PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIONES

"PLANIFICACIÓN DE PROCESOS PARA LA MIGRACIÓN DEL PROTOCOLO IPV4 A IPV6 PARA LA CONTINUIDAD DEL SERVICIO EN LOS ISP's."

DIANA DEL PILAR PANTOJA CHUGA

TRABAJO PREVIO LA OBTENCIÓN DEL TÍTULO DE:

MAGISTER EN REDES DE COMUNICACIONES

Quito – Abril 2016

DEDICATORIA

Este proyecto de investigación dedico a DIOS, por darme vida, sabiduría e inteligencia para permitirme subir un escalón más profesionalmente y guiarme por el camino correcto.

SEBASTIAN ALEJANDRO mi hijo, por ser mi fuente de inspiración y motivación por el cual quiero seguirme preparando y superando, quien me ha inspirado a ser una Madre ejemplar siguiendo los buenos valores de la vida.

A mis padres ANIBAL PANTOJA y VIRGINIA CHUGA, quienes han velado por mi bienestar y educación a lo largo de mi vida, a lo que considero la mejor herencia recibida de ellos, gracias por su gran apoyo moral e incondicional en todos los momentos y etapas de mi vida, al culminar esta nueva etapa quiero demostrar gratitud por la confianza depositada ya que he aprendido los que ahora son mis valores y principios, mismos que enseñaré a mi hijo para conseguir todas las metas que en la vida me proponga.

A mis hermanos RAMIRO y LENIN por estar siempre a mi lado, con su apoyo y con su gran amor, brindándome siempre palabras de aliento para no desmayar y culminar este nuevo reto profesional.

A mi sobrino RICHARD, por estar siempre conmigo apoyándome en los buenos y malos momentos y darme palabras de aliento para culminar mi carrera.

AGRADECIMIENTO

Mi Agradecimiento en primer lugar a mi Dios por permitirme culminar con éxito este nuevo compromiso y poder subir un escalón más profesionalmente, gracias por darme la vida y el don de la lucha y perseverancia para llegar hasta el final de esta carrera.

Al asesor Gustavo Chafla, PHD, ya que por su conocimiento, experiencia y esfuerzo dedicado a este proyecto he logrado desarrollar con éxito mi plan de tesis.

A la UNIVERSIDAD CATOLICA DEL ECUADOR, por recibirme y abrirme las puertas y permitirme adquirir nuevos conocimientos en la Maestría y formarme profesionalmente.

Agradezco a mis Padres, a mi hijo, a mis hermanos y mi sobrino porque han sido mi guía en este largo caminar, gracias por sus consejos, apoyo y sobre todo por su gran ejemplo, que me han permitido seguir y luchar para obtener este título, también quiero agradecer a las personas que han formado parte de mi vida profesional, gracias por su amistad, compañía y apoyo, solo juntos se llega así a la terminación de etapas importantes en nuestras vidas.

PRESENTACION

Señores del Jurado:

Dando cumplimiento a las normas del Reglamento de elaboración y sustentación de Tesis de la Facultad de Ingeniería, sección de Postgrado de la Pontificia Universidad Católica del Ecuador, para elaborar la tesis de Maestría, se presenta el trabajo de investigación denominado:

"**PLANIFICACIÓN DE PROCESOS PARA LA MIGRACIÓN DEL PROTOCOLO IPV4 A IPV6 PARA LA CONTINUIDAD DEL SERVICIO EN LOS ISP's.**".

En el tema de investigación se describe cómo deben actuar los ISP para la migración y coexistencia de los dos protocolos, analizando los diferentes tipos de mecanismos más recomendados con sus funcionalidades y ventajas.

De igual forma una descripción y guía con la que los proveedores deben tomar en cuenta para la migración como la realización de un plan económico de inversión, capacitación de personal y sobre todo realización de inventarios tanto de software y hardware que soporten IPv6.

Señores miembros del jurado en espera que este proyecto sea evaluado y merezca su aprobación.

Atentamente.

Diana del Pilar Pantoja Chuga.

Autor

RESUMEN EJECUTIVO

Esta tesis se realizó con el fin de aportar con una guía informativa para que los Proveedores de Servicio de Internet puedan saber cómo actuar frente a la coexistencia entre los protocolos IPv4-IPv6, tomando en cuenta la información, funcionalidad, ventajas y desventajas de cada uno de los mecanismos más recomendados internacionalmente y utilizados para la ejecución del proceso de migración.

Capítulo I, describe las razones por las cuales se desarrolla la presente investigación, tales como: justificación, antecedentes y objetivos del proyecto de migración.

Capítulo II, detalla los conceptos, ventajas, desventajas, direccionamiento y diferencias de los métodos más utilizados y recomendados a nivel internacional.

Capítulo III, se da a conocer el funcionamiento, características e inconvenientes de los métodos más recomendados para la migración y coexistencia de los protocolos IPv4 e IPv6.

Capítulo IV, se especifica cómo deben actuar los IPS para iniciar la migración de los dos protocolos con una planificación, un plan económico de inversión, capacitación al personal encargado en cada área, realización inventarios de software y hardware, realizar un calendario de actividades para llevar a cabo el desarrollo de migración.

Finalmente en el capítulo V, se establece las conclusiones y recomendaciones a las que se ha llegado luego de finalizar el estudio sobre migración de IPv4 a IPv6 planteados como objetivo de tesis.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPÍTULO I

DEFINICIÓN DEL PROYECTO

1.1. Contextualización

El Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC), responsable de la asignación de recursos para esta región, anunció el agotamiento del stock de direcciones IPv4 y expresó su preocupación por la demora de Operadores y Gobiernos en desplegar el protocolo de Internet (IPv6) en la región. LACNIC informó que al haber alcanzado la cuota de 4.194.302 direcciones IPv4 en stock, emprenden a regir políticas restrictivas para la entrega de recursos de Internet en el Continente, que significa el agotamiento de las direcciones de IPv4 para los operadores de redes en América Latina y el Caribe.

"Estamos frente a un hecho histórico que no por ser esperado y anunciado, es menos importante", afirmó el CEO de LACNIC, Raúl Echeverría, "a partir de hoy LACNIC y los Registros Nacionales sólo podrán asignar cantidades muy pequeñas de direcciones IPv4, insuficientes para cubrir las necesidades de nuestra región." La organización ha entregado más de 182 millones de direcciones IPv4 en América Latina y el Caribe desde el inicio de sus operaciones en el 2002. (LACNIC, No hay más direcciones IPv4 en América Latina y Caribe, 2012)

Según lo acordado oportunamente por la comunidad de Internet en la región, al quedar disponibles 4.194.302 direcciones IPv4, se considera oficialmente agotado el stock de LACNIC y entran en vigor las políticas de "***agotamiento gradual"*** y "***nuevos miembros***" que establecen modificaciones en los procedimientos y requerimientos para la entrega de recursos.

También se activa la política de "Transferencias de bloques IPv4 dentro de la región LACNIC", que habilita y regula la transferencia de recursos entre entidades de la región. "Desplegar el protocolo IPv6 adquiere hoy más que nunca un sentido de urgencia, volviéndose inevitable e inaplazable si los proveedores de conectividad desean satisfacer la demanda de los clientes y de nuevos usuarios. LACNIC y la comunidad de Internet han estado trabajando por años para este momento" afirmó Echeberría. El 67% de las entidades ya cuentan con direcciones IPv6 asignadas por LACNIC y los Registros Nacionales NIC.br y NIC.mx.

No obstante, el CEO de LACNIC se mostró preocupado porque "a 10 años de que LACNIC y los Registros Nacionales NIC.BR y NIC.MX empezaran a promover el despliegue de IPv6, aún hay muchos operadores y empresas que todavía no han dado los pasos necesarios para afrontar debidamente esta circunstancia."

Durante esta fase de agotamiento de IPv4 se podrán asignar 2.097.150 de las 4.194.302 direcciones permanentes, en bloques de tamaños limitados entre 256 y 1.024 direcciones

IP. A su vez, las organizaciones solamente podrán solicitar un espacio adicional luego de seis meses de haber recibido su última asignación. Cuando se terminen las 2 millones de direcciones IPv4, los miembros de LACNIC ya no podrán recibir más asignaciones de recursos IPv4.

A partir de ese momento, quedará activada la reserva para nuevos miembros, dando paso a la fase 3 del plan de agotamiento IPv4 diseñado por LACNIC y los Registros Nacionales. En esta última fase, las políticas establecen que solo se podrán hacer asignaciones de direcciones IPv4 para nuevos miembros, en bloques de 256 (/24) y 1.024 (/22) direcciones, donde cada nuevo miembro podrá recibir solamente una asignación de este espacio.

Los protocolo de internet IP (Internet Protocol), permite el funcionamiento del internet comercial en la actualidad soportado mediante la versión IPv4, y llegando inminentemente al agotamiento de direcciones IP para los usuarios, así lo dio a conocer la entidad que supervisa la asignación global de direcciones IP Internet Assignes Numbers Authority (IANA), previéndo el agotamiento para Suramérica para el año 2015. (IANA, 2012)

Es necesario entender que IPv6 es el protocolo que va a resolver problemas detectados en el protocolo IPv4 critico de este que es el aspecto de la seguridad, aunque es un expectativa, el objetivo principal de IPv6 es resolver la falta de direcciones IP con la oportunidad que esto representa para mejorar, para ello los fabricantes diseñan los dispositivos que tienen la capacidad de reutilizar direcciones para alargar el uso de IPv4.

El crecimiento explosivo del uso de internet ha llevado a desarrollar nuevas tecnologías para la comunicación mediante el protocolo IP que es el encargado del transporte de paquete de información y de ordenador a otro sobre una capa de red de versión cuatro (IPv4). Es así que IPv6, es el estándar desarrollado por el Grupo de Trabajo de Ingeniería de Internet (IETF), que es una organización que desarrolla arquitecturas de tecnologías de redes (IETF, 2012).

IPv6 permite que un mayor número de usuarios y dispositivos se comuniquen a través de Internet utilizando números de mayor tamaño para crear direcciones IP. En el protocolo IPv4, cada dirección IP se compone de 32 bits, lo que permite la existencia de 4300 millones de direcciones únicas. Dirección IPv4: 172.16.254.1. En comparación, las direcciones IPv6 se componen de 128 bits, lo que permite la existencia de aproximadamente 340 billones de direcciones IP únicas. Dirección IPv6: 2001:db8: ffff:1:201:02ff:fe03: (APLE, 2015)

IPv6 ofrece otras ventajas de red, en la mayor parte de los casos, los ordenadores y las aplicaciones detectarán y aprovecharán las redes y los servicios con el protocolo IPv6 sin que el usuario tenga que hacer nada. Además, IPv6 resuelve otros problemas de los sistemas de redes que pueden producirse debido al número limitado de direcciones disponibles con el protocolo IPv4.

El Ministerio de Telecomunicaciones y de la Sociedad de la Información MINTEL impulsa la adopción del protocolo IPv6 ejecutando acciones y diseñando políticas y mecanismos técnicos necesarios para el soporte del nuevo protocolo en este sentido la Corporación Nacional de Telecomunicaciones se centra en dar cumplimiento emitido por el MINTEL.

Este tema de investigación nos permite conocer cuál es el impacto de la migración del protocolo IPv6 en los Proveedores de Servicio de Internet (ISP's,) y los procesos de migración del nuevo protocolo, con la coexistencia del protocolo IPv4, ya que este protocolo llega a su agotamiento de direcciones IP disponibles para la gran red en su crecimiento.

Los procesos de migración permite que cada dispositivo obtenga nuevos beneficios bajo el correcto funcionamiento en las redes, plataformas y sistemas operativos en el tráfico de IPv6 ya que este protocolo cuenta con billones de direcciones IP's, y con una gran variedad de ventajas en términos de estabilidad, flexibilidad y simplicidad en la administración de las redes.

Es importante evitar que al momento de la migración de IPv6 exista perdida de conexión ya que los ISP's atienden a cientos, miles o millones de clientes diferentes, y a su vez, a los Multi-Protocol Label Switching (MPLS), no solo desde el punto de vista de IPv4, sino también desde el punto de vista del despliegue de IPv6. Los ISP's pueden contar sólo con

una red, en ocasiones extendidas a través de múltiples países o regiones geográficas, ya cuentan con centros de datos, donde alojan servicios propios de los clientes.

El proceso de migración en los ISP's es importante, de la forma en la que se va a desplegar IPv6 en dichas redes, ya que es necesario separar ciertas infraestructuras o equipamientos para diferenciar los equipos propios de los que son propiedad de los clientes. En las redes, hay que diferenciar los tipos de redes fijas, móviles y diferentes tecnologías como fibra, cobre, WiMax, WIFI, LMDS, etc, así como diferentes partes de la red troncal, distribución, agregación, acceso, etc. IPv6 ha sido diseñado para permitir su despliegue, con mecanismos de transición, sin reemplazar de la noche a la mañana a los proveedores, usuarios finales, y a los equipos de agregación (Ministerio de Industria Energia y Turismo, 2008)

Para cualquier ISP contar con IPv6 en los enlaces que se conectan al resto de Internet son denominados Proveedores de tránsito, ya que estos se conectan a intercambiadores de tráfico que permiten IPv4 como IPv6 facilitando a grandes proveedores de contenidos, que soporten IPv6, servicios duplicados y servidores DNS raíz.

1.2. Justificación

El crecimiento indetenible del Internet ocasiona que la cantidad de direcciones IP del protocolo IPv4, llegue a su límite o a una situación de una posible escasez. El 3 de febrero

de 2011, LACNIC, comunicó que el stock central de direcciones IPv4 se agotó definitivamente. Frente a esta situación, el Ministerio de Telecomunicaciones y de la Sociedad de la Información MINTEL impulsa la adopción del protocolo IPv6 diseñando políticas y mecanismos técnicos (Canal Tecnológico , 2012).

