Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

# TRANSICIÓN A IPV6 LA ÚNICA SOLUCIÓN PARA LA EXPANSIÓN DEL INTERNET: ANÁLISIS SOBRE LOS DIFERENTES MECANISMOS PARA LA IMPLEMENTACIÓN DEL NUEVO PROTOCOLO DE INTERNET Y LAS DISTINTAS OPORTUNIDADES QUE BRINDA LA IPV6

**Michael Antony Colindres Hernández**
Asesorado por el Ing. Pedro Pablo Hernández Ramírez

Guatemala, enero de 2013

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA


FACULTAD DE INGENIERÍA

# TRANSICIÓN A IPV6 LA ÚNICA SOLUCIÓN PARA LA EXPANSIÓN DEL INTERNET: ANÁLISIS SOBRE LOS DIFERENTES MECANISMOS PARA LA IMPLEMENTACIÓN DEL NUEVO PROTOCOLO DE INTERNET Y LAS DISTINTAS OPORTUNIDADES QUE BRINDA LA IPV6

TRABAJO DE GRADUACIÓN

PRESENTADO A JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

**MICHAEL ANTONY COLINDRES HERNÁNDEZ**
ASESORADO POR EL ING. PEDRO PABLO HERNÁNDEZ RAMÍREZ

AL CONFERÍRSELE EL TÍTULO DE

**INGENIERO EN CIENCIAS Y SISTEMAS**

GUATEMALA, ENERO DE 2013

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA


## NÓMINA DE JUNTA DIRECTIVA

| | |
|---|---|
| DECANO | Ing. Murphy Olympo Paiz Recinos |
| VOCAL I | Ing. Alfredo Enrique Beber Aceituno |
| VOCAL II | Inga. Pedro Antonio Aguilar Polanco |
| VOCAL III | Inga. Elvia Miriam Ruballos Samayoa |
| VOCAL IV | Br. Juan Carlos Molina Jiménez |
| VOCAL V | Br. Mario Maldonado Muralles |
| SECRETARIO | Ing. Hugo Humberto Rivera Pérez |

## TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

| | |
|---|---|
| DECANO | Ing. Murphy Olympo Paiz Recinos |
| EXAMINADOR | Ing. José Ricardo Morales Prado |
| EXAMINADOR | Ing. César Rolando Batz Saquimux |
| EXAMINADOR | Ing. Pedro Pablo Hernández Ramírez |
| SECRETARIO | Ing. Hugo Humberto Rivera Pérez |

# HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

**TRANSICIÓN A IPV6 LA ÚNICA SOLUCIÓN PARA LA EXPANSIÓN DEL INTERNET: ANÁLISIS SOBRE LOS DIFERENTES MECANISMOS PARA LA IMPLEMENTACIÓN DEL NUEVO PROTOCOLO DE INTERNET Y LAS DISTINTAS OPORTUNIDADES QUE BRINDA LA IPV6**

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha octubre de 2012.

**Michael Antony Colindres Hernández**

Guatemala, 20 de septiembre de 2012

Ingeniero
Carlos Alfredo Azurdia Morales
Coordinador de Área de Trabajos de Graduación
Escuela de Ciencias y Sistemas
Facultad de Ingeniería

Estimado Ingeniero Azurdia Morales:

Por este medio atentamente le informo como asesor del trabajo de graduación del estudiante universitario de la carrera de Ingeniería en Ciencias y Sistemas, MICHAEL ANTONY COLINDRES HERNÁNDEZ, carné 2006-11415, que he revisado el trabajo de graduación titulado: "TRANSICIÓN A IPV6 LA ÚNICA SOLUCIÓN PARA LA EXPANSIÓN DEL INTERNET: ANÁLISIS SOBRE LOS DIFERENTES MECANISMOS PARA LA IMPLEMENTACIÓN DEL NUEVO PROTOCOLO DE INTERNET Y LAS DISTINTAS OPORTUNIDADES QUE BRINDA LA IPV6", y a mi criterio el mismo está completo y cumple con los objetivos propuestos para su desarrollo.

Agradeciendo su atención a la presente,

Atentamente,

Ing. Pedro Pablo Hernández Ramírez
Asesor de trabajo de graduación
Colegiado: 7240

Pedro Pablo Hernández Ramírez
Ingeniero en Ciencias y Sistemas
Colegiado 7240

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 17 de Octubre de 2012

Ingeniero
**Marlon Antonio Pérez Turk**
**Director de la Escuela de Ingeniería**
**En Ciencias y Sistemas**

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **MICHAEL ANTONY COLINDRES HERNÁNDEZ** carné **200611415,** titulado: **"TRANSICIÓN A IPV6 LA ÚNICA SOLUCIÓN PARA LA EXPANSIÓN DEL INTERNET: ANÁLISIS SOBRE LOS DIFERENTES MECANISMOS PARA LA IMPLEMENTACIÓN DEL NUEVO PROTOCOLO DE INTERNET Y LAS DISTINTAS OPORTUNIDADES QUE BRINDA LA IPV6",** y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

**Ing. Carlos Alfredo Azurdia**
Coordinador de Privados
y Revisión de Trabajos de Graduación

ESCUELA DE CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE CIENCIAS Y SISTEMAS
TEL: 24767644

*El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, del trabajo de graduación titulado* ***"TRANSICIÓN A IPV6 LA ÚNICA SOLUCIÓN PARA LA EXPANSIÓN DEL INTERNET: ANÁLISIS SOBRE LOS DIFERENTES MECANISMOS PARA LA IMPLEMENTACIÓN DEL NUEVO PROTOCOLO DE INTERNET Y LAS DISTINTAS OPORTUNIDADES QUE BRINDA LA IPV6",*** *realizado por el estudiante MICHAEL ANTONY COLINDRES HERNÁNDEZ, aprueba el presente trabajo y solicita la autorización del mismo.*

***"ID Y ENSEÑAD A TODOS"***

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION DE INGENIERIA EN CIENCIAS Y SISTEMAS

*Ing. Marlon Antonio Pérez Turk*
*Director, Escuela de Ingeniería en Ciencias y Sistemas*

*Guatemala, 18 de enero 2013*

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

DTG. 017 .2013

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al trabajo de graduación titulado: **TRANSICIÓN A IPV6 LA ÚNICA SOLUCIÓN PARA LA EXPANSIÓN DEL INTERNET: ANÁLISIS SOBRE LOS DIFERENTES MECANISMOS PARA LA IMPLEMENTACIÓN DEL NUEVO PROTOCOLO DE INTERNET Y LAS DISTINTAS OPORTUNIDADES QUE BRINDA LA IPV6,** presentado por el estudiante universitario **Michael Antony Colindres Hernández,** autoriza la impresión del mismo.

IMPRÍMASE:

Ing. Murphy Olympo Paiz Recinos
Decano

DECANO
FACULTAD DE INGENIERIA

Guatemala, 22 de enero de 2013.

/gdech

## ACTO QUE DEDICO A:

**Dios** Por todas las bendiciones que me ha dado, por haberme dado vida, salud y la sabiduría para poder cumplir mis metas. Y haberme dado la inteligencia emocional para salir adelante a pesar de los momentos difíciles.

**Mi abuela** Fidelia Flores, por haberme criado, por sus consejos, por haber madrugado junto a mí en toda mi carrera universitaria y por su apoyo en los momentos difíciles. Ya que me ha inculcado buenos principios y valores para ser una persona de bien.

**Mi abuelo** Moises Hernández, por haberme criado, por sus consejos, por haberme enseñado a esforzarme y a trabajar duro para alcanzar mis metas, y por su apoyo en los momentos difíciles. Ya que me ha inculcado buenos principios y valores para ser una persona de bien y de éxito.

**Mi madre** Sonia Hernández, por haberme dado la vida, por criarme y que de alguna u otra manera me ha apoyado en mi carrera universitaria.

**Mi padre** Rolando Colindres, por haberme dado el apoyo económico para mis estudios, por los consejos y compartir sus experiencias de la vida para poder llegar a ser una persona de bien.

**Mis hermanos** Alejandro, Wilfredo y Paola, por haberme apoyado cuando necesitaba de su ayuda para cumplir con mis tareas y responsabilidades a lo largo de mi carrera universitaria. Por haberme facilitado los recursos y medios para lograr mis metas.

**Mi familia** Gracias a todos por el apoyo que de alguna manera me brindaron, y en especial a mis tíos y tías ya que son parte importante en mi vida.

**Mis amigos** Que en cada curso de la carrera logramos salir adelante siempre apoyándonos y en las innumerables noches de desvelo que valieron la pena para culminar la carrera.

# AGRADECIMIENTOS A:


**Dios** Porque a lo largo de mi vida siempre ha estado dándome la sabiduría necesaria para salir avante en todos los aspectos de mi vida.

**Mi asesor** Por sus conocimientos, tiempo y dedicación para lograr terminar mi investigación de manera adecuada, agradecimientos al ingeniero Pedro Pablo Hernández Ramírez.

**Mis amigos** Emilio Méndez, Elder Prado, Honard Bravo, Eduardo Quetzales, Josue Pirir, José Manuel De Paz y Gabriela Diaz. Por su apoyo y palabras de aliento en los momentos difíciles a lo largo de la carrera y a cada uno de sus familiares que me brindaron su apoyo en los momentos en que nos reuníamos para hacer los proyectos de la carrera.

**Mis catedráticos** Por transmitirnos sus conocimientos a lo largo de estos años y en especial a todos los catedráticos que brindan sin ningún complejo su experiencia y consejos.

| | |
|---|---|
| **Universidad de San Carlos de Guatemala** | Por el apoyo y la formación académica en estos años de estudio, agradecimientos a la Facultad de Ingeniería y a la Escuela de Ciencias y Sistemas. |

# ÍNDICE GENERAL

# ÍNDICE DE ILUSTRACIONES

## FIGURAS

## TABLAS

# LISTA DE SÍMBOLOS

| Símbolo | Significado |
|---|---|
| **IPv4** | *Internet Protocol version 4* |
| **IPv6** | *Internet Protocol version 6* |
| **VoIP** | *Voice over internet Protocol* |

# GLOSARIO

| | |
|---|---|
| ***Anycast*** | Es una forma de direccionamiento en la que la información es enviada a un solo destino en la topología de la red. |
| ***Backbone*** | Red de transmisión a través de la cual se transportan datos de los diferentes nodos que están conectados a ella (parte de una red que actúa como el camino primario para el tráfico con otras redes). |
| ***Back end*** | Es una base de datos a la que se accede indirectamente por los usuarios a través de una aplicación externa en lugar de aplicaciones programadas almacenadas dentro de la propia base de datos. |
| ***Buffer*** | Es un área de almacenamiento temporal reservada para el uso en las operaciones de entrada y salida, dentro de la cual los datos son leídos o escritos. |

| | |
|---|---|
| **CIDR** | *Classless Inter-Domain Routing*, es un estándar de red para la interpretación de direcciones IP, el cual facilita el encaminamiento al permitir agrupar bloques de direcciones en una sola entrada de tabla de rutas. |
| ***Core*** | Es la parte central de una red de telecomunicaciones que ofrece diversos servicios a los clientes que están conectados por la red de acceso. |
| **Datagrama** | Es un fragmento de paquete que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia nodo receptor. |
| **Dirección IP** | Es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP. |
| **DMZ** | *DeMilitared Zone*, la zona desmilitarizada, es un área de una red de computadoras que está entre la red de computadoras interior de una organización y una red de computadoras exterior, generalmente el internet. |

| | |
|---|---|
| **DSL** | *Digital Subscriber Line*, la línea de suscripción digital es un término utilizado para referirse de forma global a todas las tecnologías que proveen una conexión digital sobre línea de abonado de la red telefónica básica o conmutada. |
| **EDGE** | Es una red proporciona el intercambio de información entre la red de acceso y el núcleo de la red (*core*). |
| **FDDI** | *Fiber Distributed Data Interface*, es un conjunto de estándares para la transmisión de datos en redes de computadoras de área extendida o local mediante cable de fibra óptica. |
| ***Firewall*** | Mecanismo de seguridad en internet frente a accesos no autorizados. Básicamente consiste en un filtro que mira la identidad de los paquetes y rechaza todos aquellos que no estén autorizados o correctamente identificados, también llamado contrafuegos. |
| ***Firmware*** | Es un bloque de instrucciones de programa para propósitos específicos, grabado en una memoria de tipo no volátil, que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo. |

| | |
|---|---|
| ***Framework*** | Es un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular, que sirve como referencia para enfrentar y resolver nuevos problemas de índole similar. |
| ***Front end*** | Elementos de un sitio con los que tiene contacto directo el usuario final y que influyen en su experiencia al hacer uso de la infraestructura de red. |
| ***Gateway*** | Puerta de enlace, es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. |
| **Gobernanza** | Es el concepto de reciente difusión para designar a la eficacia, calidad y buena orientación en la gestión de las organizaciones públicas o privadas. |
| **GRE** | *Generic Routing Encapsulatio*n, es un protocolo para el establecimiento de túneles a través del internet. |

| | |
|---|---|
| **Gusano** | También llamados IWorm por su apocope en inglés, ‘I’ de internet, *Worm* de gusano, es un malware que tiene la propiedad de duplicarse a sí mismo. |
| **ICMP** | *Internet Control Message Protocol*, es el protocolo de mensajes de control de internet es el subprotocolo de control y notificación de errores del Protocolo de internet. |
| ***Intranet*** | Es una red de ordenadores privados que utiliza tecnología internet para compartir dentro de una organización parte de sus sistemas de información y sistemas operacionales. |
| **ISP** | *Internet Service Provider*, el proveedor de servicios de internet es una empresa que brinda conexión a internet a sus clientes. |
| **IPng** | *IP Next Generation*, IP de próxima generación a veces también utilizada para llamar a la IPv6. |
| **IPSec** | *Internet Protocol Security*, es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el protocolo de internet autenticando y/o cifrando cada paquete IP en un flujo de datos. |

| | |
|---|---|
| **Kernel** | Núcleo de un sistema operativo, es decir, bloque de código con la parte central del funcionamiento y arranque del sistema. |
| **LAN** | *Local Area Network*, la red de área local como su nombre indica, es una red de ordenadores de tamaño pequeño/medio localizada en un edificio. |
| ***Malware*** | Es un *software* malicioso, que ingresa al sistema de su computadora intencionalmente con el único propósito de dañar o causar pérdidas al sistema o de la información allí guardada, o para ser usado como plataforma para atacar otras computadoras. |
| **Modem** | Es un dispositivo que sirve para enviar una señal llamada portadora mediante otra señal de entrada llamada moduladora. |
| **MTU** | *Maximum Transmission Unit*, es una unidad máxima de transmisión como el tamaño máximo de los paquetes en protocolos IP. |
| **Multicast** | Multidifusión, es el envío de la información en una red a múltiples destinos simultáneamente. |

| | |
|---|---|
| **OSI** | Es un modelo de referencia de Interconexión de Sistemas Abiertos que fue el modelo de red descriptivo creado por la organización internacional para la estandarización lanzado en 1984. |
| ***Peering*** | Es la interconexión voluntaria de redes de internet administrativamente independientes con el fin de intercambiar tráfico entre los clientes de cada red. |
| ***Peer to peer*** | P2P o red de pares, es una comunicación bilateral exclusiva entre dos personas a través de internet para el intercambio de información en general. |
| **Ping** | Utilidad para TCP/IP que envía paquetes de prueba para saber si una máquina remota se encuentra en línea y el tiempo que se tarda para llegar a ella. |
| **PPP** | *Point to Point Protocol*, el protocolo punto a punto es un protocolo que permite establecer una comunicación a nivel de enlace entre dos ordenadores. |

| | |
|---|---|
| ***Plug and play*** | Conocida también por su abreviatura PnP es la tecnología que permite a un dispositivo informático ser conectado a un ordenador sin tener que configurar, de manera automática. |
| **QoS** | *Quality of Service*, la calidad de servicio son las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado. La calidad de servicio es la capacidad de dar un buen servicio. |
| **RFC** | *Request For Comments*, la solicitud de comentarios es el nombre que se da a una serie de normas que definen el protocolo TCP/IP, así como sus documentos relacionado. |
| ***Replay attack*** | Es una forma de ataque de red, en el cual una transmisión de datos válida es maliciosa o fraudulentamente repetida o retardada. |
| ***Sniffer*** | Programa que monitoriza los paquetes de datos que circulan por una red, en busca de información referente cadenas prefijadas. |
| **Socket** | Es un concepto abstracto por el cual dos programas (posiblemente situados en computadoras distintas) pueden intercambiar cualquier flujo de datos, generalmente de manera fiable y ordenada. |

| | |
|---|---|
| ***Spoofing*** | En términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación. |
| **Subnetting** | Es una colección de direcciones IP que permiten definir el número de redes y de host que se desean utilizar en una subred determinada. |
| **TCP** | *Transmission Control Protocol*, es uno de los principales protocolos en las redes TCP/IP. TCP le permite a dos computadoras anfitrionas establecer una conexión e intercambiar flujos de datos. |
| ***Traceroute*** | Es una herramienta de diagnóstico de redes que permite seguir la pista de los paquetes que van desde un host a otro. |
| **UDP** | *User Datagram Protocol*, el protocolo de datagrama de usuario es un protocolo del nivel de transporte basado en el intercambio de datagramas. |
| ***Wardriving*** | Consiste en la búsqueda de redes inalámbricas WiFi desde un vehículo en movimiento. Implica usar un vehículo y un ordenador equipado con WiFi, como un portátil o una PDA, para detectar las redes. |

| | |
|---|---|
| ***Whois*** | Es un protocolo TCP basado en petición/repuesta que se utiliza para efectuar consultas en una base de datos que permite determinar el propietario de un nombre de dominio o una dirección IP en internet. |

# RESUMEN

El nuevo protocolo de internet la IPv6 no es un tema nuevo, la IPv6 ha tomado popularidad por el agotamiento de las direcciones IPv4. Debido a este agotamiento el internet no puede seguir expandiéndose y siendo la red importante como hasta ahora lo ha experimentado. Cuando se diseño la IPv4 en la década de 1980 no se considero el enorme crecimiento que iba a tener el internet, dado que en ese tiempo el internet era para una minoría y no se preveía el éxito que ahora tiene.

Algunas de las medidas para minimizar el agotamiento de las direcciones IPv4 se fueron creando tecnologías que junto a la IPv4 prolongarían el completo agotamiento de las direcciones. Otra de las medidas tomadas por parte de los RIR fue en reclamar todas aquellas direcciones IPv4 que fueron otorgadas en los inicios del internet y no están siendo utilizadas, además se tiene un control más estricto al otorgar las pocas direcciones IPv4 que siguen sin utilizar.

Debido a los problemas del actual protocolo de internet principalmente por el agotamiento de las direcciones, se vio en la necesidad de diseñar la próxima generación del protocolo de internet. La IPv6 se volvió la sustituta del actual protocolo IPv4, pero el cambio al nuevo protocolo no ha sido fácil, dado que por lo complejidad del internet esto no se realizará de un tiempo para otro, este cambio se realizará a largo plazo y no a corto plazo como erróneamente se piensa.

IPv6 además de proveer de las direcciones IP suficientes, se diseño con varias características adicionales que la hacen mucho más segura y más fácil de configurar que la IPv4. Es por ello que en muchos países en la actualidad el tema de la IPv6 es nuevo y que aun no le han dado la importancia con la que se debe afrontar, la IPv6 debe ser tomado en cuenta lo más pronto para que los costos no se eleven y dicho cambio a la IPv6 se debe de planificar.

Dado que el cambio no es de un día para otro, los protocolos de internet IPv4 e IPv6 coexistirán por un largo tiempo hasta que el internet soporte en su totalidad en nuevo protocolo de internet IPv6. Para esto existen diferentes mecanismos de transición que ayudan empezar a dar soporte a la IPv6, los cuales se agrupan en tres grandes grupos: mecanismos de doble pila, mecanismos de traducción y mecanismos de túneles.

La transición a IPv6 tendrá un impacto importante en la infraestructura de red de los proveedores de internet, entidades públicas y privadas, usuarios finales y cada uno de los servicios de internet como son NAT, DHCP, web, DNS, entre otros. El impacto es inevitable al realizar la transición lo que sí es que se debe estar lo suficientemente preparado y conocer cada uno de las alternativas para adoptar la IPv6 para minimizar el impacto, resguardar la información crítica y para que el internet siga teniendo el potencial que la ha hecho tan popular.

# OBJETIVOS

## General

Facilitar por medio del trabajo de graduación una guía de estudio en el tema de IPv6, dando a conocer las diferentes implicaciones en la transición de los protocolos de internet IPv4 a IPv6 en los principales entornos de trabajo donde se llegue a implementar la IPv6, y proveer de una investigación que oriente a los lectores en los temas relacionados con la IPv6 para la toma de decisiones en el momento de realizar una transición al nuevo protocolo de internet.

## Específicos

1. Especificar el panorama general del nuevo protocolo de internet (IPv6) y las problemáticas del actual protocolo IPv4.

2. Dar a conocer las diferentes estrategias de transición a la IPv6 y proponer una planificación aceptada para la transición a la IPv6.

3. Dar a conocer las diferentes alternativas para realizar la transición a IPv6 en las redes actuales en donde domina el protocolo de internet versión 4.

4. Definir la seguridad inherente con que cuenta la IPv6 sobre la IPv4 y conocer las vulnerabilidades en la seguridad a las que se enfrentan al realizar la transición a la IPv6 en redes donde prevalece el actual protocolo de internet IPv4.

5. Especificar el impacto que tendrá realizar la transición al protocolo de internet IPv6 a los diferentes ambientes de trabajo donde se implemente.

# INTRODUCCIÓN

La falta de iniciativa, escasez de recursos en el área de tecnología y falta de interés de las autoridades correspondientes es lo que provoca que el país esté atrasado y esto conlleva a no ir al mismo ritmo de los avances tecnológicos, y el tema de la IPv6 no se le ha prestado la importancia que se amerita, lo cual hace que los costos que se incurren se eleven mientras más tiempo pase y no se haga frente a una transición al nuevo protocolo de internet. Todos hacen uso del internet tanto directa como indirectamente, es por ello que la transición a la IPv6 es importante tanto para quienes utilizan el servicio de internet como los que brindan el servicio.

La mejor decisión es considerar la adopción de la IPv6 lo más pronto posible, dado que entre más pase el tiempo y no se empiece a realizar las actividades para realizar la transición de IPv4 a IPv6 el costo se elevará considerablemente. Poco a poco las direcciones IP disponibles en el protocolo de internet IPv4 se están agotando, las últimas direcciones IPv4 están siendo rigurosamente controladas para que el momento del agotamiento total de las direcciones IP sea en un futuro más lejano a lo previsto, a esta problemática se le suma la creciente cantidad de dispositivos que necesitan estar conectados a internet y tener una identidad pública y única.

La cantidad de direcciones que puede proporcionar la IPv4 son alrededor de 4 mil millones de direcciones las cuales gradualmente se están agotando. Mientras el nuevo protocolo de internet IPv6 provee una cantidad de direcciones IP casi infinita, dispone de una cantidad alrededor de 340 sextillones de direcciones IP disponibles (340 billones de billones de billones).

Esta exuberante cantidad de direcciones IPv6 alcanzaría para que cada persona del planeta tenga trillones de direcciones IP lo que no se puede conseguir con el actual protocolo de internet IPv4 ya que las direcciones son insuficientes.

Realizar un cambio por completo se alcanzará a largo plazo por lo que la transición de IPv4 a IPv6 será gradual hasta llegar a tener redes IPv6 dominantes. Tarde o temprano todo dispositivo o individuo que haga uso del internet tendrá que realizar el cambio a IPv6 y se deben de conocer las diferentes opciones que se tienen para adaptarse al cambio, realizar el cambio por medio de los distintos mecanismos de transición existentes o tomar la decisión de manejar la coexistencia entre los dos protocolos de internet son alguna de las opciones a tomar en cuenta.

La seguridad es un tema delicado en toda infraestructura de red por lo que existe incertidumbre con respecto a que si la información de las organizaciones estará segura durante la transición a IPv6. Lo que sí es cierto que el nuevo protocolo de internet IPv6 es más seguro que el actual protocolo de internet IPv4. Sin lugar a dudas que el impacto que tendrá el cambio en los distintos entornos donde se utiliza el internet será inminente, ya que el cambio conlleva afrontar distintas vulnerabilidades en la seguridad, empresas, usuarios finales, proveedores de internet, entidades educativas y de investigación, y todos los servicios de internet deben de tomar en cuenta desde ya el soporte a la IPv6.

# 1. PANORAMA GENERAL

Cuando se implemento la actual generación de protocolo de internet (IPv4) en la década de los 80 no se consideró el enorme crecimiento que iba a tener el internet y conlleva al problema actual de escases de direcciones IP. La IPv4 no tiene las suficientes direcciones IP para cubrir la demanda actual.

Hoy en día el internet es uno de los medios de comunicación con más importancia para la humanidad, cada vez existen más dispositivos con la capacidad de conectarse a internet, dispositivos tales como los teléfonos inteligentes, consolas de video juegos, *tablets* y televisores, solo son algunos de los dispositivos que pueden hacer uso del internet, es por ello que lo han llamado el internet de las cosas.

Con el internet de las cosas cualquier objeto de la vida cotidiana estarán equipado para conectarse a internet, algo que ya es una realidad y se necesita de un protocolo de internet con la capacidad de brindar de direcciones IP a cada objeto que así lo requiera, esto es posible con el nuevo protocolo de internet la IPv6. La capacidad de la IPv4 es aproximadamente de 4 300 millones de direcciones IP y la mayoría ya están en uso, por otro lado la IPv6 tiene una capacidad aproximada de 340 sixtillones suficientes para la actual demanda.

El problema del agotamiento de las direcciones IP de la IPv4 es irreversible, por lo todo usuario que tenga presencia en internet deben de realizar la transición a IPv6, dicha transición debe ser gradual, dado que existen varios factores que no permiten realizar un cambio de IPv4 a IPv6 de un momento a otro.

## 1.1. Efectos del agotamiento del actual protocolo de internet IPv4

El agotamiento de direcciones IP de la IPv4 da origen a la IPv6, la cual tiene una capacidad muy superior de direcciones IP. Cada organización debe de considerar las implicaciones que conlleva la transición a IPv6 y decidir qué medidas tomarán.

El mayor problema al agotarse las direcciones IP es que los países con economías emergentes se ven rezagados al no poder hacer uso del internet como lo vienen realizando, debido a que no hay más direcciones IP que puedan usar, el internet es de vital importancia para el desarrollo de la academia, la industria y el gobierno de un país, por lo que la problemática de la IPv4 trae consecuencias serias al no tratar con tiempo el cambio a la IPv6.

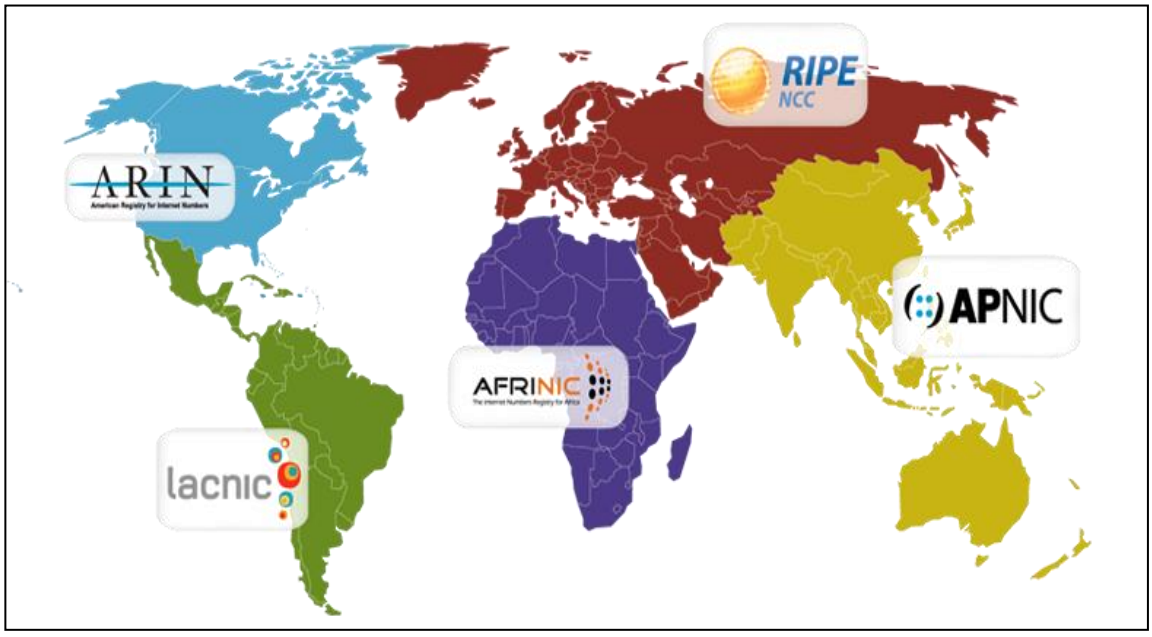
Si se deja a un lado el tema de la IPv6, más complejo se volverá conforme pase el tiempo. El tema de la adopción a la IPv6 no es nada sencillo ya que en la actualidad la mayoría de la infraestructura tecnológica no soporta la IPv6, en el peor de los casos las organizaciones cuentan con *hardware* obsoleto y que de ninguna manera soportaría a la IPv6. El cambio a la IPv6 no se realizará de un día para otro, este cambio debe ser gradual, por lo que la IPv4 y la IPv6 deben de ser capaces de coexistir por un largo periodo de tiempo hasta que toda la infraestructura de internet haga el cambio a la IPv6.

En los últimos años los usuarios de internet en Guatemala ha crecido considerablemente conectándose desde diversos dispositivos, debido al auge de las redes sociales esto se ve cada vez más notorio. Según estudio realizado por Cisco Systems se predijo que: para el 2015 habrá aproximadamente en el mundo un dispositivo móvil per cápita, y se estima que la población mundial será de 7 200 millones de personas.

### 1.1.1. Problemática IPv4

La problemática de la IPv4 consiste en que el internet *Assigned Numbers Authority* (*IANA* por sus siglas en inglés) ha asignado todos los bloques de direcciones IPv4 disponibles a los Regional Internet Registry (*RIR* por sus siglas en inglés), así cada uno de estos podrán administrar los últimos bloques de direcciones IP. Los diferentes RIR se muestran en la figura 1 y su significado en la tabla I.

Figura 1. **Diferentes RIR**




Fuente: *IANA numbers resources*, en: http://www.iana.org/numbers/. Consulta: 10 de abril de 2011.

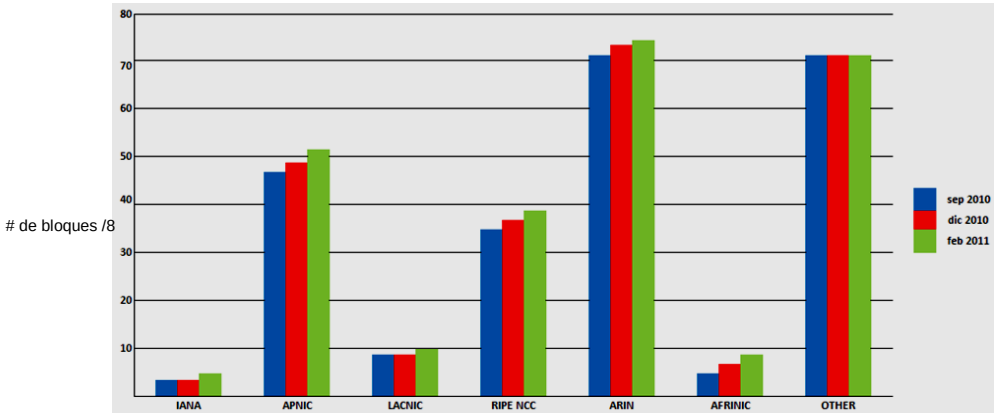
Tabla I. **Significado de cada RIR**

| Registro | Área de Cobertura |
|---|---|
| AfriNIC | Región Africana |
| APNIC | Región Asia/Pacifico |
| ARIN | Región Norteamericana |
| LACNIC | Latino América y algunas Islas Caribeñas |
| RIPE NCC | Europa, el Medio Oriente y Asia Central |

Fuente: *IANA numbers resources*, en: http://www.iana.org/numbers/. Consulta: 10 de abril de 2011.

En febrero de 2011 se realizó la asignación de los últimos bloques de direcciones IPv4 a cada RIR (vea figura 2). En la actualidad ya existen muy pocos bloques de direcciones IPv4 disponibles en cada RIR (vea tabla II), esto hace evidente la necesidad de una transición a la IPv6 lo antes posibles.

Figura 2. **Asignación de direcciones IPv4 por RIR**




Fuente: Proyecto IPv6 para Chile fase de inteligencia de mercados y competitiva informe de tendencias N°3.

Tabla II. **Estado actual de bloques de direcciones IPv4**

| Registro | Bloques disponibles / total | % de bloques disponibles |
|---|---|---|
| AfriNIC | 2,46 / 4 | 61,50 |
| APNIC | 1,43 / 47 | 3,04 |
| ARIN | 4,64 / 75 | 6,19 |
| LACNIC | 2,93 / 9 | 32,56 |
| RIPE NCC | 3,71 / 37 | 10,03 |

Fuente: Agotamiento IPv4 (Español), en: http://inetcore.com/project/ipv4ec. Consulta: 10 de abri de 2011.

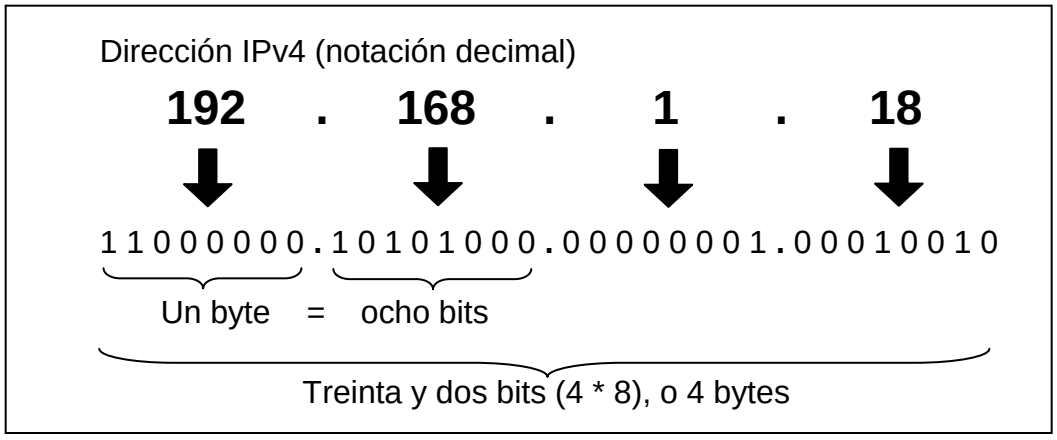
La razón del cambio a IPv6 es por direcciones, la cantidad de direcciones IPv4 libres están llegando a su fin, ya no hay más direcciones IPv4, aparte de los últimos bloques de donde se puedan seguir asignando.

### 1.1.2. Causas del agotamiento

El agotamiento de la direcciones IPv4 es una realidad y prolongar por más tiempo el uso de IPv4 es casi imposible, lo ideal es enfrentar el problema de transición a IPv6 y hacerle frente a las implicaciones que conlleva realizar el cambio gradual a IPv6.

Cuando se creó e implemento la IPv4 nunca se estimó que se necesitarán tantas direcciones IP como ahora son necesarias, es por ello que una dirección IPv4 está definida por 32 bits (vea figura 3) lo cual provee de una capacidad aproximada de 4 300 millones de direcciones IP, insuficiente para la actual demanda.

Figura 3. **Dirección IPv4**

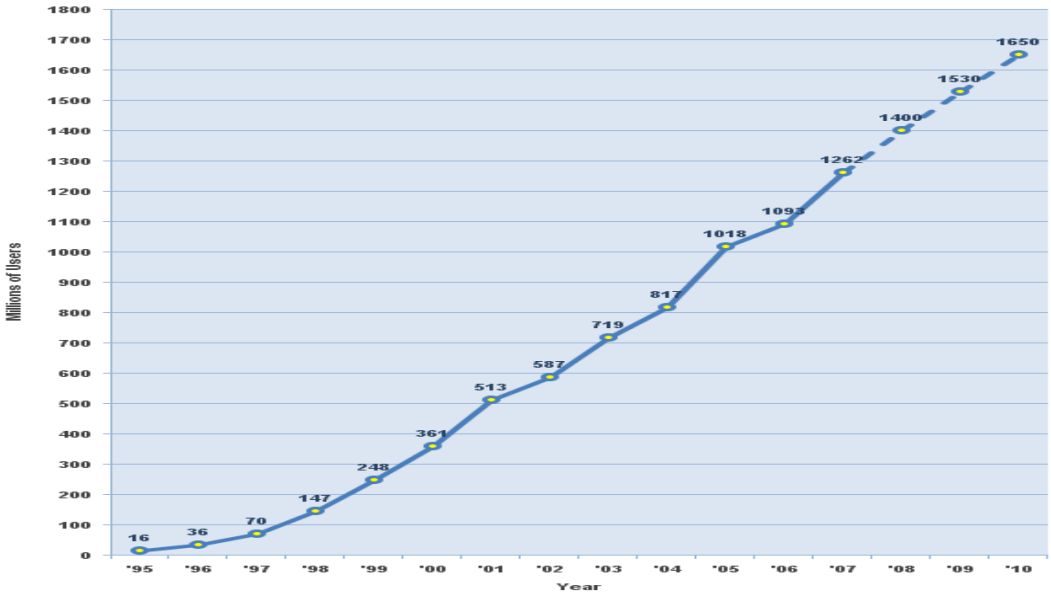



Fuente: elaboración propia.

