UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"ADECUACIÓN DE LA RED DE ISP PARA SOPORTE A IPv6"

INORME DE TRABAJO PROFESIONAL
QUE PARA OBTENER EL TÍTULO DE
INGENIERO EN TELECOMUNICACIONES

PRESENTA:
JUAN CARLOS ARROYO CASTRO

DIRECTOR DE TRABAJO PROFESIONAL:
ING. JESÚS REYES GARCÍA

CIUDAD UNIVERSITARIA **2014**

AGRADECIMIENTOS

Primero que nada quiero agradecer a Dios por darme vida y salud para compartir cada momento hasta el día de hoy con mis seres queridos, por permitirme tener la guía de mis padres por muchos años más y darle mucha salud, bienestar y paz a toda mi familia.

A mis padres, Javier Arroyo Aguilar y Yolanda Castro de Arroyo, por haberme dado la vida y por su apoyo incondicional en todo momento, por haberme ayudado en todos los proyectos que he tenido en mente y hacer todo lo que está en sus manos para que los haya visto realizados. Gracias por darnos educación y sacarnos adelante, tanto a mis dos hermanos como a mí, siempre esforzándose muchísimo y en algunas ocasiones privándose de cosas con tal de que nosotros pudiéramos tener lo necesario para salir adelante. Por eso les dedico este trabajo y quiero hacerlos partícipes de este éxito para que puedan darse cuenta de lo bien que lo hacen y estén orgullosos de haber forjado a personas de bien, trabajadoras y con ganas de seguir saliendo adelante como un reflejo de lo que ellos han venido haciendo todo este tiempo con nosotros. Gracias mamá, por siempre levantarte temprano y seguirlo haciendo para prepararnos nuestro desayuno, por todo el trabajo que haces en casa para tener nuestro hogar agradable y bonito para cuando regresamos de trabajar. Gracias papá, por todo lo que has tenido que trabajar a lo largo de los años para llevar la comida a casa y por el enorme esfuerzo que has realizado para lograr estar donde estamos ahorita.

A mis hermanos Javier y Jonatan, por su cariño y apoyo incondicional, por todas las experiencias que hemos compartido al crecer juntos y que nos han unido sólidamente como familia. Gracias por todas esas alegrías durante nuestra infancia y por el respeto mutuo que nos brindamos a pesar de las posibles diferencias que a veces pueden surgir, pero que sabemos superar de buena manera.

A mis amigos, compañeros inolvidables de la prepa y de la Facultad con quienes pasé gran parte del tiempo diario, y con quienes compartí experiencias inolvidables que nos fueron formando como personas.

A mis compañeros y amigos de trabajo, con quienes me relaciono y compartimos vivencias en las actividades laborales diarias y con quienes me ha tocado platicar, cocinar proyectos nuevos, apoyar proyectos existentes y promover el trabajo en equipo.

A mi Universidad Nacional Autónoma de México, por la oportunidad inigualable de formar parte de su comunidad y darme una excelente formación académica y de nivel, a la altura de cualquier otra universidad en el mundo, para un exitoso desarrollo profesional.

A todos mis profesores, por sus enseñanzas tan valiosas durante mi formación. Al Ing. Jesús Reyes García por su paciencia, apoyo y por la confianza que depositó en mí para conseguir este logro.

A mi jefe, el Ing. Javier Ortiz Villaseñor, por ser una persona admirable y darme la oportunidad de formar parte de su equipo de trabajo, motivarme a estudiar continuamente para adquirir nuevos conocimientos, y con ello tener un mejor nivel profesional. Por transmitirme sus conocimientos en las actividades propias del trabajo en la empresa y apoyarme en el proceso de obtención de nuevas certificaciones, así como en la culminación de este proyecto.

Agradezco a Magali Sánchez, por quererme tanto y apoyarme en todo momento, por estar conmigo, brindarme su apoyo y darme ánimos siempre. Te quiero mucho y te llevo en el corazón.

ÍNDICE

RESUMEN

Mi nombre es Juan Carlos Arroyo Castro y actualmente me encuentro laborando en la empresa *Consorcio Red Uno S.A. de C.V.* a la cual ingresé en el mes de julio del 2005 y en estos momentos tengo el cargo de *Ingeniero de Soporte Técnico Reactivo* en la *Gerencia de Soporte Técnico Reactivo* perteneciente a la *Subdirección de Operación de Red de Datos.* A lo largo de mi estancia en la empresa he participado en la implementación de nuevas tecnologías para el crecimiento de la infraestructura de la red de datos, y recientemente me encuentro trabajando en la resolución de problemas brindando soporte técnico de segundo nivel y entregando diagnósticos de causa raíz realizando tareas propias de investigación y análisis. El apoyo tanto en herramientas de monitoreo desarrolladas por terceros como en herramientas desarrolladas internamente y que han sido personalizadas para la operación diaria de los equipos es primordial para lograr dichos objetivos.

Para la eliminación de fallas recurrentes, lo que se busca es encontrar la causa raíz del incidente apoyándose en documentación de estándares internacionales, información técnica emitida por el proveedor de los equipos instalados, revisión de bitácoras almacenadas en los mismos equipos, para establecer líneas de tiempo de ocurrencia de los eventos en busca de una correlación de los mismos.

Durante este tiempo he participado activamente en el desarrollo de varios proyectos íntegramente relacionados con el campo de la Ingeniería en Telecomunicaciones. El proyecto más reciente y que aún se mantiene en progreso es el tema central de este trabajo profesional cuya finalidad es la adecuación de la infraestructura del *backbone* de la red de proveedor de servicios de Internet (*ISP* [1]) en México, para la adopción del protocolo IPv6 por la tendencia mundial de habilitar dicho protocolo para subsanar las limitantes impuestas por el mismo protocolo en su versión 4. Así como para solventar el demandante crecimiento de las redes de datos para la comunicación de toda la gama de dispositivos móviles que se han desarrollado, habilitándonos una comunicación confiable en todo momento sobre todas las aplicaciones que tenemos disponibles hoy en día.

[1] ***El glosario de acrónimos se muestra en la página 86***

Dentro de las necesidades que demanda el proyecto se consideran los elementos teóricos en el diseño y operación de redes de datos poniendo a prueba los conocimientos y facultades desarrolladas durante mi formación profesional, al aprender sobre el área en cuestión. Así como analizando propuestas para la resolución de problemas y la implementación de las soluciones debidas.

Algunas de las funciones que he desempeñado durante mi estancia en la empresa son:

- Recepción de infraestructura nueva para el crecimiento de la red: equipos, tarjetas, enlaces de infraestructura, troncales digitales, interconexiones
- Migración de equipos, enlaces e interconexiones bajo ventana de mantenimiento
- Reingeniería de nodos para modificar su topología o reasignar direccionamiento
- Participación en pruebas piloto para la integración de nuevas plataformas a la red
- Implementación de configuraciones avanzadas para la puesta en marcha de nuevas funcionalidades
- Soporte de segundo nivel para la resolución de incidentes de manera oportuna y diagnóstico de causas raíz para la mitigación de riesgo en toda la red

Como parte del plan de entrenamiento ofrecido por la empresa, he recibido capacitación en los siguientes rubros:

- Configuración de routers marca Cisco de diferentes modelos
- Configuración de routers marca Juniper de diferentes modelos
- Protocolos de ruteo: OSPF, BGP, LDP, QoS
- ITIL Foundations v3, RCV y OSA
- Fundamentos, diseño e implementación de IPv6
- ISO/IEC 20000 , ISO/IEC 27001

Las certificaciones reconocidas en la industria con las que cuento actualmente son:

- Cisco: CCNA, CCNP R&S
- Juniper: JNCIA-Junos, JNCIS-SP

LISTA DE FIGURAS Y TABLAS

OBJETIVO

Mostrar la manera en la que opera el protocolo IPv6 orientado hacia una red de Proveedor de Servicios de Internet, analizando e implementando de manera planeada una opción de transición confiable y segura, dentro de un ambiente controlado, evitando afectación al servicio de los usuarios finales.

CAPÍTULO 1

DESCRIPCIÓN DE LA EMPRESA

1.1 Antecedentes

En la actualidad las Telecomunicaciones han tomado un rol importante en nuestras vidas, facilitando el estilo de vida de todos los individuos alrededor del mundo ya que permite que la información que se genera día con día pueda ser comunicada de manera rápida y efectiva, haciéndola fluir por los distintos medios que conocemos: radio, televisión, microondas, telefonía, redes de datos, entre otros. Las redes de datos siguen cobrando relevancia gracias al Internet, con lo cual podemos comunicarnos desde cualquier computadora o dispositivo móvil a cualquier otro dispositivo en cualquier parte del mundo.

La empresa para la cual trabajo es un Proveedor de Servicios de Internet que abarca todo el territorio nacional, Estados Unidos y parte de Latinoamérica ofreciendo servicios de Internet para poder comunicar a los sitios centrales de corporativos con sus sitios remotos localizados estratégicamente, de manera geográfica, asegurando cobertura con base en las necesidades de cada cliente en particular.

El nicho de mercado que abarca la empresa es el tema central de este informe, y en el cual plasmo las tareas necesarias para poder habilitar el protocolo IP en su versión 6 dentro de la red de Proveedor de Servicios de Internet.

Primeramente se hará una breve descripción de la empresa en la que se desarrolla el proyecto en cuestión:

1.2 Descripción de la empresa

Red Uno es una empresa 100% mexicana, líder en el mercado nacional de las telecomunicaciones. Dedicada al diseño e integración de soluciones corporativas de comunicación de voz, datos, video y servicios administrados. Fundada el 20 de marzo de 1991, ya cuenta con más de 20 años de encontrarse en el sector de las Telecomunicaciones repuntando en cuestión de nuevas tecnologías, incluyendo las TICs. En el año de 1994 formó una alianza estratégica con Telmex, Grupo Carso, SBC International (Southwestern Bell) y France Telecom. En 1995 se le reconoce como *Cisco Gold Partner.*

Misión

"Ser un grupo líder en telecomunicaciones, proporcionando a nuestros clientes soluciones integrales de gran valor, innovadoras y de clase mundial, a través del desarrollo humano, y de la aplicación y administración de tecnología de punta"

Visión

"Consolidar el liderazgo de Consorcio Red Uno en el mercado nacional, expandiendo su penetración de servicios de Telecomunicaciones en todos los mercados posibles, para ubicarnos como una de las empresas de más rápido y mejor crecimiento a nivel mundial"

Son cuatro los valores de la Cultura Corporativa de la empresa:

1. Trabajo
2. Crecimiento
3. Responsabilidad social
4. Austeridad

La empresa orienta todas sus actividades hacia el cumplimiento de los principios de:

1. Servicio al cliente
2. Calidad
3. Vanguardia tecnológica

Para dar una idea clara del giro de la empresa se mencionan a continuación los servicios que se ofrecen a los clientes, así como también algunos proyectos relevantes que se han desarrollado hasta el momento.

Servicios ofrecidos:

- Dialup
- Voz (tradicional / IP)
- LAN, WAN, Videoconferencia
- Frame Relay (obsoleto)
- RPV (Red Privada Virtual)
- IDE (Internet Directo Empresarial)
- Infinitum (internet masivo) y Wi-Fi Móvil (infraestructura inalámbrica)
- Web Hosting (hospedaje de información)
- Caching
- Servicios de Valor Agregado (mesas de ayuda, outsourcing, mantenimiento)

Proyectos implementados por la empresa, en los que tuve participación:

- Migración de los equipos de *Backbone* a la plataforma *CRS,* la cual se basa en el sistema operativo IOS-XR y ofrece entre otras cosas alto desempeño, inteligencia avanzada de servicios, alta disponibilidad y soporte a protocolos de última generación
- Instalación de equipos con funcionalidad de *Route Reflectors* (reflectores de rutas de BGP, RR) a lo largo del territorio nacional como parte de la adecuación de la red para el soporte al protocolo IPv6
- Habilitación de sesiones de BGP hacia proveedores internacionales para permitir el soporte al tráfico IPv6 hacia sitios a nivel mundial
- Puesta en marcha de los eventos “Aldea Digital” y “Telmex Hub” que han tenido sus sedes en varios estados a lo largo de la república mexicana

CAPÍTULO 2

ANTECEDENTES DEL TEMA

La importancia de las redes de datos en nuestra vida diaria va tomando mayor relevancia día con día, y más aún con la llegada de la versión 6 del protocolo IP. Para esto, se requiere realizar una serie de modificaciones tanto en la infraestructura como en las aplicaciones actuales que se encuentran corriendo en IPv4, para poderlo habilitar de una manera gradual y transparente sin que esto implique afectación considerable a los servicios que operan actualmente. En los siguientes capítulos se describirá la manera de abordar esta integración, comenzando por describir un marco teórico que servirá como base para el buen entendimiento del problema planteado. Avanzando con la manera en la que se abordó esta nueva implementación en la empresa donde laboro; describiendo mi participación y aportaciones para cumplir con el objetivo propuesto.

A lo largo de este capítulo, se detallarán conceptos clave del protocolo IPv6. Partiendo de los fundamentos, más adelante se explican aspectos de arquitectura de las direcciones usadas, para posteriormente describir los mecanismos de transición que pueden emplearse para habilitar IPv6 en una red de datos considerando necesidades y recursos planeados.

A continuación se desarrollan los conceptos teóricos a usarse para la adecuación de la red de ISP para soporte a IPv6:

2.1 Fundamentos de IPv6

La estandarización del protocolo de Internet (IP), en su versión 4, se remonta al año de 1981 como resultado de toda una serie de estudios e investigaciones realizadas por el departamento de defensa de los Estados Unidos (DARPA). Su finalidad fue diseñar una red que se esperaba fuera de acceso restringido a unos cuantos miles de usuarios, en su mayoría científicos del gobierno y del ámbito académico.

Conforme se da la explosión del Internet en los años 90´s, muchos requerimientos se hicieron necesarios para el masivo crecimiento que se fue dando y la adopción a gran escala de redes de computadoras y la interconexión entre dichas redes (*internetworking*) en un ambiente empresarial. Actualmente el protocolo IPv4 da soporte a redes alrededor del mundo incluyendo negocios, redes sociales y dependencias de gobierno. Lo anterior hizo necesario el desarrollo de mecanismos para brindar a las comunicaciones de los usuarios aspectos de seguridad, calidad de servicio, movilidad, entre otras cosas.

Tres décadas de uso del protocolo IPv4 permitieron identificar diversas áreas de oportunidad para su mejora, disparando entre los organismos de estandarización el proceso de diseño de un protocolo capaz de subsanar las limitantes (primordialmente en el aspecto del agotamiento pronosticado de las direcciones IP disponibles).

Analizando la situación, se realiza el consenso determinándose que había tiempo suficiente para desarrollar un protocolo completamente nuevo, diseñado desde cero, con funcionalidades adicionales; en vez de implementar uno que únicamente proporcionara un mayor espacio de direccionamiento, otorgando no solamente una solución a mediano plazo, sino también a largo plazo.

En el año de 1993 se comienzan con dichos esfuerzos colectando requerimientos de los diversos involucrados en la industria: negocios pequeños, corporativos, gobierno, fabricantes de dispositivos, desarrolladores de aplicaciones y proveedores de servicios de Internet (ISP).

2.1.1 Limitantes de IPv4

La versión actual del protocolo IP no ha cambiado sustancialmente desde el RFC 791 *(Internet Protocol / Author: J. Postel / Date: September 1981),* publicado en el año de 1981. IPv4 ha probado ser robusto, de fácil implementación e interoperable. Sin embargo una de las mayores deficiencias de IPv4 es su limitado espacio de direccionamiento. La explosión de nuevos dispositivos habilitados para realizar conexiones usando el protocolo IP, así como el tamaño de la comunidad de Internet principalmente en regiones de Europa, Japón y Asia-Pacífico, han ido acelerando el agotamiento de las direcciones que se pueden asignar en IPv4.

Otra limitante del protocolo actual fueron los requerimientos de las aplicaciones extremo a extremo (*P2P*), las cuales se habían vuelto muy populares y era complejo soportarlas con técnicas de traducción de direcciones como NAT/PAT ya que inhibe la seguridad *end-to-end* e incrementa la complejidad de la administración de la red.

Dado el crecimiento acelerado de Internet se requirió trabajar sobre una nueva versión del protocolo IP ya existente, puesto que se identificó que se requería de mucho análisis y tiempo para crear un estándar de direccionamiento completamente nuevo para cumplir con los objetivos que se tenían planteados. Entonces se optó por la adopción de IPv6.

2.1.2 Soluciones temporales al agotamiento de direcciones IPv4

Varios métodos para extender el tiempo de vida y la utilidad de IPv4 fueron implementados rápidamente para cubrir las necesidades inmediatas:

- **CIDR (Classless Inter-Domain Routing):** Se publica en 1993 y soporta dos funcionalidades primordiales que benefician a la tabla global de rutas de Internet: rompe con el esquema rígido e ineficiente de los bloques de longitud fija, comúnmente referidos como “clases” y soporta la sumarización de rutas con el concepto de “Supernetting”, el cual consiste en representar múltiples segmentos de red con un segmento de mayor tamaño o *supernet* permitiendo la reducción del tamaño de la tabla de Internet, así como el uso más eficiente de los dispositivos que manipulan dicha tabla.

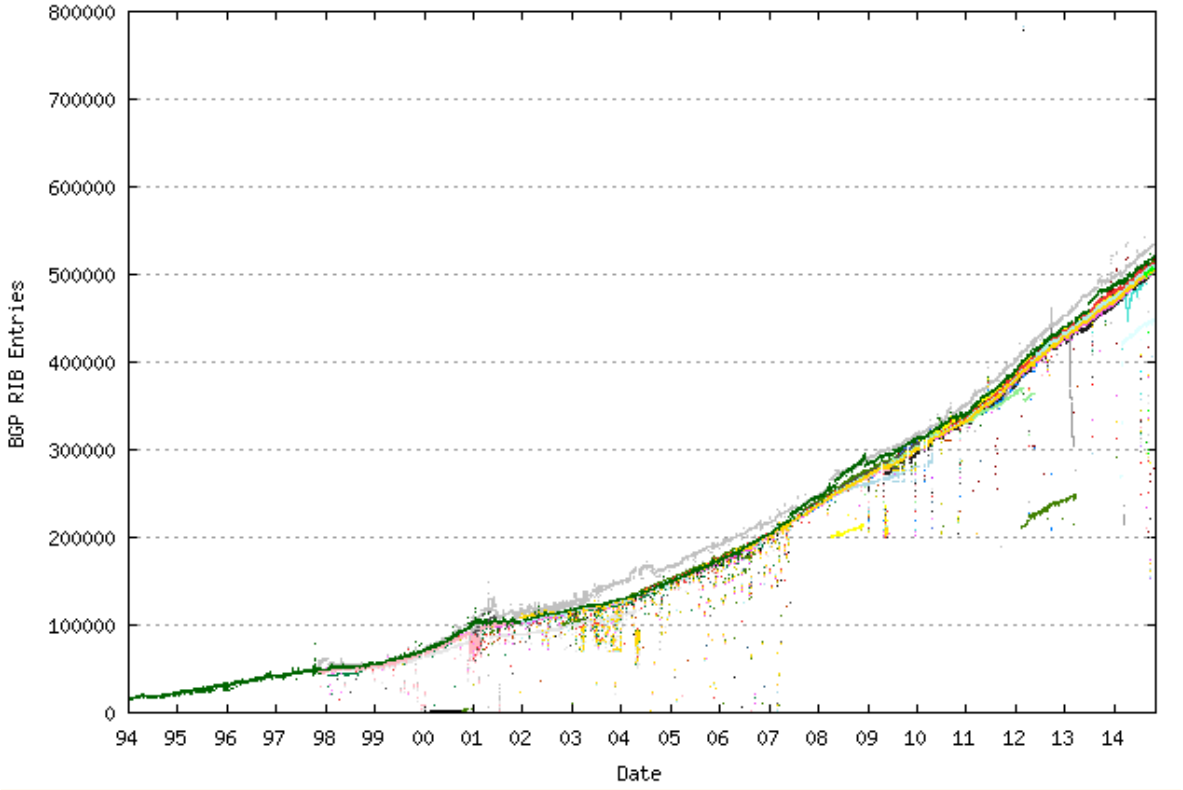

Figura 1. Crecimiento constante de la tabla de Internet
[BGP Routing Table Analysis Reports; Growth of the BGP Table - 1994 to Present; Disponible en: http://bgp.potaroo.net/]

- **VLSM (Variable Length subset Masking):** Permite el uso más eficiente de las direcciones IPv4, específicamente en segmentos pequeños como los son los enlaces seriales punto a punto. Al igual que CIDR, rompe con el esquema de clases permitiendo generar subredes de máscara de longitud variable que caen dentro de una misma red clase A, B o C.