El Ministerio de Telecomunicaciones investiga sobre la coexistencia ordenada y adecuada del protocolo IPv4 con el protocolo IPv6 con el fin de permitir que todos los ecuatorianos puedan seguir aprovechando las ventajas de la red de redes. En este sentido se adoptaron una serie de políticas y acciones que fomenten la adopción del nuevo protocolo.

La implementación del portal http://ipv6tf.ec/ en el que intercambia información técnica y vinculada con las mejores prácticas, consejos técnicos, entre otros, sobre la implementación de IPv6 en Ecuador, invitando a tod@s l@s ecuatorian@s a suscribirse para participar activamente en la construcción de esta nueva era de Internet.

La publicación e implementación de políticas públicas: en el 2011 y 2012 emitieron líneas de política por parte de MINTEL relacionadas con equipamiento, tráfico y despliegue de IPv6 en sector público y privado. Mediante Acuerdo Ministerial 007-2012, se establecieron las siguientes líneas:

Que las Instituciones del Sector Público implementen, en sus sitios web y plataformas de servicios electrónicos, el soporte y compatibilidad con el protocolo IPv6 de manera coexistente con el protocolo IPv4.

La incorporación y correcto funcionamiento del protocolo IPv6 en nombres de dominio bajo el código de país los ISP's y portadores nacionales admitan, en sus redes, plataformas y sistemas, el tráfico de IPv6 en coexistencia con IPv4 y que establezcan sus planes de direccionamiento IPv6.

Uno de los primeros sitios oficiales en contar con protocolo IPv6 es el del Ministerio de Telecomunicaciones y de la Sociedad de la Información, con el fin de incentivar al resto de organismos e instituciones públicas y privadas para que implementen el nuevo protocolo (Canal Tecnológico , 2012)

Para el cambio del nuevo protocolo el IETF ha trabajado proporcionando numerosas herramientas o mecanismos de transición, ya que la transición se iniciaría, de forma masiva en las redes de acceso,entre los 4-5 años antes del agotamiento de IPv4. Sin embargo el pausado despliegue de IPv6 ha visto la necesidad de desarrollar, casi en el último minuto, los nuevos mecanismos de transición para enfrentarse a un nuevo problema, ya que no quedan direcciones IPv4. Refiriéndose a mecanismos que realizan traducciones de IPv4 e IPv6, como los denominados DS-Lite, Carrier Grade NAT (CGN,

LSN, NAT64/DNS64, DUAL STACK, TUNELING y TRADU). (Canal Tecnológico , 2012).

|

Estos nuevos mecanismos en general no son necesarios en los ISP's que aún tienen direcciones IPv4 o puede utilizar direcciones privadas en su red, por ejemplo la red 10/8. Sólo los más grandes ISP's del mundo se ven realmente forzados al uso de estos protocolos.

En IPv4 los identificadores son números binarios con una cantidad limitada de bits 32 es decir, más de 4200 millones de direcciones posibles, sin contar con algunos rangos reservados para usos especiales, pero el crecimiento de la penetración de Internet a nivel mundial aumenta a más de 7000 millones de personas llegando así a crear el Protocolo IPv6 para cubrir todas las IP's en la gran red. (Canal Tecnológico , 2012)

Por su gran impacto, el negocio de proveer acceso a Internet ha crecido, pero actualmente e incluso se ve impulsado por los gobiernos. Estudios económicos demuestran que el incremento en la penetración del acceso a Internet genera crecimiento en el PIB(producto interno Bruto) y es considerado como un instrumento habilitante para el ejercicio de derechos humanos fundamentales como la libertad de expresión, de ahí que el plan de gobierno de muchos países considera alguna medida para lograr la masificación del Internet y cerrar la brecha digital. (Mejía, 2012)

La administración de los recursos IP actualmente tiene una estructura jerárquica, una entidad central llamada IANA que administra todo el espacio de direccionamiento disponible y es la encargada de entregar bloques de direcciones a organizaciones regionales denominadas RIR (Regional Internet Registry) conforme la demanda, quienes a su vez se encargan de la distribución/asignación a los proveedores de Internet. Se prevé que a finales del año 2012, RIPE (el RIR para la región de Europa) entre al mismo estado que APNIC. LACNIC es el RIR para la región de América Latina y Caribe, se calcula que tendrá direcciones hasta mediados de 2015 (Mejía, 2012)

Este proyecto es importante ya que permite a los ISP's conocer los procesos de migración hacia el nuevo protocolo con la menor probabilidad en la transición, perdida de datos y el impacto que los Proveedores tengan al momento de la misma.

1.3 Antecedentes

IPv4 no dejará de ser utilizado súbitamente, por el contrario IPv6 e IPv4 coexistirán durante muchos años, pero con una diferencia que actualmente los RIR distribuyen direcciones IP en base a la "necesidad de los recursos", mientras en la etapa post-agotamiento de IPv4 podría crearse en una demanda de solicitud de direcciones.

En los mercados de la tegnologia de las redes se intenta vender a IPv6 como un protocolo que resuelve los problemas encontrados en IPv4, creando falsas expectativas, pero su

función principal es resolver la escasez de direcciones IP donde la transición implica una oportunidad para mejorar la conectividad, de igual forma los fabricantes han diseñado dispositivos que permiten el reusó a gran escala de direcciones con el objetivo de prolongar el uso de IPv4 y diferir la introducción de IPv6 dentro de una red.

Como vemos la implementación de IPv6 dentro del territorio ecuatoriano es incipiente, por lo cual y a iniciativa de AEPROVI se creó la Fuerza de Trabajo de IPv6 de Ecuador (IPv6TF-EC) que permite buscar e incentivar la participación de ecuatorianas y ecuatorianos de los siguientes sectores: industria, gobierno, sector educativo, medicina y a usuarios.

En forma general la primera etapa para el despliegue de IPv6 es la capacitación al personal para conocer en detalle los servicios, equipos y configuraciones en la red actual para la toma de decisiones durante la migración al nuevo protocolo y tener un soporte adecuado desde el inicio.

Los ISP’s deben actualizar sus enrutadores, sistemas operativos gradualmente para no incluir gastos exorbitantes y la planificación de la transición debe realizarse en conjunto, ya que son el organismo regulador de nuestro país el mismo que debe definir los estándares apropiados. También es importante establecer los criterios de medición de calidad y de servicio adaptados al contexto según la infraestructura y seguridad que exista.

1.4. Objetivos

1.4.1. Objetivo general

Definir los procesos y el funcionamiento de migración hacia el nuevo protocolo IPv6, y la coexistencia entre los dos protocolos para garantizar la continuidad del servicio en los ISP's.

1.4.2. Específicos

- Determinar la situación actual en el proceso de la migración hacia el nuevo protocolo IPv6 en los Proveedores de servicio de Internet y los posibles problemas en la migración del protocolo IPv6 a los ISP's.
- Analizar los mecanismos de transición que puedan ser utilizados para la continuidad y la coexistencia de los protocolos IPv4 – IPv6 en los ISP's.
- Analizar la seguridad y ancho de banda que provee el protocolo IPv6 en los ISP's hacia los clientes.
- Analizar comparativamente el proceso de migración del nuevo protocolo en nuestro país versus el resto de América Latina u otros países en los proveedores de Internet.

1.5. Metodología de la investigación

La investigación es de carácter descriptiva del estudio de los protocolos de conexión a internet IPv4- IPv6, mediante un método de migración que permita analizar la relación causa efecto entre las técnicas y métodos de transición para conexiones de IPv4 a IPv6.

CAPÍTULO II

MARCO TEÓRICO

2.1. Introducción

IPv6 se inicio en el año de 1990, cuando se dio a conocer un informe donde se revela que el espacio de direccionamiento de IPv4 disponible se esta disminuyendo de forma exponencial debido a la gran cantidad de dispositivos que se conectan a intenet, en dicho estudio realizado por la IETF se indica que las direcciones de IPv4 se agotarian alrededor del año 2015, siendo esto el inicio de la busqueda de una nueva version del protocolo IP (Dunmore, 2005, pág. 4).

IPv6 es la abreviatura de "versión 6 del protocolo de Internet", es el protocolo de la última generación, diseñado para reemplazar al protocolo de Internet actual IP versión 4. Para comunicarse a través de Internet, las computadoras y otros dispositivos deben tener direcciones de remitente y de destinatario. Estas direcciones numéricas se conocen como "direcciones de protocolo de Internet". A medida que el Internet y la cantidad de usuarios crecen exponencialmente, también crece la necesidad de las direcciones IP.

IPv6 es un estándar desarrollado por la IETF, una organización que desarrolla tecnologías de Internet, anticipándose a la necesidad de un mayor número de direcciones IP, creó IPv6 para satisfacer la demanda del creciente número de usuarios y de dispositivos que acceden

a Internet. IPv6 permite que mayor número de usuarios y de dispositivos se comuniquen a través de Internet por medio del uso de números más grandes para la creación de direcciones IP. En IPv4, cada dirección IP se compone de 32 bits, lo que da lugar a 4300 millones de direcciones únicas. (AppleInc, 2007).

2.2. Internet protocol versión 6 (IPv6)

El crecimiento de internet así como la sofisticación de los dispositivos electrónicos han dado origen a proponer soluciones de escalabilidad al direccionamiento de internet versión IPv4, ya que con la inserción las direcciones en dicha versión no son suficientes para cubrir los requerimientos en los próximos años.

Ante esta demanda de direcciones la IETF, determina una serie de especificaciones para definir el nuevo protocolo de IP de la siguiente generación (IP Next Generation, IPng), denominado protocolo de internet versión 6 (IPv6)

El IPv6 incrementa el tamaño de la dirección IP de 32 bits a 128 bits para así soportar más niveles en la jerarquía de direccionamiento y un número mucho mayor de nodos direccionables. El diseño del protocolo agrega múltiples beneficios en seguridad, manejo de calidad, servicio, mayor capacidad de transmisión y la mejora de facilidad en la administración (IP&mx, 2011)

2.2.1. Características IPv6

El nuevo protocolo versión 6 ha implementado una serie de cambios y características que se describen a continuación.

- Direcciones largas que permiten una mejor entrega de jerarquía, sistemática y definitiva de las direcciones.
- Cambios de prefijos de routers ya que los identificadores de nodos pueden ser auto configurados independientemente del nodo.
- Seguridad a nivel de red a través de Internet Protocol Security, que es el protocolo de cifrado y validación de IP integrado en base a IPv6.
- Procesamiento simplificado en los routers mediante encabezado de paquetes más simples, sin necedad de que los routers IPv6 no hagan fragmentación.
- La trasmisión de los proveedores de IPv6 se ejecuta de forma trasparente para los usuarios finales a través de mecanismos de renumerado.
- El manejo de encabezado IPv6 es mas eficiente que IPv4 ya que existe menos campos eliminando la verificación del encabezado.

- Manejo de mecanismos de transición sin problemas en las redes que manejan IPv4 en conjunto con el protocolo IPv6.

2.2.2. Direccionamiento IPv6

Las direcciones IPv6 están definidas mediante indicadores de 128 bits para interfaces y conjuntos de interfaces. Según el RFC 1984. Existen tres tipos de direcciones IPv6, que permiten el direccionamiento del nuevo protocolo, se describen a continuación:

UNICAST: Es un identificador para una única interfaz <*uncast*>, los paquetes enviados a una dirección tipo <*uncast*> se entrega a la interfaz identificada por dicha dirección.

Tabla 1Tipos de direcciones Unicast

<unicast>	Enlace Local (Link-Local). Sitio Local (Site-Local). Agregable Global (Aggregatable Global). Loopback. Sin-Especificar (Unspecified). Compatible con IPv4.

Fuente: *(CISCO, 2014)*

MULTICAST: Son utilizadas para identificar a un grupo de interfaces IPv6, un paquete que se envía a este tipo de dirección <*multicast*> se procesa por todos los miembros del grupo <*multicast*> (IP&mx, 2011)

Tabla: 2 Tipos de direcciones <multicast>

<multicast>	Asignada (Assigned). Nodo Solicitado (Solicited Node).

Fuente: *(CISCO, 2014)*

ANYCAST: Este tipo de direcciones se asignan a múltiples interfaces es decir a <*múltiples nodos*>, los paquetes que son enviado a estas direcciones <*anyticast*> es entregado a una de las interfaces generalmente a la más cercana.

Tabla: 3 Tipos de direcciones anycast

<anyticast>	Agregable Global (Aggregatable Global). Sitio Local (Site Local). Enlace Local (Link Local).

Fuente: *(CISCO, 2014)*

Los tipos de direcciones anycast se subdividen en direcciones diseñadas para resolver casos específicos de direccionamiento, como:

Enlace Local. Se utiliza en un enlace sencillo y no debe nunca ser enrutada. Se usa para mecanismos de autoconfiguración, descubrimiento de vecinos y en redes sin ruteadores. Es útil para crear redes temporales. Puede ser utilizada sin un prefijo global.

