# DISEÑO DE LABORATORIO DE MECANISMOS DE CONVIVENCIA IPV6 E IPv4 PARA LA UNIVERSIDAD PILOTO DE COLOMBIA

**FABIOLA MOSQUERA HERNÁNDEZ**

**UNIVERSIDAD PILOTO DE COLOMBIA**

**FACULTAD DE INGENIERÍA**

**PROGRAMA DE INGENIERÍA DE TELECOMUNICACIONES**

**BOGOTÁ D.C**

**OCTUBREDE 2011**

# DISEÑO DE LABORATORIO DE MECANISMOS DE CONVIVENCIA IPV6 E IPv4 PARA LA UNIVERSIDAD PILOTO DE COLOMBIA

**FABIOLA MOSQUERA HERNÁNDEZ**

COD 620065

Proyecto de grado para optar por el título de Ingeniero de Telecomunicaciones.

Director: M.Sc(c) Ingeniero de sistemas

**RAFAEL LEONARDO OCHOA URREGO**

Semilleros de investigación del programa de Telecomunicaciones

Grupo de Investigación:

Semillero IPv6 2010 - 2011

**UNIVERSIDAD PILOTO DE COLOMBIA**

**FACULTAD DE INGENIERÍA**

**PROGRAMA DE INGENIERÍA DE TELECOMUNICACIONES**

**BOGOTÁ D.C**

**OCTUBREDE 2011**

*Dedicatoria*

*A Dios el ser que me ha brindado la fortaleza y sabiduría para llevar a cabo este proyecto.*
*A mi amado esposo, que siempre ha creído en mí, me ha apoyado en todos los aspectos de mi vida. Desde que estamos juntos la vida es más bella y florece para mí.Gracias amor.*
*A mis padres que me formaron con buenos valores y principios y me han apoyado toda mi vida.*

**Agradecimientos**

Al Ingeniero Rafael Leonardo Ochoa director de este proyecto de grado, quien durante su estancia en la Universidad apoyóy fomentóa los estudiantes a la investigación.

Nota de aceptación

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma Jurado

_____

Firma Jurado

**CONTENIDO**

**pág**.

## LISTADO DE FIGURAS

## LISTADO DE TABLAS

## LISTADO DE ANEXOS

# 1. INTRODUCCIÓN

Las aplicaciones y servicios que usamos en el día a día de nuestras vidas, se encuentran cada vez más focalizadas en el uso de Internet como medio de comunicación. Servicios como mensajería instantánea, correo electrónico y redes sociales (entre otros) utilizan la red de redes para transportar los paquetes de información que son intercambiados por las aplicaciones que usamos. Debido a la importancia que actualmente representa Internet para el mundo, es oportuno exponer las limitaciones que se han venido haciendo evidentes acerca del protocolo de red que la soporta. IPv4 *(Internet Protocol* v4) ha constituido los cimientos de la red de redes durante más de 25 años, tiempo durante el cual se ha evidenciado un crecimiento exponencial de servicios y aplicaciones que demandan no sólo direcciones válidas para su acceso, sino que también requieren de características inherentes a la calidad como son flexibilidad, estabilidad y escalabilidad. Entre las mencionadas características, algunas están completamente ausentes en la versión actual del protocolo y el espacio de direcciones se agota con cada día que pasa; por esta razón y aproximadamente desde el año 1998, la IETF (*Internet Engineering Task Force*) ha asignado recursos y grupos de investigación, que se encuentran desarrollando la publicación del RFC 2460, "*Internet Protocol, versión* 6 (IPv6)" en el cual está contenida la especificación de una nueva versión del protocolo de Internet que entrará a reemplazar el actual IPv4.

IPv6 suple las necesidades que han surgido a partir de las falencias que presenta IPv4, en teoría permitiría asignar una dirección única a cada habitante de la tierra, provee soporte para la utilización de dispositivos móviles, entre otras. En cuanto a las características de calidad, IPv6 presenta nuevas formas de utilización del ancho de banda disponible, que resulta en una transmisión de datos eficiente, gracias a sus algoritmos para enrutamiento de tráfico. Sin embargo, es necesario tener en consideración que IPv4 no puede ser eliminado del escenario de un momento a otro, es tan grande su cobertura que se están estableciendo mecanismos de convivencia, que permitan la implementación de IPv6 sin impactar negativamente los servicios y aplicaciones que funcionan en la actualidad.

Este documento pretende ser un punto de entrada al mundo de IPv6 y de algunos de los mecanismos de transición y convivencia que están siendo implementados para llevar a cabo la migración. Es importante poner en consideración de la docencia, que las generaciones venideras de ingenieros de telecomunicaciones, deberán tener el conocimiento teórico y práctico para afrontar el reto que está impactando al mundo; se presenta entonces un marco teórico que servirá de referencia para introducir conceptos básicos de IPv6, también se establece un conjunto de guías para el desarrollo de talleres prácticos, que refuercen la teoría y permitan a los estudiantes tener un primer contacto con los dispositivos y la configuración que puede ser aplicada en estos últimos.

# 2. DEFINICIÓN DEL PROBLEMA

El crecimiento exponencial de la demanda de servicios y aplicaciones ofrecidos a través de Internet que se ha presentado durante los últimos años, muchas de éstas sin la planificación requerida, hace evidente que el protocolo de comunicaciones IPv4, sobre el cuál operan las redes a nivel mundial, comienza a presentar limitaciones y deficiencias para responder adecuadamente a dicha demanda. Debido a esto, el Network Working Group (NWG) sugiere en el documento RFC2460[1]una nueva versión del protocolo de comunicaciones denominado IPv6, con el cuál aseguran suplir las necesidades actuales y que permitiría la continuidad demandada actualmente por la red mundial.

De acuerdo a esto, es evidente que el mundo debe cambiar y migrar hacia el nuevo protocolo de comunicaciones; donde la comunidad académica que enmarca a los Ingenieros de Telecomunicaciones, sea la encargada de formar y especializar a los futuros profesionales para responder a las necesidades y exigencias tecnológicas que presenta la demanda futura de la industria. Por esta razón, este proyecto de investigación busca responder ¿Cómo debería ser el diseño de un laboratorio práctico en IPv6 y mecanismos de convivencia con IPv4, de manera que contribuya a la construcción de conocimiento en el programa académico de Telecomunicaciones de la Universidad Piloto de Colombia?

## 2.1 ANTECEDENTES DEL PROBLEMA

EI protocolo IPv4 comienza a dar señales de impotencia, con más de 25 años, la versión 4 del protocolo de Internet (IP) ya no puede seguir brindando respuestas adecuadas y atendiendo la actual demanda de servicios.

El paulatino agotamiento de las direcciones IP disponibles es un proceso que culminará en unos pocos años o meses, de acuerdo al actual ritmo de crecimiento de Internet.

Una dirección IP está formada por cuatro grupos de 8 bits; las direcciones IP son útiles para la identificación de cualquier dispositivo que soporte el protocolo TCP/IP, de esta forma

[1] Network Working Group. Request for Comments: 2460.December 1998.[en línea]. Disponible en:<http://www.rfc-es.org/rfc/rfc2460-es.txt>

cada uno de ellos obtiene una identificación única dentro de la red en la cual se encuentre y permiten que la información enviada llegue efectivamente al destino deseado.

*"Sin embargo ante el enorme crecimiento de usuarios de Internet, quienes día a día presentan necesidades cada vez mayores y en menores tiempos de respuesta, la comunidad de Internet observa que IPv4 se ha vuelto insuficiente para seguir siendo el soporte de Internet. El tiempo de vida de IPv4 se ha extendido gracias a técnicas tales como reutilización de direcciones, uso temporal de asignaciones y técnicas de NAT. Si bien estas técnicas parecen incrementar el espacio de direcciones y satisfacer el crecimiento de la red, fallan en atender las necesidades de las nuevas aplicaciones"*[2].

En 1992 el grupo Internet Engineering Task Force(IEFT), convocó a la comunidad de Investigadores para estudiar alternativas a IPv4, en 1995 y como primer resultado la comunidad entrego un resultado llamado IPv6 (Internet Protocol versión 6), el cual más adelante (1998) mejoran y definen en el RFC 2460.

Este nuevo protocolo será atractivo en los sectores de redes inalámbricas, juegos, redes de Investigación, organismos militares y gobierno, y en general para toda la comunidad interesada en publicar u operar servicios en la red de redes.

[2] Codarec6: an ipv6 test bed" – Laboratorio de estudio, diseño, desarrollo, implementación, ensayo y capacitación del protocolo de internet versión 6. Carlos Taffernaberry, Alejandro Dantiacq Picolella, Gustavo Mercado y Adrián Francisconi. [en línea]. Disponible en: < http://codarec6.frm.utn.edu.ar/publicaciones/papers/CACIC-2006.pdf>.

# 3. JUSTIFICACIÓN

Internet se ha convertido en uno de los recursos más utilizados a nivel mundial para la adquisición o venta de servicios. El número de organizaciones que ofrecen o utilizan servicios en la red de redes ha aumentado exponencialmente en los últimos años y se empiezan a hacer evidentes las limitaciones que presenta el protocolo IPv4, sobre el cuál reposa el funcionamiento de Internet. Dentro de estas limitaciones, se encuentran la escasez de posibles direcciones IP que pueden ser asignadas. Según reportes del Latin American and Caribbean Internet Addresses Registry (LACNIC) y The Number Resource Organization (NRO), el espacio de direcciones remanente está por debajo del 5% [34]. Este hecho es una amenaza para la red de operaciones a nivel mundial, por lo que los Proveedores de Servicios de Internet se encuentran adelantando proyectos de migración a la versión 6 del protocolo de comunicaciones[5]cómo consecuencia, las organizaciones interconectadas a la red se verán obligadas a adelantar proyectos de transición, con el fin de minimizar el impacto que este cambio pueda imponer sobre los servicios de Internet.

En Colombia el Ministerio de Tecnologías de Información y Comunicaciones (Ministerio TIC), interesado por reducir la brecha digital en la que actualmente se encuentra el país, adelanta el proyecto *Plan Vive Digital*[6], con el cual busca fortalecer los servicios de acceso a Internet y Televisión abierta en el país. El Min TIC considera dentro de sus proyectos los cambios tecnológicos que presenta el mercado; apoyándose en la academia, la industria e instituciones dedicadas a la investigación se apropia de conocimientos para lograr los objetivos del proyecto. Un buen ejemplo de ello, fue la participación del Min TIC en el I Foro Día Mundial IPv6 Capítulo Colombia, en el cuál invitaron al país a acoger el protocolo IPv6[7].

"*Los Ingenieros de Telecomunicaciones de la Universidad Piloto de Colombia, comprometidos con los procesos de desarrollo del país, deben ser pioneros en la implementación, investigación y aplicabilidad de nuevas tecnologías que contribuyan al*

---

[3] LACNIC - Latín American and Caribbean Internet Addresses Registry) en español Registro de Direcciones de Internet para América Latina y Caribe. [en línea]. Disponible en: <http: //lacnic.net/sp/anuncios/345.html>

[4]RNO The Number Resource Organization en español Organización de registro de números. [en línea]. Disponible en: http://www.nro.net/news/remaining-ipv4-address-space-drops-below-5.

[5]Periódico el Espectador ``Elespectador.com/Cartagena''. En enero Comienza la implementación del protocolo Ipv6 en Colombia. Diciembre 6 de 2010. última fecha de consulta, Marzo 2011. [en línea]. Disponible en: http://www.elespectador.com/articulo-238991-enero-comienza-implementacion-de-protocolo-IPv6-colombia.

[6]Ministerio de Tecnologías de la información y las comunicaciones. Noticias. última fecha de consulta Marzo 2011. [en línea]. Disponible en: <http://www.mintic.gov.co/news.asp ?articleId=206>.

[7]Renata. Red Nacional Académica de Tecnología Avanzada. Junio 9 2011. Última fecha de consulta Septiembre 2011. [en línea]. Disponible en: http://www.renata.edu.co/index.php/component/content/article/5-noticias/2297-i-foro-dia-mundial-IPv6-capítulo-colombia-reunio-a-la-comunidad-academica-y-tecnica-del-pais-y-de-america-latina.html>.

*crecimiento de la ingeniera en Colombia"*[8]. Es allí donde la academia cumple un papel importante. En aras de cumplir este objetivo se considera necesaria la creación de espacios que complementen la formación de los futuros ingenieros, quienes a su vez llevarán su experiencia y conocimientos para atender las necesidades que demande la industria e innovarán para mejorar la prestación de los servicios.

[8] Comité de Autoevaluación y Currículo, Universidad Piloto de Colombia. Proyecto Educativo del Programa PEP. [documento físico] versión 2, (2010).

# 4. OBJETIVOS

## 4.1 OBJETIVO GENERAL

- Diseñar e implementar un laboratorio sobre los mecanismos de convivencia entreIPv6 e IPv4 para la Universidad Piloto de Colombia

## 4.2 OBJETIVOS ESPECÍFICOS

- Construir un marco teórico de los aspectos principales de IPv6 y de los mecanismos de convivencia de IPv6 con IPv4.
- Diseñar los laboratorios teórico - prácticos.
- Desarrollar material de apoyo docente para la orientación del laboratorio.
- Realizar 1 guía de laboratorio para la configuración inicial de IPv6 y 3 guías de laboratorio para la implementación de dos mecanismos de convivencia de Ipv6 con IPv4.

# 5. DISEÑO METODOLÓGICO

El desarrollo de las guías se llevó a cabo siguiendo minuciosamente las etapas expuestas a continuación:

- Establecimiento de un marco teórico acerca de IPv6, comparación con la versión actual IPv4 y un análisis de algunos de los mecanismos de transición.
- Implementación práctica de la teoría, por medio de la ejecución de simulaciones por software y pruebas de laboratorio en la universidad.
- Análisis de hardware y ejecución de pruebas de concepto en dispositivos específicos.

El marco teórico se estableció, haciendo un estudio inicial del nuevo protocolo IPv6, como fue concebido, las razones que llevaron a su creación, cuáles son las diferencias que presenta frente a la versión actual y las técnicas que están siendo estudiadas e implementadas para su globalización.

Se recopilaron las definiciones y conceptos que constituyen el nuevo protocolo de Internet. Se explicó cómo la IETF en el RFC 2460 expone las consideraciones que se tuvieron al diseñar IPv6, desde la longitud de las direcciones hasta los atributos de calidad y como éstos afectarían el desempeño de las redes funcionando bajo este protocolo. Teniendo en mente el objetivo principal de este documento, se realizó un estudio de las principales diferencias y ventajas que son ofrecidas por la nueva versión con respecto a su antecesor, destacando, por ejemplo, el espacio de direcciones que se hace más estrecho a cada día con el surgimiento de nuevos servicios de Internet, o como los avances tecnológicos en esos mismos servicios comienzan a demandar recursos más poderosos para su correcto funcionamiento.

Posteriormente, se realizó una investigación sobre cómo se ha pensado llevar a cabo la implementación del nuevo protocolo de Internet a nivel mundial, teniendo en cuenta que la totalidad de la red de redes se encuentra soportada sobre el actual protocolo IPv4. Como resultado de éste estudio, se explican algunos de los mecanismos de transición que están siendo considerados e implementados a nivel mundial, resaltando siempre la premisa de que la versión actual no puede ser eliminada repentinamente, principalmente debido a las consecuencias en cuanto a la prestación de los servicios que funcionan sobre ella. La comunidad es consciente de este hecho y se han hecho propuestas de convivencia mutua para llevar a cabo una transición transparente y segura.

Concluida la teoría relevante sobre el tema, se realizaron pruebas de concepto en las que, haciendo uso de dispositivos representativos a aquellos existentes dentro de las laboratorios de la Universidad Piloto de Colombia y de simulaciones basadas en software para la configuración de redes de computadores, se establecieron los diferentes pasos que conforman las guías de laboratorio para la asignatura de Redes de Computadores del programa de Ingeniería de Telecomunicaciones del establecimiento mencionado. Las guías

fueron validadas por medio del desarrollo de laboratorios piloto, utilizando los recursos del laboratorio para tal fin.

# 6. MARCO TEÓRICO

## 6.1 INTRODUCCIÓN A IPV6

IPv6 es el resultado de una investigación realizada por la durante el año 1994, llevada a cabo por los ingenieros Steve Deering y Craig Mudge. Surge como respuesta a la deficiencia en la cantidad de direcciones de red que ha venido soportando el protocolo IPv4, que a medida que pasa el tiempo, se hacen más escasas. Entre las características que marcan la evolución que ofrece IPv6 encontramos: la escalabilidad para la asignación de un mayor número de direcciones de red, mejoras en seguridad y facilidad de configuración[9].

Actualmente, el estado de alerta por la escases de direcciones de red disponibles en IPv4, ha alertado y motivado a la migración a nivel global hacia el nuevo estándar. Son muchas las compañías que ya están trabajando en productos que hacen uso del nuevo estándar de direccionamiento, como por ejemplo, estándares para redes móviles que se encontrarán basados en su totalidad en protocolos de Internet. Sin embargo, la actualización de la red al nuevo protocolo es un proceso que no se da de un día para el otro.-La transición de protocolos no debe afectar el funcionamiento de los servicios actuales, por lo que se hace necesaria la implementación de un mecanismo híbrido, que permita la convivencia de los dos protocolos por el tiempo que tome la migración total y definitiva[10].

A continuación se explica con mayor detalle las características, arquitectura y servicios que trae la nueva versión del protocolo de Internet, junto con los mecanismos de transición y convivencia que están siendo implementados actualmente.

---

[9] Shannon McFarland, Muninder Sambi, Nikhil Sharma, and Sanjay Hooda. IPv6 for Enterprise Networks. IPv6 for Enterprise Networks. Indianapolis : s.n., 2011, págs. 2,3.

[10] Loshin, Pete. IPv6: Theory,Protocol,and Practice SECOND EDITION. San Francisco : Morgan Kaufmann Publishers is an Imprint of Elsevier, 2004. pág. Capítulo 8. Vol. 2.

## 6.2 PAQUETE IPV6

A diferencia del paquete IPv4, que consta de 32 bits para la asignación de las direcciones de red, IPv6[11] soporta hasta 128 bits que se distribuyen de la siguiente forma:

Los primeros 48 bits definen el espacio de direcciones básico que se da a una organización.

16 bits son utilizados para establecer las direcciones de las subredes (ofreciendo hasta 65.535 posibles subredes.)

Los 64 bits restantes son utilizados para la asignación de direcciones por máquina.

El paquete[12] de IPv6 tiene fundamentalmente dos partes a saber: a) la cabecera y b) los datos. A continuación se describirán los campos incluidos en la cabecera y las cabeceras de extensión.

### 6.2.1 Cabecera.

La cabecera está definida en los primeros 40 bits y se encuentra distribuida como se ve en la tabla 1.

| Nombre del Campo | Tamaño | Descripción |
|---|---|---|
| ***Version*** | 4 bits | Este campo define la versión del protocolo 4 o 6 que permite al software establecer que tratamiento se dará al paquete de datos. Algunas aplicaciones en la actualidad, asumen por defecto que todo paquete venidero corresponde a la versión 4 y se saltan dicha verificación. |
| ***Differentiated Services*** *(DS)* | 6 bits | De los seis bits que componen este campo, dos están reservados para uso futuro. En IPv4 era conocido como Priority, pero para la nueva versión, su nombre ha sido cambiado a *Traffic Class*. |

[11] Network Working Group. Request for Comments: 2460 Internet Protocol, Version 6 (IPv6). December 1998. [en línea]. Disponible en: http://www.rfc-es.org/rfc/rfc2460-es.txt.