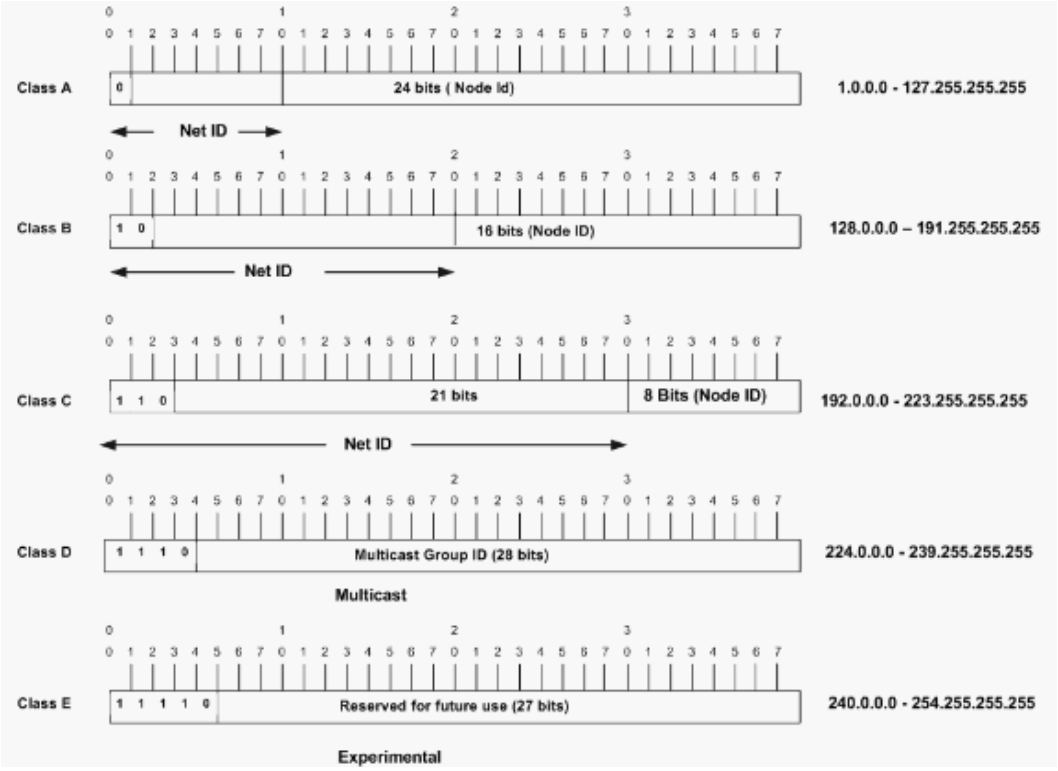

Figura 2. Esquema de clases de direcciones IPv4

[White Paper - Understanding IP Addressing:Everything You Ever Wanted To Know; 2001; 3Com; Disponible en: http://www.apnic.net/services/services-apnic-provides/helpdesk/faqs/obtaining-resources-faqs/3com]

- **NAT (Network Address Translation):** Introduce un modelo en el cual un dispositivo con interfaz hacia Internet pueda tener una o múltiples direcciones IPv4 (homologadas o públicas) ruteables globalmente, mientras que su red interna la pueda tener configurada con direccionamiento privado. Estas direcciones nunca pueden anunciarse a Internet por lo que pueden ser idénticas en múltiples redes corporativas evitando así el uso de direcciones homologadas. Los segmentos privados asignados para cada clase de red se especifican en el RFC 1918 *(Address Allocation for Private Internets / Authors: Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear / Date: February 1996)* y son:

    a) 10.0.0.0 - 10.255.255.255 (prefijo 10/8 de Clase A)
    b) 172.16.0.0 - 172.31.255.255 (prefijo 172.16/12 de Clase B)
    c) 192.168.0.0 - 192.168.255.255 (prefijo 192.168/16 de Clase C)

2.1.3 Funcionalidades y beneficios de IPv6

De manera similar a cualquier actualización en tecnología, debe haber suficientes mejoras y beneficios para garantizar el tiempo, esfuerzo y costo asociado con el proceso de actualización. IPv6 ofrece diversas mejoras sobre su predecesor y tiene además nuevas funcionalidades que ayudarán a soportar el continuo crecimiento de Internet.

IPv6 ofrece una oportunidad para asignar rangos de direcciones de una manera más sensible y eficiente, lo que en última instancia optimizará las tablas de ruteo de Internet, al mismo tiempo que brinda una amplia gama de direcciones. Una vez integrado totalmente el protocolo, hará que NAT deje de ser necesario.

Las principales diferencias en el direccionamiento IPv6 comparado con IPv4 son:

- Las direcciones IPv6 tienen una longitud de 128 bits, comparados con los 32 bits de longitud de una dirección IPv4. En otras palabras, las direcciones IPv6 son 2^{96} veces más numerosas que las de su predecesor

- Las direcciones IPv6 son representadas en formato hexadecimal en vez de decimal y usan campos de 16 bits cada uno separados por ":" (dos puntos), a diferencia de IPv4 donde se usan campos de 8 bits separados por "." (punto)

Figura 3. Formato de direcciones IPv4 / IPv6
[IPv4 and IPv6; ARIN; Disponible en: https://www.arin.net/knowledge/ipv4_ipv6.pdf]

- Los conceptos de direccionamiento privado en el RFC 1918 no aplican para IPv6; sin embargo, diferentes tipos de direcciones IPv6 existen para brindar una funcionalidad similar

- En un router Cisco con software IOS, es posible configurar múltiples direcciones IPv6 en una misma interfaz (ya sea física o lógica), todas ellas con la misma precedencia en términos del comportamiento de la interfaz. En contraste, solamente una dirección IPv4 es posible configurar por interfaz con direcciones secundarias opcionales

- Direcciones IPv6 únicas globalmente pueden ser configuradas automáticamente por un router usando el proceso incorporado de autoconfiguración sin la asistencia de protocolos tales como DHCP

- IPv6 incorpora en sí mismo el descubrimiento de vecinos, mediante el cual un nodo IPv6 tiene la capacidad de descubrir sus vecinos y cualquier router que hable IPv6 en un segmento, así como si un router desea servir como una puerta de enlace predeterminada para los nodos

2.1.3.1 Espacio de direcciones más amplio

IPv6 incrementa el número de bits para las direcciones, pasando de 32 a 128 bits. Durante la especificación del diseño, hubo un debate acerca del número de bits a usar para las direcciones, se pensó en 64, 128 ó 160 bits. La opción de usar 128 bits se encontró ser la más apropiada, porque con ella se habilita una cantidad bastante grande de nodos que pueden ser direccionados. Sin embargo, como en cualquier otro esquema de direccionamiento, no todas las direcciones pueden ser usadas.

El formato y la capacidad de direcciones para cada versión se muestran a continuación en la siguiente tabla:

	IPv4	IPv6
Longitud (bits)	32	128
Direcciones posibles (#)	$2^{32} = 4{,}294{,}967{,}296$	$2^{128} = 3.4x10^{38}$

Tabla 1. Espacio de direccionamiento IPv4 / IPv6

Con el creciente fenómeno de las redes sociales y con cada vez más personas contando con múltiples dispositivos conectados al mismo tiempo (computadoras, teléfonos IP, faxes IP, teléfonos móviles, televisiones, videojuegos, notepads, pen-tablets, servidores de contenido, etc) IPv6 es conveniente para la comunicación *end-to-end* permitiendo el uso de una dirección IP propia y permanente, así como accesible globalmente.

Incrementando el número de bits además significó un incremento en el tamaño del encabezado. Ya que cada encabezado IP contiene tanto el campo de dirección origen (SA) como el de dirección destino (DA) el tamaño de los campos del encabezado que contienen dichas direcciones es de 64 bits para IPv4 y de 256 bits para IPv6.

Un espacio de direcciones más amplio incluye diversas mejoras: flexibilidad y accesibilidad global mejorada, ruteo jerárquico soportando agregación o sumarización de prefijos que son anunciados en las tablas de ruteo, conexión a múltiples ISP, autoconfiguración, opciones plug-and-play y mecanismos simplificados de renumeración de direcciones en caso de ser necesario.

2.1.3.2 Encabezado más simple y eficiente

Un paquete tiene dos componentes: el encabezado (*header*) que contiene la información de capa 3, y la carga útil (*payload*) que lleva los datos y la información del protocolo de capa superior (upper-layer protocol).

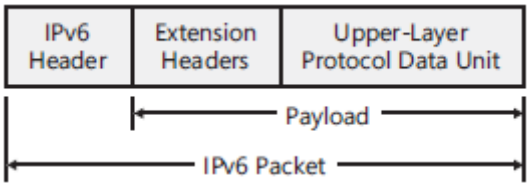

Figura 4. Estructura de un paquete IPv6

[Understanding IPv6; Davies, Joseph; 2ª ed; 2008; Microsoft Press]

La estructura del encabezado del paquete IP fue modificado en IPv6. Estos cambios reflejan algunas de las lecciones aprendidas tras años de operación de IPv4 y tienen impacto significativo en la operación del protocolo. Para entender lo que motivó las decisiones con respecto a la estructura del encabezado del paquete IPv6 es importante revisar la estructura de su predecesor.

RFC 791 define los siguientes campos para el encabezado del paquete IPv4:

a) **Version (4 bits).-** Representa la versión del protocolo IP. En este caso, su valor es 4.
b) **Header Length (4 bits).-** La longitud del encabezado únicamente, expresada en bloques de 4 bytes.
c) **Type of Service, ToS (8 bits).**- Este campo lleva información que habilita a los *routers* para clasificar y rutear un paquete de una manera diferenciada. Es un identificador de servicio importante, usado en la implementación de calidad de servicio (QoS).
d) **Total Length (16 bits).**- La longitud del paquete completo, encabezado más carga útil. Con los 16 bits disponibles en este campo, la longitud máxima de un paquete IPv4 es de 65,535 bytes.
e) **Identification (16 bits), Flags (3 bits), Fragment Offset (13bits).**- Estos tres campos habilitan a las redes IPv4 para soportar la fragmentación de paquetes sobre enlaces con diferentes unidades máximas de transmisión (MTU). La fragmentación es realizada bajo demanda por los router a lo largo de la trayectoria que sigue el paquete.
f) **Time to live (8 bits).**- Campo usado para decrementar en uno su valor conforme el paquete cruza un router, usado para evitar bucles infinitos (loops) debidos a problemas de ruteo. El paquete es descartado cuando el valor del campo es 0.
g) **Protocol Number (8 bits).**- Indica el protocolo de capa superior (TCP, UDP, ICMP, etc) que está presente en la carga útil del paquete IPv4.
h) **Header Checksum (16 bits).**- La integridad del encabezado es verificada comparando el valor calculado durante la comunicación con el valor presente en dicho campo.
i) **Source IPv4 Address (32 bits).**- Dirección IPv4 del nodo que originó el paquete.
j) **Destination IPv4 Address (32 bits).**- Dirección IPv4 del nodo destino del paquete.

k) **Options (longitud variable).-** Este campo sirve como un marcador de posición para la información relevante para el manejo adecuado de los datos que lleva el paquete, información que no está representada en los otros campos del encabezado.
l) **Padding (longitud variable).-** Usado para alinear la longitud variable del campo *Options* a un límite de 32 bits.

Los campos incluidos en el encabezado de IPv6 según el RFC 2460 *(Internet Protocol, Version 6 (IPv6) Specification / Authors: S. Deering, R. Hinden / Date: December 1998)* son los siguientes:

a) **Version (4 bits).-** Representa la versión del protocolo IP. En este caso, valor de 6.
b) **Traffic Class (8 bits).**- Este campo realiza la misma función que el campo ToS del encabezado IPv4.
c) **Flow Label (20 bits).-** Este es un campo nuevo implementado en el encabezado de IPv6, junto con los campos SA y DA permite identificar un flujo de manera única y está destinado a habilitar al router para identificar paquetes que deberían ser tratados de una manera similar sin la necesidad de un consulta profunda dentro de esos paquetes. Este campo es establecido por el origen y no debería ser cambiado por los routers que se encuentran a lo largo de la trayectoria rumbo al destino
d) **Payload Length (16 bits).**- Con la longitud del encabezado fija de 40 bytes, es suficiente para indicar la longitud de la carga útil para determinar la longitud del paquete completo.
e) **Next Header (8 bits).**- Este campo expande la funcionalidad del campo “Protocol Number” en el encabezado de IPv4. Antepone el tipo de información inmediatamente después del encabezado básico. Éste puede ser un encabezado de extensión o el protocolo de capa superior en la carga útil.
f) **Hop Limit (8 bits).**- En IPv6, el campo TTL de IPv4 fue apropiadamente renombrado porque se trata de una variable que es decrementada en cada salto (hop) y no tiene una dimensión temporal.
g) **Source IPv6 Address (128 bits).**- Dirección IPv6 del nodo que originó el paquete.
h) **Destination IPv6 Address (128 bits).**- Dirección IPv6 del nodo destino del paquete.

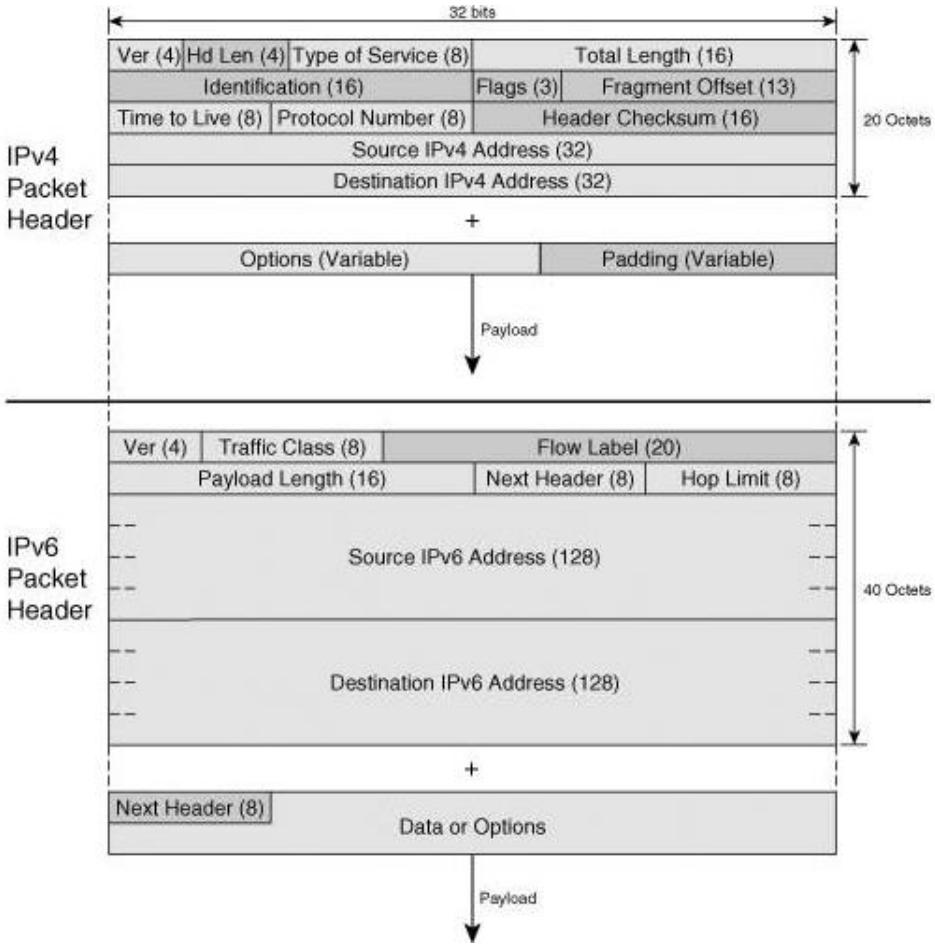

Figura 5. Formato de encabezado de paquetes IPv4 / IPv6

[Deploying IPv6 Networks; Popoviciu, Levy-Abegnoli, Grossetete; 2006; Cisco Press]

IPv6 usa un enfoque diferente a IPv4 para manejar la información opcional en el encabezado. Para tal fin define los encabezados de extensión (extension headers) que forman una cadena de encabezados enlazados por el campo “Next Header” contenido en cada uno de dichos encabezados.

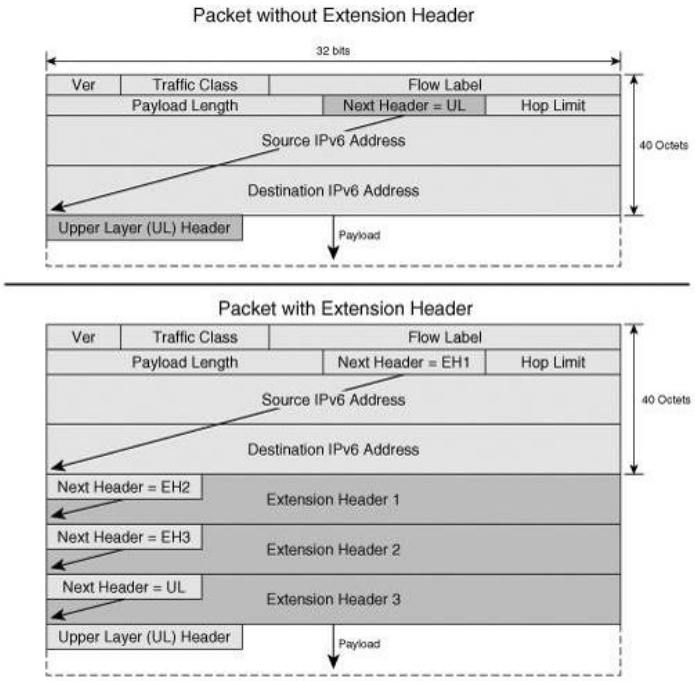

Figura 6. Uso de los encabezados de extensión IPv6
[Deploying IPv6 Networks; Popoviciu, Levy-Abegnoli, Grossetete; 2006; Cisco Press]

Cuando múltiples encabezados de extensión son usados en el mismo paquete, el orden de los mismos debería ser como se indica en la tabla 2.

Orden	Tipo de encabezado	"Next Header"
1	Encabezado IPv6 básico	-
2	Opciones SALTO-A-SALTO	0
3	Opciones de DESTINO (con opciones de RUTEO)	60
4	Encabezado de RUTEO	43
5	Encabezado de FRAGMENTACIÓN	44
6	Encabezado de AUTENTICACIÓN	51
7	Encabezado ESP (Encapsulation Security Payload)	50
8	Opciones de DESTINO	60
9	Encabezado de MOVILIDAD	135
	No hay encabezado siguiente	59
Capa superior	TCP	6
Capa superior	UDP	17
Capa superior	ICMPv6	58

Tabla 2. Encabezados de extensión IPv6

La estructura del nuevo encabezado obedece a nuevas premisas que lo hacen más simple:

- Casi la mitad de campos del encabezado IPv4 son removidos, lo que habilita procesamiento más simple de los paquetes mejorando el desempeño y la eficiencia de ruteo
- Todos los campos el encabezado IPv6 son alineados a 64 bits, lo cual habilita el almacenamiento directo y acceso a la memoria con búsquedas rápidas.
- Procesamiento eficiente basado en hardware, sin embargo este beneficio sigue siendo de interés porque las direcciones IPv6 de 128 bits son más grandes que el tamaño de palabra de los procesadores actuales lo que resulta en más consultas para obtener la dirección completa
- No hay fragmentación de paquetes, en su lugar el origen realiza descubrimiento del MTU en la trayectoria (PMTUD)
- No hay *broadcasts* y por lo tanto no hay amenaza de ataques de denegación de servicio (DoS) por inundación de este tipo de paquetes (storm)
- No hay *checksum* en la capa IP (capa 3 del modelo OSI), así como tampoco recálculo por los routers en la trayectoria del paquete
- La detección de errores es ejecutada tanto por la capa de enlace de datos (capa 2 del modelo OSI) como por la capa de transporte (capa4 del modelo OSI), por lo que en IPv6 los *checksums* son requeridos para TCP y UDP.
- Las etiquetas de flujos para el procesamiento por flujo sin la necesidad de abrir el paquete de transporte interior para identificar el flujo de tráfico.

El comparativo entre los encabezados IPv4 / IPv6 se muestra en la siguiente tabla:

Funcionalidad	IPv4	IPv6
Longitud de dirección	32 bits	128 bits
Campos del encabezado	12	8
Longitud del encabezado	20 bytes	40 bytes
Fragmentación de paquetes	SI	NO
Broadcasts	SI	NO
Checksum en IP	SI	NO

Tabla 3. Comparativo de encabezados IPv4 / IPv6

2.1.3.3 Seguridad y movilidad

La movilidad habilita a los usuarios moverse entre las redes con dispositivos de red móviles, muchos de ellos teniendo conectividad inalámbrica. Mobile IP es un estándar de la Fuerza de Tarea de la Ingeniería de Internet (IETF) disponible tanto para IPv4 como para IPv6. El estándar permite a los dispositivos móviles moverse sin cortes en su comunicación. Dado que IPv4 no brinda automáticamente este tipo de movilidad, se debe agregar realizando configuraciones adicionales. En IPv6, la movilidad es integrada en el protocolo mismo (built-in) lo que significa que cualquier nodo IPv6 puede usarlo cuando sea necesario.

IPsec es el estándar de IETF para la seguridad en redes IP, disponible tanto para IPv4 como para IPv6. Aunque las funcionalidades son esencialmente las mismas en ambos escenarios, IPsec es obligatorio en IPv6. IPsec es habilitado en todos los nodos IPv6 y está disponible para su uso. La disponibilidad de IPsec en todos los nodos hace el Internet IPv6 más seguro. IPsec además requiere llaves por cada nodo participante lo cual implica una implementación y distribución de llaves globales.