Sitio Local. Contiene información de subred dentro de la dirección, son enrutadas dentro de un sitio, pero los ruteadores no deben enviarlas fuera de éste. Además es utilizada sin un prefijo global (IP&mx, 2011)

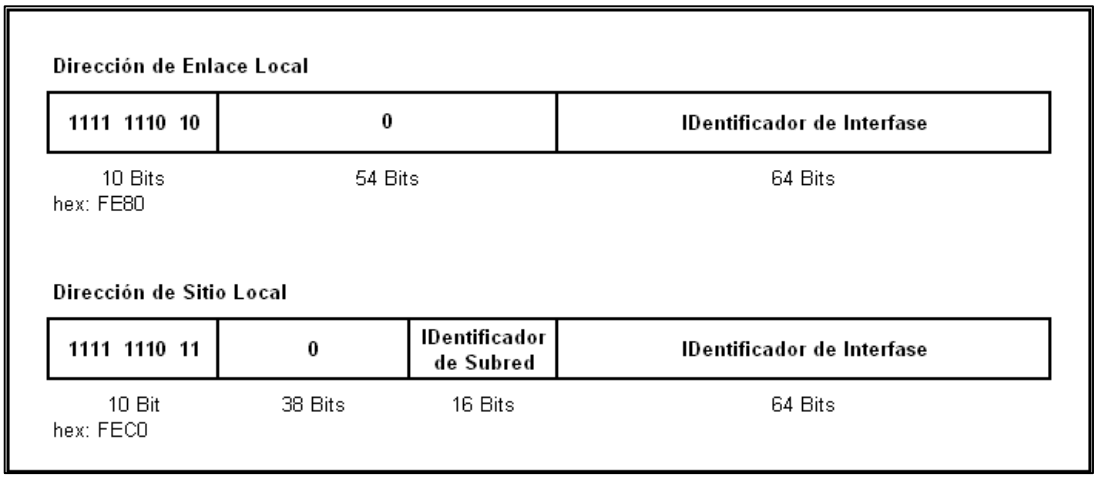


Figura: 1 Formato de direcciones de Enlace Local y Sitio Local.
Fuente: *(Network Information Center México S.C., 2012)*

2.2.3. Prefijos de IPv6

IPv6 permite mayor distribución de direcciones a distintas organizaciones y sobre todo a los operadores de servicios de internet conocidos como ISP, ya que el nuevo protocolo posibilita la disponibilidad de direcciones a través de un solo prefijo para toda una red de una organización, por ende los proveedores de servicios de internet pueden agregar en un solo nodo a los clientes y en un solo prefijo para ser anunciado al internet en IPv6.

Cuando los usuarios finales cambien al protocolo IPv6 también deben cambiar el prefijo de la nueva versión preservando la agregación global y esto acarrea a la remuneración de la red.

Address Type	Binary Prefix	IPv6 Notation
Unspecified	00...0 (128 bits)	::/128
Loopback	00...1 (128 bits)	::1/128
Multicast	1111 1111	FF00::/8
Link-Local Unicast	1111 1110 10	FE80::/10
ULA	1111 110	FC00::/7
Global Unicast	(everything else)	
IPv4-mapped	00...0:1111 1111:IPv4	::FFFF:IPv4/128
Site-Local Unicast (deprecated)	1111 1110 11	FEC0::/10
IPv4-compatible (deprecated)	00...0 (96 bits)	::IPv4/128

Figura: 2 Prefijos IPv6.
Fuente: (Center S.C., 2012)

2.3. Métodos de configuración de IPv6

La autoconfiguración conocida como configuración automática, está se encuentra definida en el RFC 2462 para el direccionamiento sin estado IPv6, permitiendo que los ruteadores configurados soporten IPv6 y envíen a través de un enlace local la información de la red a los ordenadores y a su vez estas se configuren de forma correcta. Mediante este mecanismo cada equipo conectado a una red y a un servidor de IPv6 se añaden direcciones a la capa de enlace MAC en formato EUI-64 y al prefijo de IPv6 unicast global enunciado en la subred. Ver figura 3.

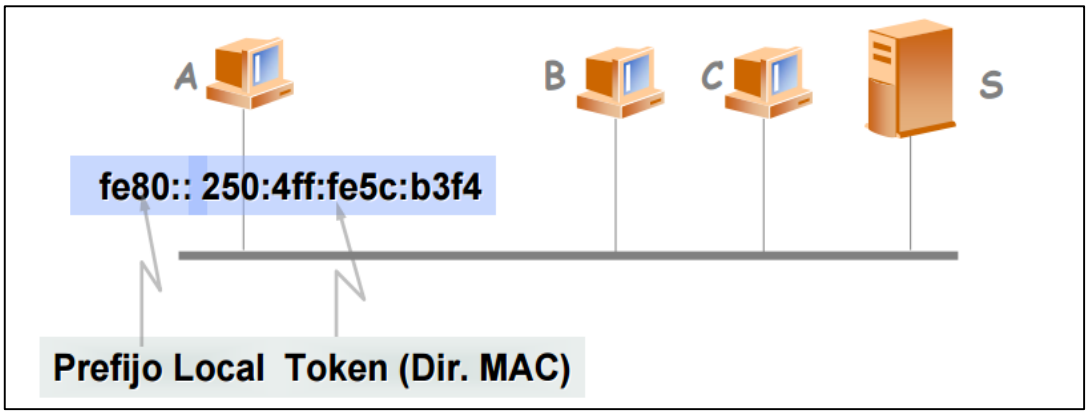


Figura: 3 Autoconfiguración sin estado
Fuente: (Fernandez, M 2004)

Configuración por servidor. Los ordenadores que utilizan este método IPv6 obtienen los parámetros como direcciones de configuración desde un Servidor a un host dinámico (DHCP) versión 6, a este modo se le denomina Configuración de direcciones con estado IPv6. Ver figura 4.

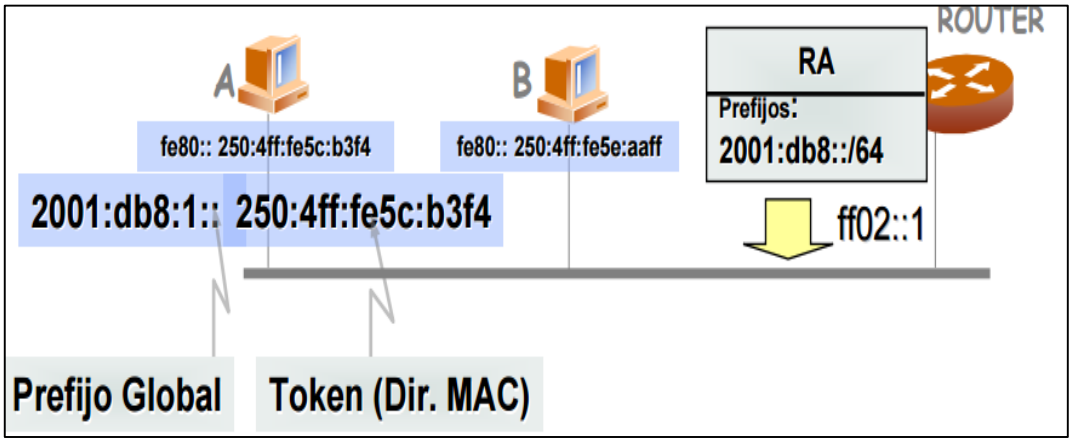


Figura: 4 Autoconfiguración por servidores
Fuente: (Fernandez, M 2004)

2.3.1. Re-numeración

Este proceso se diseña para que sea trasparente entre los proveedores IPv6 unicast y el usurio final, trabaja con el mecanismo de autoconfiguración re numerando los ordenadores a través del envió del nuevo prefijo a toda la red.

Este método presenta un problema que es la perdida de sesiones del protocolo de control de trasmisión (TCP) y del Protocolo de Datagrama de Usuario (UDP) que se da entre los ordenadores y los servidores al momento de la transición.

2.3.2. Diferencias entre protocolos IPv4 e IPv6

En las principales diferencias que existen entre los protocolos es necesario mencionar las mejoras en cuanto a seguridad y gran cantidad de disponibilidad de direcciones IPv6.

- No hay direcciones broadcast esta se sustituye por direcciones multicast para el mejoramiento de las conexiones.
- Los campos de las direcciones reciben nombres específicos (*prefijos*), a la parte de la dirección.
- A través del prefijo permite conocer donde está conectado las direcciones determinadas desde la ruta hasta el destino.

- Cualquier campo puede contener ceros o unos [0,1], salvo que explícitamente se indique lo contrario.

- Las direcciones del protocolo IPv6 diferentemente del tipo se asignan a interfaces no a nodos.

- Mediante una única interfaz se puede tener varias direcciones IPv6 de cualquier tipo según sean requeridas.

- Una misma dirección o conjunto de direcciones unicast pueden ser asignados a múltiples interfaces físicas.

- Al igual que en IPv4, se asocia un prefijo de subred con un enlace y se pueden asociar múltiples prefijos de subred al mismo enlace.

2.4. Despliegue de IPv6

Las direcciones IP se asignan mediante un sistema jerárquico en función del operador definido por la IANA, quien es la entidad que asigna direcciones IP a los cinco Registros Regionales de Internet (RIRs) a nivel mundial y estos (RIRs) son quienes asigna bloques de direcciones IP a los ISPs.

Los ISPs, son quienes asignan las direcciones a las conexiones individuales de internet como son los usuarios finales. Al existir toda una infraestructura de comunicaciones

operando en los ISP's, es necesario la convivencia y coexistencia entre las dos versiones de protocolos IPv4 e IPv6, lo que permite crear mecanismos de transición para que convican durante muchos años. Los mecanismos son:

- Doble-pila: Permite la coexistencia de IPv4 e IPv6 en el mismo dispositivo y en las redes.

- Tuneles: Es una técnica que evita dependencias cuando se actualizan host, routers o regiones.

- Técnicas de traducción: Garantiza la comunicación entre dispositivos que operan con un solo protocolo sea IPv4 o IPv6, (Dispositivos móviles, domótica, vehículos,….)

2.4.1. Ventajas de IPv6

Con el paso del tiempo las direcciones IPv4 serán pocas, por lo que será más costoso conseguirlas por los ISP. Contrariamente, las direcciones IPv6 serán menos costosas dada su abundancia, a los usuarios se les serán asignadas nuevas direcciones debido a la escasez de IPv4. En este sentido IPv6 ahorra dinero a aquellos negocios que hacen de IPv6 una prioridad ya que el nuevo protocolo trae beneficios adicionales que se describen a continuación.

- **Autoconfiguración:** IPv6 provee la opción para la autoconfiguración de la red, lo que significa que cualquier dispositivo IPv6 puede ser conectado a la red, encendido y generará exitosamente por sí mismo una dirección IPv6 sin necesidad de dar una entrada estática en un servidor DHCP. Si el dispositivo es conectado a un Router IPv6, éste puede generar una dirección local y una global, ofreciendo acceso inmediato a Internet.

- **Seguridad intrínseca:** Otro de los beneficios para IPv6 es la seguridad y la encriptación intrínseca del contenido. A diferencia de IPv4, los paquetes de IPv6 garantizan una seguridad de punta a punta dado que la información contenida en ellos no puede ser fácilmente decodificada por intermedios.

- **Soporte mejorado de la Calidad de Servicio (QoS):** La adopción de IPv6 también conlleva notables mejoras en la calidad del servicio (QoS). Las aplicaciones que requieren baja latencia, como VoIP, y aplicaciones multimedia que usen streams, pueden marcar sus paquetes con el nivel de prioridad apropiado para ser transferidos a través de una red.

- **Mejoras de ruteo:** Las tablas de ruteo de Internet se han hecho extremadamente complejas. El esquema de asignación de direcciones de red estructurada usada para IPv6 ayuda a reducir la actual carga en la estructura de red de área amplia. Adicionalmente IPv6 incluye un esquema más sensible para soportar ruteo multicasting.

- **Encabezado de paquete simplificado:** El nuevo encabezado de paquete simplificado y estandarizado usado en IPv6 también mejora el ruteo. IPv6 usa un encabezado de longitud fija de 40 bytes, de los cuales solo 8 son de información general. Esta configuración permite a la información ser ruteada más rápidamente. IPv6 además elimina los campos de fragmentación desde el encabezado del paquete para una mayor eficiencia.

- **Movilidad mejorada:** IPv6 provee mejor movilidad para los usuarios que van de una subred a otra. Una conexión a red móvil puede ser mantenida transparentemente ya que cada dispositivo, ya sea smarthphone o tableta, es identificado por su dirección original (ISOC, 2015).

En conclusión, IPv6 tiene el potencial de hacer que los usuarios usen sus dispositivos en distintas redes de forma transparente.

2.4.2. Arquitectura de transición

Una arquitectura de transición comprende tres consideraciones red, nodos finales y las aplicaciones. Figura 5.

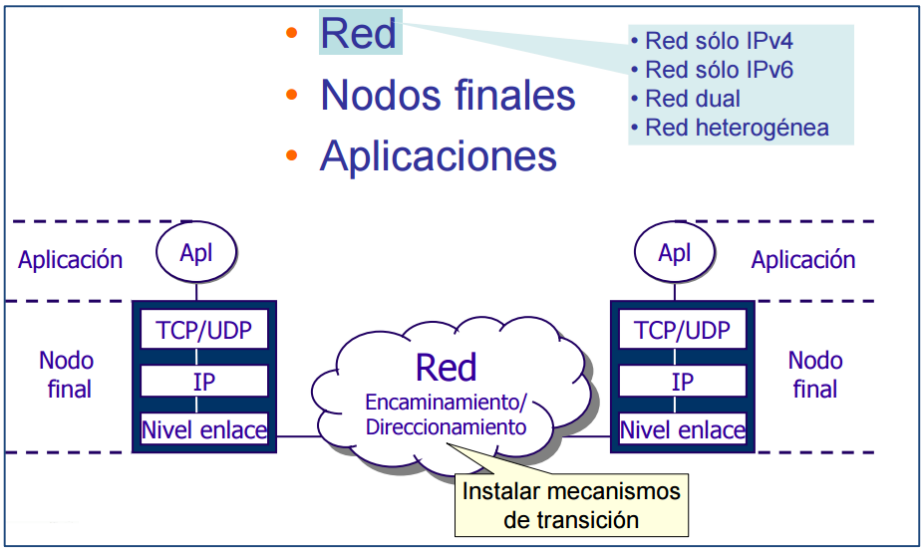


Figura: 5 Transición a nivel de red
Fuente: *(Castro, 2006, pág. 4)*

El proceso de adopción del nuevo protocolo versión 6 por parte de los proveedores de servicio deben tener en cuenta puntos clave para el proceso de migración de las redes IPv4 a IPv6, ya que la migración no solo abarca redes, servidores sino dispositivos finales, aplicaciones, y seguridades así como criterios propios en el ámbito de la aplicación de la red.