[12] Understanding Ipv6 Second Edition. Joseph Davies. Body Part Number: X14-31167. Library of Congress Control Number: 2007940506. 2008. Páginas 86-91. [Recurso Físico].

| Nombre del Campo | Tamaño | Descripción |
|---|---|---|
| ***Flow Label***. | *20 bits* | Utilizado para identificar paquetes que pertenecen a un conjunto específico o sesión concreta entre dos hosts. Un ejemplo de este caso sería una sesión de transmisión de video en línea, donde se puede establecer la tolerancia al retardo entre paquetes, entre otras características inherentes al servicio |
| ***Payload Length*** | *16 bits* | Especifica el tamaño real del paquete, excluyendo los 40 bits de la cabecera. El paquete más grande que puede ser concebido bajo este esquema es de 65.575 bits, de los cuales 65.535 son codificables. Caberesaltar que la posibilidad de transmisión de paquetes tan grandes puede significar mejoras en rendimiento, en cuanto a que son menos paquetes los que deben ser procesados dando espacio a los enrutadores para dar prioridad a paquetes más pequeños o a realizar otras tareas. Si se encuentran encabezados extendidos su longitud va incluida en este campo |
| ***Next Header*** | 8 bits | Indica el protocolo que es utilizada en el paquete IPv6. Los protocolos son identificados por código que son administrados por la IANA *Internet Assigned Numbers Authority* y relacionan protocolos de más alto nivel, como es el caso de TCP, o protocolos de extensión del mismo IPv6. |
| ***Hop Limit*** | 8 bits | Define el número de saltos que le son permitidos a un paquete IPv6 a nivel de red. Se inicializa con un valor de 255 y es decrementado en 1 cada vez que es procesado por un enrutador. Si este número llega al valor cero 0, el paquete es descartado. |
| ***Source Address*** | 128 bits | Dirección IPv6 del nodo origen del paquete. |
| ***Destination Address*** | 128 | Dirección IPv6 del nodo destino para el paquete. Para el caso de IPv6, esta dirección podría hacer referencia a un nodo intermediario diferente del destino final, de acuerdo a los encabezados extendidos que hayan sido especificados. |

Tabla 1. Campos de la cabecera.Creación propia.

### 6.2.2 Cabeceras de Extensión.

La extensibilidad del protocolo IPv6 reside en este fragmento de la cabecera, donde se definen funcionalidades que deberán ser tratadas por los enrutadores compatibles. A la fecha, se han definido ocho cabeceras que son resumidas en la tabla 2 descrita a continuación:

| Nombre del Campo | Descripción |
|---|---|
| ***Hop-by-Hop*** | Define información opcional que debe ser tratada por cada nodo participante en la ruta del paquete. Dentro de éste mismo, se han definido dos opciones a saber:<br>• ***Jumbo Payload.*** Anuncia al enrutador que los datos contenidos en *Jumbograms*, que son paquetes cuyos datos exceden los 65.535 octetos. El Enrutador debe estar condicionado para el manejo de éste tipo de paquetes, de lo contrario un error deberá ser notificado.<br>• ***Enrutador Alert.*** Permite entregar información a enrutadores dentro de la ruta del paquete, que sean diferentes al destino real indicado en la cabecera. |
| ***Routing.*** | Permite indicar nodos específicos que serán visitados por el paquete. Cada vez que el paquete alcanza un nodo, el enrutador verifica el valor de este campo, direccionando el paquete al siguiente nodo en la lista. Este procedimiento se repite hasta que el paquete llega a su destino final. |
| ***Fragment.*** | Se utiliza para la fragmentación de paquetes que exceden el tamaño de la MTU definida entre los nodos fuente y destino. Los siguientes campos son definidos por la cabecera:<br>• ***Fragment Offset.*** Es un entero de 13 bits que indica la posición de los datos del paquete dentro del bloque fragmentado completo. Cuando el valor es 0 los datos del paquete corresponden al primer fragmento, mientras que un valor de 100 indica que los próximos fragmentos corresponden a 800 octetos de datos pertenecientes al mismo paquete.<br>• ***More Fragments Flag*** *(M).* Cuando el valor de este campo es 1, indica que hay más fragmentos que vienen en los paquetes entrantes; un valor de 0 identifica al fragmento actual como el último del bloque de datos.<br>• ***Identification Field****.* Identifica cada fragmento de manera única durante el tiempo de vida del paquete. |

| | |
|---|---|
| | Todos los fragmentos que pertenecen a un mismo paquete comparten el valor de este campo.<br>• ***Destination Options***. Lleva información que ha de ser analizada por el nodo destino del paquete. Actualmente solo han sido implementadas opciones para el relleno del encabezado en un límite definido a 64 bits, que solo será utilizado en caso de ser requerido.<br>• ***Authentication*** *(AH)*. Provee mecanismos para el cálculo de un checksum a nivel criptogtráfico de las distintas partes del paquete IPv6.<br>• ***Encapsulating Security Payload*** *(ESP)*.Es el último encabezado sin encriptar de todo paquete IPv6. Indica que el resto de la carga viene encriptada y provee información para que el destino del paquete esté en capacidad de interpretarla. |

Tabla 2.Campos de la cabecera de extensión. Creación Propia.

## 6.3 ARQUITECTURA DE DIRECCIONAMIENTO

Desde su primera publicación en el año 1995, bajo el número de RFC 1884[13]denominado "Arquitectura de Direccionamiento de IPv6", es sabido que IPv6 fue concebido con la idea de utilizar identificadores para red de 128 bits. Adicionalmente, se definieron cuatrotipos de direcciones entre las cuales se encuentran las direcciones Unicast,Unicast con IPv4 embebido, multicast y anycast.

Las direcciones Unicastse utilizan como identificador para una única interfaz. Un paquete que es enviado a una dirección unicast, es entregado únicamente a la interfaz que sea identificada por la misma. Estas direcciones tienen una clasificación adicional que se explica en la tabla 2.

[13] Network Working Group. Request for Comments: 1884. IP Version 6 Addressing Architecture. December 1995. [en línea]. Disponible en: <http://tools.ietf.org/rfc/rfc1884.txt>.

| Tipo de Dirección | Descripción |
|---|---|
| ***Global.*** | Estas son direcciones únicas a nivel global y pueden ser enrutadas a través de Internet. |
| ***Link Local. Site Local.*** | Estas son destinadas a direccionar un vínculo simple, para propósitos como el de auto-configuración, descubrimiento de vecinos o cuando no hay enrutadores presentes. |
| ***Site Local*** | Estas direcciones permiten dirigir paquetes dentro de un sitio, red u organización. Los paquetes que son enviados a estas direcciones no deben salir del sitio. |

Tabla 3.Tipos de direcciones Unicast. Creación Propia.

Por otro lado se encuentran las direcciones Unicast with embedded IPv4 addresses or encoded NSAP addresses.IPv6 fue diseñado pensando en la interoperabilidad con diferentes capas de red, entre esas IPv4, direcciones *NetWare/IPX* definidas por Novell en el RFC 2373[14], *Network Service Access Point (NSAP)* usadas con el protocolo OSI *Connectionless Network Protocol (CLNP)* como se explica en el RFC 3513[15], entre otros.

***Multicast*** Un identificador asignado a un conjunto de interfaz que normalmente, pertenecen a nodos diferentes. Un paquete enviado a una dirección *multicast* será entregado a todas las interfaces que estén identificadas por la misma.

***Anycast*** La diferencia con la anterior, radica en que un paquete que sea enviado a una dirección anycast, es entregado a solo una de las interfaces identificadas por la misma, usualmente escoge la más "cercana", de acuerdo a la definición de distancia[16] dada por el protocolo de enrutamiento. Cabe anotar que una dirección unicast puede ser especificada como anycast, siempre y cuando todos los nodos configurados para responder a dicha dirección, tengan conocimiento de que de hecho son anycast y no lo unicast[17].

---

[14] Network Working Group. Request for Comments: 2373. IP Version 6 Addressing Architecture. July 1998. [en línea]. Disponible en: http://www.ietf.org/rfc/rfc2373.txt.

[15] Network Working Group. Request for Comments: 3513. Internet Protocol Version 6 (IPv6) Addressing Architecture. April 2003. [en línea]. Disponible en: http://http://www.ietf.org/rfc/rfc3513.txt.

[16] Cisco System Inc. Cisco Networking Academy. CCNA Exploration 4.0. Diccionario de conceptos. [Definición: *"Clasificación de la confiabilidad de una fuente de información de enrutamiento]."*

[17] Loshin, Pete. IPv6: Theory,Protocol,and Practice SECOND EDITION. San Francisco : Morgan Kaufmann Publishers is an Imprint of Elsevier, 2004. pág. Capítulo 8. Vol. 2

Debido a los problemas que causan las direcciones de *Broadcast* en IPv4, estas han sido eliminadas y reemplazadas por *multicast* y *anycast* en la versión 6. Esta función es realizada enviando paquetes a la dirección de todos los nodos de *multicast*.

### 6.3.1 Representaciónde las DireccionesIPv6.

El formato de las direcciones IP establecidas por IPv6, difiere bastante de la versión anterior en cuanto a que las direcciones IPv4 constan de cuatro valores decimales entre 0 y 255 separados por puntos (XXX.XXX.XXX.XXX), mientras que IPv6 utiliza ocho valores de 16 bits separados por el símbolo dos puntos (XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX). La figura 1 muestra un ejemplo de las representaciones más comunes.

| Tipo | Estándar | Comprimida |
|---|---|---|
| Unicast | 1080:0:0:0:8:800:200C:417A | 1080::8:800:200C:417A |
| Multicast | FF01:0:0:0:0:0:0:101 | FF01::101 |
| Loopback | 0:0:0:0:0:0:0:1 | ::1 |
| Sin especificar | 0:0:0:0:0:0:0:0 | :: |

Figura 1. Representaciones estándares y comprimidas de direcciones IPv6[18]

**6.3.1.1 Tipos de Direcciones Unicast Especiales**. Las direcciones *Unicast* tienen una subdivisión especial para complementar la arquitectura de direccionamiento y son explicadas a continuación:

***Unspecified***. La dirección 0:0:0:0:0:0:0:0 es denominada la dirección sin especificar. En general no debe ser asignada a ningún nodo en particular, por que indica la ausencia de una dirección. ***Loopback***. La dirección de *Loopback* es utilizada por un nodo para enviar paquetes IPv6 a sí mismo. Se identifica de la forma 0:0:0:0:0:0:0:1 y se espera que los paquetes enviados a dicha dirección se encuentren limitados por el entorno de la interfaz local, lo que quiere decir que no van a abandonar el nodo actual. Cualquier enrutador que encuentre un paquete IPv6 dirigido a la dirección de loopback, deberá descartarlo inmediatamente.

[18] Loshin, Pete. Capítulo 8, página 145. [Recurso Físico].

**6.3.1.2 Identificador de Subredes y Prefijos Globales de Enrutamiento**.Los 128 bits de una dirección de red IPv6, se dividen en dos partes para identificar, por un lado la interfaz a la que se encuentra relacionada y por el otro, la información de enrutamiento. Para las direcciones *unicast* globales, las dos partes equivalen a 64 bits. A continuación se explica cómo se encuentra distribuida la parte de red de la dirección IPv6.

***Global Routing Prefix***. Los bits de mayor orden encontrados en la parte de red de la dirección IPv6, identifican el prefijo externo de enrutamiento para las direcciones globales. Este es el espacio que es asignado a las entidades que desean solicitar espacio de direcciones en Internet.

***Subnet ID***. Los bits de menor orden que quedan en la parte de red de la dirección IP, se usan para identificar sub-redes dentro de una red IPv6. Es posible crear hasta 65.535 (2^16) sub-redes utilizando el valor mínimo actual de asignación que corresponde a 48 bits del prefijo global de enrutamiento.

Los prefijos se representan de manera similar que en IPv4, usando la notación CIDR ipv6_address/prefix_length. La Figura 2 contiene ejemplos de direcciones válidas, utilizando un prefijo global de 60 bits:

```
12AB:0000:0000:CD30:0000:0000:0000:0000/60
12AB::CD30:0:0:0:0/60
12AB:0:0:CD30::/60
```

Figura 2. Direcciones IPv6 con prefijo global de 60 bits[19].

**6.3.1.3 Direcciones Compatibles con IPv4**. Debido a los esfuerzos de migración entre las versiones de IP, se hace necesario embeber direcciones basadas en IPv4 dentro de las direcciones IPv6. Para ello, se establece un formato mixto, donde los primeros valores equivalen a una dirección IPv6 y los restantes se representan a manera de IPv4, obteniendo como resultado el siguiente formato: XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:ddd.ddd.ddd.ddd (las XXXX representan la parte IPv6 de la dirección, mientras las ddd representan la parte IPv4 de la dirección). Estas direcciones caen en dos clasificaciones a continuación descritas:

**Direcciones IPv6 compatibles con IPv4** Los mecanismos de transición entre la versión 4 y la 6, incluyen técnicas para el enrutamiento de paquetes IPv6 sobre una infraestructura

[19]Loshin, Pete.. Capítulo 8, página 152 [Recurso Físico].

basada en IPv4. Nodos IPv6 que hacen uso de esta técnica, les son asignados direcciones *unicast* que llevan una dirección IPv4 en los 32 bits de menor orden.

**Direcciones IPv6 mapeadas a IPv4** Esta técnica es utilizada para representar direcciones IPv4 en términos del formato definido para IPv6. Esta técnica está lista para ser rechazada, ya que colaboradores de la talla de Craig Metz y Jun-ichiro Itojun Hagino, opinan que este tipo de direcciones pueden presentar vulnerabilidades de seguridad.

## 6.4 PROTOCOLOS DE ENRUTAMIENTO

Los protocolos de enrutamiento usados en redes IPv6 son los mismos que se han venido utilizando en las actuales redes IPv4, con muy pocas modificaciones para adaptarse al nuevo estándar. Los más importantes de estos protocolos son RIP, OSPF y BGP. Los factores que marcan la diferencia en la utilización de estos mecanismos, están relacionados con la mayor dependencia en agregación y las direcciones más largas de IPv6. A continuación se describen con mayor detalle algunos de los protocolos mencionados.

### 6.4.1 Routing Information Protocol (RIP) y RIP Next Generation (RIPng)

Los protocolos de enrutamiento pueden usar diferentes modos para medir la conectividad de nodos a través de una red. Para el caso de RIP, el acercamiento utilizado se denomina *distance-vector*, en el que los enrutadores comparten sus tablas de enrutamiento y realizan adiciones y correcciones de acuerdo a los reportes obtenidos de otro enrutadores. Cada enrutador expresa cada ruta a manera de parejas, en las que una parte identifica al vector o red destino y la otra hace referencia a la distancia entre el enrutador y la red. Dicha distancia es medida en la cantidad de saltos o enrutadores intermediarios que un paquete tendrá que pasar para llegar a su destino.

Inicialmente, un enrutador no tiene mayor conocimiento de la red del que puede obtener a partir de sus propias interfaces. La tabla 1 muestra un ejemplo de las rutas iniciales.

| Destino | Distancia | Ruta |
|---|---|---|
| 10.0.0.0 | 0 | Directa |
| 192.168.100.0 | 0 | Directa |

Tabla 4. Tabla de rutas inicial para el enrutador X[20].

Las siguientes rutas son recibidas desde los demás enrutadores en la red. Cada uno reporta su tabla a los demás a manera de *broadcast*. Un ejemplo de esto puede verse en la tabla 5.

| Destino | Distancia |
|---|---|
| 192.168.200.0 | 0 |
| 10.1.0.0 | 0 |
| 10.10.10.0 | 3 |
| 20.0.0.0 | 3 |
| 192.168.1.0 | 4 |

Tabla 5. Mensaje con las distancias entre vectores del enrutador Y. Creación propia.

El enrutador inicial del ejemplo, tomará esta información y la fusionará a su tabla propia, esto quiere decir, que agregará las rutas nuevas e ignorará las que ya tenía disponibles. La nueva tabla de enrutamiento sería el resultado de dicha operación. En la tabla 6 se muestra un ejemplo de lo anterior:

[20]Loshin, Pete. Capítulo 8. [Recurso Físico]

| Destino | Distancia | Ruta |
|---|---|---|
| 10.0.0.0 | 0 | Directa |
| 192.168.100.0 | 0 | Directa |
| 192.168.200.0 | 1 | Enrutador Y |
| 10.5.0.0 | 1 | Enrutador Y |

Tabla 6. Tabla del enrutador X actualizada con la información de Y. Creación propia.

A medida que este proceso es ejecutado por los enrutadores de la red, las tablas se hacen más eficientes con el descubrimiento de nuevas rutas donde el número de saltos entre dos nodos sea el más corto[21][22]**.**

**6.4.1.1. RIP**. Se rige por un simple conjunto de reglas descritas en la tabla 7:

| ID Regla | Descripción |
|---|---|
| 1 | Por defecto, los enrutadores activos envían sus rutas a la red cada 30 segundos. |
| 2 | Todos los receptores de las rutas comparan la información nueva con sus propias tablas y realizan actualizaciones solo si:<br>• Hay rutas a nuevas redes que no tenían listadas anteriormente,<br>• Hay mejores rutas (más cortas) entre redes existentes, o<br>• Una de las rutas es reportada como inalcanzable y por lo tanto, debe ser descartada.<br>• Una ruta es mantenida en las tablas hasta que una mejor es reportada. |

[21] Hagen, Silvia. IPv6 Essentials. s.l. : O´REILLY

[22] Davies, Joseph. Understanding Ipv6 Second Edition. Understanding Ipv6 Second Edition. Washington : Microsoft Press, 2008

| | |
|---|---|
| | • Si existen dos rutas equivalentes (con el mismo número de saltos), la primera que llegue será la que se adicione a la tabla.<br>• Se asume que una red se encuentra caída si no ha sido reportada en un lapso mayor a tres minutos |
| Id Regla | Descripción |
| 3 | Los enrutadores reportan los cambios a medida que van ocurriendo, sin esperar al intervalo por defecto. |
| 4 | Una ruta que contenga 16 saltos se considera inalcanzable. RIP no es viable en redes con más de 15 saltos entre sus nodos |

Tabla 7. Funcionamiento RIP. Creación propia

RIP se encuentra documentado en el RFC 2453[23] "RIP Version 2". Es una implementación del algoritmo de enrutamiento conocido como *distance-vector*. Los mensajes son enviados junto con un encabezado de por lo menos y no más de 25 *RIP entries*. El encabezado consiste en los campos mencionados en la tabla8:

| **Campo** | **Descripción** |
|---|---|
| ***Command*** | Campo de un octeto de longitud, que puede tomar los siguientes valores:<br>• ***Version***. Campo de un octeto que indica la versión de RIP. Únicamente puede tomar los valores 1 y 2<br>La entrada RIP tiene longitud de 20 octetos distribuidos de la siguiente forma: |
| ***Address Family Identifier* (AFI)** | Campo de 2 octetos que indica el tipo de dirección (direcciones de Internet o cualquier otro tipo) |
| ***Route Tag*** | ***Route Tag***. Campo de 2 octetos que se utiliza para la diferenciación de rutas internas (aquellas que son pertinentes al dominio local) de las externas (aquellas que son importadas desde dominios adyacentes internos y externos). Este campo lleva el valor 0 para RIPv1. |

[23] Network Working Group. Request for Comments: 2453. RIP Version 2. Noviembre 1998. [en línea]. Disponible en: <http:// http://tools.ietf.org/html/rfc2453>

| | |
|---|---|
| ***IPv4 Address*** | Dirección de destino |
| ***Subnet Mask*** | Este campo es enviado con valor 0, lo que da espacio para errores de enrutamiento en redes que hayan sido fuertemente subdivididas |
| ***Next Hop*** | También se envía este campo con el valor 0. |
| **Campo** | **Descripción** |
| ***Metric*** | Indica la distancia de la ruta entre 0 y 15 saltos. |

Tabla 8. Encabezado RIP. Creación propia

**6.4.1.2 RIPng**: Definido en el RFC 2080[24] "RIPng for IPv6", define el protocolo para ser utilizado en redes IPv6. La tabla de enrutamiento para esta versión, contiene una entrada por cada destino alcanzable; estas entradas tienen por lo menos la siguiente información:

El prefijo IPv6 del destino.

