la respuesta del servidor WEB que es recibida por la NAT y cuando esto sucede el paquete contiene lo siguiente:

Dirección destino: 131.107.47.119

Dirección origen: 157.60.13.9

Puerto TCP destino: 5000

Puerto TCP origen: 80

La NAT compara con su tabla interna de transición la dirección y el puerto que anteriormente había transformado, después envía el paquete al host de la red interna (192.168.0.10) y el paquete contiene lo siguiente:

Dirección destino: 192.168.0.10

Dirección origen: 157.60.13.9

Puerto TCP destino: 1025

Puerto TCP origen: 80

Durante cada cambio de host en la red interna, la NAT tiene que hacer las operaciones de cambio de dirección y de puerto en cada uno de los paquetes enviados, en una dirección pública sólo se tiene que hacer la traslación de la IPv4 en el encabezado IPv4 y la traslación del puerto ya sea TCP o UDP. Para lugares con pocos dispositivos no representa gran problema la existencia de la NAT pero en instalaciones muy grandes y con servicios de alta demanda puede causar problemas.

2.1.1 Implicación económica

El impacto global de una tecnología o un conjunto de tecnologías dentro de toda una sociedad puede ser realmente evaluado años después de su creación, cuando una gran cantidad de datos ya ha sido acumulada para realizar un análisis adecuado. Por ejemplo, a lo largo y ancho de todos los posibles temas de la vida (arte, educación, política, filosofía, literatura y ciencia) el periodo del Renacimiento, que fue uno de los periodos más creativos de la historia humana, puede ser identificado por una tecnología: la imprenta moderna. El invento de Gutenberg[5] incrementó enormemente la documentación del conocimiento e información reduciendo costos de captura y más importante aún, la imprenta incrementó la accesibilidad del conocimiento reduciendo costos de duplicado. Una tecnología permitió a la civilización humana construir la base de su conocimiento y el invento de Gutenberg fue el catalizador de otras revoluciones tecnológicas. En la actualidad Internet representa el medio revolucionario por el cual se maneja la información, la forma en que se aprende, se trabaja y se vive.

Es importante hacer una clara distinción entre Internet y las aplicaciones que corren a través de él. Estas aplicaciones, muchas creadas por los propios usuarios, son una medida real del impacto económico y social de Internet, todas estas aplicaciones han creando una economía dentro del mismo Internet lo suficientemente estable como para tener una estructura que permita conocer el verdadero potencial de sus aplicaciones y servicios.

Desde su desarrollo inicial hasta estos días, Internet es una infraestructura que ha sufrido el deterioro de sus dispositivos, aplicaciones y servicios debido a la directa relación con sus capacidades de direccionamiento y escala, por ejemplo:

- **Más velocidad:** Internet está impulsando nuevas tecnologías de manera inalámbrica o por cable, que incrementan el ancho de banda y minimizan costos.

[5] Johannes Gutenberg (hacia 1398 – 3 de febrero de 1468) fue un herrero alemán inventor de la imprenta de tipos móviles en Europa.

- **Mayor crecimiento:** Continuamente Internet se está expandiendo geográficamente incluyendo cada vez más gente y negocios.

- **Nuevos dispositivos:** Internet está evolucionando a una conectividad de una enorme diversidad de dispositivos que pueden ir de servidores hasta refrigeradores.

- **Disponibilidad** Internet permite a los usuarios comunicarse continuamente sin importar el punto o dispositivos que se utilicen.

Al día de hoy nadie se puede imaginar al mundo sin conexión a Internet, el diseño original de IP no imaginó este nivel de adopción de la sociedad a la tecnología y simplemente IPv4 no tiene los recursos suficientes para conectar a toda la población de la tierra.

La demanda de acceso a la información está creciendo en sincronía con el impresionante volumen de información disponible, productos y servicios relacionados con la entrega de contenido se están incrementando enormemente y se apoyan en infraestructuras IP. Por ejemplo: [GROSSETETE 2008]

- **Entretenimiento:** Proveedores de contenido como YouTube obtienen su base de usuarios mediante el contenido gratuito pero de baja calidad y ahora se está convirtiendo en una plataforma de comunicación política y de negocios. De manera parecida IMS (IP Multimedia Subsystem – Subsistema Multimedia IP) permite la aplicación de contenido llamado servicios "triple play" que combina voz, video y datos a través de IP.

- **Educación:** La educación a distancia empieza a ser una parte significativa de las universidades. La opción de poder acomodar el horario de aprendizaje con el horario personal del estudiante hace de la educación a distancia una opción bastante atractiva para aquellos que se encuentran trabajando o realizan otras actividades.

- **Negocios:** Mediante informes de precios, reportes de noticias, planes de operaciones o inventarios, la información interviene en los negocios y ésta es adquirida mediante infraestructuras IP, entonces la disponibilidad es esencial para poder tener una apropiada operación en los negocios.

- **M2M (Machine to Machine – Máquina a Máquina).** La información es una parte importante en las comunicaciones M2M como en redes industriales. La generación y uso de información en tiempo real abre la puerta a un espectro enorme de oportunidades para manejar y construir innovaciones automáticas y más efectivas, además de tener una mejor administración y seguridad en los procesos. El número de sensores, actores y efectores dentro de un ambiente industrial ya es enorme y las emergentes redes de sensores y nano máquinas los desplazarán. Para poder utilizar

todos esos dispositivos hay que usar una infraestructura escalable que les permita adquirir y proveer información.

En un reporte del NIST(National Institute of Standars and Technology – Instituto Nacional de Tecnología y Estándares) de octubre del 2005, preparado para el Departamento de Comercio de los Estados Unidos, se realizó un análisis de la evolución sobre el cambio de protocolos IPv4 a IPv6 y la medida en tiempo con la que será desplazado IPv4, se consultaron 4 grupos principales, vendedores de dispositivos, vendedores de aplicaciones, proveedores de Internet y usuarios de Internet.

De los resultados importantes se agruparon las siguientes ventajas de IPv6 con sus respectivas aplicaciones (Tabla 2.1): [GALLAHER 2005]

Tabla 2.1 Aplicaciones y ventajas de IPv6

Ventajas	Aplicación	Ejemplos
Reducción de costos a causa de la seguridad implementada.	IPsec	Los costos de seguridad están aumentando y la tendencia es utilizar modelos de seguridad que reduzcan estos costos, IPsec puede ayudar a las compañías a integrarse mejor a estos modelos.
Reducción de costos a causa del incremento de la eficiencia.	VoIP Desuso de NAT	Si las grandes compañías telefónicas adoptarán el servicio VoIP substituyendo las tradicionales redes telefónicas, los costos se reducirían drásticamente. Las grandes compañías gastan en soluciones relacionadas con NAT y en negocios relacionados con las Tecnologías de la Información podrían reducir costos.
La importancia del acceso	Incremento de la vida útil de	Para los desarrolladores de

remoto en productos y servicios.	los productos.	productos y aplicaciones para automóviles es importante extender el tiempo de vida de sus productos, además de que pueden prestar un mejor servicio mediante soporte remoto.
Innovación en comunicaciones	Nuevos servicios de datos para dispositivos móviles.	Las compañías de productos inalámbricos podrían crear dispositivos con capacidades de expansión de red, sobre todo para teléfonos móviles.
Innovación en productos y servicios en línea.	Juego en línea.	El juego en línea requiere que el servicio sea en tiempo real por la interacción con mas jugadores, además que en el futuro las compañías ya no desarrollarán más consolas de juegos, solamente prestarán un servicio en línea para que se reciba el video en tiempo real de tus acciones.

La idea de una transición tan compleja y de infraestructuras operacionalmente críticas como lo son las redes IP de una versión a otra requiere un profundo análisis. A primera vista los costos esperados parecen ser muy elevados y la pregunta que inmediatamente llega a la mente es: ¿Cuál es el beneficio de una inversión tan grande?

Durante mucho tiempo toda la comunidad relacionada con los temas de IPv6 ha vivido debajo del gran peso de la pregunta ROI (return on investment – retorno de inversión), una pregunta que se ha vuelto muy común durante la depresión de internet que inició a principios del 2000 y que se desenvuelve en muchas cuestiones, ¿Qué tanto puedo escalar mi red y servicios actuales? y ¿Qué tan fácil es hacerlo?, ¿Qué beneficios son generados en un ambiente con suficientes recursos de infraestructura IP?. La respuesta de la ROI IPv6 es:

no se puede calcular fácilmente pero sí se puede preguntar ¿Cuáles son los costos que tiene no integrar IPv6 en las redes? y ¿Cómo es que IPv6 puede posicionar estratégicamente?

Es importante recalcar la diferencia de transición a integración, en la actualidad una transición de una red IPv4 a una IPv6 no es un objetivo realista y generalmente un objetivo difícil de justificar técnica y económicamente. IPv6 está siendo integrada paulatinamente en infraestructuras IPv4 y servicio a servicio.

Los cálculos de una ROI generalmente son aplicados a servicios y a operaciones de red. IPv6 no es un servicio, solamente soporta servicios. Los servicios y las operaciones de red son benéficos económicamente, IPv6 permite a las redes incrementar las operaciones y servicios. Este punto ha sido claramente establecido por los operadores de cable que escogen IPv6 para administrar sus infraestructuras en vez de utilizar la opción técnicamente más factible pero más cara que son las opciones IP.

En años recientes, la televisión por cable en Estados Unidos MSO (multiple system operators – operadores de sistemas múltiples) tiene interconectadas sus redes de contenido en la columna vertebral de ancho de banda nacional. Aunque el espacio de las direcciones IPv4 privadas fue suficiente para administrar los dispositivos en un ambiente consolidado, el RFC 1918 [Cc] (espacio de las direcciones privadas) no ofrece suficientes recursos para administrar los dispositivos agrupados.

Desde una perspectiva técnica, los MSO tienen la opción de federalizar sus redes, reutilizando sus direcciones privadas en cada dominio y administrar cada dominio independientemente. IPv6 podría fácilmente ofrecer a los proveedores de cable las direcciones suficientes para administrar sus dispositivos en un solo dominio. Un cálculo teórico simple basado en una presentación desarrollada por Comcast (compañía de televisión por cable en Estados Unidos) en la universidad de Pennsylvania en Noviembre del 2005, en ese momento existían 17.7 millones de suscriptores, distribuidos en varias regiones divididas de esta manera:

- Cuatro regiones con 1.5 millones de subscriptores.
- Tres regiones de 1 a 1.5 millones de subscriptores.
- Nueve regiones con 0.5 millones de subscriptores.
- Cinco regiones con menos de 0.5 millones de subscriptores.

En 2005 el costo de la licencia para proveer el servicio de tv por cable pudo ser de 1,625,000 dólares por 5 millones de subscriptores, 500,000 suscriptores por 1 millón de dólares y 175,000 dólares por 250 subscriptores. En este caso Comcast podría gastar 0-36 dólares por proveer el servicio a cada usuario en un modelo centralizado que no soporta

IPv4. En un ambiente federal, la ineficiencia en el uso de las licencias incrementa el costo a 0.64 dólares por subscriptor.

2.2 Características IPv6.

IPv6 cuenta con direcciones más largas, es decir, de tener un número formado por 32 bits (4,294,967,296 direcciones en IPv4) pasa a tener un número formado por 128 bits (aproximadamente 340 sextillones[6] de direcciones) esto cuadruplica el tamaño de bits para generar cada dirección viéndose beneficiada la cantidad de direccionamiento que IPv6 puede soportar.

En IPv6 existen tres tipos de notación para las direcciones, al tener una cifra de mayor tamaño para una dirección IP, ésta necesita ser representada por un número más grande en comparación con la utilizada en IPv4, por lo que ahora el nuevo formato adquirido para este protocolo queda estructurado por 8 grupos de cuatro dígitos hexadecimales con un tamaño de 16 bits, separados por dos puntos ":", por ejemplo:

ABCD:EF01:2345:6789:ABCD:EF01:2345:6789

Además, existen casos en donde se presentan grupos que cuentan con el valor cero, estos grupos de ceros pueden simplificar la notación indicando el carácter "::", esta notación indica que existe uno o más grupos de 16 bits de ceros, por ejemplo:

Para la siguiente dirección IPv6:

2001:0448:0000:0000:0000:0000:0000:2474

Para comprimir la dirección con el uso de la notación anterior ésta queda representa de la siguiente manera

2001:0448::2474

El carácter "::" sólo puede aparecer una sola vez en toda la dirección ya que si se utilizan dos o más, se desconocería la cantidad de grupos que cuentan con ceros, por ejemplo, la siguiente dirección no es válida.

2001::0448::2471

También los ceros se pueden indicar de la siguiente manera:

2001:0448:0:0:0:0:0:2474

[6] Prefijo del sistema internacional de unidades, sextillones se refiere a una cantidad numérica formada por mil trillones de números o en su equivalencia decimal es 1,000,000,000,000,000,000,000

Además existe una dirección IPv4 que está camuflada dentro de una dirección IPv6, esto se logra colocando la dirección IPv4 en decimal en los bytes menos significativos de la dirección IPv6 seguido del identificador FFFF, por ejemplo:

::FFFF:129:144:52:38

2.2.1 Nuevo Formato de Encabezado

IPv6 cuenta con una cabecera diseñada para minimizar el procesamiento, suprimiendo campos que no eran necesarios, así como algunas opciones que eran utilizadas sólo en procesos específicos y que rara vez son utilizados, pero sí son procesados en cada salto del paquete, un ejemplo son los procesos de verificación que se realizaban varias veces cuando éstos podrían ser únicamente procesados en el destino aligerando la carga de los nodos para así optimizar el envío de los paquetes, IPv6 no suprime por completo las opciones, las agrega cuando sólo se necesiten en forma de extensiones.

El formato de la cabecera fue modificado, anteriormente se usaban 12 campos (de carácter obligatorio) quedando solamente 8 para esta nueva versión del protocolo, en la tabla 2.2 se muestran los campos omitidos para IPv6.

Tabla 2.2 Los campos sombreados se omitieron para IPv6

<table>
<tr><td>Versión</td><td>IHL</td><td>Tipo Servicio</td><td colspan="2">Longitud Total</td></tr>
<tr><td colspan="3">Identificación</td><td>Banderas</td><td>Posición</td></tr>
<tr><td>Tiempo de vida</td><td>Protocolo</td><td colspan="3">Suma de control de cabecera</td></tr>
<tr><td colspan="5">Dirección de Origen</td></tr>
<tr><td colspan="5">Dirección de Destino</td></tr>
<tr><td colspan="4">Opciones</td><td>Relleno</td></tr>
</table>

El nuevo formato de la cabecera pasa a ser de 40 bytes es decir el doble del tamaño con el que cuenta la anterior versión (IPv4 es de 20 bytes), sin embargo, esta cabecera trae como mejoras la optimización en el envío de paquetes a través de la red ya que se procesa con mayor rapidez, el formato de cabecera para IPv6 se observa en la Tabla 2.3

Tabla 2.3 Cabecera IPv6

Versión	Clase de Tráfico	Etiqueta de Flujo	
Longitud de Carga Útil		Encabezado siguiente	Límite de saltos
Dirección Origen			
Dirección Destino			

Los campos para IPv6 son los siguientes:

a) Versión: 4 bits

Identifica la versión del protocolo de Internet, para este caso es 6.

b) Traffic Class – Clase de Tráfico: 8 bits

El campo clase de tráfico se usa para identificar y distinguir las diferentes clases o prioridades de los paquetes IPv6.

c) Flow Label – Etiqueta de flujo: 20 bits

La Etiqueta de flujo es por el momento experimental y se utilizará para aprovechar las ventajas de una subred de datagramas y una subred de circuitos virtuales, ya que se creará una pseudoconexión entre el origen con el destino para que exista un flujo continuo de datos a su vez aprovechando las tablas de ruteo permitiendo una flexibilidad para establecer un camino.

d) Payload Length – Longitud de carga útil: 16 bits

Indica la longitud del paquete en bytes que siguen a la cabecera, incluyendo las cabeceras de extensión (extension header) y el PDU[7].

e) Next Header – Encabezado siguiente: 8 bits

[7]Upper-layer Protocol Data Unit – Protocolo de unidad de datos de la capa superior. Consiste en un protocolo de comunicación entre capas de red.

Este campo indica qué cabecera de extensión sigue a la cabecera principal.

f) Hop Limit – Límite de saltos: 8 bits

Límite de saltos tiene la función de evitar que un paquete se encuentre permanentemente en la red, este campo da un tiempo de vida delimitado por los "saltos" que realiza el paquete entre los dispositivos que va cruzando en su camino antes de llegar a su destino, en cada salto se decrementa una unidad, si su valor es igual a 0 éste es descartado.

g) Source Address – Dirección de origen: 128 bits

Contiene la dirección desde donde es enviado el paquete dentro del formato de IPv6 de 128 bits.

h) Destination Address – Dirección de destino: 128 bits

Contiene la dirección hacia donde es enviado el paquete dentro del formato de IPv6 de 128 bits.

2.2.2 Tipos de Direcciones

Los tipos de direcciones sirven para identificar qué difusión va a tener el paquete que se está enviando a través de la red, definiendo a los remitentes y el alcance de la información, son clasificados por la manera en que difunden los paquetes, de uno a uno, de uno a muchos o dependiendo de la cercanía al emisor.

Los tipos de direcciones se identifican por los bits de valor más significativo, estos bits pertenecen al campo de prefijo del formato, en IPv6 existen tres tipos de direcciones:

1. Unicast

El tráfico unicast se usa para una comunicación de uno a uno con la topología de enrutamiento de unidifusión, es decir, que los paquetes que van dirigidos a una dirección unicast se entregan a una única interfaz.

Hay varios tipos de direcciones Unicast en IPv6 que son de propósito especial.

a) Global unicast address - Dirección unicast global

Esta cabecera pertenece a aggregatable global unicast address (dirección unicast global agregable), que es el formato general para las direcciones unicast (Tabla 2.4)

Tabla 2.4 Cabecera Global Unicast Addresses

3 bits	13 bits	8	24 bits	16 bits	64 bits
FP	TLA ID	RES	NLA ID	SLA ID	Interface ID

- FP (Format Prefix – Prefijo del formato):

  El FP contiene un número formado por 3 bits que sirve para identificar qué tipo de dirección es, en este caso la dirección Global unicast addresses que tiene como valor 001.

- TLA ID (Top Level Aggregator Identifiers – identificador agregado de siguiente nivel)

  Identifican a la autoridad de mayor nivel dentro de la jerarquía de encaminamiento, por su tamaño de 13 bits, permite 8,192 identificadores únicos TLA, sólo las grandes autoridades de asignación tendrán un identificador TLA.

- RES (Reserved – Reservado)

  Este campo está reservado para el futuro crecimiento de los campos TLA y NLA.

- NLA ID (Next Level Aggregation Identifiers – identificador agregado de siguiente nivel)

  Este campo puede ser usado por las autoridades de asignación TLA para subdividir el espacio de direcciones para los proveedores de servicio, este campo de 24 bits puede dirigir 16,777,216 subasignaciones de espacio de direccionamiento.

- SLA ID (Site-Level Aggregation Identifier – Identificador agregado a nivel de sitio).

  Este campo da a los usuarios finales 65,536 subredes únicas, este campo reduce la complejidad de la tabla de ruteo de un sitio.

- Interface ID (identificador de interfaz).

Este tipo de identificadores son usados para identificar una interfaz específica en una conexión, el identificador de interfaz requiere el uso del formato IEEE EUI-64[8].

b) Site-local unicast addresses (Direcciones unicast de sitios locales)

Las direcciones de tipo Site-Local son parcialmente equivalentes con las direcciones IPv4 privadas ya que los paquetes son direccionados dentro de una infraestructura de red y éstos no deben salir de los límites de la red, estas direcciones tienen el prefijo reservado 1111 1110 11 (Tabla 2.5).

Tabla 2.5 Site local Unicast Addresses

10 bits	38 bits	16 bits	64 bits
1111 1110 11	0	Subnet ID	Interface ID

c) Link-local unicast addresses – Direcciones unicast de enlace local.

Estas direcciones sólo son usadas en estaciones que se encuentran conectadas en la misma red local.

Estas direcciones están compuestas con el prefijo 1111 1110 10 y cuenta con ceros en el campo de identificador de interfaz (Tabla 2.6).

Tabla 2.6 Link local Unicast Addresses

10 bits	54 bits	64 bits
1111 1110 10	0	Interface ID

d) Loopback – Auto envío

La dirección unicast Loopback es utilizada por un nodo para enviar un paquete IPv6 a sí mismo, por lo que no está asignada a una dirección física, una dirección unicast Loopback se identifica por tener la dirección 1 teniendo solamente activado el bit menos significativo, es decir ::1

[8] Este formato está diseñado para ser identificador global único, la configuración está dada por el IEEE (Institute of Electrical and Electronics Engineers – Instituto de Ingenieros Eléctricos y Electrónicos), tiene como longitud 64 bits, los primeros 24 bits los asigna IEEE y los siguientes 40 bits son asignados por el fabricante

e) IPv4-mapped IPv6 addresses – mapeo IPv4 en direcciones IPv6

Las direcciones IPv4 pueden ser mapeadas dentro de las direcciones IPv6, este tipo de direcciones son utilizadas por dispositivos que sólo tengan la capacidad de usar IPv4 (Tabla 2.7)..

Tabla 2.7 IPv4 mapped IPv6 Addresses

80 bits	16 bits	32 bits
0000 …. 0000	FFFF	IPv4

e) IPv4 compatible IPv6 adresses

Este tipo de direcciones especiales son asignadas a dispositivos con capacidad de procesar direcciones IPv6, estas direcciones se identifican por tener un arreglo de 96 ceros seguido de la dirección IPv4 en decimal (Tabla 2.8).

Tabla 2.8 IPv4 compatible con IPv6

80 bits	16 bits	32 bits
0000 …. 0000	0000	IPv4

2. Anycast

Los paquetes son enviados a cualquier miembro de un grupo de red, de tal forma que un paquete enviado se entrega a la interfaz más cercana de acuerdo con la métrica del algoritmo de encaminamiento, estas direcciones son nuevas para el Protocolo de Internet, estas direcciones son consideradas un concepto entre las direcciones unicast y multicast.

Estas direcciones se asignan a partir del espacio de direcciones unicast utilizando cualquier tipo de formato, las direcciones anycast no tienen un formato único, lo que las hacen indistinguibles con respecto a los demás tipos de direcciones.

Cuando una dirección unicast es asignada a más de un nodo, esta dirección se convierte en una dirección anycast.

3. Multicast

Multicast es la transmisión de paquetes que se originan de un dispositivo y es recibido por múltiples destinos, el formato de las direcciones multicast se muestra en la tabla 2.8.

Tabla 2.8 Multicast

8 bits	4 bits	4 bits	112 bits
1111 1111	FLAGS	SCOPE	Multicast Group ID

El primer campo de 8 bits es el identificador de direcciones de tipo multicast y en todo el campo contiene unos.

- FLAGS (Banderas)

Este campo tiene reservados 4 bits que son usados para indicar ciertos atributos de direcciones multicast, los 3 bits más significativos están reservados y tienen el valor de cero, el último bit restante es llamado T por "transient" (transitorio) y puede tener dos valores:

0 – indica un modo permanente multicast (bien conocido).

1 – indica un modo no permanente multicast (transitorio).

- SCOPE (Alcance).

Es una serie de 4 bits que se utiliza para limitar la difusión en las redes multicast IPv6, éste puede tener los siguientes valores (Tabla 2.9):

Tabla 2.9 Scope

Valor	Alcance
0	Reservado
1	Interfaz de ámbito local
2	Enlace local
3	Subred local
4	Administrador local

5	Sitio local
6	Sin asignar
7	Sin asignar
8	Organización local
9	Sin asignar
A	Sin asignar
B	Sin asignar
C	Sin asignar
D	Sin asignar
E	Global
F	Reservado

- Multicast Group ID.