Las principales causas del agotamiento de las direcciones IPv4 son los dispositivos móviles, la demografía del internet y el uso ineficiente de direcciones. El crecimiento del volumen de los dispositivos móviles que tienen la capacidad de hacer uso del internet ha conllevado a la aceleración del agotamiento de las direcciones IPv4.

La demografía del internet se refiere a la población que hace uso de internet va creciendo de manera exponencial desde la creación de internet (vea figura 4). El protocolo de internet IPv4 actualmente no tiene capacidad de proveer una dirección a cada uno de los usuarios de internet, lo que sí es posible con la IPv6.

Figura 4. **Usuario de internet en el mundo**




Fuente: *Internet users in the world growth 1995 - 2010*, en: http://www.internetworldstats.com. Consulta: 2 de mayo de 2011.

Y por último la otra causa principal del agotamiento de las direcciones IPv4 es el uso ineficiente de las direcciones IP ya que cuando se implemento la IPv4 en la década de los 80 se asignaron direcciones IP que realmente no se utilizarían a las grandes empresas y universidades de esa época, se les asignaron bloques completos de direcciones con 16 millones de direcciones cada uno. En la actualidad varias empresas utilizan direcciones IP públicas para ordenadores que realmente no son accesibles fuera de las redes locales de la empresa, no haciendo uso así de direcciones IP privadas y dichas direcciones IP públicas podrían servir para implementaciones basadas en NAT.

### 1.1.3. Estrategias para minimizar el agotamiento de IPv4

En su momento nunca se imagino que se fueran a necesitar más direcciones IP, en la actualidad dichas direcciones IPv4 están a poco tiempo de que todas se utilicen y por lo tanto no habrán más disponibles para los usuarios que así lo requieran. El agotamiento de las direcciones IPv4 no es un tema nuevo en el internet, es un tema que tiene varios años de estar presente y debido a esto se han creado varias tecnologías, las cuales han atenuado el agotamiento

Tecnologías como redes privadas, NAT, DHCP, subredes y *hosting virtual* son las principales que han logrado prolongar el agotamiento de las direcciones IPv4, pero que hoy en día ya nada más se puede hacer para que el agotamiento se prolongue por unos años más. Otra de las medidas que se han tomado por parte de IANA es reclamar las direcciones IPv4 que no se estén usando que al inicio de la implementación de IPv4 se dieron sin restricción.

El uso de subredes le ha sacado provecho a las direcciones IPv4 y prolonga el agotamiento, también llamado *subnetting*. El objetivo de las subredes es crear múltiples subredes lógicas de un solo bloque de direcciones IP. Esto se logra variando los bits de la máscara de subred la cual indica que bits de los 32 de la dirección IPv4 son bits de la red y cual bits son para el *host*.

Otro de los métodos para aprovechar las direcciones IPv4 y así prolongar el agotamiento es el uso de redes privadas. Cuando se estableció el sistema de *subnetting* la IANA reservo rango de direcciones IPv4 para identificar a las computadoras de las redes de área local (*Local Area Network*, LAN por sus siglas en inglés).

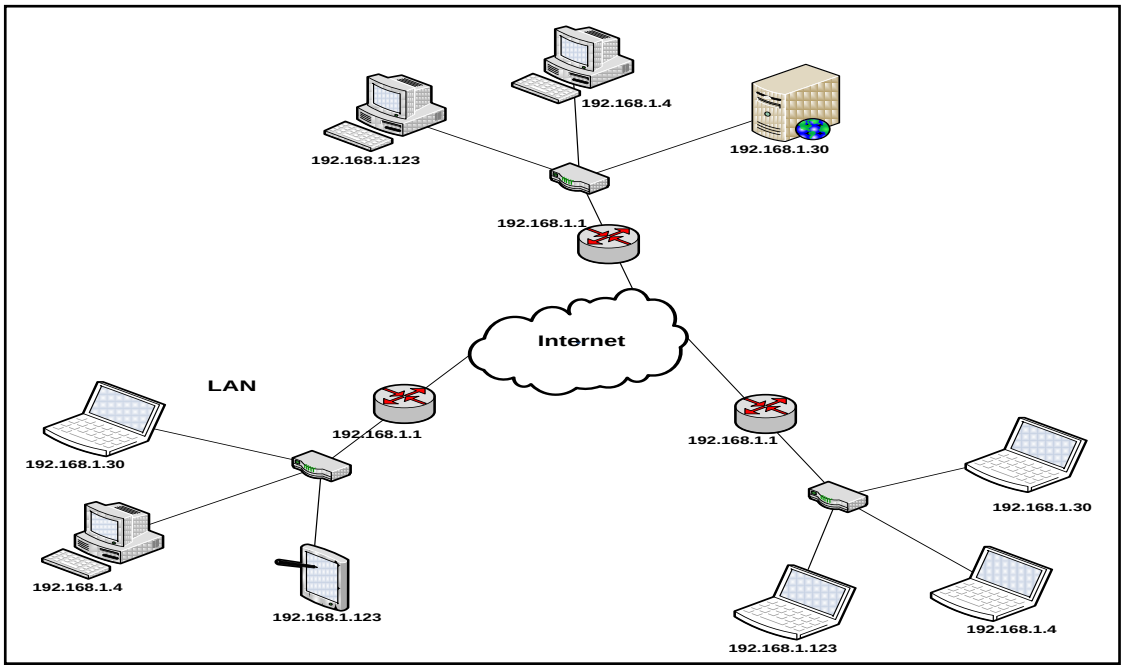
Con las direcciones IPv4 para las redes privadas se tiene la ventaja de poder repetir estas direcciones en las redes locales (vea figura 5). El rango de direcciones IPv4 privadas reservadas por IANA se muestran en la tabla III.

Tabla III. **Rango de direcciones IPv4 privadas**

| Rango de direcciones IPv4 | | Máscara de subred | Cantidad de redes | Cantidad de host por red |
|---|---|---|---|---|
| Inicio | Fin | | | |
| 10.0.0.0 | 10.255.255.255 | 255.0.0.0 | 1 | $2^{24}$ = 16 777 216 |
| 172.16.0.0 | 172.31.255.255 | 255.255.0.0 | 16 | $2^{16}$ = 65 536 |
| 192.168.0.0 | 192.268.255.255 | 255.255.255.0 | 255 | 255 |

Fuente: elaboración propia.

Figura 5. **Redes LAN**




Fuente: elaboración propia, con base a Microsoft Visio.

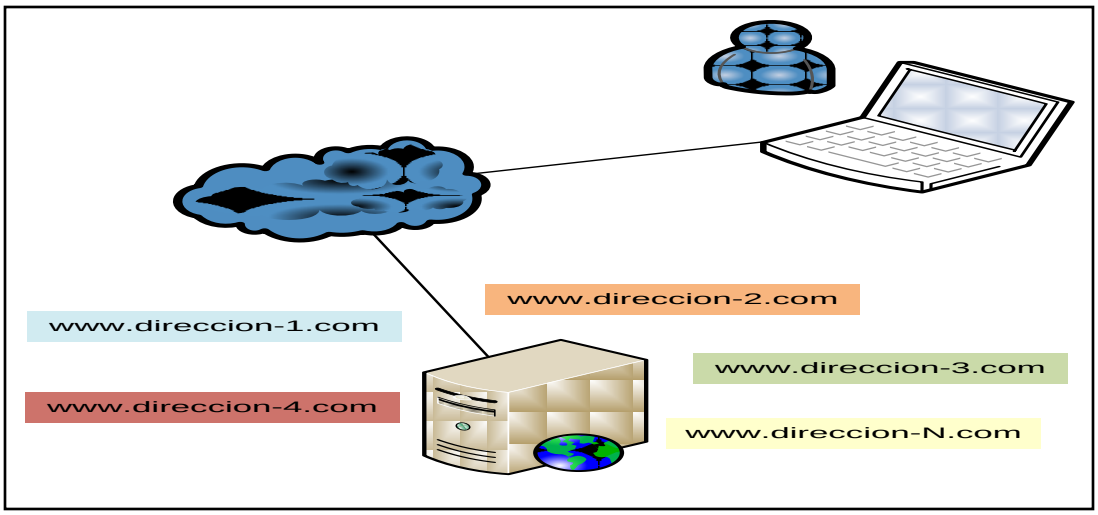
Como se ve en la figura 5 las direcciones IPv4 privadas pueden repetirse en redes de área local, ya que el tráfico de estas redes no está dirigido a exterior y cada uno de los computadores que conforman la red local, no necesitan estar públicos en internet. El uso de las redes privadas dio un gran desahogo a la escasez de direcciones IPv4 y así prolongo por algunos años más el agotamiento.

El objetivo principal de *Network Address Translation* (NAT por sus siglas en inglés) es preservar el número de direcciones IPv4 públicas que están disponibles para el internet. En general NAT consiste en utilizar una sola dirección IPv4 pública para representar a los ordenadores de una LAN, en vez de que todas las computadoras estén públicas en el internet, se utiliza una sola dirección IP pública para que represente a todas las computadoras.

El protocolo de configuración dinámica de maquinas (*Dynamic Host Configuration Protocol*, DHCP por sus siglas en inglés) a postergado el agotamiento de direcciones IPv4. El protocolo DHCP tiene como objetivo que cada *host* que conforman la red obtenga automáticamente los parámetros de configuración para hacer uso de los recursos de la red. La dirección IP, la máscara de subred, la puerta de enlace, y alguna otra configuración de servidores son algunos de los parámetros que recibe el *host* automáticamente.

Otra de las estrategias para minimizar el agotamiento de las direcciones IPv4 es el *hosting virtual* y consiste en alojar varios nombres de dominios en un computador. Con esta técnica se ayudan en gran parte a conservar las direcciones IPv4, dado que se alojan varios nombres de dominios o sitios web en un computador, en vez de utilizar una computadora por cada sitio web se pueden alojar en un solo computador (vea figura 6) y aprovechar las direcciones IP.

Figura 6. ***Hosting Virtual***




Fuente: elaboración propia, con base a Microsoft Visio.

Y por último pero no menos importante para minimizar el agotamiento de las direcciones IPv4 es reclamar direcciones IPv4 sin utilizar y tener un control exhaustivo en los RIR por parte de IANA que es la entidad reguladora de las direcciones IPv4.

## 1.2. Protocolo de internet versión 6 (IPv6)

Como una solución a las limitaciones del protocolo de internet IPv4 el *Internet Enginnering Task Force* (IETF por sus siglas en inglés) creo las IPng (*IP next generation*) también llamada IPv6. Las recomendaciones para la próxima generación de protocolo IP se definieron en la *Request For Comments* (Petición de Comentarios, RFC por sus siglas en inglés) número 1752 de la IETF en noviembre de 1994.

Las especificaciones técnicas del IPv6 son definidas en el RFC 1883, en donde se definen los detalles de cada una de las especificaciones para la IPv6. La IPv6 no solo está diseñada para eliminar las limitaciones de la IPv4 mencionados anteriormente sino también incluye varias mejoras para facilitar su administración, entre las cuales se pueden mencionar: cuenta con seguridad obligatoria mientras en la IPv4 es opcional, cuenta con cabeceras destinadas a la autenticación y la encriptación del datagrama, entre otras mejoras.

### 1.2.1. Especificaciones de la IPv6

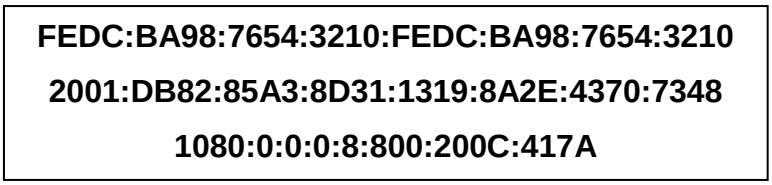
Las especificaciones de la IPv6 están definidas en el RFC 1883 definidas por la IETF, a continuación se definirán las especificaciones más importantes que de la IPv6 y sustituyendo así al actual IPv4.

El espacio de direcciones para la IPv6 es 128 bits comparado con la IPv4 que consta de 32 bits, proporcionando una cantidad casi infinita siendo esta de 340 282 366 920 938 463 374 607 431 748 211 456 x $10^{38}$, esta cantidad exuberante de direcciones IPv6 es muy superior a las 4 300 millones de direcciones IPv4 posibles las cuales en la actualidad están por agotarse. Visto de otra manera, significa que si la población mundial fuera de 10 billones habría 3,4 x$10^{27}$ direcciones IPv6 por cada habitante, siendo así muy pequeña y casi imposible la posibilidad de que se agoten las nuevas direcciones.

A diferencia de la IPv4 que se representa con notación decimal las direcciones IPv6 se representan con notación hexadecimal y constan de 8 campos de 16 bits cada uno, en la representación de las direcciones IPv6 no es necesario escribir los ceros a la izquierda de cada uno de los campos, pero al menos debe existir un numero en cada campo.

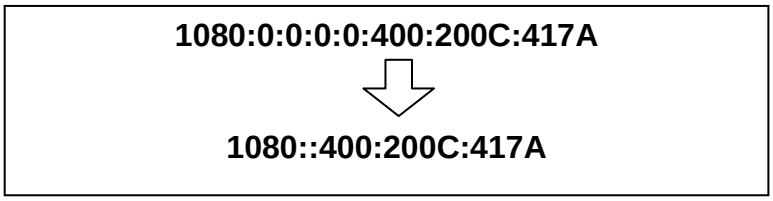
Algunos ejemplos de direcciones IPv6 se muestran en la figura 7, las direcciones IPv6 se pueden representar en formato comprimido, esto para no escribir en su totalidad las direcciones y no sea tediosa su escritura, para esto si existen ceros consecutivos se pueden omitir y representarlos con el símbolo '**::**' (vea figura 8).

Figura 7. **Representación de direcciones IPv6**




Fuente: elaboración propia.

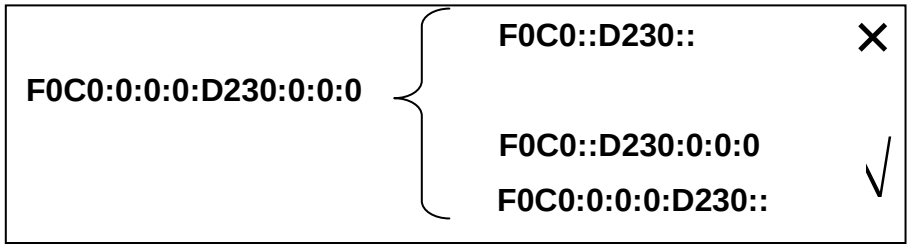
Figura 8. **Representación comprimida de las direcciones IPv6**




Fuente: elaboración propia.

Si llegaran a existir ceros consecutivos en dos partes de la dirección IPv6 solo está permitido utilizar el símbolo '**::**' una sola vez en la dirección. En la figura 9 se muestra la forma correcta e incorrecta de la representación comprimida de las direcciones IPv6.

Figura 9. **Representación comprimida de direcciones IPv6**




Fuente: elaboración propia.

La IPv6 cuenta con una arquitectura jerárquica de direcciones, lo que hace más simple y eficiente el enrutamiento de paquetes dentro de una red, obteniendo un ruteo más eficiente en el *backbone* de internet, ya que se reducen considerablemente las tablas de ruteo. Otra característica importante es la autoconfiguración de equipos lo cual consiste en un conjunto de pasos que son necesarios en el *host* para decidir como configurar sus interfaces IPv6.

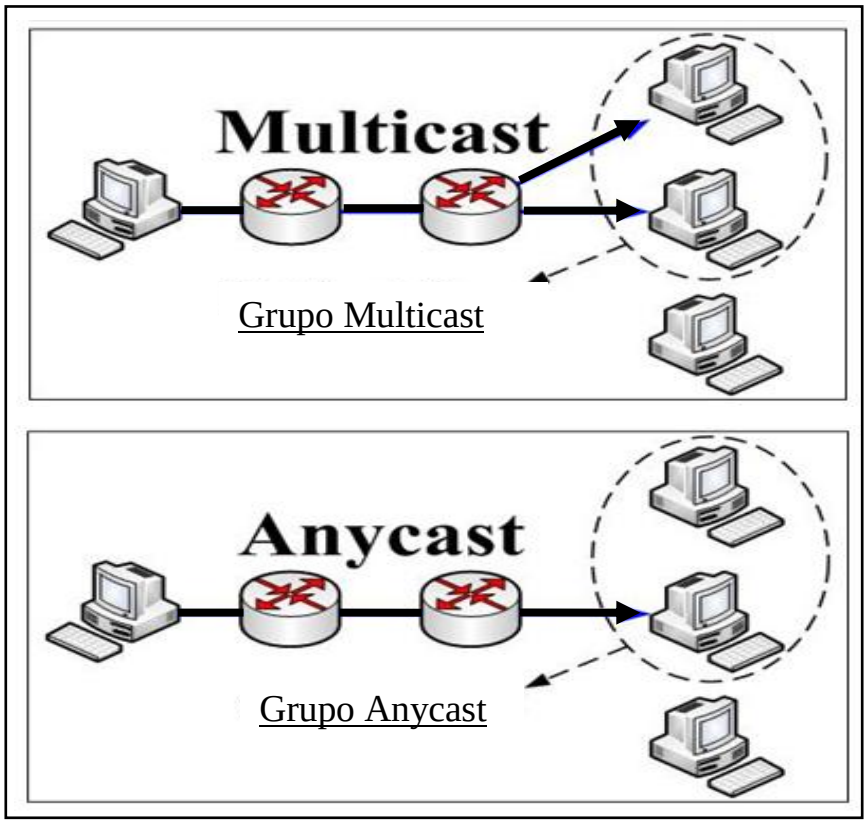
La movilidad en IPv6 consiste en la capacidad de habilitar a un nodo dentro de la red local sin necesidad de cambiar su dirección, esto permite la comunicación desde cualquier punto donde se acceda a la red. Un dato interesante es que la IPv6 esta especificada como el protocolo IP obligatorio en la prestación de servicios en redes para la telefonía móvil.

La seguridad e integridad de datos en la IPv6 está garantizada por defecto, dado que hace uso de IPSec (vea capítulo 4), por lo tanto se mantiene una conexión segura a nivel de IP y proporcionar una verificación de autenticidad y/o confidencialidad, lo que garantiza la integridad de los datos en los paquetes.

La calidad de servicio (*Quality of Services*, QoS por sus siglas en inglés) en la IPv6 provee de la capacidad de control de flujo de datos, lo cual permite marcar los paquetes que pertenezcan a un determinado tipo de tráfico y también permite la administración del ancho de banda sin necesidad de analizar cabeceras TCP ni cabeceras UDP en los paquetes.

La IPv6 tiene soporte obligatorio a *multicast* y *anycast*, el primero se refiere al envió de un mismo paquetes a un grupo de receptores y el segundo se refiere al envió de un paquete a un receptor dentro de un grupo (vea figura 10).

Figura 10. ***Multicast y anycast***




Fuente: elaboración propia, con base a Microsoft Visio.

### 1.2.2. Iniciativas de la IPv6

En todo el mundo existen iniciativas las cuales planifican la adopción de la IPv6. En la actualidad el despliegue de la IPv6 ha tenido un mayor avance que en años anteriores, debido a que la cantidad de direcciones IPv4 están prácticamente agotadas y se debe empezar a adoptar la IPv6. En todo el mundo se están creando alianzas entre el gobierno, la academia y la industria para afrontar el problema del agotamiento en conjunto y así de esta manera el problema será menos complicado.

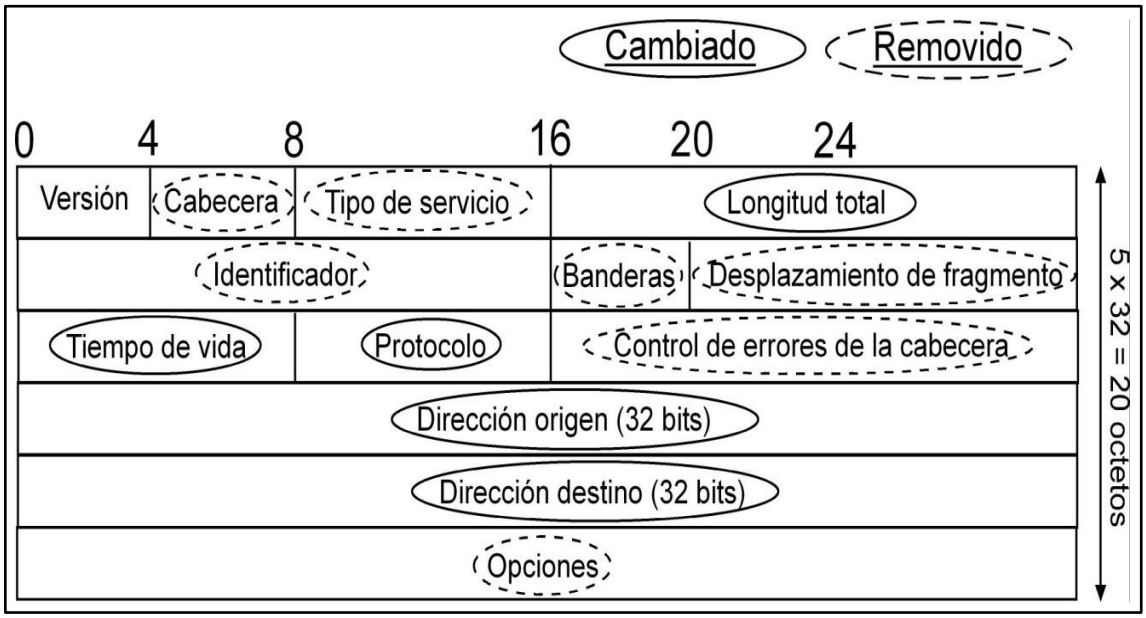
Un buen ejemplo de lo que se está realizando alrededor del mundo es el *World IPv6 Day* (Día Mundial de la IPv6) que se celebro el 8 de junio de 2011, ese día y durante 24 horas, todos los participantes activaron sus servicios a través del protocolo IPv6, realizaron mediciones y preparando así una transición exitosa desde el actual protocolo IPv4. Entre las instituciones participantes están grandes proveedores de contenido en internet como *Google*, *Yahoo*, *Facebook*; y de proveedores de infraestructura y redes como *Akamai*, *Comcast*, entre muchos otros.

### 1.2.3. Ventajas de la IPv6

La ventaja inmediata de la IPv6 es la cantidad de direcciones IP disponibles para cada uno de las personas o dispositivos que lo necesiten, siendo esta cantidad casi infinita y suficiente para los próximos años.

La cabecera de la IPv6 cuenta con un mejor formato, ha sido diseñado para acelerar el proceso de enrutamiento. La cabecera de opciones de la IPv6 se separa de la base de la cabecera. Las opciones son insertadas en la base de la cabecera sólo cuando sea requerido por los datos de capa superior. En la figura 11 se observa que partes han sufrido cambios y cuales fueron removidos del paquete IPv4 para dar lugar al paquete de la IPv6 (vea figura 12), donde se puede observar que es más simple, esto es lo que acelera el proceso de enrutamiento teniendo menos información que procesar.

Figura 11. **Paquete IPv4**




Fuente: elaboración propia, con base a Microsoft Visio.

Figura 12. **Paquete IPv6**


Fuente: elaboración propia, con base a Microsoft Visio.

La IPv6 tiene integrada la seguridad y no agregada como pasa con la IPv4. La IPv6 aprovecha el protocolo IPSec, la arquitectura, la autenticación, el cifrado de seguridad y las garantías de integridad de datos son inherentes en el protocolo IPv6.

Otra ventaja importante es que existe más facilidad en la gestión de la red, reduce la complejidad ya que permite una arquitectura de red más simple y manejable. Contiene funciones de configuración automáticas esto puede conseguir que la red sea tan fácil como conectar un cable a una computadora, ofreciendo una experiencia de *plug and play* que satisface a los usuarios y liberar al personal de TI en centrarse en el funcionamiento de la red.

IPv6 garantiza una mejor conexión *peer to peer* (punto a punto), permitiendo que todos los nodos tengan su propia dirección global y única, abriendo el camino a poderosas redes de seguridad. Esto permitirá a las personas a tener acceso y compartir recursos sin mayor complejidad. Esto introduce de nuevos servicios, tales como la voz sobre IP (VoIP) o la mensajería instantánea sea mucho más fácil.

La IPv6 tiene la ventaja de experimentar una movilidad más fluida, ya que la dirección IP permite a los ordenadores y otros dispositivos tener un ID de interfaz estática. El ID de interfaz no cambia a medida que el dispositivo de usuario cambie de un lugar a otro, así que con la IPv6 móvil se puede pasar de una red a otra, manteniendo la misma dirección IP única.

### 1.2.4. Desventajas de la IPv6

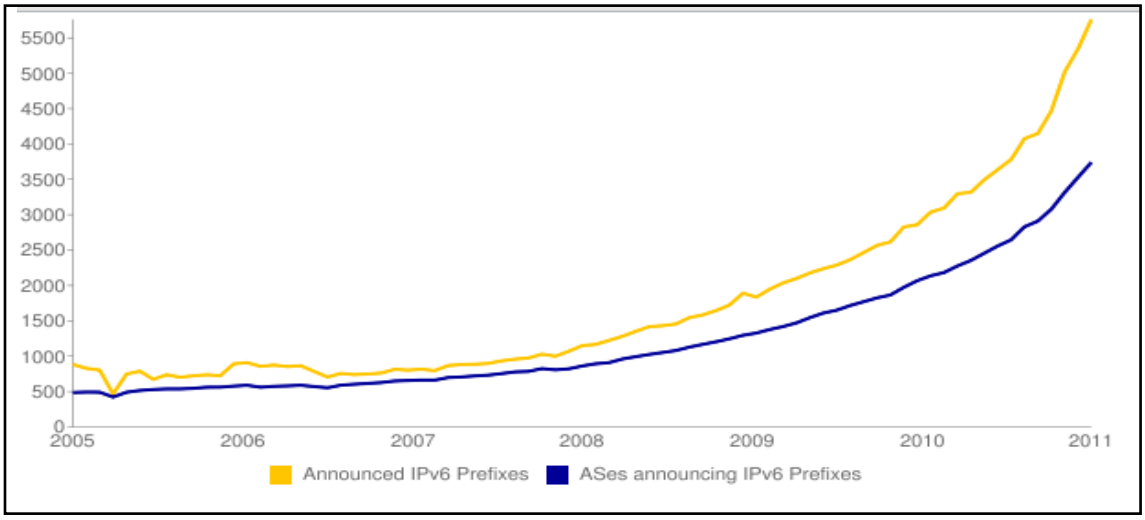
En el diseño de la IPv6 se tienen pocas desventajas. Las cabeceras son más grandes y requieren de más espacio en los *buffers* y en las tablas de enrutamiento, a pesar de que es más fácil de procesar que IPv4. La cabecera de la IPv6 es de tamaño fijo en el caso más común, pero la IPv6 tiene el enfoque de cabeceras de extensión, esto consiste en ampliar las cabeceras, lo que requiere más espacio.

Dichas cabeceras de IPv6 son opcionales, y dichos encabezados puede ser un problema en la implementación de *hardware*, ya que a excepción del primer encabezado, la información no se encuentra en un desplazamiento fijo desde el inicio del paquete. Por lo tanto, las extensiones deben ser escaneadas de forma secuencial para determinar su contenido, la ubicación y el tipo de cabecera de extensión que viene en el paquete.

## 1.3. IPv6 solución a largo plazo

IPv6 poco a poco va ganando terreno, desde el 2005 como se muestra en la gráfica de la figura 13, la IPv6 constantemente va teniendo presencia y más aun con el agotamiento de las direcciones IPv4.

Figura 13. **Presencia de la IPv6 en el internet**




Fuente: Asignación y estadísticas de enrutamiento.

Existen varios obstáculos para realizar el cambio a IPv6, principalmente la IPv6 no es directamente compatible con IPv4, lo que significa que los dispositivos conectados a través de IPv4 no se puede comunicar directamente con los dispositivos conectados a través de IPv6. Así también la implementación de IPv6 requiere medidas proactivas: la tecnología se debe mejorar, el personal de la empresa debe ser capacitado, contar con estrategias de transición acordes a las expectativas de la empresa.

Fundamentalmente los obstáculos que se describen a continuación son la disponibilidad de tecnología del internet, la disponibilidad de las aplicaciones, los costes de la nueva numeración, la experiencia operativa, y la disponibilidad de infraestructura. La disponibilidad de las tecnologías como los sistemas operativos más recientes como *MacOS X*, *Linux* y *Windows* tienen soporte para IPv6. Prácticamente casi todas las empresas y dispositivos de red que se han incorporado en los últimos cinco años tienen compatibilidad con IPv6.

Algunos dispositivos con más años soportan IPv6 al realizar una actualización del *firmware*, sin embargo, no todas las empresas tienen *hardware* compatibles y requieren sustituirlos, esto lo arroja los resultados la encuesta de la tabla IV realizada por la empresa estadunidense *Ipswitch*.

Tabla IV. **Resultados encuesta *Ipswitch***

| | |
|---|---|
| 0 – 20% | 66,1% |
| 20 – 40% | 9,6% |
| 40 – 60% | 6,5% |
| 60 – 80% | 5,8% |
| 80 – 100% | 12,0% |

Fuente: *Ipswitch poll shows disturbing gap in IPv6 readiness among enterprise networks*.

Dicha encuesta consistió en responder la pregunta ¿Qué porcentaje de su infraestructura de red está lista para IPv6? Y los resultados del estudio revelo que 88% de las redes de las empresas encuestadas no están completamente listas para el cambio a la IPv6, con dos tercios (66,1%) de los encuestados respondieron que su infraestructura de red esta de 0 a 20% lista para IPv6 como se muestra en la tabla IV.

Los costes de la nueva numeración de los dispositivos es alta, y esto consiste cambiar las direcciones IP para cada dispositivo en la red. El cambio de dirección IP a cada dispositivo no es tarea difícil, solo se debe de reconfigurar el DHCP para que los dispositivos obtengan la nueva dirección IP. Esta tarea se complica al tener que cambiar manualmente la base de datos de DHCP para cambiar las direcciones de los servidores, también así, en la actualización de las tablas de enrutamiento de los *routers* para las rutas entre redes.

Otro de los obstáculos para realizar el cambio a la IPv6 es la experiencia operativa de la IPv4 ya que tiene más de 30 años. Muchas cosas que se veía bien en papel para la IPv4 resultó ser errónea. Esta experiencia permitió el descubrimiento de muchos fallos de seguridad, tanto de la causas de aplicación y de infraestructura.

Y por último pero no menos importante es la disponibilidad de infraestructura, en la actualidad la mayoría de organizaciones con presencia en el internet no cuentan con una infraestructura de red compatible con la nueva generación del protocolo de internet y la expansión que tiene el internet hace aun más complejo realizar el despliegue de la IPv6.

La IPv6 fue diseñada pensando que los dos protocolos de internet coexistirán por varios años, hasta que se complete la transición a la IPv6. Según el informe realizado por el Instituto Nacional de Estándares y Tecnología en 2005 concluyeron que: se necesitarían alrededor de 25 años para tener una transición total a la IPv6 a un costo aproximado de 25 billones de dólares estadunidenses. Expertos consideran que los 25 años son relativamente rápido para la adopción de esta tecnología, la introducción de la conmutación digital desde la conmutación analógica tomó más de 35 años.

# 2. TRANSICIÓN A IPV6

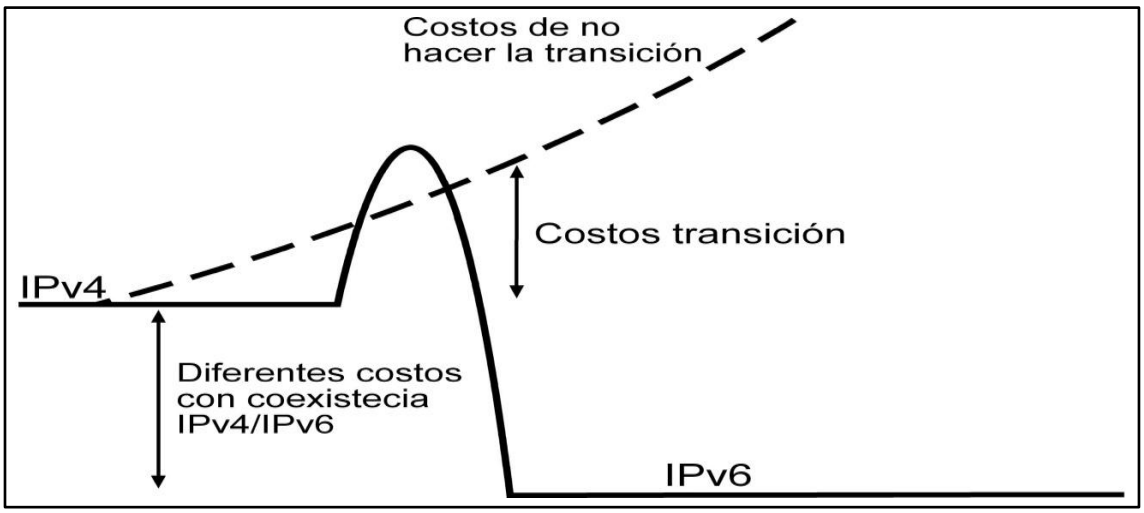
Al hablar de migración de IPv4 a IPv6 para muchos es algo complejo que tarde o temprano se debe realizar, mientras más tarde se afronte el tema de la IPv6 más costoso y más complicaciones habrá para la organización, el término migración es inadecuado dado migrar implica hacer un cambio de IPv4 a IPv6 de un momento a otro, algo imposible de realizar por la complejidad de la infraestructura de internet, lo adecuado es hablar en términos de una transición que consiste en realizar un cambio gradual de IPv4 a IPv6.

La transición a IPv6 desde IPv4 no se realizara a corto plazo dado que esto significaría dejar de utilizar la IPv4 y empezar a utilizar la IPv6, el cambio será gradual y coexistirán por varios años hasta que toda la infraestructura del internet haya realizado el cambio por completo a la IPv6. La IPv6 se diseño para coexistir con la IPv4, dar solución a las problemáticas del actual protocolo de internet y agregar a internet nuevas características.

Realizar una planificación de la transición a IPv6 es importante, en donde se deben definir tiempos, costos y demás por menores que se requerirán para realizar una transición eficiente y no tener mayores complicaciones. La planificación debe estar enfocada a realizar un cambio gradual, es decir, planificar la adopción a la IPv6 a corto, mediano y largo plazo, hasta que esté completamente implementada la IPv6. La planificación que se describe en este capítulo se basa en el RFC 5211 de la organización internacional IETF.

Los costos al no realizar la transición a IPv6 aumentan exponencialmente (vea figura 14), al contrario si se realiza la transición lógicamente los costos se disminuyen conforme coexisten los dos protocolos de internet, hasta llegar al objetivo de que todo funcione bajo la IPv6, donde los costos son aun más bajos que resistiéndose al cambio de protocolo de internet.

Figura 14. **Gráfica proyección de costos de transición**




Fuente: *IPv6 transition – industry best practices*.

## 2.1. Planificación

Toda actividad requiere de una planificación para garantizar el éxito de la misma y la transición a IPv6 no es la excepción, es por ello que en esta sección se definirá la planificación que la IETF recomienda para la transición a IPv6. Esta planificación conocida como el plan de transición de internet, donde se define la transición de un modelo de conectividad basado en IPv4 a un modelo de conectividad basado en IPv6.

La motivación para especificar un plan de transición a IPv6 es facilitar la coordinación de las innumerables entidades implicadas, por lo tanto, reducir el riesgo a la propiedad de internet de la conectividad universal. El propósito de especificar esta planificación en particular es para permitir la evaluación global de los retos a llevar a cabo en la transición y con el fin de facilitar la plena conectividad del internet durante toda la transición a IPv6, un plan de transición que proporciona una orientación clara a las entidades involucradas respecto a las expectativas que esperan tener con la transición.

