UNIVERSIDAD CATÓLICA ANDRÉS BELLO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

EVALUACIÓN DE MECANISMOS DE TRANSICIÓN A IPV6 EN INFRAESTRUCTURAS DE OPERADORES DE REDES DE TELECOMUNICACIONES. CASO CANTV

TRABAJO ESPECIAL DE GRADO

Presentado ante la:

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

Como parte de los requisitos para optar al título de

INGENIERO EN TELECOMUNICACIONES

REALIZADO POR: Carlos Guillermo Ortigoza Dempster.

Ricardo Antonio Ríos Gil.

TUTOR: Wilfredo Torres.

FECHA: Caracas, marzo de 2014.

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

EVALUACIÓN DE MECANISMOS DE TRANSICIÓN A IPV6 EN INFRAESTRUCTURAS DE OPERADORES DE REDES DE TELECOMUNICACIONES. CASO CANTV

REALIZADO POR: Carlos Guillermo Ortigoza Dempster.

Ricardo Antonio Ríos Gil.

TUTOR: Wilfredo Torres.

FECHA: Caracas, marzo de 2014.

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

EVALUACIÓN DE MECANISMOS DE TRANSICIÓN A IPV6 EN INFRAESTRUCTURAS DE OPERADORES DE REDES DE TELECOMUNICACIONES. CASO CANTV

Este Jurado; una vez realizado el examen del presente trabajo ha evaluado su contenido con el resultado: _____

J U R A D O E X A M I N A D O R

Firma: Firma: Firma:

Nombre:_____ Nombre:_____ Nombre:_____

REALIZADO POR: Carlos Guillermo Ortigoza Dempster.

Ricardo Antonio Ríos Gil.

TUTOR: Wilfredo Torres.

FECHA: Caracas, marzo de 2014.

Resumen

EVALUACIÓN DE MECANISMOS DE TRANSICIÓN A IPV6 EN INFRAESTRUCTURAS DE OPERADORES DE REDES DE TELECOMUNICACIONES. CASO CANTV

Ortigoza Dempster, Carlos Guillermo

carlos.otgz@gmail.com

Ríos Gil, Ricardo Antonio

r.riosgil9@gmail.com

La transición de IPv4 a IPv6 se ha convertido en uno de los principales problemas a resolver a nivel mundial en el ámbito de las telecomunicaciones, por lo cual en cada país los ISPs analizan los mecanismos de transición más adecuados según su topología de red interna y externa, la solicitud de direcciones a la LACNIC y el plan de direccionamiento más adecuado teniendo en cuenta la cantidad de clientes y las características de los mismos. Este es el caso de CANTV (Compañía Anónima Nacional de Teléfonos de Venezuela), que a pesar de no presentar un agotamiento en sus direcciones IPv4, hasta el momento, requiere la elaboración de la presente investigación cuyo objetivo general es evaluar mecanismos de transición a IPv6 para su infraestructura. Para cumplirlo se plantean cuatro fases, con las cuales se desea conocer si sus equipos actualmente en funcionamiento en la red son compatibles con IPv6, evaluar e implementar los mecanismos de transición y protocolos de enrutamiento en la red de su laboratorio, diseñar un plan de direccionamiento con IPv6 y desarrollar el documento final con los procedimientos y recomendaciones para la implementación de los mecanismos evaluados. La culminación y cumplimiento de cada una de estas fases generaron como conclusiones, que el mecanismo de transición más adecuado para su implementación es 6rd en conjunto con *Dual Stack*, se presentan dos opciones como protocolos de enrutamiento interior, como lo son OSPFv3 y IS-IS, manteniendo BGP como protocolo de enrutamiento exterior. En cuanto al direccionamiento se entregará una longitud de prefijo /56 a clientes residenciales y un /48 a clientes empresariales, sólo se obtendría bajo pedido esta última longitud de prefijo mencionada por clientes residenciales; se requiere un cambio de los CPE actualmente en funcionamiento por no ser compatibles con IPv6.

Palabras Claves: IPv6, IPv4, direccionamiento, equipos y mecanismos de transición.

Dedicatoria

"Este logro está dedicado a mis padres, quienes si bien toda la vida esperaron la excelencia de mí sin que exigiese nada a cambio, no como una opción sino como mi única obligación, puedo comprender apenas ahora en la madurez que ese es el único camino para dejar algo perdurable y único en el mundo.

Aun cuando este proyecto no es más que una de esas obligaciones y responsabilidades de mi parte, espero que pueda darles un poco de orgullo, ya que todo cuanto hay de bueno en mí, empezó por ustedes".

"Igualmente le agradezco a todos aquellos a los que me consideran su amigo, en especial a Francis Rodríguez, por entender a una persona a la que siempre le gustó preguntar el por qué de las cosas, aún cuando eso implicaba perder el favor de la mayoría, alguien que siempre prefirió incomodar con la verdad antes que agradar con falsas adulaciones... Y eso es algo que les agradeceré de por vida, pues es algo que no cualquiera puede hacer".

Carlos Ortigoza.

"A Dios y a la Virgen del Valle por brindarme todas las oportunidades que me han hecho la persona que hoy en día soy".

"A mi familia que durante todos estos años me han apoyado en cada una de mis decisiones y en especial a mis padres Gloria Gil y Francisco Ríos, quienes con su esfuerzo, carácter, apoyo y dedicación lograron hacerme entender que todo es posible en esta vida, siempre y cuando te lo propongas y no te rindas al intentarlo, por eso y muchas cosas más este Trabajo Especial de Grado va dedicado especialmente a ustedes que siempre se han sentido orgullosos de cada uno de mi logros".

"A mi sobrina - ahijada que con sólo una sonrisa me alegra el día, espero que poco a poco vayas cumpliendo cada una de las metas que te propongas en la vida, como también se la dedico a mi hermana por ser siempre mi ejemplo a seguir".

"A todos mis amigos que de una u otra forma desde que los conozco me han apoyado y ayudado a lograr mis metas, en especial a Franxis, Fiama, Andrea, Jonathan, Luciano y Juan José (Cumanes) quienes me brindaron su paciencia, amistad, apoyo incondicional y consejos para culminar este proyecto. Pueden contar conmigo para lo que necesiten".

Ricardo Ríos

Agradecimientos

"Le agradecemos al Ing. Wilfredo Torres, nuestro tutor académico, por todo el apoyo, paciencia y asesoramiento prestado para la culminación de este Trabajo Especial de Grado".

"Al Ing. Miguel Zambrano por todo el apoyo prestado en el Laboratorio de CANTV, como también al Ing. Francisco Flores por su colaboración y asesoramiento".

"Al Ing. Luis Molner y al Ing. Héctor González por toda la información suministrada, que sirvió como apoyo en la realización de este proyecto".

"A todas aquellas personas que de alguna u otra forma nos apoyaron durante la realización de este Trabajo Especial de Grado".

Carlos Ortigoza.

Ricardo Ríos.

Índice General

Índice de Figuras

Índice de Tablas

Introducción

En la actualidad, el gran progreso que ha tenido el Internet ha llevado a la necesidad de utilizar un nuevo protocolo IP. Es así como se presenta a IP versión 6 (IPv6) como la nueva versión de dicho protocolo, diseñado como el sucesor de IPv4, presentando diversas modificaciones destacando primordialmente capacidades de direccionamiento ampliadas pero también una simplificación del formato de cabecera, soporte mejorado para extensiones y opciones, capacidad para etiquetar flujos de tráfico, así como prestaciones de privacidad y autenticación. En consecuencia, surge el presente trabajo de investigación cuyo objetivo general es el de evaluar mecanismos de transición hacia IPv6 en el Proveedor de Servicios de Internet CANTV, para cubrir las necesidades tanto a nivel empresarial como a nivel de sus clientes.

Por ello, se llevó a cabo un proyecto factible, de investigación de campo de carácter experimental.

El trabajo está conformado por cinco (5) capítulos, estructurados de la siguiente manera:

El **Capítulo I** contiene el planteamiento del problema, los antecedentes, objetivos, justificación e importancia del estudio, el alcance y las limitaciones confrontadas en el desarrollo de toda la investigación. En el **Capítulo II** se presentan una serie de conceptos importantes que son la base para el desarrollo del estudio. En el **Capítulo III** se contempla el tipo de diseño de investigación, la población y muestra del estudio, las técnicas e instrumentos de recolección de datos utilizados, la validez y la confiabilidad en el estudio, las fases o etapas de la investigación y la conceptualización y operacionalización de las variables. El **Capítulo IV** se centra en la presentación e interpretación de los resultados obtenidos en el estudio. Por último, en el **Capítulo V** se culmina con las conclusiones y recomendaciones resultantes de la investigación.

Capítulo I

Planteamiento del Proyecto

I.1 Planteamiento del Problema.

La necesidad de implementar el nuevo protocolo IPv6 en redes de telecomunicaciones es un asunto inevitable. Si bien el agotamiento de las direcciones de IPv4 es la razón que ha disparado todo este cambio, el nuevo protocolo es algo más que un "espacio de direcciones más amplio". Entre las características que se pueden destacar resaltan las mejoras que se proponen para el soporte de movilidad, seguridad y calidad de servicio (QoS). Estos aspectos se alinean con las exigencias de las Redes de Nueva Generación (NGN), en las cuáles se ofrecen servicios de comunicaciones multimedia sobre redes paquetizadas. Si bien la propuesta del nuevo protocolo ya ha alcanzado un grado de madurez importante, y ya se están desplegando redes con el mismo, los escenarios que se están manejando a corto y mediano plazo sugieren una transición a IPv6 desde IPv4, más que una "migración". Es decir, los mecanismos propuestos para el despliegue de IPv6 implican la convivencia con IPv4 por un tiempo indeterminado. Es imposible pensar en la idea de un "apagón" súbito de IPv4 con todos los servicios de conectividad que se están prestando hoy día sobre este protocolo. En este sentido, se presenta como un desafío importante un adecuado diseño para lograr la transición efectiva, sin perder los servicios ya desplegados en IPv4, pero a la vez sin desaprovechar las bondades que trae IPv6.

Los Operadores de Redes, en este caso CANTV, como actores principales en la prestación de servicios de conectividad (y cada vez más, de aplicaciones y contenidos) necesitan evaluar muy bien los proyectos de transición a IPv6. Se requerirán diseños adecuados y de cierta complejidad para adecuar desde su infraestructura (servidores, *routers, firewalls*, etc.), pasando por los procedimientos

de asignación de direcciones a clientes de diferentes niveles, hasta el desarrollo de aplicaciones y contenidos.

I.2 Antecedentes

En la investigación y realización del presente trabajo especial de grado se analizaron diversas fuentes de información relacionadas con el tema, enfocándose directamente con la transición al nuevo Protocolo de Internet (IP). A continuación se presentarán algunos trabajos de investigación elaborados previamente:

En septiembre de 2011 fue presentado ante la Escuela de Ingeniería en Telecomunicaciones de la Universidad Católica Andrés Bello el trabajo especial de grado titulado "Estudio sobre la red de la empresa NETUNO para la implementación de IPv6 en su plataforma de multiservicio para el segundo semestre de 2011", realizado por Gabriela Fernández-Trujillo y Laura Rojas. Esta investigación se enfoca en el área de Redes o Telemática y concluye que el método más idóneo y eficiente para su implementación es *Dual Stack* logrando así la convivencia IPv4/IPv6. Sin embargo indican que este mecanismo debería trabajar con los Túneles para obtener un funcionamiento más óptimo de la red.

David García en octubre de 2011, presentó ante la Escuela de Ingeniería en Telecomunicaciones de la Universidad Católica Andrés Bello el trabajo especial de grado titulado "Diseño de una estrategia de migración de la red actual de la Universidad Católica Andrés Bello a una red basada en IPv6". Teniendo como propósito diseñar una estrategia de transición para la migración a una red basada en IPv6, concluyendo que el mejor mecanismo de transición para su migración es *Dual Stack* a nivel de servidores, túnel TEREDO en caso de trabajar con direcciones privadas y túnel 6to4 en caso de trabajar con direcciones públicas.

Por otra parte, David Nuñez, presenta en agosto de 2009 ante la Escuela Politécnica Nacional (Quito, Ecuador), el proyecto titulado "Estudio para la

Migración de IPv4 a IPv6 para la empresa proveedora de Internet MILLTEC S.A", en al cual concluye la migración a IPv6 es posible y factible pero es un proceso que lleva tiempo, se puede afirmar que los cambios requeridos son a nivel de software y la mayoría de los equipos en la actualidad cuentan con soporte para IPv6

Los antecedentes observados anteriormente dan a conocer la importancia de la transición a IPv6 y su implementación en diversas empresas e instituciones educativas, generando así un incentivo a nivel nacional e internacional para avanzar con la aplicación del nuevo Protocolo de Internet.

I.3 Objetivos.

I.3.1 Objetivo General.

Evaluar Mecanismos de Transición a IPv6 para la Infraestructura de Redes del operador CANTV.

I.3.2 Objetivos Específicos.

a.) Evaluar la compatibilidad de los elementos de la infraestructura del operador con el protocolo IPv6: dispositivos de conectividad, seguridad, y servidores.

b.) Diseñar los esquemas de direccionamiento y asignaciones IPv6 adecuadas a las operaciones y disposición de los clientes del operador.

c.) Evaluar los mecanismos de transición adecuados para la continuidad de los servicios en un entorno mixto IPv4 e IPv6.

d.) Diseñar los esquemas de enrutamiento interior y exterior para su funcionamiento sobre IPv6.

e.) Implementar una maqueta de red IPv6 funcional con los diferentes mecanismos de transición y enrutamiento para evaluar funcionamiento y desempeño.

f.) Realizar el proyecto con los procedimientos y recomendaciones resultantes para hacer operativa la red con IPv6.

I.4 Alcances y Limitaciones.

Este Trabajo Especial de Grado consta en la evaluación de mecanismos de transición al protocolo IPv6 en operadores de redes de telecomunicaciones, el cual incluirá la valoración de compatibilidad de los equipos del operador con el nuevo protocolo y los posibles rangos de direcciones que se asignarán.

Se seleccionará el mecanismo de transición a IPv6 más adecuado para su implementación en la red; de igual manera, se procederá al diseño de escenarios de pruebas con los parámetros de desempeño correspondientes y se realizará una maqueta de la red sobre la cual se está operando.

Incluirá un ensayo limitado a modo de "Prueba Piloto" en la plataforma tecnológica de la compañía CANTV, en estrecha coordinación con los líderes y responsables de las áreas pertinentes.

I.5 Justificación

Debido al progreso sostenido y ampliamente progresivo que ha visto Internet durante su historia, se hace primordial una transición a IPv6, más que una migración por la inviabilidad de la misma; sin embargo, uno de los actores principales en dicha transición son los Proveedores de Servicio de Internet. Es por ello que el presente proyecto generará importantes aportes en diferentes áreas, como son:

a.) Sentar las bases para la transición adecuada del protocolo IPv4 al protocolo IPv6 en los proveedores de servicio de Internet de gran envergadura de Venezuela.

b.) Solventar los problemas en cuanto a escasez y administración de direcciones IP por parte de CANTV a sus clientes en el largo plazo.

c.) Encaminar la red del operador CANTV con las exigencias de las Redes de Nueva Generación (NGN), acorde a sus requerimientos en sus servicios de comunicaciones multimedia sobre redes paquetizadas.

Capítulo II

Marco Referencial

II.1 Protocolo IPv4

II.1.1 Términos Básicos

Se destacan tres términos básicos en cuanto al direccionamiento en IPv4: nombres, direcciones y rutas. De ellas, "un nombre indica qué es lo que se busca. Una dirección indica donde está y una ruta indica cómo se llega ahí." [1].

Asimismo, se destaca el manejo casi exclusivo de dichas direcciones por parte del protocolo, dejando de lado la correspondencia de éstas con nombres a protocolos de capas superiores. De igual forma, se delega a protocolos de menor nivel la responsabilidad de procesar la relación entre una dirección local y una ruta, a otra dirección no local [1].

II.1.2 Clasificación de Direcciones

A pesar de que todas las direcciones IPv4 son de una longitud fija de 4 octetos o 32 bits, pueden ser clasificadas en tres formatos o clases, de acuerdo al número de bits asignados al número de red y al número de dirección de host (también conocido como campo restante o de "resto") [1]. Se describen a continuación:

- **Clase A:** en la cual el bit más significativo vale 0, lo 7 bits siguientes corresponden al número de red, y los 24 bits restantes corresponden a la dirección de host.
- **Clase B:** los dos bits más significativos son uno-cero, los 14 bits siguientes corresponden al número de red y los últimos 16 bits representan la dirección de host.
- **Clase C:** los tres bits más significativos son uno-uno-cero, los 21 bits siguientes corresponden al número de red y los 8 bits restantes representan la dirección de host.

II.1.3 Direcciones IP Privadas

Las direcciones IP privadas surgieron en principio debido al "crecimiento de Internet más allá de la previsión de cualquiera" [2], por lo que el espacio de direcciones únicas a nivel global eventualmente se agotaría. Por ello, la "Autoridad de Números Asignados en Internet", *Internet Assigned Numbers Authority* (IANA), reservó tres bloques de direcciones IP para el uso en redes privadas no conectadas a *Internet*:

- 10.0.0.0 hasta 10.255.255.255 (prefijo 10/8)
- 172.16.0.0 hasta 172.31.255.255 (prefijo 172.16/12)
- 192.168.0.0 hasta 192.168.255.255 (prefijo 192.168/16)

De estas asignaciones se observa que cada bloque no es más que un conjunto de números de redes correspondientes a cada clase, donde el primer grupo corresponde a un único número de red de Clase A; el segundo bloque a 16 números de red de Clase B consecutivos y el último bloque a 256 números de red de Clase C consecutivos [2].

Debido a que estos bloques de direcciones son de naturaleza privada, una empresa o particular que haga uso de ellas no está en la necesidad de regularse previamente con la IANA [2]. En consecuencia, en dos redes privadas distintas pueden existir direcciones idénticas, ya que en teoría no están conectadas entre sí.

II.1.4 Header IPv4.

El "*header*" IPv4 consta de una longitud de 160 bits (20 bytes) cuando se maneja sin opciones adicionales. Estos 160 bits se distribuyen en una serie de campos como se indica en la Figura 1 [1]:

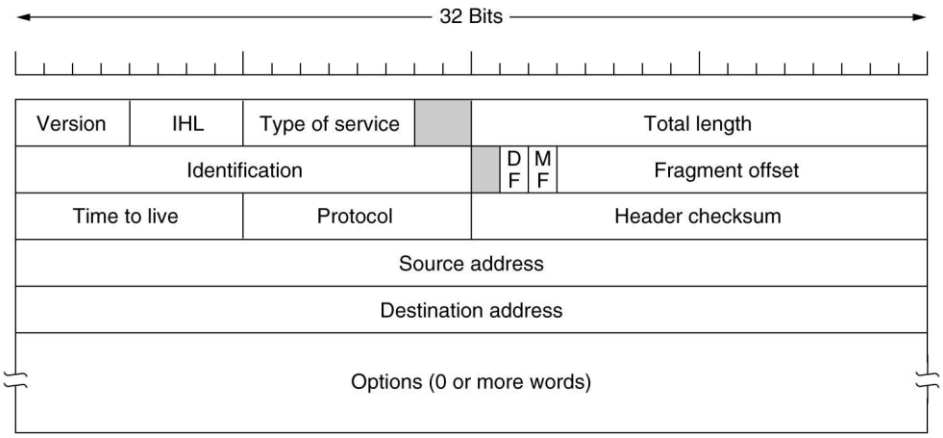

Figura 1: *Header* paquete IPv4.

Fuente: [1]

Los campos y sus funciones se describen a continuación [1]:

Campo	Descripción
Version	Campo de 4 bits destinado a indicar el formato de la cabecera IP.
IHL	*Internet Header Length*, representa la longitud de la cabecera en palabras de 32 bits y señalando, en consecuencia, el inicio de los datos. Tiene 4 bits de longitud y el mínimo valor para una cabecera correcta es de 5.
Type of service	Campo de 8 bits de longitud. Proporciona una indicación de los parámetros abstractos de la calidad de servicio deseada, los cuales son usados para guiar la selección de los parámetros de servicio reales al transmitir un datagrama a través de una red específica.
Total length	Campo de 16 bits de longitud. Representa la longitud de datagrama medida en octetos, incluyendo la cabecera del mismo y sus datos.
Identification	Campo de 16 bits de longitud. Valor de identificación asignado por el transmisor del datagrama usado para facilitar la tarea de reensamblado de los fragmentos del datagrama.
DF Flag	Campo de 1 bit. Si es igual a 0 se permite fragmentar el paquete; en caso contrario no se permite.
MF Flag	Campo de 1 bit. Si es igual a 0 indica que el fragmento actual es el último del datagrama; en caso contrario indica que aun hay fragmentos por recibir.
Fragment offset	Campo de 13 bits de longitud. Indica en qué lugar del datagrama se posiciona el fragmento actual. Está medido en unidades de 8 bytes (64 bits). El primer fragmento del datagrama tiene un *offset* nulo.
Time to live	Campo de 8 bits de longitud. A fines prácticos, su valor se reduce en una unidad por cada nodo que el paquete atraviesa; si su valor se

Campo	Descripción
	reduce a cero el paquete es descartado.
Protocol	Campo de 8 bits de longitud. Indica el protocolo del siguiente nivel usado en la parte de datos del datagrama.
Header checksum	Campo de 16 bits de longitud. Suma de control de la cabecera únicamente. Este valor es recalculado en cada punto en el que la cabecera es procesada, debido a que algunos campos de la cabecera cambian, como por ejemplo el *Time to live*.
Source Address	Campo de 32 bits de longitud. Indica la dirección de origen del paquete.
Destination Address	Campo de 32 bits de longitud. Indica la dirección de destino del paquete.

Tabla 1: Campos y Funcionamiento de *Header* IPv4.

Fuente: [1]

II.1.5 NAT (Network Address Translation)

En un principio, NAT fue propuesto como solución a corto plazo al problema de agotamiento de direcciones IPv4, desarrollándose en el proceso dos variantes: el NAT básico y *Network Address Port Translation (NAPT)*.

El mecanismo NAT trabaja entonces sobre un concepto básico, enmascaramiento de IP, y en efecto, es igualmente conocido con este nombre. Es así como inicialmente NAT estaba basado en la premisa de que solo un pequeño número de los clientes en una red privada se comunican fuera de esta red. En consecuencia, si a cada cliente se le asigna una dirección IP pública únicamente cuando éste necesita comunicarse, el número de direcciones públicas necesario se verá reducido.

El funcionamiento general del NAT básico consiste en tomar cada paquete IP saliente, y sustituir su dirección de origen de forma dinámica por otra existente en un grupo de direcciones IP públicas destinada para tal fin. Igualmente, para cada paquete IP entrante, se verifica si la dirección de destino está siendo utilizada por NAT y, en caso afirmativo, es traducida a su dirección de destino interna original.

Las direcciones IP NAT deben provenir de redes o subredes diferentes si se desea que las tablas de rutas funcionen correctamente, del mismo modo que se conectan dos

o más redes IP a través de un *router*. En el caso de que la red externa sea Internet, las direcciones NAT deben ser de carácter público, es decir, deben ser asignadas por la IANA.

Las posibles direcciones a asignar a los paquetes salientes se conservan en un lote destinado para tal fin. Al momento de establecerse una nueva conexión saliente, NAT simplemente toma la primera dirección disponible y hace uso de ella. Igualmente, mantiene un seguimiento de cuál dirección externa es asignada a cada dirección interna, de modo de ser capaz de entregar cualquier respuesta externa a la dirección IP local correcta. Sin embargo, debido a que a nivel de la capa IP no hay información que facilite determinar en qué momento una conexión ha terminado, y de este modo determinar cuándo se puede devolver la dirección IP externa utilizada al lote de direcciones NAT disponible, se acostumbra a establecer un tiempo límite de inactividad de 15 minutos antes de regresar dicha IP automáticamente al lote ya mencionado.

Mientras que NAT está limitado a traducir únicamente direcciones IP, NAPT permite traducir conjuntamente direcciones IP e identificadores de transporte, como puertos TCP/UDP. De este modo, NAPT traduce las direcciones privadas a una única dirección global exterior, asignado cada conexión a un puerto específico de ésta. Es así como NAPT permite que múltiples nodos de la red local se conecten simultáneamente a redes externas, simplemente añadiendo, con respecto a NAT, políticas de traducción para las sesiones TCP/UDP que se generen.

No obstante, se derivan una serie de limitaciones e inconvenientes, como la obligatoriedad de que todas las solicitudes y respuestas pertenecientes a una sesión sean enrutadas por el mismo *router* NAT; o el aumento en la complejidad de depuración de problemas, incluyendo violaciones de seguridad [3].

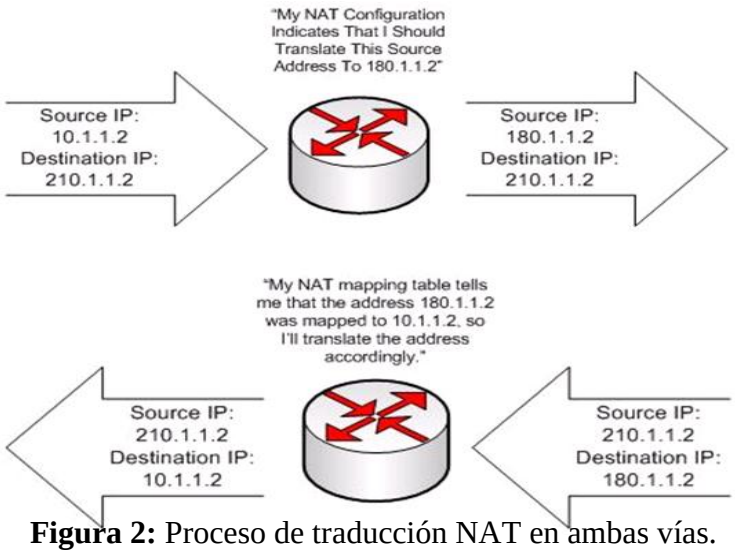

Figura 2: Proceso de traducción NAT en ambas vías.

Fuente: [4].

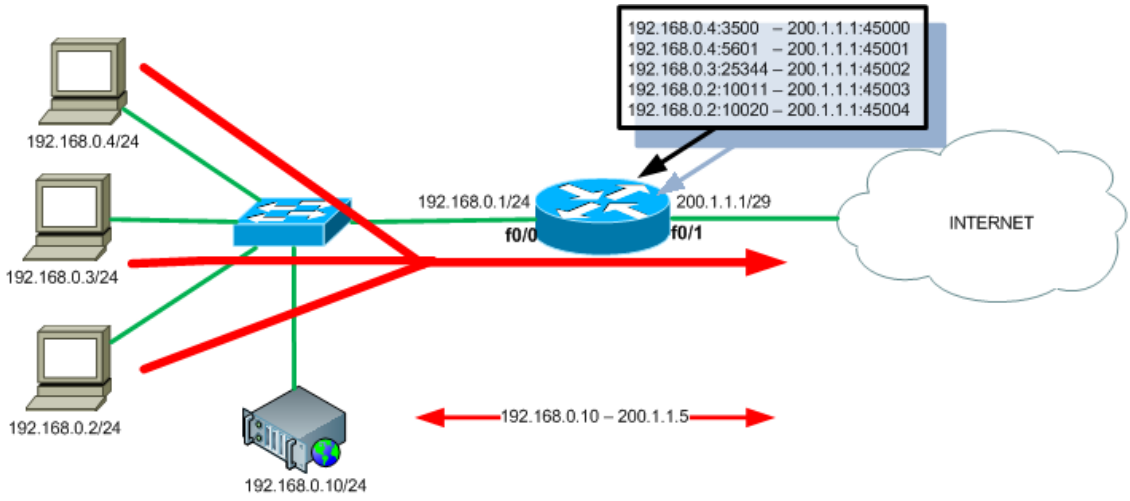

Figura 3: Proceso de traducción PAT para solicitudes salientes.

Fuente: [5].

La Figura 3 describe el proceso de traducción PAT para solicitudes salientes. En el caso planteado, cuatro clientes pertenecientes a una red local privada realizan una solicitud a su punto de salida por defecto (192.168.0.1/24). Éste asigna a cada una de estas direcciones privadas la misma dirección pública (establecida por la IANA), variando el puerto TCP/UDP de salida para identificar cuál dirección privada interna

corresponde a cada puerto de salida. Este proceso se registra en una tabla que permita al dispositivo PAT realizar el proceso inverso y conocer cuáles puertos ya han sido utilizados.

II.2 Protocolo IPv6

II.2.1 Descripción de IPv6

Se describe el protocolo IPv6 como "una nueva versión del Protocolo de Internet, diseñado como el sucesor a IP versión 4 (IPv4)" [6]. En el mismo se describen los cambios principales con respecto a su antecesor, los cuales constan principalmente de un número mucho mayor de direcciones disponibles para ser asignadas, formato simplificado de la cabecera, mayor flexibilidad para extensiones y opciones futuras; así como una nueva funcionalidad basada en el etiquetado de paquetes pertenecientes a un flujo de tráfico de datos particular.

El nuevo formato de cabecera ayuda a que los equipos de enrutamiento disminuyan su trabajo en el momento de procesar su información y le permite a IPv6 poseer una estructura de direccionamiento eficiente y jerárquica, es decir, que los *routers* que trabajan en el Internet tengan tablas de enrutamiento más pequeñas, de acuerdo a la infraestructura de red que tenga cada *Internet Service Provider (ISP).*

En consecuencia, para permitir un número mucho mayor de direcciones asignables, se realizó una serie de modificaciones en el formato de las mismas, aumentando su tamaño a un total de 128 bits, denotados como 8 grupos de cuatro dígitos hexadecimales.

Varias instituciones, empresas, agencias de gobiernos y corporaciones han aportado mejoras al protocolo, por lo que es capaz de proveer calidad de servicio (QoS), confiabilidad, escalabilidad y una entrega sólida de los datos y la información para servicios como Voz sobre IP (VoIP) e IPTV [7].

II.2.2 Características de IPv6

IPv6 posee una gran cantidad de características relevantes, entre las que se encuentra la autoconfiguración, la cual incluye la creación de una dirección de enlace local y la verificación en el caso de las direcciones si serán obtenidas mediante un proceso sin estados, con estados o ambos.

La autoconfiguración sin estado (*stateless)* no necesita una configuración manual de los servidores, ya que permite que los *hosts* generen su propia dirección mediante una combinación de información disponible localmente y anunciada por los *routers*. La dirección se genera con la combinación de los prefijos que identifican la (s) subred (es) asociada (s) a un enlace y los "identificadores de interfaz" generados por los *hosts* que identifican a una interfaz en una subred. Si no hay *routers*, los *hosts* sólo pueden generar direcciones de enlace local.

En la configuración con estado (*stateful*), se les permite a los *hosts* obtener la información de configuración y direcciones de un servidor DHCPv6 (*Dynamic Host Configuration Protocol*), ya que estos conservan una base de datos que lleva un registro de qué direcciones han sido asignadas.

Esta configuración y la mencionada anteriormente son complementarias. Por ejemplo, un *host* puede utilizar una configuración sin estados para configurar sus direcciones y una configuración con estado para obtener el resto de los parámetros para la conexión: servidores DNS (*Domain Name System*), entre otros. [8]. En la siguiente tabla se muestra una serie de características de IPv6 y sus diferencias con IPv4.