  Identifica al grupo multicast ya sea permanente o transitorio.

Por ejemplo, algunas direcciones multicast de propósito específico:

FF01::1 – todos los nodos dentro del alcance del nodo local.

FF02::1 – todos los nodos de la conexión local.

FF01::2 – todos los encaminadores dentro del alcance del nodo local.

FF02::2 – todos los encaminadores dentro del alcance de la conexión local.

FF05::2 – todos los encaminadores de un “site”

FF02::1:FFXX:XXXX – direccionamiento multicast del nodo solicitado (las X representan los últimos 24 bits de la dirección IPv6 de la dirección del nodo)

Las direcciones quedan identificadas de la siguiente manera (Tabla 2.10):

Tabla 2.10 Tipos de Direcciones

Tipo de dirección	Prefijo en binario	Notación IPv6
Sin especificar	0000…0 (128 bits)	::/128
Loopback	0000…1 (128 bits)	::1/128
Multicast	11111111	FF00::/8
Link-Local Unicast	1111111010	FE80::/10
Global Unicast	Todos los demás	

2.2.3 Extension Headers – Cabeceras de extensión

IPv6 tiene una longitud fija de cabecera logrando un procesamiento más óptimo para los dispositivos, esto se consigue eliminando campos que pocas veces se utilizaban, las cabeceras de extensión son encabezados adicionales que proveen de información extra en caso de ser necesaria sin tener que ser procesadas cuando éstas no sean menester.

Las cabeceras de extensión son la razón por la que se pudo simplificar el encabezado principal de IPv6 agregando la información necesaria en casos específicos.

Algunos ejemplos de cabeceras de extensión se observan en la tabla 2.11.

Tabla 2.11 Cabeceras de Extensión

Código	Tipo de cabecera de extensión
0	Hop-by-Hop header – Cabecera salto por salto
43	Routing header – Cabecera de encaminamiento
44	Fragmentation header – Cabecera de Fragmentos
50	Encapsulating Security Payload – Carga Útil de Seguridad Encapsulada

51	Authentication Header – Cabecera de Autenticación
59	Null – nulo
60	Destination Option Header – Cabecera Opción de Destino

El código va en el campo correspondiente al Next Header – encabezado siguiente de la cabecera principal de IPv6, sin embargo, las cabeceras de extensión pueden encadenar otras cabeceras de extensión por lo que este campo también está presente en estas cabeceras.

a) Hop-by-Hop Header – Cabecera salto por salto.

Transporta información opcional que debe ser examinada por cada nodo que se encuentre en su camino, y es usado para advertir a los routers si el paquete necesita un manejo especial, esta cabecera siempre va después de la cabecera principal.

El formato de la cabecera Hop-by-Hop es el que se muestra en la tabla 2.12

Tabla 2.12 Cabecera Hop by Hop

Siguiente Cabecera	Extensión de Longitud de la Cabecera	
Opción		

- Next Header – Siguiente Cabecera: 8 bits

El campo de siguiente cabecera identifica el tipo de cabecera que sigue inmediatamente después de la cabecera Hop-by-Hop.

- Header Extension Length – Extensión de Longitud de la Cabecera: 8 bits

Indica la longitud de la cabecera en unidades de 8 bytes, esta longitud no incluye los primeros 8 bytes.

- Option – opciones: variable

El campo de opción puede tener uno o más opciones, la longitud de este campo es variable y está determinada por el campo Header Extension Length.

El primer byte de este campo contiene información acerca de cómo debe ser procesada la opción en caso de que un nodo no la reconozca, los dos primeros bits especifican la acción que se debe realizar (Tabla 2.13)

Tabla 2.13 Significado de Bits

Bits	Significado
00	Saltar y continuar el procesamiento
01	Descartar el paquete
10	Descartar el paquete y enviar el parámetro del problema ICMP[9] código 2, envía mensaje a la dirección origen del paquete que apunta a un tipo de opción no reconocida.
11	Descartar el paquete y enviar el parámetro del problema ICMP código 2, envía mensaje a la dirección origen del paquete sólo si el destino no es una dirección multicast.

El tercer bit especifica si la información de la opción puede cambiar (valor 1) o no cambiar (valor 0) en ruta.

b) Routing Header – cabecera de encaminamiento

Se usa para dar una lista de uno o más nodos intermedios que pueden ser visitados durante el trayecto del paquete, es usado para el dispositivo de encaminamiento y Mobile IPv6 (Tabla 2.14): .

Tabla 2.14 Cabecera de encaminamiento

Cabecera Siguiente	Longitud de Extensión de la Cabecera	Tipo de encaminamiento	Segmentos Restantes
Segmentos Restantes			

[9] ICMP (Internet Control Message Protocol – Protocolo de Mensajes de Control de Internet), este protocolo sirve para informar que algún error ocurrió durante el envío de un paquete, y sólo se le informa al origen

- Next Header – Siguiente cabecera: 8 bits

El campo de siguiente cabecera identifica el tipo de cabecera que sigue inmediatamente después de la cabecera de encaminamiento.

- Header Extension Length – Longitud de Extensión de la Cabecera: 8 bits

Indica la longitud de la cabecera en unidades de 8 bytes, esta longitud no incluye los primeros 8 bytes.

- Routing Type – Tipo de encaminamiento: 8 bits

Este campo identifica el tipo de cabecera de encaminamiento.

- Segments Left – Segmentos Restantes: 8 bits

Identifica cuántos nodos restantes hay antes de que el paquete alcance su destino, si el valor de este campo es cero, el nodo debe ignorar esta cabecera y procesar la siguiente cabecera del paquete que se haya indicado.

- Type-specific Data – Tipo de datos específicos: variable

El formato de este campo está determinado por el campo de tipo de encaminamiento y de longitud tal que la cabecera de encaminamiento completa es un múltiplo de 8 bytes.

Existe una variante a la cabecera de encaminamiento llamada Type 0 (Tabla 2.15)

Tabla 2.15 Variante a la cabecera de encaminamiento Type.

Cabecera Siguiente	Longitud de Extensión de la Cabecera	Tipo de encaminamiento	Segmentos Restantes
Reservado			
Dirección[1]			
….			
Dirección [n]			

Los campos son similares a la cabecera de encaminamiento genérica, en el campo de tipo de encaminamiento tiene el valor 0 para identificar el uso de esta cabecera.

Para esta cabecera, el campo de Tipo de datos específicos consiste en un campo reservado de 32 bits y una lista de direcciones intermediarias de 128 bits y a su vez esta lista incluye a la dirección final.

c) Fragment Header – Cabecera de Fragmentos

Esta cabecera de extensión es usada cuando una dirección IPv6 necesita enviar un paquete que es más grande que el que puede permitir el MTU de la ruta a su destino, el nodo transmisor puede dividir el paquete en varios fragmentos y enviarlos en paquetes por separado, el formato de esta cabecera se muestra continuación (Tabla 2.16):

Tabla 2.16 Cabecera de Fragmentos

Cabecera Siguiente	Reservado	Fragmento de compensación	Reservado	M
Identificación				

- Next Header – Siguiente Cabecera: 8 bits

El campo de siguiente cabecera identifica el tipo de cabecera que sigue inmediatamente después de la cabecera de fragmentación.

- Reserved – Reservado: 8 bits

Este campo está inicializado a cero para la transmisión, ignorado en la recepción.

- Fragment Offset – Fragmento de compensación: 13 bits

Son los datos que siguen a esta cabecera en unidades de 8 bytes, en relación con el inicio de la fragmentación que parte del paquete original.

- Reserved – Reservado: 2 bits

Campo reservado, inicializado a cero para la transmisión, ignorado en la recepción.

- M flag – Bandera de fragmento: 1 bit

Se utilizan estas banderas para indicar si aún hay más fragmentos del paquete original, puede tener dos posibles valores:

0 – Último fragmento

1 – Más fragmentos

- Identification – identificación: 32 bits

Este campo es generado por la dirección de origen con el fin de identificar todos los paquetes que pertenecen a un paquete original en específico, este campo normalmente se implementa como un contador, con un incremento de valor uno por cada paquete.

La cabecera de fragmentación no cuenta con la bandera de No fragmentar, no es necesario ya que los encaminadores no realizan fragmentos en IPv6, sólo la dirección origen es la que puede fragmentar.

d) Encapsulating Security Payload – Carga Útil de Seguridad Encapsulada: Usado por IPSec para autenticación, confiabilidad y seguridad de los paquetes.

e) Authentication Header – Cabecera de Autenticación: Usado por IPSec para autenticación, confiabilidad y seguridad de los paquetes.

f) Null – Nulo: Sin carga útil.

g) Destination Option Header – Cabecera Opción de Destino

La cabecera de Opción de destino lleva información adicional y es procesada sólo en los nodos destino, esta información es opcional y la estructura del paquete tiene el siguiente formato (Tabla 2.17):

Tabla 2.17 Cabecera Opción de Destino

Cabecera Siguiente	Extensión Longitud de la Cabecera	
Opción		

- Next Header – Cabecera Siguiente: 8 bits

El campo de siguiente cabecera identifica el tipo de cabecera que sigue inmediatamente después de la cabecera Opción de Destino.

- Header Extension Length – Extensión Longitud de la Cabecera: 8 bits

Indica la longitud de la cabecera en unidades de 8 bytes, esta longitud no incluye los primeros 8 bytes.

- Option – opciones: variable

El campo de opción puede tener una o más opciones, la longitud de este campo es variable y está determinada por el campo Header Extension Length.

IPv6 puede contar con varias cabeceras de extensión, éstas pueden ir encadenadas una después de otra y se encuentran entre la cabecera principal y los datos del paquete (Figura 2.3).

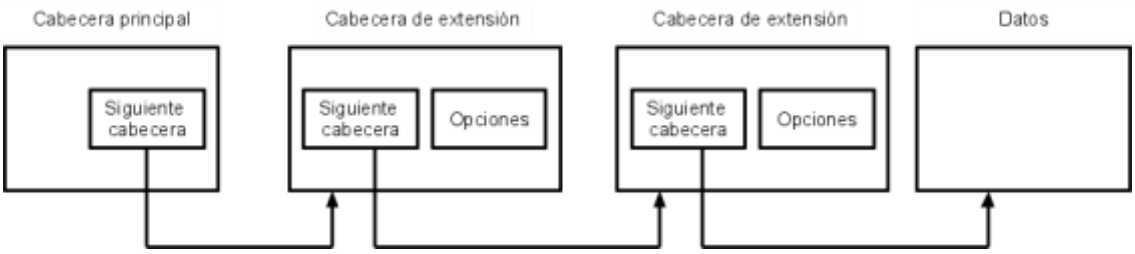

Figura 2.3 Cabeceras de Extensión

2.2.4 Cabecera IPSec

IPSec (Internet Protocol Security – Seguridad en el Protocolo de Internet) tiene como finalidad proteger paquetes IP mediante el uso de algoritmos de cifrado así como la autenticación garantizando comunicaciones privadas y seguras.

IPSec proporciona los siguientes servicios de seguridad:

1. Autenticación de datos.

   La autenticación verifica la identidad del remitente para evitar la suplantación de identidades.

2. Integridad de datos.

   La integridad de datos verifica si el contenido del paquete no ha sido modificado durante el recorrido del emisor hacia el receptor.

3. Confidencialidad de datos.

   La confidencialidad de datos sirve para que la información sea leída sólo por las entidades autorizadas, comúnmente se utilizan métodos de cifrado.

4. Protección de reproducción.

   La protección de reproducción impide que la información sea reproducida posteriormente por personas no indicadas

Para que este protocolo se pueda integrar a la tecnología de IPv6, IPSec utiliza dos cabeceras de extensión para otorgar seguridad a los paquetes, estas cabeceras definen qué operaciones se van a realizar sobre el paquete permitiendo seleccionar el algoritmo a utilizar, estas cabeceras son conocidas como Authentication Header (AH) y Encapsulating Security Payload (ESP).

a) Authentication Header – Cabecera de Autenticación

Esta cabecera proporciona integridad y seguridad contra la reproducción de la información donde se originan los datos, la finalidad de esta cabecera es principalmente la de asegurar que los datos no se hayan manipulado mientras se dirigen a su destino final, sin embargo, no ofrece confidencialidad de datos por lo que no cifra la información, la cabecera de autenticación utiliza el algoritmo HMAC[10]-MD5 así como HMAC-SHA

La cabecera de autenticación tiene la siguiente estructura interna (Tabla 2.18):

Tabla 2.18 Cabecera de Autenticación

0 – 7 bit	8 – 15 bit	16 -23 bit	24 – 31 bit
Cabecera Siguiente	Longitud de la carga útil	Reservado	
Índice de Parámetros de Seguridad			
Número de Secuencia			
Datos de autenticación (variable)			

- Next Header – Siguiente Cabecera: 8 bits

Este campo sirve para identificar qué cabecera sigue después de la cabecera de autenticación.

- Payload Length – Longitud de la carga útil: 8 bits

El campo de Longitud de la carga útil indica la longitud de la cabecera de autenticación en palabras de 32 bits (4 bytes).

- Reserved – Reservado: 16 bits

[10] HMAC (Hash-based Message Authentication Code – código de autenticación de mensajes con valores Hash), Técnica de autenticación de mensajes que se calcula usando una función de hash en combinación con una clave secreta y es usada para verificar la integridad de la información así como la autenticidad del mensaje.

Este campo está reservado para usos futuros por lo que debe tener el valor de cero, sin embargo, este valor también está incluido en el cálculo para asegurar la autenticación de los datos.

- Security Parameters Index (SPI) – Índice de Parámetros de Seguridad: 32 bits

  SPI tiene un valor arbitrario que en combinación con la dirección IP destino y el protocolo de seguridad (AH), identifica únicamente la asociación de la seguridad del paquete, el rango de valores de 1 a 255 están reservadas por la IANA para usos futuros.

- Sequence Number – Número de Secuencia: 32 bits

  Este campo contiene un número monótono siempre creciente, utilizado para evitar ataques de reproducción.

- Authentication Data – Datos de autenticación: variable

  Este campo contiene el ICV (Integrity Check Value – Valor de Comprobación de Integridad) del paquete, el campo debe tener múltiplos de 64 bits, para asegurar esta longitud se hace uso del "padding[11]".

b) Encapsulating Security Payload (ESP)– Carga Útil de Seguridad Encapsulada

Este protocolo proporciona confidencialidad de los datos y de manera opcional la autenticación, integridad y seguridad contra la reproducción de la información, a diferencia de la cabecera de autenticación, ESP ofrece cifrado de la información utilizando los algoritmos de cifrado DES, 3DES y RC4, y para la autenticación ofrecen los métodos HMAC-MD5 y HMAC-SHA.

La cabecera de ESP tiene la siguiente estructura interna (Tabla 2.19):

Tabla 2.19 Cabecera ESP

<table>
<tr><td>0 – 7 bit</td><td>8 – 15 bit</td><td>16 – 23 bit</td><td>24 – 31 bit</td></tr>
<tr><td colspan="4">Índice de Parámetros de Seguridad</td></tr>
<tr><td colspan="4">Número de Secuencia</td></tr>
<tr><td colspan="4">Carga útil de datos (variable)</td></tr>
<tr><td colspan="2"></td><td colspan="2">Relleno</td></tr>
</table>

[11] Padding – Relleno: Varios algoritmos criptográficos necesitan como entrada bloques de datos de tamaño definido, para completar el tamaño de dichos datos se utiliza este campo de relleno.

	Longitud del Relleno	Cabecera Siguiente
Datos de Autenticación (Variable)		

- Security Parameters Index (SPI) – Índice de Parámetros de Seguridad: 32 bits

  SPI tiene un valor arbitrario que en combinación con la dirección IP destino y el protocolo de seguridad (ESP), identifica únicamente la asociación de la seguridad del paquete, el rango de valores de 1 a 255 están reservadas por la IANA para usos futuros.

- Sequence Number – Número de Secuencia: 32 bits

  Este campo contiene un número monótono siempre creciente, utilizado para evitar ataques de reproducción.

- Payload Data – Carga útil de datos: variable

  La carga útil de datos que contiene los datos descritos por el campo de la siguiente cabecera, este campo es obligatorio.

- Padding – Relleno (usado por el cifrado):

  Cuando se realiza el cifrado de datos mediante el uso de algún algoritmo de cifrado, se requiere tener un bloque de cifrado con un tamaño específico, en caso de necesitar algún relleno se utiliza este campo.

  El relleno también es utilizado independientemente del cifrado de datos, se usa para garantizar que el texto cifrado contenga una longitud de 4 bytes.

- Pad Length – Longitud del Relleno: 8 bits

  Indica la longitud del relleno en bytes, el rango válido de valores son de 0 a 255, en caso de haber cero indica que no hubo relleno, este campo es obligatorio.

- Next Header – Siguiente Cabecera: 8 bits

  Este campo sirve para identificar qué cabecera sigue después de la cabecera ESP.

- Authentication Data – Datos de Autenticación: variable

  Este campo contiene el ICV del paquete, está calculado sobre el paquete ESP menos los datos de autenticación, este campo es opcional y es incluido sólo si el servicio de

autenticación ha sido seleccionado, el algoritmo de autenticación indica la longitud del ICV así como las reglas de comparación y el procesos de la validación

Existen dos modos de funcionamiento del protocolo IPsec

a) Transporte: La cabecera IP se mantiene como fue creada originalmente, por lo que sólo los datos son los que se cifran o se autentican, y la información de la cabecera no pasa ninguno de estos métodos de seguridad por lo que queda intacta.

La cabecera AH en modo transporte (Tabla 2.20):

Tabla 2. 20 Cabecera AH

Cabecera IP	Cabecera de Autenticación (AH)	Cabecera TCP/UDP	Datos nivel aplicación

El formato de la cabecera ESP en modo transporte (Tabla 2.21)::

Tabla 2. 21 Cabecera ESP en modo transporte

Cabecera IP	Cabecera ESP	Cabecera TCP/UDP	Datos nivel aplicación	Cola ESP	Autenticación ESP

b) Túnel: Todo el paquete IP incluyendo los datos y la cabecera se cifran o se autentican, por lo que crea una nueva cabecera IP y la utiliza como si fuera la cabecera principal, encapsulando el paquete original.

La estructura del paquete en la cabecera AH en modo túnel es (Tabla 2.22)::

Tabla 2. 22 Estructura del paquete en la cabecera AH en modo túnel

Cabecera IP	Cabecera AH	Datos

La cabecera ESP en modo túnel queda de la siguiente manera (Tabla 2.23):

Tabla 2. 23 Cabecera ESP en modo túnel

Cabecera IP	Cabecera ESP	Datos	Cola ESP	Autenticación ESP

2.3 Soluciones a la transición IPv6

El proceso de adopción de IPv6 reiniciará la competencia por obtener el liderazgo tecnológico y la innovación en los negocios, además para los gobiernos permitirá tener un mejor manejo de las ICT (information and communications technology – tecnologías de la comunicación y la información). En un mundo en donde los negocios son muy recompensados por el poder de las ICT, es natural tener estrategias desarrolladas para poder tratar con la actualización del protocolo IPv6.

La revolución de las ICT es un fenómeno joven relativamente, los negocios han empezado a ver el regreso de sus inversiones creadas a finales de los noventa. En muchos países, las inversiones de las ICT dieron como resultado un incremento en la productividad y acceso a mercados nuevos de manera remota.

En algunos países, el desarrollo de la industria ICT ha empezado a ser un contribuyente significativo del GDP (gross domestic product – producto doméstico bruto) que es la capacidad de gasto de los hogares, como Internet ya es parte de nuestras vidas, su valor económico ha empezado a ser incalculable.

A pesar de su corta historia, la revolución ICT y su catalizador IP han mostrado mensajes importantes a los gobiernos alrededor del mundo. La infraestructura ICT está conformada por:

- **Estrategias locales:** Son las organizaciones gubernamentales y de negocios relacionadas con las ICT.
- **Estrategias Globales:** Las ICT son esenciales para la integración de un mercado global.
- **Liderazgo e innovación:** La economía se beneficia significativamente del liderazgo en la industria de las ICT, un ejemplo claro son los Estados Unidos.

Sin lugar a duda los asuntos involucrados con los recursos limitados de IPv4 lógicamente han incrementado el interés en IPv6. En mayo de 2007, ARIN (the American Registry for Internet Numbers – El registro Americano para los números de Internet) dio aviso a la comunidad de Internet acerca de la imperiosa necesidad de migrar a IPv6.

Todos los RIR (Regional Internet Registries – registros regionales de Internet), han coordinado sus esfuerzos para asegurarse de promover un plan global de actualización del protocolo IP. Estos esfuerzos incluyen: [F]

- **Sincronización global:** Los 5 RIR procederán al mismo tiempo para tomar medidas relacionadas con la extinción de direcciones IP.

- **Un anuncio de la fecha de extinción de las direcciones IPv4:** El objetivo es establecer una fecha en la que los RIR dejen de proveer direcciones IPv4.

- **Prometer no hacer políticas muy estrictas para las direcciones IPv4 restantes:** Es importante mantener una provisión de direcciones IPv4.

- **Problemas relacionados con el reciclaje de las IPv4:** Los asuntos relacionados con las direcciones no utilizadas o su reciclaje deben ser discutidas de forma separada.

Las implicaciones económicas de la migración son objeto de una reciente iniciativa de la OECD (Organization for Economic Co-operation and Development- Organización para la co-operación y desarrollo económico), para crear un proyecto que establezca los puntos más importantes de coordinación, estrategia y esfuerzos para la integración de IPv6 lo más pronto posible [G]. La actualización del protocolo representa una oportunidad para las economías emergentes como la de México porque existe la oportunidad de integrarse profundamente en los negocios de las ICT que al haber aprendido que IPv4 fue un parte aguas en este tipo de negocios.

Las perspectivas nacionales sobre IPv6 varían dependiendo del alcance y la profundidad. Estas estrategias que surgieron entre el año 2000 y el 2007 pueden ser agrupadas en tres categorías.

- **Manejar la adopción del nuevo protocolo mediante mandatos gubernamentales:** Un mandato de gobierno junto con sus agencias relacionadas a las ICT que maneje la adopción de IPv6.

- **Patrocinio de la adopción:** Implementando políticas fiscales y legislativas que encaminen y faciliten la adopción de IPv6.

- **Patrocinio para Investigación Nacional:** Encaminar y fundar actividades de investigación que simulen el desarrollo e innovación para saber cómo utilizar el protocolo.

A continuación se describirán las acciones que han tomado algunos de los países con un crecimiento económico importante de los últimos años y su papel en la transición del protocolo IPv6.

1. Japón

El gobierno de Japón fue uno de los primeros en reconocer la importancia de las ICT y particularmente el acceso a las infraestructuras IP. El discurso dado por el primer ministro Yoshiro Mori ante el parlamento japonés el 21 de septiembre del 2000 habló del camino que el país debía seguir para estar posicionado en los primeros lugares económica y

socialmente. El primer ministro identificó "La revolución de las ICT es un movimiento nacional y es el más importante pilar para el renacimiento de Japón".

Las acciones del gobierno fueron rápidas. El ministro de asuntos interiores y comunicaciones detalló su visión y planes en el "e-Japan Policy Program" realizado el 29 de marzo del 2001. En donde el punto principal fue el desarrollo de una infraestructura de ancho de banda y acceso IP, los puntos importantes que esta política promueve son los siguientes:

- **Iniciativas Financieras:** Tomar un periodo de adopción de 2 años. Los proveedores de servicios serán beneficiados con reducciones de impuestos en la compra de productos que permitan utilizar el protocolo IPv6. Estas iniciativas favorecen a los ISP para desarrollar servicios basados en IPv6.