En una estrategia de transición la entidad ejecutante no debe de realizar la transición en toda la infraestructura a la vez, al contrario, se debe realizar la transición por fases. Los miembros del personal involucrados aprenden y experimentan los beneficios de la IPv6, mientras la transición está en marcha. Según RFC 5211 existen tres fases para la transición a IPv6 las cuales son:

- Preparación
- Transición
- Postransición

La estrategia de transición a IPv6 definida a continuación no es la única para las entidades con necesidad de implementar la IPv6, una estrategia de transición a IPv6 dependerá de la infraestructura y de los términos globales para que sea exitosa la transición. No existe una estrategia de transición general para cada entidad, se debe crear una distinta para cada entidad, la estrategia definida en este capítulo tiene como objetivo dar una idea general de lo que trata la transición a IPv6.

### 2.1.1. Fase de preparación

En esta fase están involucrados los proveedores de servicio de internet (ISP por sus siglas en inglés) que deben implementar pruebas piloto en sus servicios de red con conectividad IPv6, también están involucradas todas las entidades con presencia en internet y deben de preparar sus servicios locales orientados a internet a través de la conectividad IPv6, sin dejar de prestar sus servicios a través de la conectividad IPv4. Durante esta fase, los principios que se siguen son los siguientes:

- Preparación 1: las pruebas piloto para la IPv6 por parte del ISP en sus distintos servicios de red se realizan mediante el uso de mecanismos de transición o por medio de IPv6 nativa.

- Preparación 2: las entidades con presencia en el internet deben de disponer de conectividad IPv6 a sus servicios locales.

- Preparación 3: las entidades involucradas proporcionan conectividad a internet a través de IPv6 a los usuarios internos.

Los ISP deben realizar pruebas para brindar servicios basadas en IPv6 a sus clientes de internet por medio de los mecanismos de transición a IPv6 se describen en el capítulo 3. Las entidades involucradas deben disponer de conexión a internet basadas en IPv6 en sus servicios locales.

Los servicios orientados a internet IPv6 en los servidores de esta fase deben utilizar servidores de nombres de dominios independientes como lo define el RFC 4472 para evitar el impacto a los servicios de producción basados en IPv4, a menos que la entidad apoye la producción a través de IPv6.

### 2.1.2. Fase de transición

En la fase de transición, los ISP ofrecen los servicios de red con conectividad basada en IPv6 e IPv4 a sus clientes de internet. Las entidades involucradas ofrecen sus servicios orientados del internet a sus clientes a través de la conectividad basada en IPv6, además de la conectividad basada en IPv4, durante esta fase los principios son:

- Transición 1: los ISP deben ofrecer sus clientes sus servicios basados en IPv6. Los servicios de internet ofrecidos en IPv6 deberán ser a través de IPv6 nativa, aunque puede ser a través de mecanismos de transición IPv6 si fuese necesario.

- Transición 2: las entidades involucradas con presencia en el internet deben disponer de conexión a internet basadas en IPv6 para los servidores orientados a internet, estos servicios deben ser parte de la producción y también deber ser tratado en producción para otras entidades en el internet.

- Transición 3: las organizaciones deben proporcionar conectividad a internet basado en IPv6 a sus usuarios internos, y proporcionar de soporte IPv6 a sus servidores internos.

A diferencia de la fase de preparación en esta fase los servicios prestados deben ser en IPv6 nativa y no por medio de mecanismos de transición a menos que sea necesario, las entidades involucradas deben de proveer de los servicios de red con presencia en internet tanto a sus usuarios internos como a los usuarios externos que hacen uso del mismo y que dichas entidades deben de tomar como parte de su producción los servicios con soporte a IPv6.

### 2.1.3. Fase postransición

En la fase post-transición, las entidades involucradas proporcionan todos los servicios orientados a internet a través de la conectividad basada en IPv6, lo que permite a los nuevos clientes de internet conectarse exclusivamente por el IPv6. Durante esta fase los principios a seguir son:

- Post-transición 1: los ISP deben ofrecer los servicios basados en internet en IPv6 nativa a sus clientes. En esta fase ya no se permite el uso de mecanismos de transición para brindar los servicios.

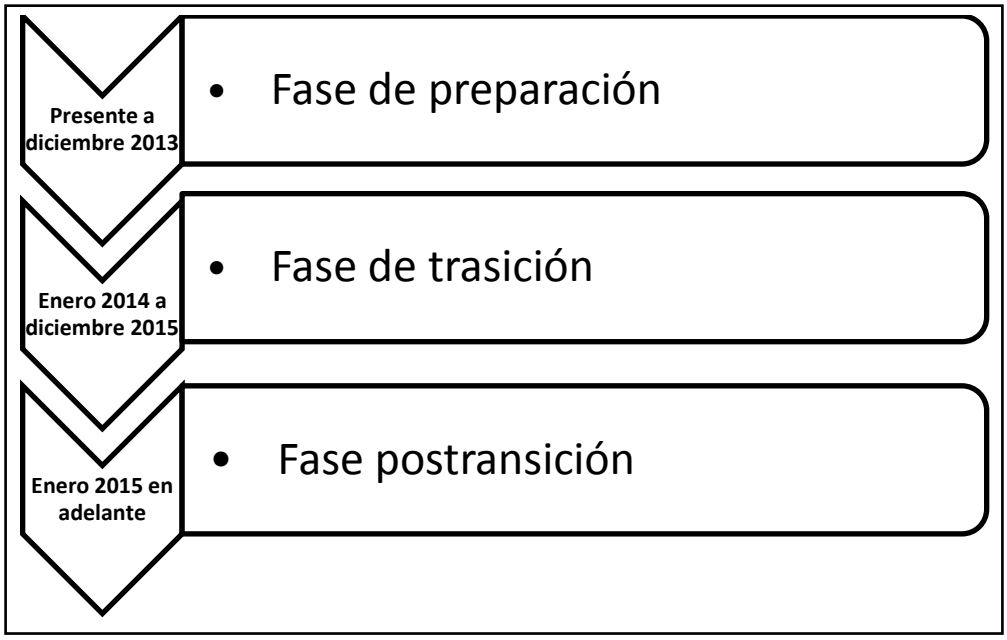
- Post-transición 2: las entidades involucradas deben disponer de conexión a internet basadas en IPv6 para los servidores orientados a internet. Los servidores públicos con IPv6 deben ser tratados sin excepción como la producción para la entidad ejecutante y para otras entidades en el internet.

- Post-transición 3: las entidades deben proporcionar conectividad a internet basado en IPv6 a sus clientes y usuarios internos, y proporcionar soporte interno a la infraestructura IPv6. La conectividad IPv6 puede ser nativa o por medio de mecanismos de transición.

- Post-transición 4: los ISP podrán mantener la conexión a internet basada en IPv4 a sus clientes de internet.

Durante las tres fases que conforman el plan estratégico todos los involucrados deben aportar de su tiempo y recursos para que la transición a IPv6 sea exitosa y se garantice la conectividad. El tiempo estimado para llevar a cabo el plan se detallan en la figura 15, donde se define un aproximado de dos años para cumplir a cabalidad sino llegara a darse ningún inconveniente.

Figura 15. **Línea de tiempo y fases de transición a IPv6**




Fuente: elaboración propia.

## 2.2. Componentes de un plan de transición a IPv6

La planificación se describió a grandes rasgos y los componentes que se describirán a continuación son importantes y se recomienda ser incluidos en la planificación específica para la infraestructura de red de la entidad ejecutante. Según el *Chief Information Officer* (CIO por sus siglas en inglés) federal del consejo de arquitectura e infraestructura del comité de los Estados Unidos de Norte América la siguiente lista de componentes pueden ser utilizados como base para realizar un plan de transición a IPv6. Dependiendo de las necesidades de la entidad interesada, así se incluirá cada uno de estos componentes. Los componentes a tomar en cuenta son los siguientes:

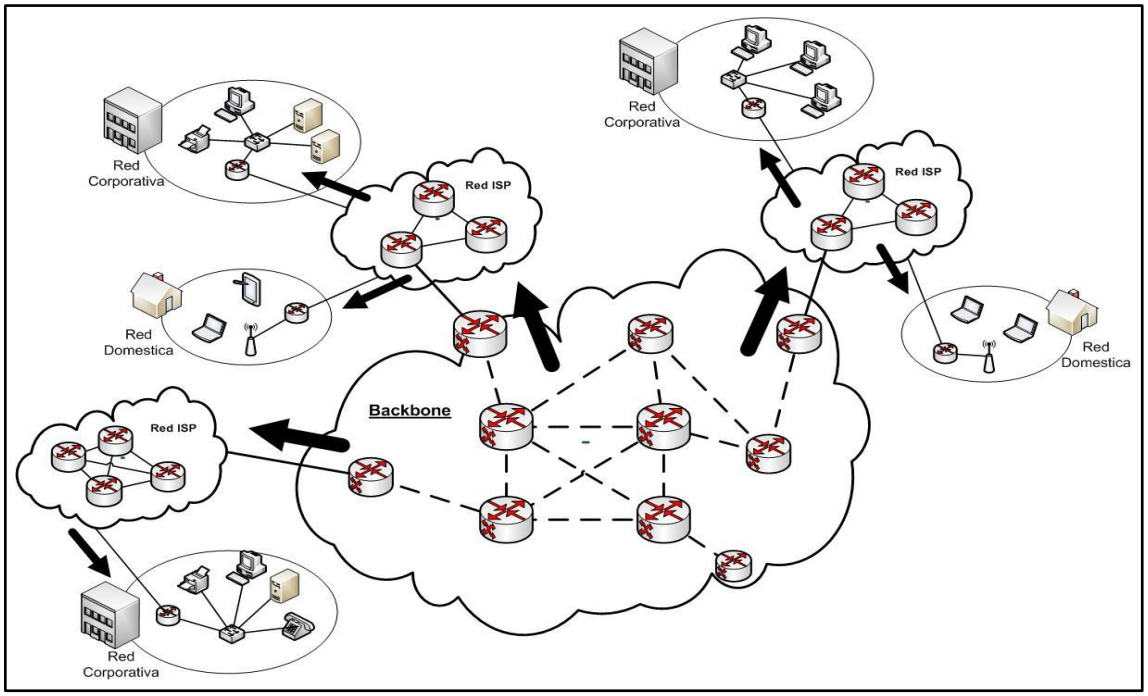
- Identificación de los objetivos estratégicos del negocio.
- Identificación de las actividades de transición.
- Identificación de las prioridades en la transición.
- Etapas de transición.
- Criterios de transición para el legado, las mejoras, y las nuevas capacidades.
- Medios para la adjudicación de créditos.
- Estrategia técnica y de selección de los mecanismos de transición para facilitar la interoperabilidad IPv4/IPv6.
- Gestión y asignación de recursos para la transición.
- Garantizar la interoperabilidad y la seguridad durante la transición.
- Uso de estándares y productos IPv6.
- Soporte a la infraestructura IPv4 durante y después del despliegue de IPv6 en la red.
- Migración de aplicaciones (si fuese necesario para apoyar la transición).
- Costos no cubiertos por la actualización tecnológica.
- Gobernanza en la transición.
    - Política
    - Roles y responsabilidades
    - Gestión de la infraestructura
    - Medición del desempeño
    - Presentación de informes
- Adquisición y contratación
- Capacitación
- Pruebas

## 2.3. Buenas prácticas en la transición a IPv6

La manera de realizar la transición a IPv6 es crítica debido a las metas y objetivos de la organización. Entre las buenas prácticas en la transición a IPv6 existen varios enfoques que se han identificado a un alto nivel, tales como: una transición desde adentro hacia afuera, de afuera hacia dentro, transición geográfica y mediantes subredes.

En el enfoque de transición desde adentro hacia afuera consiste en iniciar la transición desde en las redes *backbone*, se extiende a los proveedores de internet, posteriormente a las redes corporativas, las redes domesticas y estaciones de trabajo final, y finalmente a las aplicaciones (vea figura 16).

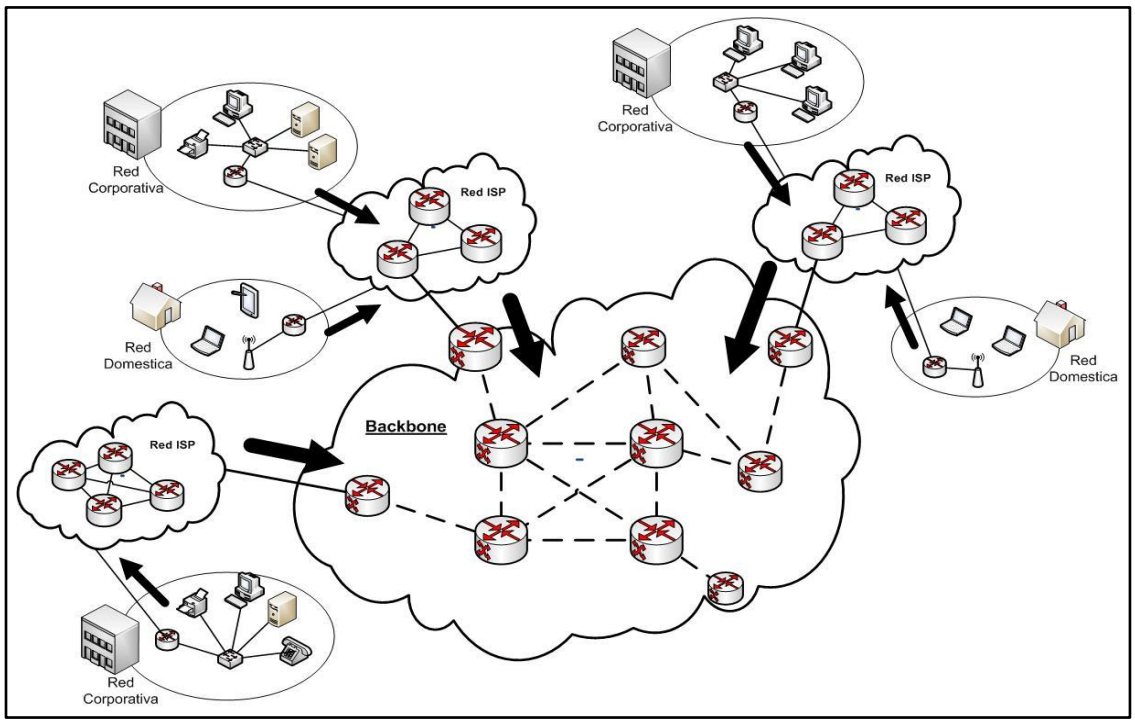
Figura 16. **Enfoque de adentro hacia afuera**




Fuente: elaboración propia, con base a Microsoft Visio.

El enfoque de afuera hacia dentro es parecido al enfoque anterior con la diferencia que la transición comienza con las aplicaciones y estaciones de trabajo, redes corporativas, redes domesticas, hasta llegar a la red *backbone* principal (vea figura 17).

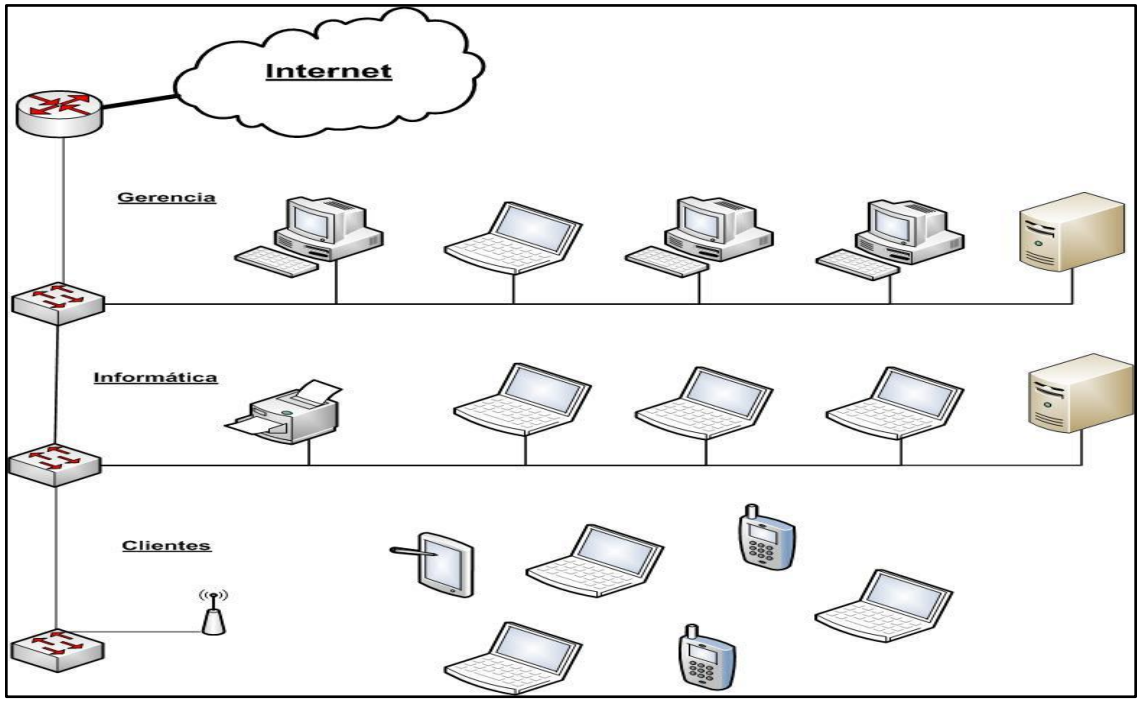
Figura 17. **Enfoque de afuera hacia adentro**




Fuente: elaboración propia, con base a Microsoft Visio.

El tercer enfoque de transición propuesto es el llamado transición geográfica y consiste en realizar la transición sobre la base geográfica de la red, es decir, enfocar la transición por áreas o departamentos de la organización hasta completar toda la transición a IPv6 (vea figura 18), para ejemplificar este enfoque al implementar la transición se empezaría por el departamento de informática, gerencia y por último los clientes.

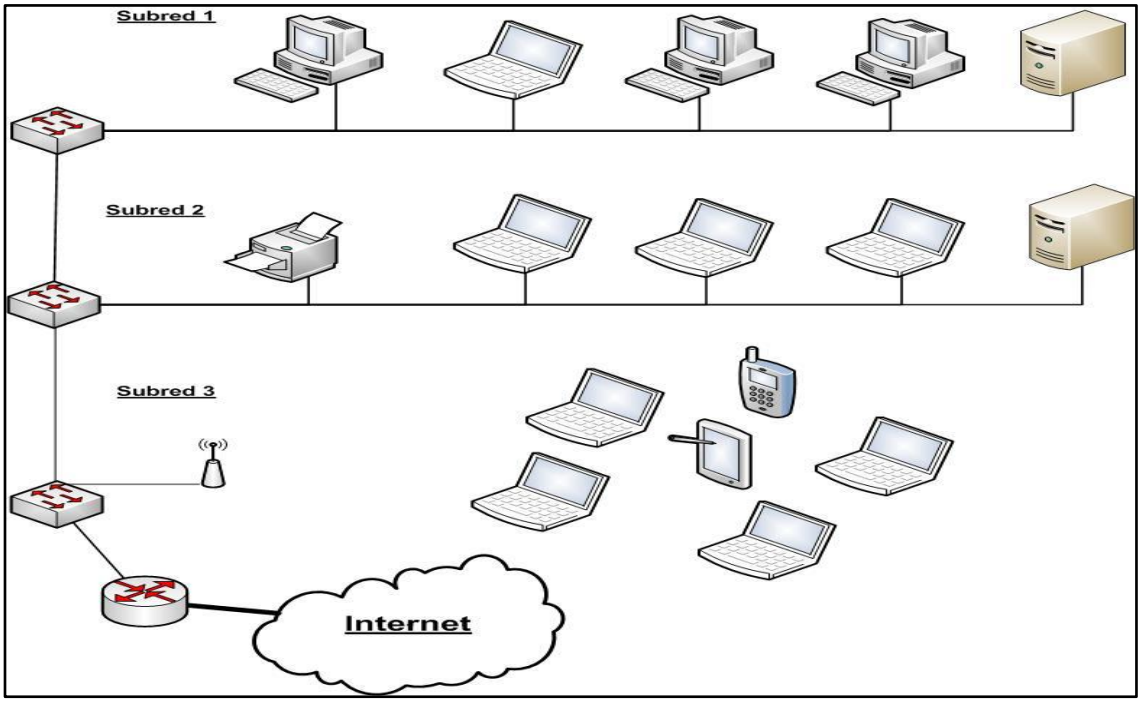
Figura 18. **Enfoque de transición geográfica**




Fuente: elaboración propia, con base a Microsoft Visio.

El último enfoque de transición pero no menos importante es el llamado subred, este enfoque consiste en realizar la transición a IPv6 sobre la base de los segmentos de subred, es decir, se realiza la transición enfocándose en una subred y hasta no completar todas las actividades a realizar no podrán tomar otra subred para iniciar la transición a IPv6 (vea figura 19), al implementar este enfoque se puede realizar enfocándose primero en la subred 1, luego la subred 2 y por último la subred 3.

Figura 19. **Enfoque de subred**




Fuente: elaboración propia, con base a Microsoft Visio.

# 3. COEXISTENCIA ENTRE PROTOCOLOS DE INTERNET IPv4/IPv6

Si la IPv6 se hubiese diseñado para ser compatible con IPv4, la transición a IPv6 sería menos compleja. Muchos profesionales coinciden en que la verdadera compatibilidad para IPv4 fue un fallo crítico sencillo, pero diseñar la IPv6 con compatibilidad con IPv4 la limitaría y no proveería de las características que brinda la IPv6. Se espera que la transición sea bastante compleja y por lo tanto inicialmente, la coexistencia entre las dos generaciones del protocolo de internet será fundamental.

La coexistencia consiste en ejecutar ambos protocolos de internet en los puntos finales o nodos, convertir de IPv4 a IPv6 y viceversa, o crear túneles en la actual infraestructura IPv4, estas alternativas tienen un papel importante en el inicio al cambio a IPv6.

La comunicación en internet según la investigación realizada por la IETF nombrada *framework* para la transición de IPv4 a IPv6 define los siguientes seis escenarios en la comunicación que merecen especial atención y requieren de las prácticas de mecanismos de transición:

- Escenario 1: un sistema IPv4 se conecta a un sistema IPv4 a través de una red IPv4.

- Escenario 2: un sistema IPv6 se conecta a un sistema IPv6 a través de una red IPv6.

- Escenario 3: un sistema IPv4 se conecta a un sistema IPv4 a través de una red IPv6.

- Escenario 4: un sistema IPv6 se conecta a un sistema IPv6 a través de una red IPv4.

- Escenario 5: un sistema IPv4 se conecta a un sistema IPv6.

- Escenario 6: un sistema IPv6 se conecta a un sistema IPv4.

## 3.1. Mecanismos de transición

En general los mecanismos de transición, se agrupan en tres formas: doble pila, traducción y túnel. El elemento principal para la transición a IPv6 es la doble pila por lo práctico a la hora de implementar y consiste en ejecutar a la IPv4 e IPv6 en paralelo. La doble pila puede ser implementada tanto en los sistemas finales como en los dispositivos de red.

El segundo grupo es la traducción y se refiere a la conversión directa de los protocolos IPv4 e IPv6. La traducción se considera transparente para el usuario final, es decir, el usuario no tiene la menor idea de que se traduce de un protocolo a otro para garantizar la comunicación. La última pieza fundamental para la transición son los túneles. Los túneles se pueden considerar técnicamente como la transferencia de un protocolo encapsulado dentro de otro protocolo entre dos nodos y/o sistemas finales.

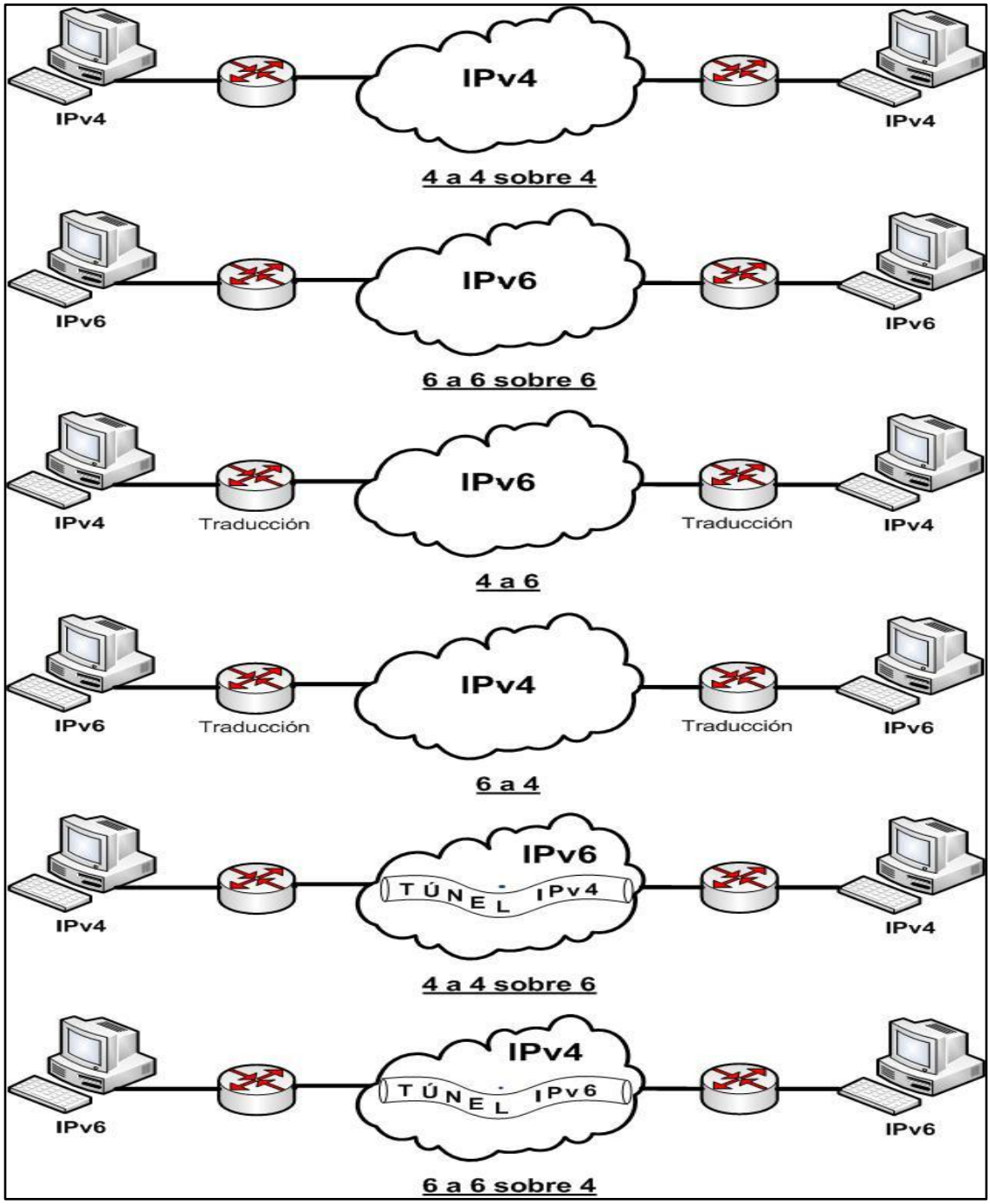
En la tabla V se especifican los mecanismos de transición más importantes, en cada uno se especifica el tipo de grupo al que pertenecen, la conectividad que indica como es la comunicación en el mecanismo de transición, por ejemplo la conectividad 4 a 6 significa que existe una traducción de protocolos de IPv4 a IPv6 o la conectividad 6 a 6 sobre 4 significa que existe comunicación de un dispositivo IPv6 a otro IPv6 sobre una red IPv4 es el caso del túnel, cada una de estas conectividades se ilustran en la figura 20. La ubicación indica donde se localiza específicamente el mecanismo de transición, ya sea en la estación de trabajo (ET), en el dispositivo de red (DR), o en medio de una combinación de las dos anteriores.

Tabla V. **Clasificación de los mecanismos de transición**

| **Nombre** | **Tipo** | **Conectividad** | **Ubicación** |
|---|---|---|---|
| Doble pila | Doble pila | 4 a 4 sobre 4, 6 a 6 sobre 6 | En un ET o DR |
| NAT-PT | Traducción | 6 a 4, 4 a 6 | En un DR |
| TRT | Traducción | 6 a 4 | En un ET o DR |
| BIS | Traducción | 4 a 6 | En un ET |
| BIA | Traducción | 4 a 6 | En un ET |
| 6to4 | Túnel | 6 a 6 sobre 4 | En medio de dos DR |
| 6over4 | Túnel | 6 a 6 sobre 4 | En medio de ET y DR |
| Teredo | Túnel | 6 a 6 sobre 4 | En medio de ET y DR |
| ISATAP | Túnel | 6 a 6 sobre 4 | En medio de ET y DR |
| DSTM | Túnel | 4 a 4 sobre 6 | En medio de ET y DR |

Fuente: Managing the coexisting network of IPv6 and IPv4 under various transition mechanisms.

Figura 20. **Conectividad mecanismos de transición**

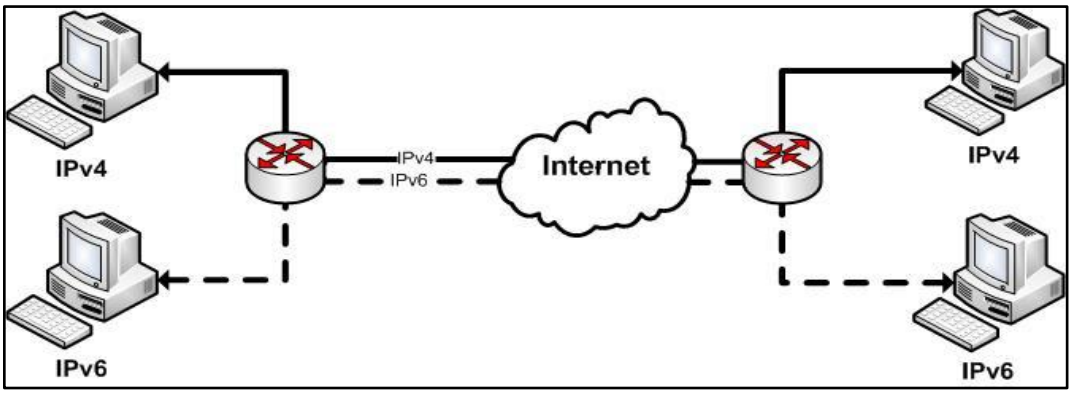



Fuente: elaboración propia, con base a Microsoft Visio.

## 3.2. Doble pila

Especificado en el RFC 2893, bajo este mecanismo, todos los nodos clientes y servidores tienen soporte tanto para IPv4 e IPv6. Esta es la solución más general y práctica, por la facilidad comparada con otros mecanismos de transición. El tráfico no será doble al tener soporte para ambos protocolos de internet, cualquier nueva conexión a través de IPv6 es típicamente una conexión menos sobre IPv4. En la figura 21 ilustra cómo las redes de doble pila pueden soportar servicios y aplicaciones IPv4 e IPv6 durante el período de transición.

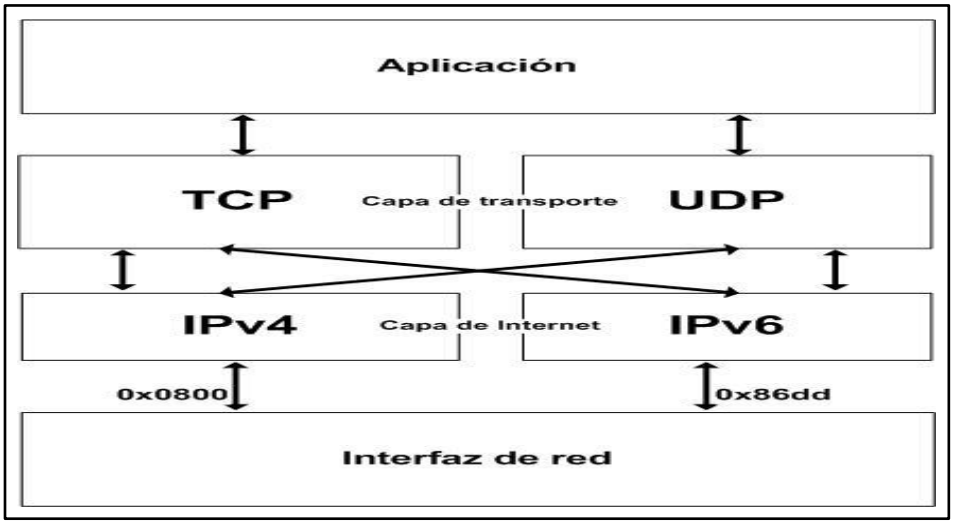
Figura 21. **Red de doble pila**




Fuente: elaboración propia, con base a Microsoft Visio.

El mecanismo de transición de doble pila cubre los escenarios 1 y 2 descritos al inicio del capítulo, en donde un sistema IPv4 se conecta a un sistema IPv4 a través de una red IPv4 y un sistema IPv6 se conecta a un sistema IPv6 a través de una red IPv6. La organización de los protocolos de internet de doble pila se detalla en la figura 22.

Figura 22. **Arquitectura doble pila**




Fuente: elaboración propia, con base a Microsoft Visio.

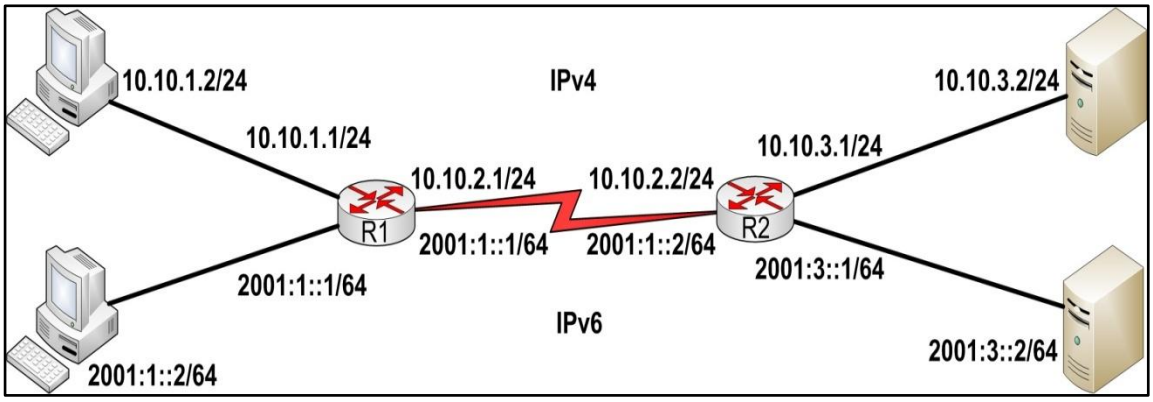
Al implementar la doble pila en un sistema final en el sistema operativo, se elige entre habilitar el protocolo IPv6 en la capa de internet o utilizar únicamente el protocolo IPv4 predeterminado como se muestra en la figura 22. Para ejecutar IPv4 e IPv6 en la capa de transporte se trabajan con los mismos protocolos, el TCP y UDP, además, se pueden ejecutar las mismas aplicaciones.

El mecanismo de transición de doble pila identifica los paquetes IPv4 e IPv6 en la comunicación desde la capa de interfaz de red hacia la capa de internet y viceversa por medio de la cabecera de los protocolos a nivel de enlace. Para ejemplificar la identificación de los paquetes en el campo protocolo de la cabecera *Ethernet* el valor para un paquete IPv4 e IPv6 es 0x0800 y 0x86dd respectivamente como se observa en la figura 22.

### 3.2.1. Implementación

En el siguiente diagrama de red (vea figura 23) se realiza la implementación, es sencilla de implementar, solo quiere de habilitar los dos protocolos de internet en las interfaces correspondientes y un par de comandos extras que se resaltan en las tablas VI y VII.

Figura 23. **Diagrama de red implementación doble pila**




Fuente: elaboración propia, con base a Microsoft Visio.

Tabla VI. **Comandos implementación doble pila *Router* 1**

| Paso | Comando o acción | Propósito |
|---|---|---|
| **1** | R1> enable | Modo privilegiado |
| **2** | R1# configure terminal | Configurar terminal |
| **3** | R1 (config)# **ipv6 unicast-routing** | Habilita la transmisión de paquetes IPv6 en las interfaces. |

Continuación de la tabla VI.

| | | |
|---|---|---|
| **4** | R1 (config) # interface FastEthernet 0/0<br>R1 (config-if) # ip address 10.10.1.1 255.255.255.0<br>R1 (config-if) # **ipv6 rip CCNA enable**<br>R1 (config-if) # no shutdown<br>R1 (config-if) # exit | Configurar interfaz de red para IPv4. |
| **5** | R1 (config) # interface FastEthernet 0/1<br>R1 (config-if) # **no ip address**<br>R1 (config-if) # **ipv6 address 2001:1::1/64**<br>R1 (config-if) # **ipv6 rip CCNA enable**<br>R1 (config-if) # no shutdown<br>R1 (config-if) # exit | Configurar interfaz de red para IPv6. |
| **6** | R1 (config) # interface Serial 1/0<br>R1 (config-if) # **ip address 10.10.2.1 255.255.255.0**<br>R1 (config-if) # **ipv6 address 2001:2::1/64**<br>R1 (config-if) # **ipv6 rip CCNA enable**<br>R1 (config-if) # clock rate 64000<br>R1 (config-if) # no shutdown<br>R1 (config-if) # exit | Configurar interfaz de red con IPv4 e IPv6. |
| **7** | R1 (config) # router rip<br>R1 (config-router) # version 2<br>R1 (config-router) # network 10.0.0.0<br>R1 (config-router) # **no auto-summary**<br>R1 (config-router) # exit | Habilitar RIP para IPv4. |

Fuente: elaboración propia.