Una métrica que representa el costo total de transportar un datagrama desde el enrutador hasta el destino especificado. Este valor es el resultado de sumar los costos asociados a las redes que serían atravesadas para llegar al destino.

La dirección IPv6 del siguiente enrutador en el camino al destino (*Next Hop*).

Un indicador de que la información de la ruta ha cambiado, también conocido como *Route Change Flag*.

Varios temporizadores asociados a la ruta.

La información de enrutamiento que es transportada por las *Route Table Entries* (RTEs) comprende: el *Route Tag*, la longitud del prefijo y una métrica de enrutamiento por cada prefijo IPv6 enrutado. Un mensaje RIPng lleva tantos RTEs como lo permita la *Maximum Transmission Unit* (MTU) definida en la política local. Para calcular los RTEs según la MTU dada, se realizan los siguientes pasos:

- Tomar el tamaño de la MTU en forma de octetos.
- Se resta el tamaño del encabezado IPv6 del ese valor.
- Se resta el tamaño del encabezado UDP de ese valor.
- Se resta el tamaño del encabezado RIPng de ese valor.

[24] Network Working Group. Request for Comments: 2080. RIPng for IPv6.January 1998. [en línea]. Disponible en: http://www.ietf.org/rfc/rfc2080.txt.

- Se divide el resultado entre el tamaño del RTE y se redondea hacia el entero menor más cercano.

La operación del protocolo RIPng es similar a la de RIP, definiendo dos comandos para el encabezado a saber:

- ***Request (command type 1)*** Solicita a los enrutadores de la red sus tablas de enrutamiento.
- ***Response (command type 2)*** Envía total o parcialmente, la tabla de enrutamiento del enrutador. Este mensaje puede ser enviado como respuesta a una solicitud directa o como actualización programada por defecto[25][26].

### 6.4.2 Open *Shortest Path First* (OSPF) y *OSPF Next Generation* (OSPFng)

Utiliza el método *link state* (estado de vínculos) para permitir a los enrutadores crear sus mapas de red. El protocolo está definido en el RFC 2328[27](20) "*OSPF Version 2*". Surgió como respuesta a los inconvenientes presentados por RIP. y entre sus ventajas frente al último se destacan la propagación rápida y estable de información de rutas, el manejo de subredes de manera adecuada, el permitir balanceo de carga cuando hay más enrutadores disponibles, soportar diferentes tipo de servicio de enrutamiento y la utilización de *multicasting*.

El método *Link State Routing* ordena que cada enrutador que pertenece a un *Autonomous System* (AS) mantenga una base de datos de *link states*. Esta base de datos representa un mapa de la topología completa del AS y es compartido por todos los enrutadores que pertenecen al mismo. Cada enrutador entrega al AS su *local state*, que se refiere a todos los vecinos que tiene a su alcance.

Por ejemplo, si el enrutador A anuncia que tiene vínculos directos con los enrutadores B, C y D sobre la red 10.0.0.0, y con el enrutador E sobre la red 192.168.0.0, entonces cualquier otro enrutador del AS podrá comenzar a ensamblar el mapa: los enrutadores A, B, C y D tienen interfaces sobre la red 10.0.0.0 y los enrutadores A y E tiene interfaces sobre la red 192.168.0.0.

---

[25] Shannon McFarland, Muninder Sambi, Nikhil Sharma, and Sanjay Hooda. IPv6 for Enterprise Networks. IPv6 for Enterprise Networks. Indianapolis

[26] Davies, Joseph. Understanding Ipv6 Second Edition. Understanding Ipv6 Second Edition. Washington : Microsoft Press

[27] Network Working Group. Request for Comments: 2328. OSPF Version 2. April 1998. [en línea]. Disponible en: http://www.ietf.org/rfc/rfc2328.txt.

Una vez los enrutadores ensamblan los mapas, proceden a calcular la ruta más corta hacia cualquier otro enrutador dado, “caminando” a través del mapa entero desde su propia ubicación. Una de las ideas detrás de éste método, es la de mantener el volumen de información de rutas que es transferido a otros enrutadores al mínimo posible. Periódicamente, cada uno de los enrutadores verifica el estado de los vínculos de sus vecinos, informando a la vez cuales de sus vínculos se mantienen vivos.

OSPF permite a los administradores de red establecer rutas alternas de acuerdo a necesidades específicas, como por ejemplo, balanceo de carga. Ofrece también gran flexibilidad en cuanto al uso de rutas separadas por tipos de servicio IP, por ejemplo, podría utilizar las rutas más rápidas para dar acceso a FTP mientras que servicios que no requieren de mayor ancho de banda como Telnet, se entregarían por otra ruta alterna.

**6.4.2.1 OSPF para IPv6**(10)**.** Definido en el RFC 274028 “OSPF for IPv6”, ofrece los mismos mecanismos que fueron concebidos para redes IPv4, salvo diferencias mínimas como el tamaño de las direcciones de red y algunos otros cambios que son enumerados a continuación:

**Procesamiento a nivel de vínculo vs. subredes** De acuerdo con IPv6, un vínculo (*link*) se define como “un medio o instalación de comunicaciones sobre el cual los nodos pueden comunicarse a nivel de la capa de vínculo” (RFC 2460). OSPF se conecta a nivel de vínculo, lo que permite que una misma interfaz sea suficiente para proveer varias subredes.

**Semántica de Direccionamiento removida** En vez de atar la identificación de los enrutadores a sus direcciones a nivel de la capa de red (IPv4/Ipv6), estos son diferenciados y accedidos por medio de su *Enrutador ID*.

**Ámbito de Flujo** Esta versión de OSFP agrega tres ámbitos diferentes para flujos, que incluyen un ámbito local (*link-local scope*), un ámbito de área (*area scope*) que es válido a través de varios vínculos y un ámbito de AS (*AS scope*) que es válido a través de todo el AS[29].

## 6.5 SERVICIOS PARA IPV6

Aunque la implementación de los servicios para IPv6 en apariencia es similar a laactual, los servicios deben ser adaptados a las características únicas que presenta el nuevo protocolo de Internet, como por ejemplo, la longitud de las direcciones de red,la definición de los

[28] Network Working Group. Request for Comments 2740. OSPF for IPv6. December 1999. [en línea]. Disponible en: http://www.ietf.org/rfc/rfc2740.txt.

[29]Yunes, Darwin Lamarck Santana. IPv6 Task Force América Latina y el Caribe. IPv6: Nueva Generación Protocolo de Internet. [En línea] <http://www.lac.ipv6tf.org/docs/tutoriales/IPv6-LACTF.pdf>

encabezados, etc. A continuación se presentan la adaptación dedos de los servicios más importantes a nivel de Internet

### 6.5.1 Domain Name System (DNS).

DNS[30] es una base de datos que almacena registros de recursos (Resource Records - RR) y que a su vez almacenan nombres asociados con direcciones principalmente, junto con otra información que extiende la identificación de recursos. La definición dada en el estándar de DNS (STD 13 - RFC 1034[31]/35[32]) dice: "*Un nombre de dominio identifica un nodo. Cada nodo tiene un conjunto de información de recursos. El conjunto de información de recursos asociado a un nombre en particular, se compone de diferentes registros de recursos*".

Los RR definen diferentes tipos de información de recursos que permiten su fácil identificación. Por ejemplo, un registro de tipo A RR contiene una dirección, mientras que un registro de tipo MX RR contiene información para el intercambio de correo. En el caso de las direcciones para IPv6, fueron definidos dos registros: a) AAAA y b) A6 RR.

#### 6.5.1.1 Resource Register (RR).

Un RR está compuesto por los campos descritos en la tabla 9:

| **Tipos de Registros RR** | **Descripción** |
|---|---|
| ***NAME*** | El nombre de dominio donde se ubica el RR; el nombre del dueño puede ser derivado por el contenido del RR. |
| **Tipos de Registros RR** | **Descripción** |
| ***CLASS*** | Especifica una familia o instancia de protocolo, por ejemplo, IN especifica el sistema de Internet. |

[30] Microsoft Technet Library. Definición de DNS. Última fecha de consulta Septiembre 13 de 2011. [en línea]. Disponible en: http://technet.microsoft.com/es-es/library/cc787920(WS.10).aspx

[31] Network Working Group. Request for Comments: 1034 Domain Names concepts and facilities. November 1987. [en línea]. Disponible en: <http://www.ietf.org/rfc/rfc1034.txt>.

[32] Network Working Group. Request for Comments: 1035 Domain Names concepts and facilities. November 1987. [en línea]. Disponible en: < http://www.ietf.org/rfc/rfc1035.txt>.

| | |
|---|---|
| ***TTL*** | El tiempo de vida del RR. Este tiempo está definido como el número de segundos antes de que el RR expire. Se utiliza principalmente para establecer por cuento tiempo se debe mantener la información del cache. |
| ***RDLENGTH*** | Indica la longitud de los datos del recurso en bytes, cuidando que la longitud de cualquier RR no exceda los 65.535 bytes. |
| ***RDATA.*** | Los datos asociados al RR. |

Tabla 9. Tipos de Registros RR. Creación propia

.

**6.5.1.2 Soporte DNS al protocolo IPv6**. Se proponen las siguientes acciones:

**Nuevo RR para direcciones IPv6.** Definición de un nuevo RR para mapear direcciones IPv6 con nombres de dominio (AAAA RR).

**Nuevo *Reverse Lookup* para IPv6.** Permite realizar búsquedas cuando está dada la dirección IP y no el nombre.

**Consultas Modificadas.** Se adicionan mecanismos para realizar búsquedas de nombres que retornen tanto direcciones IPv4 como IPv6.

**6.5.1.3 El registro AAAA.** Este registro almacena una sola dirección IPv6 de 128 bits en el campo RDATA. Cuando se realiza una consulta AAAA desde un cliente, el servidor DNS responde con la lista de registros asociados con el nombre de dominio dado.

***Reverse Lookup Domain***. Para IPv6, se encuentra definido en el RFC 1886[33] (para buscar el dominio asociado a una dirección en particular en vez de una dirección para un nombre de dominio). La dirección IPv6 a buscar, se convierte en un nombre compatible con el estándar IP6.ARPA (*Address and Routing Parameters Area*), reversando el orden de los dígitos hexadecimales, separando cada dígito con un punto (".") y añadiendo el sufijo "IP6.ARPA". Por ejemplo, la dirección4321:0:1:2:3:4:567:89ABse convierte enB.A.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6.ARPA.

**6.5.1.4Consultas DNS.**Los diferentes tipos de consultas que se pueden realizad en DNS,como por ejemplo Servidor de Nombres (*Name Server - NS*) e Intercambio de Correo

[33] Network Working Group. Request for Comments: 1886 DNS Extensions to support IP version 6. December 1995. [en línea]. Disponible en: <http://www.ietf.org/rfc/rfc1886.txt >.

(*Mail Exchange - MX*), deben ser modificadas para que retornen resultados de ambos tipos: A (IPv4) y AAAA [34].

### 6.5.2 Dynamic *Host Configuration Protocol* (DHCP).

DHCP se generó a partir de un protocolo llamado *Boot Protocol* (BOOTP) que permitía a los nodos iniciarse a partir de un servidor de red. Tanto DHCP como su versión para IPv6, permiten a los nodos configurarse a sí mismos haciendo uso de servidores DHCP. Se dice que este protocolo es de estado completo, debido a que los servidores mantienen tablas de direcciones IP de todos los nodos que hacen uso de sus servicios.

**6.5.2.1 Configuración Con o Sin Estado.** En la actualidad, existe una gran cantidad de dispositivos que hacen uso de DHCP para la configuración de nodos. Un servidor DHCP puede asignar direcciones de tres maneras:

**Distribución Automática.** El servidor DHCP asigna una dirección IP permanente al cliente.

**Distribución Dinámica**. DHCP asigna una dirección IP a un cliente durante un período de tiempo limitado, o hasta que el cliente renuncie explícitamente a la dirección dada.

**Distribución Manual**. La dirección IP de un cliente es asignada por un administrador de red.

Para cualquiera de los casos anteriores, el servidor DHCP mantiene un estado acerca de la direcciones IP que han sido asignadas a sus clientes. La autoconfiguración sin estado (*stateless*) permite a los nodos configurarse sin dependencia de ningún tipo de autoridad centralizada. En redes IPv6, es completamente normal encontrar esta doble configuración. En un escenario de *Neighbor Discovery*[35], un nodo puede utilizar una configuración *stateless* para asignarse una dirección IP que sea válida dentro de un entorno local; del mismo modo, el mismo nodo puede hacer uso de una configuración *stefull* para determinar su propia dirección IPv6 global, su prefijo de red y sus enrutadores por defecto.

---

[34] Microsoft Inc. Microsoft Technet Library. Microsoft Technet Library. [En línea] [Citado el: 13 de Septiembre de 2011.] <http://technet.microsoft.com/es-es/library/cc787920(WS.10).aspx>

[35]Network Working Group. Request for Comments: 2461 Neighbor Discovery for IP Version 6 (IPv6). December 1998. [en línea]. Disponible en: < http://www.ietf.org/rfc/rfc2461.txt>.

### 6.5.3 DHCPv6.

Es la última iteración del protocolo, publicada en el RFC 951[36], "*Boot Protocol*" en 1985. En la tabla 10 se presenta una lista de RFCs que proveen mayor información acerca de BOOTP, DHCP y DHCPv6:

| **Número RFC** | **Título** |
|---|---|
| 3118 | *"Authentication for DHCP Messages".* |
| 2132 | *"DHCP Options and BOOTP Vendor Extensions".* |
| 2131 | *"Dynamic Host Configuration Protocol".* |
| 1542 | *"Clarifications and Extensions for the Bootstrap Protocol".* |
| 1534 | *"Interoperation Between DHCP and BOOTP".* |
| 0951 | *"Bootstrap Protocol".* |

Tabla 10. RFC Recomendados para DHCP. Creación propia

.

Sin embargo, la especificación actual para DHCPv6 es aún un trabajo en progreso. Aunque presenta similitudes con DHCPv4, aún no se incluye ninguna especificación acerca de interoperabilidad entre las dos versiones.

**6.5.2.3 Mensajes DHCP.** Los mensajes del protocolo que son transmitidos a través de UDP. El cliente, que en un comienzo, no tiene una dirección IP asignada para sí mismo ni

[36] Network Working Group. Request for Comments: 951 Bootstrap Protocol (BOOTP). September 1984. [en línea]. Disponible en: <http://www.ietf.org/rfc/rfc4193.txt>.

para el entorno local, envía un requerimiento a los servidores DHCP a través de la dirección de *multicast* reservada para este fin. Estas son las dos direcciones válidas para tal fin:

***All_DHCP_Relay-Agents_and_Servers(FF02::1:2).*** Una dirección de *multicast* a nivel de vínculo que es usada por un cliente para comunicarse con agentes y servidores de *relay* que pertenezcan al grupo.

***All_DHCP_Servers (FF05::1:3).*** Dirección *multicast* a nivel de sitio, usada por un agente de *relay* para comunicarse con otros servidores, ya sea porque quiere enviar un mensaje a todos los servidores, o por que desconoce la dirección de *unicast* de dicho servidor o agente.

Siempre que estas direcciones se encuentren disponibles para un cliente, éste puede llevar a cabo su auto configuración con DHCP. Por defecto, los clientes envían mensajes a las direcciones reservadas de *multicast* en vez de a una dirección DHCP específica, para permitir que los agentes de *relay* pasen los mensajes DHCP de los clientes hasta un servidor remoto.

Están permitidos dos tipos de intercambio de mensajes, intercambio de dos mensajes e intercambio de cuatro mensajes. Los siguientes, son los tipos de mensajes que han sido definidos para el protocolo DHCPv6[37][38] se describen en la tabla 11:

| **Tipo de Mensaje** | **Descripción** |
|---|---|
| ***Solicit.*** | Los clientes envían este mensaje para ubicar los servidores DHCPv6. |
| ***Advertise.*** | Este mensaje es enviado por el servidor, como respuesta a un mensaje de solicitud, indicando que está ofreciendo el servicio de DHCP. |
| ***Route Tag*** | Campo de 2 octetos que se utiliza para la diferenciación de rutas internas (aquellas que son pertinentes al dominio local) de las externas (aquellas que son importadas desde dominios adyacentes internos y externos). Este campo lleva el valor 0 para RIPv1. |

[37] Hagen, Silvia. IPv6 Essentials. s.l. : O´REILLY. págs. 100-110

[38] Loshin, Pete. IPv6: Theory,Protocol,and Practice SECOND EDITION. San Francisco : Morgan Kaufmann Publishers is an Imprint of Elsevier, 2004. pág. Capítulo 8. Vol. 2

| Tipo de Mensaje | Descripción |
|---|---|
| ***Request***. | Un cliente envía este mensaje para solicitar los parámetros de configuración, incluyendo la dirección IP, al servidor. |
| ***Confirm***. | Un cliente envía este mensaje a cualquier servidor que se encuentre disponible para determinar si las direcciones que le fueron asignadas son apropiadas para el vínculo al cual el cliente se encuentra conectado. |
| ***Rebind***. | Este mensaje es enviado a cualquier servidor DHCP que se encuentre disponible, con el mismo propósito que tiene el mensaje *renew* pero solo en caso de que no se haya recibido ninguna respuesta a éste último. |
| ***Reply***. | Un servidor envía este mensaje, que contiene parámetros de configuración y direcciones asociadas, como respuesta a un mensaje *solicit, request, renew o rebind* recibido de un cliente. De la misma forma, este mensaje es enviado como respuesta a un mensaje *confirm* en caso de ser necesario confirmar o negar las direcciones y parámetros de configuración. Finalmente, también es enviado a manera de *acknowledgement* (reconocimiento) para mensajes *release y decline*. |
| ***Release***. | Un cliente envía este mensaje al servidor que le haya asignado su dirección, para indicarle que ya no va a hacer uso de una o más de las direcciones dadas. |
| ***Decline***. | Un cliente envía este mensaje a un servidor para indicarle que el cliente ha determinado que una o más de las direcciones que le han sido asignadas están ya en uso dentro del ámbito de vínculo al que se encuentra conectado |
| ***Reconfigure***. | Un servidor envía este mensaje a un cliente, para informar que el servidor tiene parámetros de configuración nuevos o actualizados, y que debe proceder a iniciar una transacción de tipo renew/reply o information-request/reply para recibir dichos cambios. |
| ***Information-Request*** | Un cliente envía este mensaje a un servidor para solicitar parámetros de configuración sin que le sea asignada una dirección IP. |
| ***Relay-Forw*** | Un agente de *relay* envía este mensaje para reenviar mensajes a los servidores, ya sea directamente o a través de otro agente. |

| | |
|---|---|
| ***Relay-Repl***. | Este mensaje es enviado por el servidor a un agente de *relay* junto con el mensaje original que debe ser entregado al cliente |

Tabla 11. Tipos de Mensajes Definidos para DHCPv6. Creación propia

## 6.6 MECANISMOS DE CONVIVENCIA

Debido a que IPv4 es utilizado de manera muy amplia a nivel mundial, la IETF se encuentra en la tarea de asegurar que la transición a la nueva versión del protocolo se realice sin mayores complicaciones; de lo contrario, la migración total se dará mucho más tarde de lo planeado[39].