- **Patrocinio de una migración integral:** El propósito es promocionar la tecnología y aprender de esas experiencias. Algunos de los proyectos fueron: servicios de consultoría para residentes(Taito, Tokio), servicios de video en vía "streaming live" (como los videos de youtube) (Taito, Tokio), servicio de cuidados a la salud para el hogar (Asahikawa, Hokkaido), soluciones de seguridad multi servicios sobre IPv6 en escuelas (Tokio), los resultados de las lecciones aprendidas de los proyectos pueden ser consultadas en el MIC Communications News newsletter el 20 de octubre del 2005. [H]

- **Establecer un reconocimiento internacional del desarrollo de la migración en otros países:** Se busca hacer acuerdos internacionales que permitan facilitar la adopción del protocolo sobre todo con China e India.

- **Un fondo de investigación que promueva el desarrollo y uso de IPv6**: Japón ha invertido de 10 a 13 millones de dólares en investigación al año.

2. Corea del Sur

La estrategia de Corea del Sur tiene muchas similitudes con la de Japón. Corea ha especificado la importancia de los efectos positivos de las ICT en la economía Coreana, incluyendo exportaciones y excedentes industriales. El gobierno ha hecho énfasis en la importancia de las ICT y activamente ha dado soporte al desarrollo de una infraestructura IP. El MIC (Ministry of Information and Communications – Ministerio de Comunicaciones e Información) dio a conocer las estrategias IT839 en 2003 que se enfocan en los servicios, infraestructura y productos de tecnología relacionados con IPv6.

3. Unión Europea

La Unión Europea publicó un documento a inicios del 2001 en el que establece que IPv4 está sofocando su crecimiento económico. La Unión Europea mantiene el liderazgo en tecnologías móviles GSM y su desarrollo, pero está por debajo del desarrollo de las ICT en los Estados Unidos particularmente en el área de las comunicaciones IP. Esto se debe al hecho de que en Estados Unidos se han realizado contribuciones significativas para el desarrollo de IPv4. IPv6 por sí mismo en combinación con tecnologías móviles es una importante oportunidad para tomar el liderazgo en las ICT para la Unión Europea.

Se han empezado a hacer proyectos de investigación que promuevan el protocolo IPv6. El proyecto U-2010 proveerá la integración de recursos de respuesta a emergencias para una mejor y más rápida resolución ante incidentes, esta infraestructura está basada en IPv6. El proyecto 6DISS establece a la Unión Europea con un centro de diseminación de IPv6 acumulando la experiencia a través de varios proyectos, principalmente 6NET. La Unión Europea es líder de muchas tecnologías de comunicación pero no ha hecho los mismos meritos para ser líder en el Protocolo de Internet. IPv6 ofrece una oportunidad única para obtener el liderazgo en la tecnología IP.

4. China

La rápida adopción de Internet, el acelerado crecimiento y la modernización de la economía hace del direccionamiento IP un recurso estratégico para China. IPv6 es una solución natural, aunque su principal problema no es el direccionamiento IPv6, las compañías chinas reciben su direccionamiento de APNIC. El gobierno chino ve la adopción de IPv6 con una oportunidad de tomar un papel de liderazgo en temas de tecnología y gobierno en el nuevo Internet. Es visto como una oportunidad de desarrollar una industria de las ICT.

Aunque el gobierno patrocinó la investigación de IPv6 por un largo tiempo, el primer gran paso se dio con la implementación de una estrategia nacional sobre IPv6 que fue lanzada como CNGI (China Next Generation Internet) en noviembre del 2003. El gobierno invirtió alrededor de 170 millones de dólares en el proyecto, el cual involucra a las 5 más grandes empresas (China Telecom, China Unicom, China Netcom/CSTNET, China Mobile, China RailCom). La red principal fue completada en 2005 y un panel de expertos la certificó en Septiembre del 2006, como el mayor logro estratégico. [I]

El anuncio público de este logro puso un pequeño énfasis en la viabilidad de utilizar direccionamiento IPv6. Además, el punto más importante es que fue la primera estructura en el mundo que fue construida con routers domésticos y que usó tecnologías desarrolladas en China.

CNGI se materializó como el primer paso de la estrategia de gobierno para construir una base de información nacional basada en una infraestructura IPv6. También está ayudando a

promover un ambiente de implementación relacionado con políticas de IPv6. La red CNGI fue la principal plataforma para los juegos olímpicos de Beijing en el 2008.

5. India

Siendo similar a la infraestructura de otras economías asiáticas, la infraestructura de India requiere de recursos significativos. Hay muchos temas por tratar de interés estratégico sobre IPv6. Una porción significativa de los GDP viene de la capacidad de ofrecer servicios remotamente a otros mercados. La interconexión IP debe ser mantenida a pesar de la versión de IP preferida por los clientes. Aunque el porcentaje de población con acceso a Internet doméstico es pequeño y los puntos de acceso comunes tales como un café Internet y teléfonos móviles se están esparciendo rápidamente. Para dar soporte al rápido crecimiento de las infraestructuras que están basadas en servicios IP, India requerirá de recursos de direccionamiento IPv6.

La importancia de IPv6 fue reconocida a nivel gubernamental en Agosto de 2005 en un documento creado por la TRAI (Telecom Regulatory Authority of India). Ésta provee recomendaciones para la integración y migración de IPv6. En noviembre de 2006, este documento fue seguido con el propósito de establecer un patrocinio gubernamental para conformar un ambiente de pruebas en la TEC (Telecommunication Enginnering Center). Este ambiente está encargado de certificar la disposición de IPv6 en acuerdo con las recomendaciones del TRAI. TEC es parte del Departamento de Telecomunicaciones y su función es la de especificar estándares comunes para equipo de telecomunicaciones, identificar requerimientos genéricos y de interfaz, aprobaciones de servicios, formular estándares e interactuar con agencias internacionales multilaterales para la integración internacional.

Capítulo 3

Mecanismos de Transición

IPv6 se encuentra en funcionamiento en varias partes del mundo, la migración total a este protocolo será un largo proceso por lo que en la etapa de transición ambas tecnologías tendrán que convivir, para esto, se han definido varias técnicas que ya están implementadas en los nuevos dispositivos que son capaces de comunicarse usando ambos protocolos dentro de una misma infraestructura.

Una transición de protocolos usualmente se instala y se configura en cada uno de los dispositivos que hay dentro de una infraestructura de una red y se verifica si está trabajando correctamente, sin embargo, la transición de IPv4 a IPv6 no es sencilla ya que no consiste en sólo una actualización o una configuración, se debe tener en cuenta que en algunos casos se necesita cambiar la infraestructura de la red considerando los dispositivos que aún no son capaces de procesar el nuevo protocolo.

Por lo tanto, ambos protocolos estarán conviviendo por un tiempo antes de que se despliegue por completo IPv6, por lo que se han ideado mecanismos para que ambos protocolos puedan coexistir.

Dentro de una infraestructura se han definido las capacidades de los dispositivos para procesar las direcciones:

- IPv4-only node: El nodo sólo puede procesar direcciones IPv4
- IPv6-only node: El nodo sólo puede procesar direcciones IPv6
- IPv6/IPv4 node: El nodo puede procesar ambos protocolos
- IPv4 node: cualquier dispositivo que tenga implementado IPv4
- IPv6 node: Cualquier dispositivo que tenga implementado IPv6

Para la coexistencia de ambos protocolos dentro de una infraestructura IPv4 se han definido básicamente tres mecanismos:

- El diseño de una arquitectura para el uso de ambos protocolos simultáneamente.
- Túneles para el envío de paquetes
- Mecanismos de traducción de direcciones

3.1 Utilizando ambos protocolos (IPv4 e IPv6)

Durante la transición del IPv4 a IPv6 existirán 3 etapas, la primera que es el uso único de IPv4, la convivencia de IPv4 e IPv6 debido a que no es una transición simple y el periodo final cuando sólo se use el protocolo IPv6. Por ejemplo, en el momento de la transición, algunos servidores que proporcionen algún servicio tendrán que operar con IPv6, pero otros servicios que no han sido actualizados para soportar ambos protocolos solamente utilizan IPv4, entonces los hosts deben tener la habilidad de utilizar ambos protocolos, para poder hacer esto, se utilizan ambas capas de internet en el mismo nodo, los nodos IPv4/IPv6 pueden tener las siguientes arquitecturas: [DAVIES 2008]

a) Arquitectura de capa dual IP.

b) Arquitectura de pila dual.

a) Arquitectura de capa dual IP

Una arquitectura de capa dual IP contiene ambas capas de internet (IPv4 e IPv6) con una simple implementación en los protocolos de las capas de transporte como TCP y UDP, la siguiente figura muestra la arquitectura dual. (Figura 3.1).

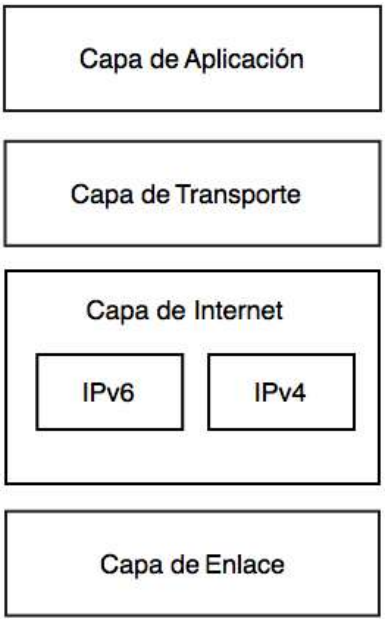

Figura 3.1 Arquitectura dual.

Cuando un nodo se encuentra equipado para soportar ambos protocolos, una u otra pila debe ser deshabilitada para poder operar. Por esta razón los nodos IPv6/IPv4 deben operar en los siguientes 3 modos: [Ct]

- Con la pila IPv4 habilitada y la pila IPv6 deshabilitada.
- Con la pila IPv6 habilitada y la pila IPv4 deshabilitada.
- Con ambas pilas habilitadas.

Los nodos IPv4/IPv6 con pila IPv6 deshabilitada operarán solamente como nodos IPv4, de manera similar los nodos IPv4/IPv6 con pila IPv4 deshabilitada operarán como nodos IPv6. Además los nodos IPv4/IPv6 deben proveer una configuración que permita habilitar o deshabilitar cada pila.

El protocolo TCP/IP en Windows Server 2008 y en Windows Vista incluye IPv4 e IPv6 en una arquitectura capa dual IP en un simple driver (Tcpip.sys) que contiene las implementaciones de ambos. Un nodo en Windows Server o Windows Vista puede crear los siguientes tipos de paquetes: [DAVIES 2008] (Figura 3.2).

- Paquetes IPv4
- Paquetes IPv6
- Paquetes IPv6 over IPv4 (paquetes IPv6 a través de IPv4).

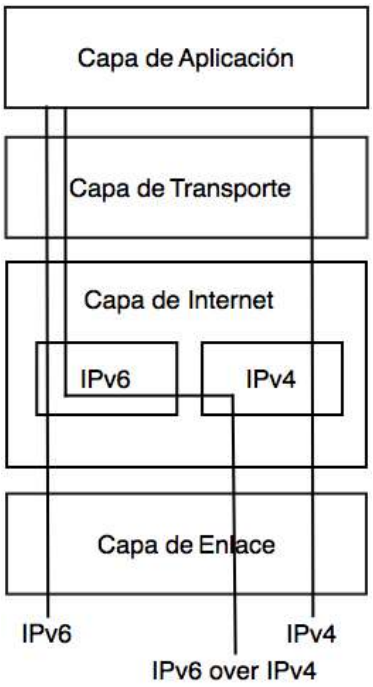

Figura 3.2 Paquetes en una arquitectura dual

b) Arquitectura de pila dual.

La arquitectura de pila dual contiene ambos protocolos en la capa de Internet, sin embargo, a diferencia de la arquitectura capa dual IP, esta arquitectura contiene por separado los datos, es decir, tiene un bloque donde se encuentra la capa Internet y la capa de transporte para cada protocolo (Figura 3.3).

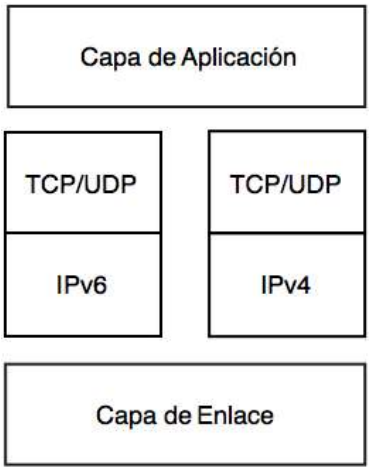

Figura 3.3 Arquitectura de pila dual

Windows Server 2003 y Windows XP tienen una arquitectura dual. El controlador (driver), Tcpip.sys, contiene los protocolos IPv4, TCP y UDP, entre otros protocolos. El controlador, Tcpip6.sys, contiene el protocolo IPv6 e implementaciones por separado de TCP y UDP. Con ambas pilas de protocolos instaladas se pueden crear los siguientes tipos de paquetes: (Figura 3.4).

- Paquetes IPv4
- Paquetes IPv6
- Paquetes IPv6 over IPv4

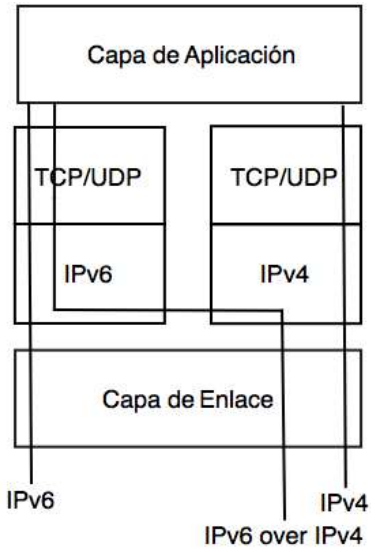

Figura 3.4 Arquitectura de pila dual

La técnica de la pila dual tiene la desventaja de requerir una actualización completa del software de red para poder ejecutar las dos versiones del protocolo. Esto quiere decir que se debe mantener la configuración y todas las tablas dualizadas. Desde el punto de vista de un administrador de red, significa que se deben utilizar comandos separados para las mismas funciones dependiendo del protocolo, por ejemplo ping.exe para IPv4 y ping6.exe para IPv6 en un dispositivo con sistema operativo de Microsoft con distintos parámetros para cada comando. También requerirá más capacidad de cómputo y memoria para conseguir el mismo rendimiento que en una red que maneje un solo protocolo.

3.2 Túneles

Los túneles son otra de las técnicas de migración hacia la red IPv6, para que un paquete IPv6 pueda ser transmitido en una red IPv4, este paquete debe ser tratado conforme al protocolo que utiliza la infraestructura, se ha ideado la manera de hacer pasar paquetes IPv6 por paquetes IPv4, a este proceso se le conoce como Encapsulado.

Existen dos tipos de túneles:

a) Túnel configurado manualmente:

> Este tipo de túneles se usa para aislar segmentos de red, enlaza a dos dominios IPv6 mediante una red con una infraestructura IPv4, en este tipo de túneles las direcciones se deben asignar manualmente, esta configuración se utiliza en las configuraciones Router – Router y Host – Router, un router es una entidad de una red que habitualmente tiene una dirección fija ya que resuelve direcciones además de segmentar la red, en un túnel el router actúa como punto terminal de éste.

b) Túnel automático:

Estos túneles permiten que se puedan comunicar nodos IPv4/IPv6 sobre una infraestructura IPv4 sin tener túneles preconfigurados, esta configuración emplea direcciones IPv6 compatibles con IPv4, estas direcciones tienen el siguiente formato (Tabla 3.1):

Tabla 3.1 Dirección IPv6 compatible IPv4

80 bits	16 bits	32 bits
0000 …. 0000	0000	IPv4

Esta dirección es asignada exclusivamente a nodos que soportan el túnel automático, se emplea comúnmente a las configuraciones Host – Host y Router – Host.

Como la dirección destino es un nodo que forma parte del extremo de una red, puede asignarse una dirección dinámica, es decir, cada vez que se integre a una infraestructura de red se le asignará una dirección que se encuentre disponible, este concepto entra en el funcionamiento de un túnel automático.

3.2.1 Configuraciones de los túneles

Un paquete puede tomar distintos caminos según se tengan configuradas las topologías donde se implementen los túneles.

Los caminos que puede tomar un paquete dentro de un túnel son los siguientes:

- Router – Router
- Host – Router
- Router – Host
- Host – Host

a) Router – Router

En esta configuración se encuentran dos routers o encaminadores que pueden procesar direcciones IPv4/IPv6, estos dispositivos están interconectados dentro de una

infraestructura IPv4, La extensión de este túnel se interpreta como un salto en el camino entre la fuente y el destino. (Figura 3.5).

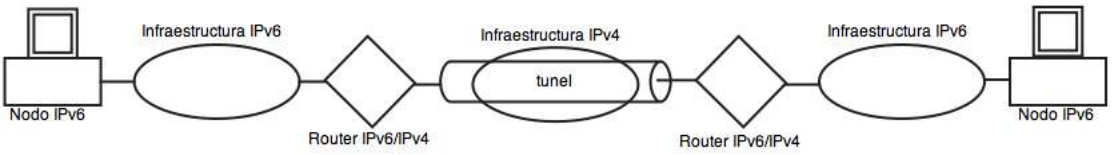

Figura 3.5 Configuración Router - Router

b) Host – Router

Esta configuración está determinada por un nodo IPv4/IPv6 conectado con un encaminador IPv4/IPv6 que se encuentra dentro de una infraestructura IPv4, el router encapsulará al paquete origen en un paquete compatible para la infraestructura, el túnel se extiende por el primer segmento del camino del paquete. (Figura 3.6).

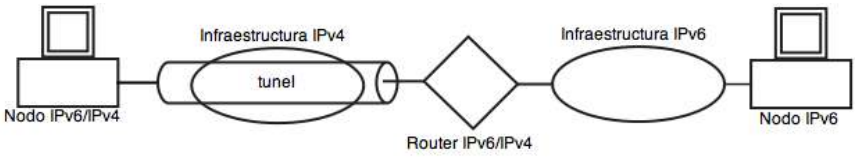

Figura 3.6 Configuración Host - Router

c) Router – Host

En esta configuración se encuentra un encaminador IPv4/IPv6 conectado hacia un nodo IPv4/IPv6, éste es la salida del túnel donde el paquete se le retira el encapsulado y se le envía al nodo como un paquete IPv6, el túnel se extiende por él como el segundo segmento del paquete. (Figura 3.7).

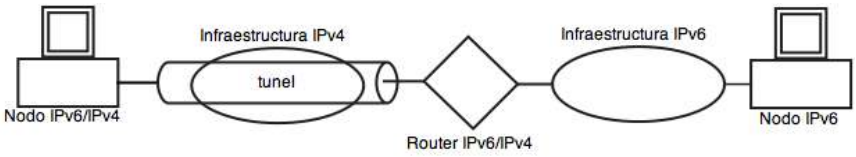

Figura 3.7 Configuración Router - Host

d) Host – Host

Dos nodos IPv4/IPv6 se encuentran interconectados en una infraestructura IPv4, los paquetes se pueden enviar mediante un túnel entre los dos nodos, el túnel se extiende por todo el camino que el paquete toma para llegar a su destino. (Figura 3.8).

Figura 3.8 Configuración Host - Host

3.2.2 Encapsulado

El encapsulado ayuda a que en una red que está configurada en su totalidad mediante IPv4 puedan trabajar nodos con tecnología IPv6, el emisor y receptor deben soportar ambos protocolos, aunque los nodos intermedios funcionen sólo con tecnología IPv4.

Sin embargo, la cabecera IPv6 seguirá siendo procesada de acuerdo con las reglas de este protocolo, si presenta cabeceras de extensión, éstas serán procesadas de igual manera, el proceso de Encapsulado necesita 20 bytes que deben ser considerados en el MTU para realizar esta operación.

Los pasos que realiza para encapsular un paquete IPv6 son los siguientes:

En el punto de inicio del túnel se decrementa en una unidad el campo de límite de saltos (Hop Limit), el paquete se encapsula en la cabecera IPv4 y se transmite, en caso de ser necesario el paquete se fragmenta, cuando el paquete llega a la salida del túnel se reensambla si se requiere, se remueve la cabecera IPv4 y se procesa el paquete IPv6 original. (Figura 3.9).

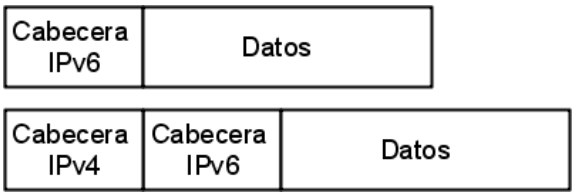

Figura 3.9 Encapsulado IPv6

Los campos de IPv4 cuando encapsulan un paquete IPv6 se le asignan los siguientes valores: [Ct]

a) Versión: 4

b) Longitud de la cabecera: 5 (en palabras de 32 bits)

c) Tipo de servicio: 0

d) Longitud total: En este campo se indica la longitud que tienen las cabeceras IPv4 agregando la cabecera IPv6 así como la longitud de su carga útil.

e) Identificación: Este campo es generado para transmitir el paquete IPv4.

f) Flags: Indica si el paquete debe ser fragmentado.

g) Fragment Offset: Se utiliza en caso de que el paquete sea fragmentado.

h) TTL: El valor de este campo depende de la implementación que se use.

i) Protocolo: 41 (asignación de número para el tipo de carga útil de IPv6).

j) Suma de control de la cabecera: Sólo se calcula la suma de control de la cabecera IPv4.

k) Dirección origen: Dirección IPv4 de la interfaz donde se encapsula el paquete.

l) Dirección destino: Dirección IPv4 del punto de salida del túnel.

En el proceso de obtención del paquete IPv6, el nodo debe ser capaz de reensamblar paquetes IPv4 con un tamaño de 1300 bytes (1280 bytes del paquete y 20 bytes de la cabecera IPv4), como parte de este proceso el nodo debe descartar los paquetes que contengan direcciones origen IPv4 inválidas, como lo son las direcciones multicast, broadcast así como las direcciones de diagnóstico, al obtener el paquete IPv6 el nodo vuelve a descartar paquetes con las mismas características con las que fueron descartados las direcciones IPv4 inválidas.

3.3 Mecanismo de traducción de direcciones

a) Infraestructura DNS

En 1995, el RFC 1886 [Cd] describió un método directo y efectivo para publicar información IPv6 en el sistema DNS que proporcionaba una vía sencilla de actualización. Sin embargo, en el año 2000, se publicó una forma más ambiciosa para hacer lo mismo en el RFC 2874 [Ce]. Este nuevo mecanismo sólo fue implementado parcialmente y la práctica mostró que quizás ésta última propuesta resultaba demasiado ambiciosa, por lo que en 2001, IETF empezó a reconsiderar el anterior RFC 1886 con algunas modificaciones menores, aunque no por ello de poca importancia, que permitió publicar RFC 3596 [Cf].

En IPv4 las direcciones se almacenan en registros A (address - direcciones) y la correspondencia inversa se realiza creando un nombre de dominio especial que consiste en valores de los bytes individuales de la dirección en orden inverso, seguidos por in-

addr.arpa. Al buscar un nombre de dominio de este tipo resulta en un registro PTR (pointer – indicador) que contiene el nombre asociado con la dirección en cuestión. El punto después del nombre de dominio indica que se trata de un FQDN (Full Qualified Domain Name – Nombre de Dominio Totalmente Calificado) y que no existen nombres de dominios de nivel superior que se le puedan añadir a la derecha.