2.1.3.4 Riqueza de opciones de transición

Existen muchas maneras de incorporar las funcionalidades existentes en IPv4 con las funcionalidades adicionales en IPv6. Cada uno de los enfoques que pueden abordarse para la integración de IPv6 en la red se detallan a continuación:

- Teniendo configurada una doble pila de protocolos tanto con IPv4 como con IPv6 en la interfaz de un dispositivo de red (Dual-Stack)
- Usando túneles IPv4 para transportar tráfico IPv6 sobre IPv4 (6to4 tunnels)
- Traduciendo protocolos entre direcciones IPv6 e IPv4. Esta traducción permite comunicación directa entre nodos hablando diferentes protocolos (NAT-PT)

2.2 Diseño de IPv6

Antes de comenzar con la implementación de IPv6 en una red se debe tener entendimiento sólido de la estructura de las direcciones a usar, de cómo se reparte el direccionamiento desde la jerarquía más alta que son los organismos encargados de la asignación de todo el espacio de direcciones disponible, de cómo se representa una dirección IPv6 y los diferentes tipos de direcciones con los que se puede trabajar al momento de comenzar con la integración del nuevo protocolo.

2.2.1 Esquema de asignación del espacio de direcciones IPv6

Con 128 bits de longitud, el espacio de direccionamiento IPv6 es más diverso y por ende más complicado de administrar por lo que es importantísima la manera de planear la utilización del espacio disponible para evitar el malgastar direcciones por una mala asignación.

Los primeros esfuerzos y pruebas para encontrar la mejor manera de asignar las direcciones IPv6 se remontan al conocido 6bone, el cual fue establecido por el IETF en 1996 y consistía en una colección de nodos y redes IPv6 que sirvió como un escenario de pruebas para probar nuevos protocolos, implementaciones, mecanismos de transición y procedimientos operativos con la finalidad de retroalimentar a los desarrolladores y diseñadores del protocolo. Así también fue el distribuidor primario de direcciones IPv6 temporales para los experimentadores iniciales. El 6bone uso el pool de direcciones **3FFE::/16.** En junio del 2004 terminó la distribución de direcciones temporales y en su lugar se alentó a los solicitantes a solicitar direcciones homologadas a los organismos de estandarización. Finalmente el 6bone terminó operaciones y fue cerrado el 6 de junio de 2006.

Algunas de las definiciones que son usadas en la delegación de direcciones son listadas a continuación:

- **Internet Assigned Numbers Autority (IANA):** IANA sirve como la organización coordinadora central para los sistemas de numeración en Internet. Además de constituir la entidad de más alto nivel para la asignación de direcciones IP a los RIRs. IANA además brinda servicios clave de nombre de dominios (DNS)

- **Internet Registry (IR):** Organización que es responsable de la distribución de espacio de direcciones IP a sus miembros o clientes y de mantener registros de dichas distribuciones. IRs son clasificados de acuerdo a su función primaria y a su alcance territorial, puede ser ya sea un IR regional (RIR) o un IR nacional (NIR)

- **Regional Internet Registry (RIR):** Comunidades regionales establecen y autorizan RIRs, los cuales son reconocidos por la IANA, para servir y representar regiones geográficas grandes. El rol primario de un RIR es administrar y distribuir direcciones de Internet públicas dentro de sus regiones respectivas

- **National Internet Registry (NIR):** Un NIR principalmente asigna espacio de direcciones a sus miembros, los cuales generalmente son registros locales de Internet (LIR) que son reconocidos a un nivel nacional. Los NIRs existen en su mayoría en la región Asia-Pacífico

- **Local Internet Registry (LIR):** Un LIR primordialmente asigna espacio de direcciones a los usuarios de los servicios de red que ellos ofrecen. Los LIRs generalmente son proveedores de servicios de Internet (ISP) cuyos clientes son principalmente usuarios finales o posiblemente otros ISPs

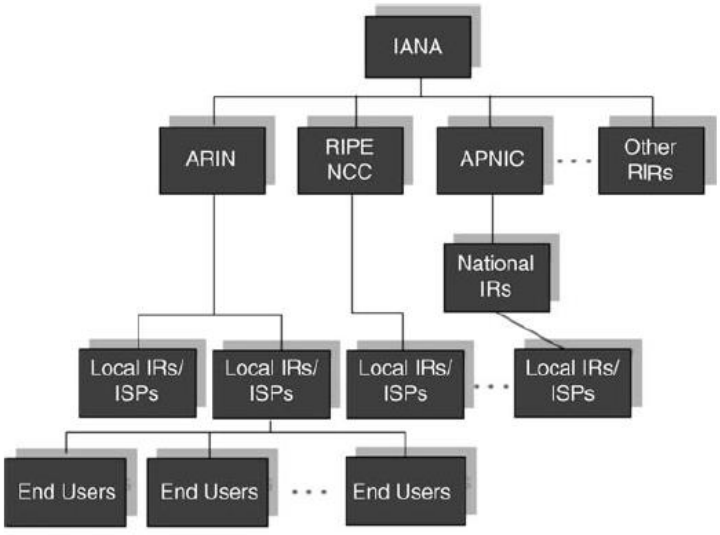

Figura 7. Jerarquía general de asignación de direcciones IP
[IP Address Management, Principles and Practice; Rooney, Timothy; 2011; IEEE Press]

Las cinco entidades regionales están ubicadas en diferentes regiones alrededor del mundo: Asia, Norteamérica, Sudamérica, Europa y África, de la siguiente manera:

i. **Asia Pacific Network Information Center (APNIC):** Asia y el Pacífico
ii. **American Registry for Internet Numbers (ARIN):** Norteamérica
iii. **Latin American and Caribbean Network Information Center (LACNIC):** Latinoamérica (Sudamérica y Centroamérica) y el Caribe
iv. **Réseaux IP Européennes Network Coordination Centre (RIPE-NCC):** Europa y Medio Oriente
v. **African Network Information Center (AfriNIC):** África

Tanto en IPv4 como en IPv6, los ISP reciben sus direcciones de estas entidades, las cuales generalmente cobran por el servicio. Los proveedores deberían aplicar a la entidad que se encuentra en su región.

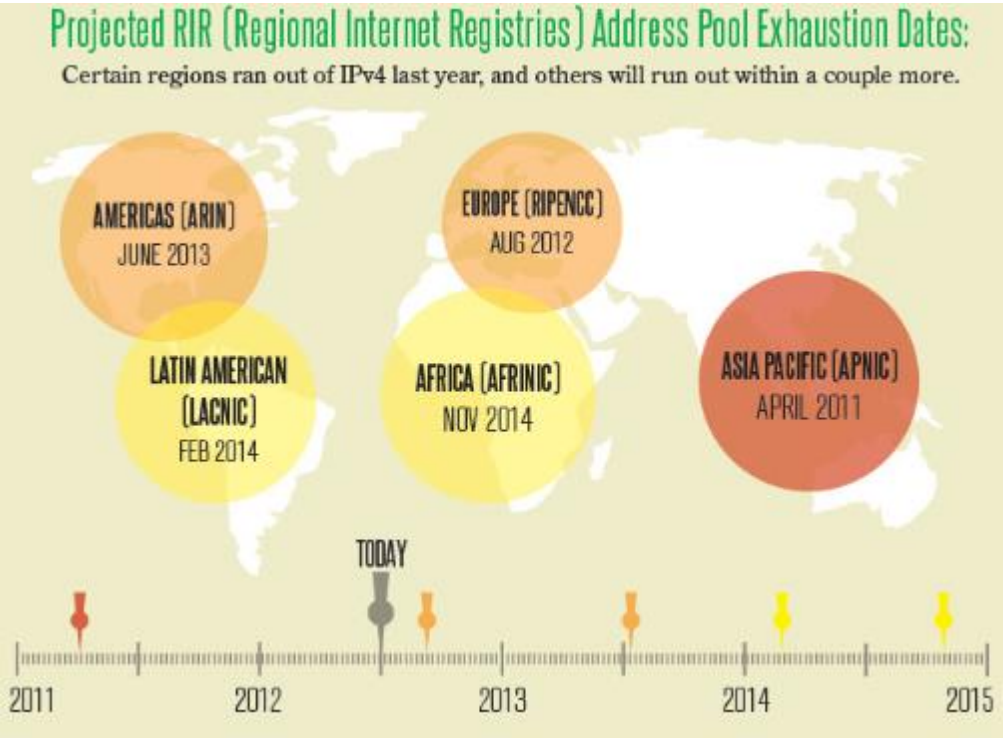

Figura 8. Entidades regionales (RIRs) para la asignación de direcciones
[APNIC Labs - IPv4 Address Pool Exhaustion; 2012; Disponible en: http://labs.apnic.net/ipv4/report.html]

El proceso de asignación de direcciones IPv6 para las organizaciones se realiza generalmente de la siguiente manera:

- IANA asigna del prefijo 2000::/3 a los RIR
- Cada RIR recibe un prefijo /12 de la IANA
- RIR asigna un prefijo /32 a un ISP
- ISP asigna un prefijo /48 (o prefijo /56) a cada cliente
- El cliente cuenta con máximo 16 bits disponibles para subnetear en LANes
- Cada LAN es un prefijo /64
- La parte de host de la dirección IPv6 se puede generar por autoconfiguración expandiendo los 48 bits de la dirección MAC a 64 bits insertando el número hexadecimal “FFFE” en los 16 bits intermedios para obtener el formato Extended Universal Identifier (EUI)-64

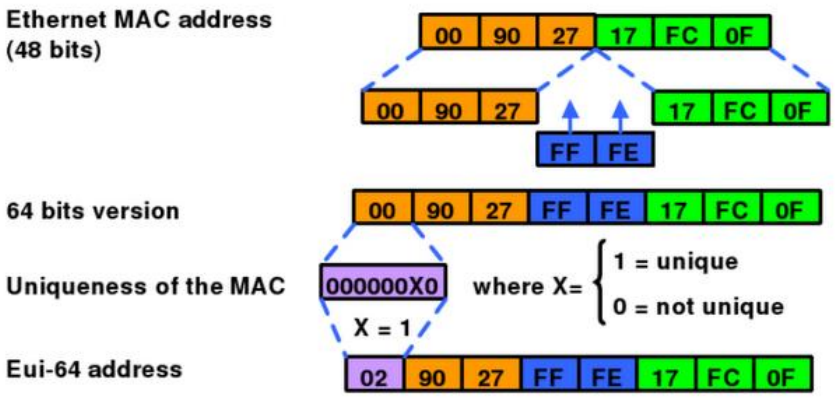

Figura 9. Formato EUI-64

[EUI-64 Guidelines; Disponible en: https://standards.ieee.org/develop/regauth/tut/eui64.pdf]

2.2.2 Arquitectura de direcciones IPv6

La arquitectura del direccionamiento IPv6 es fundamental para entender el cómo las direcciones son asignadas, cómo los nodos son numerados, cómo las tablas de ruteo son construidas, y cómo los paquetes son ruteados a través de la red.

Las direcciones IPv6 pueden ser representadas como cadenas de ceros y unos. Esta representación es una cadena bastante larga, pero es la manera que favorece a las computadoras por la lógica binaria que manejan.
Se diseñó una representación hexadecimal que reduce la cadena de 128 bits a 32 caracteres, aún así sigue siendo difícil de recordar, por lo que además fue segmentada en 8 grupos de 4 caracteres (16 bits) separados por dos puntos ":". Los valores A, B, C, D, E y F en hexadecimal son insensibles al uso de mayúsculas o minúsculas La representación decimal con la que estamos familiarizados en IPv4 no fue adoptada por IPv6.

Dos reglas adicionales fueron introducidas para optimizar más aún la representación de las direcciones IPv6:

- **La eliminación de los ceros al principio de cada campo.** Dentro de cada grupo de 16 bits (separado de los demás por los dos puntos), los ceros al inicio del campo pueden ser eliminados. Esto significa que se puede escribir **:00A1:** como **:A1:**

- **La eliminación de los campos consecutivos de ceros.** Es posible contraer los grupos de 16 bits consecutivos que contienen puros ceros. Solamente se puede usar este recurso una sola vez por dirección ya que no hay manera de identificar el tamaño de cada bloque de ceros. Esto significa que **:0000:0000:0000:** puede escribirse como **::**

En la figura 10 se ejemplifican las reglas aplicadas para lograr la máxima reducción de una dirección IPv6, lo cual facilita su manejo para aspectos de configuración y resolución de problemas (troubleshooting).

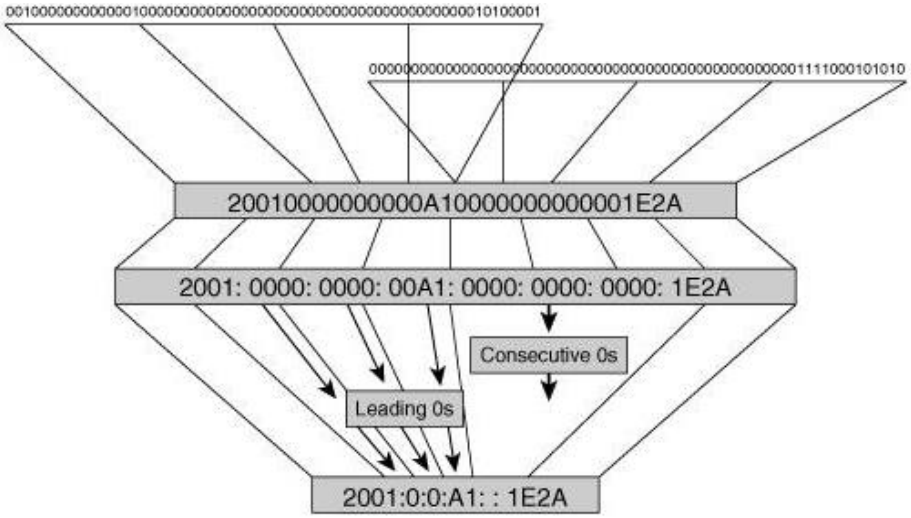

Figura 10. Representación de una dirección IPv6

[Deploying IPv6 Networks; Ciprian Popoviciu, Eric Levy-Abegnoli, Patrick Grossetete; 2006; Cisco Press]

2.2.3 Tipos de direcciones IPv6

IPv6 soporta tres tipos de direcciones, cada una de ellas tienes sus reglas específicas para su construcción y uso:

- **Unicast**
  - Dirección IPv6 que identifica a un único nodo
  - Dirección usada para la comunicación uno-a-uno
  - IPv6 tiene varias subcategorías de este tipo de direcciones, que se mencionarán más adelante

- **Multicast**
  - Dirección IPv6 que identifica a un grupo de nodos, y el tráfico destinado a una dirección multicast es enviado a todos los nodos dentro del grupo
  - Dirección usada para la comunicación uno-a-muchos
  - Habilita el uso más eficiente de los recursos de la red
  - Usa un rango de direcciones más amplio, comparándolo con el de IPv4

- **Anycast**
    - Tipo nuevo de dirección IPv6 que identifica a un grupo de nodos, y el tráfico destinado a una dirección anycast es enviado al nodo más cercano dentro del grupo
    - Dirección usada para la comunicación uno-a-el más cercano
    - Múltiples nodos comparten la misma dirección
    - Asignada del mismo espacio de direcciones que las direcciones unicast
    - Los dispositivos que originan la comunicación envían los paquetes indicando como dirección destino la dirección anycast y los routers deciden el dispositivo más cercano para alcanzar su destino basados en métricas de ruteo
    - Conveniente para servicios de balanceo de carga y entrega de contenidos

Cabe recalcar que en IPv6 no existe el concepto de dirección broadcast, en su lugar son reemplazadas por direcciones multicast y anycast.

2.2.3.1 Direcciones Unicast

Hay varios tipos de direcciones IPv6 Unicast y son:

- Global Unicast
- Link-local
- Site-local (obsoletas)
- Unique local
- Special-purpose
    - Unspecified
    - Loopback
    - IPv4-compatible
    - IPv4-mapped

Direcciones Global Unicast

Son ruteables globalmente y alcanzables en el Internet. Diseñadas para ser agregadas o sumarizadas con la finalidad de un ruteo eficiente. Su alcance y visibilidad es en todo Internet. Su rango de direcciones empieza con el valor binario 001 (**2000::/3**). La estructura de una dirección de este tipo, tal y como se define en el RFC 3587 *(IPv6 Global Unicast Address Format / Authors: S. Deering, R. Hinden / Date: August 2003),* se muestra en la figura 11 y se conforma de:

- Los 3 bits de más alto orden establecidos en **001**
- Prefijo de ruteo global
- Identificador de subred
- Identificador de interface

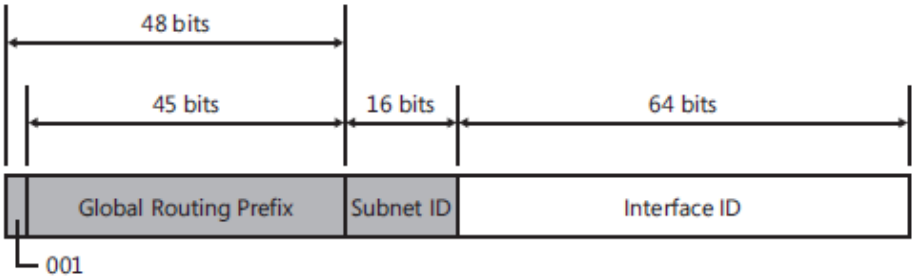

Figura 11. Estructura de una dirección global unicast
[Understanding IPv6; Davies, Joseph; 2ª ed; 2008; Microsoft Press]

Direcciones Link-local

Son usadas para la comunicación con nodos vecinos en el mismo enlace donde no hay router de por medio. Son identificadas porque sus 10 bits de más alto orden están establecidos en **1111 1110 10** y los siguientes 54 bits son ceros (**FE80::/10**). Todas las interfaces habilitadas para IPv6 deben tener una dirección link-local, la cual es creada dinámicamente y es usada para efectos de configuración automática de direcciones, descubrimiento de vecinos (*neighbor discovery*) y descubrimiento de routers. Al comunicarse con una dirección de este tipo se debe especificar la interfaz de salida ya que todas las interfaces conectan con el prefijo FE80::/10.

La estructura de una dirección de este tipo se muestra en la figura 12.

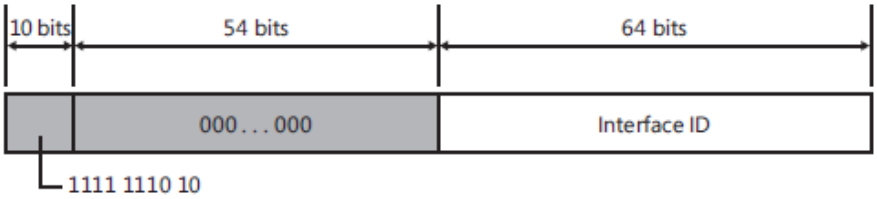

Figura 12. Estructura de una dirección link-local

[Understanding IPv6; Davies, Joseph; 2ª ed; 2008; Microsoft Press]

Direcciones Site-local

Son identificadas porque sus 10 bits de más alto orden están establecidos en un valor de **1111 1110 11** (**FEC0::/10**) y los siguientes 54 bits se pueden crear subredes dentro de la organización. Son equivalentes al espacio de direcciones IPv4 privadas (10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16). Redes internas que no tienen conexión directa ruteada a Internet pueden usar este tipo de direcciones sin tener conflicto con las *global unicast*. Han quedado formalmente obsoletas en el RFC 3879 *(Deprecating Site Local Addresses / Authors: C. Huitema, B. Carpenter / Date: September 2004)* para usarse en futuras implementaciones de IPv6, sin embargo pueden seguirse usando en implementaciones ya existentes. La estructura de una dirección de este tipo se muestra en la figura 13.

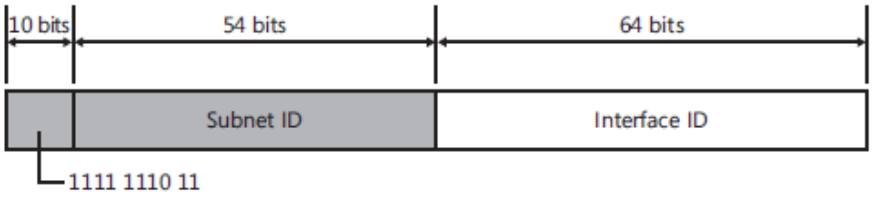

Figura 13. Estructura de una dirección site-local

[Understanding IPv6; Davies, Joseph; 2ª ed; 2008; Microsoft Press]

Direcciones Unique local

Dado que las direcciones site-local pueden ser reusadas en múltiples sitios dentro de una organización, pueden duplicarse direcciones, por lo que fueron reemplazadas por las direcciones *unique local*, las cuales son privadas a una organización pero únicas entre los sitios de la misma. No son ruteables en Internet. Los 7 bits de más alto orden están establecidos en **1111 110** (**FC00::/7**) y haciendo uso de una bandera para fijar el valor de 0 ó 1 en el bit #8 (L-local) derivándose los siguientes prefijos:

- **FC00::/8** planeado para ser administrado globalmente
- **FD00::/8** segmento destinado para los prefijos asignados localmente

La estructura de una dirección de este tipo se muestra en la figura 13.