El proceso de adopción y despliegue de IPv6 indistintamente de cualquier infraestructura de red que los proveedores tengan implementado deben contemplar las siguientes consideraciones.

- **Planificar** La planificación es un proceso importante que los proveedores de servicios de internet deben ejecutar de manera precisa, y es recomendable realizarlo por fase.

- **Pruebas.** Sobre el diseño de la nueva infraestructura que permita evaluar el funcionamiento, permitiendo detectar posibles problemas.

- **Desplegar.** Para ello la red en un entorno definido es recomendable al área y servicios menos críticos que el proveedor tenga.

2.4.3. Topología par admitir IPv6

Para la integración del protocolo IPv6 se tiene que detectar las entidades que conforman la red, además estas deben ser compatibles con el protocolo IPv6 en este sentido la implementación de IPv6 no modifica la topología de la red.Cableado, Enrutadores, Host. Adicionalmente se determinó que la adopción de IPv6 infiere tanto en la topología red, nodos finales enrutadores y las aplicaciones software por lo que se debe preparar y configurar el hardware y las aplicaciones para usuarios de IPv6.

En este sentido el departamento de comunicaciones de los ISP deben tener conocimientos sobre el funcionamiento e implementación del nuevo protocolo así como de los cambios que se deben hacer en cada uno de los componentes del ISP.

Se debe verificar que el hardware de red se pueda actualizar a IPv6, en este sentido se debe consultar la documentación del fabricante del equipo sobre la compatibilidad con la nueva versión de protocolo según el tipo de hardware como:

- Servidores de seguridad.
- Servidores.
- Conmutadores.
- Enrutadores.

En el ámbito de equipos de enrutamiento deben estar preparados y configurados para adoptar IPv6. De detectarse de que alguno de los equipos no es compatible con la nueva versión del protocolo IPv6, el ISP deberá considerar las siguientes alternativas.

- Comprar nuevo hardware de enrutamiento.
- Adoptar y evaluar un mecanismo de transición para no descartar la utilidad del equipo que no soporta IPv6.
- Verificar el año de fabricación del enrutador si traen soporte o actualización a IPv6.
- Verificar si los equipos soportan o no soportan tráfico en el protocolo IPv6.
- Analizar los procedimientos de configuración del fabricante y comprobar la documentación del elemnto de red para que administre el nuevo protocolo IPv6.
- Analizar si el ruteador no aunincia como enrutador determinado por lo que se le debe asignar la ruta predefinida (::/0), para que actue como publica.

- Analizar si la dirección IP tiene un identificador de interfaz inesperado.

- Comprobar que Internet Explorer no se conecta cuando se utilizan direcciones IPv6 literales en la dirección URL.

- Verificar si la tabla de enrutamiento contiene rutas fuera del vínculo.

- Verificar si se produce un error en los mensajes ping de solicitud de eco y si especifica un destino local del vínculo.

- Analizar el funcionamiento de IPSec en IPv6.

- Verificar el tráfico del túnel que no llega al destino (ORACLE, 2012)

- Analizar si no se configura ninguna dirección compatible con IPv4 en la Pseudointerfaz de túnel automático. (msdn, 2005)

2.4.4. Preparación de servicios de red para adoptar IPv6

Los servicios de red necesarios que los ISP deben implementar en los nodos finales se describen a continuación.

- **DHCP**. Protocolo de configuración dinámica de host») es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente.

- **DNS:** Domain Name Service) es un sistema de nombres que permite traducir de nombre de dominio a dirección IP y vice-versa.

- **HTTP:** Abreviatura de la forma inglesa Hypertext Transfer Protocol, 'protocolo de transferencia de hipertextos', que se utiliza en algunas direcciones de internet.

- **MAIL.** Servicio que permite a los usuarios enviar mensajes a través de sistemas de comunicación electrónicos.

Problemas que suelen presentarse al implementar IPv6 en el ámbito de servicios que se detallan a continuación.

- El servicio de correo Internet Message Access Protocol (IMAP) solo es apto para el protocolo versión IPv4.

- Una consideración importante que los técnicos de red deben tomar en cuenta es que deben ser configurados los nodos para IPv6 y ejecutar servicios en IPv4.

- Al activar IPv6 no todos los servicios aceptan conexiones al protocolo IPv6.

- Los servicios que están conectados con el protocolo IPv6 solo aceptan una sola conexión.

- Los servicios que no están conectados al protocolo IPv6, deben seguir funcionando con el protocolo IPv4 mediante un mecanismo de transición IPv4 –IPv6.

- Cierto tipo de modelos de enrutadores no se pueden actualizar a la nueva versión del protocolo IPv6.

- Las aplicaciones aunque se conviertan al protocolo IPv6 no activan IPv6 de forma predeterminada. En este sentido se debe configurar las aplicaciones para activar de forma predeterminada al protocolo IPv6.

- En el caso de que un servidor de aplicaciones ejecute varios servicios se presentan estas consideraciones. Servicios solo en IPv4. Servicios en IPv4 e IPv6, ocurren problemas cuando los clientes acceden a varios servicios generando confusión en el servidor.

2.5. Preparación de servidores para adoptar IPv6

A los servidores se los consideran host de IPv6, en este sentido el protocolo Neighbor Discovery (ND), configura automáticamente las direcciones IPv6.

- Algunos servidores tienen más de una tarjeta de interfaz que se suelen extraer o remplazar por lo que el protocolo ND debe asignar un nuevo ID.

- Algunos servidores no pudrían aceptar este cambio de ID, por lo que se debe configurar de forma manual el ID a la interfaz de red nueva en cada servidor de ser el caso.

- No hay ruta predeterminada para un host.

2.5.1. Seguridades de IPv6

En cuanto al aspecto de seguridad el protocolo IPv6 ha incorporado el protocolo denominado Internet Protocol security (IPsec), que tiene como función de asegurar las comunicaciones sobre el protocolo de internet (IP), que ejecuta la autentificación y cifrado de los paquetes IP en el flujo de datos (GEII, 2004).

El nuevo protocolo IPSec que fue concebido y estandarizado por el Grupo Especial sobre Ingeniería tiene las siguientes funciones.

- Limitar el acceso
- Certificar la autenticación de la persona que envía los datos.
- Encriptar los datos transmitidos a través de la red.
- Asegurar la integridad de los datos.
- Invalidar la repetición de sesiones.

Los protocolos que respaldan el funcionamiento de IPSec son: la Autenticación de Encabezado (Autentication Header, AH) y la Carga de Seguridad Encapsulada (Encapsulated Security Payload, ESP). Al estar incluidos en cada implementación de IPv6 se provee mayor seguridad ya que IPSec está presente en todos los nodos de la red (Bellovin, 1996)

Los aspectos en el campo de seguridad que se derivan con la implementación de IPv6 en la red ya configurada se deben tener las precauciones para no poner en riesgo la información y seguridad de la red.

- Los paquetes de IPv6 pasan por túneles a través de corta fuegos por lo que debe hacer que el cortafuego analice e inspeccione el contenido del túnel, y definir un cortafuego para IPv6 con reglas similares al extremo final del túnel.

- Los nodos IPv6 son accesibles desde fuera, por lo que se deben implementar directivas de seguridad de acceso publico

- Se deben establecer reglas estrictas con relación al cortafuegos preferentemente y configurar con modo de estado.

2.5.2. Impacto de IPv6 a los usuarios

Desde la perspectiva de los usuarios la implicación del nuevo protocolo IPv6, en las redes domésticas se deben considerar a usuarios finales, empresas y corporaciones que no deben verse afectados y el proceso debe ser trasparente.

En este sentido una red doméstica, corporativa o empresarial está constituida por hardware (router), software (aplicaciones, S.O.) y redes (otros dispositivos de red).

- **Encaminador.-** Es el medio de acceso, comunicación a internet y configurado por los proveedores de internet. Generalmente estos equipos no traen soporte para el protocolo IPv6, si fueron implantados antes del 2010. Por lo que deben de ser remplazados o de ser el caso actualizados por el fabricante.

- **Sistemas operativos.-** A partir del año 2001, la mayoría de sistemas operativos libres y comerciales tanto clientes como servidores ya traen soporte activado de forma predeterminada, o que se deben instalar directamente de la página del fabricante.

- **Aplicaciones.-** Se entiende como aplicación clientes al explorador web (browser) que en su mayoría ya traen soporte automático para el protocolo IPv6 **(**Internet Explorer, Firefox, Chrome, Safari. Opera), e incluso aplicaciones para compartir información a través de internet.

- **Otros dispositivos de red.-** Se entienden como otros dispositivos puntos de acceso Wi-Fi, concentradores de red, Switch, modem, Hub, entre otros estos están configurados en el llamado modo puente (bridge nivel 2), por lo que no tienen inconvenientes y el proceso es trasparente a IPv4 e IPv6. Si alguno de los elementos de red son de (nivel 3) con funciones de encaminado (routing), los usuarios deben comprobar que dicho elemento soporta IPv6, caso contrario de debe actualizar o activar el equipo, ya que de no tener en cuenta estas consideraciones no se podría llegar a dicho dispositivo.

- **Conexión a internet.-** En este aspecto los proveedores de internet deben proporcionar acceso a los clientes con soporte a IPv6 e IPv4 mediante la implementación de mecanismos de coexistencia y transacción. Para estos casos IPv6 debe de funcionar pasando por los dispositivos que soportan la red (encaminador y otros dispositivos de red, conexión a internet), si estos elementos están preparados el sistema operativo le indica a la aplicación que se puede utilizar IPv6.

En caso de que cualquiera de los tres elementos encaminador, otros dispositivos de red, conexión con el proveedor de servicios no esté preparado el sistema operativo debe ejecutar los denominados mecanismos automáticos de transición DualStack, Tunneling y Nateo.

El problema que surge con la implementación de los mecanismos de transición automáticos siempre funcionan en aplicaciones cliente –cliente mensajería, competición de ficheros, etc, pero pueden presentar fallas en las aplicaciones que se despliegan en el modelo cliente-servidor navegación en la web, correo electrónico. Esto se produce ya que el proveedor de internet no despliega los relés de los mecanismos de transición.

Como alternativa se debe implementar mecanismos de transición manuales tunnel, brokers, que son proporcionados por los IPS´s, aunque esto supone que el usuario deba implementar una configuración en el equipo.

2.5.3. Impacto de IPv6 en las empresas

El impacto para las empresas sobre la adopción del nuevo protocolo IPv6, sean estas grandes o pequeñas, en si presentan las mismas implicaciones problemas e inconvenientes que los usuarios finales

Los elementos de red que las empresas tienen se consideran Small Office-Home Office (SOHO), si son pequeñas se deben tratar como una red doméstica descritos en el apartado <***IPv6 para usuario>).*** Por lo que se describe información sobre elementos adicionales de la red de empresas Pymes, ya que requieren de más elementos.

- **Aplicaciones.-** Al tratarse de grandes empresas utilizan aplicaciones desarrolladas a medida o adquiridas de terceros, se debe comprobar que estas aplicaciones funcionen con el método de transición que se tenga implementado para permitir que usuarios de la empresa se puedan conectar.

- **Encaminadores router. P**ara este caso son routeadores de interconexión de las redes de la empresa que permiten el enrutamiento de los paquetes entre redes definiendo la ruta que deben tomar los paquetes de datos hasta llegar al destino.

  Estos equipos ya traen soporte para IPv6, o que se pueden actualizar a través del software del fabricante. Esto se debe hacer en cada uno de los múltiplos equipos routers, conexiones o enlaces con otras redes de la institución de la empresa ya que estas tienen varias oficinas, sucursales, etc.

- **Dispositivos de red:** Esto depende del tamaño de la empresa, además suelen tener dispositivos como cortafuegos, seguridades, balanceadores de carga, dispositivos de cache, proxy, dispositivos VPN, voIP, por lo que se debe implementar alternativas mediante mecanismos de transición internos antes que remplazar varios equipos.

  Respecto al proxy y fireware que estas tengan implementado se deben preparar y configurar dichos equipos con soporte a IPv6.

- **Conexión a internet y redes externas:** proveedores de internet deben garantizar en el punto de frontera conectividad a IPv6 para las empresas, siendo así deben comprobar instalando un equipo que soporte IPv6.

2.5.4. Impacto de IPv6 sobre las redes TOR

Tor es una red que permite acceder a Internet de forma anónima, oculta el origen y destino del tráfico de Internet, haciendo que otros no puedan detectar fácilmente quién navega en la Web. La red Tor son servidores que se denominan "routers cebolla" o su acrónimo de "The Onion Routing Project". El proyecto Tor, es una aplicación de código abierto que funciona sobre el internet mediante comunicaciones TCP que permite optar y elegir una ruta para la salida de los mensajes, sin ser identificados.

Tipos de entidades:

- **Nodos OR o simplemente OR (Onion Router):** Funcionan como encaminadores y como servidores de directorio (DNS). Los nodos OR mantienen una conexión TLS con cada uno de los otros OR. Las conexiones OR-OR no son nunca cerradas deliberadamente salvo cuando pasa cierto tiempo de inactividad. Cuando un OR comienza o recibe nueva información de directorio él intenta abrir nuevas conexiones a cualquier OR que no esté conectado.

- **Nodos OP o simplemente OP (Onion Proxy):** Los usuarios finales ejecutan un software local que hace la función de nodo OP y que su función es obtener información del servicio de directorio, establecer circuitos aleatorios a través de la red y manejar conexiones de aplicaciones del usuario.