Por ejemplo:

www.unam.mx. IN A 192.0.2.17

17.2.0.192.in-addr.arpa IN PTR www.unam.mx

De forma similar a IPv4, las direcciones IPv6 se almacenan en registros AAAA. Este tipo de registro se denomina AAAA porque las direcciones de IPv6 son de 128 bits, cuatro veces la longitud de las direcciones IPv4 de 32 bits. La correspondencia inversa (resolver el nombre a partir de la dirección) se lleva a cabo tomando los dígitos hexadecimales de la dirección IPv6 (todos ellos, incluidos los ceros que en otras circunstancias se omiten) en orden inverso y añadiendo ip6.int. El uso de ip6.int quedó obsoleto a favor del dominio ip6.arpa en el RFC 3152 [Cg] y que culminó finalmente en el RFC 3596 [Cf] (año 2003) que estandariza el uso de los registros AAAA y la resolución inversa bajo ipv6.arpa. El término arpa fue usado inicialmente como una alusión de la antigua ARPANET pero más tarde vino a significar en este contexto "Address and Routing Parameter Area"

Por ejemplo:

www.unam.mx. IN AAAA 2001:db8:1bff:c001:390

0.9.3.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.c.f.f.b.1.8.b.d.0.1.0.0.2.ip6.arpa IN PTR www.unam.mx

Se usa el protocolo DNS con ambas versiones para resolver los nombres y direcciones IP. Un nodo IPv6/IPv4 necesita un DNS que es capaz de resolver ambos tipos de registros de dirección DNS. El registro DNS A se utiliza para resolver direcciones IPv4 y el registro DNS AAAA se utiliza para resolver direcciones IPv6. En algunos casos, el DNS devuelve sólo una dirección IPv4 o una dirección IPv6. Si el host a resolver es dual, el DNS podría resolver ambos tipos de direcciones. Es de esperar, en este caso, que tanto el DNS que resuelve como la aplicación que usa el DNS tengan opciones de configuración para poder especificar órdenes de prioridad o filtros. Generalmente las aplicaciones que corren en nodos con implementación de doble pila necesitan mecanismos para determinar si se está estableciendo comunicación con un par IPv6 o un par IPv4.

b) Infraestructura DHCP

DHCPv6 (RFC 3315) [Cu] es la versión IPv6 de DHCP (Dynamic Host Configuration Protocol – Protocolo de Configuración Dinamica de Host). El mecanismo para usar DHCP

bajo una implementación de pila dual, consiste en que cada versión del protocolo IP utilice su propia versión de DHCP, ejecutándose en el mismo nodo físico. De forma más clara para poder obtener una dirección IPv4 se utiliza DHCPv4 y para obtener una dirección IPv6 se usará DHCPv6. Ambas versiones son similares, pero tiene diferencias importantes que surgen en la manera de usar el protocolo. DHCP tiene tres propósitos fundamentales:

- La configuración de direcciones: proporciona direcciones a los hosts individuales.
- Configuración no referida a direcciones: proporciona otra información de configuración, como direcciones de resoluciones DNS y listas de búsqueda de dominios.
- Delegación de prefijos: proporciona prefijos enteros a los routers (RFC 3633) [Ch.].

Por ejemplo:

Un cliente que esté interesado en una dirección y/o información de configuración envía un mensaje solicitando sus necesidades a la dirección multicast de enlace local FF02::1:2, puerto 547 (los mensajes son enviados del servidor al cliente mediante el puerto 546). Los servidores DHCPv6 que reciban el mensaje de solicitud pueden responder directamente o delegar la solicitud en otro servidor de su elección.

Cuando el mensaje finalmente está disponible, un mensaje de respuesta es enviado con la dirección y/o la información de configuración solicitada. Como era de suponer, las direcciones IPv6 asignadas con DHCPv6 disponen de un tiempo de vida válido. En algún momento antes de que el límite temporal expire, el cliente envía un mensaje de renovación preguntando al servidor si puede continuar usando esa dirección. Cuando el cliente deja de utilizar la dirección envía un mensaje para que sea liberada y pueda ser reasignada a otro nodo.

Para que los servidores puedan reconocer a los clientes, cada dispositivo que implementa DHCPv6 tiene un DHCP Unique Identifier (DUID- DHCP Identificador Único). En IPv4 el cliente DHCP usa una dirección MAC o una cadena suministrada por el usuario como identificador del cliente. En DHCPv6 éste es siempre el DUID. Los dispositivos pueden crear sus DUID de varias formas, en tanto que éstas deben ser únicas. Los Routers Cisco, por ejemplo, crean sus DUID basándose en la dirección MAC más pequeña del sistema.

DHCPv6 también soporta mecanismos de autenticación que permiten que clientes y servidores interactúen de forma segura, de modo que terceras partes no puedan inyectar mensajes DHCP falsos o modificar los mensajes legítimos intercambiados.

Lamentablemente, este mecanismo debe ser pre configurado manualmente en todos los servidores y clientes, anulando las ventajas de autoconfiguración de IPv6.

Capítulo 4

Tecnologías de Transición

Los Mecanismos de Transición están hechos para que poder utilizar ambos protocolos (IPv4/IPv6) en redes IPv4, encapsulando paquetes IPv6 en IPv4, todos estos mecanismo son túneles con diferentes técnicas de implementación y que en cierta medida están pensados para utilizarse para necesidades diferentes, una característica importante es que también pueden ayudar a conectarse con diferentes redes nativas IPv6 y así poder conectar las "islas" IPv6 en este océano IPv4.

4.1 ISATAP

ISATAP (Intrasite Automatic Tunnel Addressing – Direccionamiento Interno de Túnel Automático) permite la asignación de direcciones y es una tecnología de túnel automático host-to-host, host-to-router y router–to-host definida en el RFC 4214 [Hi] que emplea la conectividad IPv6 unicast entre un host IPv6/IPv4 a través de una red IPv4. Un host ISATAP no requiere de ningún tipo de configuración manual y se pueden crear direcciones ISATAP usando los mecanismos de autoconfiguración estándar para IPv6.

Las direcciones ISATAP tienen uno de los dos siguientes formatos (Figura 4.1):

- 64-bits Prefijo Unicast:0:5EFE:w.x.y.z
- 64-bits Prefijo Unicast:200:5EFE:w.x.y.z

64 bits	64 bits	
Prefijo ISATAP	0000:5EFE	Dirección IPv4

Figura 4.1 Formato de direcciones ISATAP

Una dirección ISATAP contiene un prefijo unicast de 64 bits, éste es cualquier prefijo de dirección unicast de 64 bits, incluyendo un enlace local, global y prefijos locales únicos.

Las Direcciones ::0:5EFE:w.x.y.z y ::200:5EFE: w.x.y.z son identificadores de interfaz administrados localmente. La dirección ::0:5EFE:w.x.y.z es una dirección IPv4 privada unicast. La dirección ::200:5EFE:w.x.y.z, w.x.y.z es una dirección IPv4 unicast pública. La parte de identificador de interface (ID) de una dirección ISATAP contiene una dirección IPv4 embebida que determina el destino de la dirección IPv4 en el encapsulado del encabezado IPv4 del tráfico ISATAP.

Existe una idea errónea muy común en donde se establece que antes de empezar a experimentar con la conectividad IPv6 y una aplicación de migración, se debe configurar una dirección IPv6 nativa y de ruteo, la cual requiere de un análisis detallado de esquemas de direccionamiento IPv6, actualizaciones de ruteo y configuración. ISATAP permite cambiar la parte de "sólo IPv4" de una red a una subred IPv6 lógica. Una vez que esta subred es definida y asignada a un prefijo global o único, un host IPv6/IPv4 que soporta ISATAP puede usar direcciones basadas en ISATAP para una conectividad IPv6. ISATAP

permite que una red interna que sólo maneja IPv4 sea capaz de soportar IPv6, sin modificaciones y requerimientos nuevos para la infraestructura de ruteo existente.

ISATAP permite escalar a un direccionamiento IPv6 nativo y de capacidad de ruteo en una red interna de la siguiente manera:

- Etapa 1 Red interna "sólo IPv4". En esta etapa toda la red interna puede ser una subred ISATAP lógica.

- Etapa 2 Red interna "sólo IPv4" pero con porciones de capacidad para soportar IPv6. En esta etapa la red interna tiene una parte de "sólo IPv4" (la subred lógica ISATAP) y una parte compatible con IPv6. La parte con capacidad para soportar IPv6 de la red interna ha sido actualizada para soportar direccionamiento y ruteo IPv6.

- Etapa 3 Subred con capacidad IPv6. En esta etapa toda la red interna es capaz de soportar IPv4, direccionamiento y ruteo IPv6 nativo además de que ya no es necesario utilizar ISATAP.

Con ISATAP se puede tener conectividad IPv6 entre hosts y aplicaciones durante las primeras dos fases de la transición desde una red "sólo IPv4" y una red interna con capacidad IPv6.

El tráfico IPv6 basado en ISATAP es encapsulado con un encabezado IPv4. Este túnel es automáticamente hecho por la interfaz ISATAP sobre el host que envía datos o el router que transmite. La interfaz ISATAP de túnel trata a la parte de la red interna "sólo IPv4" como una sola capa de enlace. En el caso de ISATAP, la capa de enlace de Encapsulado es IPv4.

Aunque el mecanismo de túnel ISATAP es similar a otros mecanismos de túnel, tales como 6over4 , ISATAP está designado para transportar paquetes IPv6 en un lugar en donde una infraestructura nativa IPv6 aún no está disponible. ISATAP es similar al mecanismo 6over4 en que usa una capa de enlace IPv4 para interconectar nodos IPv6 y envía mediante un túnel datagramas IPv6 a través de IPv4, creando un enlace local mediante una red IPv4. La diferencia es que ISATAP no asume que existe una infraestructura con capacidad multicast. Lo que se asume es que la infraestructura IPv4 es una subred NBMA (NonBroadcast Multiple Access) y las características de dicha red se toman en cuenta cuando las funciones son especificadas como un vecino (nodo de red) y una solicitud de ruteo.

Como sucede con muchos esquemas de transición IPv6, el direccionamiento ISATAP es la llave de su propia funcionalidad. Por ejemplo, para evadir la necesidad de utilizar

Neighbor[12] o Router Discovery[13], la parte de interfaz ID de una dirección ISATAP contiene la dirección IPv4 de la interfaz del host o router. Cuando se comunican directamente con un vecino (nodo de red), la dirección de enlace local del vecino automáticamente indica el punto final del túnel de la parte final de la interfaz ID de la dirección. Además de la dirección IPv4, la interfaz ID contiene un valor especial para el resto de los 32 bits para indicar un host o router ISATAP.

El protocolo IPv6 en Windows Server 2008 y Windows Vista crea interfases de túneles ISATAP separados por cada interfaz LAN que es instalada en una computadora que tiene un sufijo DNS diferente. Por ejemplo, si una computadora utiliza Windows Vista en dos interfases LAN y ambas están enlazadas a la misma red interna y asignadas al mismo sufijo DNS, sólo hay una interfaz de túnel ISATAP. Si estas dos interfases LAN son enlazadas con dos diferentes redes con distintos sufijos DNS, existirán dos interfases de túnel ISATAP. Para computadoras que utilizan Windows Server 2008 o Windows Vista Service Pack 1, la interfaz de túnel ISATAP es colocada en un medio de estado desconectado hasta que el nombre ISATAP pueda ser resuelto.

El protocolo IPv6 en Windows Vista sin Service packs instalados configura automáticamente la dirección de enlace local ISATAP (FE80:: 5EFE:w.x.y.z o FE80:: 200:5EFE: w.x.y.z) sobre la interfaz de túnel ISATAP por la dirección IPv4 que es asignada a la correspondiente interfaz LAN. El protocolo para Windows Server 2008 y Windows Vista con Service Pack 1 configura la dirección de enlace local ISATAP (FE80 :: 5EFE: w.x.y.z o FE80:: 200 : 5EFE: w.x.y.z) sobre la interfaz de túnel ISATAP sólo si el nombre ISATAP puede ser resuelto.

Estas direcciones de enlace local ISATAP permiten a dos hosts comunicarse a través de una red “sólo IPv4” sin el requerimiento adicional de direcciones globales o únicamente locales ISATAP. Se pueden determinar los nombres de los índices de interfaz de las interfases de túnel ISATAP desde el comando ipconfig/all.

Todas las interfases de túnel ya tiene un asterisco(“*”) predeterminado en su nombre, como “Local Area Connection*6”. Las interfases de túnel ISATAP tienen un asterisco en su nombre “ISATAP” en su descripción y son asignadas a una dirección de enlace local ISATAP. Se puede obtener la interfaz índice en un túnel ISATAP desde el número que va después del signo (“%”) en la dirección de enlace local asignado a la interfaz. Por ejemplo, el índice de una interfaz de túnel ISATAP con la dirección FE80:: 200:5EFE:131.107.9.221%10 es 10.

[12] Neighbor Discovery (descubrimiento de vecinos): Es un mecanismo con el cual un nodo que se acaba de incorporar a una red descubre la presencia de otros nodos (vecinos) en el mismo enlace, además de ver sus direcciones IP.

[13] ICMP Internet Router Discovery Protocol (IRDP) utiliza mensajes ICMP "Router Advertisement" y "Router Solicitation" para permitir a un nodo descubrir la dirección de Routers operacionales en una subred.

Se puede deshabilitar ISATAP estableciendo el registro

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Servces\tcpip6\Parameters\DisabledComponentes

con el valor de 0x4.

A continuación se observa un ejemplo de túnel ISATAP

Un host A tiene una interfaz LAN y está configurada con la dirección IPv4 de 10.40.1.29. Un host B tiene una interfaz LAN y está configurada con una dirección IPv4 192.168.41.30. IPv6 sobre un host A tiene la dirección ISATAP FE80:: 5EFE: 10.40.1.29 asignada a la interfaz de túnel ISATAP y el host B tiene la dirección ISATAP FE80::5EFE:192.168.41.30 asignada a su interfaz de túnel ISATAP. Se muestra la configuración en la figura 4.2.

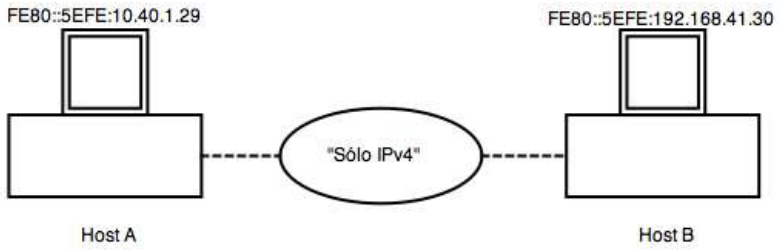

Figura 4.2 Ejemplo de configuración ISATAP

Cuando el host A envía tráfico IPv6 al host B, destinado para la dirección de enlace local ISATAP del host B, la dirección de envío y destino para los encabezados IPv6 e IPv4 están listadas en la tabla 4.1.

Tabla 4.1 Direcciones

CAMPO	VALOR
Dirección Fuente IPv6	FE80::5EFE:10.40.1.29
Dirección Destino Pv6	FE80::5EFE:192.168.41.30
Dirección Fuente IPv4	10.40.1.29
Dirección Destino IPv4	192.168.41.30

Para comprobar la conectividad entre el host ISATAP, se puede usar la herramienta ping. Por ejemplo, para hacer “ping” al host B a una dirección local ISATAP desde un host A, se puede usar el siguiente comando:

ping fe80::5efe:192.168.41.30%10

Debido a que el destino del comando ping es un dirección de enlace local, se debe usar el signo % con el identificador como parte de la dirección destino para especificar el índice de

interfaz 10, el cual es el índice asignado a la interfaz de túnel ISATAP sobre el Host A. La interfaz de túnel ISATAP usa su propia dirección de enlace local ISATAP como una dirección fuente IPv6. La interfaz de túnel ISATAP determina el destino de la dirección IPv4 del encabezado de Encapsulado IPv4 desde los últimos 32 bits en la dirección destino IPv6, la cual corresponde a la dirección embebida IPv4 del host B. Para la dirección fuente IPv4 en el encapsulado del encabezado IPv4, IPv4 y el host B determinan la mejor dirección fuente IPv4 para llegar a la dirección destino IPv4 192.168.41.30. En este caso, el host A tiene sólo la dirección IPv4 asignada, entonces IPv4 sobre el host A usa la dirección fuente 10.40.1.29.

4.1.1Componentes ISATAP

Los componentes de ISATAP son un host ISATAP, un router ISATAP, y una o más subredes ISATAP. La figura 4.3 muestra los componentes de una red interna con capacidad IPv4 que está usando una subred ISATAP.

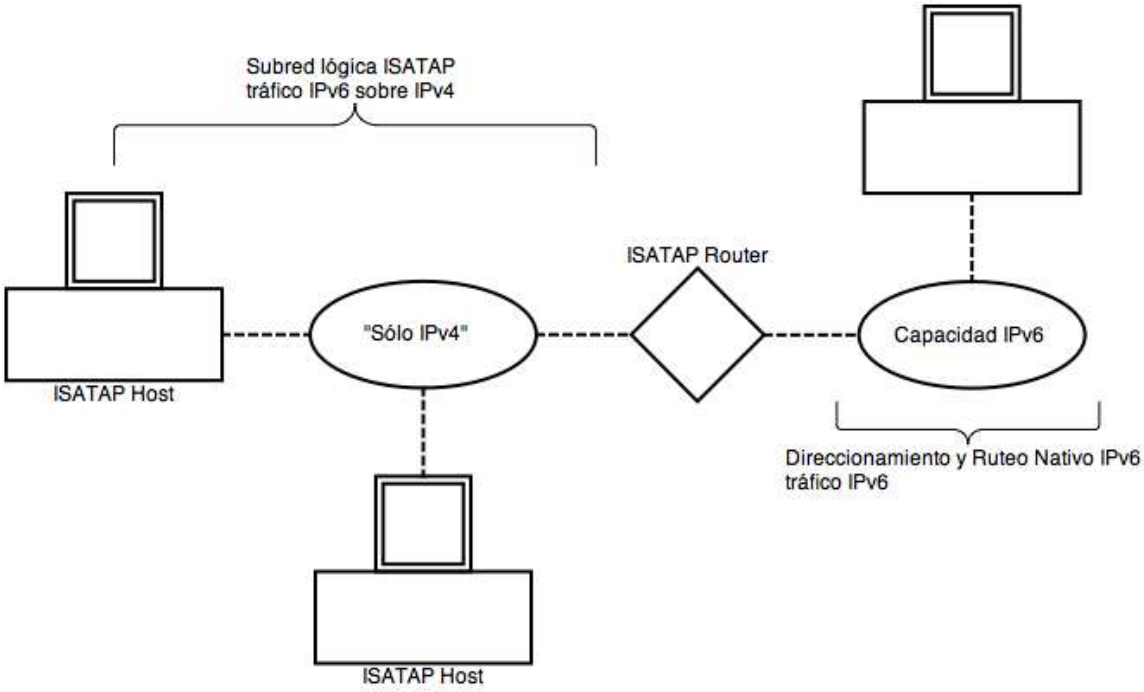

Figura 4.3 Componentes ISATAP

La parte de la red interna "sólo IPv4" es la subred ISATAP. La parte con capacidad IPv6 de la red interna tiene routers y direccionamiento nativos IPv6. El host en la parte con capacidad IPv6 de la red interna está configurado con una dirección global o únicamente local sobre la interfaz LAN y no necesita usar encapsulado IPv4 para comunicarse con cualquier otro que usa IPv6.

El host ISATAP tiene una interfaz de túnel ISATAP y realiza sus propios túneles a otros host ISATAP sobre la misma subred ISATAP (túnel host-to-host) o al router ISATAP (túnel host-to-host). El host ISATAP puede ser global, sólo local, o direcciones de enlace local ISATAP para comunicarse con cualquier otro. Para comunicarse con otros hosts ISATAP en la subred ISATAP usando su dirección global ISATAP, local, o de enlace local, el host ISATAP utiliza el túnel para pasar sus paquetes a cualquier otro. Para comunicarse con hosts IPv6 en la parte con capacidad IPv6 de la red interna usando su dirección nativa global o sólo local, el host ISATAP utiliza el túnel para enviar sus paquetes a un router ISATAP.

Un router ISATAP es un router IPv6 con una interfaz de túnel ISATAP que realiza lo siguiente:

- Envía paquetes entre el host ISATAP sobre subredes ISATAP y un host IPv6 sobre subredes con capacidad IPv6.
- Publica prefijos de direcciones a host ISATAP sobre la subred ISATAP. El host ISATAP usa la publicación de prefijos de direcciones para configurar direcciones globales ISATAP o direcciones sólo locales ISATAP.
- Actúa como un router predeterminado para host ISATAP. Cuando un host ISATAP recibe un mensaje desde el router ISATAP el cual es un mensaje de que él es el router predeterminado, el host ISATAP adhiere una ruta predeterminada(::/0) usando la interfaz de túnel ISATAP con la siguiente dirección de salto justo a la dirección de enlace local ISATAP del router ISATAP. Cuando el host ISATAP envía paquetes destinados a locaciones mas allá de su subred ISATAP, los paquetes son pasados por el túnel a la dirección IPv4 del router ISATAP correspondiente a la interfaz de router ISATAP de la subred ISATAP. El router ISATAP envía los paquetes IPv6 al siguiente salto sobre la parte de la red interna con capacidad IPv6.

La parte con capacidad IPv6 de la red interna es opcional, en caso de que el router ISATAP sólo funcione como un router que envía mensajes de advertencia y no como un router predeterminado. Este es el caso de un desarrollo inicial ISATAP en el cual no hay subredes con capacidad IPv6.

4.2 6to4

6to4 permite la interconexión de redes IPv6 aisladas mediante un túnel automático dentro de una red IPv4, la importancia de este mecanismo es que puede comunicar nodos con una configuración sencilla.

Los elementos que involucran a este mecanismo son lo siguientes:

a) 6to4 Host: cualquier nodo IPv6 que tenga configurada una dirección 6to4

b) 6to4 Router: un encaminador IPv6/IPv4 que pueda soportar túneles 6to4, así como resolver direcciones 6to4

c) 6to4 relay router – encaminador de reenvío: un encaminador IPv6/IPv4 que pueda resolver tráfico 6to4 entre encaminadores 6to4 teniendo como red nativa IPv6. Este tipo de encaminadores puede funcionar con direcciones anycast, de tal modo que los paquetes serán enviados en función a la distancia, para este propósito IANA ha reservado la dirección 192.88.99.1 donde su representación en una dirección IPv6 es 2002:c058:6301::

Las direcciones 6to4 se identifican por el prefijo 2002 teniendo dentro una dirección IPv4, tanto del host como la subred, su estructura es la siguiente (Figura 4.4):

16 bits	32 bits	16 bits	64 bits
2002	Dirección IPv4	Identificador de subred	Identificador de interfase

Figura 4.4 Formato de direcciones 6to4

Los 32 bits después del prefijo 2002 es la dirección IPv4 de la puerta de enlace en su representación hexadecimal dejando 80 bits libres para espacio de direccionamiento de una red interna.

El identificador de subred (16 bits) es usado dentro de una infraestructura de red para enumerar las subredes individuales.

El identificador de interfaz (64 bits) identifica a un nodo en una subred dentro de una infraestructura.

Las direcciones 6to4 pueden tener 2 direcciones IPv4, una para el identificador de subred así como el identificador de interfaz, dependiendo del alcance que tenga el paquete, estas direcciones pueden ser distintas o similares.

Para distinguir qué paquetes se envían dentro o fuera de una Intranet[14] se debe hacer un uso correcto de las direcciones usando un prefijo para identificar cuántos bits se están utilizando para determinar la dirección de la terminal.

[14] Intranet es una red de computadoras que comparte información utilizando Internet que a su vez implementa mecanismos de seguridad como la autenticación

Un prefijo de 64 bits (2002::/64) se utiliza para paquetes 6to4 que se encuentran en subredes separadas dentro de una intranet, a su vez un prefijo de 16 bits (2002::/16) cuando la dirección destino se encuentra fuera de una infraestructura de intranet.