*Tunneling* (uso de túneles) es el método más utilizado para establecer la convivencia entre los dos protocolos de red. Esta técnica se refiere al proceso de encapsular paquetes IPv6 dentro de paquetes IPv4 y enviarlos a través de la red; cuando el paquete llega, es extraído y transmitido a través de IPv6 a su destino. Estos túneles funcionan en reverso también, encapsulando paquetes IPv4 dentro de paquetes IPv6.

Esta técnica es clasificada en dos conjuntos a saber: *static* (estáticos) y *automatic* (automáticos). A continuación se presentan los dos métodos que fueron utilizados en el desarrollo de los talleres, detallando cómo se espera que funcione la convivencia de los dos protocolos asegurando el correcto funcionamiento de los servicios y aplicaciones que son utilizadas actualmente[40].

[39]CODAREC6: AN IPV6 TEST BED" – laboratorio de estudio, diseño, desarrollo, implementación, ensayo y capacitación del protocolo de internet versión 6. Carlos Taffernaberry, Alejandro Dantiacq Picolella, Gustavo Mercado y Adrián Francisconi. [en línea]. Disponible en: http://codarec6.frm.utn.edu.ar/publicaciones/papers/CACIC-2006.pdf.

[40]Yunes, Darwin Lamarck Santana. IPv6 Task Force América Latina y el Caribe. IPv6: Nueva Generación Protocolo de Internet. [En línea] <http://www.lac.ipv6tf.org/docs/tutoriales/IPv6-LACTF.pdf>

### 6.6.1 Dual Stack

Es la forma más directa de implementar un mecanismo de convivencia para la transición de protocolos. La idea es que los nodos pertenecientes a una red, provean tanto implementación para IPv6 como para IPv4. De esta forma, los paquetes correspondientes a cada protocolo son enviados y recibidos por la pila adecuada. Los nodos *dual-stack* pueden ser operados de tres modos a saber: Ambas pilas habilitadas, la pila IPv6 habilitada y la pila IPv4 deshabilitada, y la pila IPv4 habilitada y la pila IPv6 deshabilitada.

Teniendo la capacidad de manipular las pilas de acuerdo a las necesidades de la red, esta técnica puede ser utilizada como base para la implementación e integración de mecanismos adicionales, como por ejemplo, *6to4 tunneling*.

Al soportar los dos protocolos, cada nodo que utilice esta técnica, deberá ser configurado con direcciones IPv4 e IPv6. Es posible configurar servidores DHCP que estén en capacidad de proveer las direcciones a los nodos automáticamente.También sería posible habilitar DHCP únicamente para la pila IPv4 y asignar por medio de autoconfiguración sin estado las direcciones nativas para las interfaces IPv6[41].

En las figuras 3, 4 y 5 se presentanejemplos de implementación *Dual-Stack*para tecnologías Cisco[42], fabricante que propone, en sus soluciones de transición y convivencia, tres capas para la implementación tanto en usuarios finales (redes locales) como en soluciones de *data center* (centros de datos):

[41] Hagen, Silvia. IPv6 Essentials. s.l. : O´REILLY

[42] Cisco Systems, Inc. IPv6 Site and Solutions. 2011. [en línea]. Disponible en http://www.cisco.com y <http:// http://www.cisco.com/web/solutions/netsys/ipv6/index.html>.

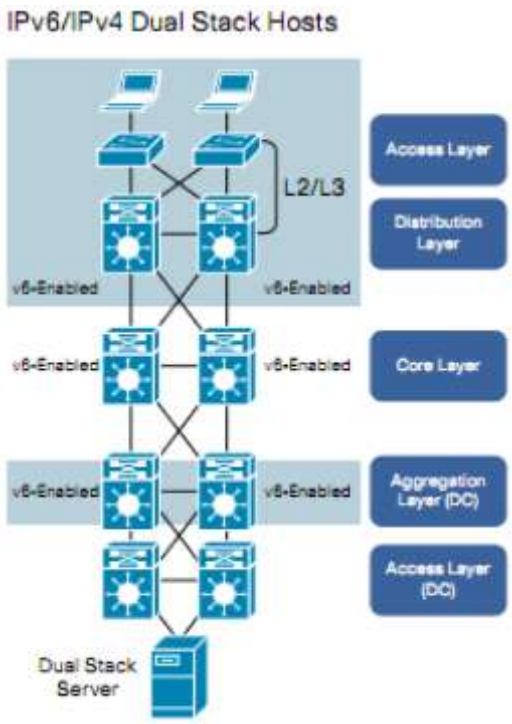


Figura 3. Implementación Dual-Stack según Cisco System[43]

43 Cysco System Inc.s Inc. Cisco IPv6 products, solutions, and services. 2010. [en línea]. Disponible en:< http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/at_a_glance_c45-625859.pdf>.

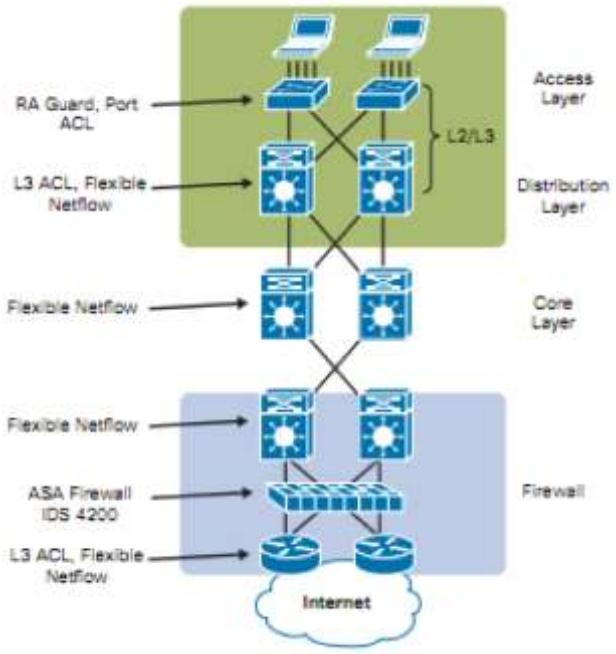


Figura 4. Implementación Dual-Stack según Cisco. Host IPv4 /IPv6[44]

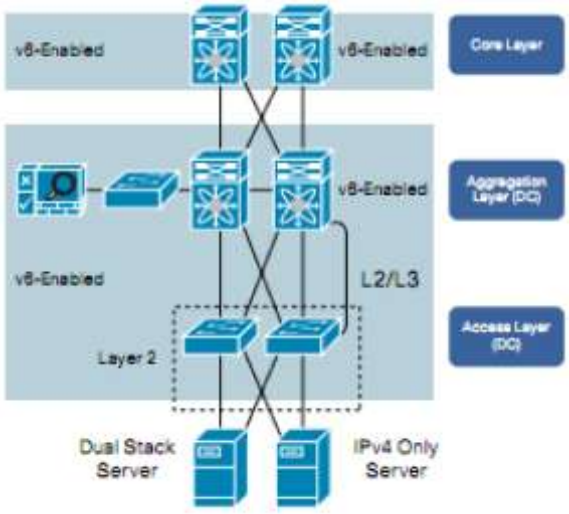


Figura 5. Implementación Dual-Stack para Centros de Datos según Cisco[45].

[44] Cisco System Inc. Application Visibility and Control for IPv6. 2011. [en línea]. Disponible en: <http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/aag_c45-665915.pdf>

### 6.6.2 6to4 Tunnels

Esta técnica es una implementación de *automatic tunneling*[46]. Permite la interconexiónde redes IPv6 desde redes IPv4 únicamente. Cualquier nodo IPv6 que se encuentre en capacidad de enviar y recibir paquetes IPv4, puede hacer uso de esta técnica y por medio de una dirección enrutable global IPv4 alcanzar redes y nodos IPv6.

Un nodo se configura como 6to4, embebiendo una dirección IPv4 dentro de una dirección IPv6. La IETF ha definido específicamente, que toda dirección IPv6 que comience con el prefijo 2002::/16 hace referencia a un nodo 6to4. Un ejemplo de esta configuración se puede ver de la siguiente forma.Un nodo con la dirección IPv4 200.150.100.30, se configura como IPv6 con la dirección 2002:C896:641E::1; donde 2002 indica que es una dirección 6to4, C8 equivale al valor 200, 96 equivale al valor 150, 64 equivale al valor 100 y 1E equivale al valor 30. El 1 al final es completamente arbitrario, típicamente configurado por el nodo mismo.

Para comunicarse, los nodos configurados de esta forma cuentan con funcionalidad 6to4 que les permite reconocer el prefijo 2002::/16 para extraer y determinar la dirección IPv4 encapsulada en el paquete original. Para transmitir los datos por la red al nodo destino, el campo *packet type* (tipo de paquete) del encabezado del paquete, lleva el valor IP in IP. Una vez llega el paquete, el nodo destino encuentra el valor del campo y des encapsula la información haciendo entrega efectiva a la dirección IPv6.

Este mecanismo funciona automáticamente para cualquier cantidad de nodos 6to4 dentro de una red IPv4 extendida. El poder de esta técnica radica en la posibilidad de asignar automáticamente direcciones IPv6 únicas a partir de direcciones IPv4, únicas también.

Existen dos formas para hacer uso de los túneles 6to4:

**6.6.2.1 6to4 node to 6to4 node(nodo a nodo 6to4).**Cualquier nodo 6to4, definido como una sola máquina configurada con IPv6 y funcionalidad 6to4, puede intercambiar paquetes con otro nodo configurado como 6to4 a través de una red habilitada únicamente para IPv4. Debido a que los 48 bits más a la izquierda son utilizados para identificar a un nodo como 6to4, los 80 restantes se pueden utilizar para una red ubicada detrás del nodo dado. Dicha red, es accesible por la dirección IPv4 embebida; este hecho convierte al nodo en un *edge-router* (enrutador de borde) que permitirá la conexión con otras redes 6to4.

---

[45] Cisco System Inc. Cisco IPv6 products, solutions, and services. 2010. [en línea]. Disponible en: <thttp://www.cisco.com/go/ipv6>.

[46] Network Working Group. Request for Comments: 3056 Connection of IPv6 Domains via IPv4 Clouds. Febraury 2001. [en línea]. Disponible en: <http://www.ietf.org/rfc/rfc3056.txt >.

Inicialmente, 6to4 permite a dos nodos individuales, que posean una única dirección IPv4 alcanzable, intercambiar paquetes IPv6 por medio de un túnel. Convirtiendo estos nodos en enrutadores, se puede configurar una red entera basada en IPv6 que será accesible por medio de IPv4 y de esta forma realizar la transición de manera transparente para los servicios y aplicaciones. Cuando llegue el momento, el único cambio que se deberá realizar, es el de los nodos que funcionan como enrutadores.

**6.6.2.2 *6to4 node to native IPv6 node*(nodo 6to4 a nodo nativo IPv6)**. Un nodo 6to4, ubicado en una red IPv4, puede comunicarse directamente con un nodo que se encuentre sobre una red nativa IPv6. Debido a que los nodos IPv6 nativos no se encuentran detrás de ningún otro nodo IPv4 y que no utilizan el prefijo reservado para este fin (2002::1/16), la IETF establece un mecanismo de transferencia por medio de unos dispositivos que han sido denominados*6to4 relays* (replicadores 6to4).Estos dispositivos son máquinas dedicadas que constan de múltiples interfaces de red, típicamente al menos una de éstas configurada como IPv4 y otra como IPv6. La interfaz IPv4 se encargará de la comunicación entre nodos y redes 6to4 mientras que la configurada como IPv6 se encargará de manejar la red nativa. Estas máquinas deben implementar una función de replicación 6to4 que se aplica como se describe a continuación.

Los *6to4 relays* son colocados en la dirección 192.88.99.1, como se propone en el RFC 3068[47].Dicha dirección es de tipo *anycast* y ha sido reservada para el intercambio de mensajes entre enrutadores 6to4. Cuando la pila IPv6 de un nodo 6to4 intenta enviar un paquete a una dirección 2002::/16, la función 6to4 entrega el paquete a la porción IPv4 codificada en la dirección de destino. Si la dirección de destino no se encuentra dentro del rango 2002::/16, la función del nodo reconocerá que la dirección efectivamente no corresponde a 6to4 y asume que dicha dirección es alcanzable por medio de un replicador, entregando el paquete a un *6to4 relay* ubicado en la dirección 192.88.99.1. El replicador encapsula el mensaje en un nuevo paquete IPv6 y lo envía al recipiente nativo.

Los replicadores también proveen funcionalidad para transmitir paquetes desde redes IPv6 a nodos 6to4 y a redes dentro de una red IPv4. Un nodo nativo IPv6 enviará todos los paquetes destinados a una dirección 2002::/16 hacia un replicador *6to4*, quien se encargará de encapsular el mensaje en un paquete IPv4 y lo enviará a la dirección codificada dentro de la dirección de destino IPv6[48].

En la Figura 6 se muestra un diagrama esquemático de una implementación de este mecanismo.

---

[47] Network Working Group. Request for Comments: 3068 An Anycast Prefix for 6to4 Relay Routers. June 2001. [en línea]. Disponible en: <http://www.ietf.org/rfc/rfc3068.txt >.

[48] Loshin, Pete. IPv6: Theory,Protocol,and Practice SECOND EDITION. San Francisco : Morgan Kaufmann Publishers is an Imprint of Elsevier, 2004. pág. Capítulo 8. Vol. 2

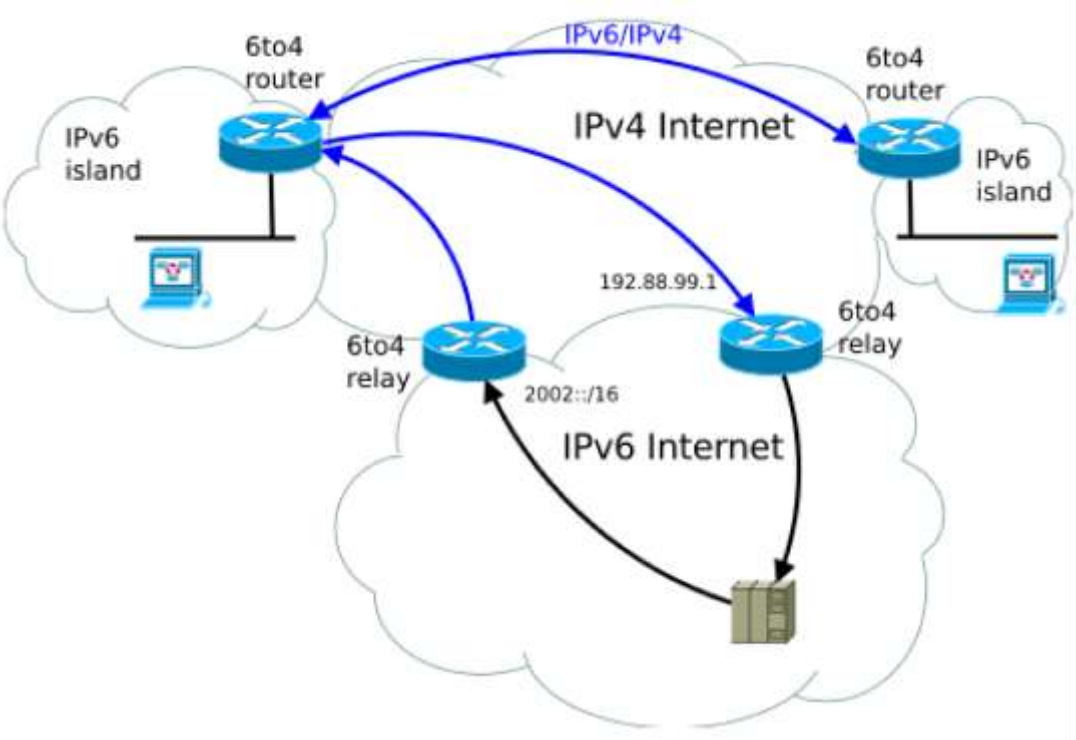


Figura 6. Ejemplo de Implementación 6to4[49].

[49] Grupo de trabajo IPv6 Chile. IPv6 Chile. 2011. [en línea]. Disponible en: <http://www.ipv6.cl>

# 7. GUÍAS DE LABORATORIO

Este capítulo contiene la especificación de cuatro guías de laboratorio que ayudarán al estudiante a fortalecer sus conocimientos en el estudio del protocolo de comunicaciones IPv6.

En primera medida, y antes de las guías de laboratorio, se presentan los comandos de configuración básicos para enrutadores cisco, los cuales serán de utilidad para el desarrollo de las guías. Posterior se describe en detalle cada una de las guías a desarrollar separadas por secciones temáticas que llevarán al estudiante a completar las configuraciones respectivas.

## 7.1 COMANDOS DE CONFIGURACIÓN PARA ENRUTADORES CISCO

Al iniciar la configuración de un Enrutador, este debe ser caracterizado con un nombre único para su fácil identificación y gestión.También se recomienda establecer una contraseña válida para permitir acceso al modo privilegiado de configuración y habilitar el modo de configuración de línea para accederlo remotamente.

A continuación se describen algunos de los más importantes comandos[50], que sirven para configuraciones en protocolos IPv4 e IPv6. Adicionalmente, estos comandos serán de utilidad para el desarrollo de las guías..

Inicialmente se describen los modos y sub-modos de configuración del enrutador:

[50] Cisco System Documents. Cisco IOS IPv6 Configuration Guide Release 12.4T. Marzo 5 de 2009. [en línea] Disponible en: <http://www.cisco.com/en/US/docs/ios/IPv6/configuration/guide/12_4t

| Modo de Configuración | Descripción |
|---|---|
| **Modo Usuario**: | Permite consultar a manera de lectura, información del enrutador. El indicador de línea de entrada que muestra el enrutador es el siguiente: Enrutador>. |
| **Modo privilegiado**: | Permite visualizar el estado del Enrutador, importar y exportar configuraciones e imágenes del IOS. El prompt que nos muestra el Enrutador es el siguiente: Enrutador #. |
| **Modo de configuración Global**: | Permite utilizar comandos de configuración generales el enrutador. El promt que nos muestra el Enrutador es el siguiente: Enrutador (config) #) |
| **Modo de Configuración de Línea**: | Permite configurar un acceso remoto al enrutador, como por ejemplo, a través de telnet. El promt que nos muestra el enrutador es el siguiente: Enrutador (config-line) #. Ejemplo: Enrutador (config) # line vty 0 4, donde line vty indica la interfaz, 0 el número de la interfaz y 4 la cantidad máxima de conexiones múltiples a partir de 0; para este caso se permiten hasta 5 sesiones telnet simultáneas. |

Tabla 12. Modos y Submodos de Configuración en enrutadores Cisco. Creación propia.