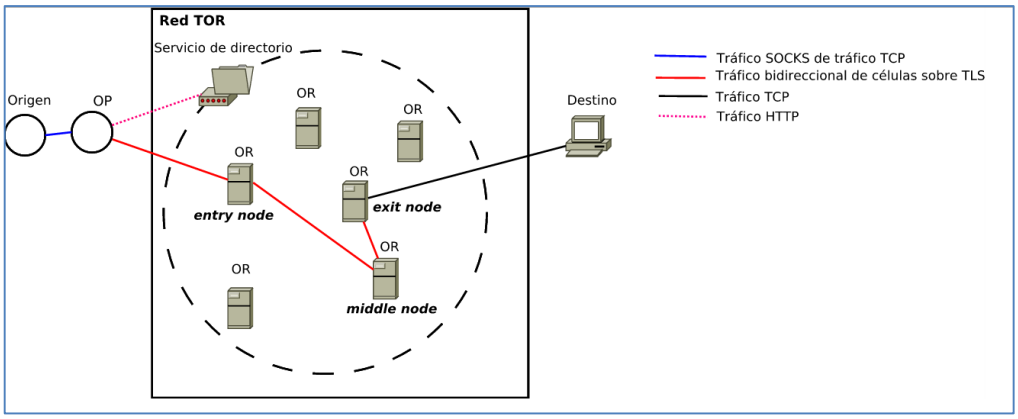


Figura: 6 Funcionamiento de la Red Tor
Fuente: https://es.wikipedia.org/wiki/Tor_%28red_de_anonimato%29

2.5.4.1 Características y debilidades

Las características y debilidades que definen una red de anonimización TOR se describen a continuación.

- El grado de anonimización que proporcionan.
- Resistencia a ataques de re-identificación,
- Su fiabilidad,
- Su ancho de banda y su latencia. Por supuesto, a mayor anonimización y fiabilidad, menor ancho de banda y mayor latencia

Por qué usar TOR:

- Proteger la comunicación de corporaciones extrañas.
- Proteger la privacidad de marketing innecesario y de ladrones de identidad
- Acceso a información prohibida en ciertos países o culturas.
- Creen ser vigilados (Carrasco, 2012, págs. 4-6)

Ventaja

Tor es una herramienta efectiva para la evasión y la protección de la identidad. La codificación de Tor oculta el contenido de las comunicaciones y del administrador de la

red local, disimula con quien nos comunicamos o qué sitios Web visitamos. Cuando se usa correctamente, brinda una mayor protección de anonimato que un proxy simple.

Riesgos

Tor es vulnerable al bloqueo, la mayoría de los nodos Tor están listados en un directorio público, así que es muy fácil para los operadores de red acceder a la lista y adicionar la dirección IP de nodos para el filtrado.

Algunos programas que se pueden usar con Tor tienen problemas que pueden comprometer el anonimato. Tor Browser Bundle viene con una versión de Firefox con Torbutton instalado. Torbutton inhabilita algunos plugins y cambia las huellas del navegador para que se parezca a cualquier otro usuario de Torbutton.

Tor no nos protege si no configuramos nuestras aplicaciones para que se ejecuten a través de Tor. Algunos plugins y scripts ignoran las configuraciones de proxis locales y pueden revelar nuestra dirección IP.

Si no estamos usando cifrado adicional para proteger nuestras comunicaciones, nuestros datos será decodificados una vez que alcancen el último nodo Tor de la cadena llamado nodo salida.

2.5.4.2 Las redes TOR e IPv6

El proyecto TOR propone el uso de encaminamientos de cebolla de modo que las comunicaciones viajen desde el origen hasta el destino a través de una serie de dispositivos de encaminamiento (routers) especiales denominados como encaminadores (onion routers). Si bien la red TOR se basa en nodos que son alcanzables a través de IPv6, para ello el equipo donde se lo tenga instalado debe estar activado el porte para IPv6, la red Tor no lo utilizara por defecto por lo que se lo debe instalar de forma explícita.

Además al ser enrutadores o encaminadores se realizan las configuraciones de la interfaz para que permitan enrutar direcciones IPv4 e IPv6, mediante mecanismos de transición DualStack, por lo tanto se siguen los mismos procedimientos para admitir IPv6.

2.5.4.3 Qué debe cambiar Tor para IPv6

Tor utiliza el Internet de muchas maneras, existen tres formas principales que se debe cambiar para el soporte IPv6.

1. Tor debe permitir conexiones desde clientes sólo IPv6 ya que en la actualidad, los routers y los puentes no escuchan direcciones IPv6, y no admiten direcciones IPv6, por lo que los clientes no pueden aprender lo que hacen.

2. Tor debe transportar el tráfico IPv6 y el tráfico DNS relacionados con IPv6. en la actualidad, sólo permite COMENZAR las conexiones con los objetivos de IPv4 o a nombres de host, y sólo permite RESOLVER para solicitar los registros A y PTR.

3. Tor debe permitir a los nodos se conectan entre sí a través de IPv6. Permitiendo sólo IPv6 a clientes de lo contrario estos clientes no podrán conectarse a Tor en absoluto.

Es importante apoyar las dependencias relacionadas con el IPv6 DNS y salir a los servicios IPv6, permitiendo a los nodos Tor soportar una pila dual de IPv4 e IPv6 para la interconexión. Donde los clientes puedan conectarse a los puentes privados sobre IPv6 ya que estos todavía necesita al menos una dirección IPv4 con el fin de conectarse a otros relés, tomando en cuenta que el usuario tiene dos líneas de puente para el mismo puente (uno IPv4 y uno IPv6).

2.6. Despliegue de IPv6 en América Latina

Despliegue de IPv6 en el mundo, Google recopila información sobre la adopción de IPv6 en Internet de forma permanente, identificando proveedores de Internet, propietarios de sitios web, y los responsables políticos como la industria lanza IPv6.

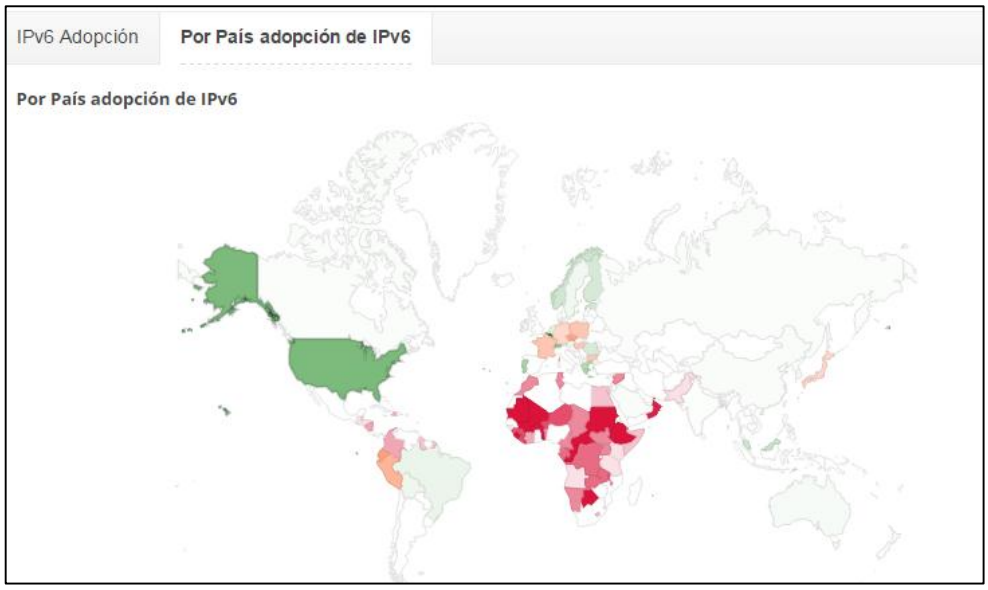


Figura: 7 Adopción de IPv6 por país
Fuente: *(Google, 2015)*

La Figura 7 muestra la disponibilidad de conectividad IPv6 en todo el mundo.

- Regiones donde IPv6 es más ampliamente desplegado (el más oscuro el verde, mayor será el despliegue) y los usuarios experimentan problemas poco frecuentes que se conectan a sitios web habilitados para IPv6.

- Regiones donde IPv6 es más ampliamente desplegados pero los usuarios siguen teniendo fiabilidad significativa o problemas de latencia que se conectan a sitios web habilitados para IPv6.

- Regiones donde IPv6 no es ampliamente desplegado y usuarios experimentan fiabilidad significativa o problemas de latencia que se conectan a sitios web habilitados para IPv6 (Google, 2015)

- Estados unidos 21.34%

En América Latina los ISP, y organizaciones que han implementado IPv6 se describen en la siguiente gráfica.

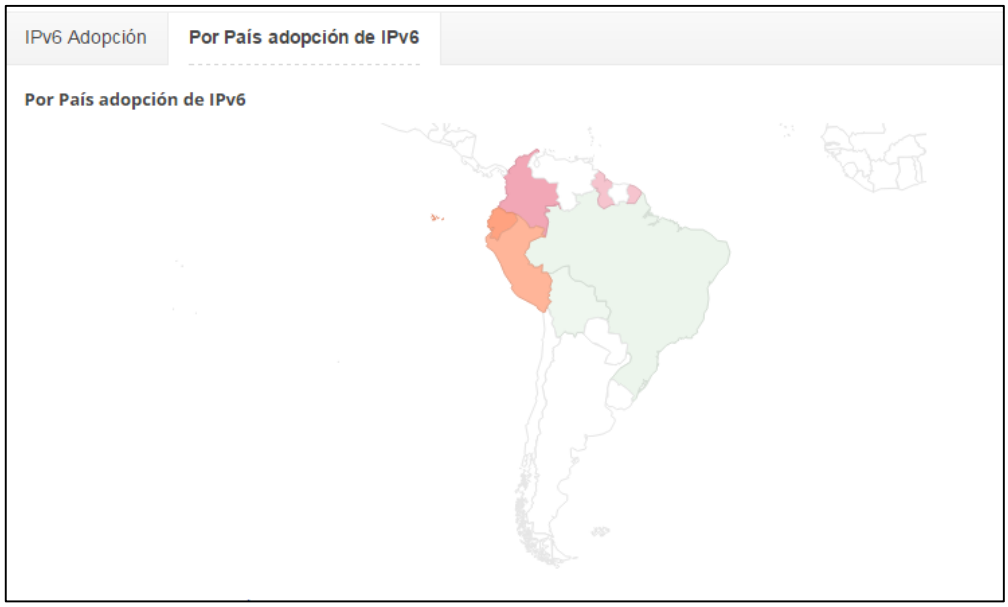


Figura: 8 Adopción de IPv6 América del sur
Fuente: (Google, 2015)

- Regiones donde IPv6 es más ampliamente desplegado (el más oscuro el verde, mayor será el despliegue) y los usuarios experimentan problemas poco frecuentes que se conectan a sitios web habilitados para IPv6.

- Regiones donde IPv6 es más ampliamente desplegados pero los usuarios siguen teniendo fiabilidad significativa o problemas de latencia que se conectan a sitios web habilitados para IPv6.

- Regiones donde IPv6 no es ampliamente desplegado y usuarios experimentan fiabilidad significativa o problemas de latencia que se conectan a sitios web habilitados para IPv6 (Google, 2015).

Tabla: 4 Adopción de IPv6 en América Latina

PAIS	PORCENTAJE DE DESPLIEGUE
Perú	15.82%
Ecuador	4.71%
Colombia	0.02%
Argentina	0.02%
Venezuela	0.01%
Brasil	3.14%
Bolivia	2.06%
Paragua	0%
Chile	0.01%
Uruguay	0.01%

Fuente: (Google, 2015).

Las estadísticas corresponden a Google obtenidos de la dirección electrónica http://www.google.com/intl/en/ipv6/statistics.html que recopila información sobre la adopción de IPv6 en Internet de forma permanente.

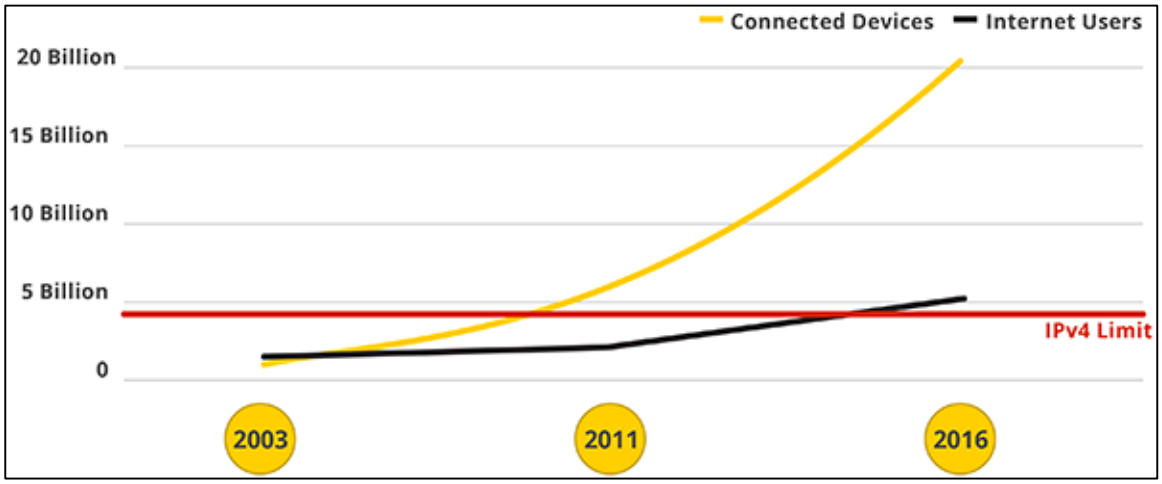


Figura: 9 Crecimiento de conexiones de IPv6
Fuente: (Google, 2015)

La figura 9 muestra el crecimiento y demanda de direcciones IP requeridos por los dispositivos que se encuentran en línea hoy y aquellos que estarán en el futuro: computadoras, teléfonos, televisores, relojes, refrigeradores, automóviles, y así sucesivamente. Más de 4 millones de dispositivos ya comparten direcciones. Como IPv4 se queda sin direcciones libres, todo el mundo tendrá que compartir.