Tabla VII. **Comandos implementación doble pila *Router* 2**

| Paso | Comando o acción | Propósito |
|---|---|---|
| **1** | R2> enable | Modo privilegiado |
| **2** | R2# configure terminal | Configurar terminal |
| **3** | R2 (config)# **ipv6 unicast-routing** | Habilita la transmisión de paquetes IPv6 en las interfaces. |
| **4** | R2 (config) # interface FastEthernet 0/0<br>R2 (config-if) # ip address 10.10.3.1 255.255.255.0<br>R2 (config-if) # **ipv6 rip CCNA enable**<br>R2 (config-if) # no shutdown<br>R2 (config-if) # exit | Configurar interfaz de red para IPv4. |
| **5** | R2 (config) # interface FastEthernet 0/1<br>R2 (config-if) # **no ip address**<br>R2 (config-if) # **ipv6 address 2001:3::1/64**<br>R2 (config-if) # **ipv6 rip CCNA enable**<br>R2 (config-if) # no shutdown<br>R2 (config-if) # exit | Configurar interfaz de red para IPv6. |
| **6** | R2 (config) # interface Serial 1/0<br>R2 (config-if) # **ip address 10.10.2.2 255.255.255.0**<br>R2 (config-if) # **ipv6 address 2001:2::2/64**<br>R2 (config-if) # **ipv6 rip CCNA enable**<br>R2 (config-if) # no shutdown<br>R2 (config-if) # exit | Configurar interfaz de red con IPv4 e IPv6. |
| **7** | R2 (config) # router rip<br>R2 (config-router) # version 2<br>R2 (config-router) # network 10.0.0.0<br>R2 (config-router) # **no auto-summary**<br>R2 (config-router) # exit | Habilitar RIP para IPv4. |

Fuente: elaboración propia.

Lo más importante de la configuración es que en las interfaces de red se debe ejecutar el comando "*ipv6 rip CCNA enable*", dicho comando habilita el RIPng (*RIP next generation*) de manera global. Otro comando importante es el "*no auto-summary*" para que no realice el resumen de rutas por clase y no se agreguen a la tabla de enrutamiento.

### 3.2.2. Ventajas

El mecanismo de transición de doble pila se caracteriza por ser el más práctico de implementar, así como se especifico en la implementación, a continuación se listan las ventajas más importantes:

- Facilidad al desplegar y altamente soportada en los sistemas finales y dispositivos de red.

- Los *hosts* con doble pila sobre redes solo con conectividad a IPv6 pueden alcanzar a nodos IPv4 en el internet.

- Las aplicaciones tradicionales IPv4 pueden estar corriendo sobre redes IPv6.

### 3.2.3. Desventajas

La desventaja más significativa de doble pila es la sobrecarga que genera en la red por el manejo de los dos protocolos de internet, a continuación se listan las desventajas más importantes:

- La topología de red requiere dos tablas de encaminamiento y dos procesos de encaminamiento.

- Incrementa la complejidad en el desarrollo de nuevas aplicaciones.

- El manejo de respuestas múltiples se complica al manejar la información recolectada desde diferentes fuentes y con distinto protocolo de internet.

## 3.3. Traducción

Las técnicas de traducción implican realizar conversión entre paquetes IPv4 e IPv6, no son recomendables que se usen ampliamente, debido al alto consumo de recursos de la red, afectando así considerablemente el *performance* de la red y afectando así el flujo de paquetes. Además, no permite que la infraestructura de red aproveche las capacidades específicas de cualquiera protocolo de comunicación.

De los escenarios listados al inicio del capítulo las técnicas de traducción cubren los escenarios 5 y 6, siendo predominante el escenario 6 dado que los sistemas IPv6 son una minoría y necesitan conectarse a la predominante red IPv4.

Existen varios mecanismos de traducción desarrollados que permiten una comunicación cruzada entre protocolos, es decir, comunicación entre *host* con diferente protocolo de internet. La diferencia entre los mecanismos de traducción, es que la traducción se lleva a cabo en capas distintas del modelo de referencia TCP/IP (vea figura 24).

Figura 24. **Modelo TCP/IP**


Fuente: elaboración propia, con base a Microsoft Visio.

Los diferentes mecanismos de traducción que se describen a continuación también se han propuesto en RFC por parte de IETF y se clasifican de la siguiente manera:

- Capa de internet
  - RFC 2766 - NAT-PT
  - RFC 2767 - *Bump in the Stack* (BIS)

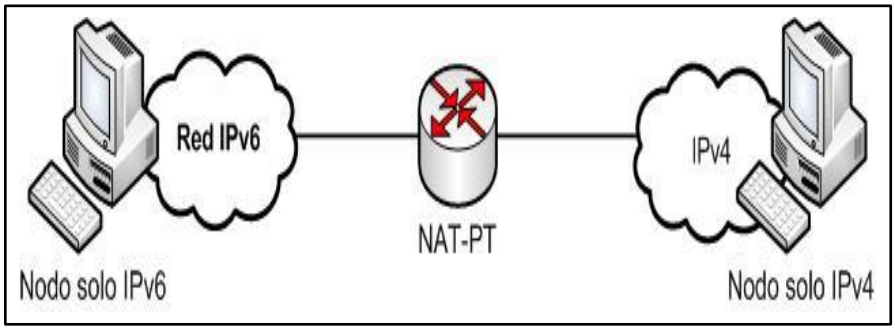
- Capa de transporte
  - RFC 3142 - *Transport Relay Translator* (TRT)

- Capa de aplicación
  - RFC 3338 - *Bump in the API* (BIA)

### 3.3.1. NAT-PT

NAT-PT (*Network Address Translation – Protocol Translation*) se especifica en el RFC 2766 y facilita a los clientes con la transición de IPv4 a IPv6. La figura 25 ilustra cómo NAT-PT se ejecuta en un *router* entre una red IPv6 y una red IPv4 para conectar un nodo sólo IPv6 con un nodo sólo IPv4.

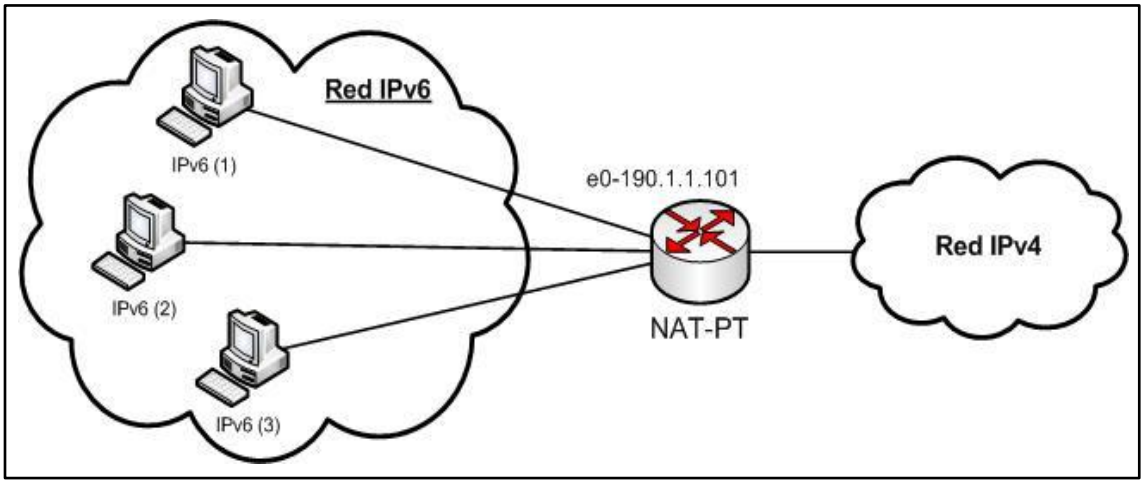
Figura 25. **Operación básica NAT-PT**




Fuente: elaboración propia, con base a Microsoft Visio.

Al igual que con NAT tradicional para IPv4, hay dos variantes en NAT-PT las cuales son: NAT-PT básica y NAPT-PT. Con NAT-PT básica, un bloque de direcciones IPv4 se reservan para la traducción de direcciones a *hosts* IPv6, y con NAPT-PT (*Network Address Port Translation – Protocol Translation*) se extiende la idea de la traducción un paso más allá, contempla también la traducción de los identificadores de transporte, por ejemplo, TCP y UDP números de puerto, identificadores de petición ICMP. NAPT-PT permite que un conjunto de *hosts* IPv6 compartan una única dirección IPv4. NAPT-PT puede ser combinado con NAT-PT básico, para que un grupo de direcciones externas se utilicen junto con la traducción del puerto (vea figura 26).

Figura 26. **NAT-PT traducción de puertos**



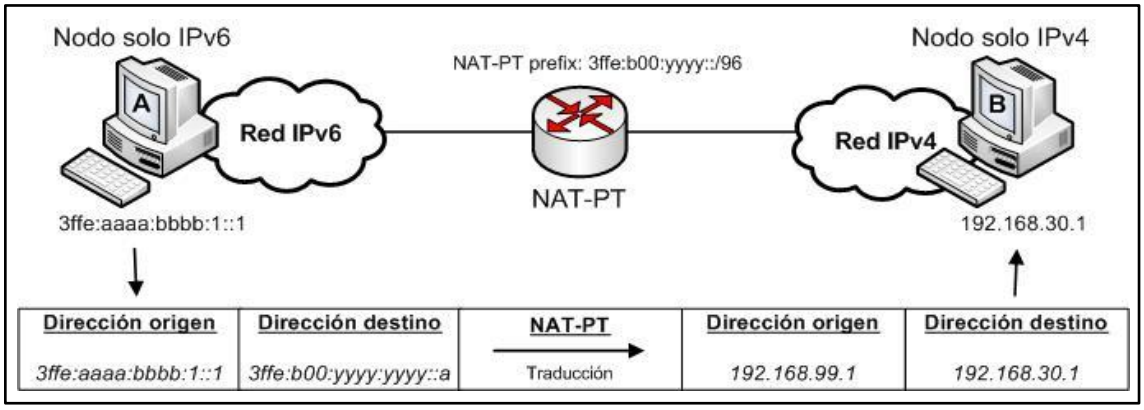

Fuente: elaboración propia, con base a Microsoft Visio.

NAT-PT es una solución de interoperabilidad que no requiere ninguna modificación o software adicionales, tales como la pila doble, para ser instalado en cualquier máquina del usuario final en cualquier red IPv4 o IPv6. NAT-PT realiza las funciones de interoperabilidad requeridas dentro de una red, este técnica de traducción es la más fácil de manejar y rápido de implementar.

#### 3.3.1.1. NAT-PT estático

NAT-PT estático usa las reglas estáticas de traducción de un mapa de direcciones IPv6 a otro de direcciones IPv4. Los *hosts* de la red IPv6 se comunican con los nodos de la red IPv4 utilizando una mapeo IPv6 de las direcciones IPv4 configuradas en el *router* NAT-PT. La figura 27 se ilustra la comunicación entre un *host* IPv6 y un *host* IPv4 mediante el uso de NAT-PT estático.

Figura 27. **Operación NAT-PT estático**



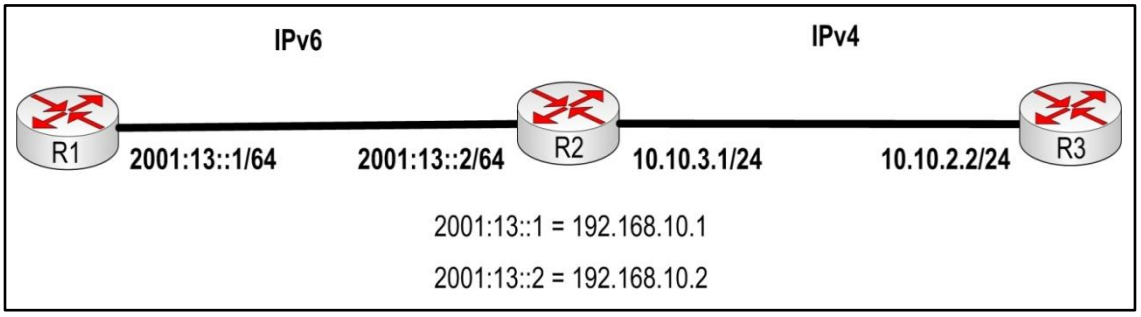

Fuente: *Implementing NAT protocol translation*.

NAT-PT también puede ser configurado para que coincida con una dirección de origen IPv4 y traducir el paquete a una dirección de destino IPv6 para permitir una comunicación de un nodo IPv4 con un nodo IPv6.

En la configuración básica de NAT-PT estático se debe especificar un prefijo (*prefix*) de IPv6 con una longitud de 96 bits. El prefijo se utiliza para que coincida con un prefijo de destino de un paquete IPv6. Si la comparación coincide NAT-PT utilizará las reglas de asignación de direcciones configuradas para traducir los paquetes IPv6 a paquetes IPv4 o viceversa.

En las tablas VIII, IX y X se describen las configuraciones necesarias para la implementación de NAT-PT estático de los *routers* R3, R1 y R2 respectivamente del diagrama de red de la figura 28, en donde se realiza una configuración simple de NAT-PT con fines ilustrativos. El *router* llamado R2 es el *router* NAT-PT en donde se realizan las traducciones.

Figura 28. **Diagrama de red implementación NAT-PT estático**




Fuente: elaboración propia, con base a Microsoft Visio.

Tabla VIII. **Comandos implementación NAT-PT estático *Router* 3**

| Paso | Comando o acción | Propósito |
|---|---|---|
| **1** | R3> enable | Modo privilegiado |
| **2** | R3# configure terminal | Configurar terminal |
| **3** | R3 (config) # interface FastEthernet 0/0<br>R3 (config-if) # ip address 192.168.10.2 255.255.255.0<br>R3 (config-if) # no shutdown<br>R3 (config-if) # exit | Configurar interfaz de red para IPv4. |
| **4** | R3 (config) # **ip route 0.0.0.0 0.0.0.0 192.168.10.1** | Configurar ruta estática por defecto. |

Fuente: elaboración propia.

Tabla IX. **Comandos implementación NAT-PT estático *Router* 1**

| Paso | Comando o acción | Propósito |
|---|---|---|
| **1** | R1> enable | Modo privilegiado |
| **2** | R1# configure terminal | Configurar terminal |
| **3** | R1 (config)# **ipv6 unicast-routing** | Habilita la transmisión de paquetes IPv6 en las interfaces. |
| **4** | R1 (config) # interface FastEthernet 0/0<br>R1 (config-if) # **no ip address**<br>R1 (config-if) # **ipv6 address 2001:13::1/64**<br>R1 (config-if) # no shutdown<br>R1 (config-if) # exit | Configurar interfaz de red para IPv6. |
| **5** | R1 (config) # **ipv6 route ::/0 2001:13::2** | Configurar ruta estática por defecto. |

Fuente: elaboración propia.

Tabla X. **Comandos implementación NAT-PT estático *Router* 2**

| Paso | Comando o acción | Propósito |
|---|---|---|
| **1** | R2> enable | Modo privilegiado |
| **2** | R2# configure terminal | Configurar terminal |
| **3** | R2 (config)# **ipv6 unicast-routing** | Habilita la transmisión de paquetes IPv6 en las interfaces. |

Continuación de la tabla X.

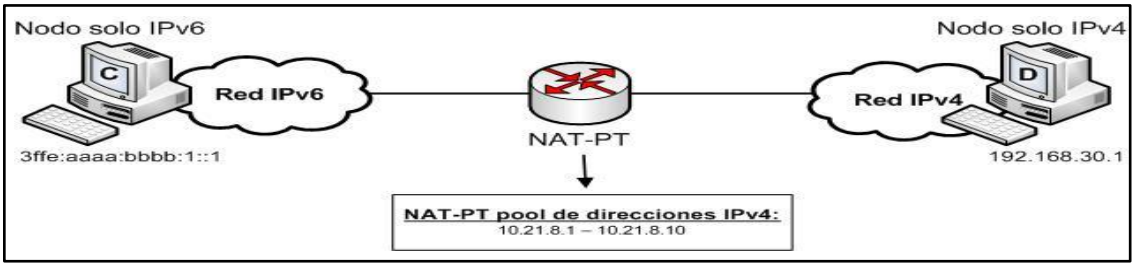
| | | |
|---|---|---|
| **4** | R2 (config) # interface FastEthernet 0/0<br>R2 (config-if) # **no ip address**<br>R2 (config-if) # **ipv6 address 2001:13::2/64**<br>R2 (config-if) # **ipv6 nat**<br>R2 (config-if) # no shutdown<br>R2 (config-if) # exit | Configurar interfaz de red para IPv6. |
| **5** | R2 (config) # interface FastEthernet 0/1<br>R2 (config-if) # **ip address 192.168.10.1 255.255.255.0**<br>R2 (config-if) # **ipv6 nat**<br>R2 (config-if) # no shutdown<br>R2 (config-if) # exit | Configurar interfaz de red para IPv4. |
| **6** | R2 (config) # **ipv6 nat v4v6 source 192.168.10.2 2001:23::2**<br>R2 (config) # **ipv6 nat v6v4 source 2001:13::1 192.168.13.1**<br>R2 (config) # **ipv6 nat prefix 2001:23::/96** | Definición las direcciones para la traducción estática. |

Fuente: elaboración propia.

#### 3.3.1.2. NAT-PT dinámico

NAT-PT dinámico permite múltiples asignaciones NAT-PT mediante la asignación de un conjunto de direcciones. En el inicio de una sesión de NAT-PT una dirección temporal se asigna dinámicamente a partir de un *pool* de direcciones, el total de direcciones en el *pool* determina el total de sesiones simultáneas, el dispositivo NAT-PT registra cada mapeo de direcciones en una tabla de estado dinámico. En la figura 29 se ilustra cómo opera el NAT-PT dinámico, en donde se define el *pool* de direcciones IPv4 10.21.8.1 a 10.21.8.10 para las direcciones IPv6.

Figura 29. **Operación NAT-PT dinámico**

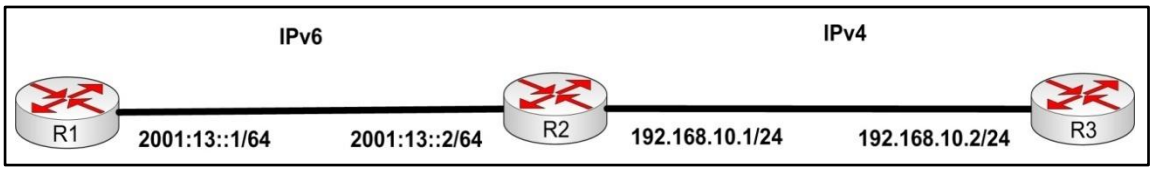



Fuente: *Implementing NAT protocol translation.*

Cuando un paquete IPv6 es identificado, NAT-PT utiliza las reglas de asignación configuradas y asigna una dirección IPv4 temporal del *pool* de direcciones IPv4. La configuración de la traducción por medio de NAT-PT dinámico requiere de al menos una asignación estática para el servidor DNS IPv4.

En la tabla XI se describen las configuraciones necesarias para la implementación de NAT-PT dinámico del *router* R2 del diagrama de red (vea figura 30), quien realiza las traducciones. Las configuraciones para los *routers* R3 y R1 son las mismas que se definieron en la tabla VII y IX respectivamente, lo que difiere es la configuración del *router* R2 por ser NAT-PT dinámico.

Figura 30. **Diagrama de red implementación NAT-PT dinámico**




Fuente: elaboración propia, con base a Microsoft Visio.

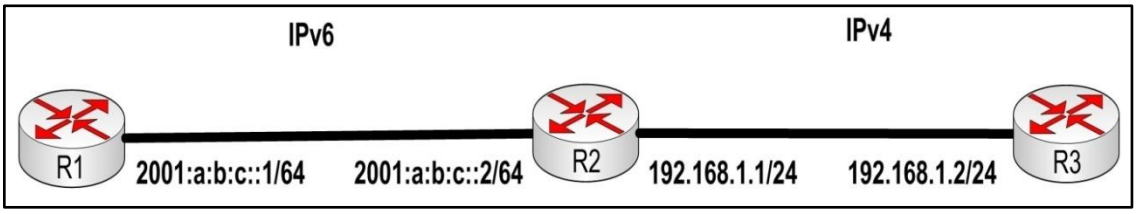
Tabla XI. **Comandos implementación NAT-PT dinámico *Router* 2**

| Paso | Comando o acción | Propósito |
|---|---|---|
| **1** | R2> enable | Modo privilegiado |
| **2** | R2# configure terminal | Configurar terminal |
| **3** | R2 (config)# **ipv6 unicast-routing** | Habilita la transmisión de paquetes IPv6 en las interfaces. |
| **4** | R2 (config) # interface FastEthernet 0/0<br>R2 (config-if) # **no ip address**<br>R2 (config-if) # **ipv6 address 2001:13::2/64**<br>R2 (config-if) # **ipv6 nat**<br>R2 (config-if) # no shutdown<br>R2 (config-if) # exit | Configurar interfaz de red para IPv6. |
| **5** | R2 (config) # interface FastEthernet 0/1<br>R2 (config-if) # **ip address 192.168.10.1 255.255.255.0**<br>R2 (config-if) # **ipv6 nat**<br>R2 (config-if) # no shutdown<br>R2 (config-if) # exit | Configurar interfaz de red para IPv4. |
| **6** | R2 (config) # **access-list 10 permit 192.168.10.0 0.0.0.255**<br>R2 (config) # **ipv6 nat v4v6 source list 10 pool ipsr**<br>R2 (config) # **ipv6 nat v4v6 pool ipsr 2001:23::1 2001:23::FFFF prefix-length 96**<br>R2 (config) # **ipv6 nat v6v4 source 2001:13::1 10.0.0.1**<br>R2 (config) # **ipv6 nat prefix 2001:23::/96** | Definición las direcciones para la traducción dinámica. |

Fuente: elaboración propia.

Para ejemplificar a NPAT-PT en las tablas XII, XIII y XIV se describen las configuraciones necesarias para la implementación en los *routers* R3, R1 y R2 respectivamente del diagrama de red (vea figura 31), el *router* R2 realiza las traducciones. NPAT-PT se extiende de NAT-PT desde traducciones de uno a uno a traducciones de muchos a uno al asociar el puerto de origen en cada flujo.

Figura 31. **Diagrama de red implementación NPAT-PT**




Fuente: elaboración propia, con base a Microsoft Visio.

Tabla XII. **Comandos implementación NPAT-PT *Router* 3**

| Paso | Comando o acción | Propósito |
|---|---|---|
| **1** | R3> enable | Modo privilegiado |
| **2** | R3# configure terminal | Configurar terminal |
| **3** | R3 (config) # interface FastEthernet 0/0<br>R3 (config-if) # ip address 192.168.1.2 255.255.255.0<br>R3 (config-if) # no shutdown<br>R3 (config-if) # exit | Configurar interfaz de red para IPv4. |

Continuación de la tabla XII.

| | | |
|---|---|---|
| **4** | R3 (config) # **ip route 0.0.0.0 0.0.0.0 192.168.1.1** | Configurar ruta estática por defecto. |

Fuente: elaboración propia.

Tabla XIII. **Comandos implementación NPAT-PT *Router* 1**

| **Paso** | **Comando o acción** | **Propósito** |
|---|---|---|
| **1** | R1> enable | Modo privilegiado |
| **2** | R1# configure terminal | Configurar terminal |
| **3** | R1 (config)# **ipv6 unicast-routing** | Habilita la transmisión de paquetes IPv6 en las interfaces. |
| **4** | R1 (config) # interface FastEthernet 0/0<br>R1 (config-if) # **no ip address**<br>R1 (config-if) # **ipv6 address 2001:a:b:c::1/64**<br>R1 (config-if) # no shutdown<br>R1 (config-if) # exit | Configurar interfaz de red para IPv6. |
| **5** | R1 (config) # **ipv6 route ::/0 2001:a:b:c::2** | Configurar ruta estática por defecto. |

Fuente: elaboración propia.

Tabla XIV. **Comandos implementación NPAT-PT *Router* 2**

| Paso | Comando o acción | Propósito |
|---|---|---|
| **1** | R2> enable | Modo privilegiado |
| **2** | R2# configure terminal | Configurar terminal |
| **3** | R2 (config)# **ipv6 unicast-routing** | Habilita la transmisión de paquetes IPv6 en las interfaces. |
| **4** | R2 (config) # interface FastEthernet 0/0<br>R2 (config-if) # **no ip address**<br>R2 (config-if) # **ipv6 address 2001:a:b:c::2/64**<br>R2 (config-if) # **ipv6 nat**<br>R2 (config-if) # no shutdown<br>R2 (config-if) # exit | Configurar interfaz de red para IPv6. |
| **5** | R2 (config) # interface FastEthernet 0/1<br>R2 (config-if) # **ip address 192.168.1.1 255.255.255.0**<br>R2 (config-if) # **ipv6 nat**<br>R2 (config-if) # no shutdown<br>R2 (config-if) # exit | Configurar interfaz de red para IPv4. |
| **6** | R2 (config) # **ipv6 nat v4v6 source 192.168.1.2 2001::10**<br>R2 (config) # **ipv6 nat v6v4 source list list_to-ipv4 interface FastEthernet0/1 overload**<br>R2 (config) # **ipv6 nat prefix 2001::/96** | Configuración de la traducción de IPv6 por puertos. |
| **7** | R2 (config) # **ipv6 access-list list_to-ipv4**<br>R2 (config) # **permit ipv6 2001:A:B:C::/64 any** | Permitir el tráfico de la red IPv6. |

Fuente: elaboración propia.

#### 3.3.1.3. Ventajas

NAT-PT es el mecanismo de traducción de más fácil implementación, a continuación se listan las ventajas más importantes de NAT-PT en general:

- No requiere de modificaciones en los nodos finales la única modificación se lleva a cabo en los *routers* dentro de infraestructura de red.

- NAT-PT dinámica tiene ventaja sobre los otros tipos, dado que con una configuración sencilla en los *routers* se realiza la transición de IPv6 a IPv4 y viceversa, sin demasiada administración.

#### 3.3.1.4. Desventajas

Todas las limitaciones de NAT tradicional están asociadas a NAT-PT, a continuación se detallan las desventajas más importantes y algunas asociadas únicamente con NAT-PT:

- Todas las peticiones y respuestas se deben realizar bajo el mismo *router* NAT-PT.

- La traducción no es sencilla dado la cabecera de IPv4 han cambiado significativamente con respecto a la cabecera IPv6 y debido a ello en la traducción se reduce el *performance* de la red.

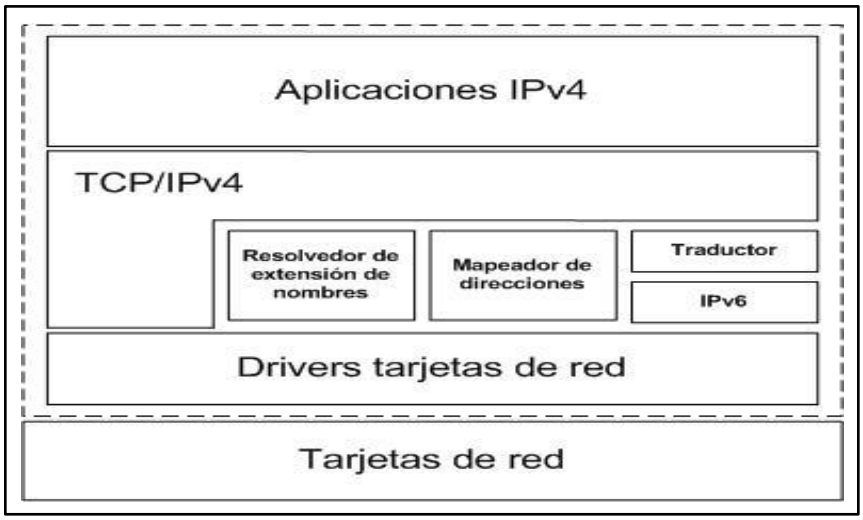
- La seguridad en la capa de red en una comunicación de punto a punto no es posible.

### 3.3.2. Otros mecanismos de traducción

En la actualidad la mayoría de aplicaciones soportan IPv4 y existen pocas aplicaciones con soporte para IPv6, el objetivo es que el número de aplicaciones IPv6 sea igual o mayor que las aplicaciones IPv4, mientras tanto, se necesita de traductores. Otros mecanismos de traducción importantes son: *Bump in the Stack* (BIS), *Bump in the API* (BIA) y *Transport Relay Translator* (TRT), estos permiten a los *hosts* convertirse en traductores autónomos, es decir, no necesitan de un traductor externo como en el caso de NAT-PT.

El mecanismo de traducción BIS agrega tres módulos los cuales son: resolvedor de extensión de nombres, mapeador de direcciones y traductor (vea figura 32), que permiten al *host* comunicarse con otros utilizando aplicaciones IPv4.

Figura 32. **Componentes de BIS**

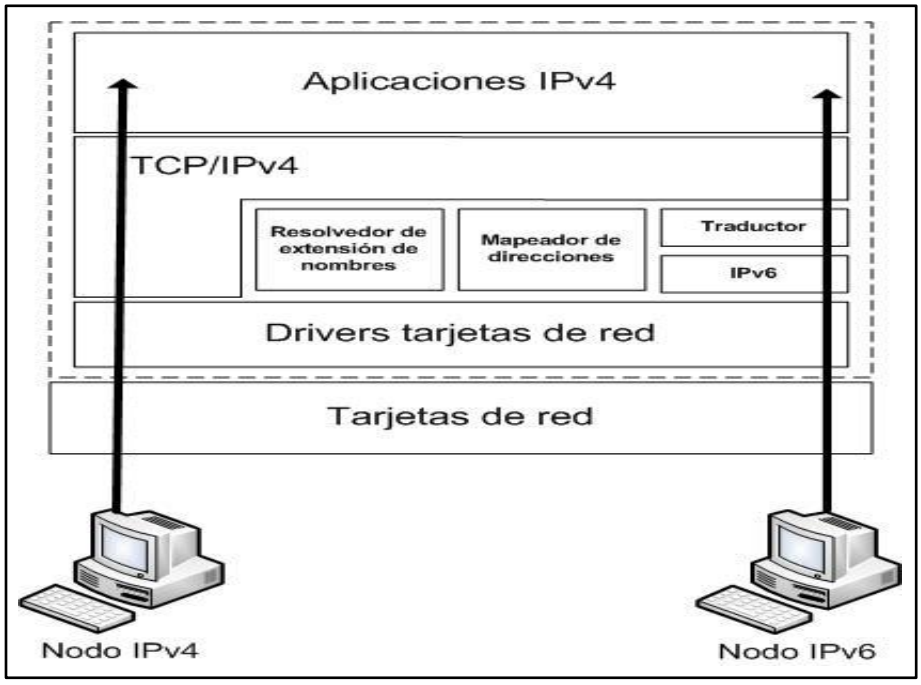



Fuente: Dual stack hosts using the "bump in the stack" technique (BIS), en: http://www.ietf.org/rfc/rfc2767.txt. Consulta: 5 de julio de 2011.

El resolvedor de extensión de nombres se encarga de responder las solicitudes de nombres de aplicación IPv4. La aplicación IPv4 hace una solicitud de tipo A para obtener la dirección IPv4 del *host* y tipo AAAA para obtener la dirección IPv6 del *host* para realizar la comunicación. Este modulo se encarga de crear las solicitudes correspondientes y enviarlas al servidor DNS.

Si el servidor responde a la requisición A, entonces el proceso de comunicación se realiza normalmente, es decir, no hay necesidad de realizar una traducción de paquetes. En caso contrario si el servidor DNS responde a la solicitud AAAA, entonces se realizara el mecanismo de traducción (vea figura 33).

Figura 33. **Comunicación BIS**

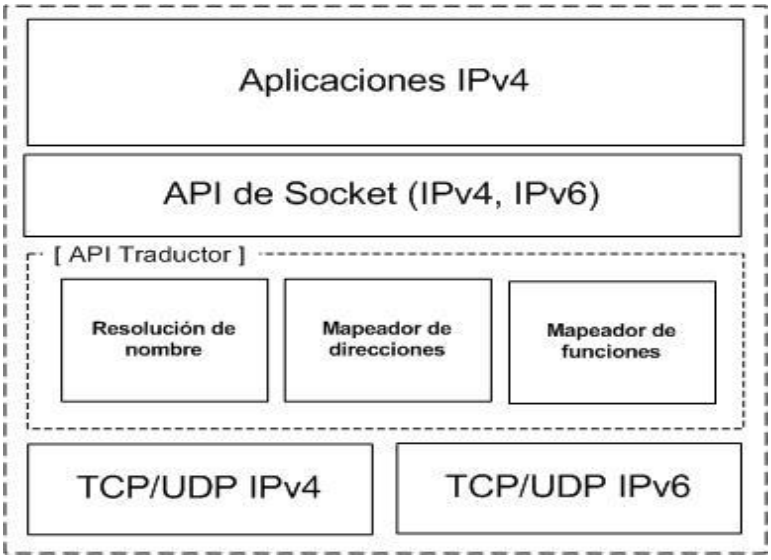



Fuente: elaboración propia, con base a Microsoft Visio.

El mapeador de direcciones consiste en un grupo de direcciones IPv4 privadas o públicas y mantiene una tabla de pares de direcciones IPv4 e IPv6. Cuando el módulo de resolvedor de extensión de nombres o traductor requiere una dirección IPv4, le notifican a este componente para que asocie una dirección IPv4 del grupo a la dirección IPv6. El traductor se encarga de efectuar la traducción entre direcciones IPv4 e IPv6, utilizando el mecanismo SIIT (*Stateless IP/ICMP Translation Algorithm*) definido en el RFC 2765.

Por otra parte BIA es muy semejante con BIS, la principal diferencia es que BIA no realiza ninguna traducción de cabeceras, sino que realiza una traducción entre el API IPv4 y el API IPv6 en la capa de aplicación. El API de BIA consta de tres componentes: resolución de nombres, mapeador de direcciones y *m*apeador de funciones (vea figura 34).

Figura 34. **Componentes BIA**



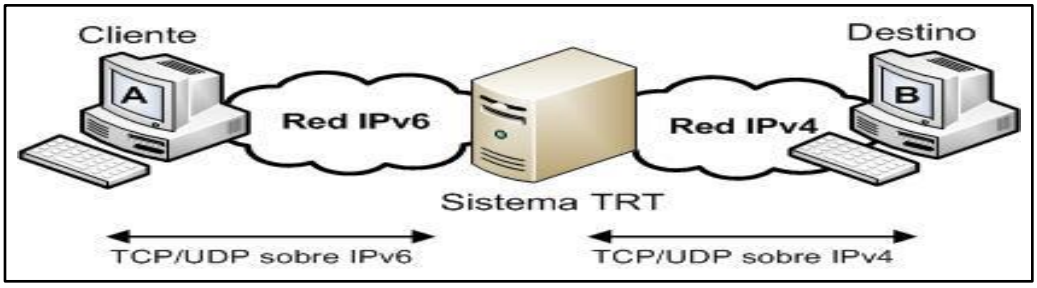

Fuente: Dual stack hosts using "bump in the API" (BIA), en: http://www.ietf.org/rfc/rfc3338.txt. Consulta: 5 de julio de 2011.

Cuando se dispone del código fuente de las aplicaciones IPv4 no es recomendable utilizar BIA. Al igual que BIS, sólo hay apoyo a la comunicación *unicast*, el RFC 3338 no da una razón clara de por qué *multicast* no es compatible.

El resolvedor de nombres de BIA cumple con la misma función descrita para el módulo de resolvedor de extensión de nombres de BIS, también así el mapeador de direcciones. El mapeador de funciones consiste en traducir las funciones del API de socket IPv4 a una equivalente en el API de socket IPv6 y viceversa.

Por último el mecanismo de traducción TRT funcionan en la capa de transporte del modelo TCP/IP (vea figura 24) y realiza la traducción en paquetes TCP, UDP, entre otros. El sistema TRT se localizada en un *host* o *router*. En el funcionamiento TRT es similar a NAT-PT, con la diferencia que la traducción se realiza en la capa de transporte. El *host* IPv6 inicia la comunicación y necesita de una dirección IPv6 de destino que solicita al sistema TRT. Todo el tráfico se envía través del sistema TRT, que funciona como un servidor de retransmisión de tráfico (vea figura 35).