IPv4	IPv6
Las direcciones de origen y destino tienen una longitud de 32 bits (4 bytes).	Las direcciones de origen y destino tienen una longitud de 128 bits (16 bytes).
La implementación de IPSec es opcional.	La implementación de IPSec es obligatoria, pero su utilización es opcional.
No hay identificación de flujo de paquetes para la entrega priorizada (QoS) por los *routers* en su cabecera IPv4.	Se incluye la identificación del flujo de paquetes para que los *routers* controlen la entrega priorizada (QoS) en su cabecera IPv6, empleando el campo "*flowlabel*".
La fragmentación la realizan los *routers* y los *hosts* causando retardo en el rendimiento del *router*.	La fragmentación la realizan sólo los *hosts* que envían paquetes, ya que éstos sólo son procesados en el nodo final de destino.
No tiene ningún requisito para el tamaño de un paquete de capa de enlace y debe ser capaz de reensamblar un paquete de 576 bytes.	La capa de enlace debe soportar un paquete de 1280 bytes de tamaño y debe ser capaz de reensamblar un paquete de 1500 bytes.
La cabecera incluye un campo "*checksum*".	La cabecera no incluye el campo "*checksum*".
La cabecera incluye el campo "opciones"	Todos los datos opcionales se encuentran en las cabeceras de extensión.
El protocolo ARP envía tramas *broadcast* para realizar solicitudes ARP con el fin de resolver una dirección de capa física.	Las tramas de solicitudes ARP son reemplazadas con mensajes *multicast* "*NeighborDiscovery*".
El *Internet Group Management Protocol* (IGMP) es utilizado para administrar los grupos de subredes locales.	El *Internet Group Management Protocol* (IGMP) es reemplazado por mensajes *MulticastListenerDiscovery* (MLD).
Internet Control MessagesProtocol (ICMP) *RouterDiscovery* es usado para determinar direcciones IPv4 del mejor *Gateway* y es opcional.	El ICMPv4 *RouterDiscovery* es reemplazado por ICMPv6 *RouterSolicitation* y mensajes de anuncio del *router* y es requerido.
Las direcciones de *broadcast* son utilizadas para enviar tráfico a todos los nodos de una sub red.	No hay direcciones *broadcast* en IPv6, en su lugar, los enlaces locales alcanzan todos los nodos de direcciones *multicast* que son usados.
Las direcciones deben ser configuradas manualmente o a través de DHCP.	Las direcciones no requieren configuración manual o DHCP para IPv6.
Usa registros de recurso (A) de direcciones de *hosts* en el *Domain Naming System (DNS)* para asignar nombres a direcciones IPv4.	Usa registros de recursos (AAAA) de direcciones de *hosts* en el DNS para asignar nombres a direcciones IPv6.

Tabla 2: Características y diferencias entre IPv4 e IPv6.

Fuente: [9].

En el RFC1886 se define el registro de recursos AAAA como el "nuevo registro específico a la clase de Internet que almacena una sola dirección IPv6" [10], es decir, resuelve un nombre de dominio completo en una dirección IPv6. Se denomina AAAA debido a que las direcciones IPv6 son cuatro veces mayores a las IPv4. Este registro se implementa como una mejora en los servidores DNS.

II.2.1 Direccionamiento IPv6.

Las direcciones IPv6 poseen 128 bits de longitud, los cuales se distribuyen en 8 bloques de 16 bits representados con caracteres hexadecimales, a diferencia de las direcciones IPv4 que poseen 32 bits, con 4 campos de 8 bits cada uno y representados con caracteres decimales. A continuación en la Figura 4 se puede observar la estructura de la dirección IPv6:

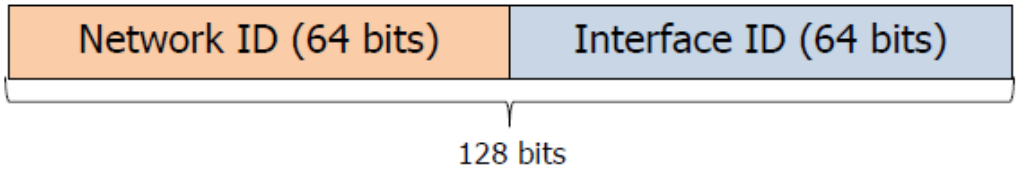

Figura 4: Estructura de Dirección IPv6.

Fuente: [11].

Network ID son los 64 bits más significativos, en donde se encuentran el *Routing ID* (48 bits o más) que es el prefijo de encaminamiento y el *Subnet ID* (16 bits o menos) que es el identificador de subred. El tamaño de cada uno de ellos puede variar, el aumentar el *Routing ID* significa disminuir el tamaño del *Subnet ID*, el cual permite establecer subredes dentro de la red.

Los 64 bits del *Interface ID* son generados de manera automática por la dirección MAC del interface y el algoritmo EUI-64, obtenidos del servidor DHCPv6 que esté en funcionamiento en la red, o asignados manualmente.

Estas direcciones IPv6 tienen una serie de reglas que se deben cumplir, pero para demostrar su funcionamiento, se utilizará como ejemplo la siguiente dirección:

2002:0000:1253:0000:0000:0000:CDAE:8B2E

Reglas en direcciones IPv6
1) Cada bloque está representado por cuatro (4) caracteres hexadecimales, separados por ":".
2) Las letras pueden ser mayúsculas o minúsculas, se pueden expresar, por ejemplo, de la siguiente manera: 2002:0000:1253:0000:0000:0000:CDAE:**8b2e**
3) Si existen ceros "0" consecutivos se puede simplificar la dirección, de la siguiente forma: 2002:**0**:1253:**0**:**0**:**0**:CDAE:8b2e
4) Si existen bloques de ceros sucesivos se pueden reemplazar por "::" pero esta regla se puede aplicar una sola vez por dirección, de lo contrario será inválida. Por ejemplo: 2002:**0**:1253**::**CDAE:8b2e , para determinar la cantidad de bloques que se reemplazaron se deben contar los existentes y restarle 8.
5) Los últimos dos bloques se pueden representar en el formato punto-decimal de IPv4.
6) Se utilizan "[]" alrededor de la dirección para representar URLs, por ejemplo: http://[2002:0:1253::CDAE:8B2E]:puerto/directorio.

Tabla 3: Reglas en direcciones IPv6.

Fuente: Los Autores.

Las direcciones IPv6 poseen generalmente dos partes lógicas, según el formato *Classless Inter-Domain Routing* (CIDR) (<dirección>/<prefijo>), si la dirección de un *host* posee el prefijo "64", como por ejemplo la dirección 2002:0:1253::CDAE:8B2E/64, quiere decir que los primeros 64 bits son de sub-red y los siguientes 64 bits son de *interfaz*. Cuando el prefijo utilizado es menor a 64 bits la dirección es resumida de un espacio de direcciones IPv6 [7].

Así mismo, ya no se aplica la clasificación de grupos o clases según un rango de direcciones determinado. Se emplea, direcciones de tipo "*unicast*", "*anycast*" o "*multicast*", como se describen a continuación:

- ***Unicast:*** emplea un identificador para una única interfaz (nodo unido a un enlace). De este modo, si se envía un paquete a una dirección *unicast*, se enviará a la

interfaz identificada con dicha dirección. Estas direcciones se dividen en cinco grupos, los cuales son:

- Direcciones *link-local:* Siempre comienza con el prefijo FE80::/10. Estas direcciones son utilizadas por los nodos para comunicarse con nodos vecinos dentro de un mismo enlace.
- Direcciones Globales: "Estas direcciones son enrutables y accesibles a nivel global sobre la porción de IPv6 en Internet" [7]. Las direcciones globales pueden ser sumarizadas para lograr un enrutamiento más eficiente, como también en IPv6 equivalen a las direcciones públicas utilizadas en IPv4.

Poseen el rango de direcciones 2000::/16 a 3FFF::/16.

- Direcciones *site-local:* sirven para identificar las interfaces de una misma área topológica perteneciente a un edificio o campus. Estas direcciones son equivalentes a las direcciones privadas de IPv4 y no son accesibles desde otros sitios. Los *routers* no deben enviar tráfico *site-local* fuera de la organización correspondiente.

Siempre comienzan en fec0::.

- Direcciones especiales IPv6: en Ipv6 existen dos tipos de direcciones especiales, las no especificadas ("0:0:0:0:0:0:0:0" o "::") que indican la ausencia de una dirección y las direcciones de *loopback* (0:0:0:0:0:0:0:1 ó ::1), lo que le permite a un nodo enviarse paquetes a sí mismo.
- Direcciones Compatibles: ayudan a la migración de IPv4 a IPv6, existen cuatro tipos de direcciones, las cuales son: direcciones 6to4, direcciones IPv4 compatibles, direcciones 6over4 y direcciones ISATAP. En el caso de 6to4 el prefijo utilizado es el 2002::/16.

- ***Anycast:*** es una dirección *unicast* que se ha replicado en diferentes nodos; para seleccionar a qué nodo dirigir el tráfico se toman en cuenta criterios del protocolo de enrutamiento subyacente. Un paquete destinado a una dirección de tipo "*anycast*", se envía a una única dirección del conjunto que las conforman. Todos los nodos con la misma dirección *anycast* deberán proporcionar el mismo servicio.

- ***Multicast:*** al igual que las direcciones "*anycast*", se emplea una dirección para un conjunto de interfaces; sin embargo, si se envía un paquete a una dirección de tipo "*multicast*", será recibido por cada una de las interfaces identificadas con la dirección. Estas direcciones utilizan de manera eficiente el ancho de banda de la red, al enviar una cantidad pequeños de datagramas a un número máximo de nodos.

Un nodo puede pertenecer a uno o varios grupos *multicast*, sin embargo puede unirse o dejar el grupo en cualquier momento. Los nodos pueden escuchar en múltiples direcciones *multicast* al mismo tiempo.

A continuación se presenta una tabla resumen con los tipos de direcciones IPv6 y sus prefijos correspondientes:

Tipo de Dirección	Prefijo
Link-Local	FE80::/10
Unspecified	::/128
Loopback	::1/128
Global Unicast	2000::/3
IPv4-Compatible	::/96
Direcciones 6to4	2002::/16
Multicast	FF00::/8
Anycast	

Tabla 4: Tipos de Direcciones IPv6.

Fuente: [11].

En la siguiente figura se muestra la estructura de una dirección *multicast* en IPv6:

8 bit	4 bit	4 bit	112 bit
1111 1111	Flags	Scope	Group ID

Figura 5: Estructura de dirección *multicast* en IPv6.

Fuente: [12]

A continuación se describen las diferentes partes de las direcciones *multicast* ilustradas en la Figura 5:

- ✓ Octeto de mayor orden: siempre es 1111 1111 (Binario).

✓ ***Flags*:** los tres primeros bits están reservados, el siguiente indica si la dirección es permanente, es decir, asignado por la *Internet Assigned Numbers Authority* (IANA) o transitoria.

✓ ***Scope*:** indica el alcance de la red IPv6, en la cual el paquete *multicast* será propagado.

Valor	Descripción
0 (0000)	Reservado.
1 (0001)	*Node-Local scope* (Interfaces locales del nodo).
2 (0010)	*Link-Local scope* (Nodos en el enlace local).
4 (0100)	*Admin-Local* (Debe ser administrativamente configurado)
5 (0101)	*Site-Local scope* (Nodos en el sitio local).
8 (1000)	*Organization-Local scope* (Nodos en la organización).
E (1110)	*Global scope* (Nodos a nivel global).
F (1111)	Reservado.

Tabla 5: Valores de *Scope*.

Fuente: [12]

✓ ***Group ID*:** identifica el grupo de *multicast* al que se hace referencia dentro de un determinado *scope*.

Este tipo de direcciones se diferencian de las *unicast* por el valor del octeto de orden superior, el cual es en binario 1111 1111, por lo tanto las direcciones *multicast* siempre empiezan por FF, demostrando que el prefijo utilizado es FF00::/8.

En la tabla mostrada a continuación podrá observar algunas direcciones *multicast* predefinidas, las cuales son de gran utilidad en el momento de realizar las configuraciones en la infraestructura:

Direcciones *Multicast* IPv6	Alcance
FF01::1	Una interfaz local que abarca todos los nodos de direcciones *multicast.*
FF01::2	Interfaces locales que alcanzan todos los *routers* de direcciones *multicast*.
FF02::1	Un enlace local que alcanza todos los nodos de direcciones *multicast*..
FF02::2	Enlaces locales que alcanzan todos los *routers* de direcciones *multicast.*
FF05::2	Todos los *routers* en el *site-local.*

Tabla 6: Direcciones IPv6 *multicast* reservadas.

Fuente: [9]

La IANA ha estipulado sufijos que especifican grupos para usos particulares, en la siguiente tabla se muestran algunos sufijos:

Direcciones *Multicast* IPv6	Grupo
FF01::1	Todos los *host*.
FF02::1	Todos los *host*.
FF01::2	Todos los *routers*.
FF02::2	Todos los *routers*.
FF01::FB	mDNSv6.
FF02::FB	mDNSv6.
FF02::1:2	Todos los agentes DHCP.
FF05::1:3	Todos los servidores DHCP.

Tabla 7: Sufijos de direcciones *multicast*.

Fuente: [12]

II.2.2 Formato Header IPv6.

El *header* de un paquete IPv6 fue expandido de 20 bytes empleados como mínimo en IPv4 a 40 bytes fijos. [6] A pesar de su tamaño extendido, el número de campos totales se ve reducido, facilitando el cómputo de la misma. En la siguiente figura se observa una muestra de éste:

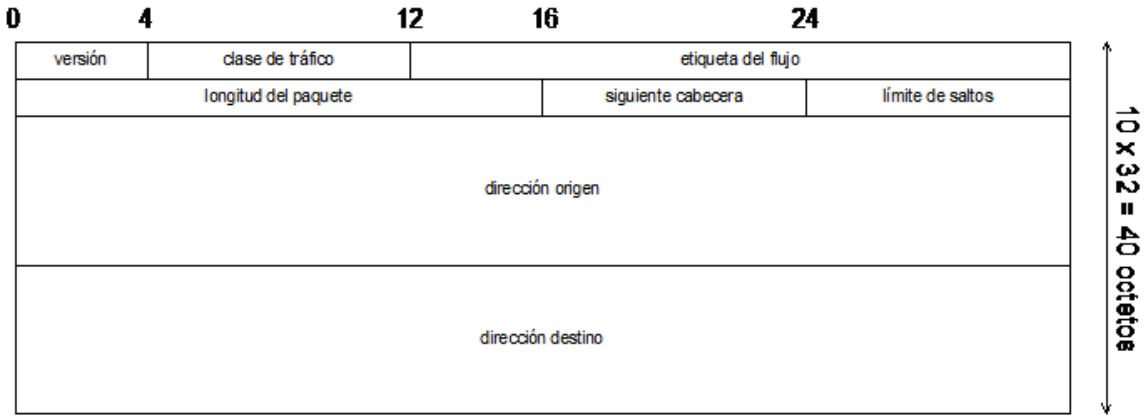

Figura 6*: Header* paquete IPv6.

Fuente: [6]

Los campos y sus funciones se describen a continuación: [6]

- ***Version:*** campo de 4 bits de longitud destinado a indicar la versión del Protocolo de Internet utilizado, en este caso la versión 6.

- ***Traffic Class*:** campo de 8 bits, usado por los nodos de origen y/o los *routers* de retransmisión para identificar y distinguir entre distintas prioridades de paquetes IPv6.

- ***Flow Label:*** campo de 20 bits, usado por una fuente para etiquetar secuencias de paquetes con el objeto de darle, según se requiera, un manejo especial por parte de los *routers* IPv6, como parámetros de calidad de servicio fuera de los valores por defecto o servicios de datos en tiempo real.

- ***Payload Length:*** campo de 16 bits, los cuales representan la longitud de la carga útil del paquete IPv6, excluyendo los bits correspondientes a la cabecera en sí. Los bits de las "cabeceras de extensión" son considerados partes de la carga útil, por lo que se incluyen como parte de la longitud de ésta.

- ***Next Header:*** campo de 8 bits. Identifica el tipo de cabecera que sigue a la cabecera IPv6. Emplea los mismos valores usados en el protocolo IPv4, descritos en el RFC 3232.

- ***Hop Limit:*** campo de 8 bits. Su valor se reduce en una unidad por cada nodo que el paquete atraviesa; si su valor se reduce a cero el paquete es descartado. Su función es equivalente al campo *Time to Live (TTL)* de la cabecera IPv4.

- ***Source Address:*** campo de 128 bits, correspondientes a la dirección que originó el paquete.

- ***Destination Address:*** campo de 128 bits, correspondiente al destinatario del paquete. Este no debe corresponder necesariamente con el destinatario final, ya que puede existir un *Routing Header* como cabecera de extensión, indicando que existe al menos un nodo intermedio entre el nodo actual y el nodo final.

II.2.3 DHCPv6

El protocolo de configuración dinámica de clientes para IPv6 o *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*, es un protocolo que permite a un servidor DHCP otorgar parámetros de configuración a los clientes que lo soliciten, como por ejemplo direcciones de red IPv6. Igualmente, ofrece la capacidad de asignación automática de direcciones de red reutilizables y flexibilidad de configuración adicional. Este protocolo es una contraparte *stateful* a los mecanismos de autoconfiguración sin estado, y se puede utilizar por separado o al mismo tiempo con este último para obtener los parámetros de configuración.

A diferencia de DHCP para IPv4, en DHCPv6 se utiliza *multicast* en la fase de descubrimiento del servidor o agente de *relay* o de retransmisión para acceder a éste. Para ello, existen grupos *multicast* reservados para este procotolo:

- **Todos los agentes *relay* y servidores DHCP (FF02::1:2):** dirección *link-local multicast* usada por el cliente para comunicarse con los agentes de transmisión y servidores vecinos. Todo servidor y agente *relay* forma parte de este grupo *multicast.*
- **Todos los servidores DHCP (FF05::1:3):** dirección *site-local multicast* utilizada por los agentes *relay* para comunicarse con los servidores.

Con este protocolo se definen una serie de mensajes utilizados durante los procesos de negociación entre el cliente y el servidor o el agente *relay*. A continuación se detallan los más comunes:

1) *Solicit (1): un* cliente envía un mensaje de este tipo para ubicar servidores DHCP.

2) *Advertise (2):* un servidor envía un mensaje de este tipo para indicar que está disponible para prestar servicio DHCP, en respuesta a un mensaje *Solicit* enviado por un cliente.

3) *Request (3):* un cliente envía un mensaje de este tipo para hacer una petición de parámetros de configuración a un servidor específico, incluyendo direcciones IP.

4) *Reply (7):* un servidor envía un mensaje de este tipo conteniendo las direcciones asignadas por éste, así como los parámetros de configuración en respuesta a un mensaje *Solicit, Request,* entre otros. Igualmente, un servidor envía este tipo de mensaje para dar acuse de recibo ante la recepción de un mensaje de tipo *Release* o *Decline.*

5) *Release (8):* un cliente envía un mensaje de este tipo al servidor que le asignó la dirección IP a éste, indicando que no utilizará una o más de las direcciones previamente asignadas.

6) *Relay-Forw (12):* un agente *relay* envía un mensaje de este tipo a un servidor, ya sea directamente o a través de otro agente *relay*. El mensaje recibido en un principio, ya sea de un cliente o un mensaje *Relay-forward* procedente de otro agente *relay,* es encapsulado en una opción en el mensaje *Relay-forward.*

7) *Relay-Repl (13):* un servidor envía un mensaje de este tipo a un agente *relay* conteniendo un mensaje que se requiere enviar a un cliente. Puede atravesar más de un agente *relay* para llegar a su destino. El servidor encapsula el

mensaje del cliente como una opción en el mensaje *Relay-reply*, el cual es extraído por el agente *relay* y enviado al cliente.

Todos los mensajes DHCP enviados entre clientes y servidores comparten un formato de cabecera idéntico y un área con formato variable para las opciones. Las opciones son almacenadas de forma serial en el campo destinado para las mismas, sin relleno alguno entre las opciones. La Figura 7 muestra el formato de un mensaje DHCPv6 enviado entre clientes y servidores.

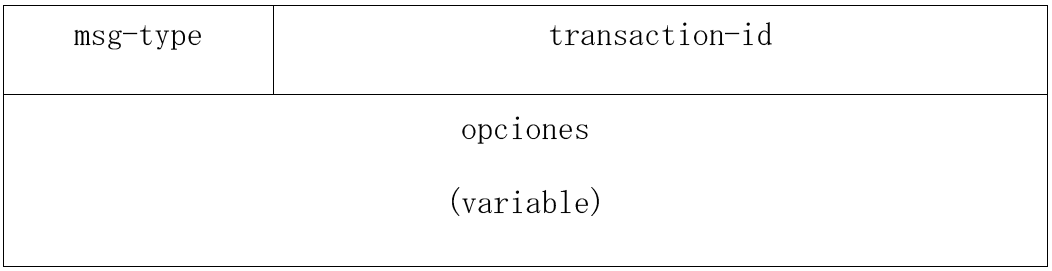

Figura 7: Formato de mensaje DHCPv6 enviado entre clientes y servidores.

Fuente: [13].

El campo *msg-type* identifica el tipo del mensaje DHCP. *Transaction-id* permite identificar el mensaje. El campo opciones está destinado a todas aquellas presentes en el mensaje.

Por otra parte, los agentes *relay* intercambian mensajes con servidores para hacer las modificaciones pertinentes entre los clientes y servidores que no están conectados en la misma red. Al igual que una solicitud DHCP entre clientes y servidores, las opciones se almacenan de forma serial en el campo destinadas para las mismas, sin relleno alguno entre las estas. La Figura 8 muestra el formato de un mensaje DHCPv6 entre dos agentes *relay*.

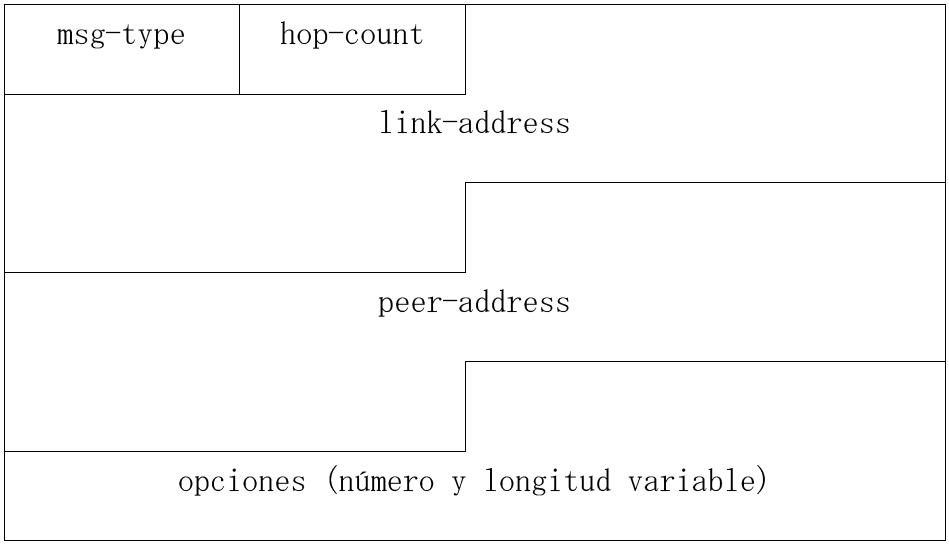

Figura 8: Formato de mensaje DHCPv6 enviado entre dos agentes *relay*.

Fuente: [13].

El campo *msg-type* puede representar un mensaje de tipo *relay-forw* o *relay-repl.* El campo *hop-count* represente el número de agentes *relay* que han retransmitido el mensaje. *Link-address* indica una dirección de alcance global o *site-local* que será utilizada por el servidor para identificar el enlace en el cual está ubicado el cliente. *Peer-address* representa la dirección del cliente o agente *relay* desde la cual el mensaje para retransmitir fue recibido. Por último, el campo opciones debe incluir un mensaje de "opción *relay"*aunque también pueden ser incluidas opciones adicionales por el agente *relay*.

II.2.4 *Domain Name System* para IP Versión 6.

Domain Name System (DNS) es un sistema de nombres distribuido jerárquico para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Se asocia información variada con nombres de dominio asignados a cada una de las entidades participantes. Su función más relevante es traducir los nombres de dominio de fácil memorización a las direcciones IP numéricas necesarias con el fin de localizar servicios y dispositivos informáticos en todo el mundo [14]. El sistema de nombres de dominio es un componente esencial de la funcionalidad de la Internet.

Los servidores DNS emplean una base de datos distribuida y jerárquica que almacena la información asociada a nombres de dominio en Internet. El DNS es capaz de asociar diferentes tipos de información a cada nombre; sin embargo, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

Es importante destacar que no es usual que un cliente comunique directamente con un servidor DNS, ya que la resolución de nombres se hace de forma transparente por las aplicaciones que éste ejecuta, ya sean navegadores, clientes de correo u otras aplicaciones que usan Internet. Al realizar una petición que requiere una búsqueda de DNS, la petición se envía al servidor DNS local del sistema operativo donde, antes de establecer alguna comunicación, verifica si la respuesta se encuentra en la memoria caché del mismo. En caso negativo, se procede entonces a enviar la petición a uno o más servidores DNS externos [14]. La Figura 9 describe el proceso en cuestión.

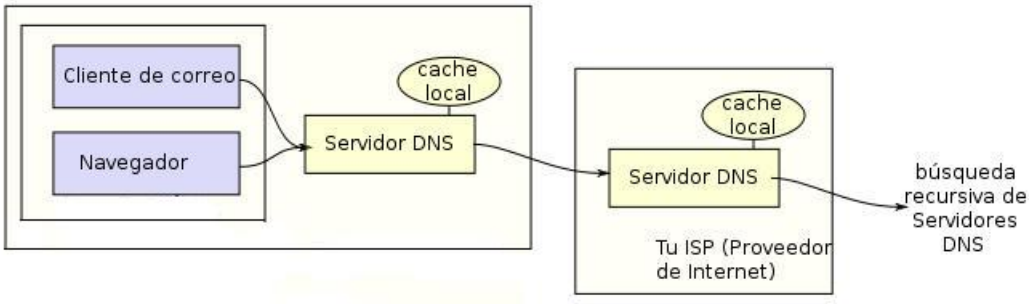

Figura 9: proceso de petición DNS por parte de un cliente.

Fuente: [14].

El espacio de nombres de dominio consta de una estructura de árbol. Cada nodo u hoja en el árbol tiene cero o más registros de recursos, que contienen la información asociada con el nombre de dominio. Los árboles se subdividen en zonas que comienzan en la zona *root* o raíz. Una zona DNS puede consistir en sólo un dominio,

o puede consistir en muchos dominios y subdominios, dependiendo de la autoridad administrativa delegada en el administrador. Es por ello que un nombre de dominio completo de un objeto consiste en la concatenación de todas las etiquetas de un camino, siendo las cadenas alfanuméricas (con '-' como único símbolo permitido), entre otras reglas definidas en el RFC 1035: Nombres de dominio – Implementación y Especificación.

La jerarquía de un dominio se lee de derecha a izquierda, donde las etiquetas individuales están siempre separadas por puntos, indicando aquél ubicado en el extremo derecho separación entre la etiqueta y la raíz de la jerarquía. La Figura 10 ilustra este comportamiento jerárquico.

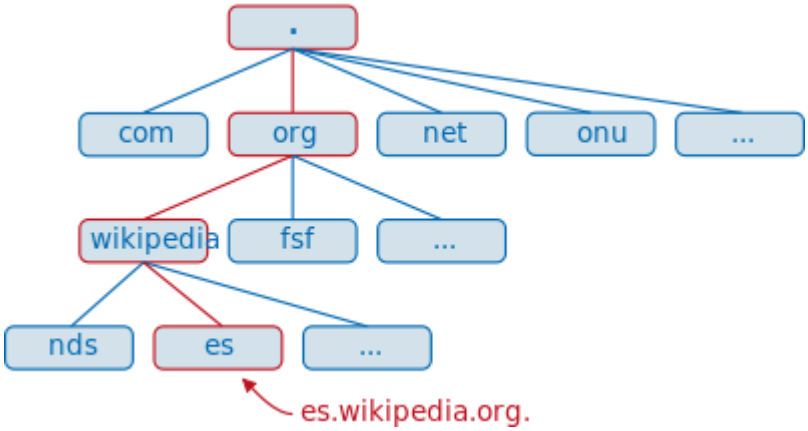

Figura 10: Ejemplo de jerarquía DNS.

Fuente: [15]

Si bien el uso de *Domain Name System (DNS)* en IPv4 está enfocado en un ámbito principalmente comercial, buscando facilitar al usuario final la navegación por sitios Web, se presenta en el futuro como un sistema de mayor y vital importancia en el mundo de la Internet y la Web. Debido a la gran longitud de una dirección IPv6, así como su formato de presentación hexadecimal, resulta de enorme complejidad e incluso imposible a la persona promedio la memorización de una dirección correspondiente al nuevo protocolo de Internet. Entre otras ventajas, destaca

igualmente el incremento del potencial de tecnologías como *Dynamic Domain Name System (DDNS)* [16].

En consecuencia, diferentes personajes y empresas como Microsoft y Cisco, han propuesto ante *The Internet Engineering Task Force (IETF)* una serie de extensiones para DNS que permitan el soporte de direcciones IPv6 en el mismo. Estos cambios incluyen un tipo de registro de recurso para almacenar una dirección IPv6, un dominio para soportar búsquedas basadas en una dirección IPv6, y definiciones actualizadas de los tipos de consulta existentes que devuelven las direcciones de Internet como parte de la sección adicional de procesamiento, siendo todas estas diseñadas para ser compatibles con las aplicaciones existentes [16].

Sin embargo, el soporte actual de direcciones en los DNS no pueden ser actualizadas fácilmente para dar soporte a direcciones IPv6, esto debido a que las diferentes aplicaciones asumen que las solicitudes de resolución de nombres devuelven únicamente direcciones IPv4 de 32 bits de longitud. Por ello, se plantean una serie de extensiones que permitan el almacenaje de direcciones IPv6 en un DNS [16]:

1) Un nuevo registro de recurso que permite mapear un nombre de dominio a una dirección IPv6.

2) Un dominio que dé soporte a búsquedas basadas en una dirección.

Estos cambios están diseñados para ser compatibles con el *software* existente, manteniendo el soporte para direcciones IPv4. Asimismo, la versión del Protocolo de Internet utilizado para hacer la solicitud de un registro de recurso es independiente de la versión del protocolo del registro de recurso en cuestión. Por ejemplo, se puede realizar una petición de un registro IPv6 haciendo uso de transporte IPv4 y viceversa [16].

En este sentido, se define un nuevo registro de recurso para almacenar una dirección IPv6 de un *host*, siendo posible manejar más de un registro si un *host* posee

más de una dirección IPv6 a la vez. Se denomina a este nuevo registro como "AAAA" (pronunciado *quad-A*), siendo la representación textual de la parte de datos del registro utilizado en un archivo de base de datos maestra la representación textual de una dirección IPv6 como se define en el RFC 3513: Arquitectura de Direccionamiento del Protocolo de Internet Versión 6 (IPv6) [16].

II.3 Protocolos de Enrutamiento en IPv6

Al igual que en IPv4 en *Internet Protocol version* 6 se utilizan protocolos de enrutamiento para facilitar el intercambio de información correspondiente a las rutas entre los *routers*, por lo tanto cuando todos los *routers* tienen la información de enrutamiento correcta en sus tablas, se puede decir que la red se encuentra en un estado estable.

En IPv6 se pueden encontrar los siguientes protocolos:

II.3.1 Routing Information Protocol New Generation (RIPng)

Es uno de los protocolos de enrutamiento menos utilizados en la actualidad, ya que su principal desventaja es que para determinar la métrica se basa en el número de saltos, descartando criterios de importancia como lo es el Ancho de banda, fiabilidad, retardo, entre otros.