CAPÍTULO III

ANALISIS DE LOS MECANISMOS DE TRANSICIÓN DE IPv4 a IPv6

3.1. Introducción

La sociedad está basada en la comunicación, que es un proceso que consiste en comunicar a la persona y a los individuos que se ponen en contacto e intercambian datos e información, es decir un emisor que envía mensajes al receptor dicha información inicia un proceso de comunicación que solo es posible entre los dos individuos que comparten un conjunto de símbolos, en el caso de los seres humanos es el lenguaje.

Con esta contextualización las redes de ordenadores siguen siendo los medios necesarios para el proceso de comunicación cables, fibra, módems que emiten información entre el emisor y el receptor de extremo a extremo.

3.2. Mecanismos de transición a IPv6

En la actualidad existen muchos mecanismos para llevar a cabo la transición de los protocolos, la migración depende de cómo los ISP's tengan implementado la infraestructura de la red, la distribución, las tecnologías, las aplicaciones y servicios propios y así como la configuración de los usuarios, ya que esto supone un serio

inconveniente a la hora de ejecutar una transición acorde a los requerimientos del proveedor de internet y el usuario.

Es por ello que para una migración total a IPv6 es recomendable ejecutar una transición sistemática de forma gradual mientras coexistan los dos protocolos IPv4 e IPv6.

Los mecanismos de transición de IPv4 a IPv6 se describen para la ejecución de los ISPs que no se podrán realizar si estos no compran equipos robustos que tengan soportes IPv6, además de aplicaciones que muchas veces dependen de la capacidad de procesamiento de los paquetes generados por los protocolos.

En los países desarrollados tecnológicamente como Estados Unidos, Europa, Asia, ya se han evaluado ciertos mecanismos que permiten la coexistencia entre ambos protocolos lo que ha permitido en el Ecuador tener una referencia significativa de mecanismos que han tenido éxito para llevar a cabo una migración progresiva de las redes, así como de los equipos de los usuarios.

Considerando el soporte extendido de IPv6, esta extensamente disponible tanto para los host y routers, lo cual es necesario considerar métodos y mecanismos de transición que se han desarrollado de la mano con el nuevo protocolo versión 6, para la comunicación entre redes que están configuradas con el protocolo IPv4 a versión IPv6 , desde las redes

domésticas así como grandes empresas que tienen redes propias configuradas con el protocolo IPv4.

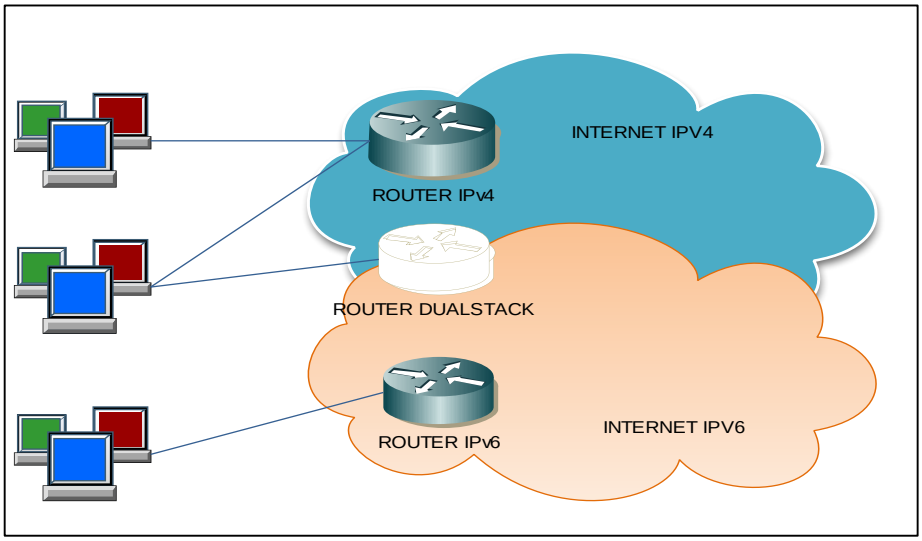


Figura: 10 Red IPv4 e IPv6
Fuente: (Castro, 2006, pág. 4)

Al existir topologías de red sobre IPv4 hay pocas redes (IPv6 -only), es por ello que se debe implementar mecanismos que permitan la coexistencia entre redes IPv4 e IPv6 antes de ser establecido el nuevo protocolo de forma definitiva.

En este sentido la realidad de los sitios que han implementado y desplegado el protocolo IPv6, no ejecutan la transición directamente a IPv6, sino que hacen una transición primero a un estado intermedio de coexistencia entre los protocolos IPv4 e IPv6, conocidos como mecanismos de transición que permiten introducir de forma gradual nodos IPv6 a medida que dejan de funcionar nodos IPv4.

Al migrar al nuevo protocolo desde pequeñas infraestructuras de una red IPv6 comprende un proceso complejo y difícil ya que existen elementos de red, topologías y tecnologías montadas sobre el protocolo anterior IPv4, es por ello que este proceso de adopción debe realizar de forma escalonada y progresiva empezando por la transición de los nodos internos (red ***core*** de los ISP´s), luego seguir con los nodos de acceso a internet y finalmente de los servicios.

Para seguir brindando servicios y garantizar la continuidad del negocio de los proveedores de servicio, se considera tener en cuenta que muchos requisitos y condiciones variadas, lo que hace necesario adoptar, evaluar y emplear varios mecanismos de transición según la particularidad de cada ISP's que pueden tener como: redes, subredes, tecnologías, varios tipos de elementos de distintos fabricantes.

El protocolo IPv6 ha sido diseñado para facilitar la transición y coexistencia con el protocolo IPv4, considerando que el despliegue de IPv6 tardara en ser desplegado sobre las redes de forma definitiva, por lo que se debe adoptar la coexistencia como medio de comunicación e interconexión entre redes IPv4 e IPv6.

Para la coexistencia de los protocolos a varios años se implementa tres mecanismos de transición:

- **Doble pila (DualStack):** permite coexistir IPv4 e IPv6 en un mismo dispositivo así como en una misma red.

- **Técnicas de túneles:** encapsula los paquetes IPv6 dentro de paquetes IPv4 esta técnica es la más utilizada y de uso común según las necesidades de cada proveedor de servicios de internet.

- **Técnicas de traducción:** Esta técnica permite la comunicación con dispositivos que son solo IPv6 con aquellos que son solo IPv4, aunque no es recomendable debido a que presenta una serie de inconvenientes y problemas.

Dependiendo de la complejidad de las redes, tecnologías, estos mecanismos suelen utilizarse de forma combinada.

3.2.1 Mecanismo DualStack

Conocido como DualStack o como dobla capa IP, este mecanismo puede manejar una pila IPv4 y una IPv6 de forma simultanea, dando soporte completo para los dos protocolos, es decir que los dispositivos con ambas pilas pueden recibir y enviar tráfico a nodos que soportan cualquiera de los dos protocolos como se ilustra en la Figura 11, también se puede configurar este mecanismos de forma manual cuando el usuario conoce la dirección IPv6 del nodo destino.

Dual Stack puede configurar y desplegar IPv6 considerando que no está lo suficientemente habilitado en muchos dispositivos ya que depende del año de fabricación si este soporta o no, los equipos nuevos desde el años 2010 ya se encuentran habilitados,y de igual forma en los sistemas operativos.

Considerando esto conlleva a desplegar el mecanismo denominado DualStack, que se describe en el RFC 2893, donde el host y el router tiene acceso a los protocolos IPv4 e IPv6 incorporados como un componente al sistema operativo y se les denomina nodo IPv4/IPv6, La configuracion con las dos direcciones envían y reciben datagramas de los dos protocolos permitiendo la comunicación con cada nodo IPv4 o IPv6 dentro de una red, siendo asi la técnica de coexistencia de los dos protocolos antes de dar el paso a la migración solo con el protocolo IPv6

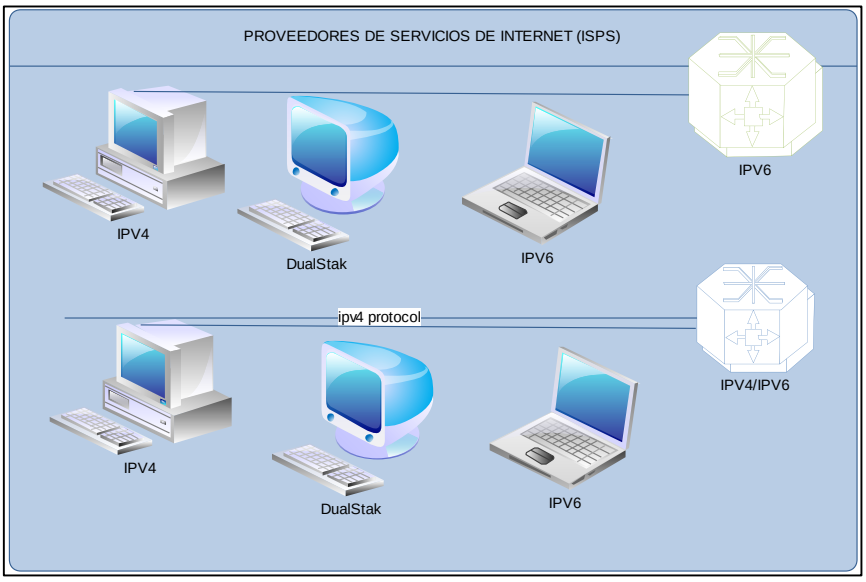


Figura: 11 Mecanismo DualStack
Fuente: ((Vives, 2014)

La técnica de doble pila habilita la transmisión de paquetes IPv4 a IPv6 sobre la misma infraestructura de la red mediante la implementación de ambas pilas en los dispositivos es decir gestiona tanto tráfico de IPv4 como de IPv6. Esta técnica proporciona una migración de forma más rápida que las demás técnicas.

Características de DualStack

- Maneja direcciones IPv4 e IPv6 a la vez.
- El DNS conoce las dos direcciones.
- Las aplicaciones conocen la existencia de la técnica Doble Pila.
- Del lado de los clientes que usan A o A6/AAAA se conectan a direcciones V4 o V6.
- Servidores en 0.0.0.0 o ::
- Las aplicaciones (o librerías) escogen la versión de IP a utilizar en función de la respuesta DNS.
- Si el destino tiene un registro AAAA, utilizan IPv6, en caso contrario IPv4.
- Permite la coexistencia indefinida de IPv4 e IPv6, y la actualización gradual a IPv6.

Inconvenientes

- Dual Stack requiere de soporte de los dos protocolos tanto IPv6 como IPv4 en cada uno de los enlaces y nodos seleccionados.
- Soporte en los hosts.
- Soporte en cada routedor o elementos que tenga la red.
- Soporte en las aplicaciones y servidores sobre todo en (web, DNS, SMTP).
- Se debe añadir componentes físicos y lógicos a nivel de seguridad.
- Requiere de nuevas políticas dependientes de las cualidades específicas de IPv6.

3.2.2 Técnica de túneles

La técnica de Tunel se utiliza a menudo en la infraestructura completa, o partes de ella, no es todavía capaz de ofrecer funcionalidad de IPv6 nativa. Por lo tanto el tráfico IPv6 tiene que cruzar la red IPv4 existente, que es posible con diferentes técnicas de construcción de túneles. Estas técnicas se eligen a menudo como un primer paso para probar el nuevo protocolo y para iniciar la integración de IPv6. (Technologies, 2008, pág. 61)

Los Túneles también se llaman encapsulación. Es un proceso mediante el cual se encapsula información de un protocolo dentro del paquete del otro protocolo, permitiendo así a los datos originales ser prorrogados en el segundo protocolo.

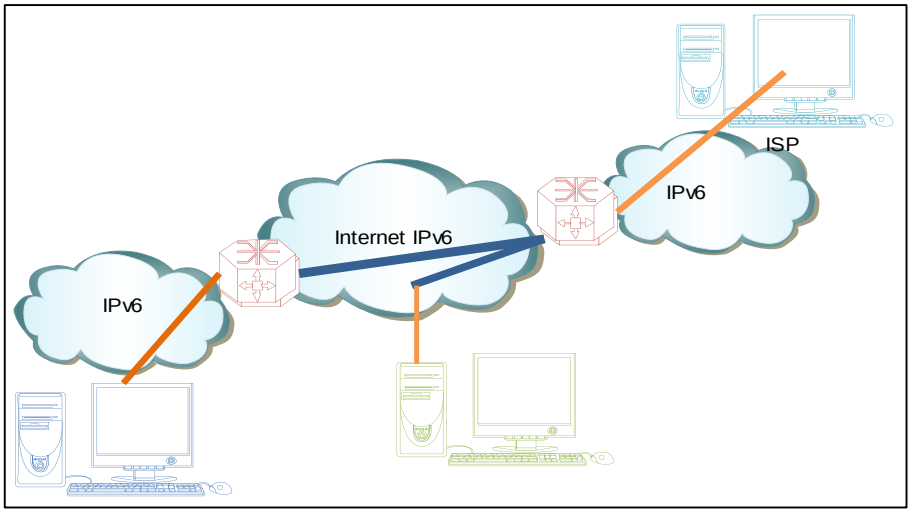


Figura: 12 Mecanismo túnel IPv6 en IPv4
Fuente: (Armendáris, 2007)

Este mecanismo puede utilizarse cuando dos nodos o redes que utilizan el mismo protocolo quieren comunicarse a través de una red que utiliza otro protocolo de red. El proceso de construcción de túneles implica tres pasos:

- Encapsulación
- Des encapsulación
- Administración del túnel

Existen varios tipos de túneles que manejan esta técnica denominada “tunelling”, que se describen a continuación.