Para asegurar una correcta operación en topologías complejas, se define un método para la asignación de direcciones para un correcto envío de paquetes. Al enviarse un paquete con dirección origen 2002, el DNS devolverá una serie de direcciones destino que contengan la dirección 2002, el emisor deberá hacer una correcta elección de la direcciones origen y destino.

Por lo general se utilizan estas consideraciones para el correcto funcionamiento del 6to4.

Si un emisor/receptor tiene asignada sólo una dirección 6to4 y otro emisor/receptor cuenta con una dirección nativa IPv6 además de una dirección 6to4, se utilizará para las transacciones la dirección 6to4.

Si ambos hosts cuentan con una dirección 6to4 y una IPv6 nativa, se debe usar un solo tipo de dirección para ambos donde la elección debe ser configurable, la configuración por defecto es la dirección nativa IPv6.

Los paquetes 6to4 son encapsulados en paquetes IPv4 para que se puedan transmitir en conexiones IPv4. El encapsulado usa el protocolo tipo 41 que es el mismo usado en la transmisión de paquetes mediante uso de túneles.

4.2.1 Flujo de paquetes

En el flujo de paquetes se considera una red que ya está previamente configurada con direcciones 6to4 y cada componente de una red puede interpretar esta dirección para que pueda ser resuelta y remitida correctamente.

Los paquetes 6to4 pueden atravesar distintos caminos como lo es una red IPv4 o una red nativa IPv6, para estas distintas topologías un flujo de paquete 6to4 tiene que ser procesado de la siguiente manera:

a) Se considera una topología como la de la figura 4.5:

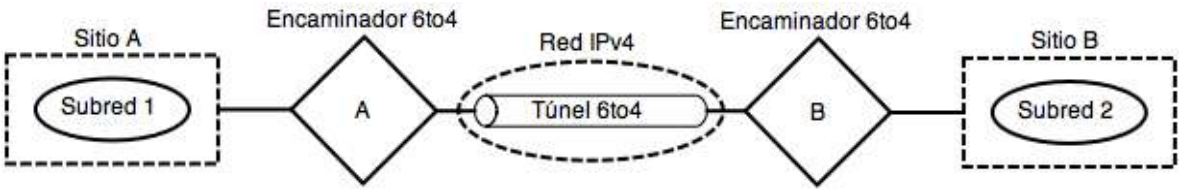

Figura 4.5 túnel 6to4

En esta configuración se envía una transmisión entre dos nodos que pertenecen a dos sitios[15] distintos, estos sitios se encuentran separados por una red IPv4, para que pueda haber comunicación entre ellos se ha configurado un túnel 6to4.

También hay que considerar que los encaminadores 6to4 se consideran como puntos finales para el túnel 6to4.

- El nodo de la subred 1 que se encuentra en la ubicación sitio A envía una transmisión a un host que se encuentra ubicado en sitio B, cada cabecera tiene una dirección origen derivada de 6to4 así como una dirección destino derivada de 6to4.

- El encaminador A encapsula cada paquete IPv6 dentro de un paquete IPv4, aquí es donde se establece la dirección IPv4 destino en la dirección del encaminador B situado en el sitio B.

- Si en el trayecto los paquetes se encontraran a un encaminador, éste utilizará la dirección IPv4 para retransmitir el paquete.

- Cuando los paquetes llegan al encaminador B, se procede a obtener el paquete original IPv6.

- El router del sitio B utiliza la dirección de destino que tiene la cabecera IPv6 para enviar los paquetes al receptor.

b) Se considera una topología como la de la figura 4.6:

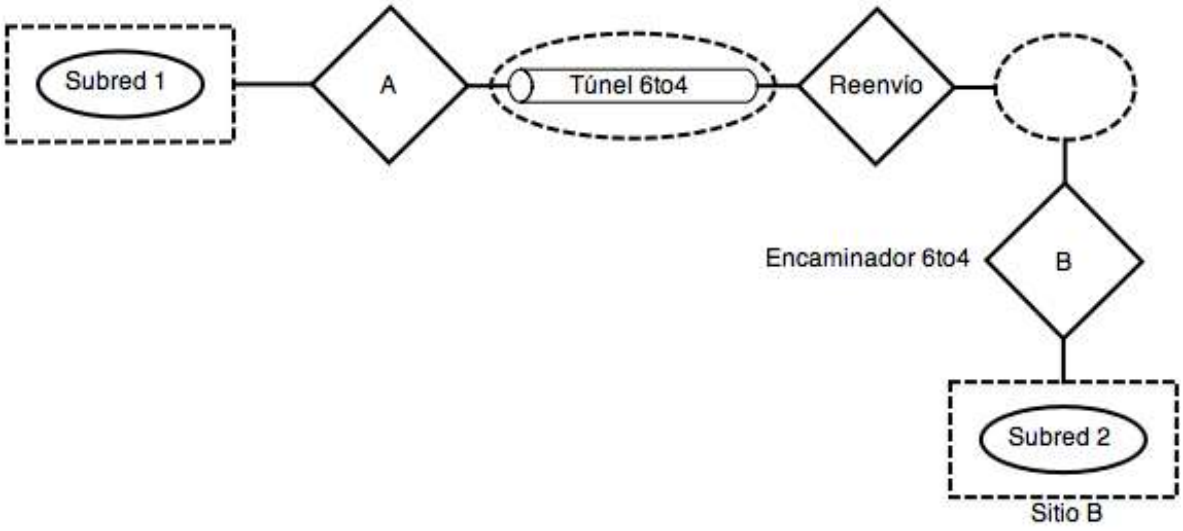

Figura 4.6 trayectoria a través de un túnel 6to4 y una red IPv6

[15] Site – sitio. Se puede expresar como un punto en Internet con una dirección única a la cual acceden los usuarios para obtener información.

Para esta configuración los paquetes tienen una red IPv4 mediante un túnel 6to4, además de una red IPv6 nativa antes de llegar a la subred donde se encuentra el nodo destino.

Esta topología necesita de un encaminador de reenvío[16] indispensable para poder comunicar encaminadores 6to4 cuando se encuentran redes con tecnologías distintas de direccionamiento

-El nodo de la subred 1 que se encuentra en la ubicación sitio A envía una transmisión a un nodo que se encuentra ubicado en el sitio B el cual se encuentra dentro de una red IPv6, el destino tiene una dirección IPv6 estándar.

- El encaminador que se encuentra en la ubicación del sitio A encapsula cada paquete dentro de un paquete IPv4, estableciendo la dirección destino el encaminador 6to4 que conecta a la red IPv6 donde se encuentra situado el nodo destino.

- Cuando el paquete llega al encaminador de reenvio, éste procede a obtener el paquete original IPv6, obteniendo la dirección IPv6 y se envía a través de la red IPv6.

- El encaminador de reenvio puede tener configurada una dirección anycast, por lo que tendría una dirección reservada 192.88.99.1 y los paquetes serían recibidos según la proximidad del origen.

- Los paquetes son recibidos por el encaminador B 6to4 resolviendo la dirección IPv6, enviándolo al nodo destino del sitio B

4.3 TEREDO

Teredo es una tecnología de transición para el protocolo IPv6 que asigna direcciones y túneles automáticos host a host para tráfico unicast cuando los nodos están localizados dentro de uno o varios NAT IPv4.

Teredo es similar al mecanismo 6to4 ya que es un túnel automático, a diferencia de 6to4 donde los límites del túnel están determinados por los encaminadores 6to4, un túnel Teredo se crea en el host y utiliza IPv4 para resolver las direcciones y enviar los paquetes a los NAT.

Una infraestructura Teredo consiste de los siguientes componentes:

- Teredo clients
- Teredo servers
- Teredo “relays”

[16] Encaminador de reenvío (Router Relay): Permite la conexión entre sitios 6to4 y redes nativas IPv6

- Teredo host-specific relays

a) Teredo clients.- Es un nodo IPv6/IPv4 que soporta túneles Teredo.

b) Teredo server.- Es un nodo IPv6/IPv4 que está conectado a una red IPv4 y a red IPv6 dando soporte a túneles Teredo, estableciendo la comunicación entre los clientes Teredo y nodos IPv6.

c) Teredo Relay.- Teredo Relay es un encaminador IPv6/IPv4 que puede retransmitir paquetes entre los clientes Teredo y nodos exclusivos IPv6 a través de una red IPv4 usando túneles Teredo.

d) Teredo host-specific relays.- Es un nodo IPv4/IPv6 que permite la conectividad entre una red IPv4 y una red IPv6, permitiendo la comunicación directa con clientes Teredo sobre una red IPv4 sin la necesidad de un intermediario Teredo Relay.

Una dirección Teredo está conformada por 5 componentes (Figura 4.7):

Prefijo	Servidor IPv4	Banderas	Puerto	Cliente IPv4
32 bits	32 bits	16 bits	16 bits	32 bits

Figura 4.7 Formato de direcciones Teredo

- Prefijo: 32 bits

  El identificador del servicio Teredo actualmente utiliza el prefijo 2001::/32

- Servidor IPv4: 32 bits

  Dirección IPv4 del servidor Teredo

- Banderas: 16 bits

  Un set de 16 bits que informa el tipo de dirección y NAT, este campo tiene asignados los bits de la siguiente manera:

  CRAAAAUG AAAAAAAA

  El identificador C es para la bandera “cone flag” (bandera cono), ése establece si un cliente Teredo está conectado a Internet a través de una NAT.

  El identificador R está reservado para uso futuro.

  El identificador U para denotar una bandera local o universal.

  El identificador G es para banderas individuales o por grupo.

  El identificador A cuenta con 12 bits para generar un número aleatorio, es usado para evitar que un usuario malintencionado pueda encontrar la dirección completa

de un cliente Teredo, el número de combinaciones que se puede realizar es 2^{12} (4096).

- Puerto: 16 bits

  Contiene el mapeo del puerto UDP "ensombrecido" del servicio Teredo hacia el cliente, recibe el nombre ensombrecido ya que el puerto no se muestra claramente, es decir, ha sido manipulado.

- Cliente IPv4: 32 bits

  Contiene el mapeo de la dirección IPv4 "ensombrecida" del cliente, recibe el nombre ensombrecida ya que la dirección no se muestra claramente, es decir, ha sido manipulada.

El formato del puerto UDP y la dirección IPv4 "ensombrecida" se refiere a que estos elementos han sido modificados, ya que cada bit se encuentra invertido, esto se realiza mediante la operación binaria XOR[17] con el valor en hexadecimal FFFF para el puerto UDP (16 bits), de la misma forma se realiza la operación con la dirección IPv4 sólo que por la extensión de la dirección (32 bits) se realiza la operación binaria XOR con el número en hexadecimal FFFFFFFF.

Los paquetes Teredo son encapsulados dentro de paquetes IPv4, el formato simple es de la siguiente manera (Figura 4.8):

IPv4	UDP	Paquete IPv6

Figura 4.8 Encapsulado simple Teredo

En transmisiones de terceros, el servidor puede insertar un indicador de origen en los primeros bytes de la carga de datos (Figura 4.9).

IPv4	UDP	Indicador de origen	Paquete IPv6

Figura 4.9 Encapsulado Teredo con indicador de origen

El campo indicador de origen es una estructura de 8 octetos que contiene los siguientes elementos (Figura 4.10):

[17] XOR. Función booleana denominada OR exclusiva que opera con dos valores binarios, el resultado se define como aquella que da por resultado uno si el valor de sus entradas es distinto y cero cuando el valor de las entradas es la misma

Nulo (0x00)	Nulo (0x00)	Número de puerto origen
Dirección IPv4 origen		

Figura 4.10 Estructura del indicador de origen

Los dos primeros octetos son valores nulos del indicador para identificar cuándo es un encapsulado simple (figura 4.9) que en ella contiene los primeros 4 bits del paquete la indicación del protocolo IPv6 y el indicador de origen.

Después de los dos octetos nulos, los siguientes 16 bits son del número de puerto ensombrecido desde el cual el paquete fue recibido, los últimos 32 bits contiene la dirección IPv4 ensombrecida desde la cual el paquete fue recibido.

Un paquete Teredo contiene una carga útil IPv6 (68 bytes + n bytes), también existe el paquete llamado burbuja Teredo que está compuesto sólo de 68 bytes sin la carga útil IPv6, este paquete es utilizado por el cliente para renovar la tabla de mapeo de la NAT e inicializar las comunicaciones Teredo

4.3.1 Indicador de autenticación

El indicador de autenticación es usado para asegurar el intercambio de mensajes de los encaminadores de solicitud y de anuncios[18] entre el cliente Teredo así como el servidor Teredo, ambos están configurados con una clave secreta usada para generar los datos de autenticación en el indicador de autenticación.

El indicador de autenticación está situado dentro de la cabecera UDP y el paquete IPv6 de la siguiente manera (Figura 4.11):

IPv4	UDP	Indicador de Autenticación	Origen	Paquete IPv6

Figura 4.11 Encapsulado Teredo con indicador de autenticación

La estructura del indicador de autenticación es el siguiente:

- Tipo de indicador (16 bits)

  Este campo especifica el tipo de indicador, para el indicador de autenticación su valor es 1, tanto el cliente Teredo como el servidor Teredo pueden determinar el indicador de autenticación de los dos primeros bytes de un paquete IPv6 ya que los 4 bits de un paquete IPv6 tiene el valor 0110 que corresponde al campo versión de la cabecera IPv6

[18] Los encaminadores de solicitud y de anuncios sirven para descubrir hosts vecinos mediante el envío de mensajes de control de Internet (ICMP)

- Longitud de identificador del cliente (8 bits)

  Indica la longitud del campo identificador del cliente

- Longitud de los datos de autenticación (8 bits)

  Indica la longitud del campo valor de autenticación

- Identificación del cliente (variable)

  Este campo contiene el valor de autenticación para el paquete, se calcula usando una clave compartida

- Nonce (8 bytes)

  Contiene una serie de números aleatorios que se utiliza para verificar el tiempo de un intercambio de paquetes además de prevenir ataques de reproducción paquetes

- Confirmación (8 bits)

  Contiene un valor que indica si el cliente Teredo está usando la correcta clave secreta.

4.3.2 Transmisión de paquetes Teredo

Cuando un cliente Teredo ha de transmitir un paquete sobre una interfaz Teredo, éste examina la dirección IPv6 destino, el cliente verifica si hay una entrada para la dirección IPv6 en la lista de enlaces Teredo.

Si la entrada para la dirección IPv6 está en la lista de enlace y su estado es "trusted" (de confianza), el paquete IPv6 se enviará mediante UDP a la dirección IPv4. El cliente actualiza la información de la última transmisión en la lista de enlaces.

Si el destino no es una dirección Teredo, el paquete queda en espera y el cliente realiza una "prueba de conectividad directa IPv6", el paquete es reenviado si este procedimiento se completa con éxito.

Si el destino es una dirección Teredo y tiene activada la bandera cono (el primer bit del campo bandera es 1), el paquete se envía sobre un paquete UDP a una dirección mapeada IPv4, así como a un puerto mapeado extraído de la dirección IPv6

Si el destino es una dirección Teredo teniendo desactivada la bandera cono (el primer bit del campo bandera es 0), el paquete queda en espera. Si el cliente no se encuentra localizado detrás de un NAT, se le enviarán paquetes burbuja Teredo en espera de una respuesta del destino, hasta que obtenga una respuesta el paquete será reenviado.

4.4 6over4

Es un mecanismo de transición de IPv6 para transmitir paquetes IPv6 entre nodos con doble pila sobre una red IPv4 con multicast habilitado. IPv4 es utilizado como un nivel de enlace virtual para poder ejecutar IPv6. Este mecanismo es diferente a 6to4 en el que se permite el descubrimiento total de los nodos vecinos gracias a que la red IPv4 se comporta como una especie de LAN virtual, no requiere de ningún prefijo especial como en 6to4 (Figura 4.12).

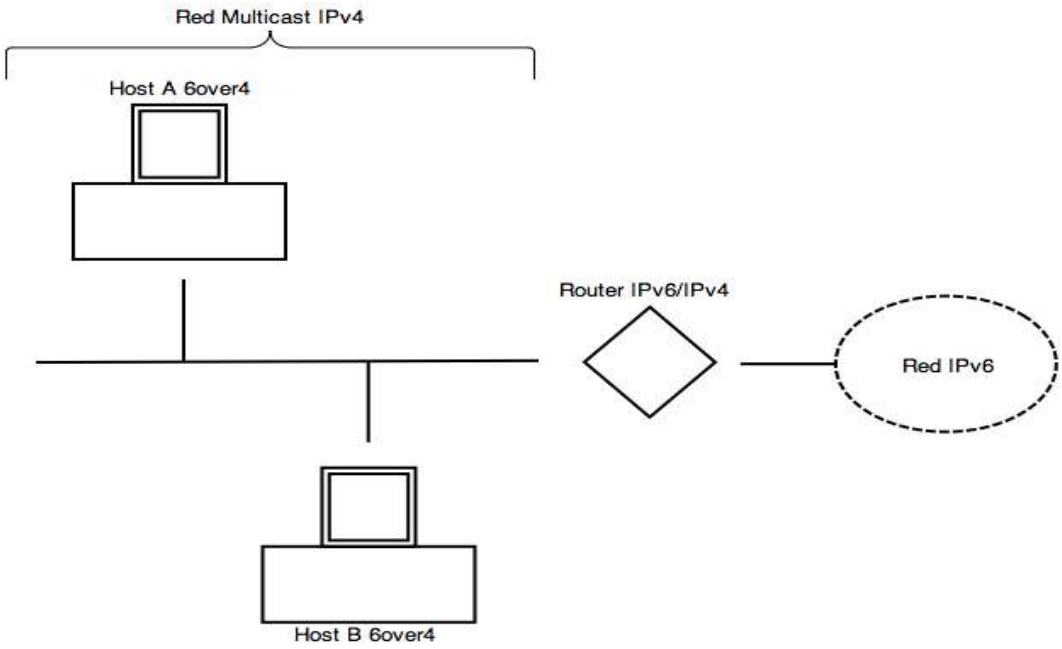

Figura 4.12 Red Lógica 6over4

Un host 6voer4 necesita una serie de direcciones, para obtener estas direcciones, el nodo 6over4 utiliza la dirección IPv4 de la interfaz, de la misma manera que un nodo con una interfaz Ethernet usa el ID de 64 bits de la interfaz (Identificador Único Extendido). Estas direcciones son presentadas a continuación:

- Dirección Unicast: Las direcciones unicast están compuestas de la siguiente forma: el host 6over4 utiliza un prefijo válido de 64 bits para las direcciones unicast y el identificador de 64 bits de la interfaz ::IPv4$_{\mathbf{dir}}$, donde IPv4$_{\mathbf{dir}}$ es la dirección IPv4 de 32 bits asignada al host.

- Dirección de enlace local: De manera predeterminada, los hosts 6over4 configuran automáticamente la dirección de enlace local FE80::IPv4$_{\mathbf{dir}}$ en cada interfaz 6ver4. Por ejemplo, un nodo con una dirección 10.0.0.1 acabará con una dirección de enlace local FE80::0A00:0001.

- Dirección multicast del nodo solicitado: Para cada una de sus direcciones unicast, al nodo se le asigna una dirección multicast. IPv6 utiliza la dirección muticast del

nodo solicitado cuando envía un mensaje de solicitud de vecindad como parte de la resolución de la dirección. La dirección multicast del nodo solicitado se utiliza de la siguiente manera, en vez de enviar un mensaje de solicitud de vecindad a cada nodo del enlace local (mediante una dirección muticast FF02::1 dirigida a todos los nodos), el mensaje de solicitud de vecindad se envía a un grupo muticast muy restringido identificado mediante la dirección muticast del nodo solicitado. La dirección muticast del nodo solicitado se construye tomando los tres últimos octetos de una dirección unicast dada y precediéndolos por FF02::1:FF00:0000/104. Por ejemplo, la dirección muticast para el nodo solicitado de una dirección unicast 2002:630:200:8100:02C0:4FFF:FE68:12CB es FF02::1:FF68:12CB (Figura 4.13). Ésta es la dirección muticast del nodo solicitado que el nodo utiliza como destino del paquete de solicitud de vecindad.

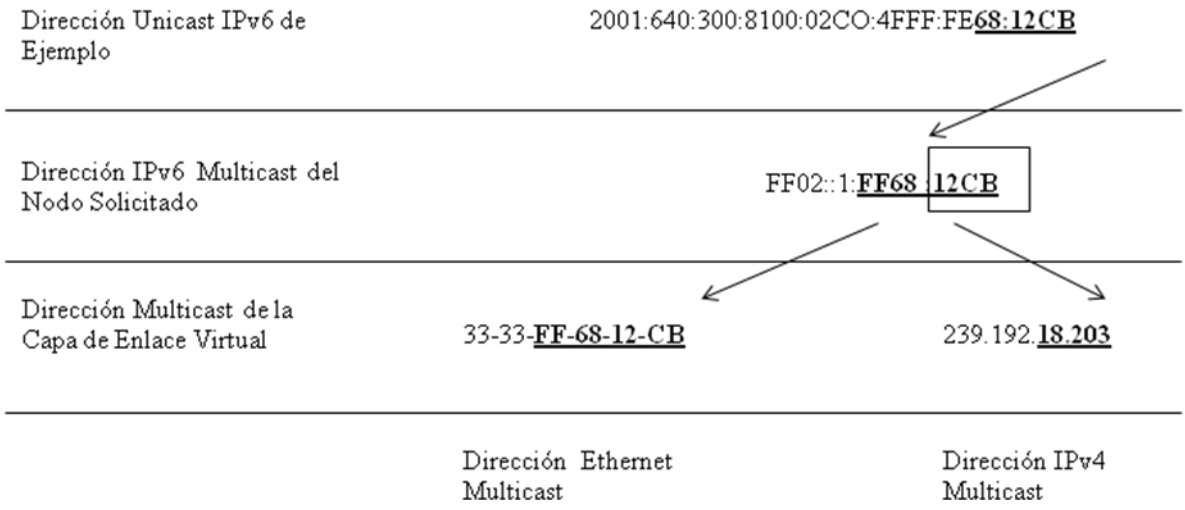

Figura 4.13 Esquema Multicast Ethernet e IPv4 para IPv6

- Para incorporar la capacidad de multicast de la red IPv4 se necesita una última correspondencia entre la dirección muticast del nodo solicitado y la dirección muticast IPv4 usada en el mensaje de la solicitud de vecindad. Aquí, una vez más se emplea un proceso análogo a aquel definido para el multicast IPv6 sobre Ethernet. Las correspondencias entre Ethernet e IPv4 se muestran en la Figura 4.13. Para Ethernet, la dirección multicast de destino se forma precediendo 33-33-(que indica multicast) a los últimos 32 bits de la dirección multicast IPv6 del nodo solicitado. En el caso de 6over4, una dirección de destino muticast del nodo solicitado se hace corresponder con una dirección muticast IPv4 extraída del bloque 239.192.0.0/16, un sub bloque de la dirección de ámbito de organización local (RFC 3171) [Cj] y concatenado a éste están los últimos 16 bits de la dirección multicast del nodo solicitado.

Con las correspondencias que se definieron se pueden seguir los procedimientos de descubrimiento de vecindad definidos en el RFC 2461 [Ck]. Estos procedimientos suponen el intercambio de mensajes de solicitud de router, aviso de router, solicitud de vecindad, aviso de vecindad y redirección ICMP. Se puede ver un ejemplo en la Figura 4.14 que ilustra un mensaje de solicitud de vecindad pidiendo la dirección de enlace IPv4 del nodo objetivo al mismo tiempo que se le proporciona a éste la propia dirección de enlace IPv4. Es un ejemplo de envío de un mensaje de solicitud de vecindad cuando un host está resolviendo la dirección unicast IPv6 indicada. Sólo se muestran los campos de cabecera fundamentales.