RIPng es utilizado en redes pequeñas y utiliza el puerto UDP 521 para anunciar sus rutas y los cambios que han ocurrido en ellas (prefijo IPv6 y dirección del próximo salto), como también utiliza la dirección *multicast* FF02::9, que es "la dirección del grupo *multicast* de todos los *routers* que están ejecutando RIPng" [17]. Es un protocolo cuya técnica de enrutamiento es el vector distancia con la utilización del algoritmo de Bellman-Ford, y al igual que en RIPv2 el número máximo de saltos para alcanzar su destino es de quince (15).

Los *routers* IPv6 con RIPng pueden enviar actualizaciones instantáneas del enrutamiento si se presentan cambios en la topología de red. [7].

A continuación se pueden apreciar algunas diferencias de este protocolo con respecto a RIPv2:

- ✓ La autenticación RIPng se basa en la seguridad proveída por IPSec.
- ✓ RIPng anuncia rutas IPv6 compuestas de prefijos IPv6 con longitud y métrica.
- ✓ La tabla de enrutamiento de IPv6 es distinta de la tabla de enrutamiento de IPv4 para RIPv1 o RIPv 2. La ruta por defecto es anunciada como ::/0.

II.3.2 Open Shortest Path First Version 3 (OSPFv3)

Es uno de los protocolos de enrutamiento más utilizados, y trabaja con la técnica de estado de enlace (algoritmo de Dijkstra) para el enrutamiento de sus paquetes. Este protocolo usa la definición de áreas para mejorar la administración, las cuales son numeradas siendo cada una de ellas una red o un conjunto de redes, conformadas por *router*s. Fuera de un área no se pueden observar los detalles de la misma.

Existen diferentes tipos de áreas como lo son [18]:

- Área *BackBone* o Área cero: es la única área que mantiene una conexión lógica o física con todas las áreas que estén configuradas en la red.
- Área *Stub*: no recibe rutas externas. Las rutas externas se especifican como rutas que fueron colocadas en OSPF desde otro protocolo de enrutamiento como por ejemplo Ripng, BGP4, entre otros..
- Área *not-so-stubby*: puede introducir rutas externas de sistemas autónomos (AS) y enviarlas al *BackBone*.

OSPFv3 está diseñado para operar en un mismo sistema autónomo, es decir, es un protocolo de enrutamiento interior. A diferencia de RIPng, sí toma en cuenta criterios como Ancho de Banda y retraso, entre otros que pueden ser relevantes para la selección de rutas adecuadas. Trabaja a nivel de red con *multicast*, diferenciándose de RIPng que emplea UDP y un puerto en capa de transporte.

Permite la sumarización o agregación de la información de enrutamiento en los límites de un área de OSPF, la cual se conoce como zona del *router* de frontera [7].

OSPFv3 mantiene al igual que en OSPFv2 los siguientes tipos de *routers* [18]:

- **ABRs (*Area Border Routers*):** son aquellos *routers* que conectan su área con el resto de áreas que pertenecen a la red. Mantienen la información de la topología de su red.

- **ASBRs (*Autonomous System Border Routers*):** permiten el envío de paquetes a redes pertenecientes a otro sistema autónomo.

Se puede observar en la siguiente tabla los tipos de paquetes que existen en OSPFv3 y la descripción de los mismos:

Paquetes OSPFv3	Descripción
Hello	Estos paquetes se envían periódicamente en todas las interfaces (incluyendo enlaces virtuales) con el fin de establecer y mantener relaciones entre vecinos.
DataBase Description	Estos paquetes se intercambian cuando se inicializa una adyacencia.
Link State Request	Después de intercambiar paquetes *DataBase Description* con un *router* vecino, un *router* puede encontrar que partes de su base de datos *Link State* están fuera de fecha.
Link State Update	Implementan la saturación de los LSAs (*Link State Advertisements*). Cada paquete *Link State Update* lleva una colección de LSAs un salto más lejos de su origen.
Link State Acknowledgment	Proveen fiabilidad al proceso de cambio de estado de enlace, reconociendo explícitamente la recepción de un mensaje *Link State Update*.

Tabla 8: Descripción de paquetes en OSPFv3.

Fuente: [18].

Las redes con múltiples *routers* presentan una situación única para OSPFv3. Si cada *router* satura la red con LSA, la misma información de estado de enlace se envía desde múltiples fuentes. Dependiendo del tipo de red OSPFv3 podría usar un solo *router*, el *router* designado (DR), para controlar los *flooding* de LSA y representar la red con el resto de la zona OSPFv3. Si el DR falla, el protocolo de enrutamiento selecciona un *router* designado de respaldo (BDR).

El DR y BDR se seleccionan sobre la base de la información en el paquete *HELLO*, cuando una interfaz envía este paquete, establece el campo de prioridad y el

campo DR y BDR. Todos los demás *routers* establecen adyacencia con el DR y BDR [18].

A continuación puede observar algunas diferencias entre este protocolo y OSPFv2:

- ✓ LSAs de *router* y red: Estos no tienen semántica de direccionamiento y sólo llevan información de topología.
- ✓ Direcciones en LSA: Estas son descritas como prefijo con una longitud de prefijo. La ruta por defecto es ::/0.
- ✓ La dirección de Siguiente-Salto es la dirección de enlace-local IPv6 de la interfaz del *router* que anuncia el prefijo.
- ✓ Nuevo LSA de Enlace-Local: Este lleva la dirección de enlace local de la interfaz del *router*, los prefijos del enlace y las opciones.
- ✓ Se eliminaron todos los datos de autenticación interna OSPF y ahora se provee seguridad con IPSec para proteger la integridad y ofrecer autenticación.
- ✓ Las direcciones *multicast* son FF02::5 para todos los *routers* OSPF y FF02::6 para todos los DR y BDR.

Por último, el protocolo de inundación o *flooding* consta básicamente en el envío de mensajes entre los diferentes *router*s o nodos de la red, partiendo el mensaje del *router* o *routers* que han advertido el cambio, de modo que cada *router* envía el mensaje recibido por todas sus interfaces menos por la que fue recibido, siempre y cuando no haya capturado ese mensaje. Para ello, cada mensaje dispone de un identificador de mensaje o contador de tiempo que permite constatar su validez [18].

A continuación puede observar en la Figura 11 el *Header* del paquete OSPFv3:

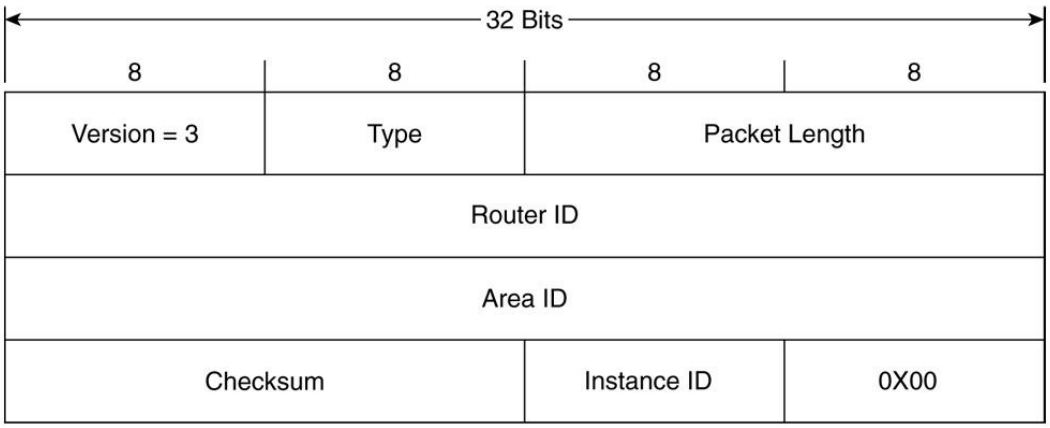

Figura 11: *Header* del paquete OSPFv3.

Fuente: [19].

En la Figura anterior se pueden observar diferentes campos, cuya explicación se presenta a continuación [18]:

- ***Version:*** el número de versión de OSPF.
- ***Type*****:** Los tipos de paquetes OSPF mencionados en la Tabla 8.
- ***Packet Length*****:** La longitud del paquete de protocolo OSPF en bytes . Esta longitud incluye el encabezado estándar OSPF.
- ***Router ID*****:** La ID del *router* de origen del paquete.
- ***Area ID:*** Un número de 32 bits que identifica el área a la que pertenece este paquete. Todos los paquetes OSPF se asocian a una sola área. Los paquetes que pasan un enlace virtual se etiquetan con el ID de área de red troncal 0.
- ***Checksum*****:** OSPF utiliza el cálculo de suma de control estándar para aplicaciones IPv6. Si la longitud del paquete no es un número de palabras de 16 bits, el paquete se rellena con un byte de cero antes de la suma de comprobación. Antes de calcular la suma de comprobación, el campo de la suma de comprobación en el encabezado del paquete OSPF se establece en cero (0).

- ***Instance ID*:** Permite múltiples instancias de OSPF que se ejecutan sobre un único enlace. Cada instancia del protocolo se le asigna un ID de instancia separada; el ID de instancia sólo tiene significado local de enlace.
- **0X00:** Estos campos están reservados. Se debe establecer en cero (0) cuando se envían paquetes de protocolo y deberá ser ignorada cuando reciben paquetes de protocolo.

II.3.3 Intermediate System to Intermediate System (Is-Is)

Es un protocolo que utiliza la técnica de estado de enlace y el algoritmo de Dijkstra para encontrar el camino más corto. Es un protocolo sin clase, permitiendo así trabajar con máscaras variables.

"Para el manejo de IPv6 con IS-IS solamente se requiere la creación de un nuevo identificador de protocolo y dos nuevos tipos de TLV, IPv6 *reachability* y IPv6 *interface address*" [17].

IS-IS me permite una actualización de enrutamiento que incluya rutas IPv4 e IPv6, resultando la utilización con mayor eficiencia de los enlaces.

Opera bajo el *Connectionless Network Service* (CLNS), el cual es un servicio de la capa de red OSI. Permite dos niveles de escala jerárquica y es análogo a un sistema autónomo (AS) en TCP/IP.

II.3.4 Border Gateway Protocol 4 (BGP4)

Es un protocolo de enrutamiento exterior, es decir, se encarga de la conexión entre sistemas autónomos. Es un protocolo que utiliza la técnica de vector camino, no hace uso de la métrica, por lo tanto utiliza una serie de atributos para seleccionar el camino más adecuado.

Este protocolo utiliza CIDR para el resumen de rutas. "La información de enrutamiento de BGP-4 es usada para crear un árbol lógico que describe a las

conexiones entre los diferentes sistemas autónomos [7]". Los mensajes en este protocolo son enviados por el puerto TCP 179.

BGP en IPv6 utiliza un *Router ID* que es un valor de 32 bits que normalmente es una dirección IPv4, para identificar los *peers* (vecinos) BGP. En el caso de que el proceso de éste protocolo utilizara sólo IPv6, sería necesario configurar manualmente el *Router ID* [20].

Posee la capacidad de configurar diferentes tipos de *Address Family*, IPv4 *unicast*, IPv6 *unicast*, IPv6 *multicast*, entre otras, configurando en cada una de ellas las redes que se van a publicar, como también se deben activar los *neighbords* en cada *Address Family*.

BGP4 presenta los siguientes paquetes para establecer comunicación entre los Sistemas Autónomos (AS) y mantener un funcionamiento eficiente entre los mismos [20]:

- *OPEN*: es el primer mensaje enviado por cada sistema autónomo al establecer una conexión TCP. Si el mensaje es aceptado, se envía un mensaje *KEEPALIVE* confirmando que el mensaje *OPEN* es enviado de vuelta.

- *UPDATE*: se utiliza para transferir información de enrutamiento entre compañeros BGP.

- *KEEPALIVE*: BGP no utiliza ningún mecanismo de conexión basada en TCP para determinar si los compañeros son accesibles. En su lugar, se intercambian mensajes *KEEPALIVE* entre pares con la suficiente frecuencia.

- *NOTIFICATION*: se envía este mensaje cuando se detecta una condición de error. La conexión BGP se cierra inmediatamente después de que se envíe.

Sin embargo este protocolo no tiene grandes diferencias con respecto a IPv4. Se pueden aplicar filtros y políticas similares a las que existen en IPv4.

II.4 Mecanismos de Transición a IPv6

En la actualidad la mayoría de las redes posee una infraestructura IPv4, que da soporte a una gran variedad de aplicaciones, principalmente en *Internet*. El agotamiento de las direcciones IP, el requerimiento de una mayor capacidad para el soporte de nuevas redes y aplicaciones, entre otros problemas, han traído como consecuencia la creación de nuevas alternativas para superarlos.

IPv6 es diseñado luego de que la nueva creación "NAT", elaborada para solucionar el problema de agotamiento de direcciones, presentara diversas fallas. Sin embargo, este nuevo protocolo se crea con nuevas opciones, entre ellas un espacio de direccionamiento más grande, más seguridad y confiabilidad para dar soporte a las redes de nueva generación, entre otros.

Desafortunadamente, debido a que los protocolos IPv4 e IPv6 son incompatibles, se requieren "mecanismos de transición" cuando por ejemplo, dos nodos con ambas versiones del protocolo desean conectarse entre sí. Por ello, *The Internet Engineering Task Force (IETF)* ha propuesto una serie de mecanismos de transición para garantizar que ésta se lleve a cabo de forma gradual e independiente, a través de servicios basados en IPv6 y ejecutados en la internet IPv4 [21].

Asimismo, en conjunto con estos mecanismos de transición, existe una serie de recomendaciones en cuanto a la distribución de direcciones IPv6 a los usuarios finales de un ISP [22], así como las etapas o fases que se deben seguir para la

introducción del protocolo IPv6 en su red actual basada en IPv4, sin perturbar ni alterar los servicios que el ISP presta actualmente [23].

Los mecanismos de transición propuestos por la *IETF Next Generation Transition Working Group (NGtrans)* se dividen en tres grupos principales: *dual stack, tunneling* y técnicas de traducción, las cuales pueden y es común que sean usadas de manera conjunta unas con otras [24].

II.4.1 Dual Stack

Descritos como el "modo más directo" de proveer compatibilidad entre un nodo IPv6 y un nodo IPv4. Esta clase de nodo es capaz de enviar y recibir tanto paquetes IPv4 como paquetes IPv6. En efecto, se comunican con nodos IPv4 utilizando paquetes IPv6 y con nodos IPv6 utilizando paquetes IPv6 [25].

En un nodo con este mecanismo implementado, se incluyen las pilas de ambos protocolos paralelamente (Figura 12).

Los criterios usados para discernir cuál tipo de paquete utilizar se basan en el campo *"Version"* de la cabecera IP recibida y en el tipo de dirección de destino del paquete a enviar [21].

Debido a que este mecanismo de transición permite únicamente que los nodos pertenecientes a redes similares se comuniquen entre sí, se requiere la implementación de otras técnicas para crear una solución completa que permite la comunicación entre ambos protocolos, incluso cuando hoy en día la mayoría de los sistemas operativos soportan *Dual Stack* [21] [26].

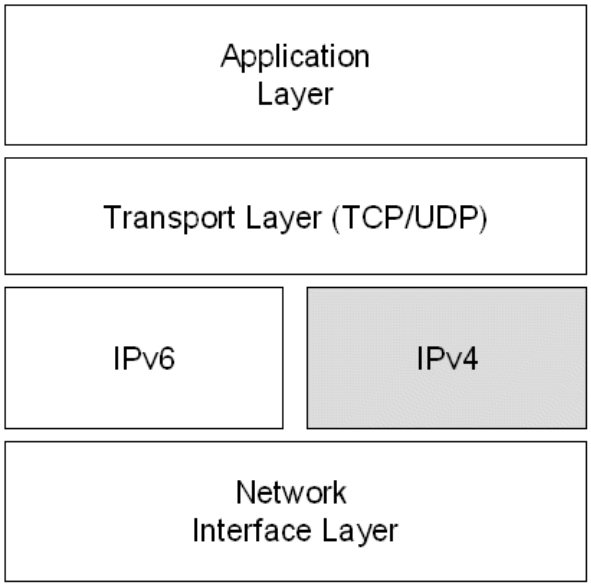

Figura 12: Distribución de capas en *Dual Stack*.

Fuente: [25].

En cuanto a la configuración de direcciones, y debido a que un nodo *Dual Stack* opera con ambas versiones del protocolo, éste tendrá tanto una dirección IPv4 como una dirección IPv6, configuradas independientemente una de otra. Es decir, la dirección IPv4 será asignada por mecanismos IPv4 (como por ejemplo, DHCPv4) y la dirección IPv6 será asignada por mecanismos IPv6 (como por ejemplo mecanismos de autoconfiguración de direcciones sin estado o DHCPv6).

Por su parte, tanto en IPv4 como en IPv6 se hace uso del sistema DNS. En el caso de IPv6, se define un nuevo tipo de recurso denominado "AAAA". Debido a que un nodo con *Dual Stack* es capaz de operar directamente con ambas versiones del protocolo IP, debe igualmente ser capaz de proveer "librerías de resolución" aptas para hacer frente tanto a registros IPv4 "A" como registros IPv6 "AAAA" [27].

II.4.2 Tunneling

Los mecanismos de *tunneling* permiten desplegar una red IPv6 "de reenvío" sobre una infraestructura basada en IPv4 que no puede o no debería ser modificada o

actualizada provisionalmente. Debido a su modo de operación, también se le denomina "encapsulamiento", ya que un protocolo es encapsulado en la cabecera de otro protocolo y reenviada la información sobre la infraestructura del segundo; en este caso, se encapsula el protocolo IPv6 sobre el protocolo IPv4 [24].

Este proceso de encapsulado consta de tres componentes:

- Encapsulación en la entrada del túnel.
- Desencapsulación en salida del túnel.
- Administración y manejo del túnel.

Las técnicas de *tunneling* y de encapsulado de paquetes IPv6 en paquees IPv4 son definidas en varios RFCs, los cuales, a rasgos generales, describen dos tipos generales de túneles [24]:

- **Túnel configurado manualmente:** en este tipo de túnel los paquetes IPv6 son encapsulados sobre paquetes IPv4 y manejados sobre una infraestructura de red IPv4. Las direcciones de entrada y salida del túnel son determinadas en el encapsulador a través de la información almacenada en cada túnel, la cual es configurada manualmente [24] [25]. Son utilizados especialmente en conexiones *router-to-router*, debido a la necesidad de configurar de manera explícita los puntos de entrada y salida del túnel. Esta clase de túneles presenta una carga elevada de trabajo administrativo; sin embargo, por razones de seguridad, en adición a mayor capacidad de control sobre el reenvío de paquetes IPv6, hace que este tipo de túnel sea más conveniente de usar en determinadas circunstancias [24].

- **Túnel automático de IPv6 sobre IPv4:** en este caso, los nodos IPv6 pueden usar diferentes tipos de direcciones para generar dinámicamente un túnel que encapsule paquetes IPv6 sobre una infraestructura y paquetes IPv4 (como se explicará más adelante en túneles 6to4 o ISATAP, por ejemplo). Estas direcciones IPv6

especiales portan una dirección IPv4 en alguna parte de los campos de la dirección IPv6 [24].

Las componentes principales de un túnel se describen en la Figura 13.

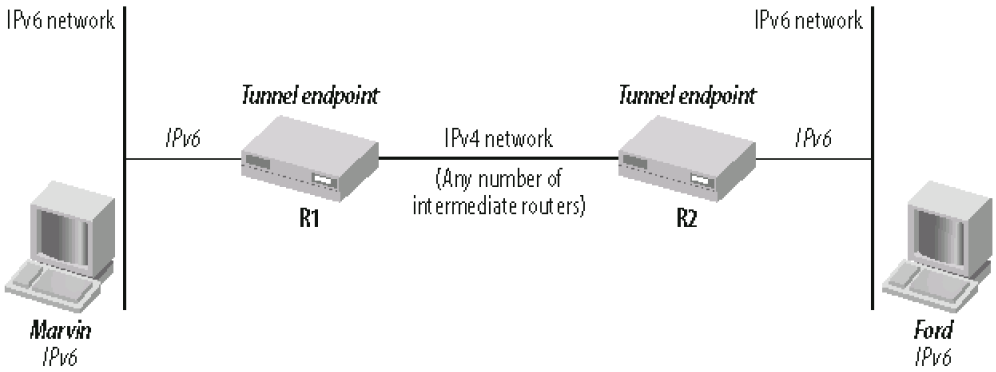

Figura 13: Componentes generales de un túnel.

Fuente: [24].

Entre los principales túneles automáticos destacan:

1) Túnel 6to4: esta clase de túnel permite el envío de paquetes IPv6 encapsulados en paquetes IPv4 sin la necesidad de configurar manualmente las direcciones de salida y entrada del túnel. Consiste en una mejora del "túnel automático" descrito en el RFC 2893, en el cual se hacía uso de una dirección de destino "IPv4 compatible" para determinar la dirección de salida de túnel. En el túnel 6to4 este tipo de dirección es descartada, haciendo uso de su propio formato de direcciones la cual incluye la dirección IPv4 de salida del túnel en el prefijo de la dirección IPv6, permitiendo configurar el túnel de manera automática. En este mecanismo, se manejan las redes IPv4 existentes como enlaces punto a punto, que permiten a los sistemas nativos IPv6 comunicarse a través de ellas por medio de un *router* 6to4 (también denominado *"6to4 gateway"*), el cual es el único que necesita ser consciente de poseer esta configuración. De este modo los paquetes IPv6 son encapsulados en paquetes IPv4 en los *routers* 6to4, requiriendo al menos una dirección IPv4 pública única [24].

Para el esquema 6to4, la IANA ha asignado un Agregador de Nivel Superior (*Top Level Aggregator (TLA)*, por sus siglas en ingles) de 13 bits para su identificación bajo el *format prefix (FP)* IPv6 de 3 bits "001". Este corresponde a 2002::/16 si es expresado como un prefijo de dirección IPv6 [28].

En la Figura 14 se muestra el formato del prefijo 6to4.

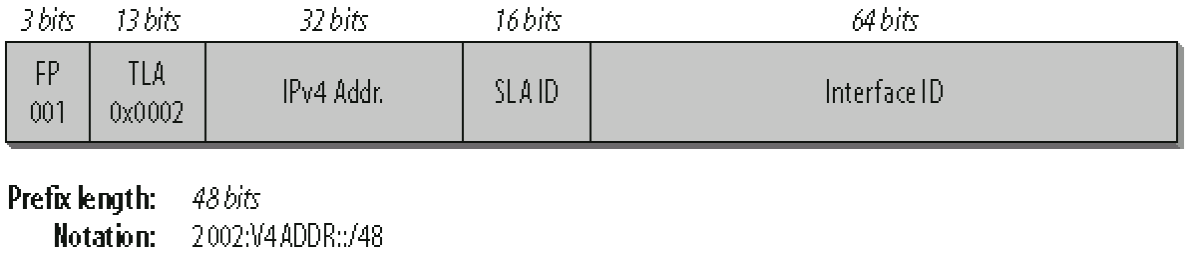

Figura 14: Formato prefijo 6to4.

Fuente: [24].

De esta forma, el prefijo tendrá exactamente el mismo formato que una red /48 entregada por un *Regional Internet Registry (RIR)*. Éste puede abreviarse como se muestra en la Figura 12: 2002:V4ADDR::/48.

2) ISATAP: denominado *Intra-Site Automatic Tunnel Addressing Protocol*, es descrito en el RFC 5214 [29]. Al igual que los túneles 6to4, permite la conexión de nodos IPv6 a través de redes basadas en una infraestructura IPv4. Se manejan igualmente las redes IPv4 existentes como enlaces punto a punto que permiten la configuración automática del túnel entre los nodos con *Dual Stack* que desean conectarse entre sí. Sin embargo, a diferencia de los túneles 6to4, este mecanismo puede usarse incluso cuando no se dispone de una dirección IPv4 pública única. El formato de direcciones ISATAP incluye una dirección IPv4 al momento de obtener la dirección IPv6 por autoconfiguraciones sin estado y a diferencia de los túneles 6to4, todos los nodos en una red ISATAP necesitan soportar dichas características [24].

En la Figura 13 se muestra el formato de una dirección ISATAP.

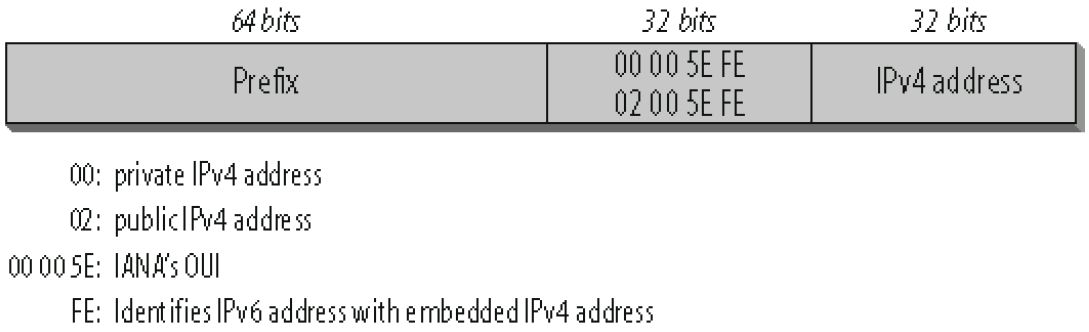

Figura 15: Formato dirección ISATAP.

Fuente: [24].

Los 64 bits correspondientes al prefijo tienen una configuración estándar y pueden pertenecer a cualquier prefijo o formato previamente establecido. En cambio, los 64 bits del identificador de interfaz están conformados por 8 bits que permiten indicar si la dirección IPv4 incluida en la dirección ISATAP corresponde a una dirección privada o pública, como se indica en la Figura 15. Seguidamente están presentes 24 bits correspondientes con el OUI (*Organizationally unique identifier*, o Identificador único de organización, por sus siglas en inglés) de la IANA "00 00 5E". El byte siguiente corresponde a un indicador de "tipo de campo", cuyo valor "FE" indica que la dirección contiene dentro de sí una dirección IPv4 [24]. Por último, los 4 bytes finales corresponden a la dirección IPv4 embebida.

3) Teredo: es descrito en el RFC 4380 [30]. Diseñado para permitir la conexión de dispositivos que soportan IPv6 a través de una o más capas de dispositivos que soportan NAT, esto a través del encapsulado de paquetes sobre *User Datagram Protocol (UDP)* [24].

Los sistemas NAT generan problemas al momento de hacer túneles IPv6 sobre redes IPv4 por dos razones fundamentales: los usuarios de NAT poseen una dirección IPv4 privada y, además, las configuraciones típicas de NAT suelen incluir filtros en el

tráfico de entrada y no permiten el paso de muchos tipos de *payload* a través de ellos [24].

Debido a que una gran cantidad de usuarios, principalmente residenciales, logran su acceso a *Internet* a través de NATs, y que los sistemas de *tunneling* descritos anteriormente encapsulan la información de los paquetes IPv6 en el *payload* del paquete IPv4, se plantea Teredo como solución temporal mientras se desarrolla la transición a IPv6 y en la cual habrá que hacer frente con las NATs que existen actualmente en las redes IPv4 [24].

Sin embargo, la complejidad de un túnel Teredo es mayor y se definen una serie de términos y componentes en su uso, como son *Teredo Service* (transmisión de paquetes IPv6 sobre UDP), *Teredo Server* (nodo que dispone de acceso a la internet IPv4 a través de una dirección IPv4 pública y es usada para proveer conectividad IPv6 a los clientes Teredo), *Teredo UDP Port* (puerto UDP en el cual servidores Teredo están a la escucha por paquetes nuevos. Su valor es 3544), *Teredo-mapped Address* y *Teredo-mapped Server* (consisten en una dirección IPv4 y un puerto UDP globales, resultantes de la traducción por parte de uno o más NATs de la dirección IPv4 y el puerto UDP de un cliente Teredo) o *Teredo IPv6 Service Prefix* (prefijo IPv6 utilizado para construir la dirección IPv6 de los clientes Teredo. Este es asignado por la IANA y corresponde a 2001:0::/32) [30].

En la Figura 16 se muestra el formato de una dirección Teredo.

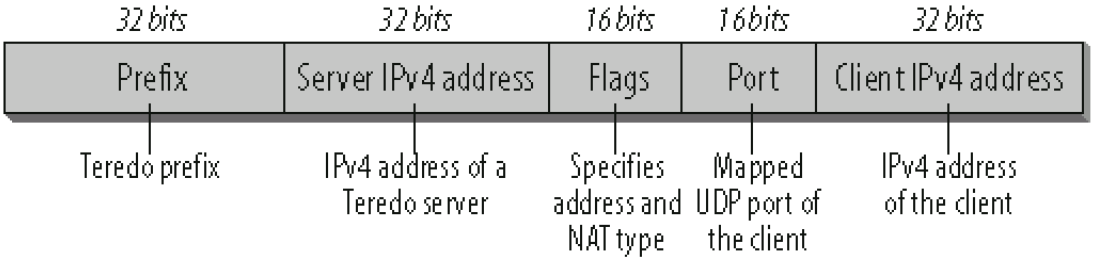

Figura 16: Formato dirección Teredo.

Fuente: [24].

El campo *"Server IPv4 address"* tiene una longitud de 32 bits y corresponde a la dirección IPv4 del *server* Teredo que está prestando el servicio al cliente actual. El campo *"Flags"* tiene una longitud de 16 bits y especifica la dirección y el tipo de NAT utilizado. El campo *"Port"* contiene el puerto UDP mapeado del servidor Teredo en el cliente. Por último, el campo *"Client IPv4 address"* contiene la dirección IPv4 mapeada del cliente.

4) ***Tunnel Broker:*** descritos en el RFC 3053 [31]. Pueden ser vistos como "proveedores virtuales de IPv6", capaces de otorgar conectividad IPv6 a usuarios con una conexión IPv4 a *Internet* [24]. Debe existir conectividad IPv4 entre el cliente y el proveedor del servicio; además, el cliente debe poseer una dirección IPv4 pública [21] [24].

Para que el servicio opere correctamente, el usuario debe contactar en principio al proveedor del túnel para realizar el registro correspondiente. Una vez realizado el registro se comunican de nuevo para el proceso de autenticación y otorgar la información necesaria para la configuración del túnel (como dirección IP, sistema operativo, etc.). Finalmente el proveedor del túnel configura el punto de salida del túnel y el servidor DNS, dejando el túnel listo y activo para ser usado por el cliente.

La Figura 17 describe las conexiones que se generan al operar un *Tunnel Broker.*

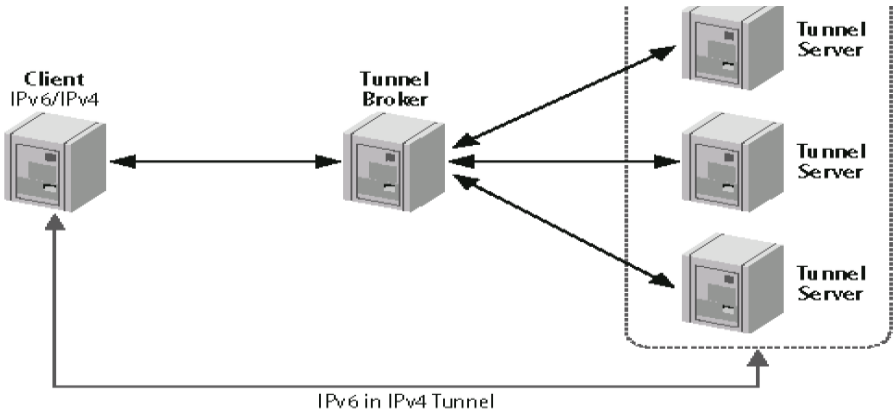

Figura 17: Conexiones generadas al operar un *Tunnel Broker*.
Fuente: [24].