Figura 35. **Comunicación TRT**



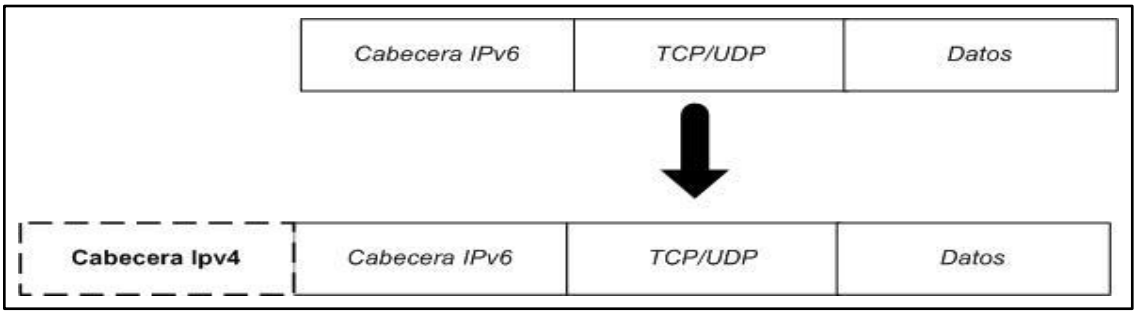

Fuente: elaboración propia, con base a Microsoft Visio.

## 3.4. Túneles

Los túneles son otro de los grupos en que se dividen los mecanismos de transición definidos por la IETF. Los túneles se han desarrollado para apoyar a la IPv6 sobre IPv4, así como la IPv4 sobre IPv6. Esta tecnología es clasificada como túnel configurado y túnel automático. Los túneles configurados se encuentran predefinidos, mientras que los túneles automáticos se crean sobre la marcha.

En general, los túneles transportan los paquetes IPv6 a través de una red IPv4 y esto implica que a cada paquete IPv6 se encapsula con un encabezado IPv4 (vea figura 36).

Figura 36. **Túnel IPv6 sobre IPv4**

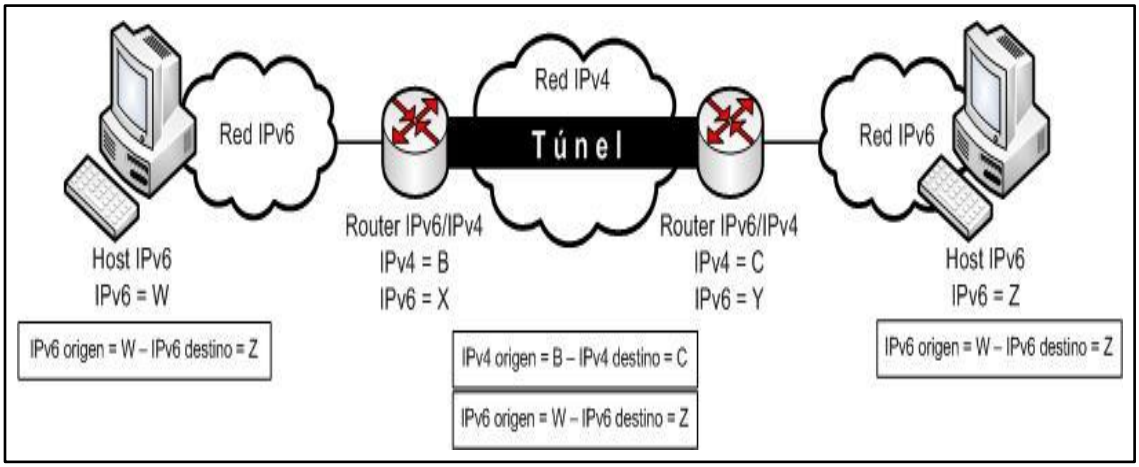



Fuente: elaboración propia, con base a Microsoft Visio.

Si bien el proceso de construcción de los túneles es el mismo para todos los tipos, hay una variedad de escenarios basados en la definición de los puntos finales del túnel, en donde se realiza el encapsulamiento. El mecanismo de transición de túneles cubre los escenarios 3 y 4 listados al principio del capítulo.

La configuración de túnel más común es la de *router* a *router* (vea figura 37), que es el método típico de los túneles configurados. En la siguiente figura se ilustra el proceso de comunicación en este tipo de túnel. Los *routers* se configuran de tal manera que el tráfico de un red hacia otra se envié por medio del túnel.

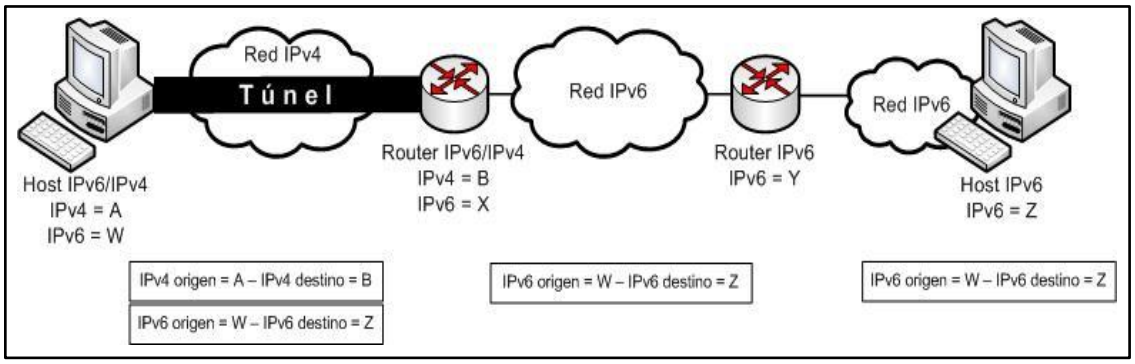
Figura 37. **Configuración túnel *router* a *router***




Fuente: *IPv4-to-IPv6 transition strategies.*

Otro tipo de configuración de túnel es el de *host* a *router* (vea figura 38) en donde un *host* es capaz de soportar los protocolos IPv4 e IPv6 simultáneamente, un túnel hacia un *router*, que a su vez desencapsula el paquete y la envía de forma nativa a través de la red IPv6, este flujo y las direcciones de cabecera del paquete se muestran en la siguiente figura.

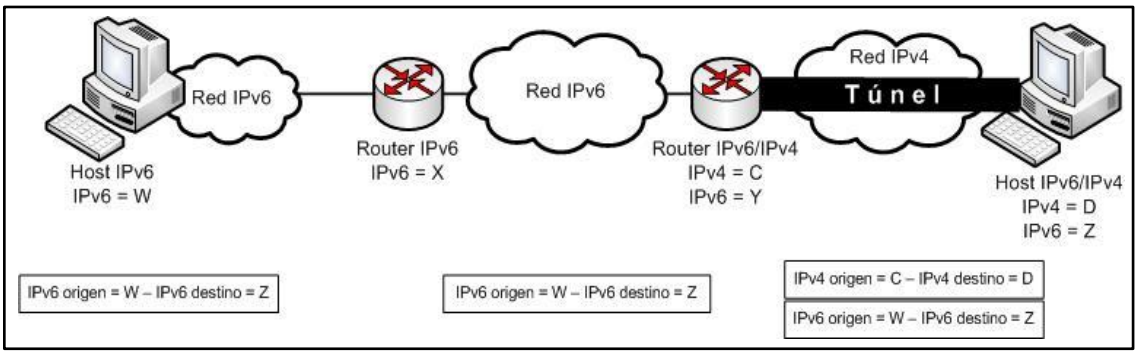
Figura 38. **Configuración túnel *host* a *router***




Fuente: *IPv4-to-IPv6 transition strategies*.

El tipo de configuración de túnel de *router* a *host* (vea figura 39), es también muy similar al túnel de *router* a *router*. El *host* IPv6 de origen a la izquierda envía el paquete IPv6 al *router* local y este transfiere el paquete al *router* más cercano de la red destino. El *router* que recibe el paquete está configurado para enviar los paquetes IPv6 sobre IPv4 al *host* destino por medio del túnel configurado, como se ve la siguiente figura.

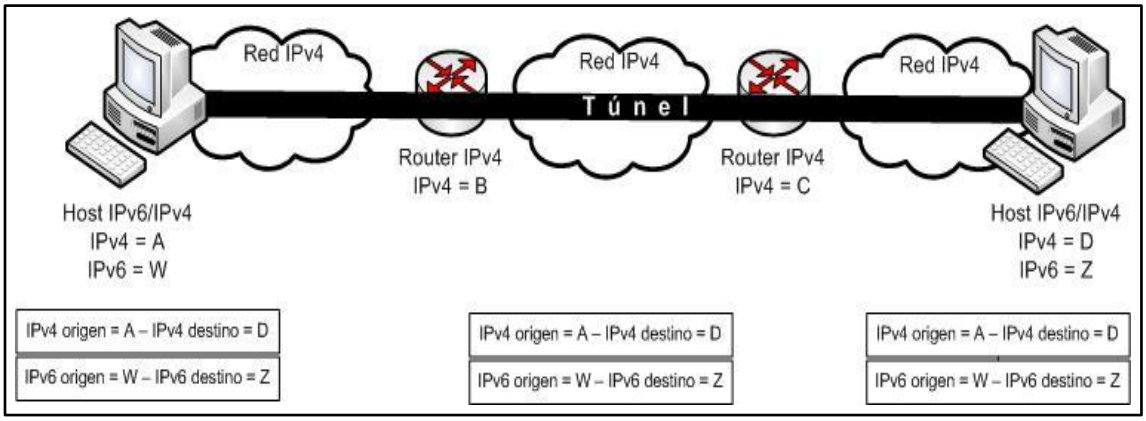
Figura 39. **Configuración túnel *router* a *host***




Fuente: *IPv4-to-IPv6 transition strategies*.

Por último la configuración de túnel de *host* a *host* el cual se extiende de extremo a extremo. Este tipo de escenario es de utilidad cuando la infraestructura de red no se ha actualizado para soportar IPv6, esta configuración permite que dos *hosts* con soporte a IPv6 e IPv4 se comuniquen a través de un túnel sobre en una red IPv4 (vea figura 40).

Figura 40. **Configuración túnel *host* a *host***

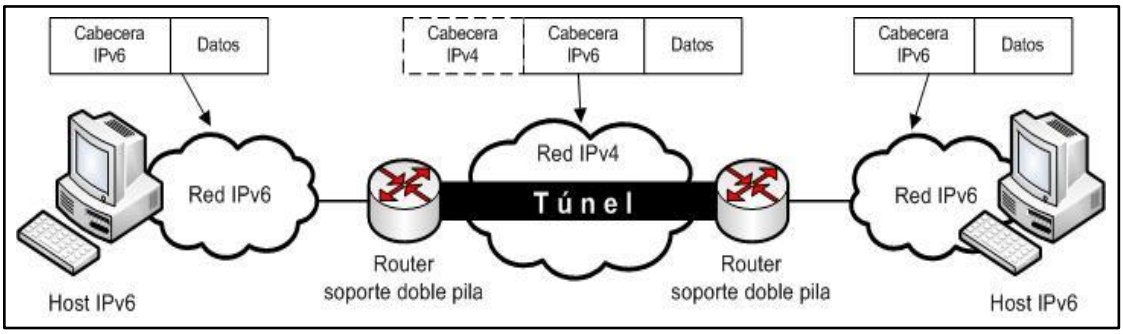



Fuente: *IPv4-to-IPv6 transition strategies*.

### 3.4.1. *6over4*

El mecanismo de túnel *6over4* (IPv6 sobre IPv4) encapsula los paquetes IPv6 adjuntando la cabecera IPv4 para que los paquetes IPv6 pueden ser transmitidos en la red IPv4 por medio del túnel, para la comunicación entre redes IPv6 aisladas (vea figura 41), donde los *routers* en los extremos del túnel deben tener soporte a doble pila.

Figura 41. **Operación *6over4***




Fuente: elaboración propia, con base a Microsoft Visio.

Un túnel de IPv6 sobre IPv4 se puede establecer entre los *host*, entre *hosts* y dispositivos, y/o entre los dispositivos. De acuerdo con la forma en que se adquirió la dirección IPv4 del destino del túnel, los túneles se dividen en: túnel configurado y túnel automático, a continuación se describen con mayor detalle dichos túneles:

- Si el destino del túnel no es el destino final de los paquetes IPv6, el dispositivo de destino al final del túnel (normalmente un *router*) desencapsula el paquete IPv6 y lo remite a su destino final. En este caso, la dirección IPv4 del destino del túnel no se puede adquirir a partir de la dirección de destino del paquete IPv6 y tiene que ser configurado manualmente, dicho túnel se llama túnel configurado.

- Si el destino del túnel es el destino final del paquete IPv6, una dirección IPv4 puede ser integrada de forma automática en la dirección IPv6 de manera que la dirección IPv4 del destino del túnel se pueda obtener en la dirección de destino del paquete IPv6, dicho túnel se llama túnel automático.

Los tipos de túnel IPv6 sobre IPv4 se distinguen de acuerdo a la forma en que se encapsula el paquete IPv6 y se dividen en los siguientes tipos:

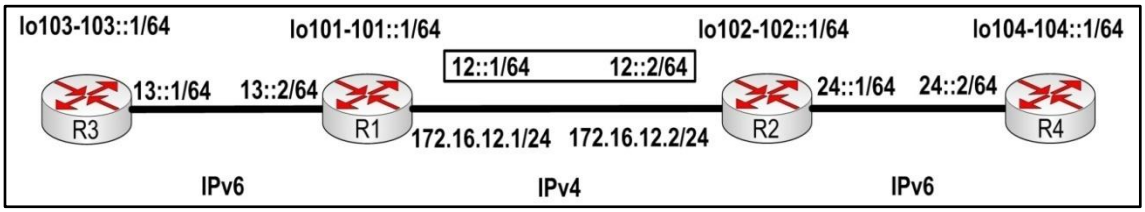
- Túnel manual IPv6
- Túnel IPv6 sobre IPv4 GRE (túnel GRE)
- Túnel automático compatible con IPv4 e IPv6
- Túnel *6to4*
- Túnel ISATAP

El túnel manual IPv6 y el túnel GRE son túneles configurados, mientras que el túnel automático, túnel 6to4, y el túnel ISATAP son túneles automáticos.

#### 3.4.1.1. Túnel manual IPv6

Este tipo de túnel es un enlace punto a punto que proporciona conexiones estables que requieran de una comunicación segura entre *routers* o entre un *router* y un *host* para el acceso a redes IPv6. En el diagrama de red (vea figura 42) se implementa el túnel, en las tablas XV, XVI, XVII y XVIII se describen las configuraciones para los *routers* R3, R4, R1 y R2 respectivamente.

Figura 42. **Diagrama de red implementación túnel manual IPv6**




Fuente: elaboración propia, con base a Microsoft Visio.

Tabla XV. **Comandos implementación túnel manual *Router* 3**

| Paso | Comando o acción | Propósito |
|---|---|---|
| **1** | R3> enable | Modo privilegiado |
| **2** | R3# configure terminal | Configurar terminal |
| **3** | R3 (config)# **ipv6 unicast-routing** | Habilita la transmisión de paquetes IPv6 en las interfaces. |
| **4** | R3 (config) # **interface Loopback103**<br>R3 (config-if) # **no ip address**<br>R3 (config-if) # **ipv6 address 103::1/64**<br>R3 (config-if) # **ipv6 enable**<br>R3 (config-if) # exit | Configurar interfaz *loopback* de red. |
| **5** | R3 (config) # interface FastEthernet 0/0<br>R3 (config-if) # **ipv6 address 13::1/64**<br>R3 (config-if) # **ipv6 rip CCNA enable**<br>R3 (config-if) # no shutdown<br>R3 (config-if) # exit | Configurar interfaz de red para IPv6. |

Fuente: elaboración propia.

Tabla XVI. **Comandos implementación túnel manual *Router* 4**

| Paso | Comando o acción | Propósito |
|---|---|---|
| **1** | R4> enable | Modo privilegiado |
| **2** | R4# configure terminal | Configurar terminal |
| **3** | R4 (config)# **ipv6 unicast-routing** | Habilita la transmisión de paquetes IPv6 en las interfaces. |

Continuación de la tabla XVI.

| | | |
|---|---|---|
| **4** | R4 (config) # **interface Loopback104**<br>R4 (config-if) # **no ip address**<br>R4 (config-if) # **ipv6 address 104::1/64**<br>R4 (config-if) # **ipv6 enable**<br>R4 (config-if) # exit | Configurar interfaz *loopback* de red. |
| **5** | R4 (config) # interface FastEthernet 0/0<br>R4 (config-if) # **ipv6 address 24::2/64**<br>R4 (config-if) # **ipv6 rip CCNA enable**<br>R4 (config-if) # no shutdown<br>R4 (config-if) # exit | Configurar interfaz de red para IPv6. |

Fuente: elaboración propia.

Tabla XVII. **Comandos implementación túnel manual *Router* 1**

| Paso | Comando o acción | Propósito |
|---|---|---|
| **1** | R1> enable | Modo privilegiado |
| **2** | R1# configure terminal | Configurar terminal |
| **3** | R1 (config)# **ipv6 unicast-routing** | Habilita la transmisión de paquetes IPv6 en las interfaces. |
| **4** | R1 (config) # **interface Loopback101**<br>R1 (config-if) # **ip address 10.1.1.1 255.255.255.0**<br>R1 (config-if) # **ipv6 enable**<br>R1 (config-if) # exit | Configurar interfaz *loopback* de red. |

Continuación de la tabla XVII.

| | | |
|---|---|---|
| **5** | R1 (config) # interface Tunnel12<br>R1 (config-if) # no ip address<br>R1 (config-if) # **ipv6 address 12::1/64**<br>R1 (config-if) # **ipv6 rip CCNA enable**<br>R1 (config-if) # **tunnel source Loopback101**<br>R1 (config-if) # **tunnel destination 10.2.2.2**<br>R1 (config-if) # **tunnel mode ipv6ip**<br>R1 (config-if) # exit | Configurar túnel manual en red IPv4. |
| **6** | R1 (config) # interface FastEthernet 0/0<br>R1 (config-if) # **ipv6 address 13::2/64**<br>R1 (config-if) # **ipv6 rip CCNA enable**<br>R1 (config-if) # no shutdown<br>R1 (config-if) # exit | Configurar interfaz de red para IPv6. |
| **7** | R1 (config) # interface FastEthernet 0/1<br>R1 (config-if) # **ipv6 address 172.16.12.1 255.255.255.0**<br>R1 (config-if) # no shutdown<br>R1 (config-if) # exit | Configurar interfaz de red para IPv4. |
| **8** | R1 (config) # router rip<br>R1 (config-router) # **version 2**<br>R1 (config-router) # **network 10.0.0.0**<br>R1 (config-router) # **network 172.16.0.0**<br>R1 (config-router) # **no auto-summary**<br>R1 (config-router) # exit | Configurar rip para la conectividad IPv4. |

Fuente: elaboración propia.

Tabla XVIII. **Comandos implementación túnel manual *Router* 2**

| Paso | Comando o acción | Propósito |
|---|---|---|
| **1** | R2> enable | Modo privilegiado |
| **2** | R2# configure terminal | Configurar terminal |
| **3** | R2 (config)# **ipv6 unicast-routing** | Habilita la transmisión de paquetes IPv6 en las interfaces. |
| **4** | R2 (config) # **interface Loopback102**<br>R2 (config-if) # **ip address 10.2.2.2 255.255.255.0**<br>R2 (config-if) # **ipv6 enable**<br>R2 (config-if) # exit | Configurar interfaz *loopback* de red. |
| **5** | R2 (config) # interface Tunnel12<br>R2 (config-if) # no ip address<br>R2 (config-if) # **ipv6 address 12::2/64**<br>R2 (config-if) # **ipv6 rip CCNA enable**<br>R2 (config-if) # **tunnel source Loopback102**<br>R2 (config-if) # **tunnel destination 10.1.1.1**<br>R2 (config-if) # **tunnel mode ipv6ip**<br>R2 (config-if) # exit | Configurar túnel manual en red IPv4. |
| **6** | R2 (config) # interface FastEthernet 0/0<br>R2 (config-if) # **ipv6 address 172.16.12.2 255.255.255.0**<br>R2 (config-if) # no shutdown<br>R2 (config-if) # exit | Configurar interfaz de red para IPv4. |
| **7** | R2 (config) # interface FastEthernet 0/1<br>R2 (config-if) # **ipv6 address 24::1/64**<br>R2 (config-if) # **ipv6 rip CCNA enable**<br>R2 (config-if) # no shutdown<br>R2 (config-if) # exit | Configurar interfaz de red para IPv6. |

Continuación de la tabla XVIII.

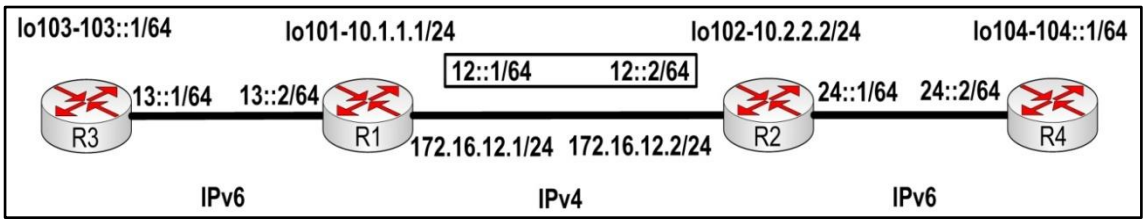
| | | |
|---|---|---|
| **8** | R2 (config) # router rip<br>R2 (config-router) # **version 2**<br>R2 (config-router) # **network 10.0.0.0**<br>R2 (config-router) # **network 172.16.0.0**<br>R2 (config-router) # **no auto-summary**<br>R2 (config-router) # exit | Configurar rip para la conectividad IPv4. |

Fuente: elaboración propia.

### 3.4.1.2. Túnel GRE

Este tipo de túnel utiliza el protocolo estándar GRE para el encapsulamiento. Al igual que el túnel manual IPv6, un túnel GRE es un enlace punto a punto. En el diagrama de red (vea figura 43) se implementa este tipo de túnel, difiere del túnel manual IPv6 en la configuración de la interface del túnel, por lo tanto en las tablas XIX y XX solamente se describen la configuración para la *interface tunnel 12* de los *routers* R1 y R2, el resto de las configuraciones es idéntica al túnel manual que se describió anteriormente. En esta configuración no se define el modo del túnel, debido a que por defecto es GRE.

Figura 43. **Diagrama de red implementación túnel GRE**




Fuente: elaboración propia, con base a Microsoft Visio.

Tabla XIX. **Comandos implementación túnel GRE *Router* 1**

| Paso | Comando o acción | Propósito |
|---|---|---|
| **1** | R1 (config) # interface Tunnel12<br>R1 (config-if) # no ip address<br>R1 (config-if) # **ipv6 address 12::1/64**<br>R1 (config-if) # **ipv6 rip CCNA enable**<br>R1 (config-if) # **tunnel source Loopback101**<br>R1 (config-if) # **tunnel destination 10.2.2.2**<br>R1 (config-if) # exit | Configurar túnel GRE en red IPv4. |

Fuente: elaboración propia.

Tabla XX. **Comandos implementación túnel GRE *Router* 2**

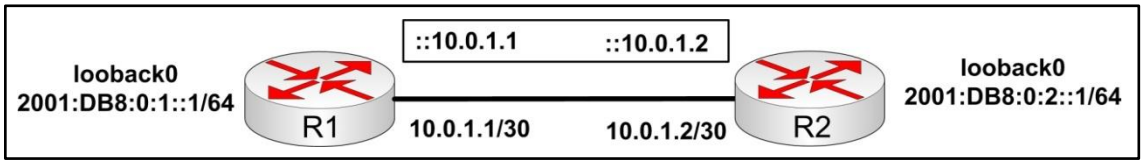
| Paso | Comando o acción | Propósito |
|---|---|---|
| **1** | R2 (config) # interface Tunnel12<br>R2 (config-if) # no ip address<br>R2 (config-if) # **ipv6 address 12::2/64**<br>R2 (config-if) # **ipv6 rip CCNA enable**<br>R2 (config-if) # **tunnel source Loopback102**<br>R2 (config-if) # **tunnel destination 10.1.1.1**<br>R2 (config-if) # exit | Configurar túnel GRE en red IPv4. |

Fuente: elaboración propia.

### 3.4.1.3. Túnel automático

Este tipo de túnel es un enlace punto a multipunto. Las direcciones compatibles con IPv4 e IPv6 se adoptan en ambos extremos del túnel. El formato de dirección es 0:0:0:0:0:0:a.b.c.d/96, donde a.b.c.d representa una dirección IPv4 incrustada. El destino del túnel se determina automáticamente por la dirección IPv4 embebida en el paquete IPv6. Sin embargo, este tipo de túnel debe utilizar direcciones compatibles con IPv4 e IPv6 y esto hace que sea dependiente de las direcciones IPv4. En el diagrama de red (vea figura 44) se implementa el túnel, en las tablas XXI y XXII se describen las configuraciones para los *routers* R1 y R2 respectivamente.

Figura 44. **Diagrama de red implementación túnel automático IPv6**




Fuente: elaboración propia, con base a Microsoft Visio.

Tabla XXI. **Comandos implementación túnel automático *Router* 1**

| Paso | Comando o acción | Propósito |
|---|---|---|
| **1** | R1> enable | Modo privilegiado |
| **2** | R1# configure terminal | Configurar terminal |
| **3** | R1 (config)# **ipv6 unicast-routing** | Habilita la transmisión de paquetes IPv6 en las interfaces. |

Continuación de la tabla XXI.

| | | |
|---|---|---|
| **4** | R1 (config) # **interface Loopback 0**<br>R1 (config-if) # **no ip address**<br>R1 (config-if) # **ipv6 address 2001:DB8:0:1::1/64**<br>R1 (config-if) # exit | Configurar interfaz *loopback* de red para IPv6. |
| **5** | R1 (config) # interface FastEthernet 0/1<br>R1 (config-if) # **ip address 10.0.1.1 255.255.255.252**<br>R1 (config-if) # no shutdown<br>R1 (config-if) # exit | Configurar interfaz de red para IPv4. |
| **6** | R1 (config) # **interface tunnel 0**<br>R1 (config-if) # **tunnel source 10.0.1.1**<br>R1 (config-if) # **tunnel mode ipv6ip auto-tunnel**<br>R1 (config-if) # exit | Configurar túnel automático en red IPv4. |
| **7** | R1 (config) # **ipv6 route 2001:DB8:0:2::/64 ::10.0.1.2** | Configurar de ruta estática IPv6. |

Fuente: elaboración propia.

Tabla XXII. **Comandos implementación túnel automático *Router* 2**

| Paso | Comando o acción | Propósito |
|---|---|---|
| **1** | R2> enable | Modo privilegiado |
| **2** | R2# configure terminal | Configurar terminal |
| **3** | R2 (config)# **ipv6 unicast-routing** | Habilita la transmisión de paquetes IPv6 en las interfaces. |
| **4** | R2 (config) # **interface Loopback 0**<br>R2 (config-if) # **no ip address**<br>R2 (config-if) # **ipv6 address 2001:DB8:0:1::1/64**<br>R2 (config-if) # exit | Configurar interfaz *loopback* de red para IPv6. |

Continuación de la tabla XXII.

| | | |
|---|---|---|
| **5** | R2 (config) # interface FastEthernet 0/1<br>R2 (config-if) # **ip address 10.0.1.1 255.255.255.252**<br>R2 (config-if) # no shutdown<br>R2 (config-if) # exit | Configurar interfaz de red para IPv4. |
| **6** | R2 (config) # **interface tunnel 0**<br>R2 (config-if) # **tunnel source 10.0.1.1**<br>R2 (config-if) # **tunnel mode ipv6ip auto-tunnel**<br>R2 (config-if) # exit | Configurar túnel automático en red IPv4. |
| **7** | R2 (config) # **ipv6 route 2001:DB8:0:2::/64 ::10.0.1.2** | Configurar de ruta estática IPv6. |

Fuente: elaboración propia.

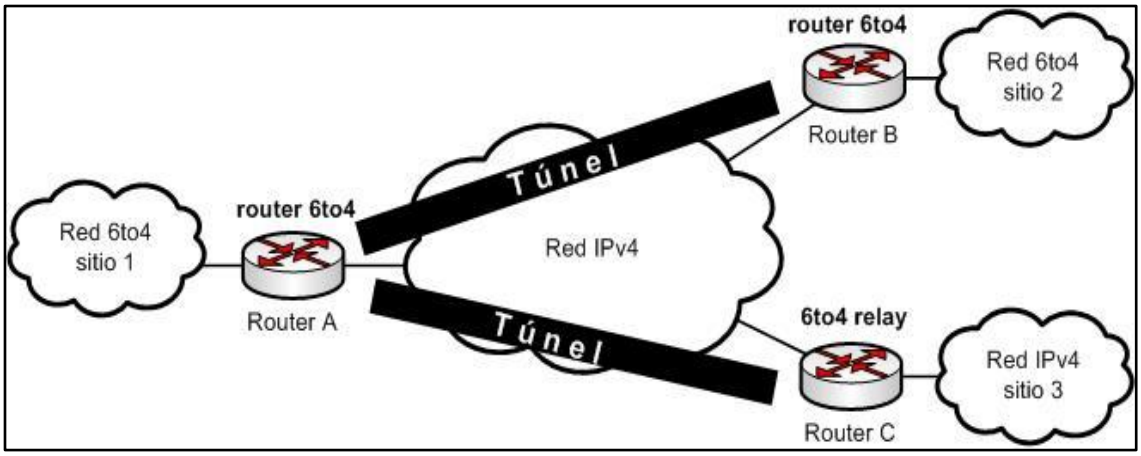
#### 3.4.1.4. Túnel *6to4*

El túnel *6to4* ordinario es uno de las dos formas de implementar este tipo de túnel, el cual es un túnel de punto a multipunto y se utiliza para conectar múltiples redes IPv6 aisladas hacia otras redes IPv6 remotas sobre una red IPv4. La dirección IPv4 embebida en una dirección IPv6 se utiliza para obtener automáticamente el destino del túnel.

El formato de dirección *6to4* es 2002:aabb:ccdd:<número de subred>::<ID interfaz>/64, en donde aabb:ccdd representa los 32 bits de la dirección IPv4 en notación hexadecimal. Por ejemplo, 5.5.5.5 puede ser representado por 0505:0505. El destino del túnel se determina automáticamente por la dirección IPv4 embebidas, lo que hace fácil la creación de un túnel *6to4*.

La otra forma del túnel *6to4* es la retransmisión, o más conocido como túnel *6to4 relay*, con este túnel se puede conectar redes cuya dirección es el prefijo 2002::/16 ó 2001::/16. Para que estas direcciones sean accesibles, un *router* 6to4 debe ser utilizado como puerta de entrada para reenviar paquetes a las redes IPv6 llamado *router 6to4 relay (*vea figura 45), una ruta estática debe configurarse en el *router* frontera de la red *6to4* y la dirección del siguiente salto debe ser la dirección *6to4* del *router 6to4 relay*.

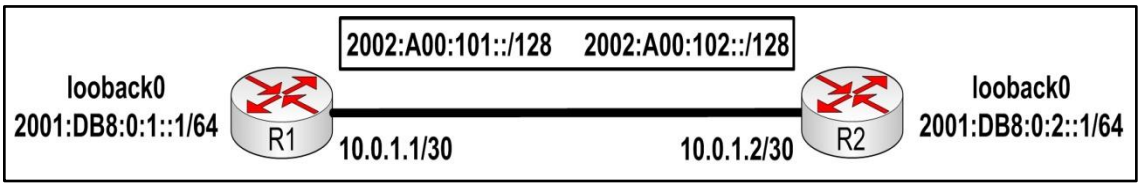
Figura 45. **Principio de túnel *6to4* ordinario y *6to4* de retransmisión**




Fuente: elaboración propia, con base a Microsoft Visio.

En el diagrama de red (vea figura 46) se implementa el túnel, en las tablas XXIII y XXIV se describen las configuraciones para los *routers* R1 y R2 respectivamente. Debido a que las configuraciones básicas ya se definieron en la implementación del túnel automático, a continuación solo se define la configuración de la interfaz del túnel y las rutas estáticas, el resto de configuraciones son idénticas a la anterior implementación.

Figura 46. **Diagrama de red implementación túnel *6to4***




Fuente: elaboración propia, con base a Microsoft Visio.

Tabla XXIII. **Comandos implementación túnel *6to4 Router* 1**

| Paso | Comando o acción | Propósito |
|---|---|---|
| **1** | R1 (config) # **interface tunnel 0**<br>R1 (config-if) # **ipv6 address 2002:A00:101::/128**<br>R1 (config-if) # **tunnel source 10.0.1.1**<br>R1 (config-if) # **tunnel mode ipv6ip 6to4**<br>R1 (config-if) # exit | Configurar túnel *6to4* en red IPv4. |
| **2** | R1 (config) # **ipv6 route 2001:DB8:0:2::/64 2002:A00:102::**<br>R1 (config) # **ipv6 route 2002:: /16 Tunnel0** | Configurar de rutas estáticas IPv6. |

Fuente: elaboración propia.

Tabla XXIV. **Comandos implementación túnel *6to4 Router* 2**

| Paso | Comando o acción | Propósito |
|---|---|---|
| **1** | R2 (config) # **interface tunnel 0**<br>R2 (config-if) # **ipv6 address 2002:A00:102::/128**<br>R2 (config-if) # **tunnel source 10.0.1.2**<br>R2 (config-if) # **tunnel mode ipv6ip 6to4**<br>R2 (config-if) # exit | Configurar túnel *6to4* en red IPv4. |

Continuación de la tabla XXIV.

| | | |
|---|---|---|
| **2** | R2 (config) # **ipv6 route 2001:DB8:0:1::/64 2002:A00:101::**<br>R2 (config) # **ipv6 route 2002:: /16 Tunnel0** | Configurar de rutas estáticas IPv6. |

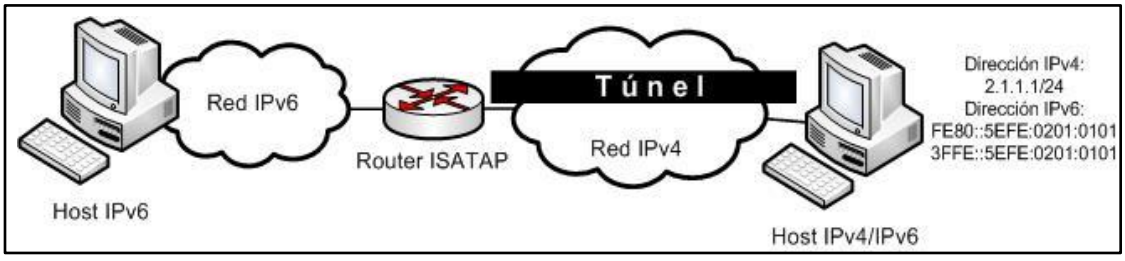
Fuente: elaboración propia.

#### 3.4.1.5. Túnel ISATAP

La tecnología de túnel ISATAP proporciona una solución satisfactoria para las aplicaciones IPv6. Un túnel ISATAP es un túnel de punto a punto automático. El destino de un túnel se puede determinar de forma automática en la dirección IPv4 embebida en la dirección de destino de un paquete IPv6.

La dirección de destino de un paquete y la dirección IPv6 de una interfaz de túnel deben tener el formato ISATAP. El formato de la es <prefijo 64 bits>::5EFE:<dirección IPv4>. La dirección IPv4 puede ser en notación decimal a.b.c.d o hexadecimal aabb:ccdd, donde aabb:ccdd representa una dirección IPv4 de 32 bits en notación hexadecimal (vea figura 47).

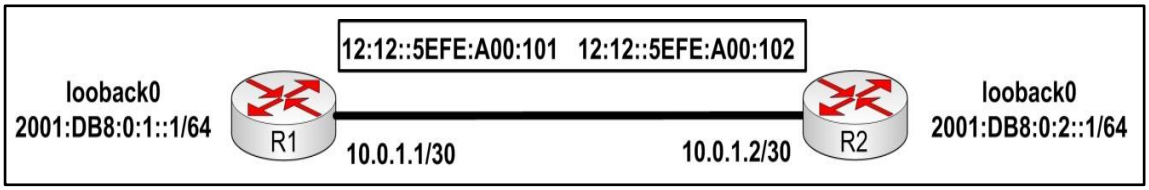
Figura 47. **Operación túnel ISATAP**




Fuente: elaboración propia, con base a Microsoft Visio.