Cabecera IPv4	• Dirección Origen: dirección IPv4 asignada a la interfaz del host que envía. • Dirección Destino: 239.192.18.203(dirección multicast IPv4)
Cabecera IPv6	• Siguiente Cabecera 58 • Dirección Origen: la dirección IPv6 asignada a la interfaz del host que envía. • Dirección Destino: FF02::1:FF68:12CB(dirección multicast del nodo solicitado).
Mensaje ICMPv6	• Tipo 133 • Dirección IPv6 Objetivo: 2001:640:300:8100:02C0:4FFF:FE68:12CB • Dirección Origen de Capa de Enlace: la dirección IPv4 asignada a la interfaz del host que envía.

Figura 4.14 Mensaje de Solicitud de Vecindad

Se debe tomar en cuenta lo siguiente:

- La dirección IPv4 de destino (239.192.18.203) es la dirección mulicast IPv4 asociada, ya resuelta la dirección unicast, el host objetivo recibirá el paquete IPv4 porque es un miembro de este grupo multicast. La dirección IPv4 de origen es de la interfaz del host que solicita la resolución de la dirección.

- Entre los campos IPv6 se incluye una dirección de origen que es la dirección asignada a la interfaz desde la que se envía el mensaje, una dirección destino que es la dirección multicast del nodo solicitado correspondiente a la dirección objetivo,

como se aprecia en la Figura 4.14 y un campo de Siguiente Encabezado con valor 58 indicando ICMPv6. ICMPv6 incluye un campo Type con el valor 153 indicando un mensaje de solicitud de vecindad, la dirección IPv6 del objetivo de la solicitud y la dirección de enlace de origen, en este caso, la dirección IPv4 asignada al host que solicita la resolución de la dirección.

- Las solicitudes de vecindad son multicast cuando el nodo necesita resolver una dirección y unicast cuando el nodo trata de comprobar si un vecino es alcanzable.

Dado que 6over4 confía en el multicast IPv4, una característica que no ha sido muy desarrollada, hace que el mecanismo 6over4 no sea de uso común.

4.5 Tunnel Brokers

Para facilitar y promover el uso de túneles configurados en una red IPv4, la IETF definió un mecanismo llamado Túnel Broker. En el RFC 3053 [Cl] (IPv6 Tunnel Broker), este mecanismo es un sistema externo, actúa como un servidor sobre una red IPv4 y recibe peticiones de túnel desde nodos de doble pila. Básicamente las peticiones son enviadas a través de nodos de pila dual IPv4 al túnel broker mediante HTTP, el usuario final puede llenar una página web solicitando un túnel configurado para sus nodos de pila dual.

A continuación el túnel broker envía de regreso la información por medio de HTTP a los nodos de doble pila tales como las direcciones IPv4, las direcciones IPv6 y las rutas predeterminadas IPv6 que serán utilizadas para establecer un túnel configurado para un router de doble pila. Un túnel broker tiene la opción de proporcionar un script a los nodos de pila dual para facilitar la configuración del túnel sobre el sistema operativo.

Finalmente, el túnel broker aplica comandos de manera remota sobre un router de pila dual para habilitar un túnel configurado. El router de pila dual debe ser conectado a un dominio IPv6. En las especificaciones del túnel broker, éste y el router de pila dual utilizan diferentes direcciones IPv4.

Un host de pila dual sobre una red IPv4 llega al túnel bróker usando HTTP. El usuario final llena una página web, entonces él obtiene una dirección IPv4 e IPv6 del túnel broker por medio de HTTP. El usuario final aplica la configuración obtenida a su host de pila dual para habilitar un túnel configurado. Simultáneamente el túnel broker aplica automáticamente la configuración final del túnel configurado sobre un router de pila dual conectado a un dominio IPv6. En la Figura 4.15 se muestra lo anterior. [KANE 2003]

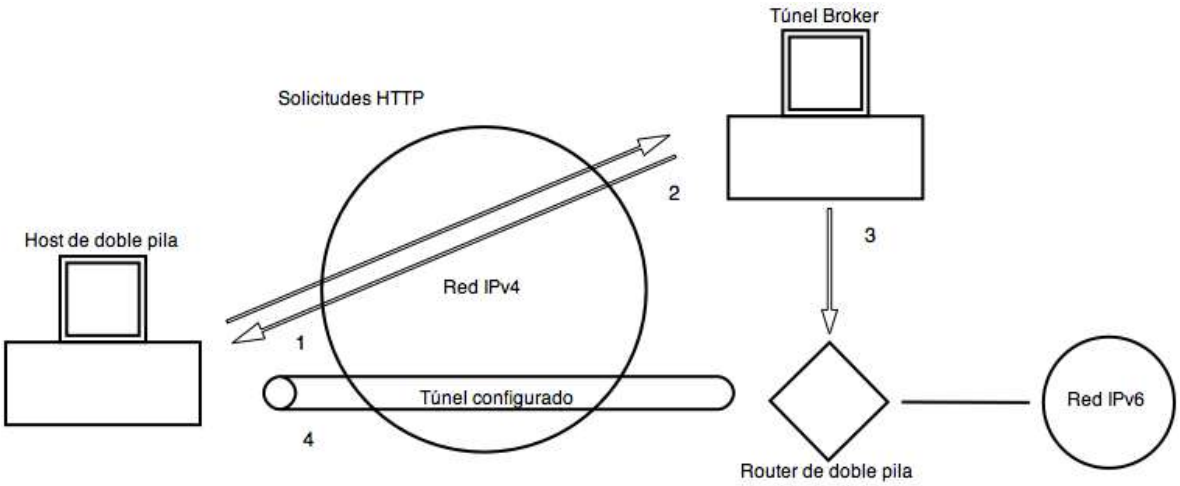

Figura 4.15 Un host de pila dual estableciendo un túnel configurado utilizando túnel broker.

El modelo de túnel broker asume que el túnel broker y el router de pila dual están controlados por la misma autoridad. Para poder controlar la configuración del router, el túnel broker debe estar conectado físicamente al puerto de la consola del router o se puede administrar la consola por medio de protocolos como Telnet o Security Shell. Esto también significa que el túnel broker debe tener los derechos y permisos para administrar la seguridad del router de doble pila.

4.5.1 Tunnel Server

El tunnel server es un modelo simplificado de túnel broker, en este método se combina el túnel broker y el router de pila dual en el mismo sistema en vez de tener dos sistemas separados. La forma de solicitar un túnel configurado es generalmente la misma que el túnel broker: HTTP over IPv4.

Un host de pila dual sobre una red IPv4, utilizando el protocolo IPv4, llega al túnel server usando HTTP. El usuario final llena una página web y obtiene direcciones IPv4 e IPv6 desde el túnel server. El usuario final aplica la configuración obtenida a su host de pila dual para habilitar un túnel configurado. Entonces el túnel server aplica localmente la configuración final al túnel configurado. Finalmente, como en el túnel broker, tan pronto como sea posible, la configuración está completamente aplicada sobre el host de pila dual y en el túnel server, el túnel configurado se establece correctamente y puede ser usado para realizar una sesión IPv6 punto final a punto final (end-to-end) sobre una red IPv4 (Figura 4.16).

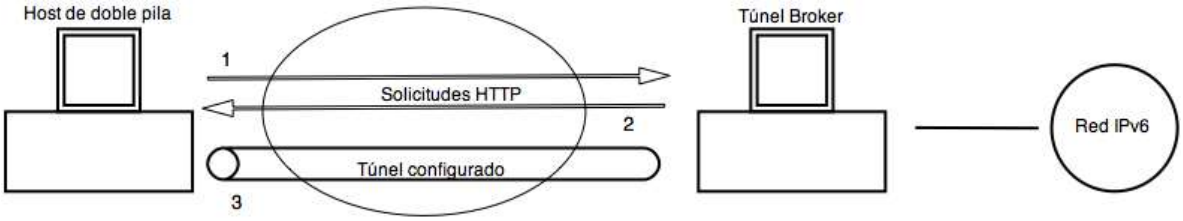

Figura 4.16 El host de pila dual estableciendo un túnel configurado usando un túnel server.

Debido a que el túnel broker y el router de pila dual se encuentran en el mismo dispositivo, el túnel server es considerado un modelo abierto que permite el desarrollo de un nuevo protocolo de control y señalización para el establecimiento de túneles configurados. Un protocolo de señalización con un túnel server construido puede proveer mucha más flexibilidad que un túnel broker para el desarrollo de conectividad IPv6 sobre una gran escala de redes IPv4 existentes. Por ejemplo, un protocolo de señalización puede permitir el desarrollo de túneles IPv6 en IPv4 a través de NAT. Desarrollar túneles IPv6 en IPv4 a través de NAT es difícil por medio del modelo túnel broker.

Capítulo 5

Tecnologías de Traducción

5.1 SIIT

SIIT (RFC 2765) [Cm], (Sateless Internet Protocol - Protocolo de Internet Sin Estado/Internet Control Messaging Protocol Translation - Protocolo de Traducción de Control de Mensajes de Internet) es un mecanismo de traducción IPv6 que permite que un host "sólo IPv6" se comunique con un host "sólo IPv4". Su estrategia consiste en una correspondencia sin estado (stateless) o algoritmo de traducción bidireccional entre las cabeceras de los paquetes IPv4 e IPv6 así como entre mensajes ICMPv4 (Internet Control Messaging Protocol) e ICMPv6. SIIT requiere que se le asigne una dirección IPv4 al host IPv6, y esta dirección IPv4 es usada por el host para formar una dirección IPv6 especial que la contiene.

La intención es preservar las direcciones IPv4 de manera que más que tener asignadas permanentemente las direcciones IPv4 a los hosts "sólo IPv6", SIIT se basa en la asignación de direcciones temporales IPv4 a los hosts "sólo IPv6". El método de asignación sobrepasa el contenido del RFC SIIT; el RFC tan sólo sugiere que DHCP podría ser la base para una asignación temporal de direcciones IPv4.

SIIT es una traducción IP/ICMP sin estado, lo que significa que el traductor es capaz de procesar cada traducción de forma individual sin ninguna referencia a paquetes traducidos previamente. La traducción de la mayoría de campos de la cabecera IP es relativamente simple; sin embargo, hay un aspecto crucial que se debe saber, como traducir las direcciones de los paquetes de IPv4 a IPv6. Traducir una dirección IPv4 a una dirección IPv6 resulta inmediato porque sólo hay que embeber la dirección IPv4 en los 32 bits menos significativos de la dirección IPv6. Dado que las direcciones IPv6 son mucho más largas, se ha definido funcionalidad adicional para esta correspondencia. La conversión inversa, IPv6 a IPv4 resulta también directa.

5.1.1PROCESO DE TRADUCCIÓN SIIT

El algoritmo SIIT puede usarse como parte de una solución que permite a los hosts IPv6, que no tienen asignada una dirección IPv4 permanente, comunicarse con los hosts "sólo IPv4". Para manejar la traducción de direcciones IP entre IPv4 e IPv6, SIIT define nuevos tipos de direcciones IPv6 adicionales:

- Direcciones IPv6 de la forma 0::FFF:v4, llamadas direcciones "mapeadas IPv4". Esta dirección se construye simplemente incluyendo la dirección IPv4(v4) del host IPv4 junto al prefijo mostrado.
- Direcciones IPv6 de la forma 0::FFFF:0:v4 (con un cero más que la anterior), denominadas direcciones "IPv4 traducidas". Esta dirección se forma incluyendo la dirección IPv4 temporalmente al host "sólo IPv6" y permite la correspondencia entre la dirección "IPv4 traducida" del host IPv6 y una dirección IPv4.

Cuando el número de direcciones únicas IPv4 globales se vuelve escaso, hay una necesidad cada vez mayor de sacar provecho de las direcciones IPv6 largas para que cada nuevo nodo en Internet no tenga que tener asignada permanentemente una dirección IPv4. SIIT permite compartir las direcciones IPv4 asignadas al host IPv6. La figura 5.1 muestra el proceso de traducción de direcciones IP: el host IPv6 ha obtenido temporalmente una dirección IPv4 (v4temp) para comunicarse con el host IPv4. Podemos ver en la figura 5.1 cómo la traducción de la dirección IP va desde el host IPv6, usando la dirección IPv4 traducida, hacia el host IPv4.

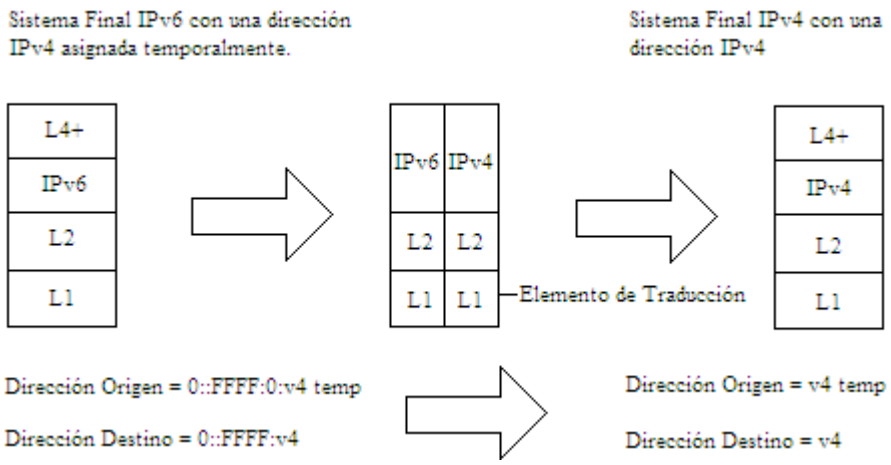

Figura 5.1 Traducción de direcciones IP, IPv6 a IPv4 (L =Layer, Capa).

La traducción del resto de los campos es directa salvo por un par de excepciones (en caso de que los paquetes requieran fragmentación). Si no hay cabecera de fragmentación, los campos de cabecera IPv4 se fijan como sigue:

- Versión: 4
- Tamaño del encabezado: 5 (sin opciones IPv4).
- Tipo de Servicio: por defecto, copia los 8 bits del campo Clase de Tráfico de IPv6.
- Tamaño total: el valor del campo Tamaño de la Carga Útil (Payload Length) de la cabecera IPv6 más el tamaño de la cabecera IPv4.
- Identificación: todo en ceros.
- Banderas: la mayor de "más fragmentos" (More Fragments) se pone en cero, la bandera de "No fragmentar" se pone en uno y la bandera de "Fragmentación en paralelo" (Fragment Offset) es todo en ceros.
- Tiempo de Vida: copiado de la cabecera Límite de saltos (Hop Limit) de IPv6 y decrementado en una unidad.
- Protocolo: se copia de la cabecera Next header de IPv6.
- Encabezado Checksum: calculado una vez que la cabecera IPv4 ha sido creada.

La traducción de direcciones en sentido inverso se ilustra en la figura 5.2. La traducción de los campos es directa excepto en el caso de paquetes que requieran fragmentación. Este tipo de paquetes tiene que ser fragmentado antes de aplicar el algoritmo SIIT. En la dirección IPv4 a IPv6, los campos de cabecera quedan como sigue:

- Versión: 6
- Clase de Tráfico: se copia de los 8 bits del campo Tipo de Servicio IP y Precedente.
- Etiqueta de Flujo: valor del campo Longitud Total de IPv4 menos el tamaño de la cabecera IPv4 y las opciones IPv4, si están presentes.
- Siguiente Encabezado: copiado el campo Protocolo de la cabecera IPv4.
- Límite de saltos: valor copiado del Tiempo de Vida de la cabecera IPv4 decrementado en una unidad.

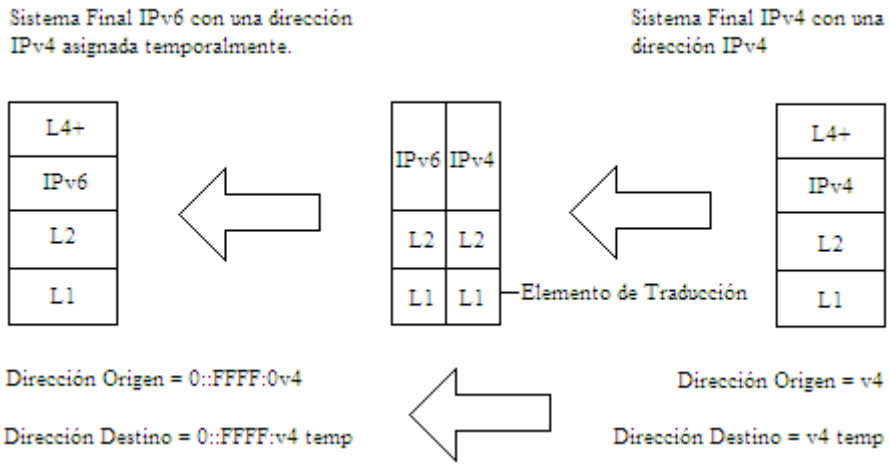

Figura 5.2 Traducción de Direcciones IP, IPv4 a IPv6 (L =Layer, Capa).

5.1.2 Traducción ICMP

Debido a las diferencias entre ICMPv4 e ICMPv6, ICMP es el único protocolo de nivel superior que tiene que ser manejado por SIIT. El protocolo ICMPv4 se ilustra en la figura 5.3. El campo Tipo (Type) indica el tipo de mensaje ICMPv4, y el campo Código (Code) se usa para proporcionar información adicional asociada al mensaje. Traducir los distintos tipos de mensajes a ICMPv6 supone lo siguiente:

Para todas las traducciones, el campo Checksum debe ser recalculado porque ICMPv6, como TCP y UDP, emplea una suma de verificación de pseudocabecera. Al traducir los mensajes a ICMPv6 supone lo siguiente:

- Solicitud de llamada y Solicitud de Respuesta (Echo Request y Echo Replay - tipos 0 y 8) se traducen a los tipos 128 y 129.

- Destino inalcanzable (Destination Unreacheable - tipo 3) se traduce al tipo 1. En el RFC se puede encontrar las traducciones del campo Code además de las del campo Tipo (Type).
- Fuente de Interferencia (Source Quench – tipo 4) se considera obsoleto en ICMPv6 porque no se utiliza en la actualidad.
- Redireccionamiento o cambio de ruta (Redirect - tipo 5) se ha eliminado porque sólo es válido en un único salto.
- Tiempo excedido (Time Exceded - tipo 11) se traduce al tipo 3.

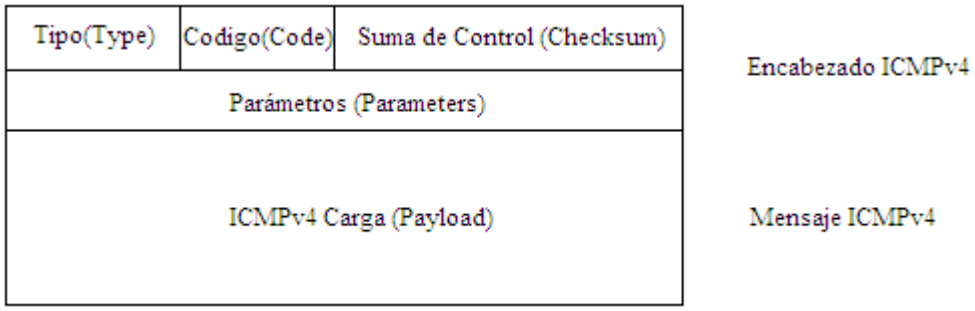

Figura 5.3 Protocolo ICMP

5.2 BIS

Bump in the Stack – Paquete en la pila es una variante de SIIT que realiza la traducción al final del sistema, esta traducción ocurre en la capa IP y permite que las aplicaciones de origen IPv4 puedan comunicarse con destinos IPv6, siempre que éstos estén ejecutando BIS.

BIS es un mecanismo de doble pila que inserta módulos entre el controlador de interfaz de red y el módulo IPv4, estos módulos “observan” el flujo de datos entre la capa IP y la capa 2 del modelo OSI, en la figura 5.4 se muestra la arquitectura BIS.

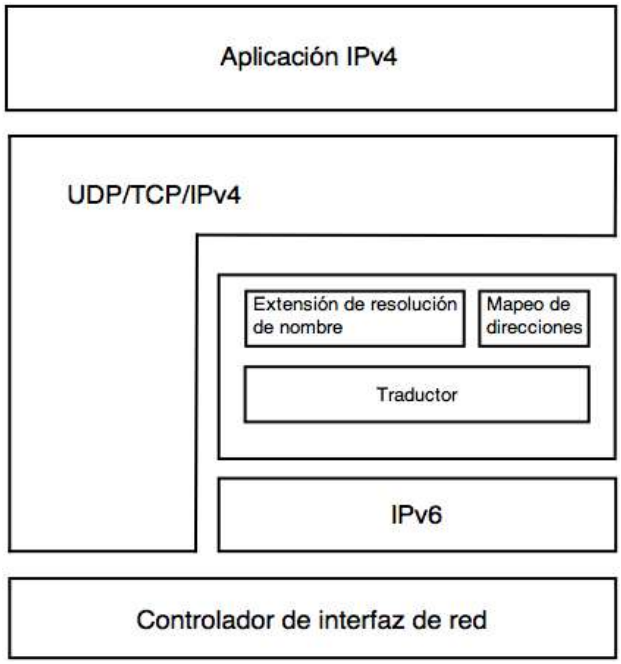

Figura 5.4 Arquitectura BIS.

5.2.1 Elementos BIS

a) Traductor

Traduce las direcciones IPv4 en IPv6 y viceversa usando el mecanismo definido en SIIT.

Cuando se recibe un paquete IPv4 de aplicaciones IPv4, se convierten las cabeceras de los paquetes IPv4 en cabeceras IPv6, se fragmentan los paquetes y se envían hacia la red IPv6. Si se reciben paquetes IPv6 de una red IPv6, el proceso es simétrico, en este caso no es necesario fragmentar los paquetes.

b) Extensión de resolución de nombre

Este módulo asegura que hay una dirección IPv4 asociada con el destino, incluso la aplicación reside en un nodo IPv6. La aplicación IPv4 en el BIS necesita una dirección tal que le permita comunicarse a la API con la capa TCP.

Una aplicación envía una consulta al DNS para resolver las direcciones con registro ‘A’ para el nombre del nodo de destino. Después de verificar la consulta se crea una consulta para resolver ambos registros ‘A’ y ‘AAAA’ para el nombre del nodo.

c) Mapeo de direcciones

El Módulo mantiene la lista de direcciones IPv4 asociadas con direcciones IPv6 que fueron devueltas por el módulo "resolución de nombre" mediante la consulta a un DNS.

Cuando se realiza una solicitud para asignar una dirección IPv4 que corresponde a una dirección IPv6, se elige y devuelve una dirección IPv4 para que sea registrada dentro de una tabla dinámica.

El registro de direcciones ocurre de las siguientes dos maneras:

1) Cuando el sistema de resolución coloca sólo un registro 'AAAA' para el nombre del nodo destino y no hay una referencia para la dirección IPv6.
2) Si el traductor recibe un paquete IPv6 y no hay una referencia para la dirección origen IPv6.

El flujo de información en BIS se da de la siguiente manera y se muestra en la figura 5.5.

1) La aplicación de IPv4 hace una petición para obtener la dirección IPv4 destino.
2) El sistema de resolución de nombres recibe la petición y solicita la dirección IPv4 e IPv6 destino.
3) El DNS devuelve la dirección IPv6 del destino.
4) El sistema de resolución solicita y recibe las direcciones IPv4 de los registros administrados por el mapeo de direcciones. El mapeo de direcciones mantiene los registros de las direcciones IPv4 – IPv6.
5) El sistema de resolución devuelve la dirección IPv4 de la aplicación IPv4 que se usará para comunicaciones posteriores.
6) El traductor recibe los paquetes IPv4 de la aplicación.
7) El traductor solicita la dirección IPv6 asociada con las direcciones IPv4 que están contenidas en la cabecera del paquete y realiza la traducción de IPv4 a IPv6
8) El paquete es enviado al destino con una dirección IPv6.