5) ***IPv6 Rapid Deployment (6rd):*** IPv6 *Rapid Deployment* (6rd) se basa en el mecanismo 6to4 para habilitar a un proveedor de servicios en el despliegue de servicios *unicast* IPv6 a sitios IPv4 equipados con un CPE. Al igual que 6to4, utiliza encapsulación sin estado de IPv6 en IPv4 para permitir así el tráfico en infraestructuras de red que operan únicamente bajo IPv4 **[32]**.

Sin embargo, a diferencia de 6to4, un proveedor de servicios que maneje 6rd utiliza un prefijo de IPv6 de su propiedad en lugar del prefijo bien conocido correspondiente a 6to4 (2002::/16).

Un proveedor de servicios francés, específicamente Free, utilizó este mecanismo para su propia "implementación rápida" de IPv6: transcurrieron tan solo cinco semanas desde la primera exposición de los principios de 6rd hasta haber más de 1.500.000 usuarios residenciales siendo provistos con IPv6 nativo, con la única condición de que activasen dicho servicio.

5.1) Implementación por parte de Free

Después de haber tenido una breve presentación del concepto de 6rd, Free, importante ISP francés, llevó a cabo todo lo listado a continuación en tan solo cinco semanas, desde el 7 de noviembre hasta el 11 de diciembre de 2007 [32]:

1) Obtuvo un prefijo IPv6 con máscara /32 de su RIR correspondiente.

2) Añadió soporte 6rd al *software* de su "*Freebox home-gateway"* (actualizando para ello un código 6to4 existente).

3) Aprovisionó la plataforma compatible con PC con un *software* de *Gateway* 6to4.

4) Modificó dicho *software* para ser compatible con 6rd.

5) Probó la operación del protocolo IPv6 con varios sistemas operativos y aplicaciones.

6) Finalizó el despliegue operacional por medio de una nueva versión del *software* descargable de sus *Freeboxes.*

7) Anunció conectividad a Internet con IPv6, sin costo extra, para todos sus clientes que deseasen activar el servicio.

5.2) ¿Por qué 6rd?

La mayoría de los ISPs no desean añadir IPv6 a su oferta actual de forma gratuita a menos que la inversión realizada y los costos operacionales sean extremadamente limitados. Para esto, los ISPs que proveen *routers* CPE a sus clientes, presentan las condiciones más favorables: estos pueden actualizar sus *routers* CPE y pueden operar como *gateways* entre sus infraestructuras IPv4 y el Internet IPv6 global, permitiendo de este modo la encapsulación de IPv6 sobre IPv4. De este modo, no necesitan más planes de enrutamiento que aquellos ya existentes en su infraestructura IPv4 [32].

Por tanto, la encapsulación como se describe en 6to4 está muy cercana a ser suficiente para este fin; sin embargo, existe una limitación que impide a los ISPs utilizarlo para ofrecer total conectividad *unicast* IPv6 a sus clientes. Mientras que un ISP que implementa 6to4 puede garantizar que los paquetes IPv6 salientes desde sus clientes serán capaces de alcanzar el Internet IPv6, y además garantizar que los paquetes provenientes de otros sitios 6to4 alcanzarán a sus clientes, no puede garantizar que los paquetes provenientes de sitios IPv6 nativo serán capaces de alcanzar a sus clientes. El problema consiste en que un paquete proveniente de una dirección IPv6 nativa necesita atravesar, en algún punto de su recorrido, un relé 6to4 para realizar la encapsulación IPv6/IPv4 requerida. No hay garantías de que existan rutas hacia un relé provenientes desde todas partes, ni hay garantía de que dichos relés hagan el reenvío de los paquetes hacia la totalidad del Internet IPv4.

Además, si un ISP opera uno o varios relés enrutadores 6to4 y abre rutas IPv6 hacia ellos en el Internet IPv6, para el prefijo 2002::/16, puede recibir en estos relés paquetes destinados a un número desconocido o hacia un 6to4 de otro ISP. Si éste no reenvía dichos paquetes, se creará un "agujero negro" en el cual los paquetes pueden perderse sistemáticamente, rompiendo parte de la conectividad IPv6. Por otro lado, si reenvía dichos paquetes, el ISP no será capaz de dimensionar sus relés enrutadores 6to4 en proporción al tráfico de sus propios clientes; en consecuencia, la calidad de servicio, al menos para los clientes 6to4 de otros ISPs será difícilmente garantizada [32].

El propósito de 6rd es modificar ligeramente 6to4 de modo que solo aquellos paquetes provenientes de Internet, destinados a los clientes de un ISP, arriben a los *gateways* 6rd del mismo. Asimismo, busca garantizar que todos los paquetes IPv6 destinados a los clientes 6rd de un ISP, y procedentes de cualquier otro lugar en la Internet IPv6, atraviesen un *gateway* 6rd de este ISP.

5.3) Especificaciones

Debido a que en un principio se define a 6rd como una versión mejorada de 6to4, es suficiente implementar en este último una serie de cambios, como son [33]:

1) Modificar las funciones de 6to4 remplazando su prefijo estándar 2002::/16 por un prefijo que pertenece al espacio de direcciones asignado al ISP. Igualmente, remplazar la dirección *anycast* 6to4 por una diferente seleccionada por el ISP.

2) El ISP operará uno o varios *gateways* 6rd (los cuales son simplemente versiones mejoradas de un *router* 6to4) en sus fronteras entre su infraestructura IPv4 y la Internet IPv6.

3) Los CPEs deben soportar IPv6 en su lado correspondiente al cliente y soportar 6rd en el lado correspondiente al proveedor.

La Figura 18 describe la estructura de una red con 6rd implementado.

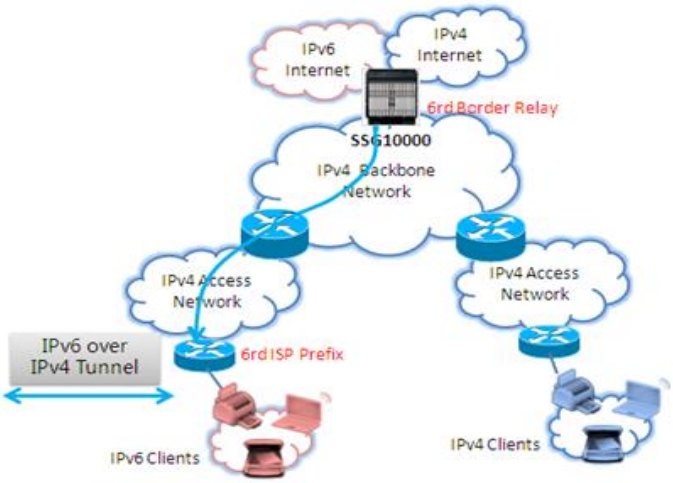

Figura 18: Despliegue rápido de IPv6.

Fuente: [34]**.**

Dentro de los conceptos tratados en 6rd, se maneja el "prefijo 6rd delegado" para el uso dentro de la red del cliente, el cual es creado al combinar el prefijo 6rd seleccionado por el ISP para su uso en su red y toda o parte de la dirección IPv4 del cliente. En 6to4, se incorpora una dirección IPv4 completa en una ubicación determinada conforme a un prefijo /16 IPv6 bien conocido; sin embargo, en 6rd el prefijo IPv6 así como la posición y el número de bits de la dirección IPv4 incorporada, varían de un dominio 6rd a otro. Éste permite a un proveedor de servicios ajustar el tamaño del prefijo 6rd, cuántos bits son usados por el mecanismo 6rd y cuántos bits son delegados a direcciones del cliente [33].

Dicho prefijo es creado al concatenar el prefijo 6rd y una serie ordenada de bits consecutivos de la dirección IPv4 del cliente. En consecuencia, la longitud del prefijo 6rd delegado es igual a la longitud del prefijo 6rd más el número de bits tomados de la dirección IPv4 del cliente.

La Figura 19 muestra cómo se deriva el prefijo IPv6 de la red de un cliente final a partir de su dirección IPv4.

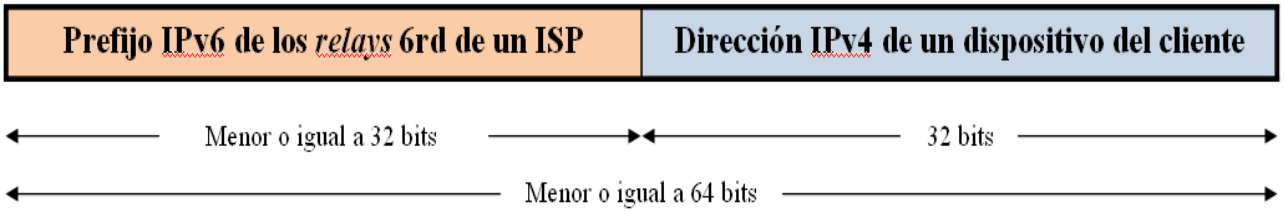

Figura 19: Formato del prefijo IPv6 asignado a un cliente 6rd.

Fuente: [33]**.**

Por ejemplo, si el prefijo 6rd es /32 y son utilizados 24 bits de la dirección IPv4 del cliente, entonces se puede calcular automáticamente el tamaño del prefijo 6rd delegado para cada equipo del cliente como /56 (32 + 24 =56).

Incorporar menos de los 32 bits de una dirección IPv4 completa es posible únicamente si está disponible un bloque sumarizado de direcciones IPv4 para un dominio 6rd dado. Si bien puede no resultar práctico con direcciones IPv4 globales, lo es en gran medida cuando se les asignan direcciones privadas a los equipos del cliente. Si las direcciones privadas se superponen o solapan dentro de un despliegue 6rd específico, éste puede ser dividido en dos dominios 6rd separados, probablemente en el mismo sentido que la infraestructura IPv4 basada en NAT lo requiera, siendo en este último caso asignado un prefijo 6rd diferente para cada dominio [33].

Cada dominio 6rd puede usar una codificación diferente para la dirección IPv4 embebida, incluso dentro del mismo ISP. Por ejemplo, si se utilizan diferentes niveles de sumarización en múltiples bloques de direcciones en la red de un proveedor de servicios, puede variar entonces entre cada bloque el número de bits necesarios de la dirección IPv4 para codificar el prefijo 6rd delegado. En este caso pueden ser utilizados prefijos 6rd diferentes, y en consecuencia dominios 6rd distintos, para permitir diferentes codificaciones [33].

Debido a que los prefijos 6rd delegados son seleccionados algorítmicamente a partir de una dirección IPv4, la modificación de esta última causará un cambio en el prefijo IPv6 delegado, el cual se propagaría a través de la red del operador, pudiendo causar efectos perjudiciales. Por lo tanto, se recomienda que el ISP asigne direcciones IPv4 a sus clientes con ciclos de vida relativamente largos [33].

La asignación de direcciones IPv6 6rd, y por lo tanto el servicio IPv6 en sí, está ligada a la concesión de direcciones IPv4. Por lo tanto, el servicio 6rd también está ligado a ello en términos de autorización, contabilidad, etc. Por ejemplo, el prefijo 6rd delegado tiene el mismo tiempo de vida que su dirección IPv4 asociada, por lo que el tiempo de vida del prefijo anunciado en *Router Advertisements* o a través de un DHCP en la LAN del equipo de cliente debe ser igual o menor que el tiempo de concesión de la dirección IPv4 [33].

II.4.3 Traductores de Protocolos y Direcciones

Los principales traductores de protocolos y direcciones son descritos en los RFCs 6145, 2766, 6535 y 3124. Su función es proveer rutas transparentes que permitan a los nodos IPv6 en una red IPv6, comunicarse con nodos IPv4 de una red IPv4 por medio de la traducción de los paquetes IP [21]. Sin embargo, se proponen las técnicas de traducción como última alternativa a tomar durante la transición de una red. En efecto, se atribuyen como solución temporal hasta que otro mecanismo de transición pueda ser implementado debido a limitaciones en el soporte de algunas funciones que presta IPv6 [24].

Entre los principales traductores de protocolos podemos encontrar los siguientes:

1) ***Stateless IP/ICMP Translation algorithm (SIIT):***

Fue definido originalmente en el RFC 2765 y posteriormente declarado obsoleto éste en el RFC 6145 [35] [36]. Por sí mismo no es un traductor de protocolos. Es el algoritmo base por el cual varios traductores de protocolos llevan a cabo sus

traducciones y operaciones, como por ejemplo BIH *(Bump-in-the-Host)* y NAT-PT *(Network Address Translation-Protocol Translation)* [21]. Este algoritmo define de qué forma un traductor de protocolos debe traducir las cabeceras IP e ICMP de cada versión de éstas para que puedan ser entendidas por la otra versión [24].

Como las cabeceras son traducidas, y no encapsuladas, se introdujo inicialmente un nuevo formato o tipo de dirección denominada "dirección IPv4 traducible" cuyo formato de prefijo es "0::FFFF:0:0:0/96". El identificador del host es una dirección IPv4 tomada de un grupo especial de direcciones y es asignada al nodo IPv6 que desea comunicarse con un nodo IPv4 [24]. Sin embargo, en el RFC 6145, el formato del prefijo a utilizar fue relegado a la información existente en el RFC 6052: *IPv6 Addressing of IPv4/IPv6 Translators*, el cual pasa a determinarse por un algoritmo y no como un valor constante.

Las opciones IPv4 y las cabeceras de opciones IPv6 de enrutamiento, *"Hop-by-Hop"* y destino no son traducidas.

2) *Network Address Translation-Protocol Translation (NAT-PT):*

Fue definido originalmente en el RFC 2766 y posteriormente declarado obsoleto en el RFC 4966, recomendando que este traductor pase a "estado histórico" ya que no es considerado conveniente como mecanismo de transición debido a una serie de inconvenientes surgidos durante su aplicación [37].

Su funcionamiento básico consistía en la implementación de este protocolo de traducción en los nodos de frontera entra una red IPv6 y una red IPv4. Cada nodo disponía de un grupo de direcciones IPv4 globales únicas que se asignaban dinámicamente cuando se iniciaba una conexión a través del nodo de borde, por lo que se permitía por medio de este mecanismo que nodos y aplicaciones IPv6 se comunicasen con nodos y aplicaciones IPv4 en ambos sentidos [21].

3) *Bump-in-the-Host (BIH):*

Este mecanismo corresponde a una implementación de NAT-PT, con la diferencia de que el traductor se encuentra dentro del sistema operativo del cliente [24]. Está descrito en el RFC 6535 y declara obsoletos los mecanismos de transición *Bump-in-the-Stack* (RFC 2767) y *Bump-in-the-API* (RFC 3338). BIH permite que aplicaciones basadas en IPv4 se comuniquen con servidores IPv6 a través de direcciones IPv4 privadas creadas a partir de registros "AAAA", con el objetivo de dar un soporte extendido de estas aplicaciones sobre redes con IPv6 como protocolo dominante. [38]La dirección IPv4 utilizada puede ser privada debido a que, a diferencia de un nodo *Dual-Stack*, BIH utiliza esta dirección únicamente para comunicaciones internas con las aplicaciones IPv4 pero jamás para comunicarse con el exterior; por lo que, desde el punto de vista de un nodo exterior, un nodo con BIH implementado es idéntico a un nodo que maneja exclusivamente IPv6 [24].

Se incluyen dos alternativas principales para la implementación de BIH: un traductor de protocolo entre las pilas IPv4 e IPv6 de un cliente o un traductor de *Application Programming Interface (API,* o Interfaz de Programación de Aplicaciones) entre el módulo *socket API* IPv4 y el módulo TCP/IP. Por lo que, en principio, se traducirá de IPv4 a IPv6 en la capa de *socket API* o en la capa IP propiamente; sin embargo, se recomienda implementar la alternativa correspondiente al traductor de API [38].

En el caso de implementarse BIH en la capa del *socket API*, el traductor intercepta la función a la que el *socket API* IPv4 está haciendo una solicitud y genera el *socket API* IPv6 correspondiente, permitiendo la comunicación con clientes IPv6 [38].

Por otra parte, cuando se implementa BIH en la capa de red, los paquetes IPv4 son traducidos a IPv6 y viceversa haciendo uso del algoritmo SIIT [38].

La Figura 20 y la Figura 21 muestran, respectivamente, la arquitectura de un cliente en el cual está implementado un traductor a nivel del *socket API* o un traductor a nivel de capa de red.

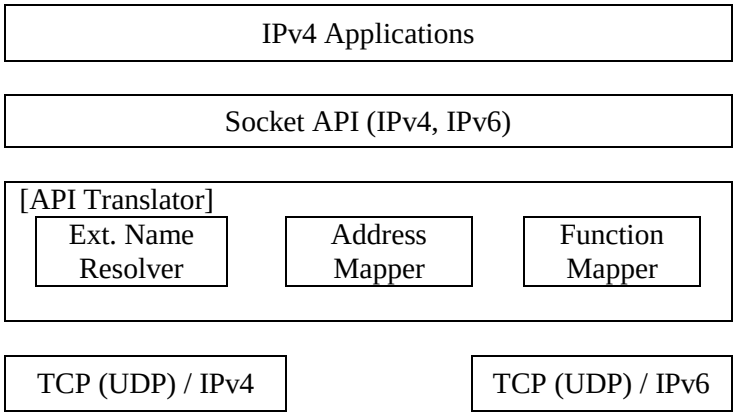

Figura 20: Arquitectura de un cliente *dual-stack* empleando BIH a nivel del *socket API*.

Fuente: [38].

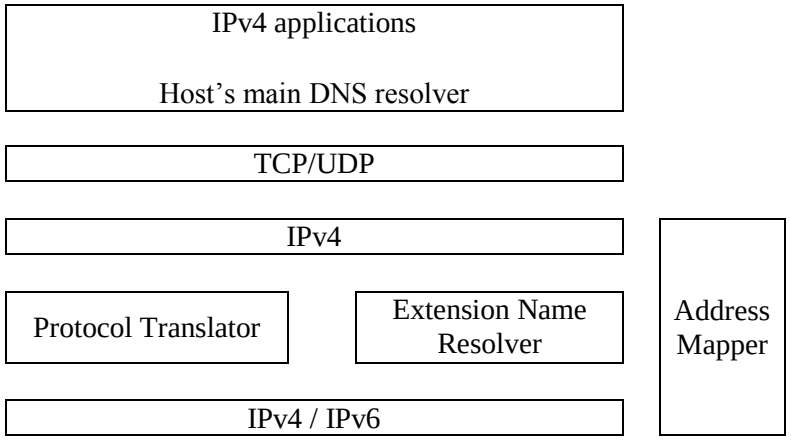

Figura 21: Arquitectura de un cliente *dual-stack* empleando BIH a nivel de capa de red.

Fuente: [38].

Como se aprecia, la arquitectura de BIH consta de un *Extension Name Resolver*, un *Address Mapper,* y dependiendo de qué implementación desee utilizarse, un *Function Mapper* o directamente de un traductor de protocolo basada en el algoritmo SIIT [38]. Sus funciones y aspectos generales se describen a continuación:

– ***Extension Name Resolver (ENR):*** devuelve una contestación en respuesta a la solicitud de resolución de nombres de la aplicación IPv4.

En el caso de implementarse BIH en la capa del *socket API*, cuando una aplicación IPv4 intenta hacer una búsqueda directa para resolver nombres a través de la biblioteca correspondiente, BIH intercepta la función a la que el *socket* está haciendo una solicitud y en su lugar llama a las funciones IPv6 equivalentes, las cuales resuelven tanto los registros tipo "A" como "AAAA"

En el caso de implementarse BIH en la capa de red, el ENR intercepta la consulta tipo "A" y genera una consulta tipo "AAAA" con un contenido similar. Posteriormente, ENR capturará las respuestas para ambas consultas y, en función de los resultados, devolverá una respuesta tipo "A" sin modificar o sintetizará una nueva respuesta tipo "A".

– ***Address Mapper:*** este módulo mantiene un lote de direcciones IPv4 que puede ser usada para la síntesis de direcciones IPv4. Igualmente, el módulo mantiene una tabla compuesta por pares de direcciones, indicando la correspondencia entre cada dirección IPv4 sintetizada y direcciones reales de destino IPv6. Cuando algún módulo del BIH hace una solicitud al *address mapper* para que asigne una dirección IPv4 a una dirección IPv6, éste selecciona y devuelve una dirección IPv4 del lote local disponible, registrando una nueva entrada en la tabla de control.

– ***Function Mapper:*** se encarga de traducir una función de un *socket API* IPv4 a una función de un *socket API* IPv6. Cuando se detecta un *socket API* IPv4 haciendo una solicitud a una aplicación IPv4, el *function mapper* intercepta la solicitud y genera el *socket API* IPv6 correspondiente.

4) ***Transport Relay Translator (TRT):***

Descrito en el RFC 3142 y con un uso orientado a la capa de transporte de redes basadas únicamente en IPv6. Se ubica en la red IPv6 y permite la comunicación entre

nodos IPv6 y nodos IPv4. Debido a que cada comunicación entre un cliente IPv6 y una aplicación IPv4 necesita pasar por el TRT, se pueden dar dos casos: la existencia de una conexión TCP o de una conexión UDP. En el caso de una conexión TCP, el TRT finaliza la conexión al cliente y genera una nueva conexión TCP en el otro extremo, hacia la aplicación IPv4, traduciendo internamente entre ambas conexiones. Por su parte, en una conexión UDP, se limita simplemente a traducir y reenviar el paquete [24] [39].

II.4.4 Asymmetric Digital Subscriber Line (ADSL).

ADSL es una tecnología proveniente de la línea DSL y es actualmente utilizada por CANTV para prestar su servicio de Acceso a Banda Ancha (ABA), esto es debido a que la empresa aprovecha la infraestructura sobre la cual opera el servicio telefónico (pares de cobre), para ofrecer acceso a Internet.

ADSL es una tecnología considerada asimétrica ya que está diseñada para poseer mayor capacidad de bajada (de la red al usuario) que de subida (del usuario a la red), esto es de gran utilidad debido a que los usuarios suelen recibir más información que la que envían.

Esta tecnología establece tres canales de comunicación:

- Servicio Telefónico.
- Envío de datos.
- Recepción de datos.

En donde el canal de recepción es más grande que el de envío, esto se debe a la característica principal de ADSL mencionada anteriormente. Sin embargo ADSL ofrece menos ancho de banda con respecto a otras tecnologías como por ejemplo Metro Ethernet y su capacidad de transmisión es menor que la obtenida con la fibra óptica.

ADSL es funcional siempre y cuando la longitud de la línea telefónica no sea mayor a 5,5 km medidos desde la central telefónica, como también es importante que no haya otros servicios por la línea que puedan interferir. Los módems ADSL trabajan en un margen de frecuencia que va desde los 25 KHz a los 1104 KHz, aproximadamente. Cumpliendo con la banda de frecuencia que se observa en la siguiente figura:

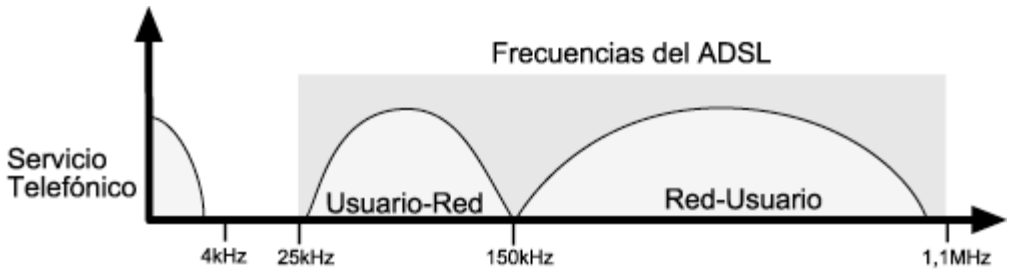

Figura 22: Banda de Frecuancia ADSL.

Fuente: [40]**.**

En la Figura 22 se puede determinar que la frecuencia de subida va desde 25 KHz hasta 150 KHz y la de bajada desde 150 KHz hasta 1,1 MHz.

Con esta tecnología se consigue aproximadamente una velocidad de bajada (de la central al cliente) de 1,5 Mbps en distancias de 6km de la central y 8 Mbps para distancias de 3km o menos de la central. De igual forma en estos tramos se logra conseguir una velocidad de subida (del cliente a la central) aproximada que va de 16 a 640 Kbps.

Generalmente la arquitectura en ADSL se conforma por los siguientes componentes:

- CPE/Módems ADSL.
- DSLAM.

En donde el modem se encarga de tomar los datos y entregarlos al cliente y el DSLAM separa las frecuencias entregando el servicio de datos a la red de datos o a Internet de manera directa y el servicio de voz a la red telefónica. Sin embargo cada ISP establece la arquitectura a implementar a partir del DSLAM. Por ejemplo CANTV posee una red Metro Ethernet a continuación del DSLAM, como observará en el desarrollo de este Trabajo Especial de Grado.

II.4.5 ADSL2+.

ADSL2+ se presenta en el mercado como la evolución de las tecnologías ADSL y ADSL2 y su principal diferencia es que puede soportar el doble de espectro, presentando una mejora significativa en el ancho de banda aumentando su capacidad de bajada a 24Mbps y subida a 2,2 Mbps. Sin embargo esta característica sólo se cumple si la distancia al teléfono es menor a 3 km, a partir de la misma empieza a afectar el ruido ya que utiliza la parte más alta del espectro. A diferencia de ADSL2, el cual sufre menos el efecto de la atenuación y cumple con sus características referentes al ancho de banda por 8 km.

ADSL2+ trabaja en el siguiente rango de frecuencia:

- Canal de Voz: 0 – 4 KHz.
- Subida de Datos: 25 – 500 KHz.
- Bajada de Datos: 550 KHz – 2,2 MHz.

Se puede observar de manera gráfica este rango de frecuencia en la siguiente figura:

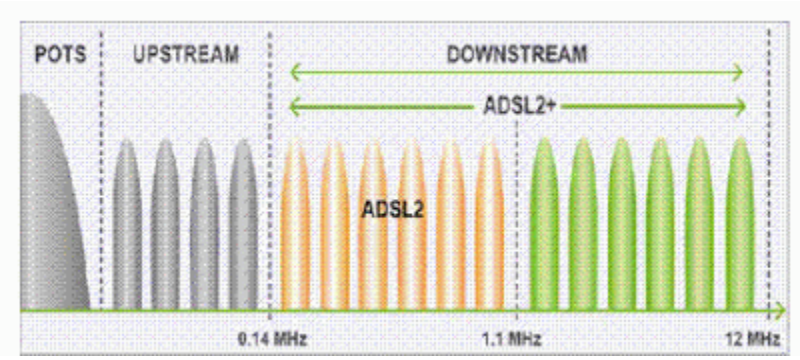

Figura 23: Banda de Frecuencia ADSL2+

Fuente: [41].

Esta tecnología presenta también mejoras en la supervisión de la conexión y la calidad de servicio (QoS), tomando en cuenta todas estas mejoras, ADSL2+ requiere cambios en la infraestructura de la red, sin embargo estos cambios no generan grandes gastos.

Observando estas características, CANTV tomó en cuenta esta tecnología y es aplicada actualmente en la Red de Acceso de Banda Ancha IP, Acceso xDSL y Arquitectura ABA.

II.4.6 Multiprotocol Label Switching (MPLS).

MPLS es una tecnología de reenvío de paquetes, la cual hace uso de "etiquetas" para tomar las decisiones relacionadas con el reenvío de los mismos. El término "*multiprocol"* se debe a que es aplicable a cualquier protocolo de capa de red. Dentro de esta tecnología se define un concepto llamado "*Forwarding Equivalence Class (FEC)"* o "Clase Equivalente de Reenvío", el cual consiste en un grupo de paquetes IP que se reenvían de la misma manera, sobre la misma ruta y con el mismo tratamiento de envío. En este sentido, una FEC puede ser definida o corresponder con diferentes factores, como por ejemplo una subred de destino o un determinado tipo de tráfico.

En un protocolo de capa de red no orientado a conexión, cada *router* decide de forma independiente el próximo salto para cada paquete que llega a éste, tomando la información obtenida de la cabecera del paquete y del resultado obtenido al ejecutar el algoritmo de enrutamiento instalado en el *router*, Sin embargo, en MPLS, la asignación de un paquete en específico a un FEC determinado se realiza una única vez, en el momento en el que el paquete accede al dominio MPLS. El FEC al cual es asignado el paquete se codifica con un valor de longitud fija denominado *"label"* o etiqueta, enviándose esta junto con el paquete cada vez que se hace el reenvío al próximo salto.

El análisis de la cabecera se realiza entonces una única vez, al momento de entrar al dominio MPLS, en el que se conoce como *Edge Label Switching Router (Edge – LSR).* Toda acción de reenvío es manejada por la etiqueta otorgada al paquete en el *Edge-LSR*, la cual es usada como un índice dentro de una tabla, indicando el próximo salto y una nueva etiqueta a asignar. La etiqueta anterior es reemplazada con la posterior y se realiza el correspondiente reenvío del paquete al próximo salto indicado en la primera etiqueta.

Este concepto de etiquetado para el reenvío y enrutamiento de los paquetes otorga una serie de ventajas con respecto a los métodos convencionales aplicados en la capa de red, como por ejemplo [42]:

– Se da la posibilidad de hacer uso de cierta información inalcanzable en los métodos de enrutamiento convencionales, ya que estos se limitan a la información existente en la cabecera de la capa de red del paquete. Así, por ejemplo, se puede utilizar la información relacionada con los puertos TCP o UDP que los paquetes estén utilizando, y asignar números de puertos distintos a FECs distintos.

– Es posible etiquetar de manera completamente distinta un paquete que accede a un dominio MPLS por un *router* y al mismo paquete pero accediendo por otro *router* totalmente distinto; de este modo, las decisiones de enrutamiento que

dependan del *router* de ingreso pueden llevarse a cabo con gran facilidad. Por otro lado, este concepto no es aplicable en los métodos convencionales de enrutamiento, debido a que la identidad del *router* de ingreso de un paquete no viaja con éste.

– Es posible, en caso de necesitarse, obligar a un paquete a seguir una ruta determinada, haciendo caso omiso de los algoritmos de enrutamiento convencionales, mediante el uso de una etiqueta que represente dicha ruta, ya sea debido a diferentes políticas que puedan existir o se quieran establecer en la red, o para permitir el soporte de ingeniería de tráfico en la misma.

La Figura 24 muestra la estructura de una etiqueta MPLS.

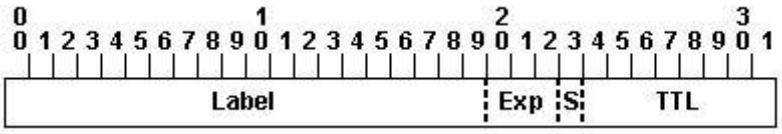

Figura 24: Formato de una etiqueta MPLS.

Fuente: [43].

– ***Label:*** valor de la etiqueta. Tiene 20 bits de longitud.

– ***Exp:*** uso experimental. Longitud de 3 bits. Actualmente es usado como un campo de *Class of Service (CoS).*

– ***S:*** indicador de final de la pila. Si su valor es igual a 1, indica que la etiqueta actual es la última de la pila.

– ***TTL:*** tiempo de vida. Longitud de 8 bits.

La etiqueta es impuesta o asignada entre la cabecera de la capa de enlace y la cabecera de la capa de red. La parte superior de la pila de etiquetas aparece primero en el paquete y la base aparece en la parte final del mismo. El paquete de la capa de red se encuentra inmediatamente después de la última etiqueta en la pila de etiquetas.

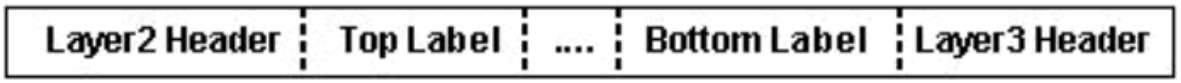

Figura 25: Ubicación de la etiqueta MPLS en un paquete.