.

Otros comandos importantes para configuraciones IPv4 e IPV6:

**Visualización de información**: Digite el comando show seguido del signo? , de esta forma podrá observar las opciones del comando. Aquí algunos ejemplos:

- IPv6 interfaces: show ipv6 interface
- IPv6 static routes: show ipv6 route
- IPV6 OSPF commands: show ipv6 osfp y show IPv6 neighbor
- **Comando para cambiar el nombre del Enrutador:** Este comando debe ejecutarse en modo privilegiado. Digite hostname seguido del nombre deseado (ejemplo: hostname midgard).
- **Comando de Copia de Seguridad:** Este comando permite realizar una copia de seguridad de la configuración actual para posterior restauración, en caso de un reinicio inesperado del enrutador. Recuerde que este comando debe ejecutarse en modo privilegiado: copy running-config startup-config.
- **Configuración de las Interfaces:** Para asignar una dirección IP a una de las interfaces del enrutador podemos utilizar los comandos:

configure terminal.

interface fa o interface gi dependiendo de la velocidad que maneje la interfaz.

ip address se digita la dirección ip deseada seguida de la máscara de red.

Por último se utiliza el comando no shutdown para habilitar la interfaz. También puede habilitar la interfaz utilizando los comandos: interface xx, luego IPv6 enable.

## 7.2 GUÍA NO. 1 - CONFIGURACIÓN INICIAL DE IPV6

Durante el desarrollo de esta guía de laboratorio el estudiante aprenderá de forma práctica la configuración básica de IPv6, utilizando los conceptos esenciales del protocolo. La presentación de esta guía en el documento es una versión resumida de la misma, puede consultarse de forma completa en el Anexo A. "Guía No 1, Configuración Inicial de IPv6".

### 7.2.1 Objetivos

**General.** Utilizar los conceptos, características y funcionalidades básicas relacionadas con IPv6.

**Específicos:**Instalar o habilitar y configurar IPv6 en los equipos del laboratorio.

Realizar la implementación de DHCPv6 sobre un Enrutador Cisco 1841.

### 7.2.2 Conceptos Básicos

- **Dirección IP:** Podría describirse como un tipo de etiqueta numérica, que identifica de manera lógica y jerárquica a un dispositivo o elemento ya sea de comunicación o conexión dentro de una red, la cual utiliza el protocolo IP (*Internet Protocol*).
- **Sistema Operativo:**"*Programa o conjunto de programas que, ordenadamente y relacionados entre sí, contribuyen a que el ordenador lleva a efecto correctamente el trabajo encomendado*"[51].

[51] Conceptos de sistemas Operativos. Juan M. Morera Pascuál,Juan A. Pérez-Campanero Atanasio. [en línea]. Disponible en: <http://books.google.com/books?id=LY2P_VSuZ3cC&pg=PA19&dq=definicion+sistema+operativo&hl=es&ei=

- **Protocolo:** Conjunto de reglas y estándares para establecer la comunicación entre dos o más computadores.
- **IPv6:** Versión 6 del protocolo de Internet. Definido en el RFC 2460[52]
- ***Enrutador*** **(Enrutador):***"Dispositivo de capa de red que usa una o más métricas para determinar la ruta óptima a través de la cual se debe enviar el tráfico de red. Los enrutadores envían paquetes desde una red a otra basándose en la información de la capa de red."*[53]*.*

### 7.2.3 Elementos Requeridos

- Computador por persona que cuente con sistemas operativos: *Windows XP, Vista o 7.*
- *Patch cord*
- Enrutador Cisco 1841
- Cables de la Consola del enrutador
- *Switch* Cisco o 3Com
- Software *Packet Tracert* v 5.3 o superior

### 7.2.4 Informe a realizar por los estudiantes.

El estudiante deberá desarrollar un informe para la siguiente clase en el que dé respuesta a las siguientes preguntas:

- ¿Cuál es la situación actual de despliegue de IPv6 en el mundo?
- Investigue: ¿Cuáles son los comandos necesarios para realizar la instalación básica de IPv6 sobre Linux?

**NOTA:**Para la elaboración de esta guía de laboratorio lea atentamente y siga cada uno de los pasos descritos a continuación (en caso de dudas consultar al profesor). Recuerde solicitar al asistente de laboratorio privilegios administrativos sobre el computador que va a utilizar.

---

[52]Network Working Group. Request for Comments: 2460. [en línea]. Disponible en:<http://www.rfc-es.org/rfc/rfc2460-es.txt>

[53] Cisco Networking Academy. CCNA Exploration 4.0. Diccionario de Conceptos. [material didáctico cursos de certificación].

### 7.2.5 Procedimiento.

A continuación se describen los pasos que deben seguir los estudiantes para desarrollar la guía.

**SECCIÓN 1. Configuración Inicial de IPv6.** Para la elaboración de los tres primeros pasos se recomienda que cada estudiante ejecute el ejercicio de forma individual.

**Paso1. Instalación de IPv6.**Instalación sobre *Windows XP/2003*. Existen dos formas de realizar la instalación sobre ésta plataforma:

**A través de la línea de comandos:**

- En el menú inicio seleccione la opción ejecutar y en el campo de texto digite la palabra cmd.
- En la línea de comandos digite IPv6 install.
- Unos segundos después aparecerá el mensaje de confirmación de la instalación.

**A través de la interfaz gráfica:**

- En el menú inicio, Panel de control, Conexiones de Red
- Seleccionar red de área local o redes inalámbricas (si es el caso)
- Clic derecho en la opción Propiedades.
- Seleccionar Microsoft TCP/IP versión 6.
- Clic en instalar protocolo.

Instalación *Windows Vista, 7 y 2008*: Estos sistemas operativos traen por defecto el protocolo instalado y habilitado, por tanto no es necesaria ninguna configuración adicional. En caso que se encuentre deshabilitado, puede utilizar el comando: netsh interface IPv6 install [54].

**Paso 2.Comprobación de la instalación**. Las siguientes son algunas formas para la comprobación de la instalación exitosa del protocolo IPv6:

**A través del comando ipconfig / all**: este comando muestra todas las interfaces de red y su respectiva información de configuración.

**A través del comando netsh**: Este comando se utiliza desde una ventana de línea de comandos. Una vez dentro de la aplicación, digite el comando interface IPv6 show interfaces cuyo resultado se verá desplegado en pantalla, mostrando las interfaces conectadas y su número de identificación.

---

54 Microsoft Inc. Technet. Comando netsh. Disponible. [en línea] <http://technet.microsoft.com/es<->es/library/cc785383\%28WS.10\%29.aspx>

**A través del comando ipv6 if**: Este comando tiene la característica de listar únicamente las interfaces con configuración IPv6.

**Probar conectividad**: Para probar la conectividad con la red local, se requiere que dentro de la red exista otra máquina configurada con el protocolo IPv6; adicionalmente se debe comprobar que el *firewall* (cortafuegos) de Windows permita el tráfico del *Internet Control Message Protocol* (ICMP). Utilice el comando ping para probar la conectividad con la dirección IPv6 de su compañero.

**Paso 3.Configuración Avanzada de IPv6**. De acuerdo al entorno y configuración de una red, puede presentarse el caso en el que se requieran otro tipo de configuraciones sobre el protocolo, como por ejemplo asignar una dirección manual. En este paso usted va a realizar una configuración de forma manual, utilizando el comando netsh. Para ello, utilice el comando de la siguiente forma:

En una ventana de línea de comandos digite netsh y presione la tecla *enter*.

A continuación, digite interface ipv6 y presione la tecla *enter*.

Digiteaddaddress[interface=]cadena[address=]direcciónipv6, donde:

- cadena especifica el número de la interfaz.
- direcciónIPv6 especifica la dirección IPv6.

**SECCIÓN 2. Configuración Inicial de DHCPv6 en Enrutadores Cisco**

Para el desarrollo de esta práctica el estudiante debe realizar la configuración inicial de un Enrutador Cisco 1841 [55] y activar el servicio DHCP en versión 6[56] De esta forma, el enrutador será el encargado de entregar el direccionamiento IPv6 a los computadores. Los estudiantes deben configurar la opción de obtener direcciones automáticamente en los computadores.

**Paso 1. Preparación del laboratorio**

Los estudiantes deben formar 4 grupos, cada grupo debe contar con los siguientes implementos:

- 1 Enrutador Cisco 1841
- 1 Cable de Consola para Enrutador.
- 1 *Switch*

---

[55] Cisco Systems. Cisco 1800 Series Integrated Services Routers. [en línea]. Disponible en: <http://www.cisco.com/en/US/prod/collateral/enrutadores/ps5853/product_data_sheet0900aecd8016a59b.html>

[56] Cysco System Inc.. Cisco IOS IPv6 Configuration Guide, Release 12.4. Implementing DHCP for IPv6. April 8, 2011. [en línea] Disponible en: <http://www.cisco.com/en/US/docs/ios/IPv6/configuration/guide/ip6-dhcp.html#wp1055621>

- 2 computadores como mínimo.
- Software Wireshark

Deben realizar la configuración para obtener la topología mostrada en la Figura 7.

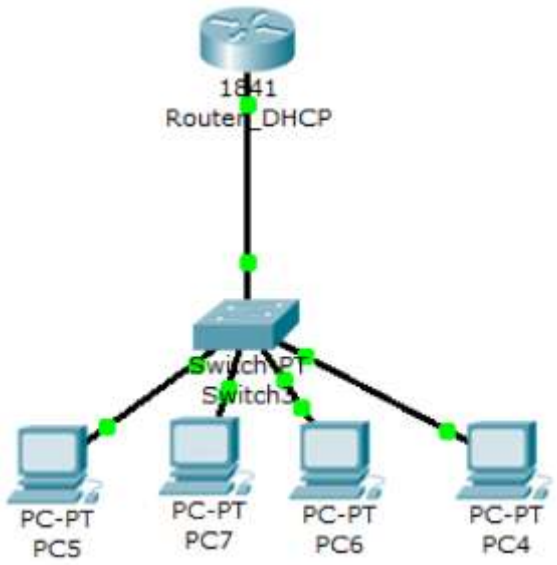


Figura 7. Topología DHCPv6 a configurar por los estudiantes.

Una vez configurada la topología propuesta, deben configurar los computadores para obtener direccionamiento dinámico. Esto se hace de la siguiente manera:

- En el menú Panel de control - clic en conexiones de red.
- En la interfaz de red que se encuentra conectada, clic derecho - propiedades.
- En TCP/IPv6 - propiedades.
- Seleccionar la opción configuración.
- Aplicar y salir.

**Paso 2. Configuración del Enrutador**

- Configure los siguientes parámetros:
- Configuración de la interfaz de red: utilice la siguiente dirección IPv6: 2001:DB8:1234:42::1/64
- Configure un nombre para el enrutador.
- Configure una contraseña.
- Realice los pasos necesarios para la configuración de línea en el Enrutador.

El siguiente paso es realizar la configuración DHCPv6 sobre el enrutador, para esto debe seguir los siguientes pasos:

- En el modo de configuración global, digitar el siguiente comando: ipv6 dhcp pool dhcp-pool, donde: dhcp-pool es el nombre del *pool*, por ejemplo ipv6 dhcp pool

Pool_Unipiloto. Este comando habilita en el enrutador el servicio DHCP y le indica el nombre del *pool* a utilizar. Es posible configurar más de un *pool* dependiendo de cómo quiera realizar la configuración del servicio en el enrutador, de la cantidad de interfaces de red que tenga el enrutador y de si desea distribuir diferentes *pools* por distintas interfaces.

- Utilizar el comando prefix-delegation pool client-prefix-dhcp-pool lifetime 1800 600. Este comando permite especificar al *pool* configurado, un prefijo local para la delegación de direcciones DHCPv6 en los clientes.
- domain-name seguido del nombre del dominio que se asignara a los clientes. Ejemplo: domain-name prueba.com.
- ipv6 local pool client-prefix-dhcp-pool direcciónipv6/máscara. Con este comando le indicamos al *pool* que rango de direcciones debe asignar. Configure la siguiente dirección 2001:db8:1200::/40. Con este paso se finaliza la configuración del servicio DHCP en el Enrutador.
- Revise que los computadores tomaron direccionamiento del rango asignado por el enrutador.
- Realice pruebas ICMPv6 entre los computadores y desde los computadores hacia el enrutador[57][58].

**SECCIÓN 3. Utilizando Wireshark para revisar los paquetes DHCPv6**

Para esta práctica el estudiante debe emplear el software *wireshark*[59]. Con este software, el estudiante podrá observar la solicitud y entrega de paquetes DHCPv6.

[57] Cisco Systems Inc. Cisco 1800 Series Integrated Services Routers. Cisco 1800 Series Integrated Services Routers. [En línea] Cisco Systems Inc. <http://www.cisco.com/en/US/prod/collateral/enrutadores/ps5853/product_data_sheet0900aecd8016a59b.html>

[58] Cysco System Inc. Cisco IOS IPv6 Configuration Guide, Release 12.4. Implementing DHCP for IPv6. Cisco IOS IPv6 Configuration Guide, Release 12.4. Implementing DHCP for IPv6. [En línea] Cysco System Inc., 8 de Abril de 2011. <http://www.cisco.com/en/US/docs/ios/IPv6/configuration/guide/ip6-dhcp.html#wp1055621>

[59] Descarga del software. Disponible [en línea] <http://www.wireshark.org/download.html>

## 7.3 GUÍA NO. 2 - IMPLEMENTACIÓN DUAL-STACK O DOBLE PILA

Durante el desarrollo de esta guía de laboratorio, el estudiante aprenderá cómo activar IPv6 en un enrutador utilizando direcciones tipo *unicast,* además de la instalación de Dual StackEsta guía se realizará en dos partes: en la primera se hará un repaso de los comandos básicos de un enrutador y la preparación del mismo para la configuración IPv6; en la segunda parte se realizará la configuración *Dual Stack*.

La presentación de esta guía en el documento es una versión resumida de la misma, puede consultarse de forma completa en elAnexo B. "Guía No.2 Implementación Dual-Stack o Doble Pila".

### 7.3.1 Objetivos

**General**.El estudiante realizará la preparación y configuración básica de un enrutador Cisco para posterior configurar Dual-Stack.

**Específicos.**Incrementar las capacidades y conocimientos de los estudiantes respecto al mecanismo de transición *Dual Stack*, mediante laboratorios prácticos que fomenten el interés de los estudiantes para el posterior desarrollo de proyectos que ayuden a la transición de la red de la Universidad, al protocolo IPv6.

### 7.3.2 Conceptos Básicos:

- **Enrutamiento Dinámico:** Enrutamiento que se adapta automáticamente a los cambios de la topología o el tráfico de la red[60].
- **Enrutamiento Estático:** Enrutamiento que depende de las rutas ingresadas manualmente en la tabla de enrutamiento.
- **OSPF:***"De sus siglas en ingles Open Shortest Path First (OSPF) es un protocolo de enrutamiento de estado de enlace desarrollado como reemplazo del protocolo de enrutamiento por vector de distancia RIP. RIP constituyó un protocolo de enrutamiento*

[60] Cisco Networking Academy. CCNA Exploration 4.0. Diccionario de conceptos

*aceptable en los comienzos del networking y de Internet; sin embargo, su dependencia en el conteo de saltos como la única medida para elegir el mejor camino rápidamente se volvió inaceptable en redes mayores que necesitan una solución de enrutamiento más sólida. OSPF es un protocolo de enrutamiento sin clase que utiliza el concepto de áreas para realizar la escalabilidad. RFC 2328 define la métrica OSPF como un valor arbitrario llamado costo. El IOS de Cisco utiliza el ancho de banda como la métrica de costo de OSPF"*[61].

- **Adyacencia:***"Relación que se forma entre enrutadores vecinos seleccionados y nodos externos con el fin de intercambiar información de enrutamiento. La adyacencia se basa en el uso de un segmento de medios comunes"*[62]
- **Costo:***"Valor arbitrario, típicamente basado en el conteo de saltos, el ancho de banda de otros medios u otras medidas asignadas por el administrador de red y utilizadas para comparar varias rutas a través de un entorno de internetwork. Los protocolos de enrutamiento utilizan valores de costo para determinar la ruta más favorable hacia un destino particular: mientras más bajo sea el costo, mejor será la ruta"*[63].
- ***Dual-Stack* o Doble Pila:** Es uno de los mecanismos de transición y convivencia de IPv4 a IPv6. En este modelo, todos los nodos presentes configurados en la red, están configurados con los dos protocolos, es decir tienen en su configuración direcciones IPv4 e IPV6, de esta forma, la comunicación se hace utilizando la pila de protocolos correspondiente, para una comunicación IPv4 se usa la pila de protocolo IPv4 y para comunicaciones IPv6 se usa la pila de protocolo IPv6[64].En las Figuras 8 y 9 se relacionan dos ejemplos de implementación *Dual-Stack*.


Figura 8. Ejemplo 1 de Implementación Dual-Stack[65]

[61] Cisco Networking Academy. CCNA Exploration 4.0. Conceptos y protocolos de Enrutamiento. Capítulo 11, numeral 11.0.1. Introducción del capítulo

[62] Cisco Networking Academy. CCNA Exploration 4.0. Diccionario de Conceptos

[63] Cisco Networking Academy. CCNA Exploration 4.0. Diccionario de Conceptos

[64] IPv6: Nueva Generación Protocolo de Internet. Darwin Lamarck Santana Yunes. [en línea]. Disponible en: <http://www.lac.ipv6tf.org/docs/tutoriales/IPv6-LACTF.pdf>

[65] IPv6 Deployment and Support. Introduction to the e-learning package. Co-existence with IPv4 Dual Stack. 2011.[en línea]. Disponible en: <http://www.6deploy.eu/e-learning/english/>.

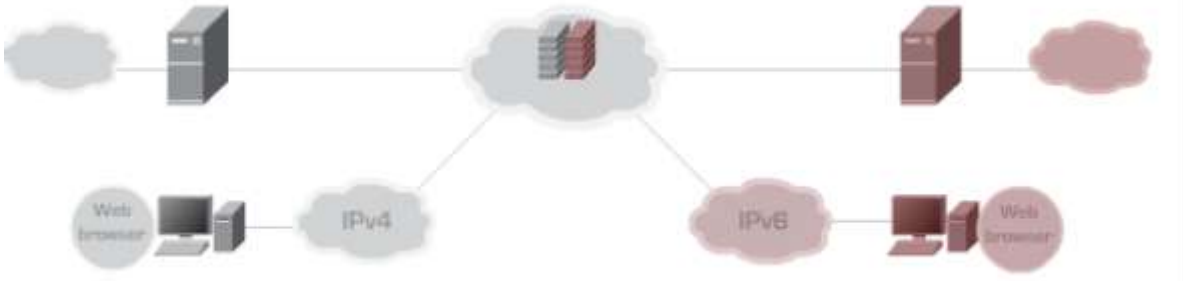


Figura 9. Ejemplo 2 de Implementación Dual-Stack

### 7.3.3 Elementos Requeridos

- Software: *Packet Tracert* 5.3
- 1 Computador por persona.
- Archivos de laboratorio: Dual-Stack.pkt -Tabla_Direccionamiento.xlsx.