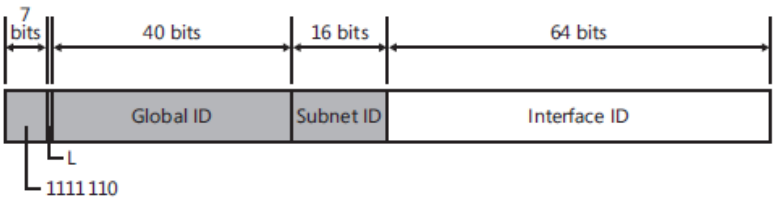

Figura 14. Estructura de una dirección unique local
[Understanding IPv6; Davies, Joseph; 2ª ed; 2008; Microsoft Press]

Con base en lo anterior, se cuentan con 40 bits en el identificador global (Global ID) para identificar a un sitio específico dentro de la organización, el cual se genera de manera aleatoria con lo cual existe poca probabilidad de duplicar direcciones IPv6 en dado caso que dos empresas se tengan que fusionar por fines administrativos minimizando el esfuerzo del proceso de renumeración de una de las redes por el traslape que pudiera existir.

El alcance predefinido para las direcciones IPv6 Unicast se muestra en la figura 15.

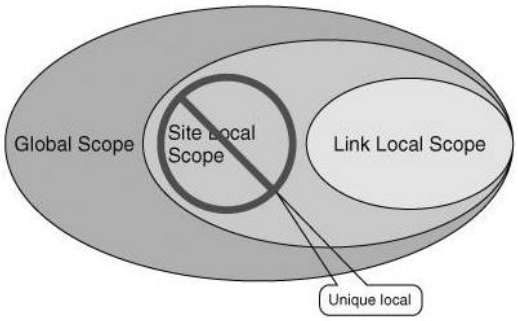

Figura 15. Alcance de las direcciones IPv6 Unicast
[Deploying IPv6 Networks; Popoviciu, Levy-Abegnoli, Grossetete; 2006; Cisco Press]

Direcciones Special-purpose

Un pequeño grupo de direcciones IPv6 ha sido definido para uso especial. Dichas direcciones no tienen un alcance predefinido por lo que se consideran independientes de los tipos que se han discutido previamente.

Hay dos direcciones básicas que tienen mucha importancia operativa:

- **Unspecified.-** No es asignada a ninguna interfaz, es usada como dirección origen por dispositivos que no tienen aún una dirección IPv6 o que no han comprobado que su dirección es única dentro del enlace local. Usada generalmente cuando el host solicita una dirección a un servidor DHCP (*Dynamic Host Configuration Protocol*). Sus 128 bits están establecidos en cero.

- **Loopback.-** Usada por cada nodo para referirse a sí mismo, es similar a la dirección 127.0.0.1 usada en IPv4 para identificar a la interfaz local en la pila del protocolo IP

Los otros dos tipos de direcciones especiales tienen que ver con la coexistencia de IPv4 con IPv6. Dos mecanismos han sido desarrollados para hacer el mapeo de direcciones de IPv4 hacia IPv6:

- **IPv4-compatible.-** Definida para usar túneles dinámicos y es construida anteponiendo 96 bits en cero a la dirección IPv4. Este tipo de dirección se hizo obsoleta y no es usada más.

- **IPv4-mapped.-** Usada para representar la dirección IPv4 en un formato de IPv6. Construida anteponiendo, 80 bits en "cero" seguidos de 16 bits en "uno"**,** a la dirección IPv4

En la tabla se indican las direcciones IPv6 de propósito especial, así como su representación tanto en formato regular como reducido.

Tipo de dirección	Dirección IPv6	Formato reducido
Unspecified	0:0:0:0:0:0:0:0	**::**
Loopback	0:0:0:0:0:0:0:1	**::1**
IPv4-compatible	0:0:0:0:0:0:IPv4	**::IPv4**
IPv4-mapped	0:0:0:0:0:FFFF:IPv4	**::FFFF:IPv4**

Tabla 4. Direcciones IPv6 de propósito especial

2.2.3.2 Direcciones Multicast

Una dirección multicast identifica a un grupo de interfaces. Tráfico que es enviado a una dirección multicast es enviado a múltiples destinos (todos los miembros del grupo) al mismo tiempo. Una interfaz puede pertenecer a cualquier cantidad de grupos de multicast. Los 8 bits de más alto orden están establecidos en **1111 1111** (**FF00::/8**). La estructura de una dirección multicast se muestra en la figura 16.

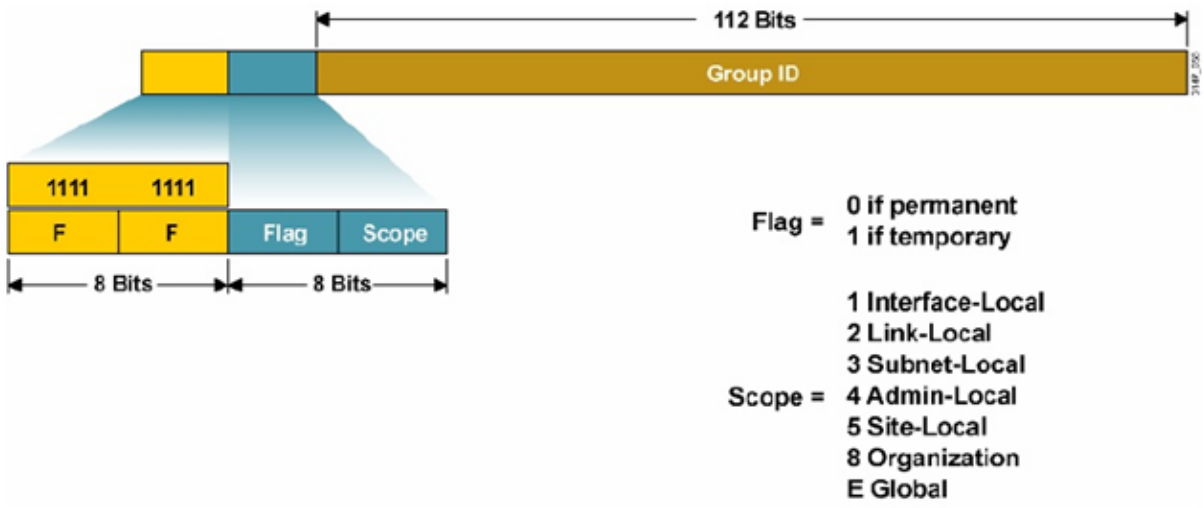

Figura 16. Estructura de una dirección IPv6 Multicast
[Implementing IPv6 Multicast; 2011; Disponible en:
http://www.cisco.com/c/en/us/td/docs/ios/ipv6/configuration/guide/12_4t/ipv6_12_4t_book/ip6-multicast.html]

Los 112 bits de menor orden constituyen el identificador de grupo de multicast (Group ID). Como ya se mencionó, no hay broadcast en IPv6 por lo que multicast es usado en su lugar. No existe el concepto de "Time To Live" (TTL) por lo que el alcance de la dirección es definido dentro de la dirección IPv6 misma haciendo uso del campo "Scope" La tabla 5 muestra la gama de opciones disponibles para el alcance de la dirección IPv6 haciendo uso del campo "Scope"

Scope (Hexadecimal)	Scope (Binario)	Formato reducido
1	0001	**Interface-local**
2	0010	**Link-local**
3	0011	**Subnet-local**
4	0100	**Admin-local**
5	0101	**Site-local**
8	1000	**Organization-local**
E	1110	**Global-local**

Tabla 5. Alcances definidos para direcciones IPv6 Multicast

Las direcciones IPv6 multicast en el rango de **FF00::** y hasta **FF0F::** son reservadas. Dentro de este rango, el RFC 2375 *(IPv6 Multicast Address Assignments / Authors: R. Hinden, S. Deering / Date: July 1998)* asigna las direcciones mostradas en la tabla 6, entre otras:

Dirección IPv6	Significado	Alcance
FF01::1	Todos los hosts	Interface-local
FF01::2	Todos los routers	Interface-local
FF02::1	Todos los hosts	Link-local
FF02::2	Todos los routers	Link-local
FF02::5	Todos los routers OSPF	Link-local
FF02::6	Todos los routers OSPF-DR	Link-local
FF02::9	Todos los routers RIP	Link-local
FF02::A	Todos los routers EIGRP	Link-local
FF02::D	Todos los routers PIM	Link-local
FF02::1:2	Todos los servidores DHCP	Link-local
FF05::2	Todos los routers	Site-local
FF05::1:3	Todos los servidores DHCP	Site-local

Tabla 6. Direcciones IPv6 Multicast reservadas

2.2.3.3 Direcciones Anycast

Una dirección Anycast es una dirección Global Unicast que es asignada a más de una interfaz. Cuando un paquete es enviado a una dirección Anycast, éste es ruteado a la interfaz "más cercana" que tenga configurada dicha dirección. En un alcance WAN, la interfaz más cercana es encontrada de acuerdo a la métrica del protocolo de ruteo en particular que se esté usando. En un alcance LAN, la interfaz más cercana representa al primer vecino del cual es aprendida.

Las siguientes son características de las direcciones Anycast:

- Son asignadas del espacio de direcciones Unicast por lo que no se pueden distinguir de ellas. Cuando la dirección es asignada a una interfaz de nodo, el nodo debe ser configurado explícitamente para saber que la dirección es una del tipo Anycast
- No deben ser usadas como direcciones origen para un paquete IPv6
- Permiten habilitar un tipo de mecanismo para descubrir el nodo más cercano de un grupo específico

La figura 17 muestra un ejemplo del uso de las direcciones Anycast.

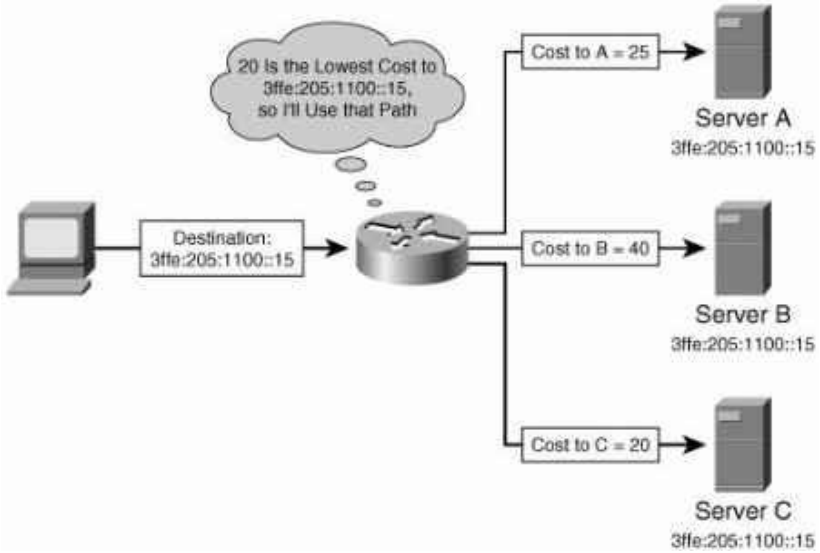

Figura 17. Ejemplo del uso de las direcciones Anycast
[Deploying IPv6 Networks; Popoviciu, Levy-Abegnoli, Grossetete; 2006; Cisco Press]

2.3 Mecanismos de transición hacia IPv6

Las transiciones de protocolo no son fáciles, y la transición de IPv4 hacia IPv6 no es la excepción. Las transiciones de protocolo generalmente son implementadas instalando y configurando el nuevo protocolo en todos los nodos dentro de la red y verificando que todos los dispositivos (tanto hosts y routers) operen de manera exitosa en base a lo esperado. Aunque esto quizá sea sencillamente gestionado en una organización ya sea pequeña o mediana, el reto de realizar una transición rápida de protocolo en una organización de mayor tamaño resulta muy complicado. Así también, dado el alcance global de Internet, la transición rápida de IPv4 hacia IPv6 de todo el ambiente de interconexión de las redes (internetworking) es una tarea imposible.

Los diseñadores de IPv6 reconocieron que la transición tomará años y que quizá haya organizaciones o nodos dentro de las organizaciones que continuarán usando IPv4 indefinidamente. Por lo tanto, aunque la migración es el objetivo a largo plazo, misma consideración se le debe dar a la convivencia provisional de IPv4 con IPv6.

Para convivir con la infraestructura de IPv4 y proporcionar una eventual migración a una infraestructura con IPv6 nativo, los estándares de transición hacia IPv6 definen los siguientes mecanismos:

- Dual-Stack (usando ambos, IPv4-IPv6)
- Tunneling (encapsulando tráfico IPv6 en paquetes IPv4)
- Translation (traducir paquetes IPv6 en IPv4 y viceversa)

Cualquiera que sea la estrategia seleccionada requiere coordinación efectiva de lo siguiente:

- ❖ Adecuada asignación de direcciones IPv4-IPv6, existentes y planeadas
- ❖ Validar la compatibilidad con IPv6 tanto de la infraestructura de red como de las aplicaciones
- ❖ Ajustar los servicios IP actuales para poder trabajar con IPv6 tales como el servicio de DNS, RADIUS, etc.

2.3.1 Enfoque de doble pila de protocolos (Dual-Stack)

La estrategia preferida para la transición hacia IPv6 es el enfoque de doble pila de protocolos (Dual-Stack), en el cual los nodos tienen habilitadas tanto la pila de protocolos de IPv4 como la de IPv6. Para funcionar, algunas aplicaciones deben ser modificadas para usar IPv6. Aplicaciones que trabajan únicamente con IPv4 continuarán funcionando como hasta ahora, mientras que las nuevas aplicaciones basadas en IPv6 toman ventaja de ambas capas IP, prefiriendo generalmente el uso de IPv6 para su comunicación.

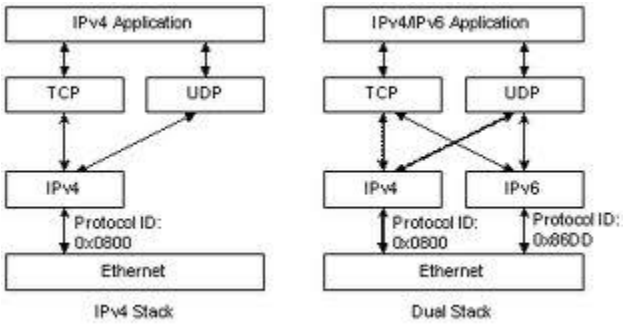

Figura 18. Enfoque Dual-Stack

[IP Address Management, Principles and Practice; Rooney, Timothy; 2011; IEEE Press]

El enfoque de doble pila de protocolos es bien conocido y ha sido aplicado en el pasado para la transición de otros protocolos.

El sistema operativo IOS de Cisco ya está preparado para la implementación de IPv6. Tan pronto y la configuración básica de IPv4 y de IPv6 está completa en la interfaz, ésta ya es "*Dual-stack*" y puede enviar tráfico generado para ambos protocolos.

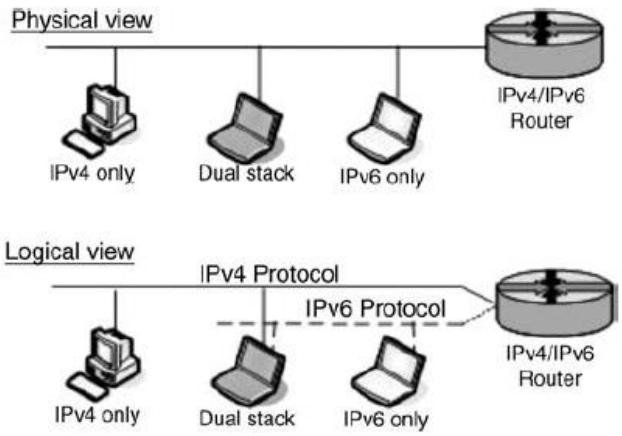

Figura 19. Ejemplo Dual-Stack

[IP Address Management, Principles and Practice; Rooney, Timothy; 2011; IEEE Press]

Dual-Stack es un método relativamente sencillo para integrar IPv6 al ambiente existente con IPv4, porque hay amplio soporte para IPv6 en los sistemas operativos más modernos. Esto, sin embargo, crea un ambiente de red más complejo.

2.3.2 Enfoque de establecimiento de túneles (Tunneling)

Al implementar IPv6, indudablemente habrá un escenario en el que una parte de la red de tránsito no soporte IPv6 de manera nativa. En dicho caso, la solución más sencilla y directa es de algún modo encapsular IPv6 y enviarlo sobre la red habilitada para IPv4.

Tunneling, en un sentido general, consiste en encapsular tráfico. Más específicamente, el término generalmente es usado para hacer referencia al proceso de encapsulación de tráfico en una capa determinada del modelo OSI dentro de otro protocolo corriendo en la misma capa. Por lo tanto, encapsular paquetes IPv6 dentro de paquetes IPv4 así como encapsular paquetes IPv4 dentro de paquetes IPv6 son ambos considerados túneles válidos.

Encapsular tráfico IPv6 y enviarlo sobre la red habilitada para IPv4 requiere un router de frontera (edge router) para encapsular el paquete IPv6 dentro del paquete IPv6, así como otro router para ejecutar la desencapsulación. Este proceso permite conectar islas IPv6 (segmentos de red con IPv6 de manera nativa) sin tener que convertir hacia IPv6 la red de tránsito en su totalidad.

Los túneles pueden establecer entre routers, entre hosts o entre router-host. Muchas técnicas se encuentran disponibles para el establecimiento de túneles:

- Configurados manualmente.- Predefinidos por los administradores de la red y requieren la configuración manual de los extremos del túnel. Ejemplos: IPv6-in-Ipv4, GRE, VPN.

- Automáticos.- No requiere preconfiguración, el túnel se establece bajo demanda cuando es necesario su uso. Ejemplos: 6to4, 6RD, ISATAP, Teredo.

Las principales desventajas giran en torno a la disminución de la carga útil (payload) de un paquete IPv6 por el hecho de tener que usar un encabezado de IPv4 para el proceso de encapsulación (mínimo 20 bytes), así como la dificultad al momento de hacer troubleshooting en caso de presentarse alguna falla.

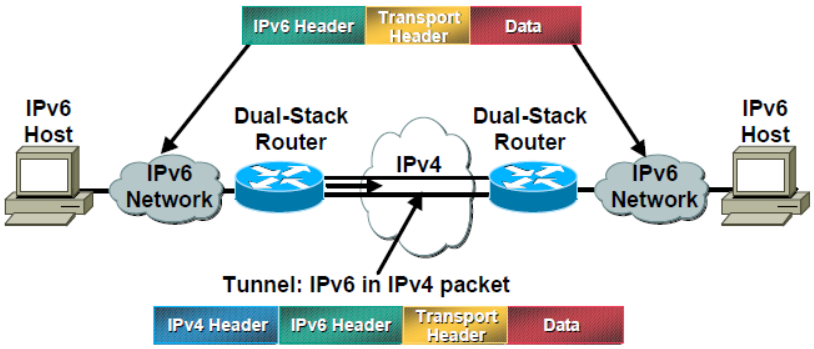

Figura 20. Ejemplo Tunneling

[IPv6 Tunnel through an IPv4 Network; 2011; Disponible en: http://www.cisco.com/c/en/us/support/docs/ip/ip-version-6/25156-ipv6tunnel.html]

2.3.3 Enfoque de traducción de direcciones (Translation)

Las técnicas de traducción realizan traducciones de IPv4 a IPv6 y viceversa, en una capa determinada de la pila de protocolo, por lo general en las capas de red, transporte o aplicación. A diferencia del tunneling, el cual no altera el paquete IPv6 sino únicamente agrega encabezados, los mecanismos de traducción sí modifican el paquete original.

NAT-PT es un mecanismo de traducción que permite a nodos que únicamente hablan IPv4 intercambiar tráfico con nodos que únicamente hablan IPv6

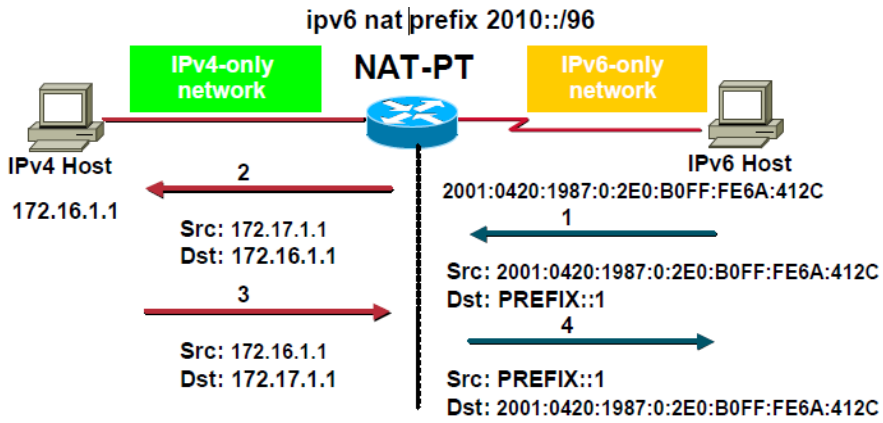

Figura 21. Ejemplo Translation

[Network Address Translator-Protocol Translator; 2013; Disponible en: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-software-releases-12-2-mainline/prod_white_paper09186a008011ff51.html]

CAPÍTULO 3

DEFINICIÓN DEL PROBLEMA, ANÁLISIS Y METODOLOGÍA EMPLEADA

El proceso de adecuación del backbone de la red de proveedor de servicios de Internet con cobertura en toda la República mexicana así como Estados Unidos y parte de Latinoamérica, para dar soporte al protocolo de nueva generación IPv6, implica arduo trabajo. Lo anterior debido a que los componentes de hardware y software, que hasta el momento se han adquirido y se han puesto en operación para ofrecer la conectividad hacia cualquier destino en Internet, requieren actualización. Resulta imposible realizar todas las acciones necesarias de un solo golpe, razón por la cual se definió una serie de fases para ir dando paso a la integración y conseguir una transición gradual hacia este nuevo entorno.