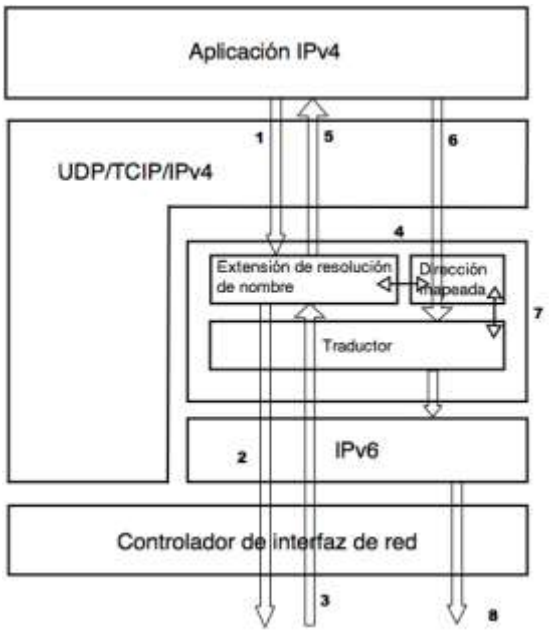

Figura 5.5 Flujo de la Información en BIS

5.3 BIA

BIA (Bump in the API – paquete en la API) opera de manera similar a BIS, con la excepción de que la traducción ocurre en las capas superiores del protocolo. El propósito principal de BIA es el mismo que BIS, permitir que las aplicaciones IPv4 puedan comunicarse con los nodos IPv6 sin realizar modificaciones de las aplicaciones IPv4.

BIA inserta un traductor API entre el Socket y el módulo TCP/IP (figura 5.6).

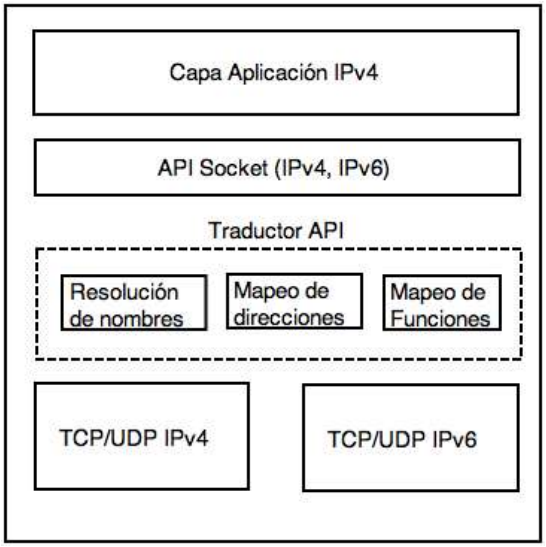

Figura 5.6 Traductor API

El flujo de una aplicación IPv4 en un nodo BIA que debe comunicarse con un nodo IPv6 es de la siguiente manera:

1) Cuando una aplicación envía una petición DNS, el sistema de resolución de nombres intercepta la petición.

2) El sistema de resolución de nombres agrega una nueva consulta para resolver los registros A y AAAA.

3) Un registro AAAA se resuelve para obtener la dirección de un nodo IPv6.

4) El sistema de resolución de nombres solicita una dirección mapeada IPv4 para asignarla a una dirección IPv6.

5) El sistema de resolución de nombres crea un registro A para la asignación de dirección IPv4 y lo devuelve a la aplicación IPv4.

6) Para la aplicación IPv4 se envía un paquete IPv4, éste hace una llamada al socket de la API de IPv4.

7) El *mapeo de funciones* detecta la función del socket de la API de las aplicaciones. En el caso de una aplicación IPv4, el *mapeo de funciones* solicita la dirección IPv6 del *mapeo de direcciones* asociada con la dirección IPv4 advertido en la función de llamada.

8) Usando la dirección IPv6, el *mapeo de funciones* invoca una "llamada a una función API socket IPv6" correspondiente a una "llamada a una función API socket IPv4"

5.4 TRT

Transport Relay Translation – Traductor de transporte de transmisión, es una de las varias técnicas de traducción que ayuda a que pueda haber comunicación entre los protocolos IPv4 con IPv6, TRT propone una traducción con una adaptación sencilla con respecto a los demás, esto se refleja en que no requiere demasiadas modificaciones en los nodos donde se implemente.

La técnica de transmisión de transporte no es nueva, se ha utilizado en varios sistemas relacionados con los firewalls, estos sistemas están diseñados para lograr lo siguiente:

- Prevenir el envío de ciertos paquetes IP a través del sistema.
- Permitir el tráfico que va a través del sistema

A TRT se le ha reservado el prefijo IPv6 C6:: /64, por lo que en la misma dirección IPv6 puede contener una dirección IPv4

La información de encaminamiento debe ser configurada para que los paquetes C6::/64 puedan ser enviados hacia el sistema TRT, además el prefijo fec0:0:0:1:/64 está reservado para mapeo de direcciones. Por ejemplo:

- Se considera un nodo destino IPv4 "exclusivo" y un nodo inicial IPv6 "exclusivo".
- Cuando un nodo origen con una dirección IPv6 desea realizar una conexión con un nodo destino con una dirección IPv4, éste necesita realizar una conexión TCP/IPv6.
- Si la dirección de C6::/64 es igual a fec0:0:0:1::/64 y la dirección destino 10.1.1.1, la dirección destino que se usará es fec0:0:0:1::10.1.1.1.
- El paquete es enviado a través del sistema TRT, el sistema captura el paquete y obtiene la dirección destino verificando los primeros 32 bits de la dirección destino para obtener la dirección real IPv4, y el paquete se envía a su destino.

TRT captura los paquetes donde termina la red IPv6, éste utilizará los primeros 32 bits del paquete original IPv6 para enviarlo sobre la red IPv4. El procedimiento es el mismo para las comunicaciones UDP (Figura 5.7).

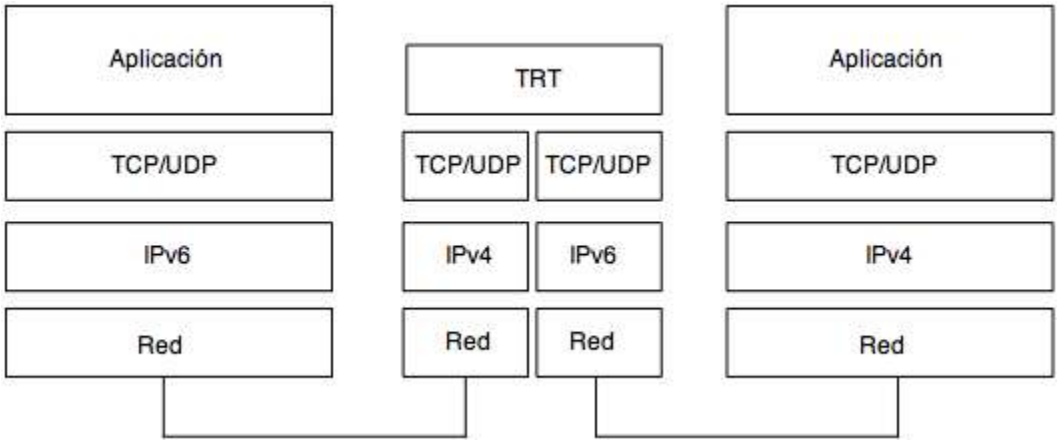

Figura 5.7 Procedimiento TRT

Las ventajas de TRT son las siguientes:

- Algunos mecanismos de traducción requieren de modificaciones adicionales en los nodos IPv6 "exclusivos" limitando las posibilidades de despliegue, por su diseño, TRT no requiere de modificaciones adicionales
- Las técnicas de conversión de cabeceras IPv6 a IPv4 deben tratar el MTU así como la fragmentación, TRT no tiene estos problemas.

Algunas desventajas de TRT:

- TRT soporta sólo tráfico bidireccional, por lo que la traducción de las cabeceras IPv6 a IPv4 debe soportar otros
- Se necesita código necesario para el transporte de protocolos inéditos NAT incluyendo IPsec no pueden cruzar un sistema TRT

Otro beneficios que hay con la implementación TRT es la configuración de MTU ya que se puede decidir el PMTU[19] independientemente del tráfico entre ambas tecnologías.

5.5 NAT-PT

NAT-PT RFC 2766 [Cn] (Network Address Translation – Protocol Translation / Traducción de Direcciones de Red – Protocolo de Traducción) es un mecanismo similar al de NAT IPv4; NAT IPv4 traduce una dirección IPv4 en otra. En este caso la traducción es entre una dirección IPv4 y una dirección IPv6. NAT-PT utiliza un conjunto de direcciones IPv4 que son asignadas a los nodos IPv6 de forma dinámica tan pronto como se inician las sesiones entre los límites de las redes y actúa como un proxy de comunicación para los nodos "sólo IPv6" que se comunican con pares IPv4. Una ventaja de NAT - PT es que no exige ningún cambio a los hosts existentes porque todas las traducciones NAT - PT se llevan a cabo en el dispositivo específico NAT - PT.

NAT - PT se diferencia del algoritmo SIIT en los siguientes aspectos: el algoritmo SIIT se basa en que a los nodos IPv6 se les asignan direcciones IPv4 para propósitos de comunicación con nodos IPv4. Con la dirección IPv4 se construye la dirección IPv6 especial "IPv6 traducida", que desde luego se utiliza para la función de correspondencia en el dispositivo de traducción de la red. NAT - PT usa el algoritmo SIIT de traducción de la cabecera IP para la mayoría de los campos de la cabecera, pero más que asignar una dirección IPv4 al nodo "sólo IPv6" para utilizarlo en una dirección especial, usa una colección de direcciones públicas IPv4 asignadas dinámicamente en el dispositivo NAT - PT a medida que se inician sesiones entre nodos "sólo IPv4" y nodos "sólo IPv6". Se mantiene una tabla en el dispositivo con las correspondencias establecidas entre las

[19] PMTU - Path MTU. Determina el tamaño mínimo de MTU a lo largo de una trayectoria.

direcciones. NAT-PT tiene la ventaja de no necesitar cambios en los sistemas finales pero es "con estado" por lo que es imprescindible el dispositivo NAT - PT para rastrear las sesiones activas. Todos los diagramas IP de entrada y salida en una sesión tienen que ser encaminados a través del dispositivo NAT - PT.

Además de la traducción de direcciones, el RFC define NAPT-PT (Network Address Port Translation - Protocol Translation / Traducción de Puertos en Direcciones de Red – Protocolo de Traducción), que permite la multiplexación de múltiples sesiones en una única dirección IPv4 mediante el uso del campo "port" en protocolos de capas superiores como TCP y UDP. Esto es similar a la multiplexación de puertos en entornos IPv4 (RFC 2663) [Co].

El sistema de traducción NAT - PT. Asume lo siguiente:

- El sistema final IPv6 está en la misma subred que el dispositivo NAT - PT y utiliza una dirección de enlace local FECD:BA98::7654:3210 cuando se comunica con el dispositivo NAT - PT.

- La sesión es establecida por el sistema final IPv6.

- El dispositivo NAT - PT tiene una colección de direcciones, incluida la subred 120.130.26.0/24, para asignar a las direcciones IPv6 de origen entrantes, en este caso, la dirección de enlace local anterior.

- El dominio IPv6 tiene asignado un prefijo PREFIJO::/96, y el sistema final IPv6 usará este prefijo cuando se direccione el nodo IPv4 en un formato IPv6. Los paquetes IPv6 con este prefijo serán encaminados al dispositivo NAT - PT. La dirección de destino resultante es PREFIJO::v4, en donde v4 es la dirección IPV4 del sistema final IPv4.

Cuando se establece una sesión desde un nodo "sólo IPv6" a un nodo "sólo IPv4", el nodo IPv6 conocerá la dirección IPv4 del nodo de destino mediante una consulta DNS. Este flujo de información se detalla en la figura (5.8). Cuando la sesión se inicia, el nodo IPv6 creará un paquete con lo siguiente:

- Dirección IPv6 de origen: FECD:BA98::7654:3210

- Dirección IPv6 de destino: PREFIJO:: 132.146.243.30

En la recepción del paquete, el dispositivo NAT - PT asignará una de las direcciones IPv4 con que cuenta y esta dirección se usará como dirección origen al encaminar el paquete hacia el nodo IPv4. El paquete traducido resultante dispondrá de:

- Dirección IPv4 de origen: 120.130.26.10, asignada de la colección de direcciones IPv4.

- Dirección IPv4 de destino: 132.146.243.30, la dirección IPv4 del sistema final IPv4

Esta correspondencia IPv6 a IPv4 se mantiene mientras dura la sesión. Precisamente con base en que esta asociación de direcciones perdura, el tráfico de retorno será reconocido por el dispositivo NAT - PT en tanto pertenezca a la misma sesión. Como NAT - PT guarda el estado de la traducción, cada sesión debe ser enrutada a través del mismo dispositivo NAT - PT.

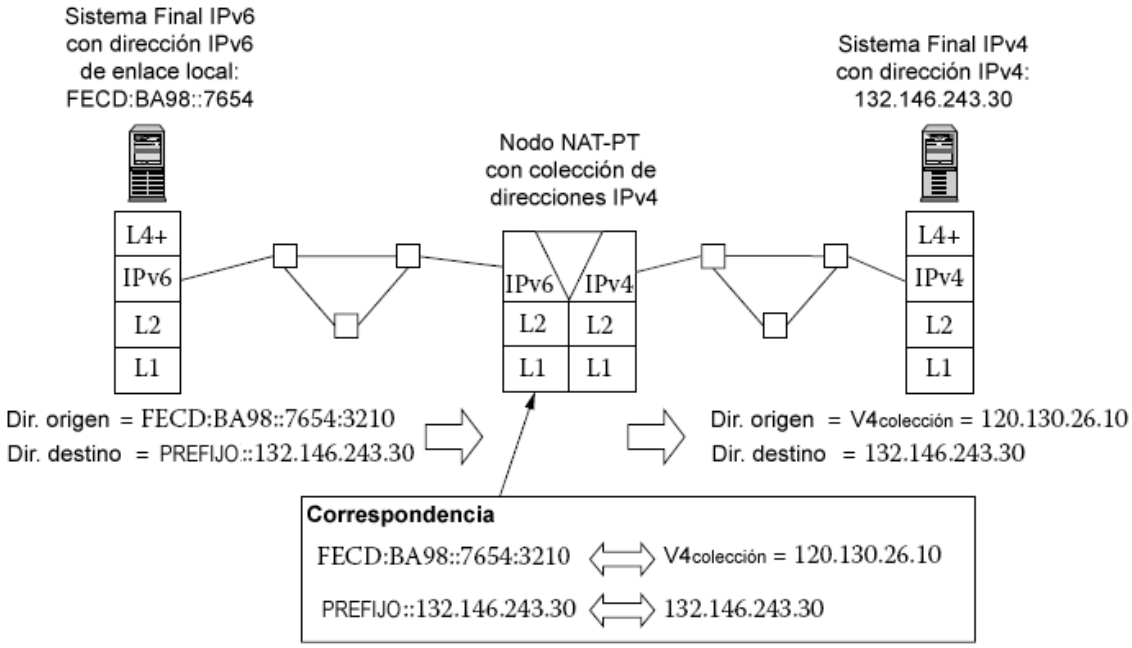

Figura 5.8 Flujo de información NAT-PT [AMOSS 2008]

Conclusión

CONCLUSIÓN

Hoy en día cualquier tipo de noticia, acontecimiento, suceso o difusión de información se realiza mediante Internet, los demás medios de comunicación como la televisión, el radio y el periódico se han visto forzados a adaptarse al cambio de velocidad del flujo de la información en el mundo. La diferencia principal de este cambio se debe a que en los medios de comunicación anteriores existe alguien o algo que difunde la información y los demás sólo la reciben, este tipo de interacción no permite que todos los integrantes dentro de un mismo canal de comunicación participen activamente complementando, corrigiendo o aportando nueva información.

Internet ofrece la posibilidad de que cualquier persona pueda compartir infinidad de información, intercambiar ideas, investigar y crear, pero para llegar a este punto en el que todos podemos tener acceso a esta enorme red, tuvieron que pasar varios años y la tecnología tuvo que evolucionar, esta evolución continuará con el cambio de IPv4 a IPv6 es fundamental para nuestra sociedad entender esta evolución y los medios existentes para realizarla.

Este trabajo pretende ayudar a entender el origen de Internet, su evolución actual y los medios de transición que ayudarán a que el cambio de protocolo de IPv4 a IPv6 suceda además de la gran oportunidad de crecimiento que esto representa para la sociedad.

Se revisaron las ventajas tecnológicas del protocolo IPv6 sobre el protocolo IPv4, la mayor capacidad de direccionamiento, la reducción de costos a causa de la seguridad implementada, un enrutamiento más eficiente ayudándonos a entender su funcionamiento así como comprender cuáles son las limitantes pudiendo tener una opinión más certera de cuáles son las recomendaciones para afrontar los cambios que se tienen que realizar.

Esta investigación responde las preguntas ¿Por qué la necesidad de cambiar de protocolo IPv4 a IPv6? y ¿Cuáles son los motivos que impulsan este cambio? Al intentar responderla, nos podemos referir no sólo a los tecnicismos sino al por qué se tienen que desarrollar estas nuevas mecánicas, metodologías y técnicas, argumentos que demuestran la necesidad de la ingeniería a la búsqueda de las nuevas tecnologías para crear nuevas técnicas nacidas a partir de las necesidades de toda una sociedad.

Encontramos que las causas principales que promueven este cambio de protocolo (de IPv4 a IPv6) que no fueron en su tiempo previstas al crear IPv4 son las siguientes:

- El crecimiento veloz de dispositivos y el termino de direcciones de IPv4.
- La necesidad de una configuración más simple.
- La importancia de una capa de seguridad
- La entrega de datos en tiempo real.

IANA asignaba direcciones IPv4 a los RIR en bloques que equivalen a la 256va parte del espacio total de direcciones IPv4. Cada bloque es denominado un "/8" o "barra 8". A primera hora del 3 de febrero, Leo Vedoga, gerente de Recursos Numéricos de IANA, anunciaban en las listas técnicas de correo electrónico la extinción de los bloques libres unicast IPv4. "Este es un día histórico en la vida de Internet,, y que hemos estado esperando desde hace bastante tiempo", afirmo Raúl Echeberría, director Ejecutivo de Lacnic y presidente de NRO "El futuro de Internet está en IPV6. Se terminaron las direcciones IPv4 del stock Central de IANA y desde ahora todos los tomadores de decisiones deberán realizar acciones concretas para adoptar IPv6 en sus organizaciones". [J]

Señalamos la importancia del protocolo TCP/IP como base en el funcionamiento de Internet que ayudó a cumplir en su momento las necesidades de comunicación existentes y que su arquitectura permitió desarrollar muchas aplicaciones.

La necesidad de poder comunicarse en un medio común dio origen al modelo OSI que es muy similar al protocolo TCP/IP pero pone énfasis en la capa de aplicación, distribuyéndola en más capas que permitirían en el futuro implementar de manera más fácil y entendible las aplicaciones desarrolladas en cualquier parte del mundo, es importante remarcar que la simplicidad y la estandarización del modelo permitió que Internet estuviera preparado incluso para aplicaciones que no estaban previstas en sus inicios.

Ya que revisamos los inicios de Internet, los motivos de su creación, la simplicidad de su arquitectura que permitió unificar la comunicación entre las diferentes redes del mundo, entendimos que el Protocolo de Internet (IP) es una pieza fundamental en las dos arquitecturas, que su funcionamiento contempla el direccionamiento, el enrutamiento y la fragmentación, características imprescindibles que permiten que el flujo de la información exista y que la comunicación se lleve a cabo sin importar qué datos sean transferidos.

Desglosamos por completo las características de IPv4, explicamos que existen las clases de direcciones A, B, C, D y E y para qué sirven, describimos el uso de las mascaras de red y la estructura interna de un paquete de datos en IPv4. Aprendimos que todo paquete en IPv4 comienza con una cabecera, ésta cuenta con 13 campos de los cuales 12 son de carácter obligatorio ya que dentro de estos campos se especifican parámetros como el destino del paquete, longitud, así como información vital para que sea recibido el paquete satisfactoriamente por el destinatario correcto. En realidad aunque teníamos idea de cómo está integrada una cabecera IPv4 no nos imaginábamos la cantidad de opciones que la conformaban.

Bajo todo el contexto anterior y el conocimiento sobre el origen de Internet, las bases que llevaron a su creación, los motivos y necesidades que llevaron a desarrollarla, las arquitecturas fundamentales TCP / IP y OSI y el completo entendimiento del protocolo IP

así como en versión IPv4, nos planteamos y contestamos la pregunta de por qué el cambio de protocolo.

Encontramos que la primera respuesta clara y decisiva que existe para cambiar de protocolo se debe al crecimiento de la población y de dispositivos que son capaces de integrarse a una red, es simple el protocolo IPv4, permite 4 294 967 296 direcciones y aunque existen técnicas para poder utilizar más direcciones, esta cantidad de direcciones ya no es suficiente para abastecer la demanda.

La comunicación privada que viaja a través de un medio público como lo es Internet y en donde todo mundo tiene la posibilidad de acceder a la información necesita de servicios criptográficos que permitan proteger los datos transmitidos evitando que sean vistos o modificados, existen protocolos como el IPsec (Internet Protocol security - Seguridad en el Protocolo de Internet) que proporcionan estos servicios pero no son obligatorios, lo que hace vulnerable al servicio.

Explicamos que en la actualidad podemos ver aplicaciones, actualizaciones, juegos, programas, servicios médicos, servicios del gobierno, escuelas que necesitan de una gran cantidad de transmisión de datos para que su comunicación sea en tiempo real y sin interrupciones, independientemente de la calidad, estado y administración de las redes que tenemos en el país, llegar á el momento en el que el protocolo IPv4 sea un embudo para la trasmisión de datos.

Pudimos identificar que el cambio de protocolo IPv4 a IPv6 no sólo depende del factor tecnológico sino también del factor económico y social en el que se encuentra la región en donde se decida realizar el cambio, el cambio será paulatino pero debe ser empujado por las organizaciones tecnológicas encargadas de promover los temas relacionados a Internet y los gobiernos de los países.

Existen grandes corporaciones como bancos, aseguradoras e instituciones gubernamentales en donde la actualización de la tecnología implica tiempo y costo que a corto plazo no se ve como una “inversión”, incluso se puede llegar ver como un gasto no justificado debido a que las empresas prestan servicios que utilicen de manera activa Internet.

El mejor camino a seguir para poder adoptar esta tecnología y sacarle provecho involucra al sector gubernamental y al educativo, se deben promover proyectos en donde se refleje claramente el beneficio del uso de IPv6 orientados a la sustitución de actividades actuales realizadas con IPv4 dentro de grandes instituciones gubernamentales, este tipo de proyectos ayudarían a promover de manera eficiente entre las grandes corporaciones el protocolo IPv6.

Las aplicaciones y servicios que utiliza Internet empezarán a empujar más la necesidad de una mayor y eficiente transmisión de datos, además la cantidad de usuarios se incrementa con el tiempo, estas actividades ayudarán a promover la migración del protocolo de IPv4 a IPv6, pero esto no será de un día a otro, seguramente se buscarán otras opciones antes de tener que invertir en el cambio, ese momento es una gran área de oportunidad para todos aquellos que nos dedicamos a las actividades relacionadas a las tecnologías de la información, si logramos realizar aplicaciones funcionales al momento de que el cambio paulatino ocurra, tendremos la posibilidades de crear actividades económicas rentables.

Lógicamente no sólo obtendríamos un beneficio económico, con un alto dominio de la tecnología se podría atraer, intercambiar o crear nuevo conocimiento con más gente del mundo, además adelantarnos a estas prácticas sería un reflejo de que podemos aprender de la historia puesto que aquellos individuos en sociedades que saben aplicar por adelantado un conocimiento aplicado a la tecnología se ven beneficiados enormemente.