Fuente: [43].

II.4.6.1 IPv6 Provider Edge Routers (6PE).

IPv6 Provider Edge Router (6PE) sobre *Multi-Protocol Label Switching* (MPLS) permite la interconexión y propagación de rutas IPv6 a través de un dominio MPLS habilitado para IPv4. Esto es posible gracias a la configuración de *Dual Stack* que presentan los 6PE, permitiendo así su conexión a dominios IPv6 y al núcleo MPLS, del cual solo se requiere su compatibilidad y operación en IPv4. Los *routers* 6PE intercambian la información de accesibilidad IPv6 transparentemente a través del *core* de la red utilizando el *Multiprotocol Border Gateway Protocol* (MP-BGP) sobre IPv4. De este modo, el campo "próximo salto" BGP se utiliza para transmitir la dirección IPv4 del *router* 6PE, de modo que una Etiqueta de Caminos Conmutados *(Label Switched Paths)* señalizada en la red MPLS-IPv4 se establece dinámicamente y puede ser usada sin la configuración explícita de un túnel. La Figura 26 describe una arquitectura con un 6PE en un dominio MPLS [44].

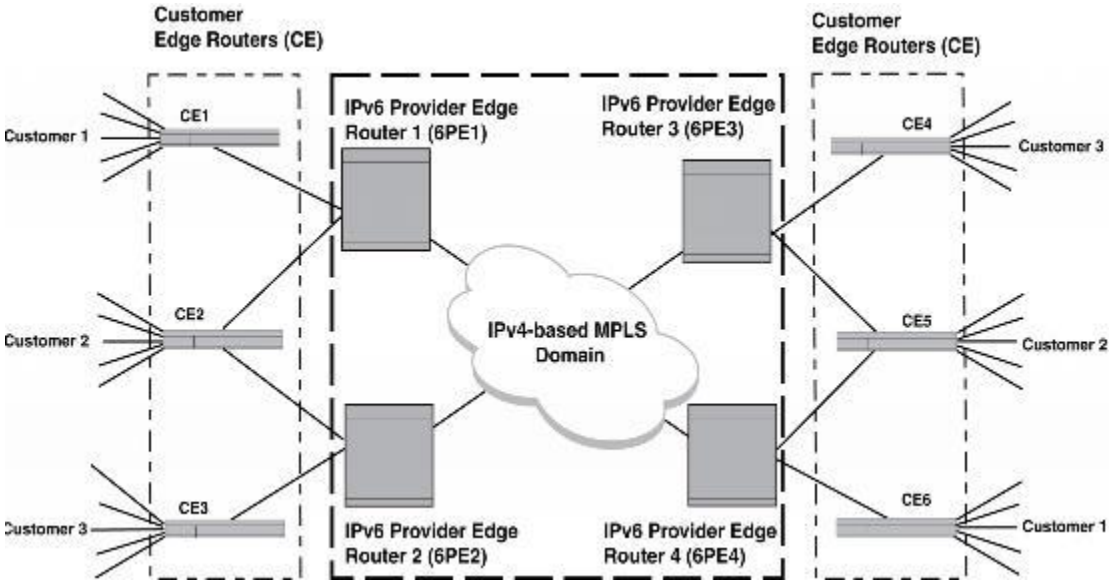

Figura 26: *Routers* 6PE en un dominio MPLS.

Fuente: [45]**.**

En la Figura 26, los *routers* desde CE1 hasta CE6 pueden ser indiferentemente IPv4 o IPv6. Por otra parte, los *routers* desde 6PE1 hasta 6PE2 emplean *Dual Stack.* El *router* CE provee conectividad con una red del cliente y un *router* 6PE. El *router* CE advierte la accesibilidad a información IPv6 de los clientes haciendo uso de rutas estáticas o protocolos de enrutamiento con compatibilidad IPv6. El *router* 6PE provee conectividad con el *router* CE y el dominio MPLS, siendo capaz de comunicarse con otros *routers* 6PE utilizando *Multiprotocol Border Gateway Protocol* (MP-BGP). Los paquetes salientes de la red del cliente son reenviados desde el *router* CE correspondiente hacia el *router* 6PE conectado a éste; mientras que los paquetes entrantes se reenvían desde el *router* 6PE al *router* CE conectado a la red del cliente [45].

Desafortunadamente, entre las limitaciones que presenta 6PE, destaca principalmente su compatibilidad únicamente con direcciones IPv6 de tipo *unicast* [45].

Enrutamiento de un paquete IPv6 a través de un dominio MPLS.

Los siguientes pasos describen el modo en que un paquete es encaminado a través de un dominio MPLS ya existente [45]:

1) El *router* 6PE recibe los paquetes IPv6 desde el *router* CE

2) El *router* 6PE asigna etiquetas a todos los paquetes IPv6 recibidos.

3) El *router* 6PE intercambia los paquetes IPv6 junto con sus respectivas etiquetas con los otros *routers* 6PE.

4) El *router* 6PE transporta los paquetes IPv6 desde el *router* CE utilizando los LSP IPv4 existentes.

II.4.6.2 IPv6 VPN Provider Edge Routers (6VPE).

Los 6VPE permiten la conexión de dos redes IPv6 privadas sobre una red pública MPLS basada en IPv4. Este puede ser un PE ya existente o un nuevo PE dedicado al tráfico IPv6. El *router* 6VPE utiliza el *backbone* MPLS existente para reenviar el tráfico IPv6 desde un PE a otro haciendo uso de etiquetas MPLS. La Figura 27 describe una topología de red para 6VPE [46].

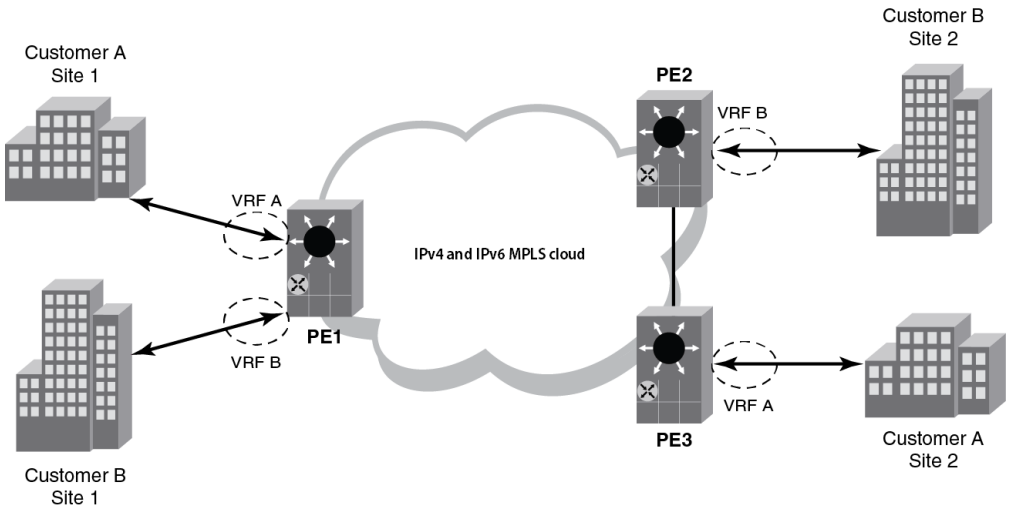

Figura 27: Topología de red para 6VPE.

Fuente: [46].

La red 6VPE consiste de los siguientes elementos claves en su topología:

1) Sitios del cliente A: anuncian rutas IPv6.

2) Sitios del cliente B: anuncian rutas IPv6.

3) PE1: el *Label Swtich Router* (LSR) de origen o ingreso.

4) PE2 y PE3: el LSR de destino o salida.

Esta topología muestra diferentes sitios de clientes conectados a través de una red MPLS IPv4 y operando con familias de direcciones IPv6. Los *routers* PE emplean *Dual Stack*. Los sitios 1 y 2 del cliente A están conectados a través de la red MPLS, mientras que se mantiene un VRF diferente para cada cliente en el PE. El sitio 1 del cliente A está conectado a PE1 con un VRF A y el sitio 1 del cliente B está conectado a PE1 con un VRF B [46].

Por otro lado, los siguientes pasos describen el funcionamiento de 6VPE en un dominio MPLS existente [46]:

1) Cada sitio del cliente anuncia sus rutas IPv6 a los *routers* PE conectados, siendo recibidas en sus VRFs específicos.

2) Los *routers* PE asignan etiquetas VRF a todos los paquetes IPv6 recibidos.

3) Los *routers* PE anuncian las rutas recibidas a los *routers* PE remotos con etiquetas VRF IPv6. La etiqueta VRF IPv6 es única para cada VRF dentro del PE.

4) Los paquetes IPv6 son reenviados en el dominio MPLS basados en las tablas de enrutamiento VRF correspondiente con las etiquetas VRF IPv6.

5) El *router* 6VPE reenvía los paquetes IPv6 desde el *router* del cliente utilizando los LSPs IPv4 existentes.

Sin embargo, al igual que 6PE, 6VPE es compatible únicamente con direcciones IPv6 de tipo *unicast* [46].

Capítulo III

Metodología y Desarrollo

III.1 Metodología

A continuación se dará a conocer el tipo de investigación al que pertenece el presente Trabajo Espacial de Grado, como también las fases y consideraciones que se plantearon para la correcta culminación del mismo.

III.1.1 Tipo de Investigación

El presente Trabajo Especial de Grado es considerado un Proyecto Factible e Investigación de Campo de Carácter Experimental [47]. Tomando en cuenta lo expresado por el Dr. Margín Rodriguez, este Trabajo Especial de Grado es de igual manera considerado de nivel analítico, de diseño experimental y de propósito aplicado (proyecto factible) [48].

Esta investigación se considera Proyecto Factible debido a que cumple con la definición del mismo, en las normas UPEL, las cuales indican que un proyecto factible es la investigación, elaboración y desarrollo de una propuesta de un modelo operativo viable para solucionar problemas, requerimientos o necesidades de organizaciones o grupos sociales; puede referirse a la formulación de políticas, programas, tecnologías, métodos o procesos. El Proyecto debe tener apoyo en una investigación de tipo documental, de campo o un diseño que incluya ambas modalidades [47].

De igual manera se considera una Investigación de Campo de carácter experimental ya que posee las características que se indican en las normas UPEL, las cuales señalan que se entiende por Investigación de Campo, el análisis sistemático de problemas en la realidad, con el propósito bien sea de describirlos, interpretarlos, entender su naturaleza y factores constituyentes, explicar sus causas y efectos, o

predecir su ocurrencia, haciendo uso de métodos característicos de cualquiera de los paradigmas o enfoques de investigación conocidos o en desarrollo [47].

Esta investigación se considera de nivel analítico ya que a lo largo de la misma se requiere analizar distintas situaciones para lograr una toma de decisiones, siendo el conjunto de estas lo que permitió la elaboración del proyecto. De igual manera se considera de diseño experimental debido a que se trabajó con diversos equipos con los que se realizó un gran número de pruebas.

Se utilizó como técnica de recolección de datos la entrevista, que consiste en la formulación de preguntas de parte del investigador a profesionales en el tema capacitados para brindar una respuesta adecuada. Como instrumento de recolección de datos se utilizó el guión de entrevista presentado en el Apéndice A, conformado por siete (7) preguntas semi-estructuradas y abiertas, para obtener la información necesaria en relación a los objetivos planteados en este trabajo especial de grado.

Los entrevistados se expresaron con libertad para exponer sus conocimientos en cuanto a los mecanismos de transición a IPv6 y prefijos más utilizados actualmente, como también en relación a la mejor manera de distribuir las direcciones IP. Sin embargo, es importante destacar que las respuestas obtenidas sólo se tomaron como referencia, debido a que los autores de este proyecto realizarían las recomendaciones necesarias para la transición a IPv6 de CANTV.

III.1.2 Procedimientos

Para la realización exitosa de este Trabajo Especial de Grado se plantearon cuatro fases:

FASE I. **Estudio y Levantamiento de Información**.

En esta etapa se lleva a cabo la búsqueda y recopilación de los modelos de equipos utilizados en la infraestructura del operador CANTV para su posterior revisión en cuanto a compatibilidad con el protocolo IPv6 en sus diferentes ámbitos. Asimismo

se hace una revisión desarrollo del marco teórico sobre IPv6 y los protocolos involucrados, haciendo énfasis en los mecanismos de transición al nuevo protocolo desde plataformas con IPv4.

FASE II. **Diseño**.

En esta fase del proyecto, se abarca el estudio de la distribución de la clientela actual de CANTV, los posibles rangos de direcciones IPv6 asignables a cada uno de estos, la investigación de los principales mecanismos de transición que pueden implementarse actualmente, así como los protocolos de enrutamiento a utilizar.

La clientela global de CANTV fue suministrada directamente por los empleados de la misma; sin embargo, por razones de confidencialidad de esta información, no es posible adjuntar el archivo que expone estos detalles en el presente Trabajo Especial de Grado.

FASE III. **Evaluación**.

En esta fase se diseñan escenarios de pruebas con los parámetros de desempeño correspondientes, según lo indicado por CANTV, ya que ellos comunican las pruebas que son primordiales para realizar su transición a IPv6 con la menor cantidad de fallas posibles en la red.

Al culminar con el diseño se procede con el montaje de la maqueta de red y se realizan las mediciones y valoraciones de desempeño correspondientes.

FASE IV. **Cierre y Recomendaciones**.

En esta fase se desarrollará el documento final con los procedimientos y recomendaciones para la implementación de los mecanismos evaluados en la red de CANTV.

III.2 Desarrollo

En este capítulo se expresa el proceso de transición a IPv6 de CANTV, describiendo con detalle cada etapa mencionada anteriormente en la metodología.

III.2.1 Estudio y Levantamiento de Información

Se realizó la recopilación de los modelos de equipos utilizados en la infraestructura (ABA) del operador CANTV para su posterior revisión en cuanto a compatibilidad con el protocolo IPv6 en sus diferentes ámbitos.

Esta investigación se realizó en base al material provisto por los empleados de CANTV, el cual permitió la realización del inventario (una muestra) de sus equipos. Por otra parte, la compatibilidad de los mismos fue revisada directamente con los fabricantes de cada equipo, a través de la información disponible en su página web o vía correo electrónico.

A continuación se presenta una tabla con los equipos recopilados de la infraestructura de CANTV:

Marca	Modelo	Arquitectura	Caracteristicas
Alcatel	7450 ESS-1 (Metro Ethernet)	Banda Ancha IP (Redes Metro Ethernet)	*Switches*
	7450 ESS-7 (Metro Ethernet)		
	7450 ESS-12 (Metro Ethernet)		
	7302	Banda Ancha IP (Red de Acceso)	*DSLAM*
Cisco	5300	Arquitectura UNIRED	*Gateways*
	5400		
	5850		
	7500		*Router*
	12000	Banda Ancha IP (Red de Acceso)	
	7600		
	7200	Banda Ancha IP	
	7609		
Juniper	E320	Banda Ancha IP	*Agregador*
	SA700		
Huawei	UA5000	Banda Ancha IP (Red de Acceso)	*DSLAM*
	MA5600		
	ME60-X8	Banda Ancha IP	*Agregador*
	HG832e	Arquitectura ABA	*Modem*
ZTE	FSAP9800	Banda Ancha IP (Red de Acceso)	*DSLAM*
	ZXHNH108L	Arquitectura ABA	*Modem*
ZYXEL	P-660RU-T1	Arquitectura ABA	*Modem*
RYGE	WA41R	Arquitectura ABA	*Modem*
SENDTEL	MS8-8817	Arquitectura ABA	*Modem*

Tabla 9: Inventario de Equipos de la Infraestructura de CANTV.

Fuente: Los Autores.

III.2.2 Diseño

Se abarcó el estudio de la distribución de la clientela actual de CANTV, cuya información fue suministrada directamente por los empleados de la empresa; sin embargo, por razones de confidencialidad de esta información, se colocará un aproximado de los mismos.

No obstante, durante el estudio de los posibles rangos de direcciones asignables a los clientes finales, en base al prefijo IPv6 otorgado por la LACNIC a CANTV el cual es un /24, se utiliza un número aproximado del total de clientes de ABA (Acceso a Banda Ancha) que posee CANTV.

El bloque de direcciones típico asignado por la LACNIC a un proveedor o ISP es un /32 [49], siendo en consecuencia el prefijo asignado a CANTV (/24) de gran tamaño con respecto al típico asignable. Tomando en cuenta el amplio tamaño del prefijo, se llevó a cabo un análisis preliminar con respecto al direccionamiento a realizarse a los usuarios finales residenciales y empresariales del operador.

Diversas referencias apuntaban inicialmente a asignar un prefijo /48 a todo usuario final, tanto empresarial como residencial, sin importar tamaño o envergadura. Sin embargo, posteriormente diversos análisis descartaron esta idea, ya que los requisitos de los usuarios finales vienen dados en distintos tamaños, por lo que asignar un prefijo tan amplio a un usuario residencial, conllevaba inevitablemente a un desperdicio elevado de direcciones, el cual debe evitarse por más que el espacio de direcciones disponible en IPv6 sea muy amplio [22].

De acuerdo a las políticas de la LACNIC, las asignaciones por parte de los ISPs deben ser realizadas de acuerdo con la necesidad presentada por el usuario del ISP y de acuerdo a las recomendaciones existentes en el RFC 6177: *IPv6 Address Assignment to End Sites* [50].

Al usuario o sitio final debe ser asignado la cantidad suficiente para atender su necesidad actual y planeada.

No menos que un /64 debe ser asignado a un usuario o sitio final, siendo una decisión operacional del ISP el tamaño exacto del bloque a asignar.

El RFC 6177 recomienda que se les asigne a los usuarios o sitios finales más que un /64 pero que no se adopte el plan de asignar un /48 por defecto a todos los usuarios finales, siendo una recomendación asignar un prefijo entre /48 y /64.

Adicionalmente, considerando los prefijos típicos para las redes y subredes en IPv6, se puede calcular de forma preliminar cuántas subredes se pueden generar a partir de cada uno de los prefijos típicos asignables por la IANA/LACNIC, como se indica a continuación:

Redes / **Subredes**	**/24**	**/32**	**/48**	**/56**
/32	256	1	N.A.	N.A.
/48	16.777.216	65.536	1	N.A.
/56	4.294.967.296	16.777.216	256	1
/64	1,1 billones apróx.	4.294.967.296	65.536	256

Tabla 10: Cantidad de Subredes en IPv6.

Fuente: Los Autores.

Se realizó una investigación de los mecanismos de transición a IPv6 existentes actualmente con el objetivo de seleccionar el más adecuado para su implementación en la infraestructura de CANTV. La información de estos mecanismos ayudó a complementar el Marco Referencial que se encuentra en el Capítulo II de este Trabajo Especial de Grado. Esta información se adquirió mediante la investigación en foros, libros, RFCs y páginas web.

Se procedió a la escogencia del mecanismo más apto para su implementación en la infraestructura de CANTV, tomando en cuenta diferentes parámetros que influirían en el correcto funcionamiento de la misma. Sin embargo, se decidió realizar una entrevista a siete profesionales o expertos en el tema tratado, para tomar en cuenta y comparar sus respuestas con las decisiones tomadas por los autores. Esta modalidad de entrevista ha sido utilizada de manera interesante en otros trabajos, como el de Fernández-Trujillo y Rojas [51], con la finalidad de determinar el mejor mecanismo de transición a IPv6 en la infraestructura de un operador de telecomunicaciones.

Considerando sus altos conocimientos en telecomunicaciones y años de experiencia en esta área se entrevistó a los siguientes profesionales:

- Ing. Miguel Zambrano (CANTV)
- Ing. Héctor González (CANTV)
- Ing. Luis Molner (Profesor UCAB)
- Ing. Carlos Fuenmayor (ZTE – Profesor UCAB)
- Ing. Francisco Flores (HUAWEI)
- Ing. Iván Carmona (Profesor UCAB)
- Ing. Alejandro Acosta (LACNIC)

Según los resultados obtenidos (Apéndice A), el mecanismo que obtuvo mayor reconocimiento por su implementación a nivel mundial fue el *Tunneling*, específicamente 6rd seguido de 6to4; sin embargo, es importante resaltar que la mayoría de los profesionales entrevistados que conocían de la implementación de 6to4 u otro mecanismo no tenían conocimiento de la existencia de 6rd o, en algunos casos, no poseían mucha información de este mecanismo, lo que no les permitía alegar que 6rd ha sido utilizado a nivel nacional e internacional, ó recomendar su implementación.

En el caso del Ing. Alejandro Acosta se recibió la recomendación según su experiencia de utilizar 6rd antes de 6to4, ya que es más eficiente en diversos aspectos, como por ejemplo, la utilización del prefijo otorgado por la LACNIC.

Con base en la información plasmada en el Marco Referencial, los resultados de la entrevista realizada y la investigación que se realizó para conocer qué mecanismos de transición a IPv6 son más utilizados actualmente por diversas empresas, se determinó que *Dual Stack* es el mecanismo que más ha sido implementado por los ISPs.

A continuación se mencionarán algunas empresas que actualmente utilizan este mecanismo:

Empresa	**País**
ALFANUMERIC S.A.	Nicaragua
BT Latinoamérica	Argentina
CENIT	Venezuela
ETB S.A. ESP	Colombia
GTD	Chile
NET	Brasil
Operbes, S.A. de C.V.	México

Tabla 11: Empresas que aplicaron el mecanismo *Dual Stack.*

Fuente: [52].

Dual Stack según esta investigación, es implementado en conjunto con otros mecanismos de transición, por ejemplo los túneles, siendo 6to4 y 6rd los más utilizados. Esta combinación permite mantener en funcionamiento una red conjunta IPv4/IPv6, lo cual es de gran utilidad actualmente, debido a que los ISPs no disponen del presupuesto y disponibilidad de equipos para sustituirle los CPE a cada cliente, y en el caso de sí disponer de estas cualidades, no se garantiza y no es recomendado una migración total a IPv6, ya que no todas las empresas a las que se le presta un servicio han iniciado sus estudios de infraestructura para su transición a IPv6, por lo tanto se recomienda mantener este tipo de red conjunta IPv4/ IPv6 por unos años.

Se ha observado la utilización de 6PE y 6VPE, por empresas que poseen una red MPLS, ya que permiten que los *routers* borde operen con el mecanismo *Dual Stack*, soportando IPv4 e IPv6 simultáneamente. Se puede tomar como ejemplo la empresa BT Latinoamérica que utilizó 6PE en su red MPLS al igual que la empresa Global Crossing que opera en América Latina y el Caribe [52]. Sin embargo la utilización de

estos mecanismos en el núcleo de la red MPLS de CANTV no aplica, debido a que la misma es una red capa 2.

Se seleccionaron los siguientes mecanismos para su implementación en red del laboratorio de CANTV:

- *Dual Stack*
- *Dual Stack* en conjunto con un Túnel 6to4
- *Dual Stack* en conjunto con un Túnel 6rd

Estos mecanismos de transición serán probados y comparados para luego determinar el más adecuado para su implementación en la red de CANTV.

Observando las especificaciones de cada protocolo de enrutamiento aplicable en IPv6, se planteó realizar pruebas con los protocolos de enrutamiento interior OSPFv3, y RIPng. En el enrutamiento exterior se planteó realizar pruebas con el protocolo BGP4+.

III.2.3 Evaluación

Para determinar el mecanismo a utilizar en la infraestructura de CANTV se planteó realizar un cuadro comparativo en donde se evalúen diversas características de los mecanismos de transición seleccionados con anterioridad. Este modelo de comparación fue utilizado por David García [53] , con la finalidad de determinar el mecanismo más eficaz para su implementación en la red de la Universidad Católica Andrés Bello.

Este cuadro reflejará diversas características como lo son:

- **Velocidad de Transmisión:** rapidez en el envío de paquetes.
- **Complejidad de Configuración:** el tiempo que requiere realizar la configuración de los equipos para que soporten los mecanismos de transición requeridos.

- **%CPU:** aumento de la carga del procesador.
- **Autonomía:** la independencia que posee el cliente con respecto al ISP para realizar su trabajo en IPv4/IPv6 sin problema alguno.
- **Costo:** el gasto que requiere aplicar los mecanismos de transición en la infraestructura (tarjetas o equipos nuevos).

Sin embargo estas características deben poseer evidentemente una escala de evaluación, la cual consta de los siguientes parámetros:

Escala de Evaluación					
Escala	**Velocidad de Transmisión**	**Complejidad de Configuración**	**% CPU**	**Autonomía**	**Costo**
1	Muy Veloz	Muy Alta	Muy Alta	Muy Alta	Muy Alto
2	Veloz	Alta	Alta	Alta	Alto
3	Regular	Regular	Regular	Regular	Regular
4	Lenta	Baja	Baja	Baja	Bajo
5	Muy Lenta	Muy Baja	Muy Baja	Muy Baja	Muy Bajo

Tabla 12: Escala de Evaluación.

Fuente: Los Autores.

Considerando los mecanismos utilizados por las diferentes empresas a nivel nacional e internacional y tomando en consideración los criterios empleados en este trabajo con respecto a la eficiencia de los diversos mecanismos de transición, se seleccionaron tres (3) de ellos para analizar su funcionalidad en la red del operador, midiendo sus características mediante la escala antes mencionada y determinando el más eficiente.

A continuación observará el cuadro comparativo elaborado:

Mecanismos de Transición	Velocidad de Transmisión	Complejidad de Configuración	% CPU	Autonomía	Costo
Dual Stack	Muy Veloz	Muy Baja	Baja	Muy Alta	Muy Bajo
Dual Stack + 6to4	Veloz	Baja	Regular	Muy Alta	Bajo
Dual Stack + 6rd	----------	Baja	----------	Muy Alta	Bajo

Tabla 13: Cuadro Comparativo de Mecanismos de Transición.

Fuente: Los Autores.

Cada uno de estos mecanismos a excepción del 6rd fue probado en los diversos escenarios establecidos en la maqueta de red del laboratorio de CANTV, para determinar su funcionalidad en la infraestructura de la empresa.

A continuación se presenta la red que actualmente está operativa en el laboratorio de la compañía:

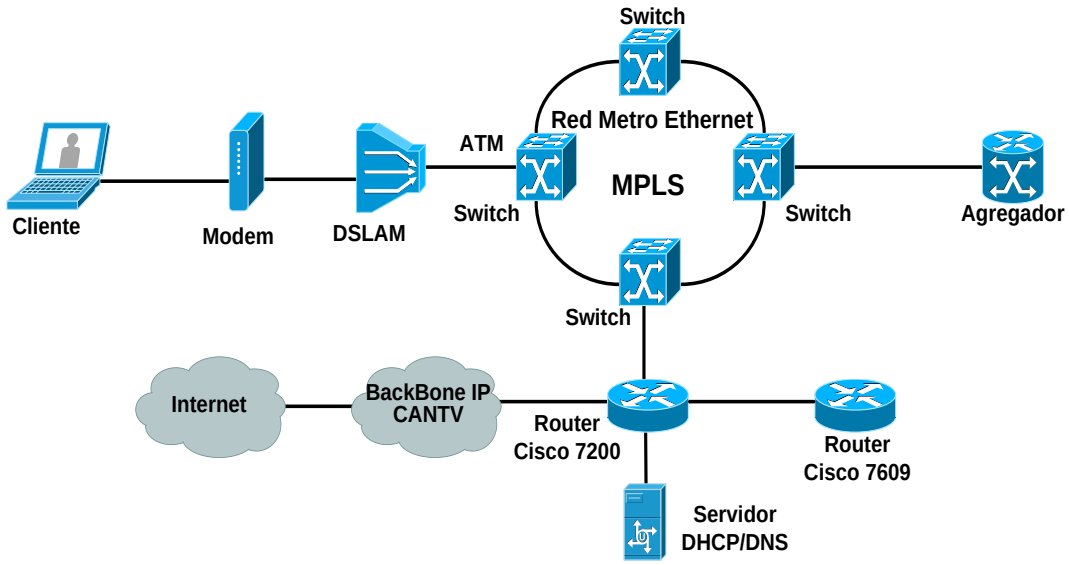

Figura 28: Red del Laboratorio de CANTV.

Fuente: Los Autores.

Un equipo final (cliente) accede a través de un CPE (Modem), que puede estar en modo *bridge* o *router*, el cual se conecta a un *DSLAM* marca Huawei modelo MA5600. Este *DSLAM* genera un túnel independiente para cada usuario que se conecta al mismo, enviando toda la información que éste transmita a través de una red

Metro-Ethernet MPLS capa 2 conformada por cuatro *switches* Alcatel 7450 ESS-7. A través de esta red, todo cliente se comunica con un agregador o BRAS (*Broadband Remote Access Server*) marca Huawei modelo ME60-x8, configurado como DHCP *relay*. Al momento de efectuar una solicitud DHCP, el agregador realiza todos los procesos de autenticación necesarios para, posteriormente, realizar una solicitud DHCP al servidor designado para tal fin y enviando su respuesta al cliente que realizó la solicitud en un inicio.

Una vez obtenida la dirección IP por parte del cliente, éste puede acceder a Internet IPv4 o IPv6, atravesando el *DSLAM*, la red Metro-Ethernet MPLS y *router* de borde para posteriormente acceder al *Backbone* de CANTV y finalmente a Internet. Detalles de cada uno de estos equipos se pueden observar en el Apéndice B.

Durante el análisis de cómo elaborar las pruebas pertinentes y crear los escenarios necesarios, se encontró con que este segmento de la red opera en Capa 2:

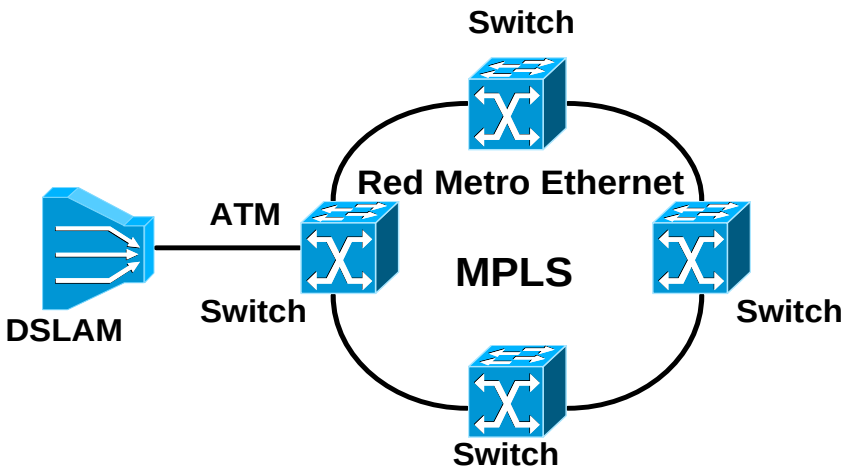

Figura 29: Segmento Capa 2 de la Red del laboratorio de CANTV.

Fuente: Los Autores.

Por lo tanto, todo paquete IP que pase por este segmento es transparente, esto se debe a que es en Capa 3 donde se toma en cuenta el tipo de paquete IP que está transitando. A pesar de tener claro este conocimiento se verificó la información con representantes de Alcatel-Lucent, quienes son los proveedores de los *switches* 7450

ESS-7 que se encuentran operando en la red Metro Ethernet, como también se conversó con representantes de Huawei por el DSLAM, MA5600 que es el equipo con el que se realizaron las pruebas. Ambos proveedores de servicios explicaron que el DSLAM, equipo que mantiene contacto directo con el CPE, trabaja netamente en Capa 2 por que se podría decir que opera como un *switch*.

Con base en esta infraestructura se elaboraron tres (3) escenarios de trabajo, para realizar las pruebas.