Dichas fases fueron: la planeación, diseño e implementación de la nueva tecnología con la finalidad de dar soporte a la nueva versión del protocolo.

En todo momento se siguió la estrategia definida por el negocio, asegurando una integración lo más transparente posible y siempre con la directriz de evitar afectar los servicios actualmente en operación, para continuar cumpliendo con los estándares de calidad que se tienen comprometidos con los clientes.

El área de desarrollo de la Ingeniería en Telecomunicaciones a la que personalmente quise dar enfoque fue la concerniente a los procesos de diseño e implementación, desarrollándome ampliamente en la tarea de adecuación y configuración de los dispositivos de la red a nivel de backbone y acceso, para los cuales se puede definir la problemática existente en cuanto a la transición se refiere.

Los problemas específicos que se presentaron fueron:

- Coordinación de esfuerzos de las áreas internas a la empresa con el fin de agendar las reuniones semanales del grupo interdisciplinario para el seguimiento del avance del proyecto

- Deficiencia en la planeación de la capacitación y adiestramiento del personal involucrado en las tareas diarias que impactan el avance del proyecto

- Ausencia de una política adecuada para la asignación del direccionamiento disponible, para una correcta administración del espacio de direcciones disponibles considerando la demanda actual y futura de los servicios que ofrece la empresa

- Posible riesgo inherente a la afectación de los servicios actuales por la integración de la nueva funcionalidad

- Acercamiento con los proveedores de la empresa para el fortalecimiento y mejoramiento de la interacción entre entidades, en caso de requerirse un mayor nivel de soporte, para resolución de problemas concernientes con la implementación de la tecnología nueva

Como se mencionó anteriormente el proceso de adecuación del backbone de la red de ISP para permitir la transición hacia el nuevo protocolo IPv6 constó de tres fases: planeación, diseño e implementación. A continuación se desglosarán y describirán a detalle las tareas y actividades en cada una de ellas:

3.1 Planeación

En esta fase se buscó alinear a todas las áreas internas a la organización, así como también a las entidades externas con las cuales se tiene interacción, con la finalidad de establecer los roles y responsabilidades de cada uno de los involucrados teniendo como objetivo común la adopción del nuevo protocolo IPv6. Del mismo modo se definieron las pautas de administración y uso del nuevo bloque de direcciones adquirido para un correcto funcionamiento, al igual que se aseguró que todos los insumos necesarios para el arranque y ejecución del proyecto. Está de más el hacer hincapié en que todos los esfuerzos y recursos que se asignaron en esta fase, apegándose a una planeación estratégica, ahorraron muchísimo esfuerzo y problemas en las fases siguientes.

3.1.1 Formación de grupo interdisciplinario

Como punto de partida para cualquier proyecto de relevancia que se lleva a cabo por parte de la empresa se define un grupo interdisciplinario conformado por personal de las distintas áreas de la organización involucradas en la ejecución y evolución para conseguir la meta deseada. Las reuniones de dicho comité sirvieron como foro para la elaboración de procesos, para el establecimiento de acuerdos de nivel de operación (OLA) entre las áreas, para aclarar las dudas que surgieron durante la ejecución del proyecto. Dicho grupo de ingenieros fue la interfaz encargada de que los objetivos y políticas hayan sido difundidos y entendidos dentro de la organización. Se encargaron de informar del avance que se fue teniendo y de los logros alcanzados en base a los tiempos compromiso estipulados. Los compromisos por cumplir vinieron dados por la Alta Dirección y se encontraron alineados a la estrategia definida por el negocio.

Las áreas participantes en el grupo interdisciplinario fueron:

- Dirección Comercial
- Estrategia y Evolución Tecnológica
- Ingeniería
- Construcción
- Gestión de Cambios y Configuraciones
- Gestión de Fallas
- Soporte Técnico
- Desempeño de la Red
- Seguridad Informática
- Proveedores: Cisco Systems, Juniper Networks, Alcatel-Lucent

3.1.2 Detección de las necesidades de capacitación

Otro punto importante que compete a la fase de planeación consistió en realizar un análisis de la nueva tecnología que se pretendía poner en operación para detectar si existía o no la necesidad de capacitación para el personal involucrado en dicho proyecto, con la finalidad de asegurar que se contaba con los conocimientos indispensables para un adecuado desenvolvimiento durante las tareas que cada área de la organización tenía a su cargo. Los programas de capacitación al personal se organizaron considerando la evolución del servicio por cada una de las etapas de su ciclo de vida: estrategia, diseño, transición, operación y mejora continua del servicio. Se seleccionó a personal clave para brindarles capacitación, quienes a su vez fueron los encargados de difundir el conocimiento hacia cada uno de sus grupos de trabajo.

3.1.3 Política de asignación de direccionamiento

Con la finalidad de tener un esquema eficiente de direccionamiento se definió una política de asignación para administrar de una manera jerárquica y escalable los bloques de direcciones IPv6 asignados por el registro regional de Internet (RIR). Dicha política establece que la asignación del espacio de direcciones se hará por región y por servicio, ya que el protocolo IPv6 de la red de ISP estará en cada uno de los diferentes servicios que la red IP ofrece.

La asignación del direccionamiento descrito se realizó tomando en cuenta las recomendaciones del IETF descritas en los RFC 3177 *(IAB/IESG Recommendations on IPv6 Address Allocations to Sites / Authors: IAB, IESG / Date: September 2001)* y RFC 5375 *(IPv6 Unicast Address Assignment Considerations / Authors: G. Van de Velde, C. Popoviciu, T. Chown, O. Bonness, C. Hahn / Date: December 2008)*, considerando la topología lógica de la red, acorde con las políticas de enrutamiento y tratando de reducir al máximo el número de anuncios BGP hacia el Internet global. Los dos bloques de direcciones IPv6 que fueron asignados a la organización son:

- **2001:1208::/32** A ser utilizado para infraestructura
- **2806:1000::/24** A ser utilizado para los servicios IP ofrecidos

El bloque 2001:1208::/32 se estará utilizando para asignar direcciones IPv6 a todos los recursos de los dispositivos de red que conforman la infraestructura de la red del ISP, considerándolo como de uso exclusivo de la red del proveedor de servicios en este caso por lo que no será enrutado al Internet global. Dichos recursos que requieren contar con una dirección IPv6 son:

- Interfaces lógicas para la gestión del dispositivo (Interfaz Loopback)
- Enlaces o conexiones punto a punto entre dispositivos de infraestructura
- Segmentos de área local para equipos de infraestructura

El bloque 2806:1000::/24 será anunciado al Internet global y se estará utilizando para la gama de servicios que actualmente ofrece la organización:

- Internet Corporativo
- Internet Masivo
- VPN (Virtual Private Network).

La asignación inicial del direccionamiento IPv6 asignado, se realizó basándose en la topología que tiene la red del ISP, la cual se divide en siete *clusters*. Un *cluster* es una división lógica de un grupo de routers que se adecua a la conexión física de la red. La red del ISP cuenta con los siguientes *clusters* repartidos a lo largo del territorio nacional y que se encargan de ofrecer la cobertura en todo el país: Noroeste, Norte, Noreste, Centro_1, Centro_2, Sur y Sureste.

Cada uno de los bloques de direcciones IPv6, tanto de Infraestructura como de Servicios IP, fue dividido en 256 bloques de tamaño idéntico y repartido entre cada uno de los *clusters* como se indica en la tabla 7.

	2001:1208::/32	**2806:1000::/24**
Cluster	**Bloques /40 INFRA**	**Bloques /32 SERVICIOS**
Noroeste	16	16
Norte	16	16
Noreste	32	32
Centro_1	32	32
Centro_2	32	32
Sur	32	32
Sureste	16	16
Reservado	80	80
TOTAL	**256**	**256**

Tabla 7. Repartición de bloques IPv6 por cluster

Con esta asignación inicial, se estarán usando un total de 176 bloques y quedan 80 bloques reservados en cada caso para futuro crecimiento.

La repartición de los bloques IPv6 de Infraestructura se realizó tomando en consideración en primera instancia cada una de las áreas de OSPF dentro del cluster, y después la subcategoría de segmento para Loopback, WAN o LAN.

La repartición de los bloques IPv6 de Servicios se realizó tomando en consideración si se trataba de Internet Corporativo o de Internet Masivo. Para el caso del servicio VPN se asignó un segmento único, a usarse para las conexiones WAN que van del CPE-PE del ISP.

A continuación se muestra el desglose de cada uno de los bloques asignados por cluster para la parte de Servicios, así como el servicio que cubrirá cada uno de ellos. El esquema de asignación del direccionamiento interno no se muestra ya que es propio de la empresa.

Cluster Noroeste

Bloque IPv6	Uso (Servicio)
2806:1000::/32	Internet Corporativo
2806:1001::/32	Internet Corporativo
2806:1002::/32	Internet Corporativo
2806:1003::/32	Internet Corporativo
2806:1004::/32	Internet Masivo
2806:1005::/32	Internet Masivo
2806:1006::/32	Internet Masivo
2806:1007::/32	Internet Masivo
2806:1008::/32	Internet Masivo
2806:1009::/32	Internet Masivo
2806:100A::/32	Internet Masivo
2806:100B::/32	Internet Masivo
2806:100C::/32	6RD
2806:100D::/32	Reservado
2806:100E::/32	Reservado
2806:100F::/32	Reservado

Tabla 8. Direccionamiento para el cluster Noroeste

Cluster Norte

Bloque IPv6	Uso (Servicio)
2806:1010::/32	Internet Corporativo
2806:1011::/32	Internet Corporativo
2806:1012::/32	Internet Corporativo
2806:1013::/32	Internet Corporativo
2806:1014::/32	Internet Masivo
2806:1015::/32	Internet Masivo
2806:1016::/32	Internet Masivo
2806:1017::/32	Internet Masivo
2806:1018::/32	Internet Masivo
2806:1019::/32	Internet Masivo
2806:101A::/32	Internet Masivo
2806:101B::/32	Internet Masivo
2806:101C::/32	6RD
2806:101D::/32	Reservado
2806:101E::/32	Reservado
2806:101F::/32	Reservado

Tabla 9. Direccionamiento para el cluster Norte

Cluster Noreste

Bloque IPv6	Uso (Servicio)
2806:1020::/32	Internet Corporativo
2806:1021::/32	Internet Corporativo
2806:1022::/32	Internet Corporativo
2806:1023::/32	Internet Corporativo
2806:1024::/32	Internet Corporativo
2806:1025::/32	Internet Corporativo
2806:1026::/32	Internet Corporativo
2806:1027::/32	Internet Corporativo
2806:1028::/32	Internet Masivo
2806:1029::/32	Internet Masivo
2806:102A::/32	Internet Masivo
2806:102B::/32	Internet Masivo
2806:102C::/32	Internet Masivo
2806:102D::/32	Internet Masivo
2806:102E::/32	Internet Masivo
2806:102F::/32	Internet Masivo
2806:1030::/32	Internet Masivo
2806:1031::/32	Internet Masivo
2806:1032::/32	Internet Masivo
2806:1033::/32	Internet Masivo
2806:1034::/32	Internet Masivo
2806:1035::/32	Internet Masivo
2806:1036::/32	Internet Masivo
2806:1037::/32	Internet Masivo
2806:1038::/32	6RD
2806:1039::/32	6RD
2806:103A::/32	Reservado
2806:103B::/32	Reservado
2806:103C::/32	Reservado
2806:103D::/32	Reservado
2806:103E::/32	Reservado
2806:103F::/32	Reservado

Tabla 10. Direccionamiento para el cluster Noreste

Cluster Centro_1

Bloque IPv6	Uso (Servicio)
2806:1040::/32	Internet Corporativo
2806:1041::/32	Internet Corporativo
2806:1042::/32	Internet Corporativo
2806:1043::/32	Internet Corporativo
2806:1044::/32	Internet Corporativo
2806:1045::/32	Internet Corporativo
2806:1046::/32	Internet Corporativo
2806:1047::/32	Internet Corporativo
2806:1048::/32	Internet Masivo
2806:1049::/32	Internet Masivo
2806:104A::/32	Internet Masivo
2806:104B::/32	Internet Masivo
2806:104C::/32	Internet Masivo
2806:104D::/32	Internet Masivo
2806:104E::/32	Internet Masivo
2806:104F::/32	Internet Masivo
2806:1050::/32	Internet Masivo
2806:1051::/32	Internet Masivo
2806:1052::/32	Internet Masivo
2806:1053::/32	Internet Masivo
2806:1054::/32	Internet Masivo
2806:1055::/32	Internet Masivo
2806:1056::/32	Internet Masivo
2806:1057::/32	Internet Masivo
2806:1058::/32	6RD
2806:1059::/32	6RD
2806:105A::/32	Reservado
2806:105B::/32	Reservado
2806:105C::/32	Reservado
2806:105D::/32	Reservado
2806:105E::/32	Reservado
2806:105F::/32	Reservado

Tabla 11. Direccionamiento para el cluster Centro_1

Cluster Centro_2

Bloque IPv6	Uso (Servicio)
2806:1060::/32	Internet Corporativo
2806:1061::/32	Internet Corporativo
2806:1062::/32	Internet Corporativo
2806:1063::/32	Internet Corporativo
2806:1064::/32	Internet Corporativo
2806:1065::/32	Internet Corporativo
2806:1066::/32	Internet Corporativo
2806:1067::/32	Internet Corporativo
2806:1068::/32	Internet Masivo
2806:1069::/32	Internet Masivo
2806:106A::/32	Internet Masivo
2806:106B::/32	Internet Masivo
2806:106C::/32	Internet Masivo
2806:106D::/32	Internet Masivo
2806:106E::/32	Internet Masivo
2806:106F::/32	Internet Masivo
2806:1070::/32	Internet Masivo
2806:1071::/32	Internet Masivo
2806:1072::/32	Internet Masivo
2806:1073::/32	Internet Masivo
2806:1074::/32	Internet Masivo
2806:1075::/32	Internet Masivo
2806:1076::/32	Internet Masivo
2806:1077::/32	Internet Masivo
2806:1078::/32	6RD
2806:1079::/32	6RD
2806:107A::/32	Reservado
2806:107B::/32	Reservado
2806:107C::/32	Reservado
2806:107D::/32	Reservado
2806:107E::/32	Reservado
2806:107F::/32	Reservado

Tabla 12. Direccionamiento para el cluster Centro_2

Cluster Sur

Bloque IPv6	Uso (Servicio)
2806:1080::/32	Internet Corporativo
2806:1081::/32	Internet Corporativo
2806:1082::/32	Internet Corporativo
2806:1083::/32	Internet Corporativo
2806:1084::/32	Internet Corporativo
2806:1085::/32	Internet Corporativo
2806:1086::/32	Internet Corporativo
2806:1087::/32	Internet Corporativo
2806:1088::/32	Internet Masivo
2806:1089::/32	Internet Masivo
2806:108A::/32	Internet Masivo
2806:108B::/32	Internet Masivo
2806:108C::/32	Internet Masivo
2806:108D::/32	Internet Masivo
2806:108E::/32	Internet Masivo
2806:108F::/32	Internet Masivo
2806:1090::/32	Internet Masivo
2806:1091::/32	Internet Masivo
2806:1092::/32	Internet Masivo
2806:1093::/32	Internet Masivo
2806:1094::/32	Internet Masivo
2806:1095::/32	Internet Masivo
2806:1096::/32	Internet Masivo
2806:1097::/32	Internet Masivo
2806:1098::/32	6RD
2806:1099::/32	6RD
2806:109A::/32	Reservado
2806:109B::/32	Reservado
2806:109C::/32	Reservado
2806:109D::/32	Reservado
2806:109E::/32	Reservado
2806:109F::/32	Reservado

Tabla 13. Direccionamiento para el cluster Sur

Cluster Sureste

Bloque IPv6	Uso (Servicio)
2806:10A0::/32	Internet Corporativo
2806:10A1::/32	Internet Corporativo
2806:10A2::/32	Internet Corporativo
2806:10A3::/32	Internet Corporativo
2806:10A4::/32	Internet Masivo
2806:10A5::/32	Internet Masivo
2806:10A6::/32	Internet Masivo
2806:10A7::/32	Internet Masivo
2806:10A8::/32	Internet Masivo
2806:10A9::/32	Internet Masivo
2806:10AA::/32	Internet Masivo
2806:10AB::/32	Internet Masivo
2806:10AC::/32	6RD
2806:10AD::/32	Reservado
2806:10AE::/32	Reservado
2806:10AF::/32	Reservado

Tabla 14. Direccionamiento para el cluster Sureste

El servicio VPN utilizará direccionamiento para los enlaces WAN (conexión PE-CPE), es decir la conexión que va del equipo en la frontera del ISP con el equipo en el sitio del cliente, del bloque **2806:10FF::/32** para todo el país.

3.2 Diseño

Para poder identificar las adecuaciones necesarias a la red del ISP se partió de la situación actual, por lo que a continuación se detallará la topología actual, así como los protocolos con los que se cuenta actualmente y el funcionamiento que tienen para ofrecer los servicios mencionados a los usuarios finales.

La red de ISP, tal y como se mencionó anteriormente, consta de 7 *clusters* que cubren todo el territorio nacional. Así mismo se cuentan con equipos instalados en dos localidades de Estados Unidos, cuya función en la red es la de interconectar la red de ISP en México con los *Peering* (puntos de intercambio de redes) y *Carriers* (proveedores internacionales). En la figura 22 se muestra la conexión de los puntos de presencia (PoPs) en Estados Unidos con los proveedores y *carriers* internacionales: NTT, Sprint, Verizon, ATT, Google, MSN, etc.

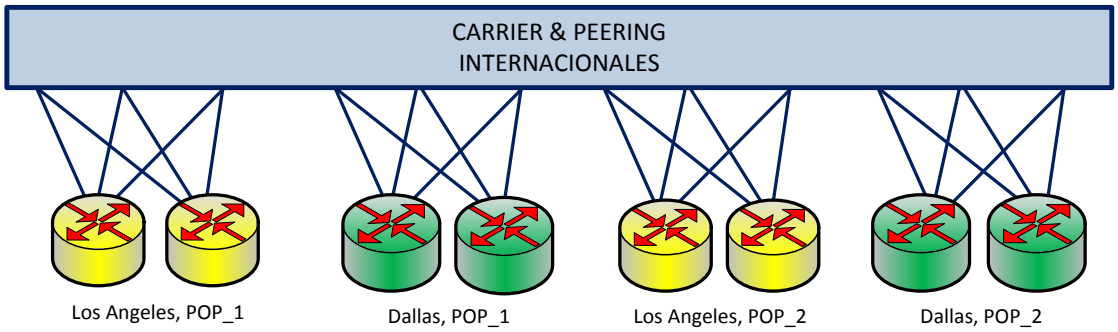

Figura 22. Conexión de PoPs USA con proveedores internacionales

La estructura de la red es jerárquica, es decir que cuenta con varios niveles o capas que la conforman, cada una realizando funciones particulares e interconectando con las demás capas. Dichas capas se muestran en la figura 23 y se muestran a continuación:

- **Acceso:** Es la capa donde se tienen los equipos dedicados que ofrecen el servicio a los usuarios finales. Es la capa donde se ubican los equipos PE, que son los equipos encargados de recibir las conexiones de los clientes.

- **Distribución:** Es la capa encargada de la conectividad basada en políticas. Contiene a los equipos de tránsito, conocidos como equipos P, que son equipos internos a la red del ISP. También se le conoce como tránsito.

- ***Backbone* (*core* o núcleo):** Capa encargada del envío de paquetes (*forwarding*) a una tasa alta. Es el nivel de mayor jerarquía y constituye la espina dorsal de la red.