### 7.3.4 Informe a realizar por los estudiantes.

El estudiante realizará un informe posterior a este laboratorio, en el que se dé respuesta a las siguientes preguntas:

- ¿Qué rutas OSPF debería configurar en caso de que las redes LAN operaran con IPv6? Explique.
- En caso de que el *Internet Services Provider* (ISP) cambiara alguno de los enlaces WAN, ¿Qué cambios debería realizar en su configuración OSPF para modificar los costos?¿Estos se modificarían automáticamente? Explique.

### 7.3.5 Procedimiento.

A continuación se describen los pasos que deben realizar los estudiantes, para realizar la configuración de una red *Dual-Stack*.

**SECCIÓN 1. Configuración de una Red *Dual-Stack***

Durante esta práctica, el estudiante realizará la preparación y configuración de un enrutador cisco para ser utilizado de manera doble, es decir soportando dos pilas de protocolos (IPv4

e IPv6). También realizará la configuración de los protocolos de enrutamiento OSPFv4 yOSPFv6[66].Debe tener en cuenta la utilización de algunos comandos descritos al inicio del capítulo.

**Instalación Software Cisco *Packet Tracert***. Debe realizar la instalación del software, recuerde que debe tener privilegios administrativos sobre el computador.

**Paso1. Configuración general de los enrutadores**. Solicite al profesor los archivos Dual-Stack.pkt y Tabla_Direccionamiento.xlsx. El primer archivo contiene la configuración del escenario propuesto para el desarrollo de la guía de laboratorio, observará que las interfaces correspondientes al protocolo IPv4 ya se encuentran configuradas. El segundo archivo contiene la configuración que debe realizar en cada una de las interfaces de red, encontrará las configuraciones para IPv4 e IPV6. Realice la configuración de los nombres de los enrutadores de acuerdo a lo propuesto en el archivo Tabla_Direccionamiento.xlsx.

**Paso 2.Configuración de las Interfaces de Red.** Ya que las interfaces de red para IPv4 ya están configuradas, realice la configuración de las interfaces para IPv6 de acuerdo al archivo Tabla_Direccionamiento.xlsx.

**Paso 3. Activación delProtocolo y Configuración de una red Dual-Sack[67]**. Antes de iniciar la configuración en los nodos de una red, es necesario activar el protocolo IPv6 y las direcciones tipo *unicast* con las que se trabajará en este laboratorio.

- Usar el comando: ipv6 unicast-routing [68]en modo privilegiado.
- Para asignar una dirección IPv6 a una interfaz de un nodo de la red (enrutador), se debe usar el comando ipv6 address <prefijo de red/longitud de prefijo de red>. Para ingresar la máscara de red basta con colocar / y el prefijo de la máscara. Ejemplo IPv6 address 2002:13b0:1061::1/64.
- Para ver el estado de las interfaces puede utilizar el comando show ipv6 interface.

En la figura 10, se visualiza la configuración de la red *Dual-Stack*propuesta.

---

[66] Cysco System Inc. Inc. Cisco IOS IPv6 Configuration Guide, Release 12.4. Implementing OSPF for IPv6. July 25, 2011. [en línea] Disponible en: <http://www.cisco.com/en/US/docs/ios/IPv6/configuration/guide/ip6-ospf.html>

[67]Juan Camilo Villanueva, Chistian David Velásquez Díaz. I Curso Taller: Redes de Telecomunicaciones Avanzadas. Manual del curso Taller de Redes de Telecomunicaciones Avanzadas. Perú, Perú : s.n., Agosto de 2010. <http://www.willay.org.pe>

[68] Network Working Group. Request for Comments: 4193 Unique Local IPv6 Unicast Addresses. October 2005. [en línea]. Disponible en: <http://www.ietf.org/rfc/rfc4193.txt>

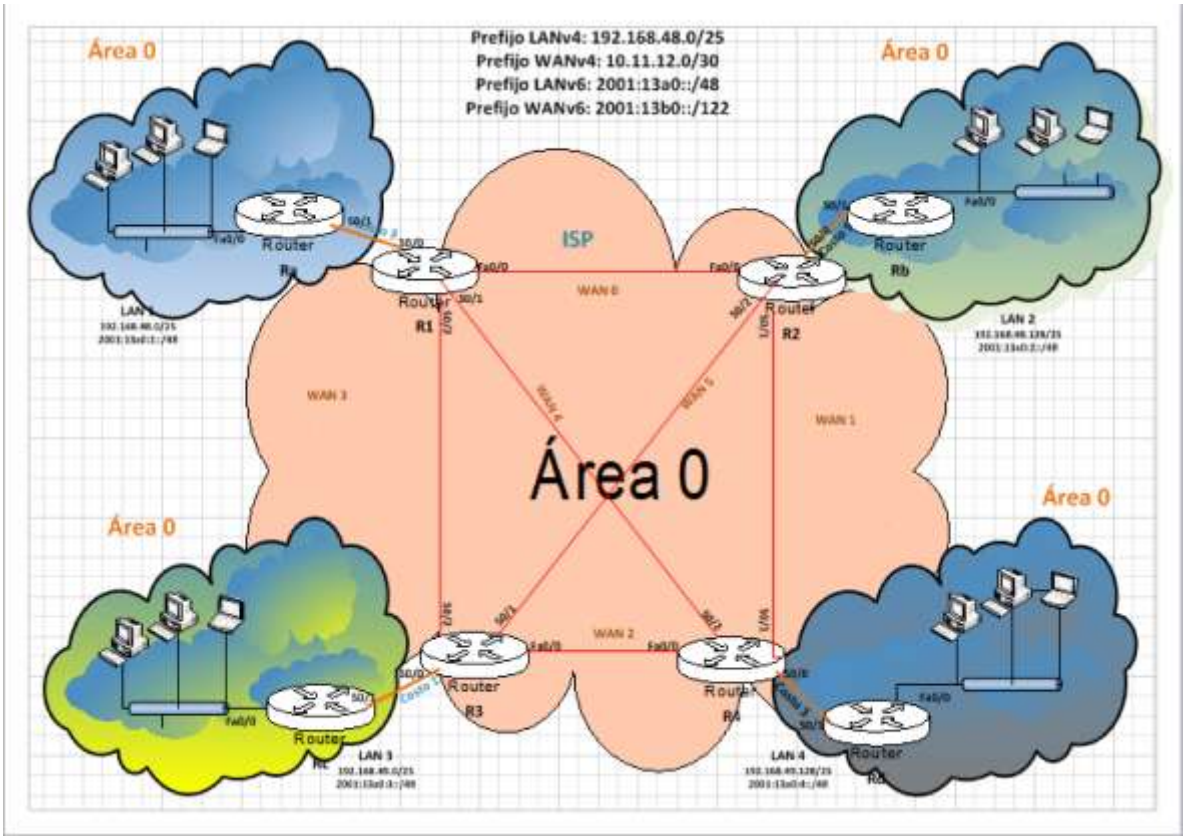


Figura 10. Topología a configurar por los estudiantes para la realización del laboratorio. Creación propia.

- **Configuración Interfaces de Red en IPv4:** Esta configuración viene predeterminada en el archivo que contiene el escenario propuesto. No olvide que los prefijos de subred para los enlaces LAN y WAN son: 192.168.48.0/21 y 10.11.12.0/30 respectivamente.
- **Configuración Interfaces de Red en IPv6:** Realice la configuración de las interfaces de acuerdo a la información suministrada en el archivo *Tabla_Direccionamiento.xlsx*. Recuerde que los prefijos de las redes LANv6 y WANv6 son: 2001:13a0::/48 y 2001:13b0::/122 respectivamente. **Configuración del protocolo *OSPF* para IPv4:** Para realizar esta configuración debe digitar los siguientes comandos:

enrutador osfp # id del proceso

network dirección IP del identificador de red a configurar seguido de la máscara de red y el área a la cuál va a pertenecer. Debe ejecutar estos comandos cada vez que requiera publicar una red. Un ejemplo de esta configuración puede apreciarse en la figura 11:

```
R2>enable
R2#configure terminal
R2(config)#router ospf 2
R2(config-router)#network 60.4.7.4  0.0.0.3  area 1
R2(config-router)#network 191.1.2.0  0.0..0.255 area 1
R2(config-router)#network 60.4.7.8  0.0.0.3 area 0
R2(config-router)#network 142.2.0.0  0.0.255.255 area 0
R2(config-router)#exit
```

Figura 11. Comandos de configuración para OSPFv4. Creación Propia

- Realice la configuración *OSPF* para las redes IPv4 de acuerdo a la topología propuesta en la figura 10. **Nota**: use el número 1 para el proceso de *OSPF* en todos los enrutadores.
- Revise la tabla de enrutamiento utilizando el comando show ip route.
- Realice la configuración IP apropiada para los computadores en cada una de las redes.
- Pruebe conectividad entre todos los computadores y los enrutadores disponibles.

**Configuración del protocolo OSPF para IPv6:** La versión del protocolo *OSPF* para IPv6 es el *OSPFv3* y es especificado por la IETF en el RFC 2740 "*OSPF for IPv6"*[69]. La configuración de este protocolo en IPv6, en comparación con la configuración que debe realizarse para IPv4, es mucho más sencilla. Para realizar la configuración debe emplear el comando:

- Recuerde que al trabajar con direcciones *unicast*, debe emplear el comando: IPv6 unicast-routing para configurar al enrutador a utilizar direcciones de este tipo.
- Con el comando ipv6 ospf <identificador de proceso OSPF> área <área donde pertenece la interfaz> se realiza la configuración de este protocolo de enrutamiento en el enrutador. En la figura 12 puede apreciar un ejemplo.

```
Router>enable
Router#configure terminal
Router(config)#interface fastethernet 0/1
Router(config-if)#ipv6 ospf 1 area 4
Router(config-if)#exit
```

Figura 12.Comandos de Configuración OSPFv6. Creación propia.

[69] Network Working Group. Requests for Comments: 2740 OSPFv6.December 1999. [en línea].Disponible en: <http://www.ietf.org/rfc/rfc2740.txt>

- Realice la configuración OSPF para las redes IPv6 de acuerdo a la topología propuesta en la figura 10.

  **Nota:** use el número 1 cómo identificador de proceso de OSPF en todos los enrutadores.

- Revise la tabla de enrutamiento utilizando el comando show ipv6 route.
- Pruebe conectividad entre todos los computadores y enrutadores; puede emplear el comando ping desde cualquiera de los enrutadores hacia una de las direcciones IPv6 de los enrutadores vecinos.
- Observe el trayecto que sigue la información enviada desde una de las LAN hacia las demás. Explique (puede apoyarse en el comando tracert).
- Puede realizar la configuración de los computadores con direcciones IPv6 para que realice pruebas entre las LAN con ICMPv6.
- Una vez finalizada y comprobada la conectividad de todos los computadores y enrutadores tanto en IPv4 cómo en IPv6, la configuración *Dual-Stack*[70] habrá finalizado con éxito.

## 7.4 GUÍA NO. 3 - IMPLEMENTACIÓN TÚNELES 6TO4

En esta guía el estudiante realizará una configuración para activar un túnel 6to4[71] entre dos enrutadores. También repasará y pondrá en práctica los conceptos de enrutamiento. Durante el desarrollo de la guía se utilizará el protocolo *Enhanced Interior Gateway Routing Protocol* (EIGRP)[72] para el enrutamiento del protocolo IPV4. No obstante, el estudiante puede realizar modificaciones para utilizar *OSFP*, que fue utilizado en la guía 2.

---

[70] 6deploy. IPv6 Deployment and Support. IPv6 Deployment and Support. [En línea] [Citado el: ] <http://www.6deploy.eu/e-learning/english/>

[71] Cysco System Inc. Implementing Tunneling for IPv6. June 24, 2011. [en línea] Disponible en: http://www.cisco.com/en/US/docs/ios/ios_xe/IPv6/configuration/guide/ip6-tunnel_xe.html.

[72] Cisco System. Cisco IOS XR Routing Configuration Guide, Release 3.7. Implementing EIGRP on Cisco IOS XR Software. [en línea]. Disponible en: <http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.7/routing/configuration/guide/rc37egp.html>

La presentación de esta guía en el documento es una versión resumida de la misma, puede consultarse de forma completa en elAnexo C. "Guía No. 3, Implementación de Túneles 6to4"

### 7.4.1 Objetivos

**General.** Realizar la preparación, configuración y enrutamiento de túneles 6to4 con enrutadores Cisco.

**Específicos.** Otorgar al estudiante conocimientos generales para la configuración de un enrutador cisco basado en el protocolo de enrutamiento EIGRP.

Afianzar los conocimientos de los estudiantes en protocolos de enrutamiento y mecanismos de convivencia entre los protocolos IPv4 e IPv6.

### 7.4.2 Conceptos Básicos

- ***EIGRP.****"El Enhanced Interior Gateway Routing Protocol (EIGRP) es un protocolo de enrutamiento por vector de distancia, como su nombre lo sugiere, EIGRP es un IGRP de Cisco mejorado (Interior Gateway Routing Protocol). Los dos son protocolos patentados de Cisco y sólo funcionan con los enrutadores de Cisco. Aunque EIGRP puede actuar como un protocolo de enrutamiento de estado de enlace, todavía sigue siendo un protocolo de enrutamiento por vector de distancia*"[73].
- **Túneles *6to4.****"Este mecanismo se puede implementar para comunicar redes IPv6 aisladas por medio de una red IPv4. El enrutador extremo de la red IPv6 crea un túnel sobre IPv4 para alcanzar otra red IPv6. Los extremos del túnel son identificados por el prefijo del sitio IPv6. Este prefijo consiste en 16 bits fijos que indican que estamos utilizando 6to4 más 32 bits que identifican al enrutador externo del sitio"*[74].
- **Interfaz *Loopback***. Una interfaz de loopback es una interfaz virtual pero que realiza todas las funciones de un interfaz física normal, puede ser configurada con el comando interface loopback interface-number, donde interface-*number* es un número entero. Las interfaces de *loopback* se encuentran siempre en estado "up and up" a menos que sean administrativamente puestas en estado shutdown.[75].

---

[73] Cisco Networking Academy. CCNA Exploration 4.0. Conceptos y protocolos de Enrutamiento. Capítulo 9, numeral 9.0.1. Introducción del capítulo.

[74] IPv6: Nueva Generación Protocolo de Internet. Darwin Lamarck Santana Yunes. Disponible. [en línea] <http://www.lac.ipv6tf.org/docs/tutoriales/IPv6-LACTF.pdf>

[75] CCNA ICND2 Official Exam Certification guide Second Edition, página 367. [Curso de Certificación de Cisco].

### 7.4.3 Elementos Requeridos

- Computador por persona que cuente con sistemas operativos: *Windows XP, Vista o 7.*
- *Patch cord*.
- Enrutador Cisco 1841
- Cables de Consola para el Enrutador.

### 7.4.4 Informe a realizar por los estudiantes.

El estudiante debe detallar el procedimiento para realizar una configuración como la que se aprecia en la figura 13,en la cualpermita un túnel 6to4 entre los enrutadores R1 y R5. Adicionalmente, debe anexar la configuración de los Enrutadores R1 y R5 y de Frame Relay. Puede utilizar las herramientas*GNS*3 o *Packet Tracer* para realizar la configuración.

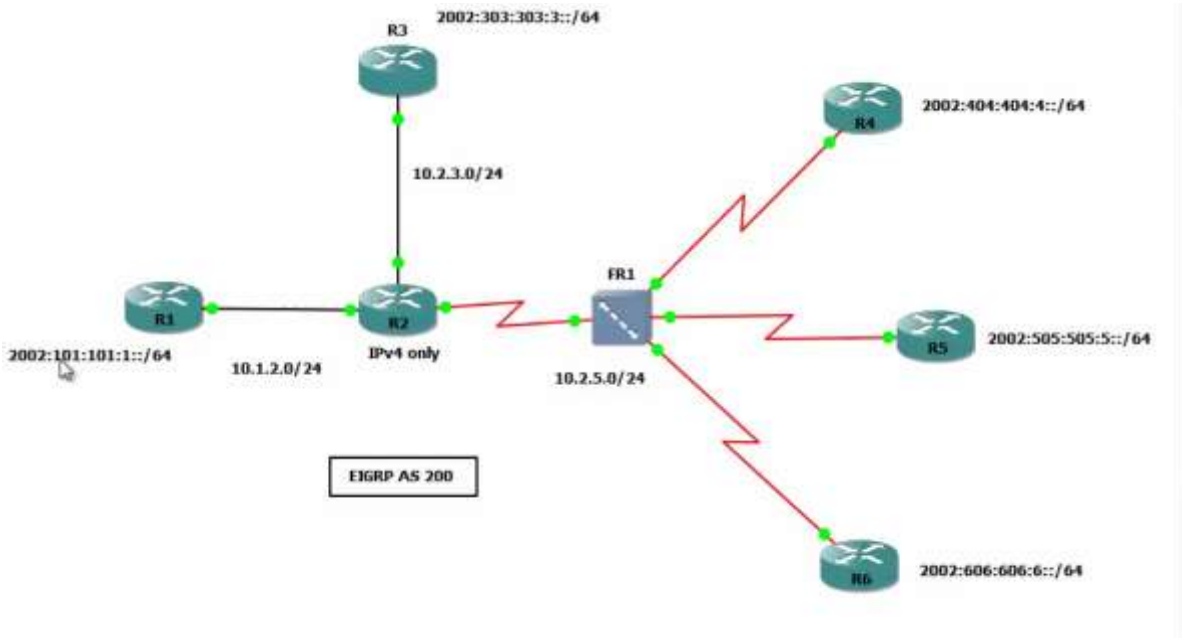


Figura 13. Topología propuesta para realizar por el estudiante posterior al laboratorio.[76]

[76] GNS3. Graphical Network Simulator. GNS3, an opensource multiplatform graphical network simulator 2011 [en línea]. Disponible en: <http://www.gns3-labs.com/>

### 7.4.5 Procedimiento.

A continuación se describen de forma detallada, los pasos a realizar por los estudiantes para la configuración de un túnel empleando el mecanismo de túneles 6to4 y el protocolo de enrutamiento *EIGRP*.

**SECCIÓN 1. Configuración de un túnel 6to4**

Durante esta práctica, el estudiante realizará la configuración para permitir la comunicación entre dos redes a través de un túnel 6to4 [77] utilizando el protocolo de enrutamiento EIGRP, el cual servirá para realizar el enrutamiento de las redes IPv4. Debe tener en cuenta la utilización de algunos comandos descritos al inicio del capítulo.

**Paso1. Preparación del enrutador.** Borre la configuración actual que posee el enrutador y reinícielo; esto evitará que tenga conflictos con configuraciones anteriores. Asegúrese que la versión de IOS que tiene el enrutador sea la 12.4.