III.2.3.1 Escenario 1: Acceso *Dual Stack*, Core IPv6 e Internet IPv4.

A continuación toda la red operará en IPv6, a excepción del cliente que puede solicitar direcciones IPv4, IPv6 ó ambas simultáneamente y del *BackBone* IP, que actualmente trabaja en IPv4.

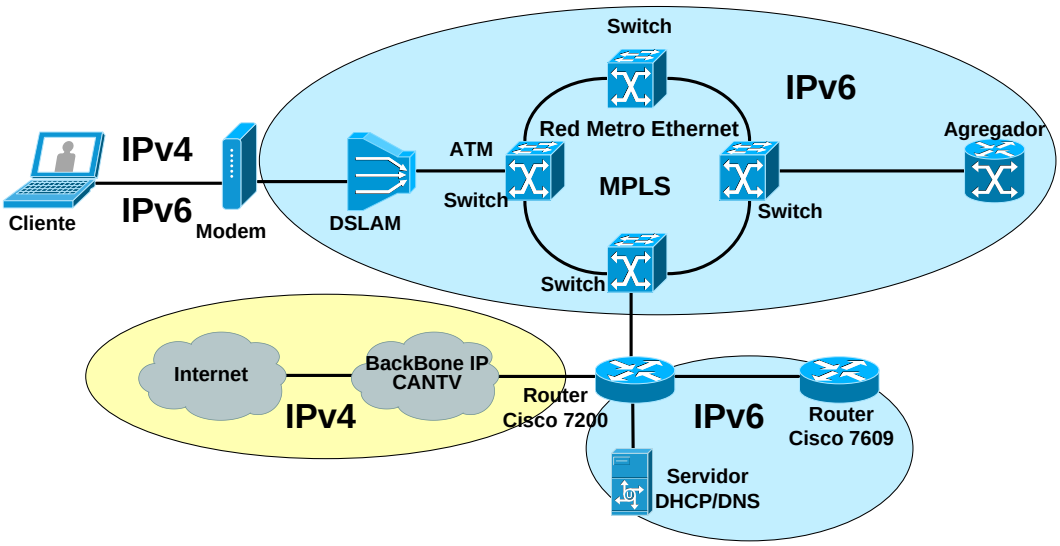

Figura 30: Escenario de prueba uno.

Fuente: Los Autores.

En este escenario se encontró que sólo era necesario aplicar el mecanismo de *Dual Stack* en el *Router* Cisco7200 y en el Modem a utilizar, esto se debe a que era

totalmente innecesario la utilización conjunta de *Dual Stack* con un túnel, ya que el único segmento en IPv4 era el *BackBone* IP y la salida a Internet; para poder completar un túnel se necesita otro enrutador que tenga configurado IPv6 al final del *BackBone*.

Observando la red en la cual se están realizando las pruebas, se vio la obligación de configurar rutas estáticas IPv6 entre el servidor DHCP y el *router* Cisco 7200, como también entre éste y el agregador. Sin embargo, se configuraron como se muestra en la Figura 31 los siguientes protocolos de enrutamiento entre los *routers* Cisco 7200, 7609 y el agregador o BRAS ME60-x8:

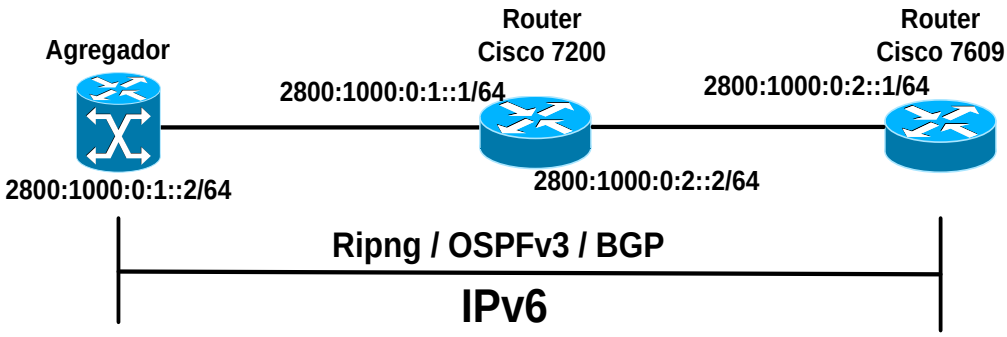

Figura 31: Aplicación de protocolos de enrutamiento.

Fuente: Los Autores.

A continuación se puede observar la configuración de los equipos y las tablas de enrutamiento en donde se refleja el funcionamiento de la red con el protocolo de enrutamiento RIPng. En la Figura 32 se puede observar la configuración en la subinterfaz del *router* Cisco 7609.

```
R7609-NGN-I10.1.1.7# sh run inter ten 1/0/0.7
Building configuration...

Current configuration : 171 bytes
!
interface TenGigabitEthernet1/0/0.7
 encapsulation dot1Q 7
 ip address 10.100.0.2 255.255.255.252
 ipv6 address 2800:1000:0:2::1/64
 ipv6 enable
 ipv6 rip 1 enable
end
```

Figura 32: SubInterfaz de *router* Cisco 7609 (Ripng).
Fuente: Los Autores.

Se presenta en la Figura 33 la tabla de enrutamiento del *router* Cisco 7609 en donde se refleja el funcionamiento del RIPng, comprobando conectividad realizando un *ping* entre el *router* Cisco 7609 y el agregador.

```
R7609-NGN-I10.1.1.7#sh ipv6 route
IPv6 Routing Table - default - 4 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
R   2800:1000:0:1::/64 [120/2]
     via FE80::20A:8BFF:FE45:3019, TenGigabitEthernet1/0/0.7
C   2800:1000:0:2::/64 [0/0]
     via TenGigabitEthernet1/0/0.7, directly connected
L   2800:1000:0:2::1/128 [0/0]
     via TenGigabitEthernet1/0/0.7, receive
L   FF00::/8 [0/0]
     via Null0, receive
R7609-NGN-I10.1.1.7#
```

Figura 33: Tabla de enrutamiento *router* Cisco 7609 (RIPng).

Fuente: Los Autores.

Se realizaron pruebas con OSPFv3 debido a que es el protocolo utilizado actualmente en la red IPv4 de CANTV. A continuación podrá observar en las Figuras 34 y 35 la tabla de enrutamiento del *router* Cisco 7609 y del agregador ME60-x8 respectivamente:

```
R7609-NGN-I10.1.1.7#sh ipv6 route
IPv6 Routing Table - default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OE2 2800:1000::/64 [110/20]
     via FE80::20A:8BFF:FE45:3019, TenGigabitEthernet1/0/0.7
O   2800:1000:0:1::/64 [110/2]
     via FE80::20A:8BFF:FE45:3019, TenGigabitEthernet1/0/0.7
C   2800:1000:0:2::/64 [0/0]
     via TenGigabitEthernet1/0/0.7, directly connected
L   2800:1000:0:2::1/128 [0/0]
     via TenGigabitEthernet1/0/0.7, receive
OE2 3FF3:200::1/128 [110/20]
     via FE80::20A:8BFF:FE45:3019, TenGigabitEthernet1/0/0.7
L   FF00::/8 [0/0]
     via Null0, receive
R7609-NGN-I10.1.1.7#
```

Figura 34: Tabla de enrutamiento del *router* Cisco 7609.

Fuente: Los Autores.

```
Destination  : 2800:1000:0:1::              PrefixLength : 64
NextHop      : 2800:1000:0:1::2            Preference   : 0
Cost         : 0                           Protocol     : Direct
RelayNextHop : ::                          TunnelID     : 0x0
Interface    : GigabitEthernet1/0/0.600    Flags        : D

Destination  : 2800:1000:0:1::2            PrefixLength : 128
NextHop      : ::1                         Preference   : 0
Cost         : 0                           Protocol     : Direct
RelayNextHop : ::                          TunnelID     : 0x0
Interface    : GigabitEthernet1/0/0.600    Flags        : D

Destination  : 2800:1000:0:2::             PrefixLength : 64
NextHop      : FE80::20A:8BFF:FE45:3019    Preference   : 10
Cost         : 2                           Protocol     : OSPFv3
RelayNextHop : ::                          TunnelID     : 0x0
Interface    : GigabitEthernet1/0/0.600    Flags        : D
```

Figura 35: Tabla de enrutamiento del BRAS ME60-x8.

Fuente: Los Autores.

Se comprobó conectividad al realizar *ping* entre el *router* Cisco 7609 y el agregador, confirmando el funcionamiento del protocolo de enrutamiento.

A continuación se puede observar el comportamiento del protocolo de enrutamiento exterior BGP4+ en la red del laboratorio de CANTV.

Se presenta en la Figura 36 la configuración de BGP en el *router* Cisco 7609, la cual se realizó ejecutando los mismos comandos en el *router* Cisco 7200, la diferencia se presenta en el número del Sistema Autónomo (AS) el cual es el cien (100).

```
!
router bgp 2
 bgp router-id 10.100.0.2
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 2800:1000:0:2::2 remote-as 100
 !
 address-family ipv4
  no synchronization
  no auto-summary
 exit-address-family
 !
 address-family ipv6
  no synchronization
  network 2800:1000:0:1::/64
  neighbor 2800:1000:0:2::2 activate
 exit-address-family
!
```

Figura 36: Configuración BGP4+ en *router* Cisco 7609.

Fuente: Los Autores.

En la Figura 37 se puede observar la tabla de enrutamiento del *router* Cisco 7609, en donde se aprecia el enrutamiento BGP hacia la red 2800:1000:0:1::/64.

```
R7609-NGN-I10.1.1.7#show ipv6 route
IPv6 Routing Table - default - 4 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
B   2800:1000:0:1::/64 [20/0]
     via FE80::20A:8BFF:FE45:3019, TenGigabitEthernet1/0/0.7
C   2800:1000:0:2::/64 [0/0]
     via TenGigabitEthernet1/0/0.7, directly connected
L   2800:1000:0:2::1/128 [0/0]
     via TenGigabitEthernet1/0/0.7, receive
L   FF00::/8 [0/0]
     via Null0, receive
R7609-NGN-I10.1.1.7#
```

Figura 37: Tabla de enrutamiento *router* Cisco 7609.

Fuente: Los Autores.

Al establecer la comunicación con otros Sistemas Autónomos (AS), por medio de este protocolo de enrutamiento exterior, se procede a publicar los prefijos globales de la empresa. En el caso CANTV se establece comunicación con los siguientes NSP (*Network Service Provider*):

- Columbus Networks
- MCI
- LANautilus
- Global Crossing.
- Telefonica
- Sprint
- TISCALI
- France Telecom

Publicándose en la tabla de enrutamiento el prefijo del *router* de borde por el que se salga.

III.2.3.2 Escenario 2: Módem y agregador (BRAS) en IPv6.

A continuación se puede observar cómo se plantea este escenario en donde el módem y al BRAS trabajaran en IPv6, este último ejerciendo funciones de DHCP.

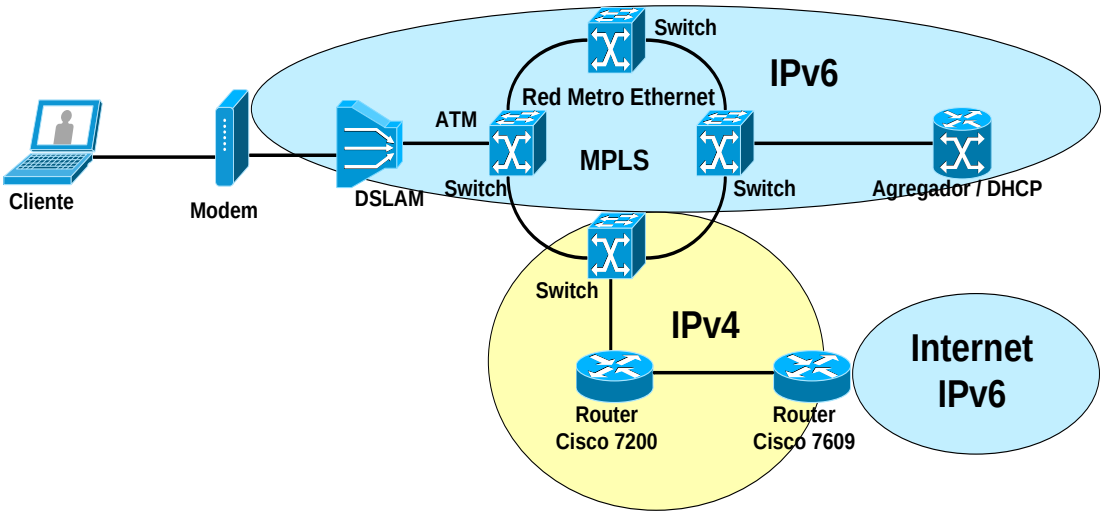

Figura 38: Escenario de prueba dos.

Fuente: Los Autores.

Este escenario presentado en la Figura 38 permite representar el *BackBone* IP de CANTV, con la utilización de los *routers* Cisco 7200 y Cisco 7609, simulando que

para su salida a Internet se trabaja en IPv6, lo cual me permite establecer una solución en caso de no poder implementar la transición a la nueva versión de Protocolo de Internet, en el *BackBone* IP por alguna circunstancia (económica, disponibilidad de personal, tiempo de implementación, entre otras) generando el ambiente necesario para probar los siguientes mecanismos:

- **Dual Stack + 6to4:** para lograr establecer estos dos mecanismos es necesario configurarlos en los equipos que lo requieran, según la red en la cual se va a trabajar.

Para poder entender lo planteado con este escenario, se presenta a continuación en la Figura 39, el funcionamiento de la red en este escenario.

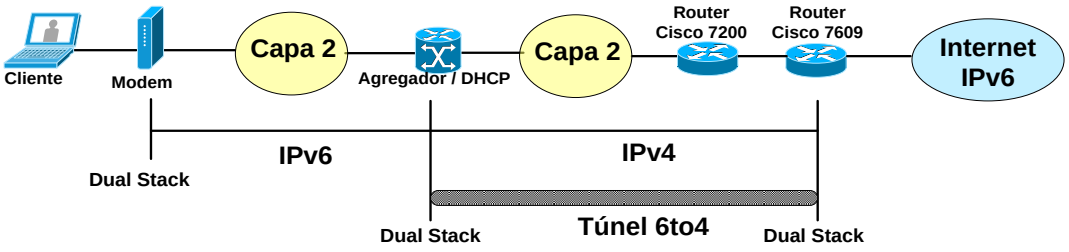

Figura 39: Funcionamiento de la red en escenario dos.

Fuente: Los Autores.

A continuación en las Figuras 40 y 41 se puede observar la activación del mecanismo *Dual Stack*, en el BRAS y *router* Cisco 7609 respectivamente. Este mecanismo de transición es necesario para que los nodos finales operen en IPv4/IPv6, lo que permite posteriormente el correcto funcionamiento de un túnel en caso de ser implementado.

Figura 40: Activación de *Dual Stack* en BRAS ME60-x8.

Fuente: Los Autores.

```
!
ipv6 unicast-routing
!
```

Figura 41: Activación de *Dual Stack* en *router* Cisco 7609.

Fuente: Los Autores.

En las Figuras 42 y 43 se puede observar cómo se configuró el túnel 6to4 en el *router* Cisco 7609 y en el BRAS ME60-x8 respectivamente. En la interfaz Tunnel 0 del *router* se puede apreciar cómo se configuró la dirección IPv6 a utilizar, la interfaz de origen y el tipo de túnel implementado respectivamente de manera descendiente. En el BRAS se aprecia la configuración de los mismos parámetros pero a diferencia del *router* Cisco 7609 primero se establece el tipo de túnel a utilizar y luego la interfaz de origen.

```
interface Tunnel0
 no ip address
 no ip redirects
 ipv6 address 2002:A64:2::1/64
 tunnel source TenGigabitEthernet1/0/0.7
 tunnel mode ipv6ip 6to4
end
```

Figura 42: Configuración del Túnel 6to4 en *router* Cisco 7609.

Fuente: Los Autores.

```
interface Tunnel1/0/0
 ipv6 enable
 ipv6 address 2002:AC10:4AE2::1/64
 tunnel-protocol ipv6-ipv4 6to4
 source 172.16.74.226
```

Figura 43: Configuración del Túnel 6to4 en el BRAS ME60-x8.

Fuente: Los Autores.

De igual manera se puede observar en las Figuras 44 y 45 cómo se configuró la dirección a la cual se dirige el túnel, configuración necesaria para establecer un correcto funcionamiento del mismo.

```
!
ipv6 route 2002:AC10:4AE2::/64 Tunnel0
!
```

Figura 44: Dirección de destino del Túnel 6to4 en el *router* Cisco 7200.

Fuente: Los Autores.

```
ipv6 route-static 2002:A64:2:: 64 Tunnel1/0/0
```

Figura 45: Dirección de destino del Túnel 6to4 del BRAS ME60-x8.

Fuente: Los Autores.

Se puede notar que se realiza el *ping* a una dirección IPv6, esta dirección posee según la teoría del túnel 6to4 la dirección IPv4 que ya está configurada en la interfaz el equipo. Por ejemplo:

IPv6: 2002:A64:02::1/64 IPv6: 2002:ac10:4ae2::1/64

A64:02 = 172.16.74.226 ac10:4ae2 = 10.100.0.2

IPv4: 172.16.74.226 **IPv4: 10.100.0.2**

Al ejecutar el comando del túnel 6to4 éste automáticamente configura los parámetros del túnel tomando las direcciones IPv4 incluidas en los equipos.

Se puede visualizar en las Figuras 46 y 47 cómo se establece la comunicación entre el *router* Cisco 7609 y el BRAS ME60-x8, a través del túnel 6to4.

```
R7609-NGN-I10.1.1.7#ping ipv6 2002:ac10:4ae2::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002:AC10:4AE2::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/8/36 ms
```

Figura 46: *Ping* del *router* Cisco 7609 al BRAS ME60-x8.

Fuente: Los Autores.

```
[cnt-bras-03--172.16.74.226]ping ipv6 2002:a64:02::1
  PING 2002:a64:02::1 : 56  data bytes, press CTRL_C to break
    Reply from 2002:A64:2::1
    bytes=56 Sequence=1 hop limit=64  time = 3 ms
    Reply from 2002:A64:2::1
    bytes=56 Sequence=2 hop limit=64  time = 2 ms
    Reply from 2002:A64:2::1
    bytes=56 Sequence=3 hop limit=64  time = 3 ms
    Reply from 2002:A64:2::1
    bytes=56 Sequence=4 hop limit=64  time = 2 ms
    Reply from 2002:A64:2::1
    bytes=56 Sequence=5 hop limit=64  time = 2 ms

  --- 2002:a64:02::1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/2/3 ms
```

Figura 47: *Ping* del BRAS ME60-x8 al *router* Cisco 7609.

Fuente: Los Autores.

En este escenario no se puede probar el túnel 6rd, debido a que el agregador (BRAS) no es compatible con este mecanismo, por lo tanto se crea un tercer escenario para probar su funcionamiento en un punto de la red.

III.2.3.3 Escenario 3: Red IPv6, *BackBone* IPv4 e Internet IPv6.

Se mantiene en IPv4 el enlace entre los *routers* Cisco simulando el *BackBone* IP de CANTV, esto se realiza para probar el funcionamiento de *Dual Stack* en conjunto con 6rd, el cual posee mejoras con respecto al túnel 6to4 y es actualmente mucho más recomendado en caso de necesitar la implementación de un túnel en la red del operador. Este escenario al igual que al anterior es presentado para establecer una solución en caso de no poder implementar la transición a la nueva versión de Protocolo de Internet, en el *BackBone* IP por alguna circunstancia (económica, disponibilidad de personal, tiempo de implementación, entre otras). En la Figura 48 observara el planteamiento del escenario.

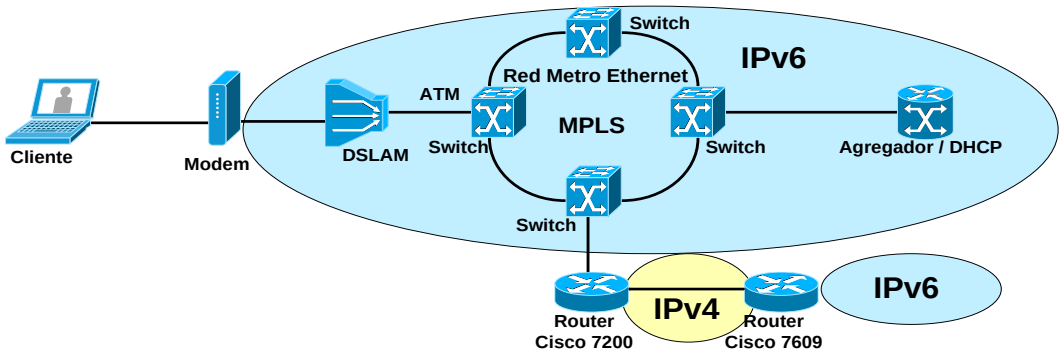

Figura 48: Escenario de prueba tres.

Fuente: Los Autores.

Buscando una mejor comprensión de lo planteando en este escenario, se presenta a continuación la Figura 49, en la cual se explica el funcionamiento de la red.

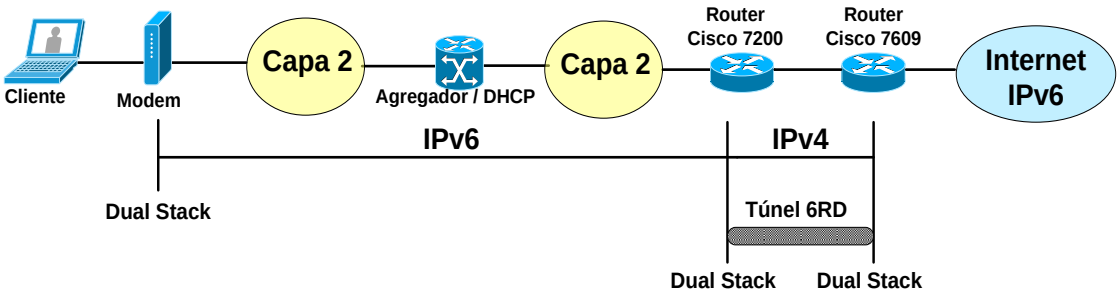

Figura 49: Funcionamiento de la red en escenario tres.

Fuente: Los Autores.

Al empezar a configurar los dos *routers*, se comprobó que ninguno de los dos es compatible actualmente con el mecanismo 6rd, es decir, que se necesita de un *firmware* para su utilización. Comprobando lo mencionado anteriormente se presenta en la Figura 50, cómo el *router* Cisco 7609 no reconoce los comandos de configuración.

En primer lugar se debe introducir el comando:

Router(config)#ipv6 general-prefix Entrega 6rd Tunnel 0

```
R7609-NGN-I10.1.1.7(config)#ipv6 general-prefix Entrega 6rd Tunnel 0
                                                          ^
% Invalid input detected at '^' marker.

R7609-NGN-I10.1.1.7(config)#
```

Figura 50: Detección de entrada inválida en "6rd" en el Cisco 7609 (1).

Fuente: Los Autores.

Se comprueba en la Figura 51, utilizando la modalidad de "ayuda" que presenta el *router*, que no existe la opción de 6rd para la configuración.

```
R7609-NGN-I10.1.1.7(config)#ipv6 general-prefix Entrega ?
  6to4               Create 6to4 prefix from IPv4 address
  X:X:X:X::X/<0-128>  IPv6 prefix

R7609-NGN-I10.1.1.7(config)#ipv6 general-prefix Entrega
```

Figura 51: Verificación de la inexistencia de 6rd como opción de configuración *router* Cisco 7609 (1).

Fuente: Los Autores.

A pesar de que no se podía seguir avanzando sin la utilización de este comando se comprueba en las Figuras 52 y 53, como tampoco reconoce y no posee la opción de 6rd en la **interfaz Tunnel 0**, el comando de configuración es el siguiente:

Router(config-if)# Tunnel mode ipv6ip 6rd

```
R7609-NGN-I10.1.1.7(config-if)#tunnel mode ipv6ip 6rd
                                                  ^
% Invalid input detected at '^' marker.

R7609-NGN-I10.1.1.7(config-if)#
```

Figura 52: Detección de entrada inválida en "6rd" en el Cisco 7609 (1).

Fuente: Los Autores.

```
R7609-NGN-I10.1.1.7(config-if)#tunnel mode ipv6ip ?
  6to4         IPv6 automatic tunnelling using 6to4
  auto-tunnel  IPv6 automatic tunnelling using IPv4 compatible addresses
  isatap       IPv6 automatic tunnelling using ISATAP
  <cr>

R7609-NGN-I10.1.1.7(config-if)#tunnel mode ipv6ip
```

Figura 53: Verificación de la inexistencia de 6rd como opción de configuración *router* Cisco 7609 (1).

Fuente: Los Autores.

Sin encontrar resultados positivos en la configuración del *router* Cisco 7609, se procedió a comprobar la inexistencia de la opción 6rd para la configuración del *router* Cisco 7200:

```
R7204-RUT-10.1.1.1(config)#ipv6 ?
  access-list      Configure access lists
  cef              Cisco Express Forwarding for IPv6
  hop-limit        Configure hop count limit
  host             Configure static hostnames
  icmp             Configure ICMP parameters
  local            Specify local options
  nat              NAT-PT Configuration commands
  neighbor         Neighbor
  ospf             OSPF
  prefix-list      Build a prefix list
  route            Configure static routes
  router           Enable an IPV6 routing process
  source-route     Process packets with source routing header options
  unicast-routing  Enable unicast routing

R7204-RUT-10.1.1.1(config)#ipv6
```

Figura 54: Verificación de la inexistencia de 6rd como opción de configuración *router* Cisco 7200 (1).

Fuente: Los Autores.

En la Figura 54 se observa como el *router* no posee la opción de "*general-prefix*" la cual es esencial para lograr configurar el prefijo 6rd. En la Figura 55 se puede demostrar como en la **Interfaz Tunnel 0** no posee la opción de 6rd.

```
R7204-RUT-10.1.1.1(config-if)#tunnel mode ipv6ip ?
  6to4         IPv6 automatic tunnelling using 6to4
  auto-tunnel  IPv6 automatic tunnelling using IPv4 compatible addresses
  isatap       IPv6 automatic tunnelling using ISATAP
  <cr>

R7204-RUT-10.1.1.1(config-if)#tunnel mode ipv6ip
```

Figura 55: Verificación de la inexistencia de 6rd como opción de configuración *router* Cisco 7200 (2).

Fuente: Los Autores.

Sin embargo con la actualización pertinente, la cual se puede observar en la página web de cisco [54] y la correcta configuración se puede lograr configurar este mecanismo de transición.

III.2.3.4 Configuraciones Adicionales.

DHCPv6.

Buscando realizar una solicitud DHCPv6 satisfactoria al CPE por parte de un equipo final, se instaló en una máquina Linux con distribución Ubuntu el paquete *Dibbler-Client,* con el cual se realizó una solicitud al *modem* y se verificó la correcta negociación de la dirección IPv6 e información adicional como la dirección del DNS. Sin embargo, a pesar de que se verificó como abierto el estado del puerto UDP 546 en una computadora con Windows Vista, no se logró recibir respuesta del CPE, aun cuando la computadora envió un *DHCPv6 Solicit.*

A continuación se puede observar en las Figuras 56 y 57 cómo se configuró manualmente la dirección IP del *modem* (WAN) y el *pool* de direcciones a entregar por el CPE (LAN):

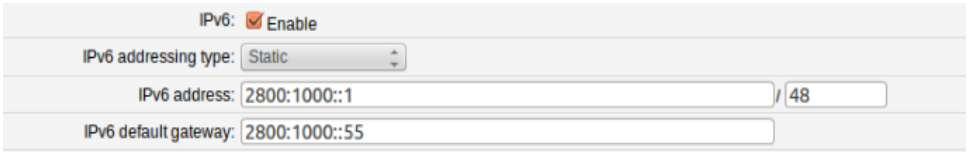

Figura 56: Configuración de la WAN.

Fuente: Los Autores.

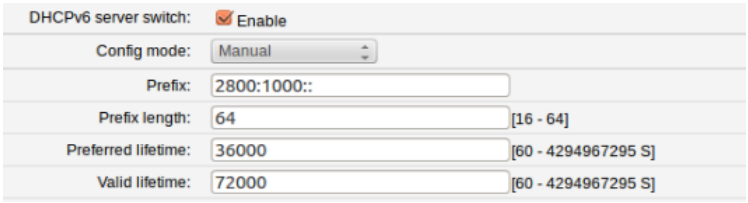

Figura 57: Configuración de la LAN.

Fuente: Los Autores.

Se observa en la Figura 58 como se genera todo el proceso de solicitud y respuesta de dirección IPv6 por parte del cliente al CPE.

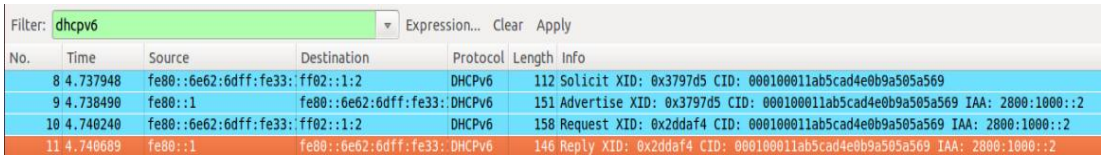

Figura 58: Proceso de solicitud y respuesta de direcciones IPv6.

Fuente: Los Autores.

Finalmente se observa en la Figura 59 la información de la interfaz de red del cliente, logrando denotar la dirección IPv6 y su longitud de prefijo otorgada (2800:1000::2/64):

Figura 59: Interfaz de red del cliente.

Fuente: Los Autores.

Inicialmente se planeaba utilizar un servidor ISC DHCPv6 para la asignación de direcciones a los clientes finales; sin embargo, no fue posible configurar correctamente dos instancias del servidor, de modo que operara simultáneamente en IPv4 e IPv6, procediéndose entonces a instalar una única instancia configurada para IPv6 en un servidor físico diferente, obteniendo el mismo resultado negativo. En consecuencia, se recomendó al personal de CANTV emplear un servidor *Dibbler*, el cual se instaló y configuró sin mayor inconveniente. En el archivo de configuración del mismo se abarcaron diversos tipos de asignación de direcciones, con el objetivo inicial de visualizar el comportamiento del CPE ante estos (por ejemplo, delegación de prefijo y asignación de dirección específica), distribuyendo segmentos del prefijo asignado a la CANTV de forma arbitraria, por tratarse de un entorno netamente experimental. La Figura 60 muestra el archivo de configuración del servidor *Dibbler*.

```
log-level 8
log-mode short
preference 0

iface "eth2" {
 t1 1800-2000
 t2 2700-3000
 prefered-lifetime 3600
 valid-lifetime 7200

 class {
   pool 2800:1000::/48
 }

 ta-class {
    pool 2800:1000:1::/64
 }

 pd-class {
     pd-pool 2800:1000:2::/48
     #pd-poll 2800:1000:3::/48
     pd-length 64
 }
 option dns-server 2800:1000::1
 option domain ipv6.net
}
```

Figura 60: Archivo de configuración del servidor *Dibbler* DHCPv6.

Fuente: Los Autores.

El servidor está a la escucha en el puerto UDP 547 del grupo *multicast* FF02::1:2, estado que se puede comprobar ejecutando el comando **netstat –ntuap |grep :547.** La Figura 61 muestra el resultado de dicho comando.

```
root@mail:~# /etc/init.d/dibbler-server restart
Restarting DHCPv6 server: dibbler-server.
root@mail:~# netstat -ntuap |grep :547
udp6       0      0 fe80::20e:cff:fe67::547 :::*                    24357/dibbler-serve
udp6       0      0 ff02::1:2:547           :::*                    24357/dibbler-serve
root@mail:~#
```

Figura 61: Direcciones del servidor a la escucha en el puerto UDP6 547.