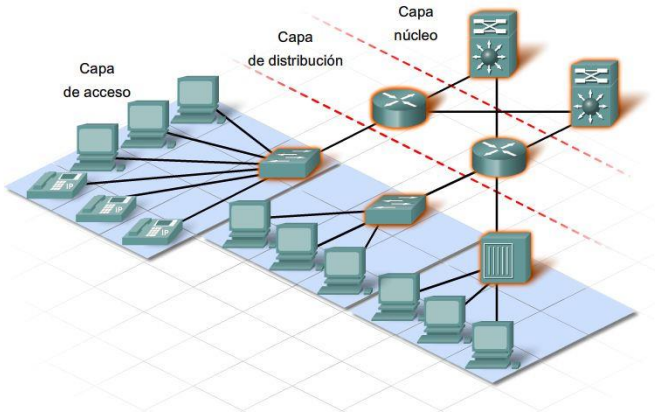

Figura 23. Estructura jerárquica de la red de ISP
[Deploying IPv6 Networks; Popoviciu, Levy-Abegnoli, Grossetete; 2006; Cisco Press]

Los protocolos actualmente soportados son:

- OSPF como protocolo interno
- LDP para intercambio de etiquetas
- MPLS para ruteo basado en etiquetas
- MP-BGP como protocolo externo

El protocolo interno (IGP) para manejar y compartir las redes propias de la infraestructura de la red es OSPF, el cual es un protocolo de ruteo tipo Link-State que permite segmentar la red en porciones más pequeñas conocidas como áreas e interconectadas por el área de *backbone* (área 0) para una mejor administración de la red.

El protocolo LDP permite asignar e intercambiar etiquetas con sus equipos vecinos con la finalidad de ser usadas por MPLS para contar con un ruteo más eficiente basado en etiquetas, haciéndolo más rápido y eficiente ya que únicamente lo que hacen los equipos es ir intercambiando etiquetas a lo largo de la trayectoria del paquete evitando las búsquedas (*lookups*) en la tabla de ruteo de cada router que resultan ser más lentas y demandan más procesamiento de los equipos.

El protocolo MPLS sirve para implementar servicios de redes privadas virtuales (VPN) para ofrecer conexiones seguras a los clientes sobre una red pública. El protocolo BGP es usado para interconectar con redes externas y para transportar las redes de clientes.

La red de ISP en su conjunto es un backbone MPLS, la cual es una tecnología de ruteo (*forwarding*) de paquetes que usa etiquetas para la toma de decisiones de las trayectorias a usar. Entre los beneficios que brinda la tecnología MPLS se encuentran:

- Ruteo de capa 3 basado en el intercambio de etiquetas. Las etiquetas son impuestas en el router de ingreso (*ingress PE*). El cambio de etiquetas (*swapping*) es usado en vez de las consultas a las tablas de ruteo y la etiqueta es retirada en el router de egreso (*egress PE*)
- El análisis del encabezado de capa 3 es hecho solamente una vez, en la frontera de ingreso al backbone de MPLS, lo cual hace más eficiente el ruteo basándolo únicamente en las etiquetas intercambiadas vía el protocolo de distribución de etiquetas (LDP)
- Hay muchas bondades, implementadas en el ISP, que se pueden ofrecer con esta tecnología: redes privadas virtuales (VPN), calidad de servicio (QoS), los routers internos al ISP requieren menos memoria y sobrecarga de CPU al ser invisibles para ellos los prefijos de los clientes. Entre otras funcionalidades que se pueden implementar en la red de ISP puede ser la ingeniería de tráfico (*TE*) así como AToM

El diagrama de la figura 24 ejemplifica la estructura del backbone MPLS de la red del ISP, el cual se encuentra conformado por los siguientes componentes:

- Red del proveedor.- Es el backbone MPLS controlado por el ISP. Dentro de los equipos instalados en dicha red se encuentran los equipos P, el cual es un router interno a la red del ISP y que se encarga únicamente del *swapping* (intercambio) de etiquetas. Además, los equipos PE que se encargan ya sea de añadir las etiquetas al ingreso a la red del proveedor o de extraerlas al momento de abandonar la red del proveedor y son los que tienen comunicación directa con los equipos de los clientes.
- Red de cliente.- Es la porción de la red bajo la administración de cada uno de los clientes que usan los servicios del ISP. En esta red se encuentran los equipos CE, los cuales junto con los equipos PE forman la interfaz de comunicación con la red del proveedor.

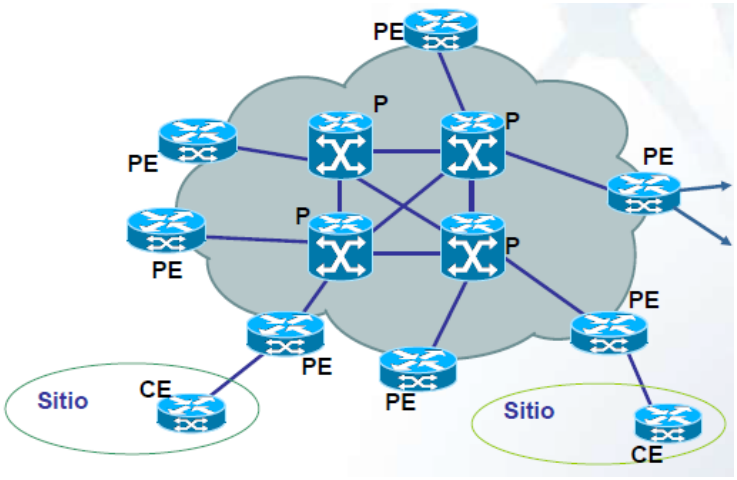

Figura 24. Componentes de una red MPLS
[Implementing MPLS VPN in Provider's IP Backbone; Luyuan Fang; 2000; Disponible en: https://www.ietf.org/proceedings/49/slides/ppvpn-7.pdf]

De manera análoga, el mismo backbone de MPLS puede ser usado para integrar las redes privadas virtuales (VPN) para ofrecer conexiones seguras simulando que la red es dedicada para cada uno de los clientes pero compartiendo los recursos de la misma red para dar soporte a toda una gama de usuarios sin que haya visibilidad entre cada una de estas redes de los clientes. La figura 25 muestra la integración de los servicios VPN al backbone de MPLS.

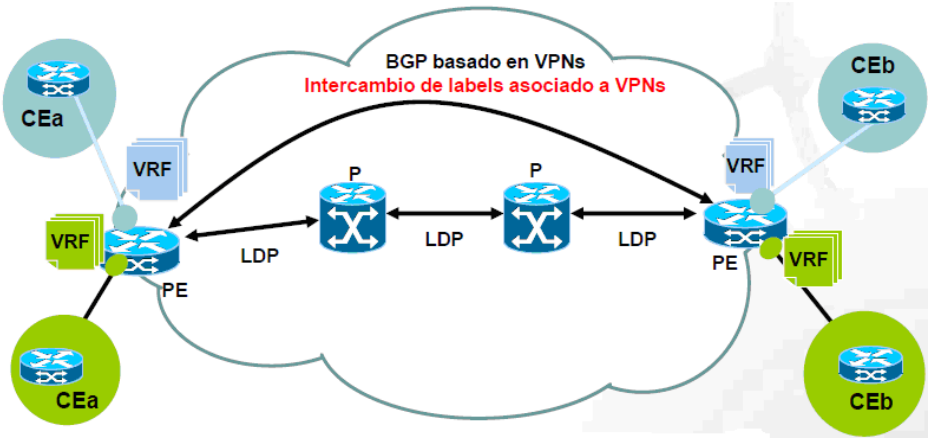

Figura 25. Diagrama de una red MPLS/VPN
[Implementing MPLS VPN in Provider's IP Backbone; Luyuan Fang; 2000; Disponible en: https://www.ietf.org/proceedings/49/slides/ppvpn-7.pdf]

El protocolo MP-BGP configurado dentro del sistema autónomo del ISP sirve para anunciar las redes de los clientes, con la finalidad de no mezclarlas con las redes propias de la infraestructura de la red, así como para anunciar las redes a otros sistemas autónomos (ya sea algún otro ISP o cliente).

El protocolo BGP soporta varias familias de direcciones (AF), para el caso de los servicios de Internet clásicos se configura el AF IPv4, para los servicios de VPN basados en MPLS se configura el AF VPNv4. Para poder soportar la versión 6 de IP será necesario habilitar una familia de direcciones más para cada uno de estos servicios.

La topología lógica usada para el protocolo BGP en una red de proveedor de servicios requiere que para tener consistencia de enrutamiento dentro del sistema autónomo es indispensable que todos los equipos hablen dicho protocolo (conocido como topología de malla completa o *Full-Mesh*), sin embargo esto no resulta escalable cuando la red es muy grande, como es el caso de un ISP, para lo cual se hace uso de una funcionalidad conocida como Route-reflectors (RR) jerárquicos para subsanar las limitaciones que impone la topología lógica de BGP.

El esquema conceptual de los Route-reflectors jerárquicos se muestra en la figura 26 donde se observa que los equipos Route-reflectors se van asignando conforme a cada una de las capas definidas en la red: acceso, distribución y backbone. Un equipo de backbone juega el rol de route-reflector de uno o varios equipos de la capa de distribución. Éste último juega el rol de cliente para el equipo de mayor jerarquía, pero a su vez también juega el rol de route-reflector para el equipo en la jerarquía menor (acceso). Esto evita el hecho de configurar malla completa de sesiones de BGP de todos contra todos, lo cual reduce la cantidad de configuración por aplicar en ese caso.

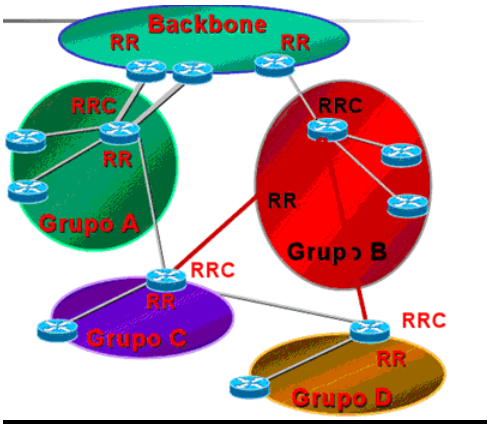

Figura 26. Route-reflectors jerárquicos
[Implementing MPLS VPN in Provider's IP Backbone; Luyuan Fang; 2000; Disponible en: https://www.ietf.org/proceedings/49/slides/ppvpn-7.pdf]

En el nivel de mayor jerarquía es imposible evitar la topología de malla completa por lo que resulta necesario configurar en Full-Mesh todos los equipos de la capa de backbone, pero obviamente es menor la cantidad de equipos comparando con los instalados en su totalidad. Se define una pareja de equipos RR por *cluster* por redundancia como muestra la figura 27.

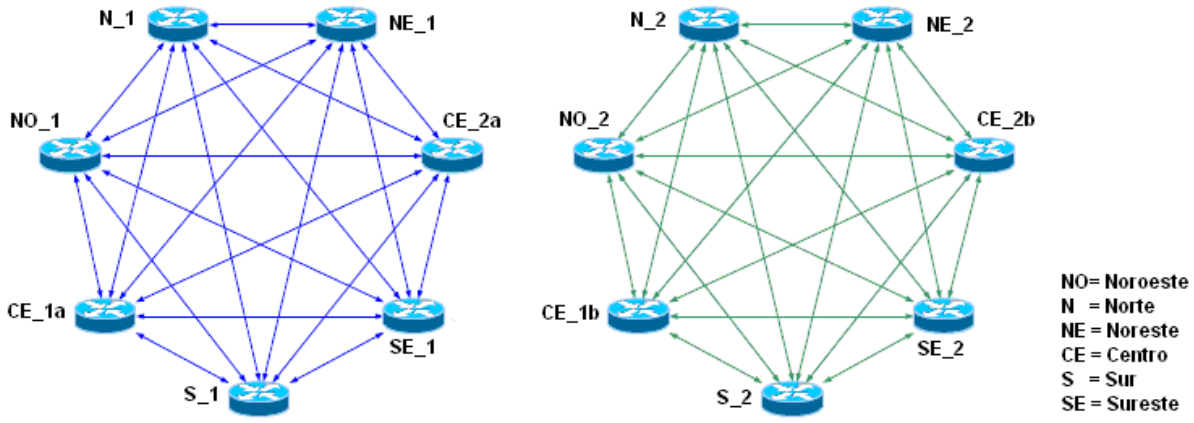

Figura 27. Diseño de Route-reflectors jerárquicos en ISP

3.2.1 Adecuación del servicio DNS

La implementación exitosa de un Sistema de nombres de dominio (DNS) es crítica para la creación de una red IPv6 robusta. DNS es un servicio de directorio distribuido de Internet que es usado para traducir de nombres de dominio a direcciones IP (forward lookups), y de direcciones IP a nombres de dominio (reverse lookup).

El protocolo DNS ha sido actualizado para soportar IPv6 además de IPv4. Las dos tareas principales fueron:

- Habilitar la traducción de nombres de dominio a direcciones IPv6
- Habilitar los servidores para comunicarse entre sí tanto en IPv6 como en IPv4

Los servidores DNS mantienen una base de datos con las relaciones entre los nombres de dominio (por ejemplo http://www.cisco.com) y la dirección IP asociada con dicha liga. Esta información es almacenada en forma de registros, los cuales pueden ser:

- **Registros tipo A**: relacionan nombre de dominio con dirección IPv4
- **Registros tipo AAAA**: relacionan nombre de dominio con dirección IPv6

Cuando el servidor DNS recibe una solicitud de consulta para un registro tipo A contesta con la dirección IPv4 asociada al host por el cual se preguntó. De la misma manera, cuando el servidor DNS reciba una solicitud de consulta para un registro tipo AAAA contesta con la dirección IPv6 asociada al host.

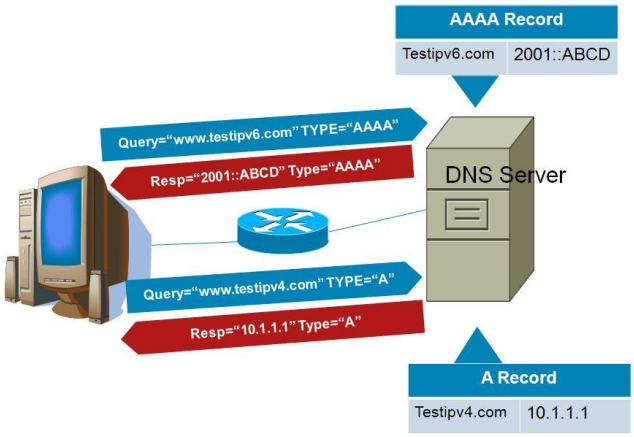

Figura 28. Funcionamiento de servidor DNS
[IPv6 Addressing and Basic Connectivity; DNS for IPv6; Disponible en: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xe-3s/ip6b-xe-3s-book/ip6-add-basic-conn-xe.html]

En un escenario donde se cuente con equipos habilitados para ambos protocolos (Dual-Stack) resulta de suma importancia la correcta operación de dicho servicio para la administración de la mayoría de los problemas relacionados con resolución DNS y selección de direcciones. El proceso es como sigue:

Etapa 1: El DNS request es enviado. Una aplicación habilitada tanto para IPv4 como IPv6 envía consultas al DNS para todos los tipos de direcciones para el hostname destino
Etapa 2: El servidor DNS envía una respuesta. El servidor DNS contesta con todas las direcciones disponibles para el hostname consultado
Etapa 3: La aplicación selecciona la dirección correcta. La aplicación selecciona alguna de las direcciones (por defecto selecciona la dirección IPv6)
Etapa 4: La aplicación conecta con el host destino. La aplicación solicita que el host origen conecte al host destino usando la dirección IPv6

3.2.2 Adecuación de la red de acceso

Hay muchas maneras de entregar servicios IPv6 a los usuarios finales. Las redes de los ISP cuentan con características únicas que muchas veces no están presentes en otros ambientes, por ejemplo los ambientes empresariales o las redes de los clientes.

Existen tres métodos principales que son usados para que los ISP que únicamente soportan servicios de IPv4 puedan ofrecer nuevos servicios de IPv6 a sus clientes ya existentes o inclusive a nuevos clientes que se vayan incorporando a la red. Cada estrategia tiene fortalezas y debilidades que determinan su capacidad para adaptarse a un ISP en particular. Dichos métodos son:

- Actualizar la red en su totalidad para que sea Dual-Stack.
- Implementar una red con IPv6 nativo, paralela a la ya existente.
- Actualizar a Dual-Stack únicamente la frontera de la red del ISP y usar tunneling a lo largo de toda la red con IPv4 puro.

La solución más rentable a todas luces es el último método que se menciona, que consiste actualizar únicamente los routers de frontera del ISP (PE routers). Esta solución implica actualizar o implementar nuevas funcionalidades para IPv6 en la frontera del ISP, que es la interfaz hacia los clientes que requieren el servicio, pudiendo hacerse habilitando Dual-Stack en cada uno de los routers de frontera del proveedor (PE routers) y dejando intactos los routers internos a la red del proveedor (P routers).

Las redes de los ISP pueden clasificarse en dos grandes rubros: redes basadas en MPLS y redes no basadas en MPLS. Los proveedores de servicios de Internet que ya cuentan con su backbone habilitado con MPLS cuentan con técnicas adicionales para la integración de IPv6 a su red. Tres de las opciones disponibles para estos ISP, que representan soluciones directas ya que usan la infraestructura y habilidades que ya se encuentran disponibles, son:

- 6PE (IPv6 Provider Edge router over MPLS)
- 6VPE (IPv6 VPN Provider Edge router over MPLS)
- 6RD (IPv6 Rapid Deployment)

Se explica el funcionamiento de cada una de estas opciones más adelante.

- **6PE (IPv6 Provider Edge router over MPLS)**

Estrategia de integración de servicios IPv6 al backbone actual de IPv4/MPLS definida en el RFC 4798 *(Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE) / Authors: J. De Clercq, D. Ooms, S. Prevost, F. Le Faucheur / Date: February 2007)* y ofrece conectividad IPv6 global a través de un backbone MPLS con soporte exclusivo a IPv4. Las principales características de esta estrategia son:

- ❖ Los routers de frontera (ahora denominados 6PE) deben soportar Dual-Stack
- ❖ Los prefijos IPv6 existen en la tabla global de los 6PE únicamente
- ❖ La información de ruteo es intercambiada por los 6PE vía MP-BGP
- ❖ Los paquetes IPv6 son transportados de 6PE-6PE dentro de MPLS
- ❖ El backbone usa protocolos para versión 4 (IGPv4, LDPv4, MP-BGP)
- ❖ Se minimizan cambios en el backbone del ISP al no tocar los routers P
- ❖ Se elimina la necesidad de usar túneles IPv6-sobre-IPv4
- ❖ El router del cliente (CPE) puede correr IPv4, IPv6 o ambos
- ❖ Únicamente se agrega el **address-family ipv6** en la configuración de MP-BGP

El diagrama de implementación para esta opción de transición se muestra en la figura 29.

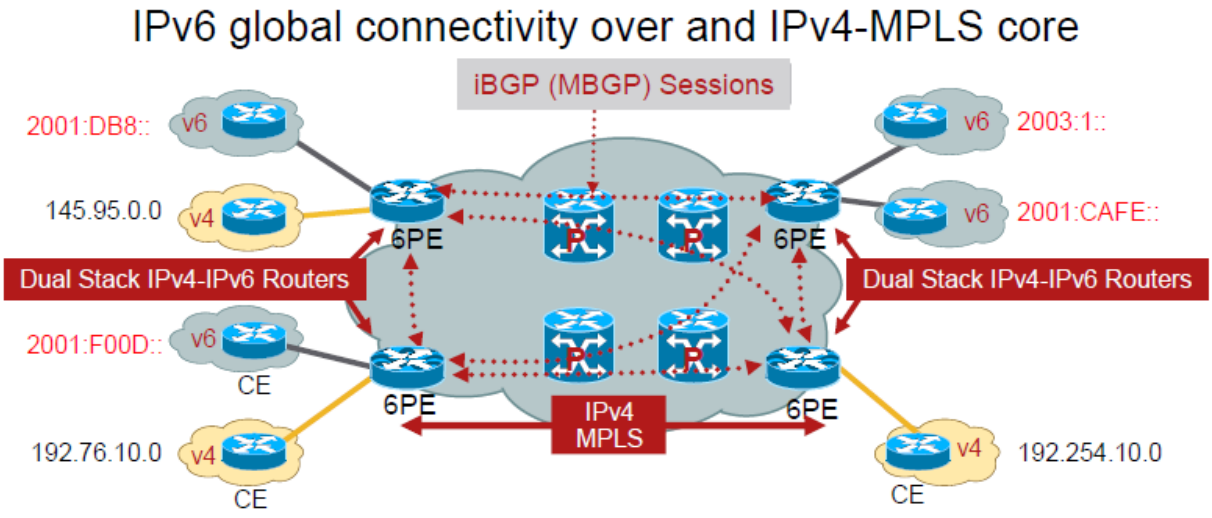

Figura 29. Diagrama de implementación 6PE

[Transition mechanisms for IPv6; Hernán Contreras G; Disponible en: http://www.cu.ipv6tf.org/lacnic16/05-6RD_LACNOG_draft.pdf]

- **6VPE (IPv6 VPN Provider Edge router over MPLS)**

Estrategia de integración de servicios IPv6 al backbone actual de IPv4/MPLS definida en el RFC 4659 (BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN / Authors: J. De Clercq, D. Ooms, M. Carugi, F. Le Faucheur / Date: September 2006) y ofrece conectividad IPv6 segura haciendo uso de una red privada virtual ofrecida a través de un backbone MPLS con soporte exclusivo a IPv4. Las principales características de esta estrategia son:

- Los routers de frontera (ahora denominados 6VPE) deben soportar Dual-Stack
- Añade el soporte a IPv6 para los servicios de VPN en versión 4
- Brinda de manera lógica tablas de ruteo independientes por cada VPN
- Soporta ambas VPN (IPv4/IPv6) concurrentemente en las mismas interfaces
- El backbone usa protocolos para versión 4 (IGPv4, LDPv4, MP-BGP)
- Se minimizan cambios en el backbone del ISP al no tocar los routers P
- El router del cliente (CPE) puede correr IPv4, IPv6 o ambos
- Únicamente se agregan los **address-family ipv6 y address-family vpnv6** en la configuración de MP-BGP

El diagrama de implementación para esta opción de transición se muestra en la figura 30.