**Paso2. Configuración general de los enrutadores**. Realice las configuraciones necesarias para establecer los nombres en los enrutadores de acuerdo a la topología propuesta en la figura 14

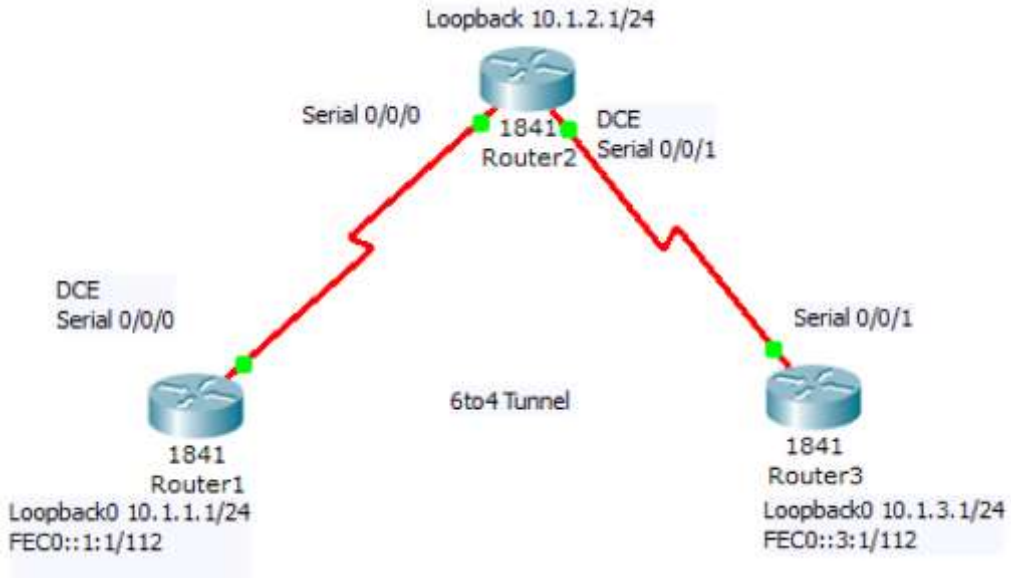


Figura 14. Topología propuesta para la configuración de túneles 6to4. Creación propia.

[77] Cedia. Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado. Curso Ipv6 Enero 2010. Práctica 1. Configuración IPv6, rutas estáticas y túneles 6in4. [en línea]. Disponible en: <http://dspace.cedia.org.ec/bitstream/123456789/44/2/cedia IPv6curso.pdf>.

**Nota:**Recuerde que esta topología es propuesta y está sujeta a cambios de acuerdo a los recursos de laboratorio y el número de estudiantes.

**Paso 3. Configuración de las Interfaces Físicas y de *Loopback***. Configure las interfaces físicas y de *loopback* para IPv4 e IPv6 en todos los enrutadores. Realice también la configuración de relojes de acuerdo a lo indicado en la figura anterior. Los pasos para realizar la configuración son:

**Enrutador R1:**

interface loopback0

ip address 10.1.1.1 255.255.255.0

ipv6 address FEC0::1:1/112 interface serial0/0/0

ip address 172.16.12.1 255.255.255.0

clockrate 64000

no shutdown

**Enrutador R2:**

interface loopback0

ip address 10.1.2.1 255.255.255.0

interface serial0/0/0

ip address 172.16.12.2 255.255.255.0

no shutdown

interface serial0/0/1

ip address 172.16.23.2 255.255.255.0

clockrate 64000

no shutdown

**Enrutador R3:**

interface loopback0

ip address 10.1.3.1 255.255.255.0

ipv6 address FEC0::3:1/112

interface serial0/0/1

ip address 172.16.23.3 255.255.255.0

no shutdown

**Paso 4. Configuración de las Rutas *EIGRP***. Realice la configuración para realizar el enrutamiento entre los tres enrutadores. Para realizar este enrutamiento se configurará el protocolo *EIGRP* utilizando las redes 172.16.0.0 y 10.0.0.0. Una vez realizada esta configuración, debe tener conectividad entre los tres enrutadores. La configuración que debe realizar es la siguiente:

**Enrutador R1:**

enrutador eigrp 1

no auto-summary

network 10.0.0.0

network 172.16.0.0

**Enrutador R2:**

enrutador eigrp 1

no auto-summary

network 10.0.0.0

network 172.16.0.0

**Enrutador R3:**

enrutador eigrp 1

no auto-summary

network 10.0.0.0

network 172.16.0.0

**Paso 5. Configuración del túnel 6to4**. Un túnel es una interfaz lógica que actúa como un vínculo lógico entre dos puntos de conexión. Sin embargo al no ser una interfaz física, pueden estar involucrados más de dos puntos de conexión, es decir, podríamos configurar un túnel para más de dos enrutadores. Un túnel 6to4 usa direcciones IPv6 especiales dentro del rango 2002::/16. Los primeros 16 bits son el número 2002 en hexadecimal, y los 32 bits siguientes corresponden a la fuente original de la dirección IPv4 en formato hexadecimal. Un túnel 6to4 no requiere una dirección de destino, ya que no es un enlace punto a punto. En este laboratorio, se van a configurar los enrutadores R1 y R3 como túnel *6to4* para proporcionar conectividad IPv6 entre sus interfaces de *loopback*. Para configurar un túnel 6to4, debe obtener la configuración de la interfaz de túnel, puede utilizar la interfaz serie 0. luego, debe establecer el modo de túnel sobre el enrutador, para esto puede emplear el

comando tunnel mode ipv6ip 6to4, más adelante observará la secuencia completa de comandos para culminar la configuración en su totalidad[78].

Ahora debe saber cuál es la dirección IPv6 que será utilizada para el túnel. Para esto debe utilizar el concepto revisado en el párrafo anterior, de este modo, la dirección a configurar en el enrutador R1 es 2002:AC10:0C01:1::1/64, donde AC10:0C01 corresponde a la dirección 172.16.12.1, con 172 = AC, 16 = 10, 12 = C y 1 = 1. El 1 indica la subred específica y el 1 al final es la dirección de host. Para realizar el cálculo de la dirección del enrutador R3, se emplea el mismo mecanismo, por tanto la dirección para este enrutador es: 2002:AC10:1703:1::3/64. Tenga en cuenta que las dos direcciones no están en la misma subred /64[79].

Después de configurar las direcciones IPv6, deberá continuar con la interfaz de origen para el túnel utilizando el comando tunnel source. Una vez realizada la configuración del túnel, debe establecer una ruta IPv6 estática para todo el rango 2002::/16; use el comando ipv6 route para la interfaz del túnel en la que realice la configuración. A continuación se detallan los pasos para realizar la configuración sobre cada uno de los enrutadores:

**Enrutador R1:**

interface tunnel 0

tunnel mode ipv6ip 6to4

ipv6 address 2002:AC10:0C01:1::1/64

tunnel source serial0/0/0

exit

ipv6 route 2002::/16 tunnel0

**Enrutador R3:**

interface tunnel 0

tunnel mode ipv6ip 6to4

ipv6 address 2002:AC10:1703:1::3/64

tunnel source serial0/0/1

exit

ipv6 route 2002::/16 tunnel0

---

[78] Cisco Systems. 6bone Connection Using 6to4 Tunnels for IPv6. Document ID: 45741. Augost 10, 2005. [en línea]. Disponible en:http://www.cisco.com/en/US/tech/tk872/technologies_configuration_example09186a00801f3b4f.shtml.

[79] Cisco Networking Academy Program. CCNP: Building Scalable Internetworks v5.0 - Lab 8-3. Páginas 1-9.

Realice pruebas de ICPM a través del comando ping desde cada uno de los enrutadores para comprobar conectividad. En caso que las respuestas desde ambos extremos no sean satisfactorias, debe revisar cada uno de los pasos antes descritos para encontrar la falla.

**Paso 6. Configuración de rutas estáticas IPv6**. Al igual que IPv4, IPv6 puede tener rutas estáticas dentro de su tabla de enrutamiento. En el paso anterior usted creó una ruta estática para el rango 2002::/16. Durante este paso, se configuró una ruta estática en R1 especificando cómo llegar a la interfaz de *loopback R3* y viceversa. Al igual que en IPv4, en IPv6 las rutas estáticas se crean con la dirección del próximo salto, en este caso el siguiente salto para los enrutadores es la dirección IPv6 del otro extremo del túnel. Recuerde que antes de comenzar a realizar el enrutamiento debe habilitar el enrutador para uso direcciones *unicast* con el comando ipv6 unicast-routing. A continuación se explica la configuración detallada a realizar:

**Enrutador R1:**

ipv6 unicast-routing

ipv6 route FEC0::3:0/112 2002:AC10:1703:1::3 Luego, puede observar la configuración completa de la tabla de enrutamiento utilizando el comando show ipv6 route.

Debe obtener una respuesta similar a esta: S 2002::/16 [1/0] vía ::, Tunnel0; donde ***S*** especifica que es una ruta estática; puede guiarse observando las convenciones que aparecen en el enrutador una vez digitando el comando.

**Enrutador R3:**

ipv6 unicast-routing

ipv6 route FEC0::1:0/112 2002:AC10:C01:1::1

De igual forma puede revisar la tabla de enrutamiento con el comando: show ipv6 route.

Puede verificar la conectividad validando las tablas de enrutamiento, o ejecutando el comando ping a las interfaces IPv6 de *loopback* en cada uno de los enrutadores.

## 7.5 GUÍA NO. 4 - IMPLEMENTACIÓN DE REDES USANDO DOS MECANISMOS DE TRANSICIÓN Y CONVIVENCIA

Con base en las dos guías anteriores, el estudiante simulará una pequeña red en la cual conecte dos redes a través de un ISP (simulado) configurando *6to4* y *Dual Stack*.

La presentación de esta guía en el documento es una versión resumida de la misma, puede consultarse de forma completa en el Anexo D. "Guía No. 4".

### 7.5.1 Objetivos

**General**. Implementar la configuración de laboratorios que permitan utilizar mecanismos de transición y convivencia tal y como se trabajaría en entornos reales empresariales. Esta guía se desarrollará utilizando la modalidad de caso de estudio, para así facilitar el acercamiento a ambientes de producción.

**Específicos.** Orientar al estudiante en la configuración de laboratorios que permitan realizar pruebas posteriores de conectividad con redes IPv6 reales.

Motivar al estudiante a realizar planteamientos en mecanismos de transición y convivencia que posteriormente sirvan a la Universidad Piloto de Colombia a realizar la transición de su infraestructura a IPv6.

### 7.5.2 Elementos Requeridos

- Computador por persona que cuente con sistemas operativos: Windows XP, Vista o 7.
- *Patch cord*
- *Packet Tracert* o *GNS3*
- *Wireshark*

### 7.5.3 Informe a realizar por los estudiantes.

El estudiante debe detallar el procedimiento para realizar la configuración propuesta en la figura 15

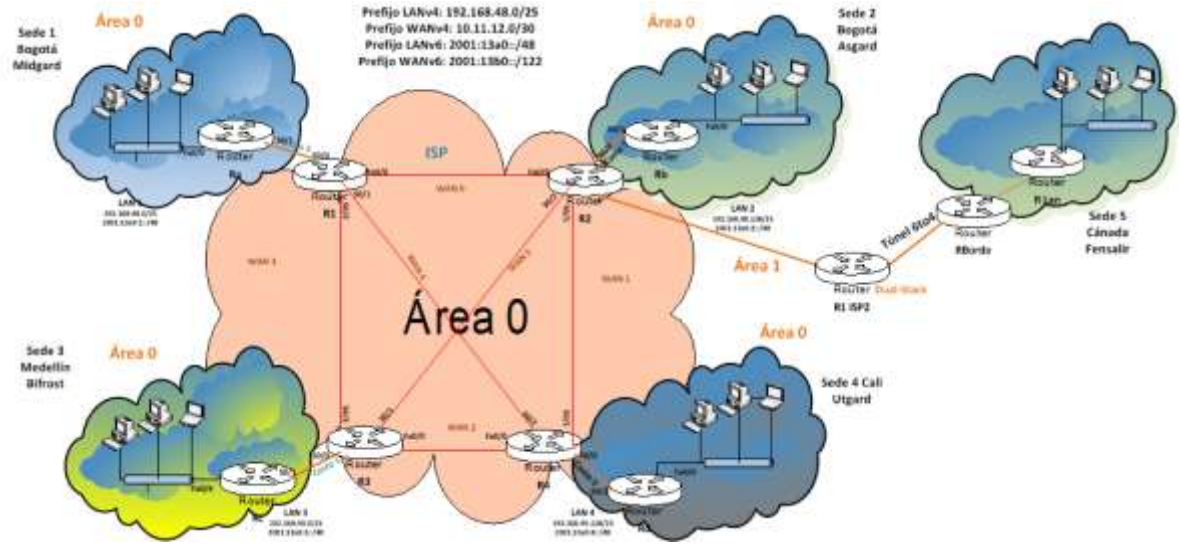


Figura 15. Topología propuesta para la realización del laboratorio. Creación propia

### 7.5.4 Procedimiento.

Durante esta guía el estudiante realizará la configuración propuesta de acuerdo a la figura 15, teniendo en cuenta el siguiente escenario:

**SECCIÓN 1. Caso de estudio**

La compañía Sigma Telecomunicaciones dedicada a la prestación de servicios de *hosting* (alojamiento), se encuentra en proceso de expansión de su negocio a nivel internacional. Bajo este precedente y la demanda de servicios de sus clientes actuales, ha decidido comenzar la transición de IPv4 a IPv6, lo cual le permitirá mejorar la velocidad en los servicios ofrecidos a sus clientes y mantenerse actualizados según la estandarización a nivel mundial. De acuerdo con esto, la compañía cuenta con 5 sedes distribuidas así:

- **Sede 1. Midgar**: Esta es la sede principal de la compañía en la cual se encuentran las áreas administrativas, áreas de soporte técnico niveles 1 y 2, y un *datacenter* (centro de datos o centro de procesamiento de datos) que aloja todos los servicios corporativos.
- **Sede 2 Asgard**: En esta sede se encuentran las áreas de soporte nivel 3, desarrollo y otro datacenter que tiene una réplica exacta de los servicios prestados en Midgar y algunos servicios de clientes pequeños.
- **Sede 3 Bifrost**: En esta sede se encuentra el alojamiento de todos los clientes de la compañía, además tiene una cintoteca para copias de seguridad (debido a que la principal se encuentra en manos de un tercero) en la que almacenan las copias realizadas a los servicios de sus clientes.
- **Sede 4 Udgard**: Esta sede tiene una réplica exacta de los servicios prestados por el datacenter de Bifrost, adicionalmente cuenta con personal de soporte nivel 1.

- **Sede 5 Fensalir**: Esta es la más reciente de las sedes de la compañía que aún no se encuentra en funcionamiento y que tendrá un *datacenter* que replicará con Bifrost. Esto con el fin de prestar servicios internacionales requeridos por los clientes, además alojará servicios que se contratarán con clientes de Estados Unidos y Canadá.

De acuerdo a las especificaciones anteriores, el estudiante debe realizar la configuración para conectar a Midgar, Asgard, Bifrost y Udgar con Fensalir. Puede apoyarse en la configuración que se realizó en la guía No. 2, teniendo en cuenta el direccionamiento IP y las configuraciones OSPF realizadas tanto para IPv4 como para IPv6. Tenga en cuenta que la red administrativa perteneciente a Midgar no debe verse con la red de Fensalir y además debe suponer que en Bifrost debe crearse una nueva red para pruebas que tenga conectividad con las demás sedes, pero no con la red administrativa.

Realice los siguientes pasos:

**Paso 1**: Realice el diseño de direccionamiento, para IPv4 e IPv6 (use direcciones tipo *unicast*) de las redes LAN y WAN.

**Paso 2**: Realice las configuraciones correspondientes a OSPF y *Dual-Stack* para la interconexión de las cuatro sedes en Colombia.

**Paso 3**: Realice la configuración *Dual-Stack* en los enrutadores R1 ISP2 y Rborde.

**Paso 4**: Realice la configuración de túnel 6to4 para conectar los routes R1 ISP2 y Rborde.

**Paso 5**: Realice pruebas de conectividad entre las sedes, en especial con Fensalir.

**Paso 6**: Apóyese en el programa Wireshark para observar el trazado y estructura del paquete IPv6 cuando realiza las pruebas de conectividad.

**Paso 7**: En las sedes Bifrost y Fensalir, configure dos servidores Web, uno con direccionamiento v6 y el otro con direccionamiento v4.

**Paso 8**: Realice peticiones Web (en ipv4 e IPv6) a través del puerto 80 entre los servidores de las dos sedes.

# 8. MATERIAL DOCENTE

El material a continuación descrito apoyará al docente en la instrucción de los contenidos teóricos que debe tener el estudiante antes de la realización de las guías 1,2 y3.

La presentación del material docente se presenta de forma completa en el Anexo E.

## 8.1 MATERIAL DOCENTE PARALA GUÍA DE LABORATORIO NO. 1

| Requisitos | Especificación |
|---|---|
| Asignatura Redes de Computadoras | Conocimientos generales en el protocolo de comunicaciones IPv6 |
| **Resultados Esperados:** | |
| El estudiante realizará la guía de laboratorio propuesta en el capítulo 7 numeral 7.2 anexo A, una vez el docente haya explicado el fundamento teórico presentado en el capítulo 6 y en Anexo E. | |

### 8.1.1 Unidades Temáticas

| Guía | Nombre de la Unidad | Duración |
|---|---|---|
| 1 | Introducción a IPv6 | 2 Horas |

| Contenidos | Resultados de Aprendizaje | Referencias Bibliográficas |
|---|---|---|
| 1. Introducción a IPv6<br>2. Características de IPv6.<br>3. Diferencias entre IPv4 e IPv6.<br>4. Composición del paquete IPv6.<br>5. Arquitectura de direccionamiento. | Al final de la sesión se espera que el estudiante:<br>1. Reconoce los conceptos de básicos de IPv6.<br>2. Reconoce la importancia IPv6 como nuevo protocolo de comunicación.<br>3. Identifique las diferencias entre IPv4 e IPv6. | RFC 2460<br>Microsoft<br>Introducción a IPv6.<br>Referencias mencionadas en el capítulo 6. |

| | | |
|---|---|---|
| | 4. Identifique los conceptos básicos involucrados composición del paquete IPv6.<br>5. Identifique la arquitectura de direccionamiento en IPv6 y encuentre las diferencias respecto a IPv4. | |

## 8.2 MATERIAL DOCENTE PARALA GUÍA DE LABORATORIO NO. 2

| Requisitos | Especificación |
|---|---|
| Asignatura Redes de Computadoras | Mecanismo de Convivencia Dual-Stack. |
| **Resultados Esperados:** | |
| El estudiante realizará las guías de laboratorio propuestas en el capítulo 7 numeral 7.3 una vez el docente haya explicado el fundamento teórico presentado en el capítulo 6 y en el Anexo F. | |

### 8.2.1 Unidades Temáticas

| Guía | Nombre de la Unidad | Duración |
|---|---|---|
| 2 | Mecanismo de Convivencia Dual-Stack | 2 Hora |

| Contenidos | Resultados de Aprendizaje | Referencias Bibliográficas |
|---|---|---|
| 1. Protocolos de Enrutamiento principales para configuraciones LAN.<br><br>1.1 RIP<br>1.1.1 Características en IPv4<br>1.1.2 Características IPv6<br><br>1.2 OSPF.<br>1.2.1 Características en IPv4<br>1.2.2Características en IPv6.<br><br>2. Mecanismo de Convivencia Dual – Stack<br>2.1 Características<br>2.2 Beneficios | Al final de la sesión se espera que el estudiante:<br>1. Comprenda el funcionamiento de Dual-Stack.<br>2. Identifique los protocolos de enrutamiento que puede usar para implementar Dual-Stack. | Referencias mencionadas los capítulos 6 y 7.<br>Adicionales:<br>https://learningnetwork.cisco.com<br>http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/ipv6_sol/ipv6dswp.pdf<br>http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html |

| | | |
|---|---|---|
| | | http://www.6deploy.eu/e-learning/english/ |

### 8.3 MATERIAL DOCENTE PARALA GUÍA DE LABORATORIO NO. 3

| Requisitos | Especificación |
|---|---|
| Asignatura Redes de Computadoras<br>Asignatura Internet | Mecanismo de Convivencia Túnel 6to4 |
| **Resultados Esperados:** | |
| El estudiante realizará la guía de laboratorio propuesta en el capítulo 7 numeral 7.4 una vez el docente haya explicado el fundamento teórico presentado en el capítulo 6 y en el Anexo G. | |

#### 8.3.1 Unidades Temáticas

| Guía | Nombre de la Unidad | Duración |
|---|---|---|
| 3 | Mecanismo de Convivencia Túnel 6to4 | 2 Hora |
| **Contenidos** | **Resultados de Aprendizaje** | **Referencias Bibliográficas** |
| 1. Protocolos de Enrutamiento principales para configuraciones WAN.<br>1.1 EIGRP<br>1.1.1 Características en IPv4<br>1.1.2 Características IPv6<br><br>2. Mecanismo de trancisiónTúneles 6to4.<br>2.1 Características.<br>2.2 Beneficios | Al final de la sesión se espera que el estudiante:<br>1. Comprenda el funcionamiento del mecanismo de convivencia túneles 6to4.<br>2. Identifique cuando realizar una implementación Dual-Stack o 6to4. | Referencias mencionadas los capítulos 6 y 7<br><br>Adicional:<br><br>https://labs.ripe.net/Members/emileaben/6to4-how-bad-is-it-really<br><br>http://gridtics.frm.utn.edu.ar/docs/EnIDI%2008%20IPv6%20Transicion.pdf |

# 9. CONCLUSIONES Y RECOMENDACIONES

## 9.1 SOBRE IPV6 Y LOS MECANISMOS DE CONVIVENCIA

Día a día crece el número de usuarios conectados a la red de redes lo que ha implicado una creciente demanda de los servicios que son ofrecidos por la misma. De la misma forma, dichos servicios son cada vez más especializados y requieren transmitir paquetes más grandes de tipo multimedia. De acuerdo con esto, es evidente que IPv4 comienza a presentar falencias al enfrentar dicha demanda. IPv4 no fue concebido teniendo en consideración el crecimiento exponencial de la demanda causada por los servicios y aplicaciones en la actualidad.