Bajo todo el contexto anterior de la necesidad del cambio de protocolo ya sea por necesidades económicas, sociales o tecnológicas dejamos claro los motivos por los cuales este cambio se dará paulatinamente, determinamos que es una buena oportunidad para México de elevar su entorno tecnológico e intelectual.

Ya que identificamos las necesidades, empezamos a desglosar las características de IPv6 y la manera en que mejora el protocolo anterior que es IPv4.

Determinamos que IPv6 cuenta con direcciones más largas de tener un número formado por 32 bits (4,294,967,296 direcciones en IPv4) pasa a tener un número formado por 128 bits (aproximadamente 340 sextillones de direcciones) esto cuadruplica el tamaño de bits para generar cada dirección viéndose beneficiada la cantidad de direccionamiento que IPv6 puede soportar.

Referimos la importancia de que IPv6 sea capaz de soportar IPv4, esto se debe a que en muchas ocasiones la migración de las redes será de una manera inadecuada y tal vez forzada por las instituciones, hay que recordar que en la actualidad existen redes que están muy mal administradas que trabajan sobre IPv4, también es una buena oportunidad para

estas instituciones poner orden en sus redes claro, siempre y cuando estén dispuestas a invertir de manera adecuada sus recursos.

Encontramos que el formato de encabezado de IPv6 pasa a ser de 40 bytes, el doble del tamaño con el que cuenta IPv4 que es de 20 bytes, esta cabecera trae como mejoras la optimización en el envío de paquetes a través de la red ya que se procesa con mayor rapidez.

La seguridad dentro de IPv6 es más amplia y consta del protocolo IPSec (Internet Protocol Security – Seguridad en el Protocolo de Internet) tiene como finalidad proteger paquetes IP mediante el uso de algoritmos de cifrado así como la autenticación, garantizando comunicaciones privadas y seguras. Las funciones que realiza son la autenticación de datos, la integridad de datos, la confidencialidad de datos y la protección de reproducción.

A nivel internacional definimos las tareas que se tratarán de realizar para difundir el uso del nuevo protocolo, la sincronización global, un anuncio de la fecha de extinción de las direcciones IPv4, prometer no hacer políticas muy estrictas para las direcciones IPv4 restantes y los problemas relacionados con el reciclaje de las IPv4, estas medidas puede que parezcan no ser muy importantes o que sean reglas dictatoriales que nadie va a respetar pero su importancia radica en dar un inicio formal en el cambio de protocolo.

Presentamos las tareas que las distintas potencias del mundo tomarán para promover la actualización del protocolo, estas actividades se agrupan en acciones para manejar la adopción del nuevo protocolo mediante mandatos gubernamentales, el patrocinio de la adopción y el patrocinio para Investigación Nacional. Como ya mencionamos, para el caso de México existe la posibilidad de que estas iniciativas se den debido a la influencia de Estados Unidos pero debemos tomar este proceso como una muy buena oportunidad de nivelar la dependencia y entablar relaciones con otros países que nos permitan crecer, en este caso en el rublo tecnológico.

Ya que describimos las características de los dos protocolos (IPv4 e IPv6) las diferencias y las mejoras que se establecieron, los puntos no tecnológicos necesarios para el patrocinio del uso de esta tecnología comenzamos a describir aquellos mecanismos que nos permitirán realizar paulatinamente esta gran migración.

La intención de este trabajo para esta parte es mostrar una referencia clara y rápida de todas las posibilidades con las que se cuenta para poder empezar a realizar la migración de protocolo o la convivencia de los dos protocolos en la misma red o el uso de sólo IPv6, la posibilidad de situaciones referidas a una migración en una red son muy grandes porque depende de mucho factores que pueden ir desde una mala administración de la red hasta falta de conocimiento, lo importante de este trabajo es conocer las tecnologías que permitan esta migración para poder tomar la que mejor se adapte al caso en el que nos encontremos y puede suceder que hasta se deba manejar más de un método o adaptarlo a una red

El primer paso y lógico a entender es que las redes IPv4 e IPv6 en un principio van a coexistir, de esta manera definimos tres mecanismos, el diseño de una arquitectura para el uso de ambos protocolos simultáneamente, túneles para el envío de paquetes y mecanismos de traducción de direcciones. Con estas 3 técnicas podemos tener una base que nos permita iniciar nuestra migración.

Este trabajo cuanta con la información básica para servir como una referencia para la construcción de proyectos donde se pretenda migrar una red IPv4 a IPv6, nos da una idea clara del alcance de los mecanismos y las necesidades que podemos cubrir para cada caso en el que se necesite utilizar el protocolo IPv6, desglosamos y definimos claramente las características de cada protocolo y planteamos las necesidades por las cuales el protocolo IPv4 está dejando de ser una opción viable a futuro para la transmisión de datos en Internet. Se pretende ser una guía de partida para el uso de los mecanismos de transición de IPv4 a IPv6.

GLOSARIO

3DES Este algoritmo realiza triple cifrado DES, fue desarrollado por IBM en 1978.

6OVER4 Es un mecanismo de transición de IPv6 para transmitir paquetes IPv6 entre nodos con doble pila sobre una red IPv4 con multicast habilitado. IPv4 se utiliza como un nivel de enlace virtual (Ethernet virtual) sobre el que se debe ejecutar IPv6.

APNIC (Asia Pacific Network Information Centre – Centro de Información de Red Asia Pacífico). APNIC es uno de los 5 Registros regionales de Internet que se encuentran operando en el mundo, provee servicios de asignación y registros.

ARPA (Advanced Research Projects Agency – Agencia de Investigación de Proyectos Avanzados) Agencia del departamento de defensa de los Estados Unidos responsable del desarrollo de nuevas tecnologías para uso militar.

BROADCAST (Difusión) Es un modo de transmisión de datos a donde una sola transmisión es recibida por múltiples receptores.

CIDR (Classless Inter-Domain Routing – Enrutamiento Inter-Dominios sin clase). Método para la clasificación de direcciones IP útil para dividir segmentos de red según las necesidades para la administración de una red, está definida en el RFC 4632 [Cp].

CNGI (China Next Generation Internet). Proyecto iniciado por el gobierno chino con el propósito de tener una posición importante en el desarrollo de la adopción de la tecnología IPv6

DES (Data Encryption Standard – Estándar de cifrado de datos). Algoritmo de cifrado desarrollado por IBM, trabaja sobre bloques de 128 bits teniendo una clave de igual longitud, se basa en operaciones lógicas booleanas.

DHCP (Dynamic Host Configuration Protocol - Protocolo Configuración Dinámica de Anfitrión) Protocolo de red de computadoras que permite a los clientes obtener Parámetros de configuraciones específicas así como un mecanismo para la asignación de direcciones IP, se encuentra definido en el RFC 2131 [Cq].

Dirección/Puerto "ensombrecido". Una dirección o un puerto adquieren el nombre de dirección/puerto ensombrecidos ya que se encuentran modificados mediante el uso de la operación binaria XOR.

DNS (Domain Name System – Sistema de Nombre de Dominio) Es un sistema de nomenclatura jerárquica para computadoras, básicamente es una base de datos distribuida que almacena información asociada a nombres de dominio en redes como Internet, está formalmente definido en el RFC 1034 [Cr].

DUID (DHCP Unique Identifier) Cada componente DHCP tiene un DUID el cual es usado para identificar el dispositivo que está intercambiando mensajes DHCPv6.

Encaminamiento o Enrutamiento. Proceso mediante el cual se busca el mejor camino entre dos puntos, el mejor camino se calcula usando algoritmos de encaminamiento.

ESP (Carga Útil de Seguridad Encapsulada). Protocolo de seguridad que pertenece a la suite de IPsec, proporciona confidencialidad de los datos y de manera opcional la autenticación, integridad y seguridad contra la reproducción de la información.

FLAGS (Banderas) Campo que puede contener los valores DF (Don't Fragment), MF (More Fragments) y ZERO que es reservado para indicar si un paquete está fragmentado o no, se utiliza cuando un paquete IPv6 está encapsulado en un paquete IPv4.

FRAGMENT OFFSET Indica la posición (en múltiplos de 8 octetos) que ocupa en el datagrama original el primer octeto de los datos transportados por el fragmento. Cuando una estación destino recibe el último fragmento (bit M=0) de un datagrama original, ella calcula la longitud que tienen los datos en el datagrama original mediante los valores de los campos Fragment offset, Header Length y Total Length del último fragmento (El valor del campo Total Length en cada fragmento hace referencia a la longitud total de dicho fragmento).

FTP (File Transfer Protocol - Protocolo de Transferencia de Archivos) Es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

GDP (gross domestic product – producto doméstico bruto) Es el valor monetario total de la capacidad para adquirir productos y hacer gastos en el hogar.

HMAC (keyed-Hash Message Authentication Code). Provee mecanismos para la integridad de la información transmitida que requiere de funciones criptográficas mediante una función hash definida en el RFC 2104 [Cs], existen funciones que se han implementado como SHA o MD5.

HOST ISATAP Es un dispositivo de red (comúnmente una computadora) que tiene una interface de túnel ISATAP y que ejecuta su propio túnel hacia otros hosts ISATAP sobre la misma subred.

HTML (HyperText Markup Language/Lenguaje de Marcado de Hipertexto) Es un lenguaje pensado para la elaboración de páginas web. Es usado para describir la estructura y el contenido en forma de texto, así como para complementar el texto con objetos tales como imágenes. HTML se escribe en forma de "etiquetas", rodeadas por corchetes angulares.

IANA (Internet Assigned Number Autority - Autoridad de asignación de números en Internet) Es la entidad encargada de coordinar algunos elementos de Internet,

específicamente almacena códigos y los sistemas de numeración únicos que se utilizan en los estándares técnicos (“protocolos”) http://www.iana.org/about/

ICMP (Internet Control Message Protocol – Protocolo de Mensajes de Control de Internet) Subprotocolo de diagnóstico y notificación de errores del protocolo de Internet, es utilizado para enviar mensajes de errores cuando un servicio no está disponible o un host no puede ser encontrado.

ICMP (ROUTER DISCOVERY) Internet Router Discovery Protocol (IRDP) utiliza mensajes ICMP "Router Advertisement" y "Router Solicitation" para permitir a un nodo descubrir la dirección de Routers operacionales en una subred.

ICT (information and communications technology – tecnologías de la comunicación y la información). Se refiere a las ciencias, tecnologías y negocios implicados en el manejo de la información y comunicaciones.

ICV (Integrity Check Value – Valor de Comprobación de Integridad). Mecanismo para garantizar la integridad de la información mediante una implementación de un código.

IETF (Internet Engineering Task Force, en español Grupo de Trabajo en Ingeniería de Internet) Es una organización internacional abierta de normalización que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, tales como transporte, encaminamiento, seguridad. Fue creada en Estados Unidos en 1986.

IP (Internet Protocol/Protocolo de Internet) Es un protocolo primario en la capa de internet dentro de la Suite del Protocolo de Internet utilizado por el origen y destino para la comunicación de datos a través de una red de paquetes conmutados. Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o datagramas.

IPsec (Internet Protocol security). Conjunto de protocolos cuya finalidad es ofrecer servicios de seguridad en las comunicaciones sobre el protocolo de Internet ofreciendo autenticación, confiabilidad e integridad de los paquetes.

MAC (Media Access Control – Control de Acceso al Medio) es un identificador de 48 bits que es asignado a los adaptadores de red o a las tarjetas de interface de red, su configuración está dada por el fabricante (los primeros 24 bits) y por el IEEE (los últimos 24 bits), trabaja en la capa 2 del modelo OSI y son únicas a nivel mundial.

MD5 (Message-Digest algorithm 5). Ampliamente utilizado con la funciones de criptografia Hash.

MIT Instituto Tecnológico de Massachusetts (Massachusetts Institute of Technology) Es una de las principales instituciones dedicadas a la docencia y a la investigación en Estados Unidos, especialmente en ciencia, ingeniería y economía. El Instituto está situado en

Cambridge, Massachusetts, y cuenta con numerosos premios Nobel entre sus profesores y antiguos alumnos. MIT es considerado como una de las mejores universidades de ciencia e ingeniería del mundo.

MTU (Maximum Transmission Unit) Establece el tamaño máximo en bytes que puede enviarse en un paquete a través del Protocolo de Internet.

MULTICAST (Multidifusión) Es una tecnología de red para el envío de información a un grupo de destinos de manera simultánea, utilizando la estrategia más eficiente para el envío de mensajes sobre cada enlace sólo una vez.

NAT (Network Address Translation - Traducción de Dirección de Red). Es un mecanismo que forma parte de una red el cual traduce una dirección IP privada a una IP pública y viceversa, es una de las soluciones que se dio ante el agotamiento de direcciones de la tecnología IPv4, se encuentra definida en el RFC 2663 [Co].

NEIGHBOR DISCOVERY (descubrimiento de vecinos): Es un mecanismo con el cual un nodo que se acaba de incorporar a una red, descubre la presencia de otros nodos (vecinos) en el mismo enlace, además de ver sus direcciones IP. Este protocolo también se ocupa de mantener limpios las cachés donde se almacena la información relativa al contexto de la red a la que está conectado un nodo. Así cuando una ruta hacia un cierto nodo falla, el enrutador correspondiente buscará rutas alternativas. Emplea los mensajes de ICMPv6, y es la base para permitir el mecanismo de autoconfiguración en IPv6.

NSF (The National Science Foundation - Fundación Nacional de Ciencia) Agencia del gobierno de los Estados Unidos que apoya a la investigación y la educación en los campos de ingeniería y ciencia exceptuando la medicina.

NSFN (National Science Foundation Network – Red de la Fundación Nacional de Ciencia) En 1988 IBM colaboró con MCI Communications y la universidad de Michigan para crear una red informática donde se establecieron las bases para el crecimiento explosivo de Internet en la década de 1990.

OSI (Open System Interconnection – Interconexión de Sistemas Abiertos) Es la propuesta que realizó ISO (International Organization for Standardization) junto con el UIT – T, para la estandarización de las redes.

RAND (Research ANd Development) Es un think tank (Un think tank o tanque de pensamiento es una institución investigadora u otro tipo de organización que ofrece consejos e ideas sobre asuntos de política, comercio e intereses militares. El nombre proviene del inglés por la abundancia de estas instituciones en Estados Unidos y significa "depósito de ideas". Algunos medios en español utilizan la expresión "fábrica de ideas" para referirse a los think tank) norteamericano formado, en un primer momento, para ofrecer investigación y análisis a las fuerzas armadas norteamericanas.

RC4 Conocido como “Rivest Cipher 4”, es un método de cifrado de datos que garantiza que la información no puede ser leída a menos que se tenga el permiso y las herramientas adecuadas, otorgando así la privacidad de la información.

RFC Dentro de la red de ingeniería de cómputo, un Request for Comments (RFC) es un memorándum publicado por el Internet Engineering Task Force (IETF) dentro de éste se describen métodos, ambientes, investigaciones o innovaciones aplicables al desarrollo de Internet y de sistemas conectados a Internet.

RIR (Regional Internet Registries – registros regionales de Internet). Organismo para la supervisión de asignación y registros de los recursos de Internet dentro de una región en particular del mundo.

ROI (Return on investment – Retorno de Inversión). Medida de rendimiento utilizado para evaluar la eficacia de una inversión o serie de inversiones. Para calcular el retorno de la inversión, el beneficio de una inversión se divide entre el costo de la inversión y el resultado se expresa como un porcentaje.

Router Dispositivo de hardware que forma parte de una infraestructura de una red que opera en la capa tres del modelo OSI, tiene como finalidad determinar el camino que los paquetes deben tomar para llegar a su destino.

Router Relay Encaminador de reenvío, esencialmente son puentes entre sitios 6to4 y dominios IPv6 nativos, reenviando el tráfico con dirección 6to4 entre los encaminadores 6to4 en una red IPv6.

SGML Standard Generalized Markup Language o "Lenguaje de Marcado Generalizado". Consiste en un sistema para la organización y etiquetado de documentos. La Organización Internacional de Estándares (ISO) normalizó este lenguaje en 1986.

SHA. Conjunto de funciones de hash criptográfico diseñado por la Agencia de Seguridad Nacional (NSA) de los Estados Unidos.

SMTP (Simple Mail Transfer Protocol/Protocolo Simple de Transferencia de Correo) Es un protocolo de la capa de aplicación. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre dispositivos. Está definido en el RFC 2821.

TELNEL Telnet (**TEL**ecommunication **NET**work) es el nombre de un protocolo de red (y del programa informático que implementa el cliente) que sirve para acceder mediante una red a otra máquina, para manejarla remotamente como si se estuviera sentado delante de ella. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones.

TCP (Transmission-Control-Protocol, en español Protocolo de Control de Transmisión) En la pila de protocolos TCP/IP, TCP es la capa intermedia entre el protocolo de internet (IP) y la de aplicación. Habitualmente, las aplicaciones necesitan que la comunicación sea fiable y, dado que la capa IP aporta un servicio de datagramas no fiable (sin confirmación), TCP añade las funciones necesarias para prestar un servicio que permita que la comunicación entre dos sistemas se efectúe libre de errores, sin pérdidas y con seguridad.

TRAI (Telecom Regulatory Authority of India). Independencia reguladora creada por el gobierno de India para administrar el negocio de telecomunicaciones.

TTL (Time To Live – Tiempo de vida) Es un límite en el periodo de tiempo o número de iteraciones de una transmisión en una red de computadoras, es utilizado en un paquete IP donde un ruteador analiza si el paquete debe ser reenviado o descartado con base en el tiempo que lleva el paquete en la red.

UDP (User Datagram Protocol – Protocolo de Datagrama de Usuarios) Es un Protocolo que fue diseñado por David P. Reed en 1980 y está formalmente definido en RFC 768, forma parte de los miembros principales de la suite de protocolo de Internet, UDP utiliza un modelo de transmisión sin un diálogo implícito de Hand – Shaking que garantiza confiabilidad e integridad, proporcionando un servicio fiable para el envío de datos.

UNICAST El tráfico unicast se usa para una comunicación de uno a uno con la topología de enrutamiento de unidifusión.

VLSM (Máscaras de subred de tamaño variable / variable length subnet mask) El concepto básico de VLSM es muy simple: se toma una red y se divide en subredes fijas, luego se toma una de esas subredes y se vuelve a dividir tomando bits "prestados" de la porción de hosts, ajustándose a la cantidad de hosts requeridos por cada segmento de nuestra red.

VoIP (Voice over Internet Protocol). Mecanismos que hacen posible transportar señales de voz sobre el protocolo de Internet mediante el uso de paquetes.

XOR Función booleana denominada OR exclusiva que opera con dos valores binarios, el resultado se define como aquella que da por resultado uno si el valor de sus entradas es distinto y cero cuando el valor de las entradas es la misma.

REFERENCIAS

REFERENCIAS BIBLIOGRÁFICAS (NORMA ISO 690)

- AMOSS, John. MINOLI, Daniel. *Handbook of IPv4 to IPv6 Transition*. Estados Unidos : Auerbach Publications Taylor & Francis Group, 2008. ISBN 13: 978-0-8493-8516-2.

- DAVIES, Joseph. *Understanding IPv6*, Segunda Edición, Washington: Microsoft Press Redmond, 2008, Library of Congress Control Number: 2007940506.

- GROSSETETE, Patrick.,et al. *Global IPv6 Strategies* From Business Analysis to Operational Planning, Indianápolis: Cisco Press, 2008. ISBN 978-1-58705-343-6.

- TANENBAUM, Andrew. *Redes de Computadoras*. Tercera Edición en Español, Naucalpan de Juárez Edo de México: Pearson Educación, 1997. ISBN 968-880-958-6.

REFERENCIAS INFORMES (NORMA ISO 690)

- GALLAHER, Michael. *IPv6 Economic Impact Assesment Final Report*. Estados Unidos: RTI International, Octubre 2005. RTI Project Number 008236.003.

- KANE, John [Editor-In-Chief] Cisco Self-Study: Implementing IPv6 Networks, Indianapolis: Cisco Press, 2003, ISBN 1-58705-086-2.

REFERENCIAS ELECTRÓNICAS (NORMA WEAPAS)

A. Millán, José Antonio, (Noviembre 10, 1999). *Breve Historia de Internet* [Documento WWW]. URL: http://jamillan.com/histoint.htm (visitado 10/02/2009)

B. Quantum Networks Web, (Junio 18, 2006). *Cuál fue el inicio de Internet* [Documento WWW]. URL:http://www.quantum-networks.com/articulos/cual-fue-el-inicio-de-internet.html (visitado 11/02/2009)

C. The Internet Engineering Task Force, (n.d/2009). *RFC* [Documento WWW]. URL: http://www.ietf.org (visitado14/1/2009)

a) 791 INTERNET PROTOCOL
b) 950 Procedimiento Estándar para División en Subredes en Internet
c) 1918 Address Allocation for Private Interne
d) 1886 DNS Extensions to support IP version 6
e) 2874 DNS Extensions to Support IPv6 Address Aggregation and Renumbering
f) 3596 DNS Extensions to Support IP Version 6

g) 3152 Delegation of IP6.ARPA

h) 3633 IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6

i) 4214 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

j) 3171 IANA Guidelines for IPv4 Multicast Address Assignments

k) 2461 Neighbor Discovery for IP Version 6 (IPv6)

l) 3053 Service Management Architectures Issues and Review

m) 2765 Stateless IP/ICMP Translation Algorithm (SIIT)

n) 2766 Network Address Translation - Protocol Translation (NAT-PT)

o) 2663 IP Network Address Translator (NAT) Terminology and Considerations

p) 4632 Classless Inter-domain Routing (CIDR):The Internet Address Assignment and Aggregation Plan

q) 2131 Dynamic Host Configuration Protocol

r) 1034 DOMAIN NAMES - CONCEPTS AND FACILITIES

s) 2104 HMAC: Keyed-Hashing for Message Authentication

t) 2893 Transition Mechanisms for IPv6 Hosts and Routers

u) 3315 Dynamic Host Configuracion Protocol for IPv6 (DHCPv6)

D. Central Intelligence Agency, (Marzo 01, 2009). *The World Factbook* [Documento WWW]. URL: https://www.cia.gov/library/publications/the-world-factbook/geos/xx.html#People. (visitado 29/03/2009)

E. Miniwatts Marketing Group, (n.d/2009). *Internet World Stats* [Documento WWW]. URL: http://www.internetworldstats.com/stats.htm (visitado 29/03/2009)

F. RIPE, (n.d/2009). *Policy Proposals* [Documento WWW]. URL: http://www.ripe.net/ripe/policies/proposals/2008-03.html. (visitado 29/03/2009)

G. ITAA, (n.d/2009). *OECD Economic Considerations in the IPv4 to IPv6 Transition* [Documento WWW]. URL: http://www.itaa.org/upload/es/docs/OECD%20Economic%20Considerations%20i%20the%20IPv4%20to%20IPv6%20Transition.pdf. (visitado14/1/2009)

H. Mic Communications News, (October 20, 2005). *Broad Outlines Of Fy 2006 Ict Policy Principles* [Documento PDF]. URL: http://www.soumu.go.jp/joho_tsusin/eng/Releases/NewsLetter/Vol16/Vol16_01/Vol16_01.pdf.

I. Paltemaa, L. (n.d/2009). *Regime Transition and the Chinese Politics of Technology: From Mass Science to the Controlled Internet* [Documento PDF] URL: http://news.xinhuanet.com/english/2006-09/24/content_5130188.htm. (visitado 29/03/2009)

J. IPv6 Chile, (n.d/2011) *El espacio de direcciones IPv4 es historia* [Documento WWW]. URL: http://www.ipv6.cl/noticia/el-espacio-de-direcciones-ipv4-ya-es-historia (visitado 1/11/2011)