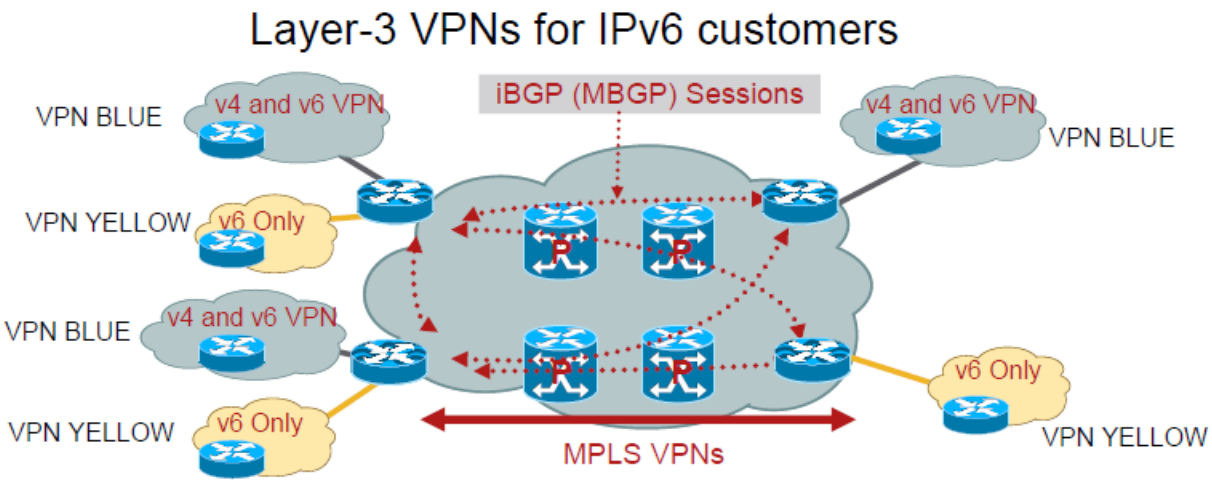

Figura 30. Diagrama de implementación 6VPE

[Transition mechanisms for IPv6; Hernán Contreras G; Disponible en: http://www.cu.ipv6tf.org/lacnic16/05-6RD_LACNOG_draft.pdf]

- **6RD (IPv6 Rapid Deployment)**

Estrategia de integración de servicios IPv6 al backbone del ISP definida en el *RFC* 5969 *(IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification / Authors: W. Townsley, O. Troan / Date: August 2010)* y ofrece la oportunidad a un ISP a implementar soporte IPv6 sin cambiar su *core.* Las principales características de esta estrategia son:

- Utiliza *tunneling* (encapsulación 6to4 modificada)
- El backbone del core no requiere contar con MPLS
- Usa un prefijo IPv6 asignado por el ISP en vez del reservado **2002::/16** para el establecimiento de túneles 6to4
- Su operación se basa en la delegación automática de un prefijo IPv6 a los sitios del cliente con lo cual se forma la dirección IPv6 que tendrá asignada éste último considerando además su dirección IPv4 codificada (IPv4-compatible)
- Requiere de un equipo denominado 6RD Border Relay (BR) que será el encargado de tener la conectividad global con el backbone de IPv6 y será el equipo encargado de asignarlo dirección IPv6 al usuario residencial
- Permite esquema redundante si se configuran direcciones Anycast para los equipos Border Relay (BR)
- Inherente desventaja del MTU capaz de usar por el *overhead* de los encabezados
- Demanda de mayores recursos de CPU a los equipos
- Añade mayores retardos al tráfico de los usuarios
- Se minimizan cambios en el backbone del ISP
- De gran utilidad cuando equipos involucrados no soportan Dual-Stack

El diagrama de implementación para esta opción de transición se muestra en la figura 31.

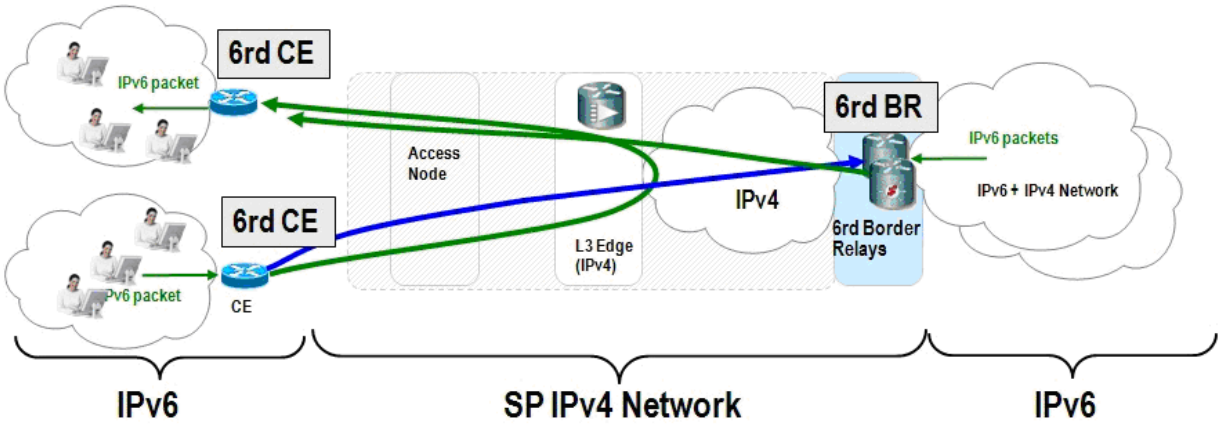

Figura 31. Diagrama de implementación 6RD
[Transition mechanisms for IPv6; Hernán Contreras G; Disponible en: http://www.cu.ipv6tf.org/lacnic16/05-6RD_LACNOG_draft.pdf]

3.2.3 Adecuación de la red de backbone

Como se observa en el punto anterior, las opciones de transición para las redes de los ISP que operan bajo MPLS se centran en la actualización y ajustes en los equipos que se encuentran en la frontera de la red del proveedor, y que son la interfaz de acceso al servicio para los clientes. La bondad de estas opciones es que se evita el tener que tocar la red de backbone del proveedor, manteniéndolo con sus funcionalidades IPv4 actuales sin necesidad de requerirse actualización de hardware ni de software en los routers P del proveedor.

3.3 Implementación

Para la adopción del nuevo protocolo IPv6 se definieron diferentes etapas, éstas fueron divididas por servicios. El primer servicio que soportó el protocolo IPv6 fue el servicio de Internet Corporativo, después le siguió el servicio VPN y por último el Internet Masivo.

Para la parte de la implementación en la red de ISP se consideraron dos fases principales para poder habilitar el servicio IPv6 a los usuarios finales, las cuales fueron: habilitación del protocolo hacia los ISP internacionales, que se encuentran en una jerarquía más alta y son los encargados a su vez de tener conexiones con otros proveedores alrededor del mundo y permitir la conectividad global; la segunda fase fue la de habilitar los routers de acceso al servicio, que son los routers de frontera del ISP (routers PE) para el soporte hacia los clientes. A continuación se describirán más a detalle cada una de estas fases.

3.3.1 Configuración de IPv6 con ISPs internacionales

La descripción de la configuración del protocolo IPv6 en cada uno de los routers de backbone de los PoPs de Estados Unidos (routers de frontera que brindan la conexión hacia los proveedores internacionales) es la siguiente, aclarando que se utilizan direcciones ficticias por aspectos de confidencialidad ya que son de uso interno exclusivamente:

1. Configuración del Dual-Stack en la interfaz del equipo de Estados Unidos que conecta con el router del proveedor internacional

```
Router_USA#
configure terminal
interface TenGigE0/0/1/0
description "ENLACE TENGIGABIT A CARRIER INTERNACIONAL "
 bandwidth 10000000
 ipv4 address 10.10.10.2 255.255.255.252
 ipv6 address fe80:418:1000:2000::16 link-local
ipv6 address 2001:418:1000:2000::16/126
…
```

2. Configuración de una sesión de BGP IPv6 con cada uno de los proveedores internacionales para recibir todas las rutas de IPv6 (*Full-Routing)*

```
Router_USA#
configure terminal
prefix-set IPV6_ISP
2806:1000::/24 le 128
…
end-set
```

```
Router_USA#
configure terminal
router bgp 8151
 neighbor 2001:418:1000:2000::15
  remote-as 2914
  description "CARRIER-INT_IPv6"
  address-family ipv6 unicast
   route-policy IPV6_ISP out
…
```

3. Anuncio del bloque de IPv6 asignado al ISP, únicamente el relativo a la parte de los servicios ya que el bloque propio de la infraestructura no será anunciado al Internet

```
Router_USA#
configure terminal
router static
address-family ipv6 unicast
  2806:1000::/24 Null0
router bgp 8151
address-family ipv6 unicast
  network 2806:1000::/24
…
```

3.3.2 Configuración de IPv6 en la red de acceso: 6PE, 6VPE y 6RD

La configuración que se agregó, a la ya existente para el protocolo IPv4, para la implementación de la funcionalidad de 6PE para el servicio de Internet Corporativo se describe a continuación:

1. Configuración de una sesión de iBGP (Internal BGP) IPv4 entre el router de backbone del PoP de Estados Unidos y el equipo PE utilizando la funcionalidad de 6PE

```
Router_USA#
configure terminal
router bgp 8151
 neighbor 192.168.10.1
  remote-as 8151
  description "Router_PE_IC"
  update-source Loopback0
  address-family ipv6 labeled-unicast
…
```

```
Router_PE_IC#
configure terminal
router bgp 8151
 neighbor 192.168.10.2 remote-as 8151
 neighbor 192.168.10.2 description "Router_USA"
 neighbor 192.168.10.2 update-source Loopback0
address-family ipv4
 neighbor 192.168.10.2 activate
address-family ipv6
 neighbor 192.168.10.2 activate
 neighbor 192.168.10.2 send-label
…
```

2. Configuración de IPv6 en los equipos Route-Reflector, usados para mejorar la escalabilidad del protocolo y asegurar una malla completa (Full-Mesh) que conecte a todos los equipos dentro del sistema autónomo de manera eficiente, permitiendo reducir las líneas de configuración. En ellos se tendrá que habilitar el Address-Family IPv6 para poder transportar la información de las rutas de IPv6

```
Router_RR#
configure terminal
router bgp 8151
neighbor 192.168.10.1 remote-as 8151
 neighbor 192.168.10.1 description "Router_PE_IC"
 neighbor 192.168.10.1 update-source Loopback0
address-family ipv6
  neighbor 192.168.10.1 activate
  neighbor 192.168.10.1 send-community
  neighbor 192.168.10.1 route-reflector-client
  neighbor 192.168.10.1 send-label
…
```

3. Configuración de una sesión de eBGP (External BGP) IPv6 entre el equipo PE y el equipo CPE del cliente, actualmente ya existe una sesión de External BGP IPv4 entre estos equipos, por lo cual se tendrán dos sesiones de eBGP entre ellos

```
Router_PE_IC#
configure terminal
interface POS3/0/4
 description "ENLACE HACIA CPE-IPV6"
 bandwidth 155000
 ip address 10.10.20.2 255.255.255.252
encapsulation ppp
ipv6 address 2001:1208:AAA1::2/126
 ipv6 address FE80:1208:AAA1::2 link-local
…
```

```
Router_PE_IC#
configure terminal
router bgp 8151
neighbor 2001:1208:AAA1::1 remote-as 65535
 neighbor 2001:1208:AAA1::1 description "CPE-IPV6"
address-family ipv6
 neighbor 2001:1208:AAA1::1 activate
 neighbor 2001:1208:AAA1::1 send-community
…
```

La configuración que se agregó para la implementación de la funcionalidad de 6VPE para el servicio de VPN se describe a continuación:

1. Configuración de una sesión de MP-iBGP (Internal BGP) VPNv6 entre equipos PE

```
Router_PE_VPN_1#
configure terminal
router bgp 8151
 neighbor 192.168.20.6 remote-as 8151
 neighbor 192.168.20.6 description "PE_VPN_2"
neighbor 192.168.20.6 update-source Loopback0
address-family vpnv6
 neighbor 192.168.20.6 activate
 neighbor 192.168.20.6 send-community both
…
```

```
Router_PE_VPN_2#
configure terminal
router bgp 8151
 neighbor 192.168.20.5 remote-as 8151
 neighbor 192.168.20.5 description "PE_VPN_1"
neighbor 192.168.20.5 update-source Loopback0
address-family vpnv6
 neighbor 192.168.20.5 activate
 neighbor 192.168.20.5 send-community both
…
```

2. Configuración del AF IPv6 en la definición de la VRF del cliente en el equipo PE

```
Router_PE_VPN_1#
configure terminal
vrf definition CLIENTE
rd 8151:200
 address-family ipv4
  route-target export 8151:200
  route-target import 8151:200
address-family ipv6
  route-target export 8151:200
  route-target import 8151:200
…
```

```
Router_PE_VPN_1#
configure terminal
interface GigabitEthernet1/0/0
 description "ENLACE HACIA CPE-VPNv6"
 bandwidth 1000000
vrf forwarding CLIENTE
 ip address 10.10.30.6 255.255.255.252
ipv6 address 2806:10ff:cafe::2/64

…
```

3. Configuración de una sesión de eBGP (External BGP) IPv6 entre el equipo PE y el equipo CPE del cliente, actualmente ya existe una sesión de External BGP IPv4 entre estos equipos, por lo cual se tendrán dos sesiones de eBGP entre ellos

```
Router_PE_VPN_1#
configure terminal
router bgp 8151
address-family ipv6 vrf CLIENTE
 neighbor 2806:10ff:cafe::1 remote-as 65535
  neighbor 2806:10ff:cafe::1 description "CPE-VPNv6"
  neighbor 2806:10ff:cafe::1 activate
…
```

El diagrama de implementación de las funcionalidades 6PE/6VPE se muestra en la figura 32.

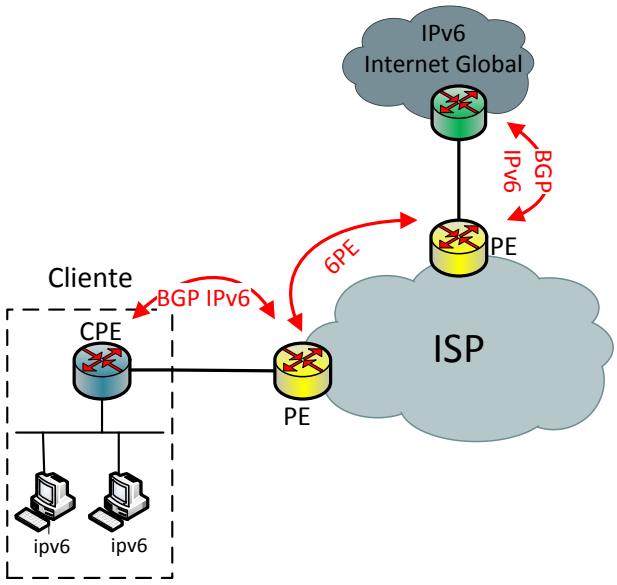

Figura 32. Diagrama de implementación 6PE/6VPE en ISP

La configuración que se agregó para la implementación de la funcionalidad de 6RD para el servicio de Internet Masivo se describe a continuación:

1. Configuración de interfaz Loopback100 definida para el funcionamiento Anycast del equipo 6RD Border Relay

```
configure terminal
interface Loopback 100
 description "LOOPBACK DEFINIDA PARA ANYCAST 6RD"
 ip address 10.10.40.10 255.255.255.255
!
router ospf 64512
network 10.10.40.10 0.0.0.0 area 50
...
```

2. Configuración de túneles hacia los equipos de los clientes (CPEs) y delegación automática del prefijo IPv6 en los equipos dedicados para la funcionalidad de 6RD Border Relay (BR)

```
configure terminal
interface Tunnel1
 description "TUNNEL DEFINIDO PARA 6RD"
 no ip address
 no ip redirects
 ipv6 address 2806:100C::1/64 anycast
 tunnel source Loopback100
 tunnel mode ipv6ip 6rd
 tunnel 6rd prefix 2806:100C::/32
 tunnel 6rd ipv4 prefix-len 0
...
```

3. Anuncio del prefijo 6RD en el protocolo BGP

```
configure terminal
ipv6 route 2806:100C::/32 Tunnel1
!
router bgp 8151
 address-family ipv6
  network 2806:100C::/32
...
```

4. Configuración de una sesión de iBGP (Internal BGP) IPv4 entre el equipo BR y el equipo con la conectividad IPv6 en su región, apoyándose de los equipos RR y utilizando la funcionalidad de 6PE

```
Router_RR#
configure terminal
router bgp 8151
 neighbor 192.168.30.10 remote-as 8151
 neighbor 192.168.30.10 description "BR_6RD"
 neighbor 192.168.30.10 update-source Loopback0
!
 neighbor 192.168.10.2 remote-as 8151
 neighbor 192.168.10.2 description "Router_USA"
 neighbor 192.168.10.2 update-source Loopback0
!
address-family ipv4
  neighbor 192.168.30.10 activate
  neighbor 192.168.10.2 activate
```

```
!
address-family ipv6
  neighbor 192.168.30.10 activate
  neighbor 192.168.30.10 send-community
  neighbor 192.168.30.10 route-reflector-client
  neighbor 192.168.30.10 send-label
!
  neighbor 192.168.10.2 activate
  neighbor 192.168.10.2 send-community
  neighbor 192.168.10.2 route-reflector-client
  neighbor 192.168.10.2 send-label
…
```

El diagrama de implementación de la funcionalidad 6RD se muestra en la figura 33.

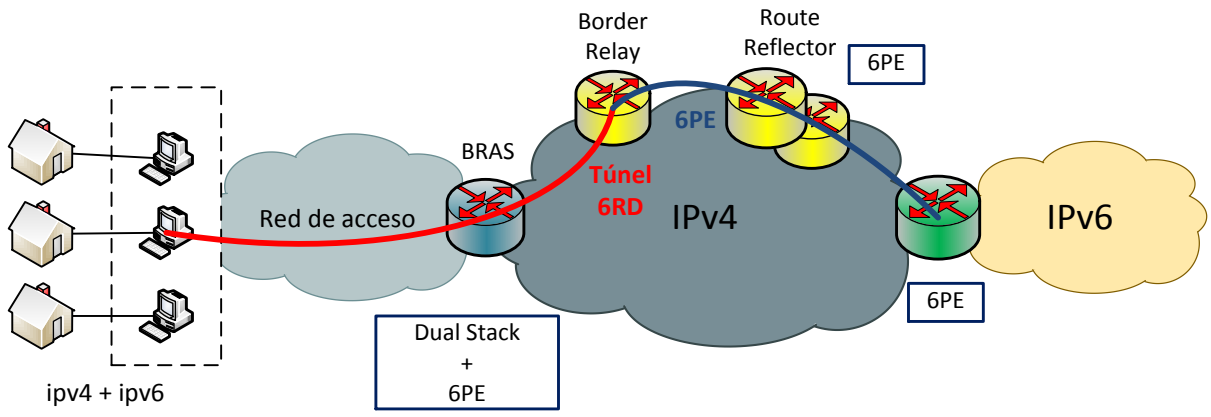

Figura 33. Diagrama de implementación 6RD en ISP

CAPÍTULO 4

PARTICIPACIÓN PROFESIONAL, RESULTADOS Y APORTACIONES

Al principio de este proyecto de adecuación de la red para soporte a IPv6 se identificaron las necesidades de capacitación para los directamente involucrados en dicha transición. Por lo que fue necesario conformar un grupo interdisciplinario con personal de cada una de las áreas involucradas en el proyecto para la impartición de un curso de capacitación de dicha tecnología enfocado al diseño, implementación y resolución de fallas con la finalidad de ser capaces de soportar la operación diaria de la red. Tuve la oportunidad de formar parte de dicho grupo interdisciplinario con lo que pude estar inmerso en todo el avance que se fue dando y en algunos casos tuve la responsabilidad de asignar direccionamiento para los servicios nuevos que se fueron configurando ajustándome a la política definida para la asignación.