En el diagrama de red (vea figura 48) se implementa el túnel, en las tablas XXV y XXVI se describen las configuraciones para el *routers* R1 y R2 respectivamente. Debido a que las configuraciones básicas ya se definieron en la implementación del túnel automático, a continuación solo se define la configuración de la interfaz del túnel y las rutas estáticas, el resto de configuraciones son idénticas a la implementación del túnel automático.

Figura 48. **Diagrama de red implementación túnel ISATAP**




Fuente: elaboración propia, con base a Microsoft Visio.

Tabla XXV. **Comandos implementación túnel ISATAP *Router* 1**

| Paso | Comando o acción | Propósito |
|---|---|---|
| **1** | R1 (config) # **interface tunnel 0**<br>R1 (config-if) # **ipv6 address 12:12::/64 eui-64**<br>R1 (config-if) # **tunnel source 10.0.1.1**<br>R1 (config-if) # **tunnel mode ipv6ip isatap**<br>R1 (config-if) # exit | Configurar túnel ISATAP en red IPv4. |
| **2** | R1 (config) # **ipv6 route 2001:DB8:0:2::/64 Tunnel0 FE80::5EFE:A00:102** | Configurar de ruta estática IPv6. |

Fuente: elaboración propia.

Tabla XXVI. **Comandos implementación túnel ISATAP *Router* 2**

| Paso | Comando o acción | Propósito |
|---|---|---|
| **1** | R2 (config) # **interface tunnel 0**<br>R2 (config-if) # **ipv6 address 12:12::/64 eui-64**<br>R2 (config-if) # **tunnel source 10.0.1.2**<br>R2 (config-if) # **tunnel mode ipv6ip isatap**<br>R2 (config-if) # exit | Configurar túnel ISATAP en red IPv4. |
| **2** | R2 (config) # **ipv6 route 2001:DB8:0:1::/64 Tunnel0 FE80::5EFE:A00:101** | Configurar de ruta estática IPv6. |

Fuente: elaboración propia.

#### 3.4.1.6. Ventajas

La principal ventaja del túnel IPv6 sobre IPv4 es el ser tranparente para las aplicaciones y usuarios, a continuación se listan las principales ventajas:

- Los túneles IPv6 sobre IPv4 son transparentes a nivel de IPv6 y, por lo tanto, no afectan a las aplicaciones existentes.

- Permite probar la IPv6 en algunos nodos de la red IPv4 sin tener que instalar la pila IPv6 en los *router* internos.

- Los túneles automáticos son útiles para redes grandes donde definir túneles configurados es una tarea tediosa y no recomendable.

#### 3.4.1.7. Desventajas

Las desventajas más importantes de túnel IPv6 sobre IPv4 se listan a continuación:

- Los mecanismos de túneles en su mayoría solo son recomendables para redes locales con poca carga de tráfico.

- En los túneles configurados la complejidad es alta en el enrutamiento.

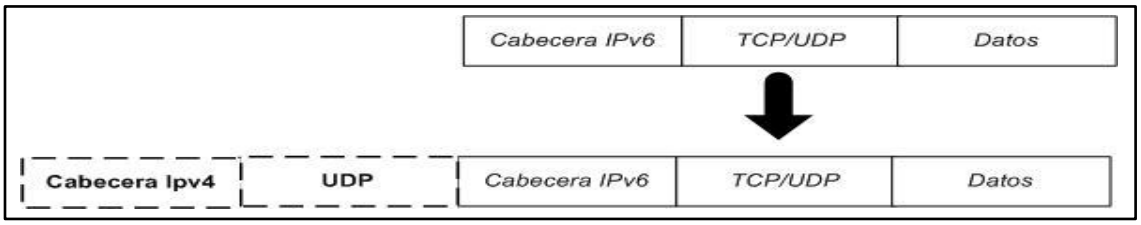
- IPv6 sobre IPv4 se basa en la disponibilidad del *multicast* en IPv4, que no tiene un amplio soporte de la infraestructura de red IPv4 (*multicast* es casi tan reciente como IPv6).

- El túnel ISATAP es la alternativa más compleja para IPv6 sobre IPv4 ya que no se basa en IPv4 *multicast*.

### 3.4.2. Otros mecanismos de túneles

Teredo es uno de los mecanismos de túneles importantes dentro de la transición a IPv6, teredo es mecanismo de asignación de direcciones y de tecnología de túnel automático que proporciona conectividad IPv6 *unicast* a través de internet IPv4 al igual que *6to4*, teredo resuelve los problemas de la falta de funcionalidad de *6to4*, dado que los dispositivos *NAT/firewall* no permite el recorrido de los paquetes IPv4 con el campo protocolo establecido a 41, que indica la encapsulación des un paquete IPv6 en IPv4. Teredo incorpora la cabecera UDP adicionales para facilitar el paso por el *NAT/firewall* (vea figura 49).

Figura 49. **Teredo cabecera**

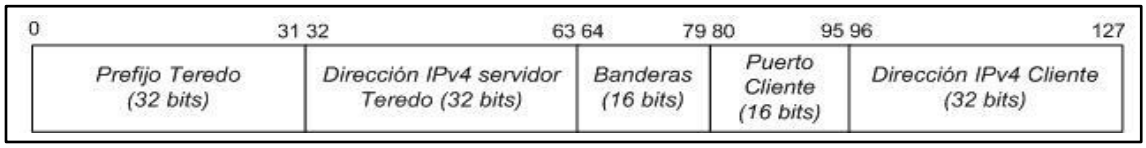



Fuente: *IPv4 to IPv6 transition strategies*.

En resumen, teredo es una tecnología de transición IPv6 que permite la configuración de túnel IPv6 automático entre *hosts* que se encuentran tras uno o más dispositivos NAT IPv4. El tráfico IPv6 desde los *hosts* teredo puede fluir a través de NAT, ya que se envía como un mensaje UDP IPv4. El NAT admite teredo si soporta traducción de puertos UDP, la excepción es en NAT simétrico, teredo está definido en el RFC 4380.

El formato de la dirección IPv6 teredo (vea figura 50) tiene un prefijo 2001::/32 predefinido, las banderas indican el tipo de NAT, ya sea de cono completo con un valor de 0x8000 o cono restringido y/o cono restringido a puerto con un valor de 0x0000. El campo puerto del cliente y dirección IPv4 cliente están representados en notación hexadecimal.

Figura 50. **Formato de dirección IPv6 teredo**




Fuente: *IPv4 to IPv6 transition strategies*.

Es importante definir los tipos de NAT para este tipo de túnel, dado que la presencia de NAT puede conducir a la necesidad de realizar un paso adicional para inicializar las asignaciones de la tabla NAT y de esto teredo se encarga facilitando el trabajo. Según las restricciones en la comunicación NAT, los tipos son:

- Cono completo: los *hosts* externos pueden comunicarse con otro *host*, simplemente con transmitir a la dirección asignada y el puerto exterior.

- Cono restringido: un *host* externo puede comunicarse con el *host* interno si el *host* interno previamente había enviado un paquete al *host* externo.

- Cono restringido a puerto: es similar al cono restringido, con la restricción que incluye los puertos. Los *hosts* externos pueden comunicarse con el *host* interno, solo si el *host* interno previamente envió un paquete al *host* externo, usando la dirección del *host* externo y el mismo puerto.

- Simétrico: los paquetes provenientes de la misma dirección y puerto con la misma dirección IP y puerto de destino utilizan la misma asignación de dirección IP y puerto, se asigna una diferente dirección IP y puerto si la dirección IP de destino y puerto son diferentes.

Teredo requiere de cuatro diferentes componentes lo cual conforman la infraestructura teredo (vea figura 51), los cuales son:

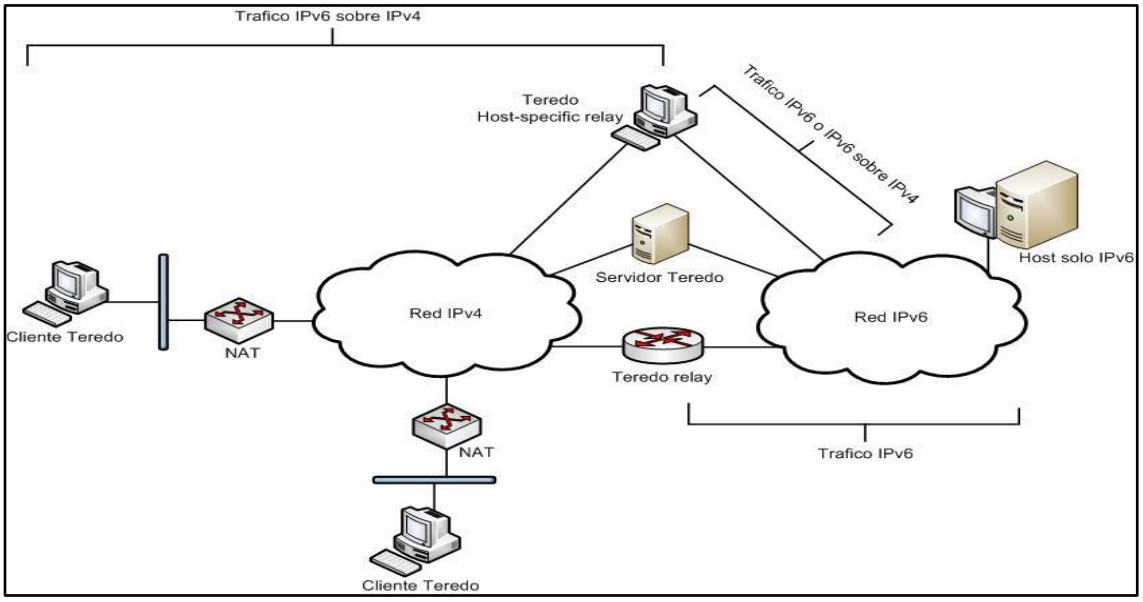
- Cliente teredo: es un nodo IPv6/IPv4 que soporta una interfaz de túnel teredo. Un cliente teredo se comunica con el servidor para obtener el prefijo de la dirección, configurar la dirección teredo IPv6, para iniciar la comunicación con otros clientes teredo u otros *hosts* de internet IPv6.

- Servidor teredo: es un nodo IPv6/IPv4 que está conectado a la red internet IPv4 e IPv6, es compatible con una interfaz de túnel teredo. La función principal es la configuración del cliente y facilitar la comunicación inicial.

- Teredo *relay*: es un *router* IPv6/IPv4 que puede reenviar paquetes entre los clientes teredo en internet IPv4 y a los *hosts* sólo IPv6. El teredo *relay* al igual que el servidor teredo escuchan en el puerto UDP 3544 para el tráfico teredo.

- Teredo *host-especific relay*: es un nodo con conectividad a internet IPv4 e IPv6, puede comunicarse directamente con los clientes teredo a través de internet IPv4, sin la necesidad del intermediario teredo *relay*.

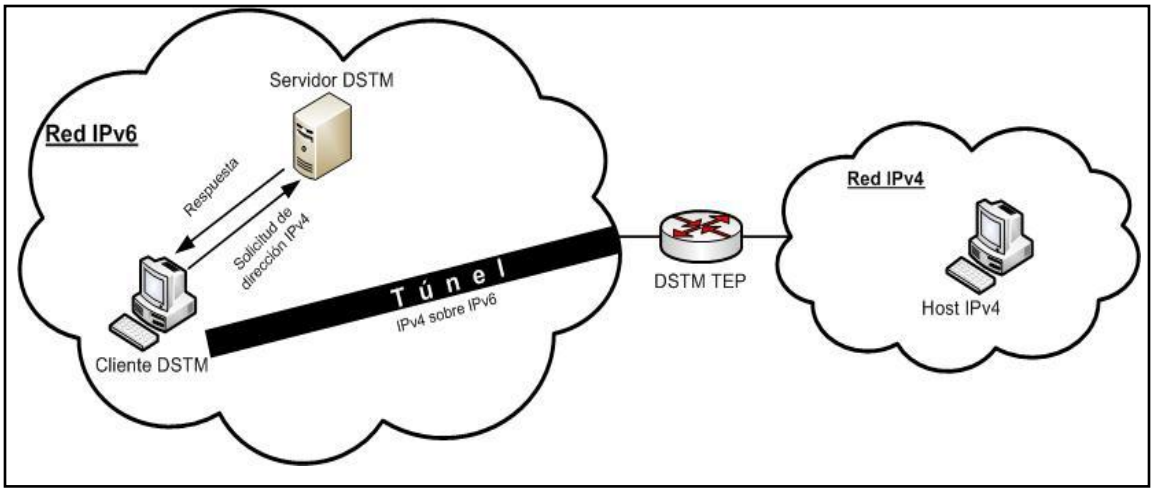
Figura 51. **Componentes en infraestructura Teredo**




Fuente: *Teredo overview*, en: http://technet.microsoft.com/en-us/library/bb457011.aspx. Consulta: 6 de julio de 2011.

Otro de los mecanismos de túneles importante por definir es el *Dual Stack Transition Mechanism* (*DSTM por sus siglas en inglés*), este tipo de túnel utiliza un túnel IPv4 sobre IPv6 para proporcionar a los *hosts* IPv6 en una red IPv6 dominante de la compatibilidad hacia atrás y comunicarse con *hosts* IPv4 en las redes IPv4 tradicional. DSTM consta de tres componentes (vea figura 52), los cuales son: cliente DSTM, servidor DSTM y DSTM TEP.

Figura 52. **Componentes DSTM**




Fuente: elaboración propia, con base a Microsoft Visio.

Un cliente DSTM es un *host* IPv6 en la red IPv6 con un módulo de software DSTM cliente instalado, lo que permite que el *host* IPv6 pueda conectarse con los *hosts* IPv4. El servidor DSTM proporciona un *pool* de direcciones IPv4 que se asignan a un cliente DSTM y se mantiene la asignación de IPv6 a IPv4 en la caché del servidor. El punto final del túnel o DSTM *Tunnel End Point* (TEP por sus siglas en inglés) es el *router* en el extremo final de la red IPv6 que tiene instalado el *software* TEP, el cual funciona como un intérprete, desencapsula y encapsular el tráfico IPv4 entre la red IPv6 e IPv4.

#### 3.4.2.1. Ventajas

Las principales ventajas de los mecanismos de transición de túneles teredo y DSTM se listan a continuación:

- Teredo es una tecnología NAT para el tráfico IPv6. El tráfico IPv6 utilizando túneles teredo puede atravesar uno o múltiples dispositivos NAT.

- DSTM mantiene políticas IPv6 nativas dentro de la red IPv6 donde se despliega, la gestión de IPv4 no es necesaria dentro de esta red, esto simplifica la administración de la red.

- En DSTM no hay traducción de protocolo. El tráfico IPv4 se envía por el túnel entre el cliente DSTM y el TEP, lo que hace que la comunicación sea directa.

#### 3.4.2.2. Desventajas

Las principales desventajas de los mecanismos de transición de túneles teredo y DSTM se listan a continuación:

- Teredo no es compatible con todos los dispositivos NAT. El tipo cono completo, cono restringido y cono restringido a puerto de dispositivos NAT son compatibles, mientras que el NAT simétrico no lo es.

- El servidor DSTM pueda que no cubra con la demanda cuando el tráfico IPv4 es demasiado al tener un *pool* de direcciones IPv4 pequeño.

- El ancho de banda disponible para todos los clientes teredo hacia el internet IPv6 se ve limitada por la disponibilidad del teredo *relay*.

- El DSTM TEP al ser la única salida para el tráfico IPv4, debe de tener los recursos suficientes para que soporte la carga de tráfico en la infraestructura de red.

# 4. SEGURIDAD

¿Es el protocolo IPv6 más seguro que su antecesor? La IPv6 es mucho más segura, debido a que IPSec es obligatoria y no opcional como sucede en IPv4, lo que la hace más vulnerables. La seguridad ofrecida por IPSec entra en juego en la capa de internet del modelo TCP/IP (vea figura 24), ofreciendo varios servicios de seguridad, incluyendo encriptación, autenticación, integridad, protección de replicación y confidencialidad en las comunicaciones de extremo a extremo.

La flexibilidad y transparencia del protocolo IPSec permiten adaptar una configuración de seguridad para cada necesidad, sin embargo, ciertos aspectos de IPSec como el uso de una cabecera de autenticación y de gestión de intercambio de llaves, son incompatibles con NAT, una razón más para avanzar hacia la transición a IPv6 y eventualmente reducir los dispositivos NAT hasta prescindir de su uso.

## 4.1. IPSec

IPSec es un conjunto de protocolos que tienen como fin proporcionar seguridad en la comunicación en la capa de red del modelo OSI (vea figura 64), a la que pertenece el protocolo IPv6, y de ese modo, a todos los protocolos de las capas superiores. En IPv6 la propia arquitectura extensible del protocolo permite implementar IPSec de forma natural y en IPv4 la implementación de IPSec se define en una especificación diferente a la del propio protocolo.

Es importante aclarar que la IPv6 habilita la posibilidad de usar IPSec y no los mecanismos de cifrado y autenticación propios de IPSec. IPSec tiene dos modos de funcionamiento que proporcionan distintos niveles de seguridad, los cuales son: modo transporte y modo túnel. Además IPSec tiene dos protocolos de transferencia, que a su vez pueden funcionar en modo túnel o transporte, los cuales son: cabecera de autenticación y carga de seguridad encapsulada. Los modos de funcionamiento así como los protocolos de transferencia se describen a mayor detalle en las siguientes secciones.

### 4.1.1. Protocolos de transferencia

Seleccionar un protocolo seguro, determinar los algoritmos, su uso y colocar en su lugar la encriptación para las llaves requeridas, es el conjunto de servicios que son proporcionados por uno o ambos de estos protocolos de transferencia y se pueden implementar individualmente o combinados con otros, para proporcionar un conjunto de servicios necesarios para IPv6. Cada protocolo proporciona los siguientes servicios:

- La cabecera de autenticación proporciona integridad sin conexión, autenticación de los datos de origen y un servicio opcional de antireplicación.

- El protocolo de carga de seguridad encapsulada garantiza la confidencialidad y provee de confidencialidad limitada del flujo de tráfico. Puede proporcionar integridad sin conexión, autenticación de los datos de origen, y un servicio de antireplicación.

#### 4.1.1.1. Cabecera de autenticación

*Authentication Header* (AH por sus siglas en inglés) tiene como propósito transmitir la información de autenticación en el datagrama IP. La información de autenticación se calcula utilizando todos los campos del datagrama que no varían. El tipo de carga de AH es de 51. Estos son algunos de los servicios proporcionados por AH:

- Ofrece antireplicación de servicio a la discreción del receptor, para ayudar a contrarrestar los ataques de denegación de servicio.

- Es un protocolo adecuado para implementar cuando la confidencialidad no es necesaria.

- Proporciona la autenticación de las partes seleccionadas de la cabecera IP, que puede ser necesaria en algunos contextos. Por ejemplo, si la integridad de una cabecera de extensión IPv6 deben ser protegidos en el camino entre emisor y receptor.

#### 4.1.1.2. Carga de seguridad encapsulada

*Encapsulated Security Payload* (ESP por sus siglas en inglés) tiene como propósito transmitir los datos cifrados de los datagramas IP. Los datos encriptados se obtienen mediante una transformación específica de encriptación a los datos que deban protegerse. El tipo de carga de ESP es de 50. Estos son algunos de los servicios que ESP proporciona:

- Opcionalmente, puede proporcionar confidencialidad para el tráfico, la fortaleza del servicio de confidencialidad depende, en gran parte, del algoritmo de cifrado empleado.

- Proporcionar servicios de autenticación de manera opcional.

- La carga útil puede ser invocada para ocultar el tamaño de los paquetes, además de ocultar las características externas del tráfico.

### 4.1.2. Modos de funcionamiento

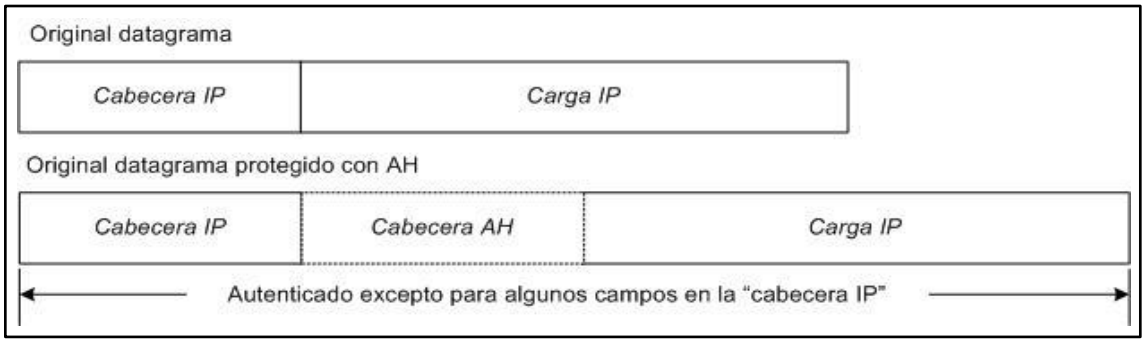
Existen dos modos de funcionamiento o de encriptación, los cuales son: modo transporte y modo túnel. En el modo transporte los protocolos proporcionan protección, sobre todo para los protocolos de capas superiores y en el modo de túnel los protocolos se aplican a los paquetes IP del túnel. La principal diferencia es que en modo transporte en cada paquete solo la carga útil se cifra y en modo túnel todo el paquete es cifrado incluyendo la carga útil.

#### 4.1.2.1. Modo transporte

Este modo es el predeterminado para IPSec y se utiliza para las comunicaciones de extremo a extremo. Cuando el modo de transporte es utilizado IPSec cifra sólo la carga IP. El modo de transporte ofrece la protección de la carga IP a través de una cabecera AH o ESP. La AH proporciona autenticación, integridad y protección antireplicación para todo el paquete, la cabecera IP y la carga útil.

En AH no se proporciona confidencialidad, es decir, los datos no se cifran. Los datos son legibles, pero protegido de la modificación, en AH se utilizan algoritmos *hash* en clave para firmar el paquete de integridad. La protección de integridad de la cabecera IP, la cabecera AH, y la carga IP de datos le asegura al receptor que el emisor fue quien envió los datos y no fueron modificados. La integridad y la autenticación son proporcionadas por la colocación de la cabecera AH entre la cabecera IP y la carga IP (vea figura 53).

Figura 53. **Modo transporte AH**




Fuente: elaboración propia, con base a Microsoft Visio.

AH puede ser implementado solo o en combinación con la carga útil del protocolo ESP. La cabecera AH incluye los siguientes campos (vea figura 54):

- Siguiente cabecera: identifica la carga IP mediante el uso de la ID del protocolo IP.

- Longitud de carga: indica la longitud del paquete AH.

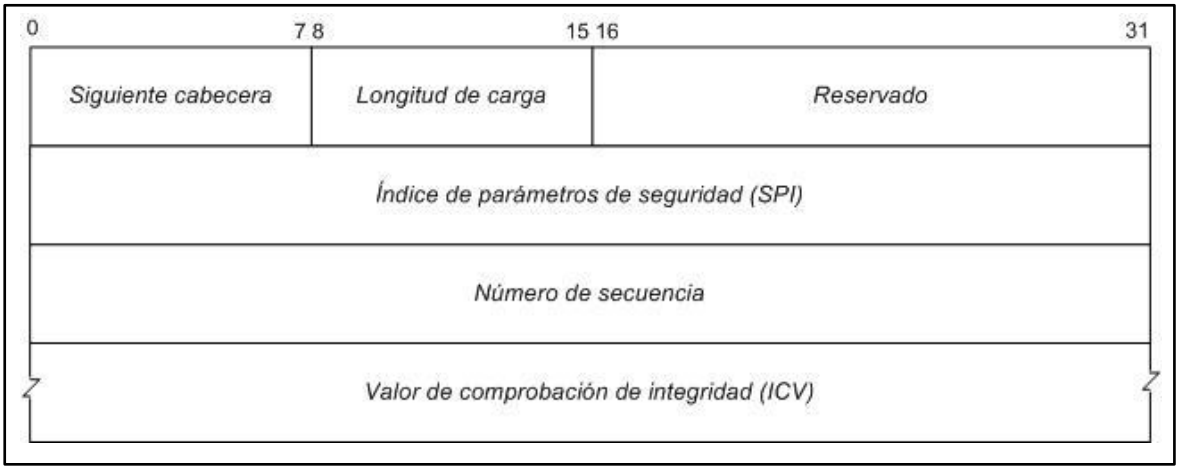
- Reservado: reservado para usos futuros (se colocan todo a ceros).

- Índice de parámetros de seguridad (SPI): se utiliza en combinación con la dirección de destino y el protocolo de seguridad AH o ESP para identificar la asociación de seguridad correcta para la comunicación.

- Número de secuencia: ofrece protección antireplicación para los paquetes, consta de de 32 bits, aumentando gradualmente la cantidad en el campo, iniciando en 1.

- Valor de comprobación de integridad (ICV): también conocido como el código de autenticación de mensajes, se utiliza para verificar la autenticación y la integridad de los mensajes.

Figura 54. **Formato de cabecera AH**

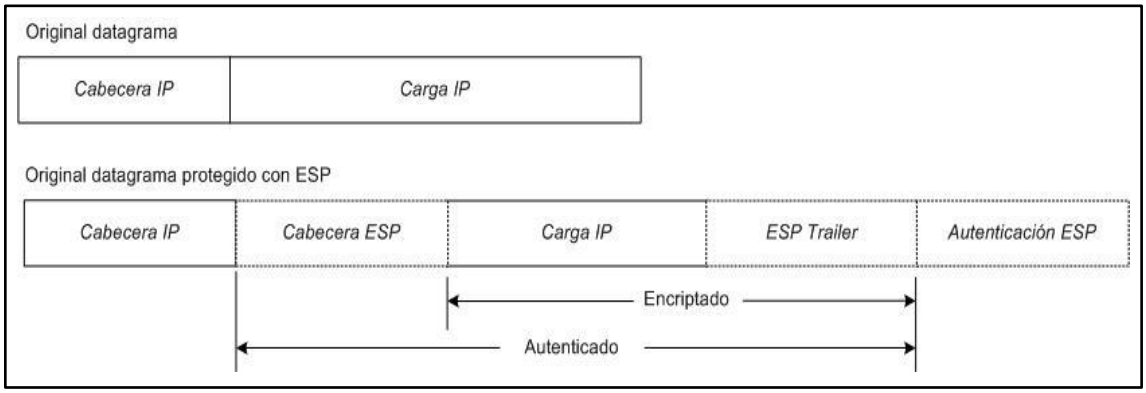



Fuente: elaboración propia, con base a Microsoft Visio.

La carga de seguridad encapsulada (ESP) ofrece confidencialidad además de la protección de autenticación, integridad y antireplicación para la carga IP.

ESP en modo de transporte no firma todo el paquete, sólo la carga IP está protegida. Con esto el equipo receptor puede estar seguro de que fue el emisor quien envió los datos, los datos están sin modificar, y nadie más fue capaz de leerlos. La cabecera ESP se coloca antes de la carga IP, y el ESP *trailer* y la autenticación ESP se coloca después de la carga útil IP (vea figura 55). ESP puede ser utilizado solo o en combinación con AH.

Figura 55. **Modo transporte ESP**




Fuente: elaboración propia, con base a Microsoft Visio.

A continuación se detallan los campos que contienen la cabecera ESP, ESP *trailer* y autenticación ESP, el encabezado ESP contiene los siguientes campos:

- Índice de parámetros de seguridad (SPI): al igual que en AH identifica la asociación de seguridad.

- Número de secuencia: al igual que en la cabecera AH ofrece protección antireplicación para el paquete.

Otro de los campos que se le agregan al datagrama original es el ESP *trailer* que se compone de los siguientes campos:

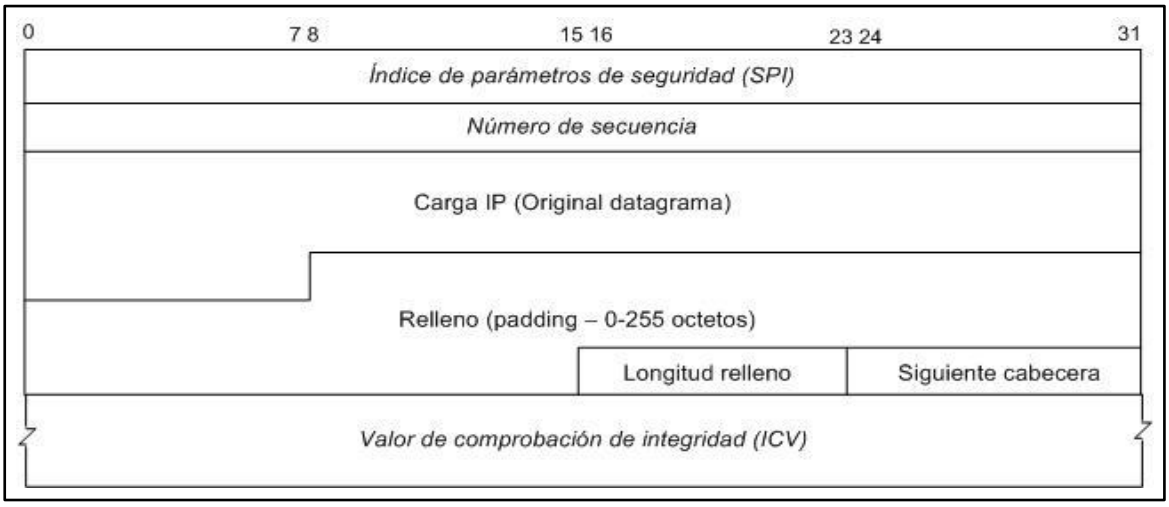
- Relleno (*padding*): con un valor de 0 a 255, se utiliza para asegurar que la carga útil encriptada con los bytes de relleno se encuentran en los límites requerido por el algoritmo de cifrado.

- Longitud relleno: indica la longitud del campo relleno en bytes.

- Siguiente cabecera: identifica el tipo de datos de la carga IP.

El último campo que se agrega al datagrama original es la autenticación ESP y consta de los datos de autenticación, que al igual que en la cabecera AH contiene el valor de ICV que se utiliza para verificar la autenticación y la integridad de los mensajes.

Figura 56. **Formato ESP**



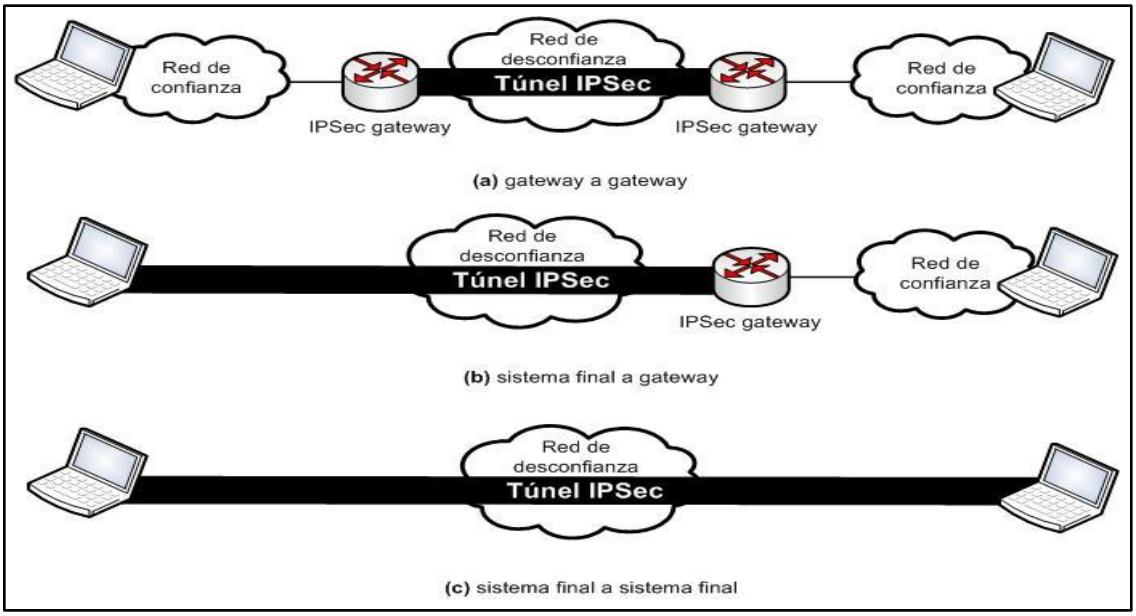

Fuente: elaboración propia, con base a Microsoft Visio.

#### 4.1.2.2. Modo túnel

Con este modo IPSec encripta tanto la cabecera IP como la carga IP. El modo de túnel proporciona la protección de un paquete IP y el paquete IP se encapsula con un encabezado AH o ESP y una cabecera IP adicional. Las direcciones IP de la nueva cabecera IP no son la de origen y de destino original sino de los extremos del túnel. El modo de túnel se utiliza principalmente para la interoperabilidad con *gateways* o sistemas finales, la IPSec se puede utilizar en las siguientes configuraciones (vea figura 57):

- *Gateway* a *gateway*
- Sistema final a *gateway*
- Sistema final a sistema final

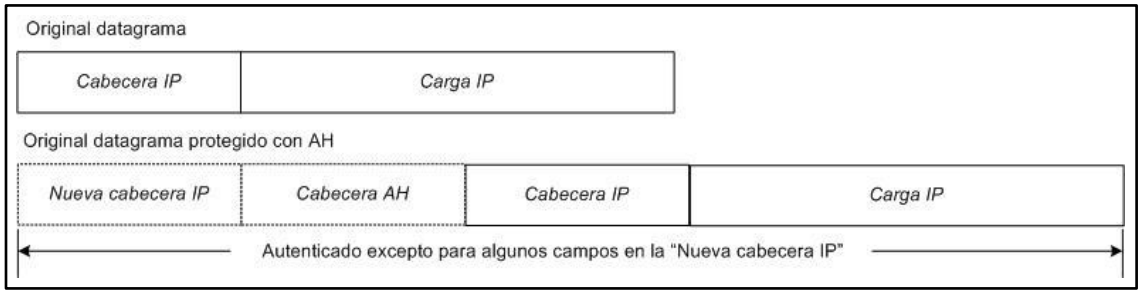
Figura 57. **Configuraciones modo túnel IPSec**




Fuente: elaboración propia, con base a Microsoft Visio.

La AH en modo túnel encapsula el paquete IP con la cabecera AH y una nueva cabecera IP y firma todo para la integridad y autenticación (vea figura 58), la cabecera AH tiene el mismo formato que con el modo trasporte (vea figura 54).

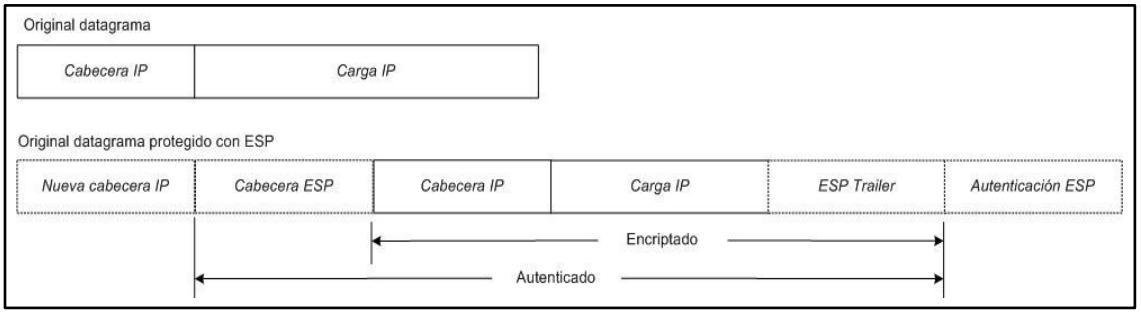
Figura 58. **Modo túnel AH**




Fuente: elaboración propia, con base a Microsoft Visio.

En el ESP para este modo de IPSec (vea figura 59) se encapsula todo el datagrama anteponiendo una nueva cabecera IP y ESP, y agregando al final el campo de autenticación ESP.

Figura 59. **Modo túnel ESP**




Fuente: elaboración propia, con base a Microsoft Visio.