- Túneles configurados.

- Túneles automáticos.
- Túneles 6to4.
- 6bone/m6bone.

Se sequiere dos extremos de túnel, que en el caso general son los nodos doble pila IPv4/IPv6 enrutadores, para manejar la encapsulación y des encapsulación. Existirá problemas de desempeño asociados con túneles, tanto para la latencia en (en/de) encapsulamiento y el ancho de banda adicional usado.

En general, un túnel de paquetes IPv6 en una red IPv4 implica prefijando un paquete IPv6 con un encabezado IPv4. Esto permite que el paquete tunelado sobre una infraestructura de enrutamiento IPv4, los paquetes IPv6 se consideran simplemente carga dentro del paquete IPv4. El nodo de entrada del túnel, ya sea un encaminador o host, realiza la encapsulación.

3.2.2.1 Túneles configurados

Los túneles configurados se actualizan en el RFC2893 como túneles IPv6 sobre IPv4, esta configuración se realiza bajo la técnica denominada punto a punto y que se debe configurar de forma manual en los extremos ya que las direcciones del protocolo versión 4 dependen de la configuración de dichos nodos en ambos extremos. Este proceso es tedioso ya que intervienen los administradores de red tanto del proveedor de servicio de

internet así como el administrador de la organización para llevar a cabo este procedimiento.

Esta técnica de túneles configurado se utiliza de forma extendida en la conexión que provee conectividad en el protocolo IPv6 al exterior para redes completas de las empresas. Estos túneles son utilizados de forma extendida en mbone, multiprotocolo (IPX, Appletalk), sobre IP, MIP.

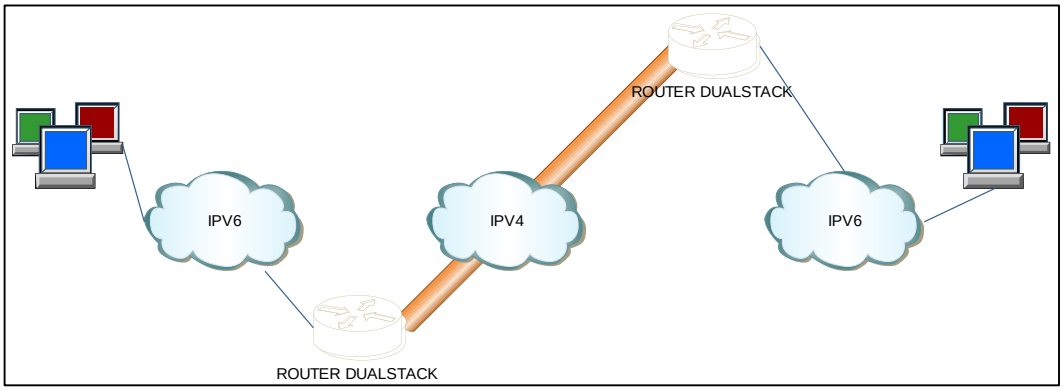


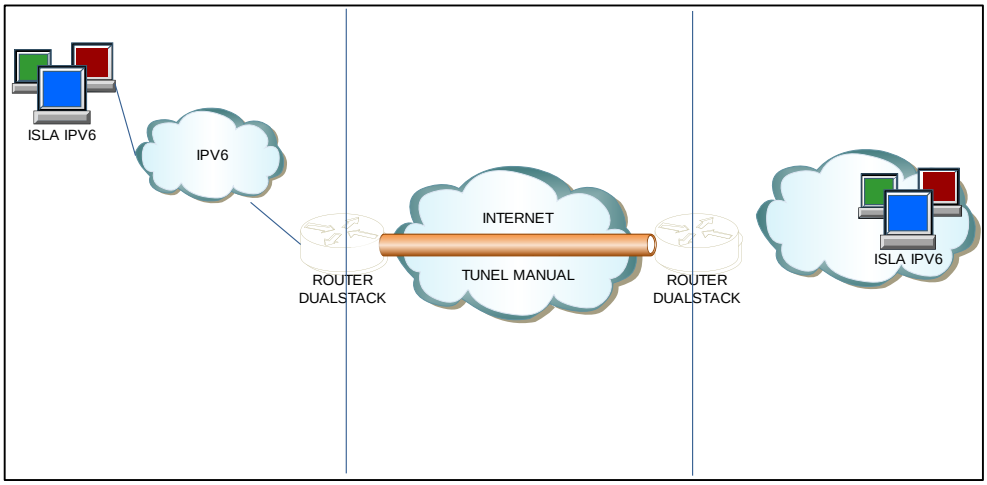
Figura: 13 Mecanismo túnel configurados
Fuente: (Fo Olivert, 2011)

Esta técnica de túnel configurado tiene la característica y particularidades específicas sobre nodos finales que deben ser configurados por los ISP.

- Comunica dos routers de frontera
- Proporciona conexiones seguras y estables
- Conexión de redes IPv6 aisladas
- Los routers necesitan direcciones IPv4 e IPv6, deben de tener pilas duales.
- Requiere de rutas estáticas en cada extremo del tunel

3.2.2.2 Túneles manuales

El túnel manual, es la configuración estática de un túnel, utilizan una relación de direcciones IPv4 con IPv6 de forma estática y solamente podrá transportar paquetes de IPv6 a islas previamente establecidas. Se concidera las limitantes de un túnel manual similares a las limitantes de rutas estáticas. Este método permite la comunicación interna de las redes LAN o comunica dos nodos cuando la ruta no radica en IPv6.



Figura; 14 Mecanismo túnel manual
Fuente: (Ralli, Macanismos de transicion de IPv4 a IPv6, 2007)

Túnel tiene una serie de ventajas pero requiere la implementación del método dual:

- Su función es de interconectar islas de IPv6 a través de redes versión IPv4.
- Cada extremo es un nodo dual que se debe configurar direcciones IPv4 e IPv6 tanto locales como remotas.
- Método utilizado para el acceso a l 6-Bone.

- Está integrado y disponible en las distintas plataformas.

- Es un método trasparente respecto al nivel de IPv6, superiores con lo cual no afecta a las aplicaciones.

- No requiere o consume excesivamente los recursos de red, así como no excede la unidad máxima de trasferencia (MTU) en 20 bytes típica de IPv4.

- Permite la conexión principal con el ISP -IPv6 de forma remota a través de internet. (Ralli, Mecanismos de Transicion , 2012)

Inconvenientes

- No se implementan de forma dinámica, sino que requieren de configuraciones manuales o en modo semiautomático.

- Si se va intercomunicar N islas y la topología de red no considera un nodo central o intercambiador el número de túneles a implementar en cada sitio crese exponencialmente de N-1.

- Si de ser el caso se va a conectar entre si miles de islas IPv6 distribuidas por internet este método no es funcional.

3.2.2.3 Túneles Bróker

Este método es un intermediario al que los usuarios finales se conectan a través de una interfaz web. El usuario solicita al bróker crear un túnel que le asigne una dirección IPv6 proporcionando las instrucciones para dicha solicitud en el lado del usuario.

El TB también configura el router que representa al extremo final del túnel para el usuario también existe TSP que es un caso especial de TB que no está basado en un interfaz web sino en una aplicación cliente que instala el usuario y se conecta con un servidor.

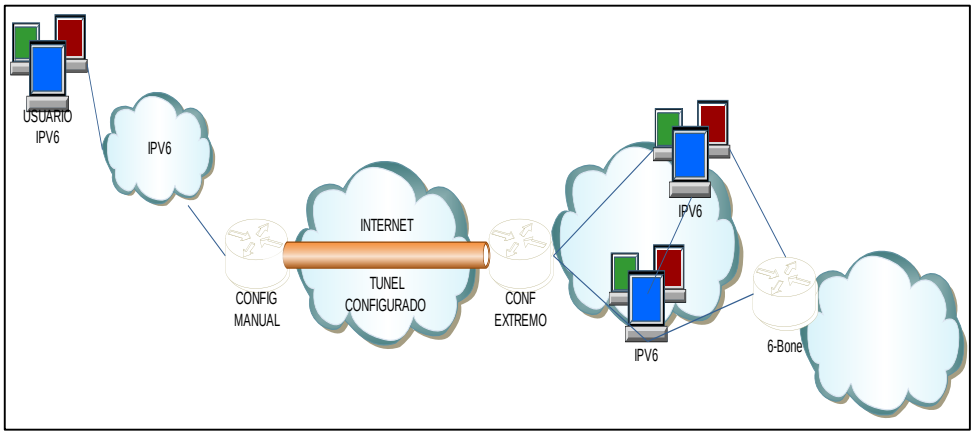


Figura: 15 Mecanismo túnel Bróker
Fuente: (Ralli, Macanismos de transicion de IPv4 a IPv6, 2007)

Este tipo de túnel bróker permite que en vez de configurar de forma manual cada extremo de los túneles, se remplace a través de un script para automatizar el proceso si las direcciones IPv4 globales son dinámicas y son definidas por RFC 3053.

El túnel al igual que los métodos manuales es de utilidad cuando un host debe conectarse a una red IPv6 y si el Sistema Operativo tiene DualStack. TB requiere que el proveedor

de servicio de túnel bróker debe facilitar el servicio HTTP para IPv4 y disponer de un router dual Stack capaz de aceptar la configuración por comandos automáticos que permiten crear túneles nuevos hacia el host remoto de los usuarios.

Los TB´s, constituyen importantes herramientas de ayuda a la transición ya que habilitan de forma fácil el acceso a redes IPv6, aunque se debe considerar los saltos que deben dar todos los paquetes de tráfico con IPv6, y el tiempo de demora.

3.2.2.4 Túneles automáticos

Los túneles automáticos definidos en RFC 2893, permiten la interconexión de redes aisladas de IPv6 a través de infraestructura IPv4 ya que este método crea túneles de forma dinámica punto – multipunto que son encapsulados en paquetes IPv4.

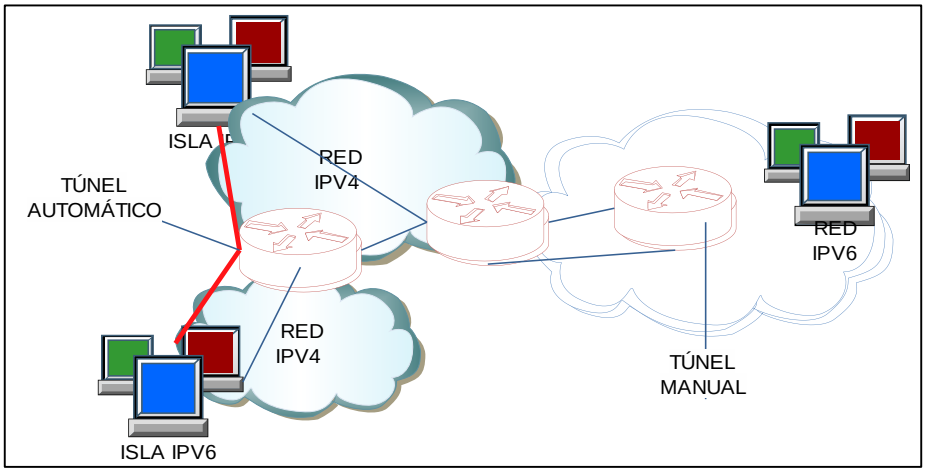


Figura: 16 Mecanismo túnel automático
Fuente: (Armendáris, 2007)

Características

- Permite a los nodos duales la comunicación a través de una infraestructura IPv4.
- Permite que las direcciones IPv6 sean compatibles con IPv4 con el prefijo 0::/16 mas la dirección IPv4.
- Cuando un router 6to4 ve un paquete de prefijo 2002::/16 lo encapsula en IPv4 hacia la IP pública, permitiendo definir virtualemnte la interfaz para que se compatible con las direcciones IPv4
- Los paquetes destinados a direcciones IPv4 se envían por el túnel automático.

Para permitir que los host asi como las topologías de red que utilizan 6to4 intercambien tráfico con redes IPv6 nativas se definieron Routers Relay según RFC 3068, estos ruteadores interconectan redes IPv4 con redes IPv6, los paquetes 6to4 que son enviados desde el router relay desde una interfaz IPv4 son des encapsulados y enviados hacia la red IPv6 nativa cuya dirección sea IPv6 con prefijo 2002::/16 se encapsulan en paquetes IPv4 hacia la red IPv4.

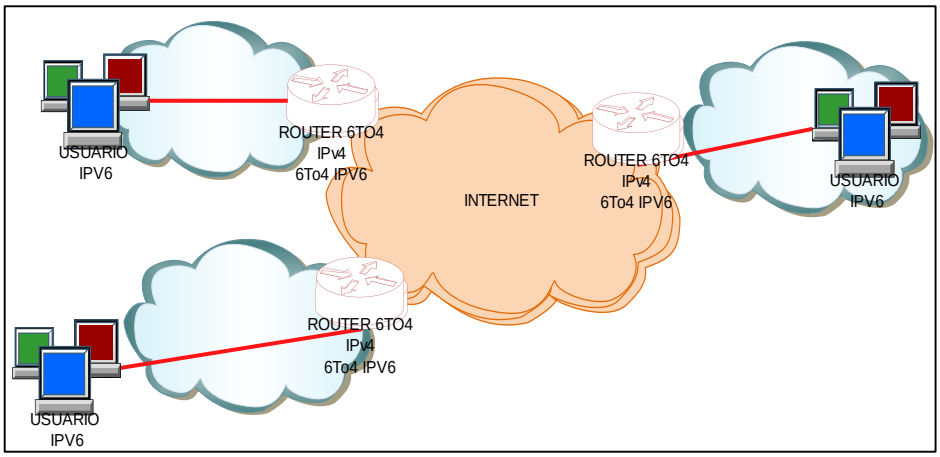


Figura: 17 Mecanismo túnel 6To4
Fuente: (Armendáris, 2007)

Características

Al igual que los túneles configurados de forma manual estos son trasparentes a nivel de IPv6 y por lo tanto no afectan a las aplicaciones. Al ser túneles definidos de forma dinámica y sin configuración previa.