La parte del diseño de esta nueva funcionalidad a implementar corrió a cargo del área de Estrategia y Evolución Tecnológica, quienes fueron los encargados de realizar todas las pruebas pertinentes en ambiente de laboratorio para estar en posibilidad de emitir la norma de configuración a usarse para cada una de las plataformas presentes en la red en producción. Dicha norma de configuración constituyó una entrada habilitadora para el proceso en el que cual yo participé, que fue el de implementación durante mi estancia en la Gerencia de Cambios y Configuraciones. Posteriormente, al integrarme a la Gerencia de Soporte Técnico Reactivo mi rol de actividades se enfocó a la resolución de fallas presentadas sobre IPv6, las cuales no hayan podido ser resueltas por el equipo de atención de fallas de primer nivel.

Propiamente, en la fase de implementación, configuré Dual-Stack en los routers de frontera en Estados Unidos, así también se me encomendó la tarea de configurar algunas de las sesiones de BGP que se establecieron contra los equipos de los proveedores internacionales. Posteriormente, realicé la configuración para habilitar la funcionalidad de 6PE y 6VPE entre algunos de los equipos PE de la red de ISP.

En primera instancia, participé en una prueba piloto para ejecutar los movimientos de manera controlada y evaluar el comportamiento y posible impacto que ello generaría a los servicios que ya se encontraban en operación en ese momento. La finalidad fue estructurar de la mejor manera un proceso que nos permitió asegurar la adecuada implementación de los servicios IPv6 sin degradar o afectar el servicio de los clientes actuales.

Para realizar la prueba piloto seleccioné un router en particular de la red de ISP instalado en Estados Unidos para configurar de manera remota la sesión de BGP IPv6 hacia un router de uno de nuestros proveedores internacionales, en mi caso fue hacia un router del proveedor NTT, por lo que fue necesario sostener un audio con personal de dicha empresa para compartir información propia para el establecimiento de la sesión de BGP, tales como: dirección IP a usar, número de sistema autónomo remoto, esquema de ruteo ya sea usando una interfaz Loopback o la interfaz directamente conectada al equipo del otro ISP, lista de redes a compartir a través de la sesión de BGP, número máximo de prefijos a permitir en dicha sesión, entre otros dependiendo cada caso en particular.

Posteriormente, me di a la tarea de habilitar las funcionalidades de 6PE, 6VPE y 6RD en ese mismo router de frontera hacia un router PE en cada caso, al cual se conectaban clientes piloto, uno para cada uno de los servicios ofrecidos. Coordiné, en conjunto con compañeros de otras áreas, ventanas de tiempo para la configuración necesaria entre los equipos CPE-PE. Una vez aplicada la configuración, la mantuvimos en monitoreo y completamos el periodo de validación transcurrida una semana de haber activado los servicios.

Completado el tiempo de prueba, y en coordinación con compañeros de otras áreas, procedí a habilitar a los demás equipos operativos para programar en calendario y ejecutar implementaciones masivas en todos los equipos en operación realizando planes de trabajo por *cluste*r cumpliendo con los tiempos comprometidos por la Alta Dirección, dado que no podían realizarse los movimientos en una sola ventana de tiempo por la gran cantidad de equipos a intervenir.

Durante la implementación en todos los equipos de la red que cubren el territorio nacional, con el apoyo y coordinación entre las diferentes áreas operativas de la empresa, se presentaron infinidad de contratiempos y problemas lo cual me motivó a adoptar una actitud de análisis para poderles dar solución haciendo uso de los conocimientos adquiridos durante mi formación académica en la Facultad de Ingeniería, ya sea internamente o con el apoyo del proveedor de la infraestructura instalada para los casos en los que llegué a detectar defectos de software, comúnmente conocidos como *bugs*, así como cualquier comportamiento anómalo en la operación de los equipos en el ambiente de producción.

En este proyecto, gracias a la participación de todos los equipos de las diferentes áreas operativas, se logró como resultado el haber configurado un total de 1236 equipos de acceso al servicio (PE) para la adopción del protocolo IPv6, que incluyen los equipos que dan soporte a los tres servicios que ofrece la empresa y que son el Internet Corporativo, Internet Masivo y el servicio de red privada virtual VPN.

Con esta implementación, desde ese momento la empresa se encuentra en posición de soportar los servicios IPv6 que los usuarios demandan con base en sus requerimientos para su adopción de IPv6, contando con las premisas necesarias para poder ofrecer el servicio y únicamente atendiendo a la demanda se irán configurando con Dual-Stack los enlaces de acceso de los usuarios para con ello completar la topología extremo a extremo del nuevo servicio IPv6 a soportar.

La siguiente gráfica muestra la distribución de los equipos PE que se habilitaron para cada uno de los servicios ofrecidos:

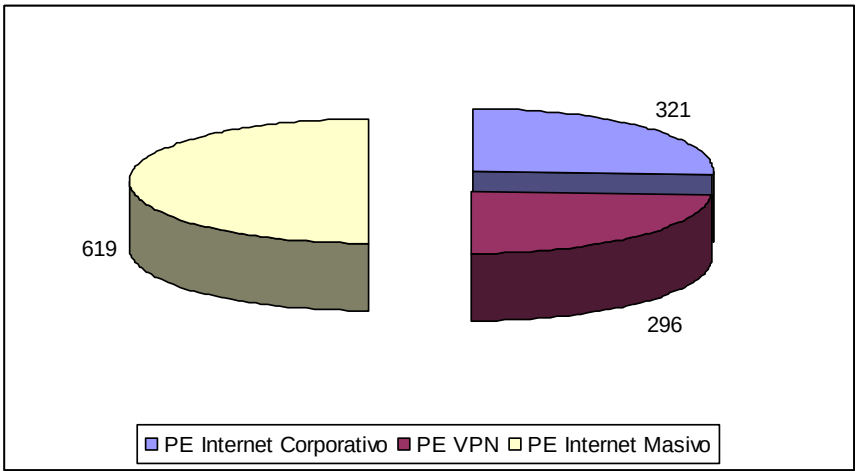

Figura 34. Gráfica de equipos configurados por servicio

La distribución y el detalle de cuántos equipos se encuentran instalados en cada uno de los *clusters* definidos para la red de ISP, por servicio, se plasma en las siguientes tablas:

Cluster	PE Internet Corporativo
Noroeste	5
Norte	46
Noreste	48
Centro_1	77
Centro_2	43
Sur	66
Sureste	36
TOTAL	**321**

Tabla 15. Distribución de PE Internet Corporativo por cluster

Cluster	PE VPN
Noroeste	8
Norte	33
Noreste	45
Centro_1	87
Centro_2	38
Sur	60
Sureste	25
TOTAL	**296**

Tabla 16. Distribución de PE VPN por cluster

Cluster	PE Internet Masivo
Noroeste	0
Norte	68
Noreste	93
Centro_1	179
Centro_2	86
Sur	131
Sureste	62
TOTAL	**619**

Tabla 17. Distribución de PE Internet Masivo por cluster

Con el esfuerzo logrado para la implementación de IPv6, y su coexistencia con la versión actual del protocolo, se da un gran paso en la eficiencia de asignación del direccionamiento, ya que con los 32 bits de las direcciones IPv4 se tiene un límite teórico máximo de 2^{32} direcciones (4.2 billones de direcciones) mientras que en la realidad es mucho menor a dicho valor debido a la distribución jerárquica del espacio de direccionamiento para múltiples capas de redes, después subredes y finalmente hosts. El RFC *1715 (The H Ratio for Address Assignment Efficiency / Authors: C. Huitema / Date: November 1994)* ofrece un análisis de la eficiencia en la asignación de las direcciones, en el cual fue propuesta una escala logarítmica como una medida de dicho factor, la cual fue definida como el cociente H:

$$H = \frac{\log_{10}(\#\text{ de direcciones})}{\#\text{ de bits disponibles}}$$

Con cerca de los 2.4 billones de hosts actualmente en Internet, el cociente H actual es de 0.293, es decir una eficiencia del 29.3% en la asignación del direccionamiento. La medición de eficiencia de asignación para IPv6, con su cantidad masiva de espacio de direcciones, no es calculada basada en el cociente H; un cociente diferente, el cociente HD (*Host Density*), es definido en el RFC 3194 *(The H-Density Ratio for Address Assignment Efficiency An Update on the H ratio / Authors: C. Huitema / Date: November 2001)* y usado para dicho fin:

$$HD = \frac{\log_{10}(\#\text{ de direcciones asignadas})}{\log_{10}(\#\text{ máximo de direcciones por asignar})}$$

El valor "# de direcciones asignadas" medidos en el cociente HD para IPv6 son las direcciones IPv6 para los sitios dentro de una misma empresa (/48) asignados de un prefijo IPv6 de tamaño determinado.

Los bloques de direcciones /48 son aquéllos que se esperan ser asignados por el LIR/ISP a cada usuario final. Por lo que en nuestro caso para el segmento /32 otorgado para la infraestructura de la red, al tener la asignación inicial de 176 subredes /40s, podemos alcanzar a llegar hasta una eficiencia de $\log_{10}(45056)/\log_{10}(65536)=0.966$. Para el caso del segmento /24 que será utilizado para los servicios IP ofrecidos, al tener la asignación inicial de 176 subredes /32s, podemos alcanzar a llegar hasta una eficiencia de $\log_{10}(11534336)/\log_{10}(16777216)=0.977$.

La configuración del protocolo IPv6 en el *backbone* de la red del ISP habilitará a la empresa a participar en este nuevo sector del mercado ofreciendo servicios de nueva generación a los usuarios finales, mientras se continúa operando sin disrupción alguna con la versión 4 de dicho protocolo.

Del mismo modo, se podrá seguir desarrollando soporte a las aplicaciones de los usuarios que trabajen con la nueva versión del protocolo, todo esto alineado a la estrategia definida por el negocio.

CONCLUSIONES

De acuerdo al objetivo establecido al principio del proyecto, se puede afirmar que fue alcanzado de manera exitosa y cumpliendo las expectativas iniciales ya que se tuvo una planeación adecuada, se analizó y diseñó una ruta para alcanzar el objetivo de implementar una opción de transición al protocolo IPv6 que resulta ser confiable y segura, sin poner en riesgo la operación de los servicios actuales ofrecidos a nuestros clientes; y por ende, asegurando el cumplimiento de los niveles de servicio comprometidos, dejando en claro una buena imagen de trabajo en equipo entre las áreas internas a la empresa hacia nuestros clientes actuales y potenciales.

Gracias a los esfuerzos bien plasmados en la planeación del proyecto se pudo definir una política de asignación del espacio de direccionamiento jerárquica y escalable considerando la topología lógica de la red, acorde con las políticas de enrutamiento vigentes y tratando de reducir al máximo el número de anuncios de BGP hacia el Internet global. En un principio la distribución general de direcciones IPs se realizó sin ciertas pautas, dando paso a una estructura mal repartida y desorganizada, surgiendo así una serie de arreglos para intentar solucionar temporalmente el problema.

Ahora, la finalidad es evitar los errores que se detectaron en la operación actual del protocolo IPv4 y que en su sucesor se pretenden erradicar en mayor medida, consiguiendo tener una solución no únicamente a corto plazo, sino también a mediano plazo mientras se da la transición completa hacia IPv6 en un futuro próximo, quizá algunas décadas considerando el tamaño impresionante que tiene actualmente el Internet y las tareas que deben realizarse para alcanzar dicho objetivo teniendo en consideración los recursos de todo tipo, incluyendo el recurso humano, imprescindible para la configuración, operación y mantenimiento de la red de ISP.

Un factor importante y que aseguró el éxito del proyecto representa el aspecto teórico, para el cual fue de vital importancia los conocimientos sólidos adquiridos durante mi formación en la Facultad de Ingeniería y que me dieron la pauta para poder abordar de manera excepcional este proyecto y estar en capacidad de resolver los problemas que se fueron presentando durante su ejecución. La situación para habilitar este nuevo protocolo de primera vista parecía una tarea titánica y con la necesidad de mucha inversión, pero conforme se fue analizando a detalle se pudo ir concretando de manera exitosa gracias a una adecuada planeación, al personal altamente capacitado que labora en la empresa así como también al seguimiento y solución de las problemáticas experimentadas que fueron resueltas de la mejor manera posible.

La adopción exitosa en el mercado de cualquier nueva tecnología depende de su fácil integración con la infraestructura existente sin implicar interrupción en los servicios, así mismo la transición debe ser técnicamente factible y con una buena relación costo-beneficio por lo que la decisión de integrar la nueva versión del protocolo a la red con las funcionalidades de 6PE, 6VPE y 6RD son las idóneas ya que aprovechan las bondades de los protocolos MPLS y MP-BGP, si ambos ya se encuentran implementados en la infraestructura de la red de ISP resultando un enfoque atractivo para la transición de cualquier red de ISP que ya cuente con un *backbone* habilitado con MPLS, dejando en posibilidad de ofrecer servicios tales como redes privadas virtuales de capa 2 (L2) y de capa 3 (L3).

Entre los distintos enfoques para implementar tráfico IPv6 sobre un backbone MPLS, 6PE y 6VPE permiten su implementación con un costo y riesgo bajos. Además, no impactan al core IPv4 ya que IPv6 solamente es activado en los equipos en la frontera, sobre la red existente de MPLS, la cual no es manipulada en lo absoluto por lo que tampoco se requiere entrenamiento adicional para la operación de la red. Los dispositivos habilitados para IPv6 son agregados gradualmente conforme se requiera.

Es un hecho que no hay un día establecido para convertir todo a IPv6, tampoco existe la necesidad de convertir todo de un solo intento al mismo tiempo, además de que no resulta técnicamente factible. Lo importante a destacar es el hecho de que el direccionamiento IPv6, y el protocolo en sí mismo, ha madurado lo suficiente durante casi dos décadas para poder ser implementado y funcionar sin grandes problemas en infraestructura de redes grandes como lo son los proveedores de servicios de Internet.

El desarrollo de IPv6 se irá dando conforme todos los involucrados en dicha tecnología vayan aportando lo necesario para ampliar el abanico de posibilidades para los servicios que se quieran ir ofreciendo. Entre las entidades que juegan un rol importante en el avance de IPv6 tenemos a los pequeños negocios, empresas, proveedores de servicios de Internet, desarrolladores de contenido, entidades de gobierno, así como las autoridades encargadas de la toma de decisiones en el sector de las telecomunicaciones.

Desde mi perspectiva, como egresado de la Facultad de Ingeniería y actualmente inmerso en el campo laboral, considero que los conocimientos que ahí se me transmitieron son excelentes e invaluables, permitieron mantenerme estar en un nivel óptimo para poder competir con los egresados de cualquier otra universidad a nivel mundial, habilitándome una integración transparente al campo laboral y facilitándome la interacción con mis demás compañeros de área gracias a que en la Facultad se promueve bastante el trabajo en equipo al momento de organizar grupos de trabajo para la elaboración de proyectos finales que constituyen parte importante de la evaluación semestral. Todo lo anterior me permitió entender perfectamente el proyecto en el que participé asegurando muy buenos resultados como producto de dicho esfuerzo.

Dado que casi la totalidad de la documentación y literatura en temas de Ingeniería se encuentra disponible en idioma inglés, considero que es de vital importancia el hecho que se imparta dicho idioma como asignatura dentro del plan de estudios de todas las carreras impartidas en la Facultad, ya que incluyendo ese número de horas dentro de las horas de estudio semanales permitirá que los estudiantes salgan mejor preparados en el entendimiento de dicha lengua extranjera, en aspectos importantes tales como la expresión oral de manera fluida, capacidad de escuchar y entender a sus interlocutores sin ninguna complicación independientemente del acento que pudiera llegar a complicarlo, facilidad en la redacción de artículos en idioma inglés para el caso de participar en la redacción de algún artículo de temas afines a la Ingeniería.

Considero también, desde mi perspectiva, que otra cuestión importante a considerar durante la formación de los actuales estudiantes de la Facultad de Ingeniería, y que al momento de mi formación quizá no se desarrolló de manera completa, es el promover que los estudiantes además de conocer los aspectos teóricos de cada una de las asignaturas sean capaces de poderlos expresar tanto de manera escrita como de manera oral sin dificultad alguna hacia otros grupos de personas, inclusive que no se encuentren inmersos en el campo de la Ingeniería. Esto con la finalidad de desarrollar habilidades para una adecuada comunicación al momento de tener que hablar en público, ser capaces de participar y obtener buenos resultados durante una negociación, así como aspectos de delegación de actividades cuando se tiene personal a su cargo.

Personalmente, me considero contento con lo que he logrado hasta el momento en la empresa donde laboro, hasta el momento me he desempeñado en dos áreas de la Dirección de Operaciones de la Red de Datos, dando mi mayor esfuerzo para entregar un trabajo de calidad que pueda permitirme reflejar la formación adquirida durante mi trayectoria académica. He obtenido certificaciones que avalen mis conocimientos poniendo en práctica el autoestudio y me considero motivado con mi trabajo, lo que me ayuda a poner todo de mi parte para hacer las cosas bien y conseguir buenos resultados.

GLOSARIO DE TÉRMINOS

6PE. - IPv6 Provider Edge router over MPLS
6RD. - IPv6 Rapid Deployment
6VPE. - IPv6 VPN Provider Edge router over MPLS
AF. - Address Family
AfriNIC. - African Network Information Center
APNIC. - Asia Pacific Network Information Center
ARIN. - American Registry for Internet Numbers
AToM. - Any Transport ver MPLS
BGP. - Border Gateway Protocol
BR. - Border Relay
CCNA. - Cisco Certified Networking Associate
CCNP. - Cisco Certified Networking Professional
CE. - Customer Edge router
CIDR. - Classless Inter-Domain Routing
CPE. - Customer Premises Equipment
CPU. - Central Processing Unit
CRS. - Carrier Routing System
DA. - Destination Address
DARPA. - Defense Advanced Research Projects Agency
DHCP. - Dynamic Host Configuration Protocol
DNS. - Domain Name System
DoS. - Denial of Service
GRE. - Generic Routing Encapsulation
IANA. - Internet Assigned Numbers Autority
ICMP. - Internet Control Message Protocol
IDE. - Internet Directo Empresarial
IEC. - International Electrotechnical Commission
IETF. - Internet Engineering Task Force
IGP. - Interior Gateway Protocol
IOS. - Internetwork Operating System
IOS-XR - Internetwork Operating System XR
IPv4. - Internet Protocol versión 4
IPv6. - Internet Protocol versión 6
IR. - Internet Registry
ISATAP. - Intra-Site Automatic Tunnel Addressing Protocol
ISO. - International Organization for Standardization
ISP. - Internet Service Provider
ITIL. - Information Technology Infrastructure Library

JNCIA-Junos	-	Juniper Networks Certified Associate Junos
JNCIS-SP	-	Juniper Networks Certified Specialist – Service Provider
LACNIC.	-	Latin American and Caribbean Network Information Center
LAN.	-	Local Area Network
LDP.	-	Label Distribution Protocol
LIR.	-	Local Internet Registry
MP-BGP	-	Multi Protocol BGP
MPLS.	-	Multi Protocol Label Switching
MTU.	-	Maximum Transmission Unit
NAT/PAT.	-	Network Address Translation/Port Address Translation
NAT-PT	-	Network Address Translation - Protocol Translation
NIR.	-	National Internet Registry
OLA.	-	Operational Level Agreement
OSA.	-	Operational Support & Analysis
OSI.	-	Open Systems Interconnection
OSPF.	-	Open Shortest Path First
P.	-	Provider router
P2P.	-	Peer to peer
PE.	-	Provider Edge router
PMTUD.	-	Path MTU Discovery
POP.	-	Point of Presence
QoS.	-	Quality of Service
R&S.	-	Routing and Switching
RCV.	-	Release Control & Validation
RFC.	-	Request For Comments
RIPE-NCC	-	Réseaux IP Européennes Network Coordination Center
RIR.	-	Regional Internet Registry
RPV.	-	Red Privada Virtual
RR.	-	Route Reflector
SA.	-	Source Address
TCP.	-	Transmission Control Protocol
TE.	-	Traffic Engineering
TICs.	-	Tecnologías de la Información y Comunicaciones
TTL.	-	Time To Live
UDP.	-	User Datagram Protocol
VLSM.	-	Variable Length subset Masking
VPN.	-	Virtual Private Network
WAN.	-	Wide Area Network

BIBLIOGRAFÍA

LIBROS:

- Manual de inducción Red Uno
- Código de ética. El valor de lo que se debe ser…y hacer. Red Uno
- IPv6 Fundamentals, Design, and Deployment. Student Guide. Cisco Systems, 2010
- Deploying IPv6 Networks. Popoviciu, Levy-Abegnoli, Grossetete. Cisco Press, 2006
- IP Address Management: Principles and practice. Timothy Rooney. Ed. IEEE Press
- Understanding IPv6. Joseph Davies. Ed. Microsoft Press. 2a edición, 2008

PÁGINAS WEB:

- http://www.ipv6actnow.org
- http://www.worldipv6launch.org
- http://www.iana.org
- http://www.ripe.net
- http://www.lacnic.net/web/lacnic/manual-4
- http://www.ipv6tf.org
- http://www.mx.ipv6tf.org
- http://bgp.potaroo.net
- http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html
- http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/aag_c45-625513.pdf
- http://ciscovoiceguru.com/1907/deploying-ipv6-in-a-cisco-uc-environment-part-3/