La parte autenticada indica que el paquete está firmado por la integridad y autenticación. La parte encriptada indica que el paquete está protegido por la confidencialidad. La nueva cabecera IP sólo se utiliza para enviar el paquete desde el punto de origen al punto final del túnel

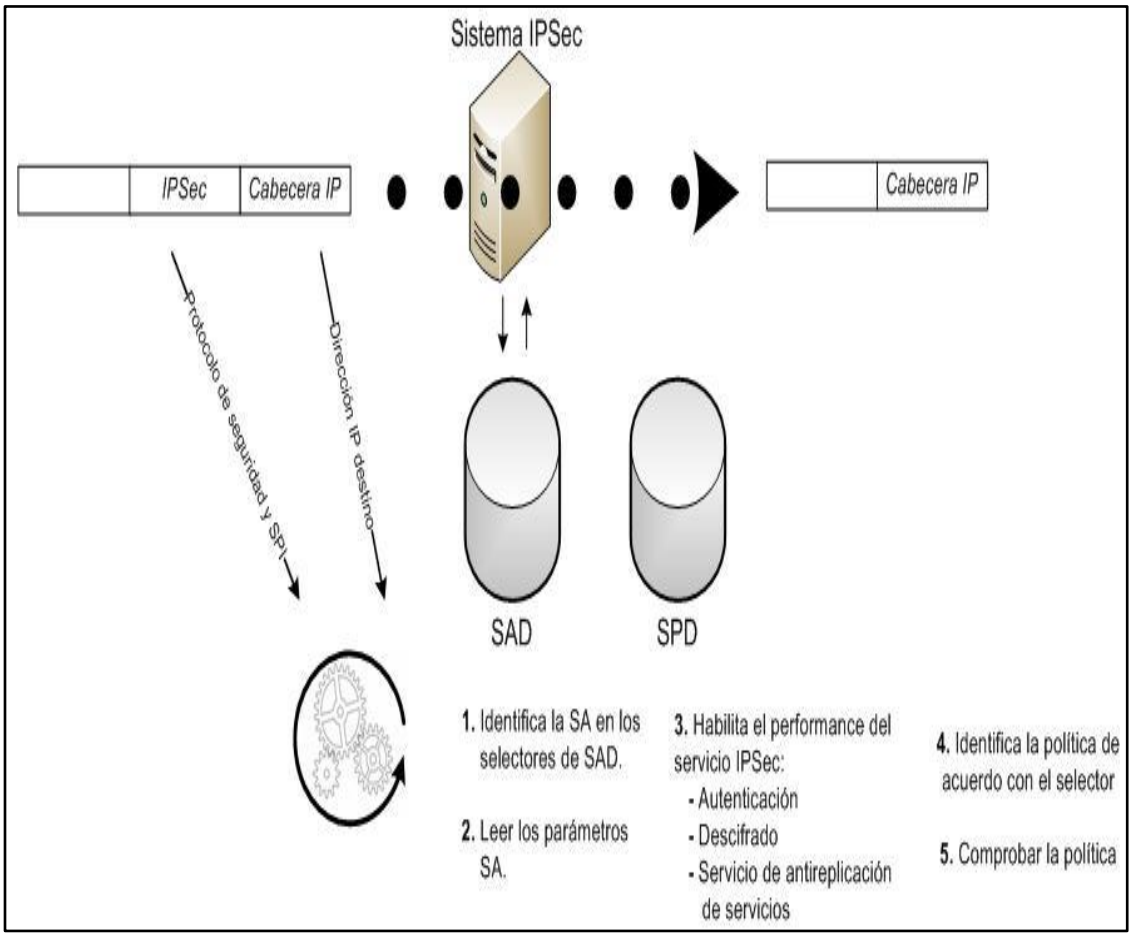
### 4.1.3. Asociación de seguridad

*Security Association* (SA por sus siglas en inglés) es un identificador único que se compone del índice de parámetros de seguridad, una dirección IP de destino, y un identificador de protocolo de seguridad, la dirección de destino puede ser una dirección *unicast*, de difusión, o de un grupo *multicast*.

El conjunto de los servicios de seguridad ofrecidos por SA depende del protocolo de seguridad seleccionado, el modo, los extremos del SA, y de la elección de los servicios opcionales dentro del protocolo.

En cada implementación de IPSec hay una base de datos de asociación seguridad (*Security Association Database*, SAD por sus siglas en inglés), en cada entrada a la base de datos se definen los parámetros asociados a SA. Una asociación de seguridad es una herramienta de gestión utilizada para hacer cumplir las políticas de seguridad en el entorno IPSec.

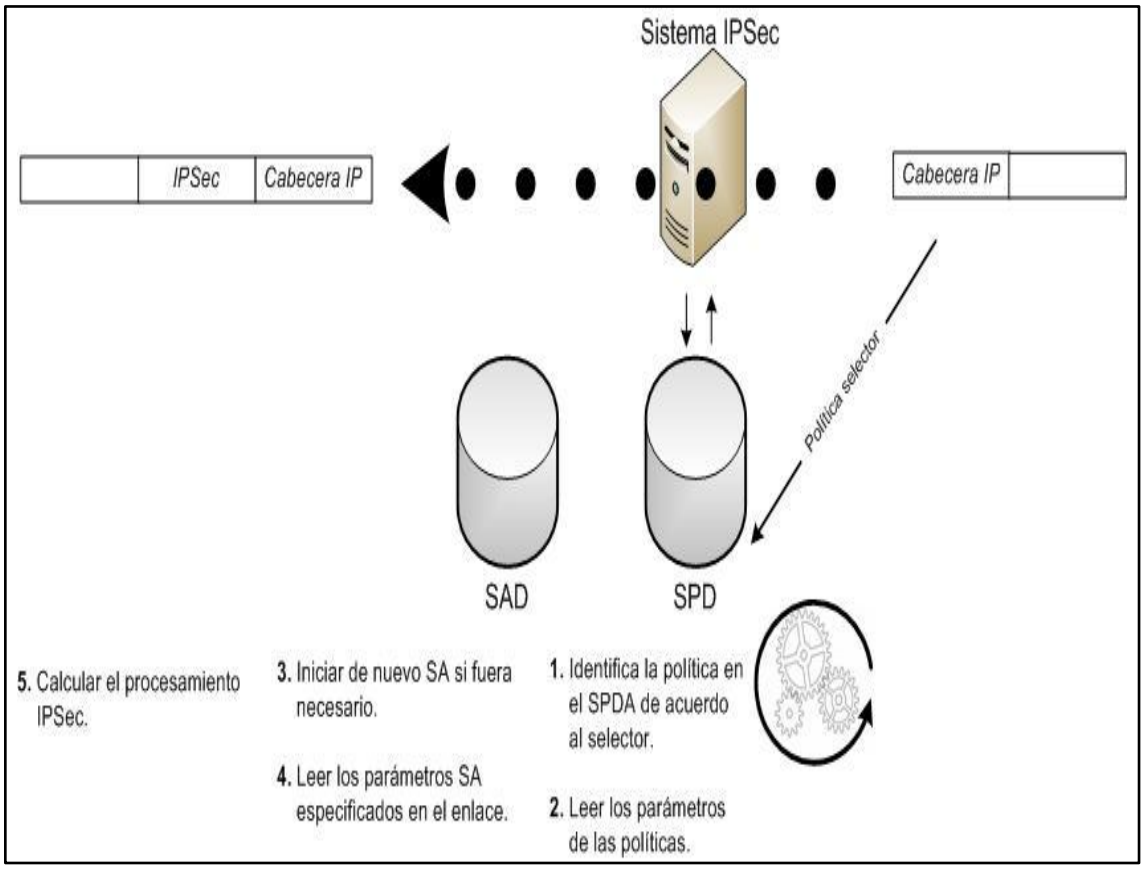
Figura 60. **Proceso de entrada SA**




Fuente: elaboración propia, con base a Microsoft Visio.

Para el proceso de salida (vea figura 61), las entradas se enlazan por medio de anotaciones en la base de datos de políticas de seguridad (*Security Policy Database*, SPD por sus siglas en inglés) y para el procesamiento de entrada (vea figura 60), cada entrada en la SAD es indexada por una dirección IP de destino, tipo de protocolo IPSec y SPI. El SPD es un elemento esencial del proceso SA ya que especifica qué servicios se ofrecerán en los datagramas IP y de qué manera.

Figura 61. **Proceso de salida SA**




Fuente: elaboración propia, con base a Microsoft Visio.

### 4.1.4. Intercambio de claves de internet

Debido a que algunos de los servicios prestados por IPSec requieren del uso de claves encriptadas (valores secretos compartidos), pero se basa en un mecanismo separado, este es el intercambio de claves de internet (internet Key Exchange, IKE por sus siglas en inglés) con el objetivo de enviar claves encriptadas a su destino final. El propósito de IKE, es negociar y proporcionar las claves para autenticar las asociaciones de seguridad de forma protegida.

IPSec se puede configurar sin IKE, pero no es recomendable ya que IKE realza el IPSec, proporcionando características adicionales de flexibilidad y facilidad de configuración. IKE negocia automáticamente las asociaciones de seguridad IPSec y permite la comunicación segura sin necesidad de configuraciones manuales costosas. A continuación se listan alguno de los beneficios proporcionados por IKE:

- Elimina la necesidad de especificar configuraciones manuales.

- Encriptar las claves para intercambiar durante las sesiones de comunicación IPSec.

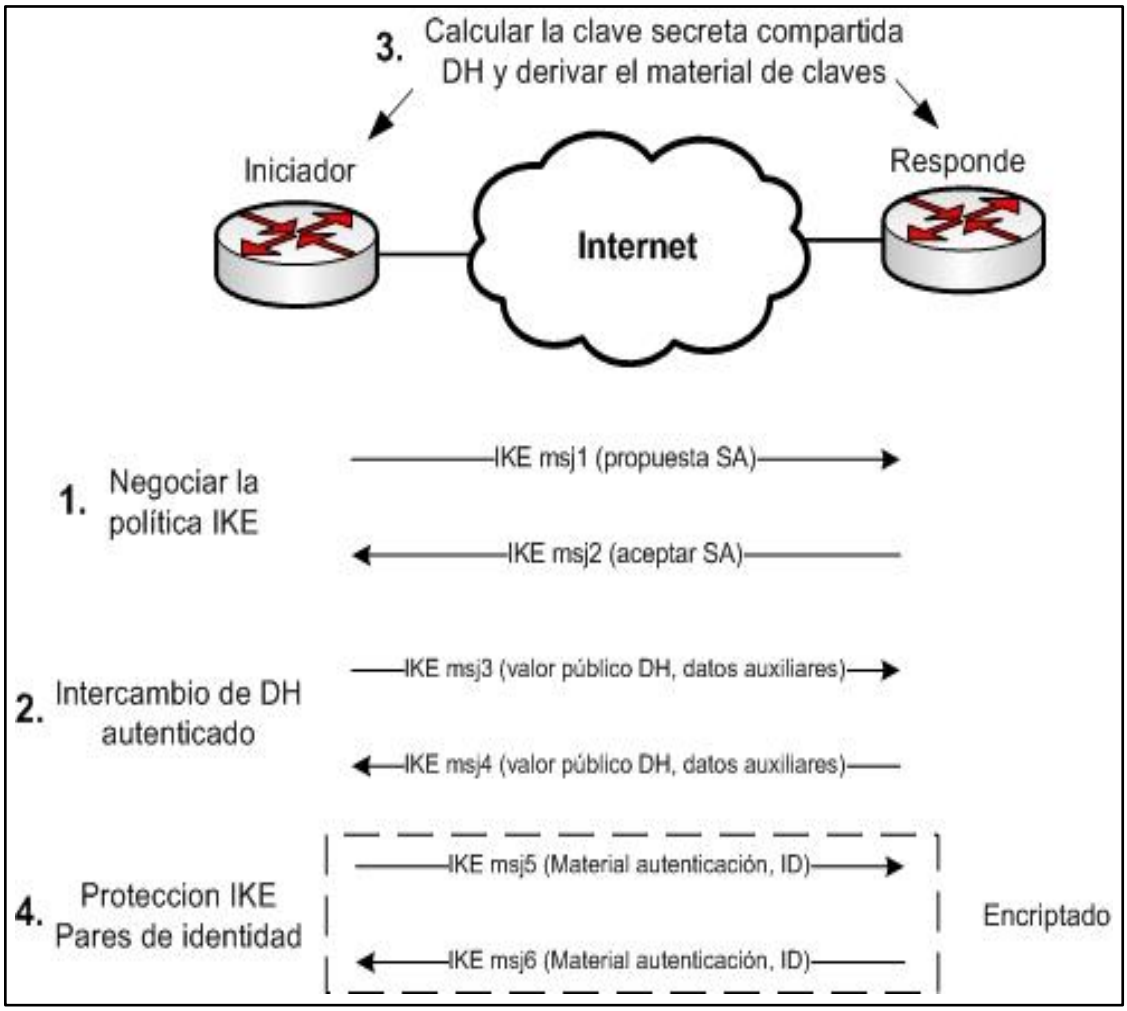
- Permite soporte a certificados de autoridad para una implementación IPSec manejable y escalable.

Existen dos métodos básicos utilizados para establecer IKE, por medio de protocolo de intercambio de llaves *Diffie-Hellman* (DH) los cuales son:

- Modo principal: los dos primeros mensajes son para negociar la política, los dos próximos intercambios de los valores públicos DH y los datos auxiliares, y por último los dos mensajes para autenticar el intercambio de claves DH e ID (vea figura 62).

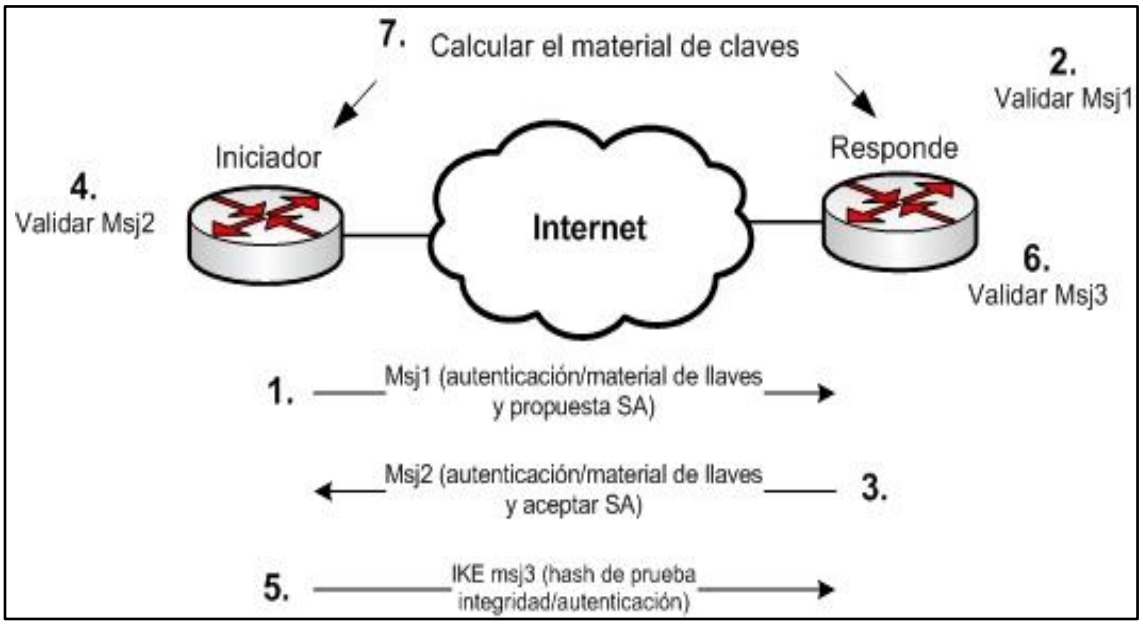
- Modo rápido: el primer mensaje es para la negociación política, el intercambio de los valores públicos DH y los datos auxiliares necesarios para el intercambio y las identidades. El segundo mensaje autentifica la respuesta y el tercer mensaje autentica el iniciador y proporciona una prueba de la participación en el intercambio (vea figura 63).

Figura 62. **IKE modo principal**




Fuente: elaboración propia, con base a Microsoft Visio.

Figura 63. **IKE modo rápido**




Fuente: elaboración propia, con base a Microsoft Visio.

## 4.2. Problemas que afectan tanto a IPv4 e IPv6

Las redes TCP/IP basadas en IPv4 están plagadas de problemas de seguridad ya que están diseñados para trabajar en un ambiente agradable y con conexiones seguras. Cuando estos supuestos no se cumplen como sucede hoy en día, las debilidades en la seguridad en redes IPv4 se manifiestan y pueden ser fácilmente explotados por personas mal intencionadas.

Muchos de los problemas de seguridad son similares tanto para IPv4 como para IPv6, los principales problemas que comparten son: IP *spoofing*, modificación del contenido de paquetes, *replay* y *sniffers*.

El *spoofing* se refiere al uso diferentes técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación. En el caso de la modificación del contenido de paquetes IP es parecido al IP *spoofing*, pero en este caso se modifica el contenido del paquete IP por algún otro contenido malicioso que sea perjudicial para la infraestructura del destinatario.

El *replay* o también llamado ataque de reinyección consiste en la transmisión de datos válida maliciosa o fraudulentamente repetida o retardada. Por último están los *sniffers* que pueden ser una aplicación de software independiente que actúan como espías, examinando el tráfico de red, haciendo una copia de los datos sin redirigir o alteración con fines maliciosos.

## 4.3. Amenazas en IPv6

El foco de atención de personas mal intencionadas hoy en día no son las redes IPv6 sino las redes IPv4, pero con forme pase el tiempo se enfocaran en redes IPv6 para encontrar vulnerabilidades.

Varios proveedores de *hardware* y *software* han publicado errores y/o vulnerabilidades en IPv6, no solo de la tecnología IPv6 sino también en las aplicaciones. Los ataques a las capas inferiores y por encima de la capa de red no se ven afectados por la seguridad que es inherente en IPv6, lo que hace que las personas malintencionadas se centren en la capa de red del modelo OSI (vea figura 64).

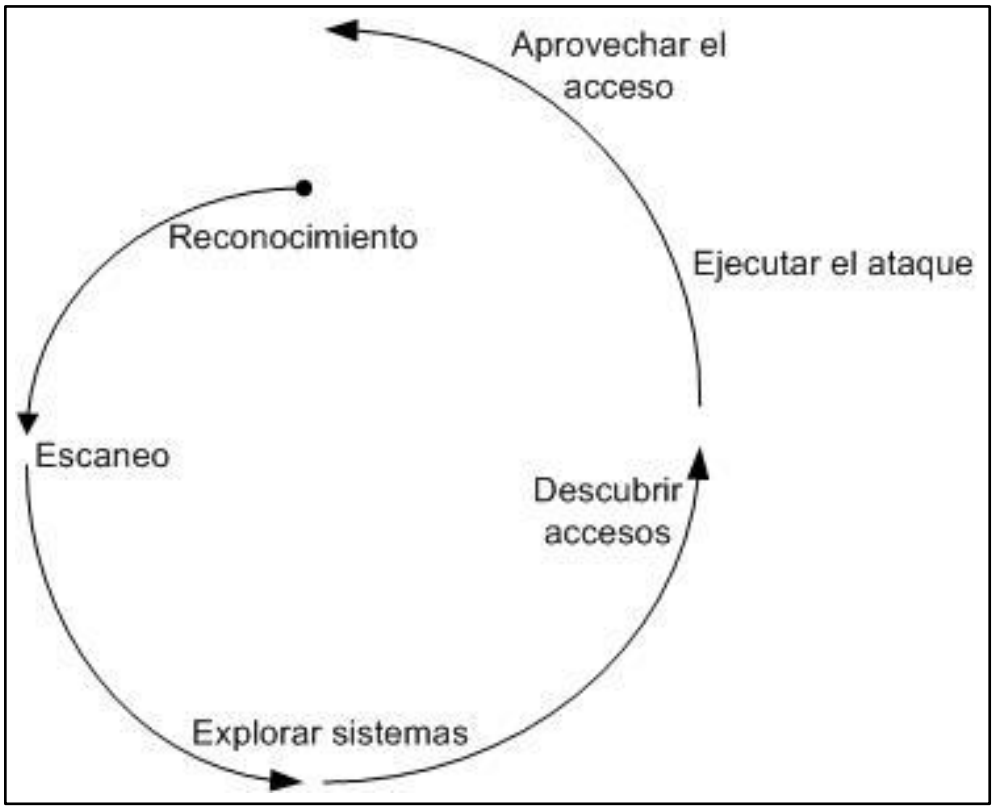
Figura 64. **Modelo OSI**


Fuente: elaboración propia, con base a Microsoft Visio.

Uno de los errores más comunes y es una amenaza importante es el mal diseño de la infraestructura de red IPv6, esto al llegar a oídos de personas ajenas a la entidad puede afectar a la red al infiltrarse, robo de información, ataques frecuentes, y en el peor de los casos afectar de manera irreversible a la red e información de la entidad.

Un ciclo general de cómo se vulnera una red o un sistema de información (vea figura 65), el primer pasó en el ciclo para vulnerar una red es el reconocimiento para ubicar el objetivo del ataque, esto consiste en hacer uso de herramientas especializadas ayuden a localizar objetivos potenciales.

Figura 65. **Ciclo vulnerabilidad redes**




Fuente: *IPv6 security v2*.

El segundo paso a realizar es el escaneo que luego de localizar el objetivo se utilizan técnicas de escaneo para encontrar las vulnerabilidades y por medio de las cuales se concreta el ataque. El tercer paso es explorar sistemas y consiste en utilizar herramientas específicas en las vulnerabilidades. El paso de descubrir accesos está inmerso en el tercer paso ya que se busca como lograr accesos no autorizados para tener acceso de los recursos del sistema atacado. Una vez se descubren los accesos al sistema se ejecuta el ataque que corresponde al paso cinco y por último se aprovecha de una u otra manera el objetivo vulnerado.

La vulneración de una red no siempre es con fines maliciosos, en otros casos el ataque se realiza con fines de investigación para lograr sistemas más seguros. El mayor problema para la seguridad de la redes IPv6 no son los ataques sino son los propios empleados, aunque esto sea difícil de creer en innumerables ocasiones los empleados ponen en peligro información confidencial que luego cae en manos equivocadas y así concretándose los ataques.

## 4.4. Vulnerabilidades y riesgos en la transición a IPv6

La IPv6 inicialmente se diseño para solucionar el espacio limitado de direcciones IPv4 e incluye características de seguridad que proporcionan autentificación confidencial e integración de datos. Sin embargo, la IPv6 no se ocupa de los problemas de disponibilidad del servicio y de la seguridad que pueden derivarse de la transición a IPv6. A todo esto la IPv6 proporciona mayor seguridad a través de IPSec que su antecesora IPv4. Las amenazas que debemos considerar con IPv6 son:

- Equipos que no cumplen con los estándares de seguridad: ¿Realmente el *hardware* soporta *IPv6*? Muchos proveedores ofrecen versiones especiales que soporta IPv6 o requieren una licencia para operar, pero incluso si el soporte a IPv6 está habilitado, se debe tener cuidado y entender la forma en que estos dispositivos funcionan.

- Dispositivos IPv6: las capacidades de configuración automática sin estado que están incorporadas en las direcciones IPv6 permiten a piratas informáticos a establecer un dispositivo capaz de asignar direcciones IP a todos los dispositivos de la red IPv6.

- Vulnerabilidades IPv6: los administradores de redes IPv6 deben ser conscientes de las vulnerabilidades, aunque IPSec se incluye en la definición básica del protocolo, en la práctica se comprueba que algunos ataques de red vulneran la seguridad básica de la IPv6 proporcionada por el IPSec, este no se ocupa de todas las vulnerabilidades de una red IPv6.

- Mecanismos de túneles IPv6: el tráfico IPv6 puede derivarse a través de túneles sobre redes IPv4 utilizando los tipos de túneles descritos en el capítulo 3. Los *hackers* pueden explotar los túneles IPv6 para infiltrarse, a sabiendas de que los paquetes IPv6 pueden parecer tráfico normal IPv4.

- Encriptación IPv6: los piratas informáticos pueden hacer uso de túneles encriptados para realizar ataques directamente al servidor, debido a que los *firewalls* actuales e ISP por lo general no inspeccionan el contenido del tráfico IPv6.

- Ataques distribuidos de denegación de servicio: los ataques *Distributed Denial of Service* (*DDoS* por sus siglas en inglés) de red están diseñados para paralizar a los equipos y los servidores con volúmenes de tráfico mayores a los de su capacidad.

# 5. IMPACTO DE LA TRANSICIÓN A IPV6

El impacto de la IPv6 será importante principalmente en las redes LAN e internet, todos los mecanismos de transición que se han descrito en el presente trabajo de graduación poco a poco serán incluidos las redes, pero no habrá un día específico en donde se realice el cambio a IPv6, el cambio será gradual y llevará tiempo.

La transición a IPV6 no tendrá un impacto inmediato en el uso diario de internet, sin embargo, permitirá ampliar la perspectiva de crecimiento a una mayor cantidad de dispositivos. Algunos entornos se verán más afectados que otros, en algunos casos con poco impacto como en los usuarios finales y otros tendrán el mayor impacto como en el caso de las empresas e ISP. El impacto de la transición conllevará consecuencias tanto económicas, tecnológicas y de seguridad, entre las principales están:

- Incompatibilidad entre IPv4 e IPv6, compartir datos o archivos entre protocolos de internet no es posible sino cuenta con algún mecanismo de transición descrito en el capítulo 3.

- La mayoría de las empresas no ven clara la inversión de tiempo ni de dinero que exige la transición a IPv6, sobre todo en un momento económico complicado.

- IPv6 puede ser un problema para aquellas empresas cuya infraestructura de red no se actualice al nuevo protocolo de internet.

- La infraestructura de red no es moderna en muchas empresas de países subdesarrollados y requiere de un cambio total en gran parte de la misma.

- La seguridad se ve afectada, ya que la transición a IPv6 debe ser llevada acabo por empleados calificados y no poner en riesgo la seguridad.

## 5.1. Usuario final

El usuario final es el menos afectado, debido a que el soporte a IPv6 requiere de pocas configuraciones y/o instalación de actualizaciones. Con respecto a los sistemas operativos hoy en día la mayoría soportan la IPv6 y permiten el uso simultáneo de IPv4 e IPv6. Los principales sistemas operativos tienen soporte para IPv6 que viene activado por defecto y no requiere intervención por parte del usuario final.

El sistema operativo con mejor soporte a IPv6 es *Microsoft Windows* ya que cuenta con las pilas IPv6 más completas en el mercado. Las plataformas *Windows* con soporte a IPv6 son: XP SP1 y posteriores, *Server* 2003, *Vista*, *Server* 2008 y 7. Otras plataformas de *Microsoft Windows* tienen una funcionalidad limitada para IPv6 siendo estas: XP sin SP y 2000 hasta SP1, otras plataformas de *Windows* no mencionadas tienen soporte por terceros, sin soporte de *Microsoft*. En términos generales las características que da soporte *Microsoft* son: autoconfiguración, túnel *6in4*, túnel *6to4*, túnel teredo, túnel ISATAP e IPSec.

El sistema operativo *GNU/Linux* en sus versiones de *kernel* más reciente soportan IPv6 y se pueden encontrar un gran número de utilidades básicas y aplicaciones que funcionan con soporte a IPv6. *Apple MacOS* tiene solamente soporte para doble pila de IPv6.

## 5.2. Empresas

Las empresas deben prepararse para realizar la implementación de IPv6 en su infraestructura de red, la interrogante que surge es ¿Por qué necesito implementar IPv6, sí tengo suficientes direcciones IPv4? Las dos razones principales para realizar el cambio a IPv6 son:

- Los usuarios dentro de la red local en la empresa necesitaran del acceso a contenido en el internet que en un futuro solo estará disponible en IPv6.

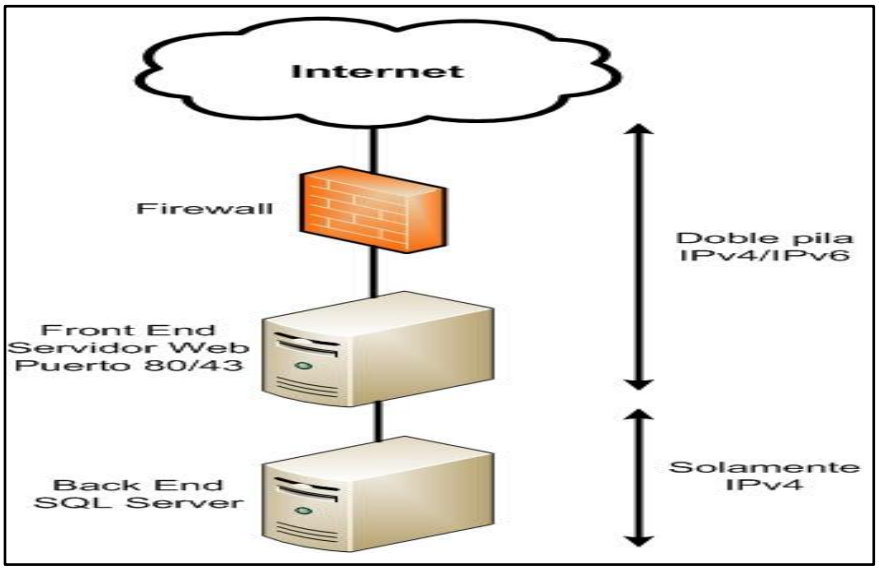
- Los servicios proporcionados por la empresa al exterior deberán tener soporte a IPv6, dado que con seguridad existirán clientes que solo soporten IPv6.

El tiempo de desarrollo e implementación depende del tamaño de la infraestructura de red. Para conocer el impacto de la IPv6 se debe conocer a detalle los equipos y las aplicaciones con que se cuentan, esto suele ser uno de los desafíos más grandes, dado que muchas veces este conocimiento no se tiene, dificultando la evaluación del impacto de la IPv6 en la red empresarial y evaluando el impacto de la implementación en plena transición a IPv6.

Las tareas previas a realizar para lograr una implementación exitosa de IPv6 en la red empresarial son: informarse, conocer el impacto, tener la experiencia de una primera implementación con IPv6 y elaborar una planificación. La mejor forma de iniciar este tipo de actividades complejas, es ir cumpliendo un objetivo específico a la vez.

Uno de los casos más comunes para poder ejemplificar estas situaciones son las empresas de *hosting*, el objetivo principal de estas empresas es que todo su contenido sea accesible tanto para IPv4 e IPv6. El análisis del impacto de la IPv6 de esta empresa incluye que la comunicación dentro de la red local no necesita soporte IPv6, esto incluye conexiones SQL, acceso a servidores, etc. Con este pequeño análisis se determina que solo se necesita implementar la IPv6 en el acceso de la red y el *front end web* (vea figura 66), simplificando la tarea de implementación y disminuyendo los costos.

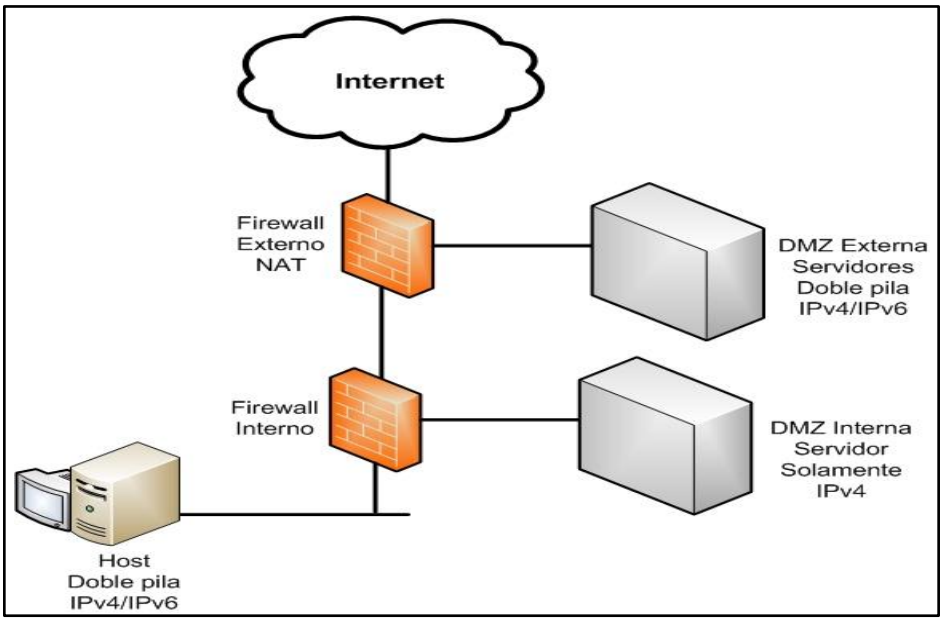
Figura 66. **Infraestructura de red empresa de *hosting***




Fuente: elaboración propia, con base a Microsoft Visio.

El segundo caso a ejemplificar son las empresas con *hosts* que consultan contenido en el internet, en este caso se evalúa que los *host* y servidores externos deben soportar IPv4 e IPv6 por medio de doble pila (vea figura 67). Otros elementos que pueden verse afectados en la implementación de IPv6 dentro de la red empresarial se detallan en la sección 5.5. de este capítulo.

Figura 67. **Infraestructura de red empresa con *host* de navegación**




Fuente: elaboración propia, con base a Microsoft Visio.

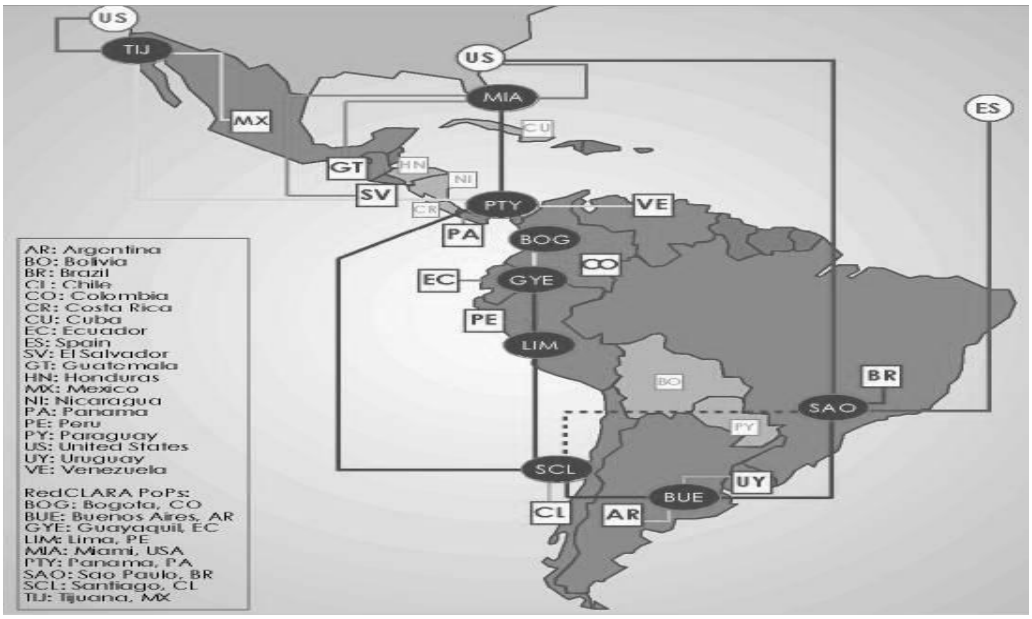
## 5.3. Entidades académicas y de investigación

Este tipo de entidades por lo general abarcan las universidades y centros de investigación, la infraestructura de red de estas entidades son importantes dado que la academia y los investigadores juegan un papel importante en la creación de nuevas tecnologías.

Para tener una idea de la importancia de las entidades académicas y de investigación los primeros despliegues de la IPv6 a gran escala se dan en el marco de redes académicas o de investigación, como *Albilene* (internet 2) en los Estados Unidos, CERNET2 y CST-NET2 en China o WIDE y JGN2 en Japón. En Europa a través de varios proyectos de investigación ha impulsado el avance de IPv6, proyecto tales como 6NET, Euro6IX o *Geant*.

La infraestructura de red en una universidad o centro de investigación es parecido a la que se define en la sección 5.2. Con respecto a los servicios de red que puede brindar se detalla en la sección 5.5. La red académica a la que pertenecen las universidades de Guatemala es la RedClara (vea figura 68), llamada *Research and Education Network* (REN por sus siglas en inglés). Las redes que forman parte de REN tienen soporte a IPv6 hace tiempo.