Fuente: Los Autores.

Sin embargo, buscando comprobar el correcto funcionamiento del servidor DHCPv6 de forma práctica, se conectó directamente al servidor una computadora Linux con distribución Ubuntu y el paquete *Dibbler-Client* activo. De este modo, se

realizó una solicitud DHCPv6 con resultado positivo, comprobando la correcta operación del servidor. La Figura 62 muestra una captura de paquetes donde se refleja el proceso de negociación de DHCPv6, incluyendo la dirección IPv6 asignada. Por otra parte, la Figura 63 muestra la configuración de la interfaz Ethernet de la computadora utilizada una vez culminada la negociación DHCPv6, apreciándose que la dirección IPv6 coincide con la mostrada en la Figura 62

Figura 62: Proceso de solicitud y respuesta de direcciones IPv6 con cliente directamente conectado.

Fuente: Los Autores.

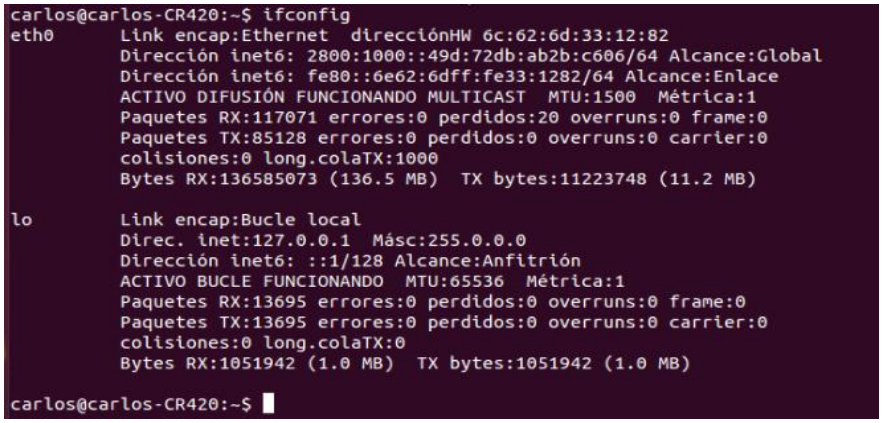

Figura 63: Configuración de Interfaz Eth0.

Fuente: Los Autores.

DNS

Por otra parte, el servidor DNS consta de una distribución Bind9, que fue igualmente instalada en la misma máquina física que el servidor *Dibbler*. Este servidor DNS fue configurado para resolver dominios IPv6 exclusivamente. El dominio del mismo fue definido como “ipv6.net” y, aprovechando la importante simplificación en el manejo de direcciones que supone un servidor DNS en IPv6, se asignó un registro a cada interfaz del *router* conectado al servidor, así como al

agregador, facilitando las operaciones de *troubleshooting* y diagnóstico para estos equipos. La Figura 64 muestra el archivo de configuración del servidor DNS, mientras que la Figura 65 muestra diferentes operaciones de *ping* dirigidas a los diferentes nombres de dominio asignados a los equipos mencionados anteriormente, así como al servidor mismo.

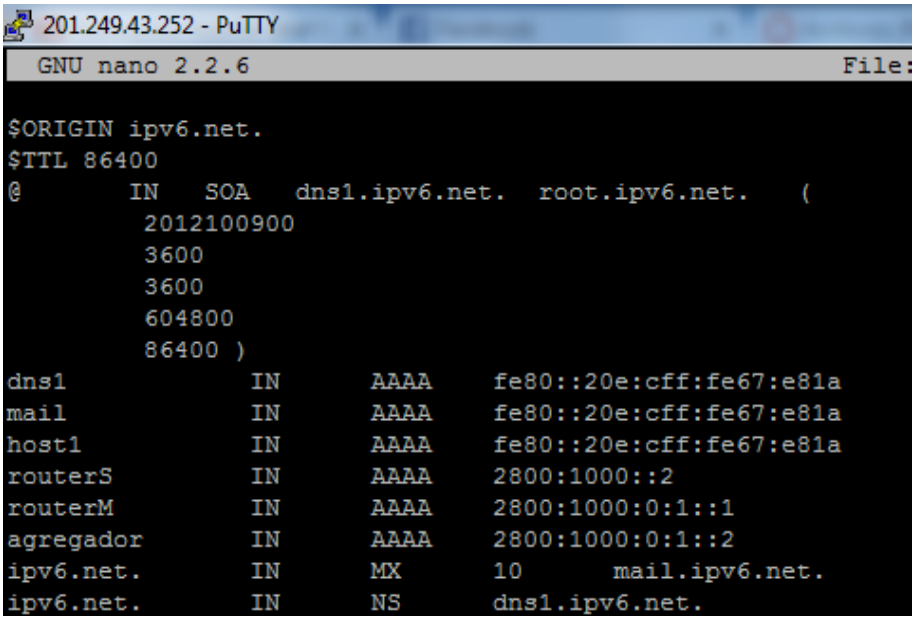

Figura 64: Archivo de configuración del servidor DNS Bind9.
Fuente: Los Autores.

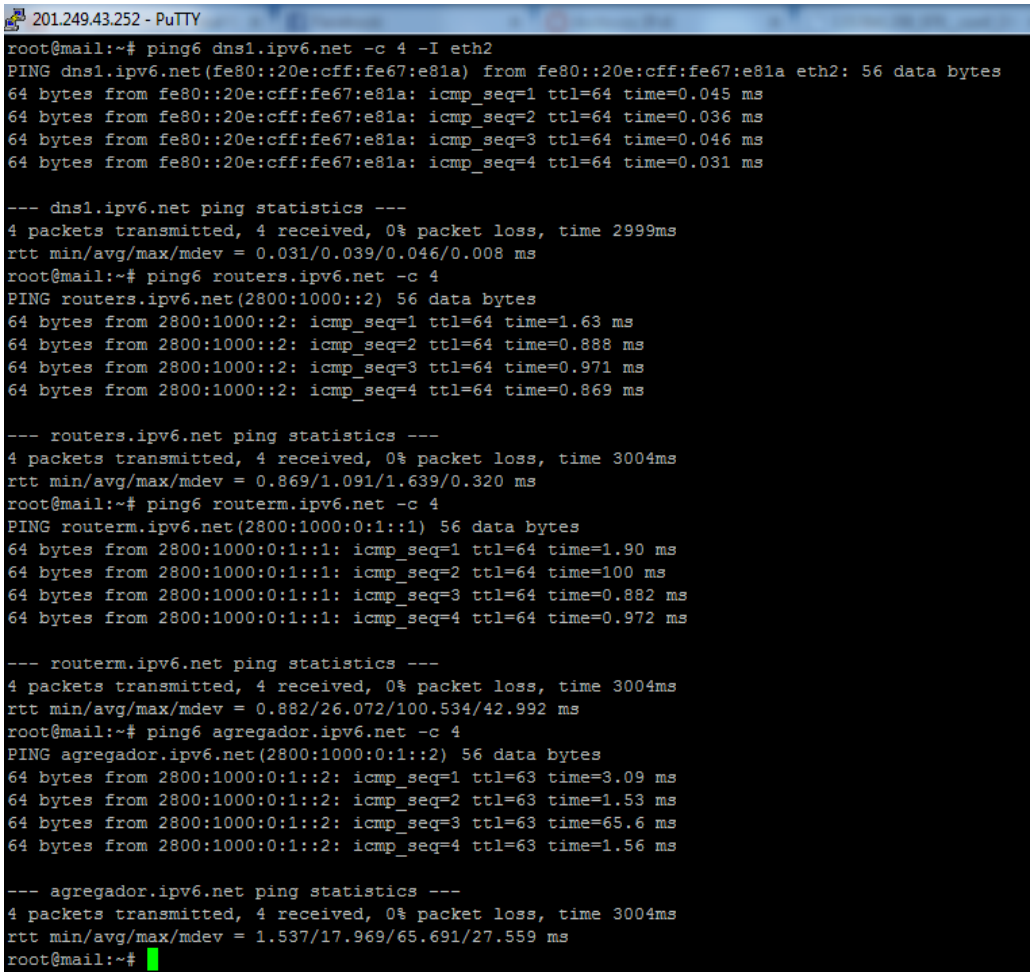

Figura 65: Archivo de configuración del servidor DNS Bind9.
Fuente: Los Autores.

III.2.4 Cierre y Recomendaciones.

Como parte fundamental del desarrollo de este Trabajo Especial de Grado, los autores proveerán una lista incluyendo una serie de pasos sistemáticos recomendados para todo ISP que desee realizar su transición a IPv6 satisfactoriamente y de la forma más eficiente posible. Estas recomendaciones se realizan con base en todo lo reflejado en el Marco Referencial, así como las entrevistas y las experiencias propias de los autores durante los procesos de configuración de los diferentes equipos de la red del operador CANTV.

Capítulo IV

Resultados

Este capítulo contiene los resultados obtenidos en este Trabajo Especial de Grado, los cuales dan respuesta a los objetivos específicos indicados en el Capítulo I. Los mismos son presentados a continuación:

Se realizó una investigación exhaustiva para determinar la compatibilidad de los equipos reflejados en la Tabla 9, ubicada en el Capítulo III. Esta investigación se realizó por medio de páginas web y consulta a los proveedores por correo electrónico.

A continuación se puede observar en la Tabla 14 la compatibilidad de los equipos mencionados en la Tabla 9, siendo importante mencionar que estos equipos están en funcionamiento actualmente en la red de CANTV; sin embargo, no están incluidos todos los equipos que están en funcionamiento hoy en día, esto debido a que el archivo que envió el personal de CANTV a los autores de este proyecto consta del año 2007 y una gran parte de los equipos ahí reflejados han sido reemplazados. Debido a esto se incluyeron equipos que también se encuentran actualmente en la red del laboratorio de CANTV, el cual es una representación a pequeña escala de la red actual de la empresa.

Se confirmó el funcionamiento de todos los equipos colocados en la tabla presentada a continuación:

Marca	Modelo	Arquitectura	Caracteristicas	Compatibilidad con IPv6
Alcatel - Lucent	7450 ESS-1 (Metro Ethernet)	Banda Ancha IP (Redes Metro Ethernet)	*Switches*	Compatible
	7450 ESS-7 (Metro Ethernet)			
	7450 ESS-12 (Metro Ethernet)			
	7302	Banda Ancha IP (Red de Acceso)	*DSLAM*	
Cisco	5300	Arquitectura UNIRED	*Gateways*	
	5400			
	5850			
	7500		*Router*	
	12000	Banda Ancha IP (Red de Acceso)		
	7600			
	7200	Banda Ancha IP		
	7609			
Juniper	E320	Banda Ancha IP	*Agregador*	No se obtuvo respuesta
	SA700			
Huawei	UA5000	Banda Ancha IP (Red de Acceso)	*DSLAM*	Compatible
	MA5600			
	ME60-X8	Banda Ancha IP	*Agregador*	
	HG532e	Arquitectura ABA	*Modem*	
ZTE	FSAP9800	Banda Ancha IP (Red de Acceso)	*DSLAM*	
	ZXHNH108L	Arquitectura ABA	*Modem*	
ZYXEL	P-660RU-T1	Arquitectura ABA	*Modem*	No Compatible
RYGE	WA41R	Arquitectura ABA	*Modem*	
SENDTEL	MS8-8817	Arquitectura ABA	*Modem*	

Tabla 14: Compatibilidad con IPv6 de los Equipos de la Infraestructura de CANTV.

Fuente: Los Autores.

Es importante resaltar que la Tabla 14 representa una muestra de los equipos actualmente en funcionamiento en la red de CANTV.

La mayoría de los equipos que son compatibles con IPv6 necesitan una actualización de *firmware* para su funcionamiento con algunos mecanismos de transición. En el caso específico, por ejemplo, de los *routers* Cisco 7609, 7200 y el BRAS ME60-x8, necesitan una actualización (Cisco IOS Release 15.1(3)S5a) para poder trabajar con el túnel 6rd.

Los equipos que no son compatibles no podrán funcionar con IPv6, por lo tanto al momento de la transición se necesitará realizar un cambio de los mismos. Partiendo de la Tabla 14, se aprecia que estos equipos son *Modems* o CPE, por lo tanto se necesita hacer un estudio de los costos que involucraría este reemplazo.

CANTV como el ISP más grande de Venezuela realizó una solicitud de un bloque de direcciones IPv6 a la LACNIC, la cual otorgó a la empresa el siguiente rango de direcciones:

Dirección IP: 2800:1000:0000:0000:0000:0000:0000:0000
Longitud del prefijo: /24
Red: 2800:1000:0:0:0:0:0:0
Dirección del prefijo: FFFF:FF00:0000:0000:0000:0000:0000:0000
Rango de direcciones: 2800:1000:0000:0000:0000:0000:0000:0000 -
2800:10FF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
Total de direcciones disponibles: 20.282.409.603.651.670.423.947.251.286.016

El otorgamiento de una longitud de prefijo /24 es uno de los más grandes que la LACNIC le ha entregado a un ISP, ya que lo que se acostumbra entregar es un /32.

CANTV posee aproximadamente:

Clientes Activos ABA Residenciales: 2.080.000

Clientes Activos ABA Empresariales: 200.000

Se plantea el siguiente plan de direccionamiento con base en la Red Troncal IP 2010 – 2012 de CANTV, que podrá observar en el Apéndice C.

Capa Acceso	
Total Clientes Residenciales Aprox.	2080000
Total Clientes Residenciales Proyectados	6240000
Total Clientes Empresariales Aprox.	200000
Total Clientes Empresariales Proyectados	600000
Cantidad de Servidores	14
Cantidad de Agregadores Aproximado	40

Tabla 15: Conformación de la Capa de Acceso.

Fuente: Los Autores.

Se puede observar en la Tabla 15 el cálculo de una proyección de la cantidad de clientes residenciales y empresariales, esto se debe a que la "LACNIC recomienda reservar al menos un 300% del crecimiento de la empresa en el momento de distribuir las direcciones IPv6 [51] ". También se puede observar que actualmente CANTV cuenta con un aproximado de 40 agregadores en su capa de acceso, conectados a un balanceador y este a su vez con 14 servidores DHCP. El balanceador cumple con la función de distribuir equitativamente las peticiones de direcciones IP hacia los distintos servidores, evitando así una sobre carga en alguno de ellos.

En la Figura 66 se puede observar lo comentado anteriormente:

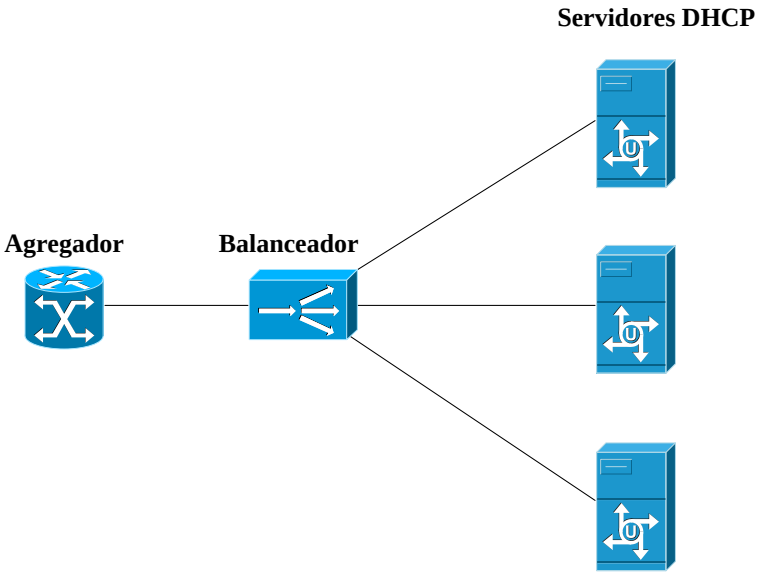

Figura 66: Comunicación entre el Agregador, Balanceador y Servidores DHCP.

Fuente: Los Autores.

A causa de esta cantidad de servidores DHCP se plantean en la Tabla 16 dos opciones de distribución de *pool* de direcciones en los mismos:

Opción	Prefijos /32
1	2800:1000::/32 - 2800:1011::/32
2	2800:1000::/32 - 2800:1040::/32

Tabla 16: Opciones de direccionamiento en servidores DHCP.

Fuente: Los Autores.

En la primera opción se propone configurar en los servidores DHCP un grupo de once (11) prefijos /32, con los cuales se cubre en totalidad los requerimientos de direcciones IPv6 de todos los clientes empresariales y residenciales a nivel nacional. Por otra parte, la segunda opción plantea un escenario de mayor holgura, ya que se configurarían en los servidores DHCP un grupo de cuarenta (40) prefijos /32, correspondientes cada uno a un único Agregador presente en la red, otorgando mayor

independencia y descentralización en la asignación de prefijos a los clientes de manera local.

Igualmente, se plantea una distribución de prefijos para las direcciones IPv6 administrativas, separadas por Capas, como se muestra en la Tabla 17.

Capas	Prefijos /32
Capa Core - Distribución	2800:1050::/32
Capa Distribución Internet - Core	2800:1051::/32
Capa Borde - Distribución Internet	2800:1052::/32
Internet - Borde	2800:1053::/32

Tabla 17. Direccionamiento para administración.

Fuente: Los Autores.

Se evaluaron tres mecanismos de transición a IPv6 como se pudo observar en la Tabla 13 ubicada en el Capítulo III, en ella se puede apreciar que el mejor mecanismo a aplicar es el *Dual Stack*, sin embargo se plantearon tres escenarios, dentro de los cuales fue probado el túnel 6to4 en conjunto con *Dual Stack.*

En la red actual del laboratorio de CANTV es necesario un mecanismo de túnel en el *BackBone* IP.

Las pruebas con el túnel 6to4 se desarrollaron sin ningún tipo de problema, en cambio con el túnel 6rd fue imposible realizar prueba alguna, esto debido a la falta de compatibilidad de los *routers* Cisco 7200 y 7609, como también del agregador ME60-x8 con ese mecanismo.

Se puso a prueba en la red del laboratorio de CANTV los protocolos de enrutamiento interior (OSPFv3 y RIPng) y exterior (BGP) más utilizados en la actualidad.

Se plantea utilizar OSPFv3 en todos los enlaces existentes entre la Capa de Borde, Distribución Internet, Core, Distribución y Acceso. El protocolo BGP sería

implementado entre la Capa Borde e Internet conectándonos así con otros Sistemas Autónomos (AS) como por ejemplo Global Crossing.

Se implementó una maqueta funcional de red con tres escenarios, los cuales funcionaron correctamente con los mecanismos de transición y protocolos de enrutamiento configurados. Sin embargo, no se logró que el cliente navegara en Internet directamente en IPv6, ya que la solicitud de direcciones IPv6 por parte del CPE no pasa por el DSLAM, debido a que éste descarta los paquetes IPv6.

Se comprobó la conectividad de los equipos (*Routers*, agregador y servidores) en IPv6 con la realización de *ping* entre ellos.

CANTV no publicaría su prefijo /24, por lo tanto publicara todos los prefijos /32 que estén utilizando hasta el momento, logrando así que todos los sistemas autónomos conectados a la empresa por medio de BGP4+ conozcan los prefijos que posee.

La transición a IPv6 es un proceso complejo porque, entre diferentes razones, es único para cada ISP, ya que dependerá de la infraestructura que tenga instalada, abarcando desde modelos específicos de los equipos utilizados, protocolos implementados en dicha infraestructura hasta la topología de la red misma del operador, entre otros factores.

Se puede entonces realizar una lista de procedimientos y recomendaciones que permitan configurar con éxito una red IPv6 completamente operativa, como se detalla a continuación:

FASE I. **Estudio y Levantamiento de Información**.

En esta etapa se lleva a cabo la búsqueda y recopilación de los modelos de equipos utilizados en la infraestructura del operador para su posterior revisión en cuanto a compatibilidad con el protocolo IPv6 en sus diferentes ámbitos.

Esta revisión implica el chequeo de compatibilidad con diferentes mecanismos de transición a IPv6 de los diferentes equipos, así como los procedimientos y procesos necesarios para hacer que éstos sean compatibles, en caso de no serlo en un inicio.

FASE II. **Diseño**.

En esta fase del proyecto, se abarca el estudio de la distribución de la clientela actual del operador, los posibles rangos de direcciones IPv6 asignables a cada uno de estos, la investigación de los principales mecanismos de transición que pueden implementarse actualmente, así como los protocolos de enrutamiento a utilizar.

Debido al carácter jerárquico que plantea el enrutamiento en IPv6, es de suma importancia realizar una distribución adecuada de los prefijos a los diferentes equipos intermedios del operador en cuestión, así como aquellos que se entreguen a cada usuario final de cualquier tipo, ya sea residencial o empresarial.

FASE III. **Evaluación**.

En esta fase el operador debe diseñar escenarios de pruebas con los parámetros de desempeño correspondientes, buscando verificar de forma práctica que la configuración seleccionada para sus equipos funciona correctamente.

Estos escenarios abarcan la configuración precisa de cada equipo de la infraestructura de la red del operador, yendo desde CPEs, DSLAMs, *switches, routers*, servidores hasta, inclusive, los equipos finales de los usuarios del operador.

Igualmente, la configuración de cada equipo debe abarcar la ejecución del mecanismo de transición en cuestión seleccionado por el ISP, verificando su correcta operación tanto a nivel de Capa 2 del modelo OSI como Capa 3 del mismo; esto debido a que, si bien IPv6 es un protocolo de capa de red equivalente a Capa 3 del modelo OSI, su predecesor hacía uso del *Address Resolution Protocol (ARP)*

perteneciente a Capa 2, lo cual podría traer inconvenientes al momento de realizar las configuraciones pertinentes.

Capítulo V

Conclusiones y Recomendaciones

En el presente capítulo se dan a conocer las conclusiones y recomendaciones que surgen de la investigación realizada.

V.1 Conclusiones

No es factible realizar una migración a IPv6 ya que no se concibe la posibilidad de realizar un apagón de la Internet IPv4 para dar paso al nuevo protocolo. Es por ello que se plantea en cambio una transición, realizando un cambio progresivo y sostenido hacia el nuevo protocolo.

En ese sentido, el mecanismo de transición más conveniente a utilizar es 6rd en conjunto con *Dual Stack*, ya que existen antecedentes que muestran su alta facilidad y velocidad de implementación a gran escala en ISPs de envergadura, como es el caso de Free, segundo mayor proveedor de servicios de Internet en Francia. La implementación del mismo abarcó apenas cinco semanas, incluyendo procesos propios del desarrollo inicial del mecanismo de cuestión (actualización del código instalado en los CPEs del ISP partiendo de uno existente para 6to4 y adecuación de la plataforma del ISP para el nuevo mecanismo). Igualmente, en dicho período fue posible realizar las pruebas pertinentes con diferentes sistemas operativos y aplicaciones. Además, en el caso específico de CANTV, ya fue realizada una solicitud a la LACNIC y dispone de un prefijo IPv6 de alcance global, proceso que fue realizado por Free en el mismo período de implementación del mecanismo, es decir, en las cinco semanas totales.

Igualmente, presenta las condiciones más favorables para los ISPs a nivel de gastos, ya que en condiciones ideales estos pueden actualizar sus *routers* CPE y pueden operar como *gateways* entre sus infraestructuras IPv4 y el Internet IPv6

global, permitiendo de este modo la encapsulación de IPv6 sobre IPv4. Asimismo, si bien esto es absolutamente transparente para el cliente final, no lo será para la infraestructura de CANTV, pues éste debe considera el nuevo direccionamiento existente en IPv6, así como el enrutamiento correspondiente para el mismo.

Además, mientras que un ISP que implementa 6to4 puede garantizar que los paquetes IPv6 salientes desde sus clientes serán capaces de alcanzar el Internet IPv6, y además garantizar que los paquetes provenientes de otros sitios 6to4 alcanzarán a sus clientes, no puede garantizar que los paquetes provenientes de sitios IPv6 nativo serán capaces de alcanzar a sus clientes. El problema consiste en que un paquete proveniente de una dirección IPv6 nativa necesita atravesar, en algún punto de su recorrido, un relé 6to4 para realizar la encapsulación IPv6/IPv4 requerida. No hay garantías de que existan rutas hacia un relé provenientes desde todas partes, ni hay garantía de que dichos relés hagan el reenvío de los paquetes hacia la totalidad del Internet IPv4, mientras que con 6rd no se presenta este problema, ya que si bien 6to4 hace uso de un prefijo estándar bien conocido (2002::/16), éste emplea un prefijo que ha sido asignado al proveedor en cuestión, quien al ser dueño del mismo, puede manejarlo y publicarlos según sus preferencias.

Por otra parte, si un ISP opera uno o varios relés enrutadores 6to4 y abre rutas IPv6 hacia ellos en el Internet IPv6, para el prefijo 2002::/16, puede recibir en estos relés paquetes destinados a un número desconocido o hacia un 6to4 de otro ISP. Si éste no reenvía dichos paquetes, se creará un "agujero negro" en el cual los paquetes pueden perderse sistemáticamente, rompiendo parte de la conectividad IPv6. Por otro lado, si reenvía dichos paquetes, el ISP no será capaz de dimensionar sus relés enrutadores 6to4 en proporción al tráfico de sus propios clientes; en consecuencia, la calidad de servicio, al menos para los clientes 6to4 de otros ISPs será difícilmente garantizada

Asimismo, los protocolos de enrutamiento interior más eficientes en IPv6 son IS-IS y OSPFv3, los cuales a diferencia de RIPng utilizan la técnica de estado de enlace, lo que permite tomar en cuenta aspectos importantes como Ancho de Banda y retrasos, evitando depender de un número máximo de saltos para llegar al destino. Estos protocolos además de poseer estas características que los hacen prevalecer ante RIPng, también tienen un aspecto de gran relevancia como lo es una distancia administrativa menor, permitiendo tener prioridad ante otros protocolos. Se mantiene en IPv6 la implementación de BGP como protocolo de enrutamiento exterior, debido a su gran rendimiento para establecer comunicación entre dos o más Sistemas Autónomos (AS). Estos protocolos reflejaron un comportamiento óptimo en los dispositivos que conforman la red del laboratorio de CANTV, que es representativa de cara a la prestación de servicios con conectividad IPv6 hacia clientes residenciales y empresariales.

En cuanto a direccionamiento, se establece entregar una longitud de prefijo /56 a clientes residenciales, por lo que el promedio de direcciones IP utilizadas en un mismo instante en una residencia es de diez (10), con un máximo de treinta (30), de igual manera es importante resaltar que cada cliente residencial promedio, posee un *router* para implementar una red privada lo cual genera otra subred y hace necesario entregar esta longitud de prefijo. En el caso de los CPE que se encuentran en prueba y que se han comentado durante el desarrollo del Trabajo Especial de Grado, que trabajan en modo *routing* también necesitarían esta longitud de prefijo ya que permiten crear dos *Service Set IDentifier* (SSID) , también se considera importante la elección porque en la actualidad se trabaja *subnetting* por saltos de *nibble* en *nibble* (la mitad de un byte o 4 bits), lo cual permite trabajar actualmente con longitudes de prefijo /64, /60, /56, /52, entre otras; pero siempre es recomendable trabajar con las denominadas “buenas prácticas” y actualmente se establece repartir un /56 a clientes residenciales. La entrega de esta longitud de prefijo se basa en el estudio realizado y recomendaciones realizadas por diferentes expertos en el área. Sólo se entregaría bajo pedido y el estudio adecuado un /48 a clientes residenciales, descartando opciones

como un prefijo /56, pues éste no figura como un estándar sólido que favorezca los nuevos esquemas de enrutamiento en IPv6. En lo referente al direccionamiento para clientes empresariales se establece otorgar un /48, cumpliendo con las recomendaciones estándar estipuladas en diversos RFCs y organismos pertinentes como la LACNIC.

Finalmente, es requerido un cambio de los CPEs actualmente distribuidos por CANTV, ya que no poseen la compatibilidad con IPv6; sin embargo, actualmente se están realizando pruebas con los modelos HG532e (Huawei) y ZXHNH108L (ZTE), los cuales son compatibles con IPv6, soportando *Dual Stack* y pudiendo operar en modo *router*, ya que esta modalidad facilita una serie de prestaciones que no son posibles de realizar en modo *bridge*, como por ejemplo el control remoto. Este reemplazo de los CPE involucra un costo que está reflejado en el Apéndice D.

V.2 Recomendaciones.

Si se determina la implementación de 6rd como mecanismo de transición, se recomienda solicitar una actualización de *firmware* de los equipos actualmente en funcionamiento en la red de CANTV, lo cual no generaría costos adicionales en la implementación de IPv6.

Estudiar la posibilidad de desarrollar en la red de CANTV el Escenario uno (1) planteado en el capítulo III, ya que permite utilizar sólo *Dual Stack* como mecanismo de transición. Sin embargo, es recomendable establecer un cronograma con los proveedores para mantener los equipos lo más actualizados posible.

Abrir la posibilidad de recibir cursos de capacitación para todo el grupo de trabajo que se encargue de la transición a IPv6 por parte del ISP.

Sólo se recomienda utilizar el método de traducción en equipos que sólo trabajen en IPv4 y se tengan que comunicar con equipos que sólo operen en IPv6. Sin

embargo, es de gran importancia incluir estos equipos en una lista para su posterior reemplazo.

Realizar pruebas a mayor escala, con una red piloto conectada a los proveedores de mayor jerarquía: NSPs

Profundizar en las pruebas de BGP4+ en los *routers* de borde de sistema autónomo

Hacer estudios detallados de las implicaciones de seguridad en la transición al nuevo protocolo. Aunque ese no es un objetivo de este proyecto (estaba fuera del alcance planteado) se considera que es crítico hacerlo.

Bibliografía

[1] Information Sciences Institute, University of Southern California, "The Internet Engineering Task Force (IETF)," Septiembre 1981. [Online]. Available: http://www.ietf.org/rfc/rfc791.txt. [Accessed 12 Mayo 2013].

[2] Rekhter, Y.; Cisco Systems; Moskowitz, B.; Chrysler Corp.; Karrenberg, D.; RIPE NCC; de Groot, G. J.; Lear, E.; Silicon Graphics, Inc.;, "The Internet Engineering Task Force (IETF)," Febrero 1996. [Online]. Available: http://tools.ietf.org/html/rfc1918. [Accessed 14 Mayo 2013].

[3] "RFC3022," Enero 2001. [Online]. Available: http://www.rfc-es.org/rfc/rfc3022-es.txt. [Accessed 15 Mayo 2013].

[4] C. Bryant. [Online]. Available: http://www.thebryantadvantage.com/Network+FreeTutorialRFC1918PrivateIPAddressNATPAT.htm.

[5] P. Colomés, Agosto 2010. [Online]. Available: http://www.redescisco.net/v2/art/implementando-nat-en-*router*s-cisco/.

[6] "RFC2460," Diciembre 1998. [Online]. Available: http://www.rfc-es.org/rfc/rfc2460-es.txt. [Accessed 20 Enero 2013].

[7] D. Nuñez, *Estudio para la migración de IPv4 a IPv6 para la empresa proveedora de internet MILLTEC S.A*, Quito: Tesis.Escuela de Electrónica.Ingeniería.Escuela Politecnica Nacional, 2009.

[8] Thomson, S. ; Bellcore; Narten, T., "RFC2462," Diembre 1998. [Online]. Available: http://www.rfc-es.org/rfc/rfc2462-es.txt. [Accessed 18 Mayo 2013].

[9] J. Davies, Understanding IPv6, Washington: Microsoft Press, 2008.