En este trabajo se deja claridad acerca de la importancia y necesidad de llevar a cabo la implementación del protocolo de comunicaciones IPv6, ya que las mejoras que ofrece están relacionadas con una mejor calidad en el servicio, soporte a mayor demanda tecnológica por parte de las aplicaciones y trae consigo soporte nativo para redes móviles, que se encuentran madurando significativamente en la actualidad.

Inicialmente, establecer la convivencia para la transición entre los dos protocolos no será una tarea trivial. Sin embargo, no es imposiblepero es importante que las organizaciones que comiencen con sus respectivos planes de transición, sean precisas con la información que poseen acerca de los dispositivos de comunicaciones con los que cuenta, para asegurar que éstos soportan el nuevo protocolo o en caso contrario, consolidar planes de adquisición de dispositivos compatibles; por otra parte es transcendental que la información sobre la topología física y lógica de la red de la organización, sea conocida por todas las personas involucradas en el plan, con el fin de permitir apoyar la toma de decisión de manera informada, acerca del mecanismo de convivencia más adecuado para cada caso específico.

## 9.2 SOBRE IPV6 Y EL DISEÑO DE LABORATORIOS

El aporte del presente trabajo, establece una base teórico-práctica de conocimientos, preparación y acercamiento a los estudiantes del programa de Ingeniería de Telecomunicaciones de la Universidad Piloto de Colombia, sobre el nuevo protocolo de comunicaciones IPv6, su importancia en el mundo y la necesidad de estar preparados para atender la demanda que se presentará durante su implementación y transición a nivel mundial.

Los laboratorios se diseñaron para que el estudiante realice un paso a paso según las actividades propuestas en cada una.

## 9.3 RECOMENDACIONES

La Universidad Piloto de Colombia tiene en su inventario de dispositivos de laboratorio, enrutadores marca Cisco modelo 1841, los cuales son utilizados en la industria como para configuraciones de redes pequeñas [80], son apropiados para realizar prácticasen configuraciones IPv6y se encuentran en buenas condiciones físicas. Sin embargo, y como parte de los hallazgos derivados del desarrollo del presente trabajo, se realizan las siguientes recomendaciones:

- Los dispositivos enrutadores con los cuales cuenta la Universidad Piloto de Colombia relacionados en el Anexo H (inventario de equipos de Laboratorio) deben realizar una actualización de IOS (Internetwork Operative System) o Sistema Operativo del enrutador.

En la guía No. 3 se indica la versión IOS que deben tener los dispositivos para permitir las configuraciones propuestas en las guías de laboratorio anexas.En los Anexos I y J se relacionanlos correos electrónicoscon los cuales se solicita al director de laboratorios de Telecomunicaciones realizar dicha actualización.

- Validación de cada uno de los enrutadores ya que algunos no tienen ninguna versión de IOS cargada, por tanto no es posible realizar ninguna práctica con ellos. En el anexo I se relacionan los dispositivos con este problema.

- Antes de realizar cualquier práctica de laboratorio con los dispositivos enrutadores o switch, es recomendable realizar un borrado a la configuración para que no interfiera con configuraciones anteriores. En la guía No. 4 se indica esta recomendación.

- La guía No.2 sugiere una topología basada en 8 enrutadores, la universidad Piloto de Colombia únicamente cuenta con 4 enrutadores modelo 1841 y dos enrutadores modelo 805 (la implementación de IPv6 sobre estos dispositivos dependen netamente de sus capacidades físicas para soportar el IOS apropiado), los cuales son insuficientes para realizar una práctica de laboratorio como la planteada en esta guía, por esta razón se creó una simulación usando el software Packet Tracer para tal fin. Es recomendable que

[80]Cisco Systems Inc. Cisco 1800 Series Integrated Services Routers. Cisco 1800 Series Integrated Services Routers. [En línea] Cisco Systems Inc. <http://www.cisco.com/en/US/prod/collateral/enrutadores/ps5853/product_data_sheet0900aecd8016a59b.html>

la Universidad cuente con más dispositivos enrutadores para realizar prácticas de este tipo, ya que esto permite a los estudiantes contar con ambientes más reales y no simulaciones.

## BIBLIOGRAFÍA


6deploy. IPv6 Deployment and Support. IPv6 Deployment and Support. [en línea] Disponible en: <http://www.6deploy.eu/e-learning/english/>

CCNA ICND2 Official Exam Certification guide Second Edition, página 367. [Curso de Certificación de Cisco].

Cedia. Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado. Curso Ipv6 Enero 2010. Práctica 1. Configuración IPv6, rutas estáticas y túneles 6in4. [en línea]. Disponible en: <http://dspace.cedia.org.ec/bitstream/123456789/44/2/cedia IPv6 curso.pdf>.

Cisco Networking Academy Program. CCNP: Building Scalable Internetworks v5.0 - Lab 8-3. Páginas 1-9.

Cisco Networking Academy. CCNA Exploration 4.0. Conceptos y protocolos de Enrutamiento. Capítulo 11, numeral 11.0.1. Introducción del capítulo

Cisco Networking Academy. CCNA Exploration 4.0. Conceptos y protocolos de Enrutamiento. Capítulo 9, numeral 9.0.1. Introducción del capítulo.

Cisco Networking Academy. CCNA Exploration 4.0. Diccionario de Conceptos. [material didáctico cursos de certificación].

Cisco Networking Academy. CCNA Exploration 4.0. Diccionario de conceptos

Cisco System Documents. Cisco IOS IPv6 Configuration Guide Release 12.4T. Marzo 5 de 2009. [en línea] Disponible en: <http://www.cisco.com/en/US/docs/ios/IPv6/configuration/guide/12_4t

Cisco System Inc. Application Visibility and Control for IPv6. 2011. [en línea]. Disponible en: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/aag_c45-665915.pdf

Cisco System Inc. Cisco IPv6 products, solutions, and services. 2010. [en línea]. Disponible en: <thttp://www.cisco.com/go/ipv6>.

Cisco System Inc. Cisco Networking Academy. CCNA Exploration 4.0. Diccionario de conceptos. [Definición: *"Clasificación de la confiabilidad de una fuente de información de enrutamiento]."*

Cisco System. Cisco IOS XR Routing Configuration Guide, Release 3.7. Implementing EIGRP on Cisco IOS XR Software. [en línea]. Disponible en: <http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.7/routing/configuration/guide/rc37egp.html>

Cisco Systems Inc. Cisco 1800 Series Integrated Services Routers. Cisco 1800 Series Integrated Services Routers. [En línea] Cisco Systems Inc. <http://www.cisco.com/en/US/prod/collateral/enrutadores/ps5853/product_data_sheet0900aecd8016a59b.html>

Cisco Systems, Inc. IPv6 Site and Solutions. 2011. [en línea]. Disponible en http://www.cisco.com y <http:// http://www.cisco.com/web/solutions/netsys/ipv6/index.html>.

Cisco Systems. 6bone Connection Using 6to4 Tunnels for IPv6. Document ID: 45741. Augost 10, 2005. [en línea]. Disponible en:http://www.cisco.com/en/US/tech/tk872/technologies_configuration_example09186a00801f3b4f.shtml.

Cisco Systems. Cisco 1800 Series Integrated Services Routers. [en línea]. Disponible en: <http://www.cisco.com/en/US/prod/collateral/enrutadores/ps5853/product_data_sheet0900aecd8016a59b.html>

Comité de Autoevaluación y Currículo, Universidad Piloto de Colombia. Proyecto Educativo del Programa PEP. [documento físico] versión 2, (2010).

Cysco System Inc. Implementing Tunneling for IPv6. June 24, 2011. [en línea] Disponible en: http://www.cisco.com/en/US/docs/ios/ios_xe/IPv6/configuration/guide/ip6-tunnel_xe.html.

Cysco System Inc. Inc. Cisco IOS IPv6 Configuration Guide, Release 12.4. Implementing OSPF for IPv6. July 25, 2011. [en línea] Disponible en: <http://www.cisco.com/en/US/docs/ios/IPv6/configuration/guide/ip6-ospf.html>

Cysco System Inc.. Cisco IOS IPv6 Configuration Guide, Release 12.4. Implementing DHCP for IPv6. April 8, 2011. [en línea] Disponible en: <http://www.cisco.com/en/US/docs/ios/IPv6/configuration/guide/ip6-dhcp.html#wp1055621>

Cysco System Inc.s Inc. Cisco IPv6 products, solutions, and services. 2010. [en línea]. Disponible en:< http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/at_a_glance_c45-625859.pdf >.

DAVIES, Joseph. Understanding Ipv6 Second Edition. Washington. Microsoft Press, 2008 509 p. Library of Congress control number: 2007940506.

GNS3. Graphical Network Simulator. GNS3, an opensource multiplatform graphical network simulator 2011 [en línea]. Disponible en: http://www.gns3-labs.com/

Grupo de trabajo IPv6 Chile. IPv6 Chile. 2011. [en línea]. Disponible en: http://www.ipv6.cl

HAGEN, Silvia. IPv6 Essentials. O´REILLY. 2002. 360 p. ISBN:978-0-596-00125-4

IPv6 Deployment and Support. Introduction to the e-learning package. Co-existence with IPv4 Dual Stack. 2011.[en línea]. Disponible en: <http://www.6deploy.eu/e-learning/english/>.

LACNIC - Latín American and Caribbean Internet Addresses Registry) en español Registro de Direcciones de Internet para América Latina y Caribe. [en línea]. Disponible en: <http: //lacnic.net/sp/anuncios/345.html>

LOSHIN, Pete. IPv6: Theory, Protocol, and Practice SECOND EDITION. San Francisco. Morgan Kaufmann Publishers is an Imprint of Elsevier, 2004.523 p. Capítulo 8. Vol. 2. ISBN: 1-55860-810-9

Microsoft Technet Library. Definición de DNS. Última fecha de consulta Septiembre 13 de 2011. [en línea]. Disponible en: http://technet.microsoft.com/es-es/library/cc787920(WS.10).aspx

Ministerio de Tecnologías de la información y las comunicaciones. Noticias. Última fecha de consulta Marzo 2011. [en línea]. Disponible en: <http://www.mintic.gov.co/news.asp ?articleId=206>.

Network Working Group. Request for Comments 2740. OSPF for IPv6. December 1999. [en línea]. Disponible en: http://www.ietf.org/rfc/rfc2740.txt.

Network Working Group. Request for Comments: 1034 Domain Names concepts and facilities. November 1987. [en línea]. Disponible en: <http://www.ietf.org/rfc/rfc1034.txt>.

Network Working Group. Request for Comments: 1035 Domain Names concepts and facilities. November 1987. [en línea]. Disponible en: <http://www.ietf.org/rfc/rfc1035.txt>.

Network Working Group. Request for Comments: 1884. IP Version 6 Addressing Architecture. December 1995. [en línea]. Disponible en: <http://tools.ietf.org/rfc/rfc1884.txt>.

Network Working Group. Request for Comments: 1886 DNS Extensions to support IP version 6. December 1995. [en línea]. Disponible en: <http://www.ietf.org/rfc/rfc1886.txt >.

Network Working Group. Request for Comments: 2080. RIPng for IPv6.January 1998. [en línea]. Disponible en: http://www.ietf.org/rfc/rfc2080.txt

Network Working Group. Request for Comments: 2328. OSPF Version 2. April 1998. [en línea]. Disponible en: http://www.ietf.org/rfc/rfc2328.txt

Network Working Group. Request for Comments: 2373. IP Version 6 Addressing Architecture. July 1998. [en línea]. Disponible en: http://www.ietf.org/rfc/rfc2373.txt.

Network Working Group. Request for Comments: 2453. RIP Version 2. Noviembre 1998. [en línea]. Disponible en: <http:// http://tools.ietf.org/html/rfc2453>

Network Working Group. Request for Comments: 2460 Internet Protocol, Version 6 (IPv6). December 1998. [en línea]. Disponible en: http://www.rfc-es.org/rfc/rfc2460-es.txt.

Network Working Group. Request for Comments: 2460. [en línea]. Disponible en:<http://www.rfc-es.org/rfc/rfc2460-es.txt>

Network Working Group. Request for Comments: 2461 Neighbor Discovery for IP Version 6 (IPv6). December 1998. [en línea]. Disponible en: < http://www.ietf.org/rfc/rfc2461.txt>.

Network Working Group. Request for Comments: 3056 Connection of IPv6 Domains via IPv4 Clouds. Febraury 2001. [en línea]. Disponible en: <http://www.ietf.org/rfc/rfc3056.txt >.

Network Working Group. Request for Comments: 3068 An Anycast Prefix for 6to4 Relay Routers. June 2001. [en línea]. Disponible en: <http://www.ietf.org/rfc/rfc3068.txt >.

Network Working Group. Request for Comments: 3513. Internet Protocol Version 6 (IPv6) Addressing Architecture. April 2003. [en línea]. Disponible en: http://http://www.ietf.org/rfc/rfc3513.txt.

Network Working Group. Request for Comments: 4193 Unique Local IPv6 Unicast Addresses. October 2005. [en línea]. Disponible en: http://www.ietf.org/rfc/rfc4193.txt

Network Working Group. Request for Comments: 951 Bootstrap Protocol (BOOTP). September 1984. [en línea]. Disponible en: <http://www.ietf.org/rfc/rfc4193.txt>.

Network Working Group. Requests for Comments: 2740 OSPFv6.December 1999. [en línea].Disponible en: http://www.ietf.org/rfc/rfc2740.txt

PÉREZ, Juan, et, al. Conceptos de sistemas Operativos. Universidad Pontificia Comillas. Madrid.2002. 641 p.ISBN: 84-8468-063-0

Periódico el Espectador ``Elespectador.com/Cartagena''. En enero Comienza la implementación del protocolo Ipv6 en Colombia. Diciembre 6 de 2010. Última fecha de consulta, Marzo 2011. [en línea]. Disponible en: http://www.elespectador.com/articulo-238991-enero-comienza-implementacion-de-protocolo-IPv6-colombia.

Renata. Red Nacional Académica de Tecnología Avanzada.I Foro día Mundial IPv6. Junio 9 2011. Última fecha de consulta Septiembre 2011. [en línea]. Disponible en: http://www.renata.edu.co/index.php/component/content/article/5-noticias /2297-i-foro-dia-mundial-IPv6-capítulo-colombia-reunio-a-la-comunidad-academica-y-tecnica-del-pais-y-de-america-latina.html>.

RNO The Number Resource Organization en español Organización de registro de números. [en línea]. Disponible en: http://www.nro.net/news/remaining-ipv4-address-space-drops-below-5.

SHANNON, McFarland, et, al. IPv6 for Enterprise Networks. Indianapolis. Cisco Press, 2011. 361p. ISBN: 978-1-58714-227-7.

TAFFERNABERRY, Carlos, et al.Codarec6: an ipv6 test bed" – Laboratorio de estudio, diseño, desarrollo, implementación, ensayo y capacitación del protocolo de internet versión 6. [en línea]. Disponible en: <http://codarec6.frm.utn.edu.ar/publicaciones/papers/CACIC-2006.pdf>.

VILLANUEVA, Juan Camilo et, al. I Curso Taller: Redes de Telecomunicaciones Avanzadas. Manual del curso Taller de Redes de Telecomunicaciones Avanzadas. Perú, Perú :s.n., Agosto de 2010. [en línea]. Disponible en: <http://www.willay.org.pe>

YUNES, Darwin Lamarck. IPv6 Task Force América Latina y el Caribe. IPv6: Nueva Generación Protocolo de Internet. [En línea] <http://www.lac.ipv6tf.org/docs/tutoriales/IPv6-LACTF.pdf>

## ANEXOS

Anexo A: Guía No. 1 Configuración Inicial de IPv6

../Anexos/Guia_1/Guía_No1.docx

Anexo B: Guía No. 2 Implementación Dual-Stack o Doble Pila

..\Anexos\Guia_2\Guía_No2.docx

Anexo C: Guía No. 3 Implementación Túneles 6to4

..\Anexos\Guia_3\Guía_No3.docx

Anexo D: Guía No. 4 Implementación de redes usando dos mecanismos de transición y convivencia

..\Anexos\Guia_4\Guía_No4.docx

Anexo E: Material Docente Guía No. 1

..\Anexos\Material_Docente\Anexo_E.pptx

Anexo F: Material Docente Guía No. 2

..\Anexos\Material_Docente\Anexo_F.pptx

Anexo G: Material Docente Guía No. 3

..\Anexos\Material_Docente\Anexo_G.pptx

Anexo H: Inventario de Dispositivos de Laboratorio

..\Anexos\Laboratorio\Anexo_H.xls

Anexo I: Solicitud de Actualización de IOS y Hallazgos de los dispositivos de laboratorio
..\Anexos\Laboratorio\Anexo_I.pdf

Anexo J: Solicitud de Actualización de IOS

..\Anexos\Laboratorio\Anexo_J.pdf