Figura 68. **REN RedClara**

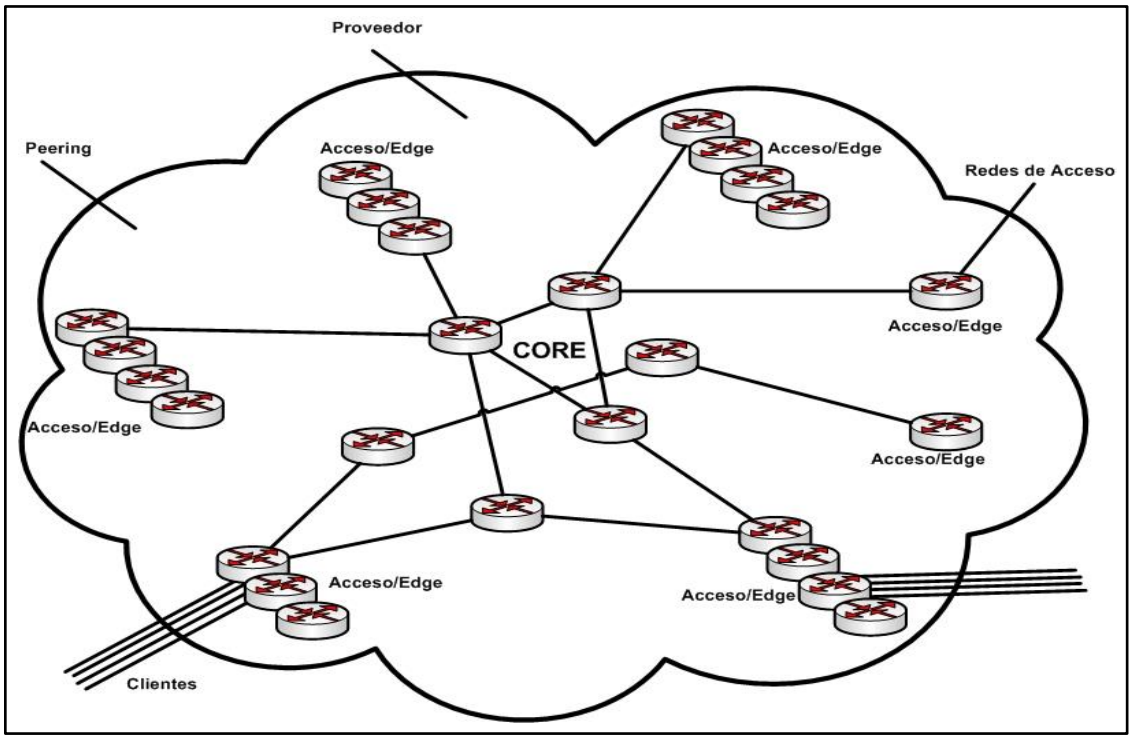



Fuente: estructura de Red Clara.

## 5.4. Proveedores de servicio de internet

En esta sección se da un perspectiva muy general de cómo un ISP hace frente a IPv6. En este entorno el impacto es mayor, dado por la dimensión de la red que administran. En la siguiente figura se ilustra la topología de red típica de un ISP, que tiene a su cargo el *backbone* IP.

Figura 69. **Backbone IP del ISP**




Fuente: elaboración propia, con base a Microsoft Visio.

Para el despliegue de IPv6 en el *backbone* IP existen diferentes alternativas a tomar en cuenta, las cuales dependen del servicio brindado por el ISP, el tamaño de la red y la capacidad del equipo en la infraestructura de red, por lo que la alternativa tomada será decisión de cada administrador de red.

En general lo primero que se debe hacer en la transición a IPv6 en el *backbone* IP es capacitar al personal que está a cargo de la implementación. Es de suma importancia que cada uno de los involucrados conozca cada una de las actividades de la transición a IPv6 y entiendan a detalle cada uno de los servicios, equipos y configuraciones en la red actual y así tomar la mejor decisión durante la planificación e implementación de la IPv6.

Cada ISP deben de solicitar el *pool* de direcciones IPv6 al RIR que le corresponda (vea tabla I), en el caso de Latinoamérica el RIR es LACNIC (vea figura 1). Luego de haber obtenido el *pool* de direcciones y de haber capacitado al personal, se debe analizar de manera oportuna que mecanismo de transición se implementara en el ISP mientras se implementa en su totalidad la IPv6 nativa.

Para los ISP los mecanismos de túneles son los menos recomendados, debido a su poca eficiencia, está alternativas es una solución a corto plazo que no permite la escalabilidad. Los túneles implementados en los ISP hacen que los diagnósticos en la red sean complejos, dificulta la ultimación de los recursos de la infraestructura de red y lo más grave que afectan la disponibilidad de los servicios.

## 5.5. Servicios

El mayor impacto del cambio que con lleva la tecnología IPv6 se da en las capas inferiores del modelo TCP/IP (vea figura 24), los demás protocolos TCP/IP y servicios también se ven afectados si trabajan con direcciones y configuraciones de *hosts*. A continuación detallan el impacto de IPv6 en los principales servicios IPv4, tales como: DHCP, DNS, FTP, NAT, entre otros.

### 5.5.1. *Telnet* y SSH

*Secure Shell* (*SSH* por sus siglas en inglés) facilita la comunicación segura entre sistemas usando una arquitectura cliente/servidor y permitiendo la encriptación. En contra parte *telnet* es un protocolo poco seguro, debido a que se intercambia el usuario y contraseña en texto plano, sin ninguna encriptación.

El impacto de IPv6 sobre estos dos servicios es mínimo, ya que requieren de solo habilitar y/o instalar los respectivos programas para el soporte a IPv6.

### 5.5.2. FTP

*File Transfer Protocol* (*FTP* por sus siglas en inglés) se ha diseñado para trabajar sobre IPv4. En el RFC 2428 se definen las extensiones FTP para IPv6 y NAT, esta especificación permite trabajar sobre IPv4 e IPv6 de manera simultánea. Durante la coexistencia de IPv4 e IPv6 es importante que el servidor FTP negocie el protocolo de internet para realizar la sesión. Con respecto a las aplicaciones para FTP no necesitan de mayor trabajo, dado que la mayoría tienen soporte IPv6. FTP solamente necesita habilitar y/o instalar el soporte, para soportas las solicitudes IPv6.

### 5.5.3. *Mail*

El servicio de *mail* o correo electrónico es el más utilizado hoy en día y sin lugar a duda este servicio debe estar actualizado para soportar IPv6. Este servicio se basa en el modelo cliente/servidor por medio de los protocolos SMTP, POP3 o IMAP4; debido a esto tanto los servidores y los clientes deben de soportar IPv6.

Los proveedores de *software* utilizado en el servidor de correo electrónico han absorbido los pormenores para dar soporte IPv6 a este servicio, por lo que no requiere de tantas configuraciones. El impacto sobre el *mail* es mínimo ya que las aplicaciones han agregado el soporte IPv6 necesario.

### 5.5.4. Multimedia

Con el avance en la transición a IPv6 de las tecnologías multimedia, cada día es más fácil y de bajo o sin ningún costo. Este es el caso de tecnologías tales como video, audio, *streaming* en tiempo real, video llamadas, entre otros. La mayoría de empresas optan por soluciones de terceros lo que facilita en gran medida la administración de red, debido a esto, son muy pocas las empresas que tienen en su infraestructura de red los servicios nativos de multimedia, estas empresas deben habilitar el soporte IPv6 en cada uno de sus servicios multimedia.

### 5.5.5. Web

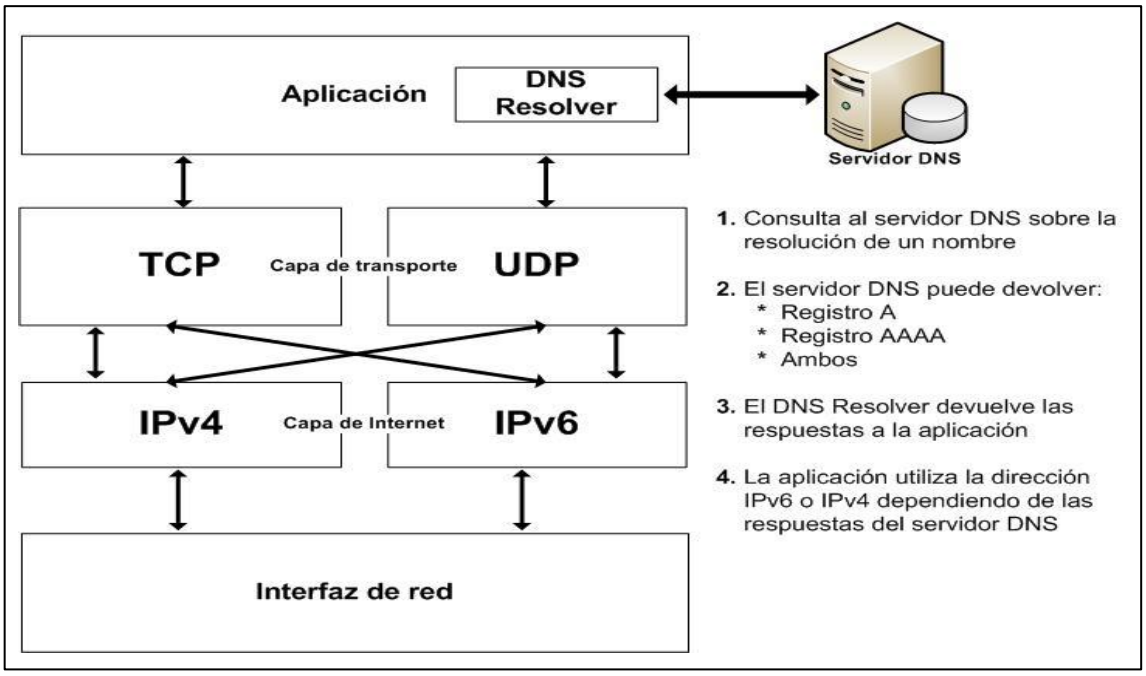
Los sitios web se ven afectados por la conectividad IPv6, dado que los servidores web en algunos casos no soportan IPv6. Por lo general los servidores web soportan ambos protocolos de internet, basta con realizar las respectivas configuraciones para que estén habilitados. El caso más común en la actualidad es el servidor web Apache el cual se recomienda utilizar versiones posteriores a 2.x que vienen con soporte IPv6. Varias iniciativas surgen en el internet para probar la IPv6, este es el caso de Google que tiene habilitado sus servicios IPv6 en http://ipv6.google.com, que al ingresar sabrá si el dispositivo tiene habilitado el soporte IPv6.

### 5.5.6. DNS

El servidor DNS debe considerarse antes de configurar los *hosts*. Los servidores DNS de 32 bits no pueden manejar la resolución de nombres de direcciones IPv6 que constan de 128 bits, este problema es solucionado por los diseñadores de la IETF con la definición del estándar de DNS para IPv6.

El DNS para IPv6 se especifica en el RFC 1886, en donde se define el registro de 128 bits para este DNS, el cual es definido como AAAA y tienen como fin la resolución de los nombres de dominio para las direcciones IPv6. Una aplicación solicita la resolución de nombres por medio del *DNS Resolver* que se encarga de hacer las solicitudes y devolver la dirección correspondiente al nombre de la solicitud (vea figura 70).

Figura 70. **Doble pila y servidor DNS**




Fuente: elaboración propia, con base a Microsoft Visio.

### 5.5.7. NAT

A medida que la IPv6 gane terreno y vaya reemplazando a la IPv4, el proceso de traducción de direcciones será inútil y redundante, por lo que la NAT desaparecerá con el tiempo.

Con la conectividad de extremo a extremo que caracteriza al nuevo protocolo de internet IPv6, prácticamente el NAT desaparecerá. NAT ayudo a prolongar aun más el agotamiento de las direcciones IPv4, sin embargo, con IPv6 existen suficientes direcciones para que todos dispositivos sean públicos en el internet.

### 5.5.8. DHCP

El DHCP para IPv6 es completamente un nuevo protocolo comparado con DHCP para IPv4. Las principales diferencias entre cada DHCP se lista a continuación:

- Los anfitriones siempre tienen una dirección de enlace local que se puede utilizar en las solicitudes, en IPv4 la dirección 0.0.0.0 se utiliza como dirección de origen.

- Los *hosts* en la red puede solicitar varias direcciones IPv6 a la vez.

- El cliente puede enviar múltiples peticiones relacionadas con los mismos o diferentes servidores.

- Existe un mensaje de reconfiguración que los servidores pueden enviarle a los clientes para configurarlos, esta función es opcional.

El DHCP para el protocolo IPv6 se conoce como DHCPv6 y está definido en el RFC 3315. Una de las mejoras en DHCPv6 es la estrategia global para facilitar la administración de los dispositivos IP, incluyendo la configuración del *host*. Existen dos métodos básicos que se definen para la autoconfiguración, los cuales son:

- Autoconfiguración sin estado (*stateless autoconfiguration*): permitir que un *host* se configure sin la ayuda de ningún otro dispositivo.

- Autoconfiguración de estado (*stateful autoconfiguration*): proporciona información de configuración a un *host* por medio del servidor, método utilizado también en DHCPv4.

El impacto de la IPv6 en este servicio es considerable, ya que trabaja directamente con las direcciones IP y la información de configuración básica para los *host* dentro de la red.

### 5.5.9. *Firewall*

Con la llegada de la IPv6 el *firewall* afecta la comunicación dado que las reglas no permiten IPv6 en la mayoría de redes, es por ello, las medidas tomadas es dejar pasar el tráfico IPv6 que llega al *firewall* sin mayor restricción, sin embargo, es una mala práctica dado que el tráfico pueda no ser confiable y pueden ocasionar problemas serios en la infraestructura de red.

En el *firewall* con el tráfico IPv6 la mejor práctica a realizar es definir las reglas pertinentes por parte del administrador de red de acuerdo a sus necesidades y así evitar problemas. Un *firewall* no procesa todos los campos dentro de un paquete de la misma manera, algunos de los campos u opciones de cabecera se pueden evaluar de forma autónoma y tomar medidas al respecto de inmediato. Este tipo de función de limpieza de paquetes se puede aplicar a todos los paquetes en todos los ámbitos. Otros campos deben ser evaluados como parte de un conjunto de condiciones definidas en una o varias políticas a configurar y definir prioridades en el filtrado del *firewall*.

# CONCLUSIONES

1. El agotamiento de las direcciones IPv4 y la seguridad del actual protocolo de internet, son las principales problemáticas, debido a esto es necesario un cambio a IPv6. IPv6 fue diseñada para proveer suficientes direcciones IP y hacen de la seguridad algo obligatorio, y no opcional como pasa con IPv4.

2. La planificación propuesta está definida en el RFC 5211, donde se define un plan de transición en el internet desde un modelo de conectividad basado en IPv4 a un modelo de conectividad basado en IPv6 propuesto por la IETF. Los dos enfoques descritos son el enfoque de adentro hacia fuera y el enfoque de afuera hacia adentro, cualquier de los dos que se tome ayuda a la transición a la IPv6.

3. En general los mecanismos de transición, se agrupan en tres formas: doble pila, traducción y túnel. La doble pila, como su nombre indica, literalmente, mantiene dos pilas de protocolos: el IPv4 e IPv6 que operan en paralelo. La traducción se refiere a la conversión directa de los protocolos IPv4 e IPv6. La traducción se considera transparente para el usuario final, es decir, el usuario no tiene la menor idea de que se traduce de un protocolo a otro para garantizar la comunicación.

Y los túneles se pueden considerar técnicamente como la transferencia de un protocolo encapsulado dentro de otro protocolo entre dos nodos y/o sistemas finales. La encapsulación del protocolo se realiza en la entrada del túnel y desencapsulación se realiza en el punto de salida del túnel.

4. La IPv6 es más segura que la IPv4, dado que en la IPv4 la seguridad es opcional, mientras que en la IPv6 la seguridad es inherente al nuevo protocolo de internet, pero existen problemas que comparten ambos protocolos de internet.

   Entre las vulnerabilidades y riesgos en la transición a IPv6 están el *hardware* que no cumple con los estándares de seguridad, mecanismos de túneles mal implementados que ayudan a infiltraciones en la red, implementar una débil encriptación en IPv6, *malware* más sofisticado, entre otras vulnerabilidades y riesgos existentes.

5. El impacto de la transición a IPv6 en los diferentes entornos de trabajo es inevitable, ya sea un impacto donde los cambios a realizar sean considerables o donde el impacto sea mínimo como en el caso de los usuario finales, pero este impacto se puede minimizar aun más realizando una transición planificada y lo más pronto posible, dado que los costos se elevan si se va postergando el afrontar el cambio a IPv6.

# RECOMENDACIONES

1. A los administradores de red afrontar el tema de la IPv6 lo más pronto posible y crear una planificación acorde a sus necesidades e infraestructura de red para que la transición a la IPv6 sea exitosa y los costos sean mínimos.

2. Animar a las entidades con presencia en el internet para aprender y comprender los pasos que debe dar para migrar a IPv6, y a seguir un plan de despliegue coherente que asegure la conexión desde ahora, tanto para IPv4 e IPv6.

3. Favorecer la difusión y formación en IPv6 en la educación superior, proveyendo de cursos que den el conocimiento adecuado para afrontar el cambio a IPv6.

4. Se deben crear, apoyar e impulsar las iniciativas para incrementar las actividades de investigación por parte de la industria y la educación guatemalteca, aportando conocimiento al tema de la IPv6.

# BIBLIOGRAFÍA


1. 6Deploy. *IPv6 Security*. [en línea] <http://www.6deploy.eu/tutorials/111-6deploy-security-short_v0_3.pdf>. [Consulta: 02 de junio de 2011].

2. AHROUCH, A. A.; EZZINE, S. *IPv4 to IPv6 Migration*. [en línea] [ref. 02 de julio de 2004.] <http://ftp.coolmax.one.pl/pub/docs/ipv6/IPv4toIPv6 migration.pdf>.

3. AHUATZIN SÁNCHEZ, Gerardo L. *Teoría y métodos de transición IPv4 e IPv6. Desarrollo de un esquema de traducción de direcciones IPv6-IPv4-IPv6*. Puebla: Universidad de las Américas Puebla, 2005. 131 p.

4. *Asignación y estadísticas de enrutamiento*. *IPv6 act now*. [en línea] <http://www.ipv6actnow.org/info/statistics/>. [Consulta: 02 de junio de 2011.].

5. BAKER, Fred. *IPv6 Transition and Scalable Deployment*. [en línea] <http://www.oucs.ox.ac.uk/its3/seminar-notes/2009-01-26_Cisco_IPv6_transition.pdf>. [Consulta: 09 de julio de 2011].

6. BLANCHET, Marc; PARENT, Florent. *IPv6 transition mechanisms*. [en línea] <http://edu.nida.or.kr/other/summit/UK2000/PDF/MBlanchet_IPv6-transition-mec_v1.01.pdf>. [Consulta: 11 de julio de 2011].

7. BT Diamond IP. 2007. *IPv4-to-IPv6 transition strategies*. [en línea] [ref. febrero de 2007.]. Disponible en Web: <http://www.networkworld.com/whitepapers/nww/pdf/bt_wp_IPv6_Transition_Strategies.pdf>.

8. CAICEDO, Carlos E.; JOSHI, James B.D.; TULADHAR, Summit R. *IPv6 Security Challenges*. [en línea] <http://www.v6summit.com/Tutorial/CLASSROOMTUTORIAL_ROUTAGE_SECURITY.pdf>. [Consulta: 21 de julio de 2011].

9. CANNON, Robert. *Potential Impacts on Communications From IPv4 Exhaustions & IPv6 Transition*. Washington D. C.: FCC Staff Working, 2010. 27 p.

10. CARTER, Earl. *IPv6 Security Considerations*. [en línea] <http://www.txv6tf.org/wp-content/uploads/2010/08/Carter-Tutorial-IPv6-Security-Texas.pdf>. [Consulta: 25 de julio de 2011].

11. CHOI, Y.B: et al. *Introduction to IPSEC (internet Protocol Security)*. [en línea] <http://ettrends.etri.re.kr/PDFData/14-6-6.pdf>. [Consulta: 23 de julio de 2011].

12. CHOWN, Tim; BONNESS, Olaff; LADID, Latif. *Deliverable D4 Final Project Report*. [en línea] <http://www.cu.ipv6tf.org/casos/ipv6tf-sc_pu_d4v1_7.pdf>. [Consulta: 26 de julio de 2011].

13. CHOWN, Tom. *IPv6 Transition and Integration with IPv4*. [en línea] <http://www.6diss.org/tutorials/transitioning.pdf>. [Consulta: 26 de junio de 2011].

14. CICILEO, Guillermo; et al. *IPv6 para Todos: guía de uso y aplicación para diversos entornos*. Buenos Aires: internet Society, 2009. 151 p.

15. CIO COUNCIL. *IPv6 Transition Guidance*. [en línea] <http://ebookbrowse.com/ipv6-transition-guidance-doc-d177351961>. [Consulta: 26 de junio de 2011].

16. Cisco Systems, Inc. *Cisco Network Address Translation (NAT)* . [en línea] <http://www.cisco.com/en/US/tech/tk648/tk361/tk438/tsd_technology_support_sub-protocol_home.html>. [Consulta: 26 de junio de 2011].

17. ————————. *Implementing IPsec in IPv6 Security*. [en línea] <http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide /ip6-ipsec.html>. [Consulta: 06 de julio de 2011.].

18. ————————. *Cisco IOS IPv6 Configuration Guide*. [en línea] [ref. 6 de agosto de 2008.]. Disponible en Web: <http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_4/ipv6_12_4_book.html>.

19. ————————. *Implementing IPv6*. [en línea] <http://www.cisco.com/web/solutions/trends/ipv6/implement.html>. [Consulta: 06 de julio de 2011.].

20. ————————. *Implementing NAT Protocol Translation. Implementing IPv6 for Cisco IOS Software*. [en línea] <http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-nat-trnsln.html>. [Consulta: 06 de julio de 2011.].

21. ————————. *Implementing IPv6 in the enterprise network*. [en línea] [ref. 20 de septiembre de 2011.] Disponible en Web: <http://www.hh.se/download/18.2515361d13513694471800015309/1330503857473/IPv6_VT2012.pdf >.

22. ————————. *Implementing NAT protocol translation*. [en línea] [ref. 04 de julio de 2011.]. Disponible en Web: <http://solomon.ipv6.club.tw/IPv6/cisco_natpt.pdf>.

23. CURRAN, John. *An internet Transition Plan RFC 5211*. [en línea] <http://www.nanog.org/meetings/nanog44/presentations/Tuesday/Curran_transitionRFC5211_N44.pdf>. [Consulta: 08 de junio de 2011].

24. DAVIES, Joe. *Understanding IPv6 Transition Technologies*. [en línea] <http://sitpug.com/Presentations/UnderstandingIPv6_TransTech.pdf>. [Consulta: 07 de junio de 2011].

25. Department of Computer Science National Chung-Hsing University. 2005. *Managing the co-existing network of IPv6 and IPv4 under various transition mechanisms*. [en línea] 2005. [ref. 14 de junio de 2011.]. Disponible en Web: <http://www.csis.pace.edu/~ctappert/dps/d861-06/pres-ipv6-1.pdf>.

26. DROMS, Ralph. *IPv6 Transition Work in the IETF*.: [en línea] <http://tools.ietf.org/html/draft-arkko-ipv6-transition-guidelines-14>. [Consulta: 22 de junio de 2011].

27. DUQUE, Sivia; VALLEJO, David. *Mecanismos de transición de IPv4 a IPv6*. [aut. libro] Universidad Técnica del Norte. Análisis del protocolo IPv6 su Evalución y Aplicabilidad. 120 p.

28. El espectador.com. *En el 2015 habrá un dispositivo móvil por habitante en el mundo*. [en línea]. [ref. 1 de febrero de 2011.]. Disponible en Web: <http://www.elespectador.com/tecnologia/articulo-248363-2015-habra-un-dispositivo-movil-habitante-elmundo>.

29. ELMORE, Hillary A.; CAMP, Jean; STEPHENS, Brandon P. *Diffusion and Adoption of IPv6 in the United States* . [en línea] <http://www.cs.indiana.edu/ftp/techreports/TR661.pdf>. [Consulta: 07 de julio de 2011].

30. Eurescom. *Introduction to IPSec in IPv6*. Alemania: Telenor AS, 2001. 38 p.

31. *Federal CIO Council Architecture and Infrastructure Committee*. 2006. [en línea]. [ref. febrero de 2006.]. Disponible en Web: <http://www.cio.gov/documents/IPv6_Transition_Guidance.doc>.

32. GARCÍA MARTÍNEZ, Cesar. *Doble pila mecanismo de transición IPv6*. [en línea] <http://www.tlalpan.uvmnet.edu/oiid/download/Mecanismo%20de%20Transici%C3%B3n_04_ING_ISC_PIT_E.pdf>. [Consulta: 14 de julio de 2011].

33. GLAGIANO, *Roque. Planificando IPv6*. [en línea] <http://lacnic.net/documentos/lacnicxii/presentaciones/Planificacion.pdf>. [Consulta: 16 de julio de 2011].

34. Global Technology Resources Inc. *IPv6 security v2*. [en línea] [ref. 10 de diciembre de 2010.]. Disponible en Web: <http://www.txv6tf.org /wp-content/uploads/2010/08/Scott-Hogg-IPv6-Security.pdf>.

35. Gobierno de España. *IPv6 Protocolo de internet Versión 6*. [en línea] <http://www.ipv6.es/es-ES/Paginas/Index.aspx>. [Consulta: 24 de junio de 2011.].

36. Gobierno de Hong Kong. *IPv6 Security*. [en línea] <http://www.infosec.gov.hk/english/technical/files/ipv6s.pdf>. [Consulta: 26 de junio de 2011.].

37. HOAGLAND, James. *The Teredo Protocol:Tunneling Past Network Security and Other Security Implications*. Cupertino: Symantec, 2007. 36 p.

38. HOGG, Scott. *Internet Protocol verion 6 - The Next Generation Protocol*. [en línea] <http://www.garykessler.net/library/ipv6_exp.html>. [Consulta: 28 de junio de 2011.].

39. HOVELL, Peter; et al. *Deliverable D3.4 IPv6 Overall Status*. [en línea] <http://cordis.europa.eu/search/index.cfm?fuseaction=result.document&RS_LANG=IT&RS_RCN=8294117&q=>. [Consulta: 24 de junio de 2011.].

40. iABG & EADS. *IPv6 security models and dual-stack (IPv4/IPv6) implications*. [en línea] <http://ec.europa.eu/information_society/policy/ipv6/docs/studies/executive_summary_v1.3_en.pdf>. [Consulta: 25 de junio de 2011.].

41. IEEE USA. *Next Generation Internet: IPv4 Address Exhaustion, Migration Strategies and Implications for the U.S*. [en línea] <http://www.ieeeusa.org/policy/whitepapers/IEEEUSAWP-IPv62009.pdf>. [Consulta: 22 de junio de 2011.].

42. IEFT. RFC 2766 - *Network Address Translation - Protocol Translation (NAT-PT)*. [en línea] [ref. febrero de 2000.]. Disponible en Web: <http://www.ietf.org/rfc/rfc2766.txt>.

43. ————————. *Framework for IPv4/IPv6 Translation*. [en línea] [ref. 17 de agosto de 2010.]. Disponible en Web: <http://www.tools.ietf.org/html/draft-ietf-behave-v6v4-framework-10>.

44. ————————. *RFC 1883 - Internet Protocol, Version 6 (IPv6) Specification*. [en línea] [ref. diciembre de 1995.]. Disponible en Web: <http://www.ietf.org/rfc/rfc1883.txt>.

45. ————————. *RFC 1886 - DNS Extensions to support IP version 6*. [en línea] [ref. diciembre de 1995.]. Disponible en Web: <http://www.ietf.org/rfc/rfc1886.txt>.

46. ————————. *RFC 2765 - Stateless IP/ICMP Translation Algorithm (SIIT)*. [en línea] [ref. febrero de 2000.]. Disponible en Web: <http://www.ietf.org/rfc/rfc2765.txt>.

47. ————————. *RFC 2767 - Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS)*. [en línea] [ref. febrero de 2000.]. Disponible en Web: <http://www.ietf.org/rfc/rfc2767.txt>.

48. ————————. *RFC 2767 - Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS)*. [en línea] [ref. febrero de 2000.]. Disponible en Web: <http://www.ietf.org/rfc/rfc2767.txt>.

49. ————————. *RFC 2893 - Transition Mechanisms for IPv6 Hosts and Routers*. [en línea] [ref. agosto de 2000.]. Disponible en Web: <http://www.ietf.org/rfc/rfc2893.txt>.

50. ————————. *RFC 3142 - An IPv6-to-IPv4 Transport Relay Translator*. [en línea] [ref. junio de 2001.]. Disponible en Web: <http://www.ietf.org/rfc/rfc3142.txt>.

51. ————————. *RFC 3315 - Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*. [en línea] [ref. julio de 2003.]. Disponible en Web: <http://www.ietf.org/rfc/rfc3315.txt>.

52. ————————. *RFC 3338 - Dual Stack Hosts Using "Bump-in-the-API" (BIA)*. [en línea] [ref. octubre de 2002.]. Disponible en Web: <http://www.ietf.org/rfc/rfc3338.txt>.

53. ————————. *RFC 4213 - Basic Transition Mechanisms for IPv6 Hosts and Routers*. [en línea] [ref. octubre de 2005.]. Disponible en Web: <http://www.ietf.org/rfc/rfc4213.txt>.

54. ————————. *RFC 4380 - Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs).* [en línea] [ref. febrero de 2006.]. Disponible en Web: <http://www.ietf.org/rfc/rfc4380.txt>.

55. ————————. *RFC 4472 - Operational Considerations and Issues with IPv6 DNS*. [en línea] [ref. abril de 2006.]. Disponible en Web: <http://www.ietf.org/rfc/rfc4472.txt>.

56. ————————. *RFC 5211 - An internet Transition Plan*. [en línea] [ref. julio de 2008.]. Disponible en Web: <http://www.ietf.org/rfc/rfc5211.txt>.

57. ————————. *RFC 2428 - FTP Extensions for IPv6 and NATs.* [en línea] [ref. septiembre de 1998.]. Disponible en Web: <http://www.ietf.org/rfc/rfc2428.txt>.

58. IFTF. *RFC 1752 - The Recommendation for the IP Next Generation Protocol*. [en línea] [ref. enero de 1995.]. Disponible en Web: <http://www.ietf.org/rfc/rfc1752.txt>.

59. INTECO-CERT. *Informe sobre las implicaciones de seguridad en la implantación de IPv6*. España: Iteco, 2010. 19 p.

60. Inter Agency Policy & Projects Unit, tasmanian. *Tasmanian Government IPv6 Transition Strategy*. [en línea] <http://www.egovernment.tas.gov.au/__data/assets/pdf_file/0003/77952/IPv6_transition_strategy.pdf>. [Consulta: 21 de junio de 2011.].

61. Ipswitch. *Ipswitch poll shows disturbing gap in IPv6 readiness among enterprise networks*. [en línea] [ref. 10 de mayo de 2011.]. Disponible en Web: <http://www.whatsupgold.com/resources/pressDetail.aspx?id=124>.

62. IPv6 act now. *Asignación y estadísticas de enrutamiento*. [en línea] [ref. 02 de junio de 2011.]. Disponible en Web: <http://www.ipv6actnow.org/info/statistics/>.

63. IPv6 Chile. *Proyecto IPv6 para Chile*. [en línea] <http://www.ipv6.cl/>. [Consulta: 19 de julio de 2011.].

64. ————————. *Proyecto IPv6 para Chile fase de inteligencia de mercados y competitiva informe de tendencias N°3*. [en línea] [ref. 10 de abril de 2011.]. Disponible en Web: <http://www.ipv6.cl/system/files/Informe-Tendencias-IPv6-marzo-2011.pdf>.

65. IPv6 Task Force. *Análsis y recomendaciones para la transición a la nueva generación del protocolo de internet (IPv6).* [en línea] <http://www.spain.ipv6tf.org/public/IPv6TF_Spain_v10.pdf>. [Consulta: 15 de julio de 2011.].

66. ————————. *IPv6 transition – industry best practices*. [en línea] [ref. 02 de febrero de 2006.]. Disponible en Web: <http://www.moonv6.org/lists/att-0539/NAv6TF_IPv6_Transition_Best_Industry_Practices_20060202.pdf>.

67. IPv6.com, *Inc. IPv6*. [en línea]. <http://ipv6.com/>. [Consulta: 24 de junio de 2011.].

68. Juniper Networks. *Guide for Federal Agencies Transitioning to IPv6*. [en línea] <http://www.juniper.net/us/en/local/pdf/validation-reports/ipv6-world-report-v1-exec.pdf>. [Consulta: 17 de julio de 2011.].

69. KAEO, Merike. *IPv6 Security*. Christchurch, Nueva Zelanda: Double Shot Security, 2008. p. 1-5.

70. LACNIC. *LACNIC portal IPv6*. [en línea] [ref. 12 de Mayo de 2011.]. Disponible en Web: <http://www.portalipv6.net/es/ipv6-2011>.

71. LIOY, Antonio. *Security Features of IPv6*. Torino: Politecnico di Torino, 1997. 200 p.

72. MALIHA, Ayman; et al. *IPv4 to IPv6 Transition Technologies*. Gaza: Computer Engineering College, 2000. 123 p.

73. NIC Chile Research labs. *IPv6 Chile*. [en línea]. <http://www.ipv6.cl/>. [Consulta: 14 de agosto de 2011.].

74. NTT Communications. 2009. *IPv6 transition mechanisms and strategies*. [en línea] [ref. 12 de abril de 2009.]. Disponible en Web: <http://www.rmv6tf.org/2009-IPv6-Summit-Presentations/Chuck%20Sellers%20-%20090421-IPv6-Transition-Mechanisms-Sellers.pdf>.

75. ————. IPv6: *Not if*, when. U.S. [en línea]. <http://www.us.ntt.net/downloads/papers/Network_World_Executive_Guide_IPv6.pdf>. [Consulta: 11 de agosto de 2011.].

76. ORACLE. *Planificación de una red IPv6 (tareas)*. [en línea] 2010. [ref. 23 de Mayo de 2011.]. Disponible en Web: <http://download.oracle.com/docs/cd/E19957-01/820-2981/ipv6-planning-1/index.html>.

77. PATEL, Jaimi*. The Migration from IPv4 to IPv6*. Italia: Global IP Summit, 2000. 250 p.

78. PALET, Jordi. *IPv6 para España: Agotamiento de IPv4 o Transición a tiempo a IPv6 para el adecuado crecimiento de la Banda Ancha*. Madrid: The IPv6 Company Consulintel, 2011. 32 p.

79. ————————. *La innovación con IPv6 frente al agotamiento de IPv4*. [en línea]. <http://www.ipv6summit.com.mx/documentos/JordiPalet_Consulintel.pdf>. [Consulta: 29 de agosto de 2011.].

80. PEREYRA MOLINAS, Nicolás. *Blog de Nicolás Pereyra Molinas*. [en línea]. <http://npereyra.ywork.net/>. [Consulta: 10 de agosto de 2011.].

81. POTYRAK, Casimir A. 2007. *Firewall Design Considerations for IPv6*. Washington: SNAC, 2007. 50 p.

82. PUNITHAVATHANI, D. Shalini; SANKARANARAYANAN, K. *IPv4/IPv6 Transition Mechanisms.* s.l. India: EuroJournals, 2009. 125 p.

83. RedClara. *Estructura de Red Clara*. [en línea] [ref. junio de 2008.]. Disponible en Web: <http://culturadigital.br/redeclara/2010/01/19/potencial-red-de-cooperacion-audiovisual-en-america-latina-2/>.

84. ROONEY, Tim. *IPv4-to-IPv6 Transition Strategies.* [en línea]. <http://www.usipv6.com/6sense/2004/oct/ipv6_transition_strategies.pdf>. [Consulta: 21 de agosto de 2011.].

85. RTI International. *IPv6 Economic Impact Assessment.* [en línea] [ref. octubre de 2005.]. Disponible en Web: <http://www.6journal.org/archive/00000282/01/report05-2.pdf>.

86. SOLTILLO, Samuel. 2006. *IPv6 Security Issues*. [en línea]. <http://pdf.aminer.org/000/291/395/automatic_configuration_of_ipv_tunneling_in_a_dual_stack_host.pdf>. [Consulta: 29 de agosto de 2011.].

87. TechNet Microsoft. *IPv6 Transition Technologies*. [en línea] <http://technet.microsoft.com/en-us/library/bb726951.aspx>. [Consulta: 02 de septiembre de 2011.].

88. ————————. 2007. *Teredo Overview*. [en línea] <http://technet.microsoft.com/en-us/library/bb457011.aspx>. [Consulta: 05 de septiembre de 2011.].

89. ————————. *Características de seguridad para IPv6.* [en línea] [ref. 02 de julio de 2011.]. Disponible en Web: <http://technet.microsoft.com/es-es/library/cc775898(WS.10).aspx>.

90. The 6net Consortium. *An IPv6 Deployment Guide*. España: 6net, 2005. 423 p.

91. VERDEJO ALVAREZ, Gabriel; BORRELL VIADER, Joan. *El protocolo IPv6 y sus extensiones de seguridad IPSec*. [en línea]. <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>. [Consulta: 20 de agosto de 2011.].

92. VYNCKE, Eric. *IPv6 Security Best Practices*. [en línea]. <http://www.cisco.com/web/SG/learning/ipv6_seminar/files/02Eric_Vyncke_Security_Best_Practices.pdf>. [Consulta: 05 de agosto de 2011.].

93. WADDINGTON, Daniel G.; CHANG, Fangzhe. 2002. *Realizing the Transition to IPv6. Bell Research Laboratories*. [en línea]. <http://www.researchgate.net/publication/3196737_Realizing_the_transition_to_IPv6>. [Consulta: 15 de agosto de 2011.].

94. XIA, Haidong; BOUND, Jim; POUFFARY, Yanick. *The Evaluation of DSTM: An IPv6 transition mechanism*. [en línea]. <http://people.cs.pitt.edu/~hdxia/papers/icn2006_xia.pdf>. [Consulta: 15 de noviembre de 2011.].