[10] S. Thomson, Bellcore and C. Huitema, "RFCes," Diciembre 1995. [Online]. Available: http://www.rfc-es.org/rfc/rfc1886-es.txt. [Accessed 24 Noviembre 2013].

[11] W. Torres, *IPv6*, Caracas, 2012.

[12] S/A, "Apuntes de Networking," 2010. [Online]. Available: http://apuntesdenetworking.blogspot.com/2012/12/ipv6-direcciones-multicast.html. [Accessed 11 Julio 2013].

[13] J. Bound, B. Volz, T. Lemon, C. Perkins and M. Carney, "Rfc 3315," Julio 2003. [Online]. Available: www.ietf.org/rfc/rfc3315.txt. [Accessed 14 Marzo 2014].

[14] P. Mockapetris, "Rfc 1035," Noviembre 1987. [Online]. Available: tools.ietf.org/html/rfc1035. [Accessed 15 Marzo 2014].

[15] P. Mockapetris, "Rfc 1034," Noviembre 1987. [Online]. Available: tools.ietf.org/html/rfc1034. [Accessed 15 Marzo 2014].

[16] S. Thomson, C. Huitema, V. Ksinant and M. Souissi, "Rfc 3596," Octubre 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3596.txt. [Accessed 10 Marzo 2014].

[17] E. Ariganello and E. Barrientos Sevilla, Redes Cisco. CCNP a Fondo. Guía de estudio para Profesionales, Ciudad de Mexico, Distrito Federal: Alfaomega Grupo Editor, 2010.

[18] R. Coltun, D. Ferguson, J. Moy and A. Lindem, "Rfc 5340," Julio 2008. [Online]. Available: http://tools.ietf.org/html/rfc5340. [Accessed 18 Febrero 2014].

[19] J. Doyle and J. Carroll, "Network World," 1 Mayo 2007. [Online]. Available: http://www.networkworld.com/subnets/cisco/050107-ch9-ospfv3.html. [Accessed 24 Febrero 2014].

[20] Y. Rekhter and S. Hares, "Rfc 4271," Enero 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4271.txt. [Accessed 22 Febrero 2014].

[21] D. Shalini Punithavathani and K. Sankaranarayanan, "IPv4/IPv6 Transition Mechanisms," *European Journal of Scientific Research*, vol. 34, no. 1, pp. 110-124, Julio 2009.

[22] Narten, T.; IBM; Huston, G.; APNIC; Roberts, L.; Stanford University;, Marzo 2011. [Online]. Available: http://www.rfc-editor.org/rfc/rfc6177.txt.

[23] Lind, M.; TeliaSonera; Ksinant, V.; Communications, Thales; Park, S.; Electronics, SAMSUNG; Baudot, A.; Telecom, France; Savola, P.; CSC/Funet, Marzo 2005. [Online]. Available: http://www.ietf.org/rfc/rfc4029.txt.

[24] S. Hagen, IPv6 Essentials, Segunda edición ed., T. Apandi and M. Loukides, Eds., O'Reilly, 2006.

[25] Nordmark, E.; Sun Microsystems, Inc.; Gilligan, R.; Intransa, Inc.;, Octubre 2005. [Online]. Available: http://www.rfc-editor.org/rfc/rfc4213.txt.

[26] L. Zhou, V. Renesse and M. Marsh, "Implementing IPv6 as a Peer-to-Peer Overlay Network," *Proceedings of the 21st IEEE Symposium on Reliable Distributed Systems*, pp. 347-351, Octubre 2002.

[27] S. Thomson, Cisco, C. Huitema, Microsoft, V. Ksinant, 6WIND and M. Souissi, Octubre 2003. [Online]. Available: http://www.rfc-editor.org/rfc/rfc3596.txt.

[28] B. Carpenter and K. Moore, Febrero 2001. [Online]. Available: http://www.rfc-editor.org/rfc/rfc3056.txt.

[29] Templin, F.; Boeing Phantom Works; Gleeson, T.; Cisco Systems K. K.; Thaler, D.; Microsoft Corporation;, Marzo 2008. [Online]. Available: http://www.rfc-editor.org/rfc/rfc5214.txt.

[30] Huitema, C.; Microsoft;, Febrero 2006. [Online]. Available: http://www.rfc-editor.org/rfc/rfc4380.txt.

[31] Durand, A.; SUN Microsystems, Inc.; Fasano, P.; Guardini, I.; CSELT S.p.A.; Lento, D.; TIM;, Enero 2001. [Online]. Available: http://www.rfc-editor.org/rfc/rfc3053.txt.

[32] R. Despres, "Rfc 5569," Enero 2010. [Online]. Available: http://tools.ietf.org/html/rfc5569. [Accessed 21 Enero 2014].

[33] M. Townley and O. Troan, "RFC 5969," Agosto 2010. [Online]. Available: https://tools.ietf.org/html/rfc5969. [Accessed 22 Enero 2014].

[34] Chengdu SKSpruce Technology, Inc, "SKSPRUCE," 2012. [Online]. Available: http://www.skspruce.com/Article96/108.html. [Accessed 22 Enero 2013].

[35] Nordmark, E.; Sun Microsystems;, Febrero 2000. [Online]. Available: http://tools.ietf.org/html/rfc2765.

[36] Li, X.; Bao, C.; CERNET Center/Tsinghua University; Baker, F.; Cisco Systems;, Abril 2011. [Online]. Available: http://tools.ietf.org/html/rfc6145.

[37] Aoun, C.; Energize Urnet; Davies, E.; Folly Consulting;, Julio 2007. [Online]. Available: http://tools.ietf.org/html/rfc4966.

[38] Huang, B.; Deng, H.; China Mobile; Savolainen, T.; Nokia;, Febrero 2012. [Online]. Available: http://tools.ietf.org/html/rfc6535.

[39] Hagino, J.; Yamamoto, K.; IIJ Research Laboratory;, Junio 2001. [Online]. Available: http://tools.ietf.org/html/rfc3142.

[40] Ayuda-Internet.net, "Test Velocidad," [Online]. Available: http://www.test-velocidad.net/adsl.php. [Accessed 10 Marzo 2014].

[41] T. Michell, "Investtavitatelecomunicaciones," 29 Marzo 2009. [Online]. Available: http://investtavitatelecomunicaciones.blogspot.com/2009/03/que-es-dsl-o-adsl.html. [Accessed 10 Marzo 2014].

[42] Rosen, E.; Cisco Systems, Inc.; Viswanathan, A.; Force10 Networks, Inc.; Callon, R.; Juniper Networks, Inc.;, Enero 2001. [Online]. Available: http://tools.ietf.org/html/rfc3031.

[43] Cisco Systems, Inc.;, Septiembre 2008. [Online]. Available: http://www.cisco.com/image/gif/paws/4649/mpls_faq_4649.pdf.

[44] J. De Clercq, D. Ooms, S. Prevost and F. Le Faucheur, "RFC 4798," Febrero 2007. [Online]. Available: http://tools.ietf.org/html/rfc4798. [Accessed 23 Enero 2014].

[45] Multi-Service IronWare, "6PE over MPLS," [Online]. Available: http://www.brocade.com/downloads/documents/html_product_manuals/NI_05500c_MPLS/wwhelp/wwhimpl/common/html/wwhelp.htm#context=MPLS_Guide&file=6PE.11.2.html. [Accessed 23 Enero 2014].

[46] Multi-Service IronWare, "6VPE Routing," [Online]. Available: http://www.brocade.com/downloads/documents/html_product_manuals/NI_05500c_MPLS/wwhelp/wwhimpl/common/html/wwhelp.htm#context=MPLS_Guide&file=6PE.11.7.html. [Accessed 23 Enero 2014].

[47] U.P.E.L, Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales, Caracas: FEDUPEL, 2003.

[48] D. Rodriguez, Estrategias Exitosas para la Investigación, Maracay : Aragua: La Liebre Libre, 2007.

[49] Latin American and Caribbean Internet Addresses Registry, [Online]. Available: http://www.lacnic.net/web/lacnic/ipv6-isp.

[50] Latin American and Caribbean Internet Addresses Registry, Julio 2013. [Online]. Available: http://www.lacnic.net/web/lacnic/manual-4.

[51] G. Fernández-Trujillo and L. E. Rojas Galindo, *Estudio sobre la Red de la Empresa NETUNO para la Implementación de IPv6 en su Plataforma de Multiservicio para el Segundo Semestre de 2011,* Caracas: Tesis.Escuela de Ingeniería en Telecomunicaciones.Ingeniería.Universidad Católica Andrés

Bello, 2011.

[52] LACNIC, "Portal IPv6," [Online]. Available: http://portalipv6.lacnic.net/quienes-implementan/. [Accessed 3 Enero 2014].

[53] D. García Vargas, *Diseño de una estrategia de migración de la red actual de la Universidad Católica Andrés Bello a una red basada en IPv6,* Caracas: Tesis.Escuela de Ingeniería en Telecomunicaciones.Ingeniería.Universidad Católica Andrés Bello, 2011.

[54] Cisco, "Cisco," 8 Abril 2013. [Online]. Available: http://www.cisco.com/c/en/us/td/docs/ios/15_1s/release/notes/15_1s_rel_notes.pdf. [Accessed 15 Marzo 2014].

Acrónimos

6PE: *IPv6 Provider Edge Routers*.

6rd: *IPv6 Rapid Deployment.*

6VPE: *IPv6 VPN Provider Edge Routers.*

ABA: *Acceso a Banda Ancha.*

ABRs: *Area Border Routers*.

ADSL: *Asymmetric Digital Subscriber Line*.

API: *Application Programming Interface.*

ARP: *Address Resolution Protocol.*

AS: *Autonomous System*

ASBRs: *Autonomous System Border Routers*

BDR: *Backup Designated Router*.

BGP4: *Border Gateway Protocol 4*.

BIH: *Bump-in-the-Host.*

BRAS: *Broadband Remote Access Server*.

CANTV: Compañía Anónima Nacional de Teléfonos de Venezuela.

CIDR: *Classless Inter-Domain Routing*.

CLNS: *Connectionless Network Service*.

CoS: *Class of Service.*

CPE: *Customer Premises Equipment.*

DDNS: *Dynamic Domain Name System.*

DHCPv6: *Dynamic Host Configuration Protocol for IPv6.*

DNS: *Domain Naming System.*

DR: *Designated Router*

DSLAM: *Digital Subscriber Line Access Multiplexer.*

Edge – LSR: *Edge Label Switching Router.*

ENR: *Extension Name Resolver.*

FEC: *Forwarding Equivalence Class.*

FP: *Format Prefix.*

IANA: *Internet Assigned Numbers Authority.*

ICMP: *Internet Control MessagesProtocol*.

IETF: *The Internet Engineering Task Force.*

IGMP: *Internet Group Management Protocol*.

IPv4: *Internet Protocol version* 4.

IPv6: *Internet Protocol version* 6.

ISATAP: *Intra-Site Automatic Tunnel Addressing Protocol.*

IS-IS: *Intermediate System to Intermediate System*

ISP: *Internet Service Provider*.

LACNIC: *Latin America & Caribbean Network Information Centre.*

LAN: *Local Area Network.*

LSAs: *Link State Advertisements*.

LSR: *Label Swtich Router*.

MLD: *MulticastListenerDiscovery*.

MP-BGP: *Multiprotocol Border Gateway Protocol* .

MPLS: *Multiprotocol Label Switching*.

NAT: *Network Address Translation.*

NAT-PT: *Network Address Translation-Protocol Translation.*

NGN: *Next Generation Networking*.

NGtrans: *Next Generation Transition Working Group*.

NSP: *Network Service Provider*.

OSPFv3: *Open Shortest Path First Version 3.*

OUI: *Organizationally unique identifier.*

QoS: *Quality of Service*.

RIPng: *Routing Information Protocol New Generation.*

RIR: *Regional Internet Registry*.

SIIT: *Stateless IP/ICMP Translation algorithm.*

TLA: *Top Level Aggregator.*

TRT: *Transport Relay Translator*.

UDP: *User Datagram Protocol.*

VoIP: Voz sobre IP.

WAN: *Wide Area Network.*

Apéndices

Apéndice A.

Entrevista y Resultados.

En esta entrevista se realizaron las siguientes preguntas:

1. Según su opinión ¿Cuál de los métodos de transición a IPv6 son los más utilizados actualmente?
2. ¿Tiene conocimiento de la utilización de estos métodos en algunos ISPs?
3. Diferentes fuentes debaten acerca de la longitud de prefijo que un ISP debería otorgar a sus usuarios finales, debiendo éste ser siempre igual o menor a /64 pero no menor de /48. ¿Considera usted necesaria la asignación de un prefijo menor a /64 a un usuario residencial venezolano promedio? ¿Por qué?
4. ¿Es factible entregar por defecto /64 y máscaras menores sólo bajo pedido de un usuario específico?
5. De acuerdo a lo comentado en la pregunta anterior. ¿Considera usted necesaria la asignación de un prefijo menor a /64 a un usuario empresarial venezolano promedio? ¿Por qué?
6. ¿Tiene conocimiento de la longitud de prefijo más utilizada actualmente por los ISP a nivel mundial?
7. ¿Cuál es la mejor manera de distribuir los prefijos de un ISP a sus diferentes tipos de usuarios (domésticos, empresariales)?

Los resultados de la entrevista se presentan sin especificar cuál fue la respuesta de cada profesional, se plantean la respuesta de sujetos sin tomar en cuenta algún orden en específico.

Sujeto	1	2
Pregunta 1	La mayoría utiliza *Dual Stack*	Túnel 6rd
Pregunta 2	Telefónica y Operadoras en Latinoamérica	Empresas en Francia
Pregunta 3	No, Es más conveniente entregar un /64, ya que con esa cantidad de direcciones están cubiertas las necesidades del cliente, además que la velocidad máxima otorgada en Venezuela es de 10 Mbps y no hay capacidad física para aumentar el Ancho de Banda.	No, un /64 y sin embargo me parece mucho.
Pregunta 4	Si	Si
Pregunta 5	Si lo requiere si	Si
Pregunta 6	/48	No
Pregunta 7	Hay que analizarlos para verificar los costos y seguridad, no podría recomendarte ninguna.	Pueden ser las dos

Tabla 18: Resultados de Entrevista (1).

Fuente: Los Autores.

Sujeto	3	4
Pregunta 1	Túnel 6rd	Métodos de Traducción
Pregunta 2	No que yo sepa	En particular con este método no sabría decirte
Pregunta 3	No lo se	Yo pienso que se deberían entregar menos direcciones a un usuario.
Pregunta 4	No lo se	Si

Sujeto	**3**	**4**
Pregunta 5	No lo se	Si
Pregunta 6	No, ya que no he escuchado que lo estén utilizando mucho	No en específico, pero creo que un /64
Pregunta 7	No sabría decirte	Autoconfiguración es muy bueno, pero recomendaría mantener DHCP

Tabla 19: Resultados de Entrevista (2).

Fuente: Los Autores.

Sujeto	**5**	**6**
Pregunta 1	Túnel 6to4	*Dual Stack*
Pregunta 2	Si en Maroc Telecom (Marruecos)	Si Movistar
Pregunta 3	No, porque ya /64 nos da de por sí muchas direcciones IP.	No, porque ya es suficiente la cantidad de direcciones.
Pregunta 4	Si	Si
Pregunta 5	A uno promedio No, pero si a empresas grandes.	Si
Pregunta 6	Si, /64	Si, /64
Pregunta 7	DHCPv6	DHCPv6

Tabla 20: Resultados de Entrevista (3).

Fuente: Los Autores.

Sujeto	**7**
Pregunta 1	*Dual Stack*
Pregunta 2	Si, Movistar Perú
Pregunta 3	Si un barra 56 es el estándar utilizado actualmente.

Sujeto	7
Pregunta 4	Si
Pregunta 5	Si, es el estándar utilizado actualmente para las empresas.
Pregunta 6	/56 residencial y /48 corporativa
Pregunta 7	DHCPv6

Tabla 21: Resultados de Entrevista (4).

Fuente: Los Autores.

A continuación se presentan los resultados de las entrevista de manera gráfica (circular) para un cómodo análisis de los mismos.

1. Según su opinión ¿Cuál de los métodos de transición a IPv6 son los más utilizados actualmente?

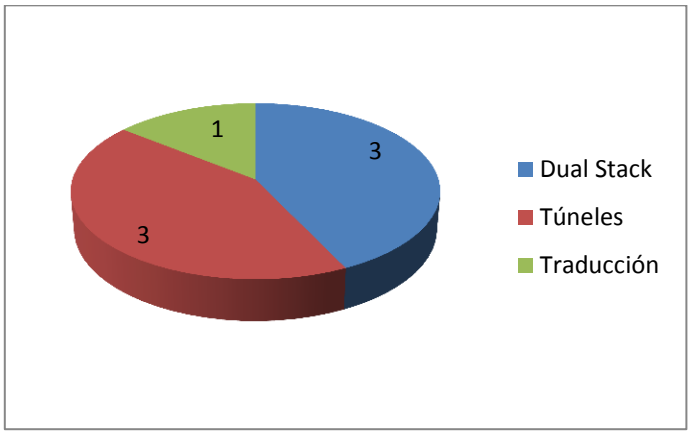

Figura 67: Gráfica pregunta uno (1).

Fuente: Los Autores.

2. ¿Tiene conocimiento de la utilización de estos métodos en algunos ISPs?

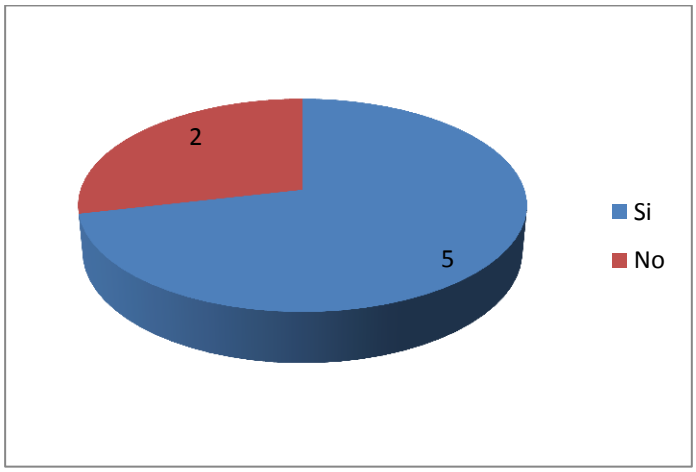

Figura 68: Gráfica pregunta dos (2).

Fuente: Los Autores.

3. Diferentes fuentes debaten acerca de la longitud de prefijo que un ISP debería otorgar a sus usuarios finales, debiendo éste ser siempre igual o menor a /64 pero no menor de /48. ¿Considera usted necesaria la asignación de un prefijo menor a /64 a un usuario residencial venezolano promedio? ¿Por qué?

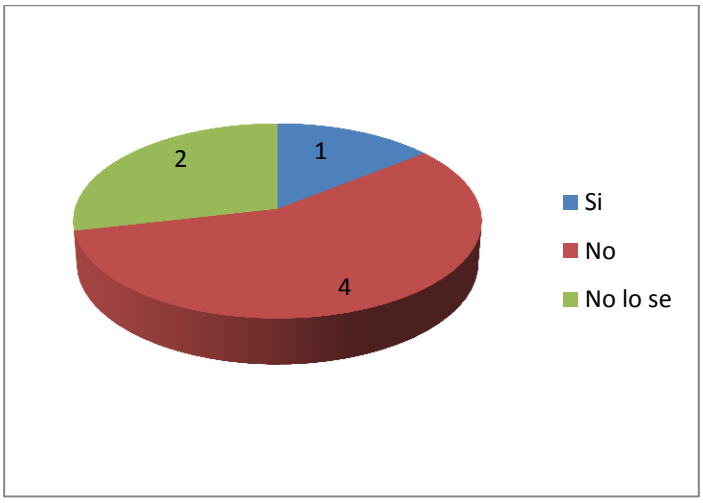

Figura 69: Gráfica pregunta tres (3).

Fuente: Los Autores.

4. ¿Es factible entregar por defecto /64 y máscaras menores sólo bajo pedido de un usuario específico?

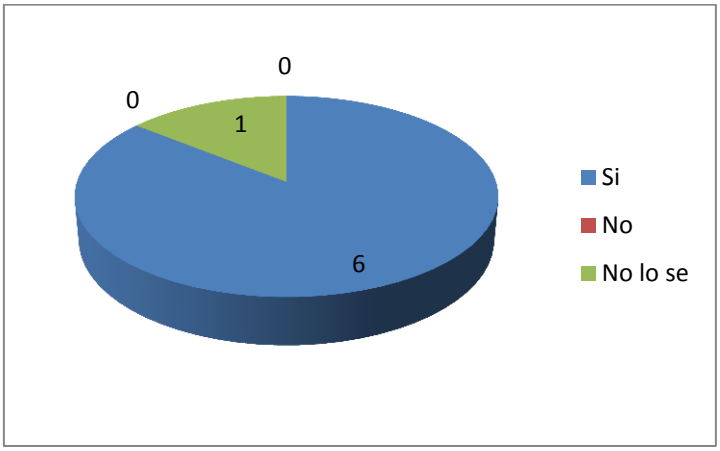

Figura 70: Gráfica pregunta cuatro (4).

Fuente: Los Autores.

5. De acuerdo a lo comentado en la pregunta anterior. ¿Considera usted necesaria la asignación de un prefijo menor a /64 a un usuario empresarial venezolano promedio? ¿Por qué?

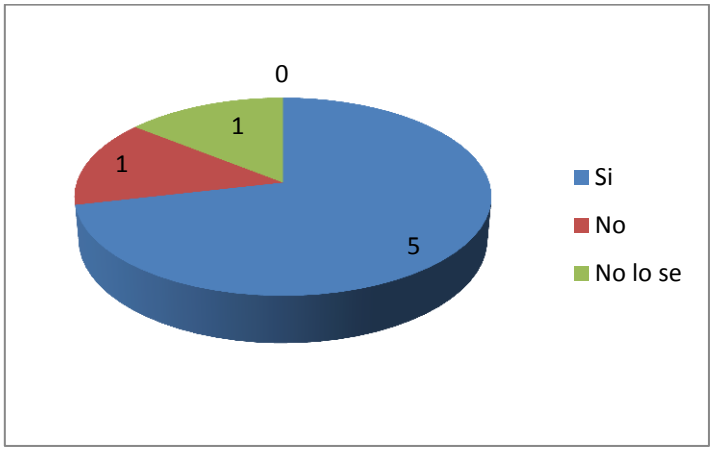

Figura 71: Gráfica pregunta cinco (5).

Fuente: Los Autores.

6. ¿Tiene conocimiento de la longitud de prefijo más utilizada actualmente por los ISP a nivel mundial?

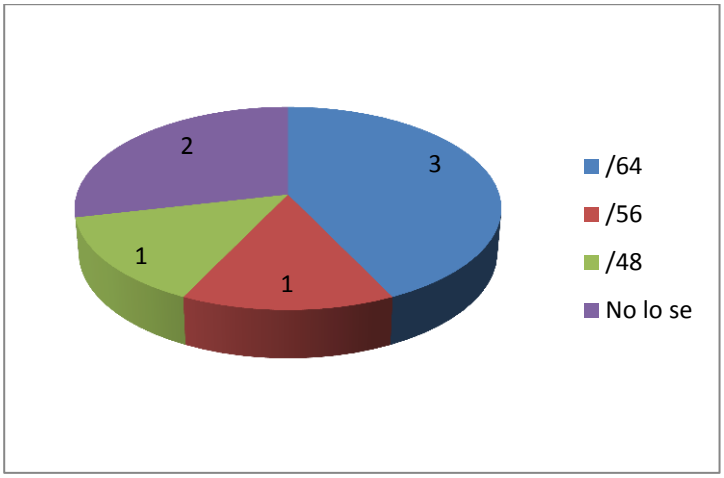

Figura 72: Gráfica pregunta seis (6).

Fuente: Los Autores.

7. ¿Cuál es la mejor manera de distribuir los prefijos de un ISP a sus diferentes tipos de usuarios (domésticos, empresariales)?

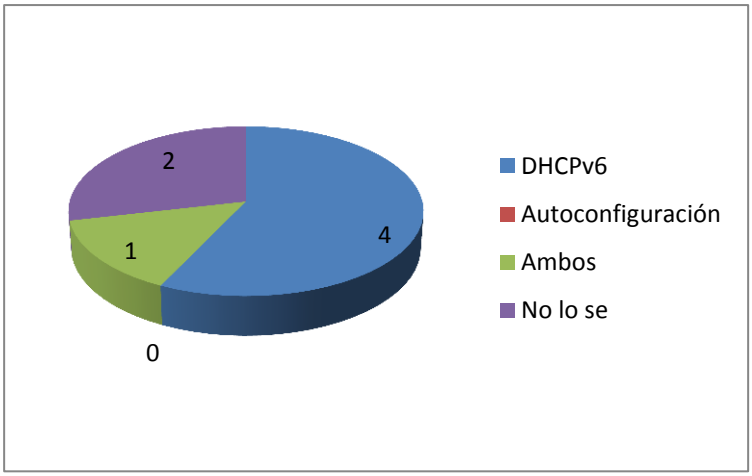

Figura 73: Gráfica pregunta siete (7).

Fuente: Los Autores.

Apéndice B.

Imágenes de los equipos.

CPE Huawei HG532e.

Figura 74: Modem Huawei HG532e.

Fuente: Los Autores.

CPE ZTE ZXHNH108L

Figura 75: Modem ZTE XHNH108L.

Fuente: Los Autores.

DSLAM Huawei MA5600.

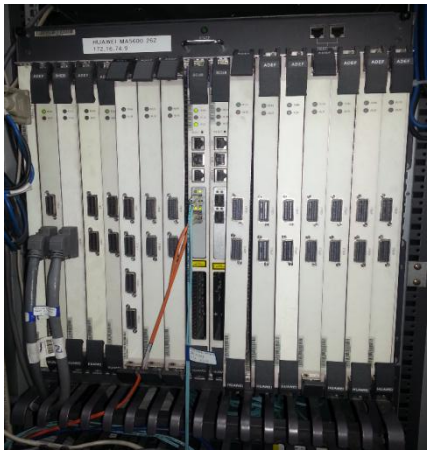

Figura 76: DSLAM Huawei MA5600.

Fuente: Los Autores.

***Switch* Metro Ethernet 7450 ESS-7.**

Figura 77: *Switch* Alcatel-Lucent 7450 ESS-7.

Fuente: Los Autores.

Agregador Huawei ME60-x8.

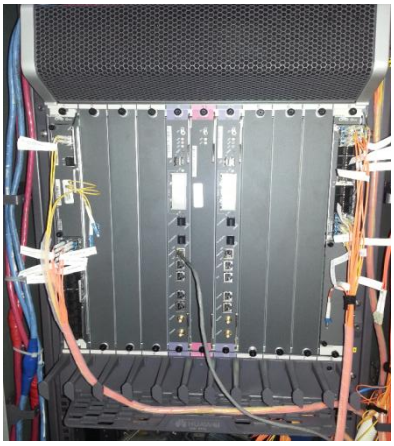

Figura 78: BRAS Huawei ME60-x8.

Fuente: Los Autores.

***Router* Cisco 7200.**

Figura 79: *Router* Cisco 7200.

Fuente: Los Autores.

***Router* Cisco 7609.**

Figura 80: *Router* Cisco 7609.

Fuente: Los Autores.

Servidor.

Figura 81: Servidor DHCPv6 y DNS.

Fuente: Los Autores.

Apéndice C.

Diagrama de Red Troncal 2010 - 2012.

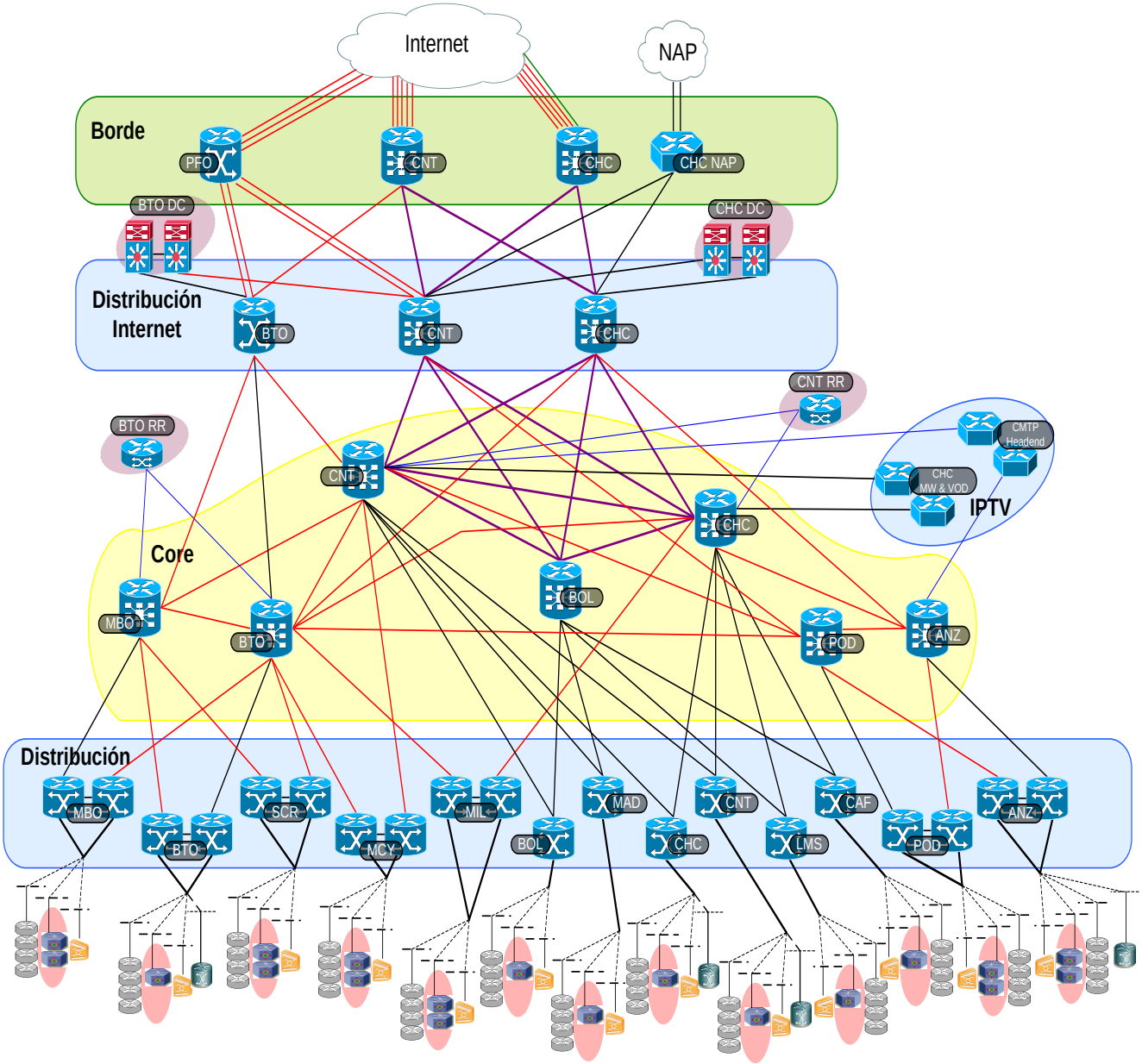

Figura 82: Diagrama de Red Troncal 2010 – 2012.

Fuente: Los Autores.

Apéndice D.

Tabla de Costos.

Tipo de Modem	Costo ($)	Clientes Totales Aprox.	Total
Básico (1 puerto)	20$	2.280.000	45.600.000 $
Básico con WiFi	32$		72.960.000 $
4 puertos con WiFi	40$		91.200.000 $

Tabla 22: Tabla de Costos.

Fuente: Los Autores.