- Dadas N islas en IPv6 solo es necesario crear y establecer los túneles para conexiones activas en el momento de ser solicitados.

- Un host en la ubicación 6to4 Site A envía una transmisión que especifica como destino un host en la ubicación IPv6 nativa Site B. El encabezado de cada paquete tiene una dirección derivada 6to4 como dirección de destino. La dirección de destino es una dirección IPv6 estándar.

- El enrutador 6to4 de la ubicación Site A encapsula cada paquete dentro de un encabezado IPv4, que tiene la dirección IPv4 del enrutador de reenvío 6to4 como destino.

- El enrutador 6to4 utiliza procedimientos IPv4 estándar para reenviar el paquete a través de la red IPv4. Cualquier enrutador IPv4 que encuentren los paquetes en su camino los reenviará al enrutador de reenvío 6to4.

- El enrutador de reenvío 6to4 de difusión por proximidad más cercano físicamente a la ubicación Site A recibe los paquetes destinados al grupo de difusión por proximidad.

- El enrutador de reenvío desencapsula el encabezado IPv4 de los paquetes 6to4 y, de este modo, revela la dirección de destino IPv6 nativa.

- El enrutador de reenvío envía paquetes, que ahora son sólo IPv6, a la red IPv6, donde los recibe un enrutador de la ubicación Site B. El enrutador reenvía los paquetes al nodo IPv6 de destino (ORACLE, 2010)

Inconvenientes

Para las organizaciones que se conectan a IPv6 remotos no es necesario implementar este mecanismo se debe implementar métodos de túneles manuales que su uso es más extendido.

- Error del dispositivo con el adaptador de red 6to4.
- Incompatibilidad con adaptadores de red con el protocolo IPv6.
- Adaptador 6to4 no permite actualizar los controladores.
- El adaptador 6to4 aparece con error Código 31, no permite actualizar los controladores, este error afecta la conectividad inalámbrica.

3.2.2.5 Túneles 6over4

Este método es una tecnología de túneles automáticos definido mediante el RFC 2529 que permite la conexión unicast y multicast de IPv6 entre los nodos de una intranet con infraestructura IPv4. Este método permite manejar infraestructura IPv4 mediante una asociación simple con capacidad de conectividad multicast mediante la resolución de direccionamientos y detectando ruteadores que trabajan con enlace físico que deben ser habilitados en IPv4, mapeando la red para traducir las direcciones IPv6 multicast en direcciones IPv4 multicast.

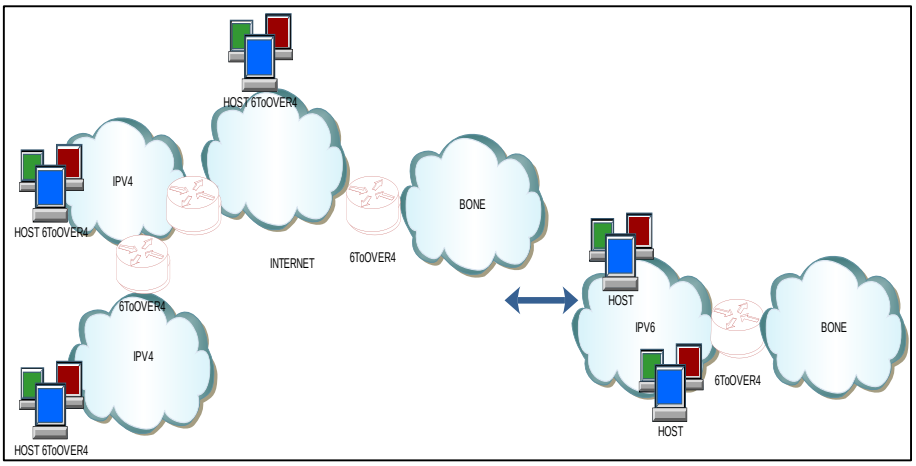


Figura: 18 Mecanismo túnel 6over4
Fuente: (Armendáris, 2007)

Características

- Nodos IPv6 dispersos sobre subredes IPv4 que permite formar una red LAN virtual IPv6.
- Todos los routers 6over4 con acceso a 6BONE son accesibles mediante este método.
- Permite el tráfico de paquetes IPv6 encapsulados en IPv4.
- Permite obtener direcciones IPv4 multicast

Inconvenientes

- Solo se implementa en redes finales únicamente.

- No se encuentra implementado de forma amplia en Windows.

3.2.2.6 Túneles Teredo

Teredo referido al RFC 4380, es un método de traslado de direcciones de red Network Address Translation (NAT) para IPv6 y diseñado para host IPv4 que tengan direcciones IPv6 a través de una o más capas de IPv6, mediante la creación de túneles con el protocolo UDP, los mecanismos automáticos de host a host se comunica con IPv6, mientras que los host Dual Stack están detrás de una o mas NATs encapsulando paquetes IPv6 en mensajes UDP de IPv4. Taredo usa dos entidades que se describe a continuacion.

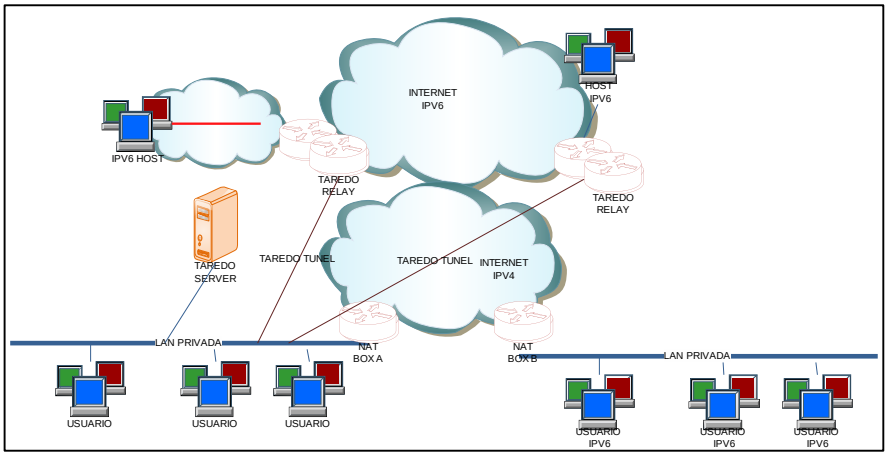


Figura: 19 Mecanismo túnel Teredo
Fuente: (Armendáris, 2007)

Server Teredo: Escucha los requeriemientos de los clientes a traves del puerto 3544 del protocolo UDP resolviendo con direcciones IPv6 mediante la siguiente estructura.

- Prefijo Teredo (32 bits) : Dirección IPv4 del Servidor Teredo : Flags (16 bits)

- Estructura:: Puerto externo (16 bits) : Dirección externa (32bit).

Relay: Envia paquetes IPv6 con IPv4 encapsulados desde el cliente Teredo Relay actuando como un router. Esta tecnica debe ser considerada como ultimo recurso.

Caracteristicas

- Muchas de las redes corporativas tienen experiencia en la administracion, implementacion de redes NATs.
- Es implementable en las tecnologias de routers Cisco, Telebit, Linux, asi como en plataformas de nodos finales windows server.
- Si la comunicación de extremo a extremo es heterogenia (IPv4 a IPv6) NAT.PT es adecuado pero se debe considerar la carga del trafico previsto.

Inconvenientes

- Método complejo de configurar además no asegura o garantiza que trabaje de forma correcta debido a las distintas implementaciones de NATs existentes.
- No funciona en NATs de tipo Symmetric (Solventado en Windows Vista). Se debe configurar el server también como relay si solo tiene conectividad IPv6 con otros clientes de Teredo.

- Tener NAT no es recomendable por el alto costo de administración y gestión que estas requieren para ser implantadas.

- La traducción es más costosa en términos de recursos que se requieren para llevar a cabo este proceso.

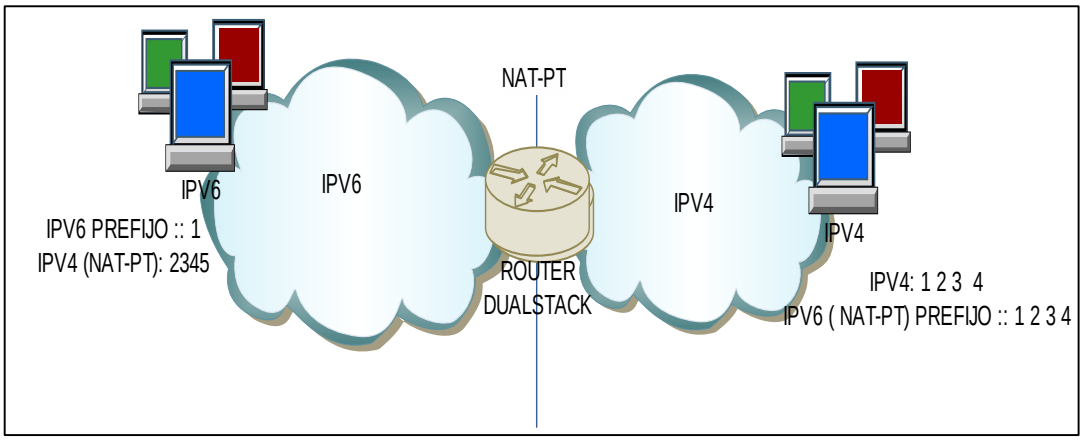
- Si en los protocolos de aplicación intercambian direcciones IP DNS, FTP, SMTP, se requiere de una extensión que debe incluir algoritmos para darle tratamiento específico según la aplicación que lo requiera.

3.2.3. Mecanismo de traducción

El método de traduccion utiliza elementos de red que permite la conversión de paquetes de IPv4 a IPv6 y viceversa, permitiendo la traducción y comunicación bidireccionalmente, existen algunos métodos como:

3.2.3.1.Traducción de Dirección de Red/Traducción de Protocolo (NATPT)

Este método de traducción definido en el RFC 2766, a nivel de puertos además de las direcciones que se envían a través de la red, permite evitar que dos host del mismo lado del mecanismo utilicen el puerto al otro lado del método.



Figura; 20 Mecanismo de traducción NAT-PT
Fuente: (Ucedo, 2004)

Características

- NAT- Tradicional: Traduce direcciones entre conexiones de redes con direcciones IPv4 privadas.
- NAT- PT. Traduce direcciones y protocolos en host.
- Mecanismo de traducción que se basa en algoritmo Stateless IP/ICMP Translation SIIT (RFC 2765).
- No traduce de forma trasparente a nivel de las aplicaciones.
- Traduce protocolos IPv6 a IPv4, para nuevos tipos de dispositivos de internet como celulares, vehículos y dispositivos móviles.
- Evita que dos hosts en el mismo lado del mecanismo utilicen el mismo puerto al otro lado.

Inconvenientes.

- Problemas de escalabilidad de redes, host y demás dispositivos de comunicación de la red.

- Causa inestabilidad de las aplicación o fallos de seguridad por lo que este mecanismo esta obsoleto.

- Se debe tener cuidado con los protocolos que no atraviesan NAT, ya que pueden ser accedidos por intrusos y se ocaciona un serio problema de seguridad.

- NAT, tiene un alto costo de administracion y se vuelve compleja la gestion ya que la seguridad es un punto critico al implemntar este metodo.

- Requiere gran cantidad de recursos en el proceso de traduccion mas que los metodos de tunel.

- Si la comunicacion extremo-extremo es homogenea no se recomienda este método ya que al tener dos sistemas de traduccion consecutivos es inadecuado.

- Si en los protocolos de aplicación intercambian direcciones IP (DNS, FTP, SMTP,…se requiere de una extensión que debe incluir algoritmos para darle tratamiento específico según la aplicación que lo requiera (DNS- ALG FTP-ALG).

CAPÍTULO IV

PROPUESTA DE MIGRACION DE IPv4 A IPv6 PARA LOS ISP's

4.1 Etapa de Planificación

La presente fase de planificación nos permite identificar y establecer planes a futuro para determinar el proceso necesario y llevar a cabo la adopción del nuevo protocolo IPv6 juntamente con el protocolo IPv4 para los ISP's que desean y a su vez deben implementar direcciones IPv6 para los usuarios finales, esta fase permite evaluar toda la información que posee cada proveedor y así aportar con un resultado favorable y recomendable.

Su principal objetivo es: Determinar los recursos económicos y humanos necesarios para delegarles funciones y responsabilidades en cada área y llevar a cabo el proyecto de adopción de IPv6 y coexistencia de los dos protocolos.

La presente descripción de la etapa de Planificación es: la selección del personal que va estar a cargo en cada área de TI, para la ejecución del proyecto y adopción de IPv6 con IPv4, se debe elegir en función de las capacidades, responsabilidades y funciones necesarias para la implementación de la red con el nuevo protocolo, en la siguiente tabla 5, se describe el personal requerido para llevar a cabo la migración y coexistencia de los dos protocolos.

Tabla: 5. Definir el equipo de técnicos para Implementar IPv6.

PERSONAL ADMINISTRATIVO		
ÁREA	Administración TI	DESCRIPCIÓN DEL PUESTO
CARGO	Director TI	Persona con capacidad técnica de guiar y dirigir al personal, un líder inspirador que sirva como modelo para todos sus trabajadores con la finalidad de obtener un buen clima laboral y de esta manera, asegurar que se cumplan las tareas encomendadas y guiadas hacia el cumplimiento del objetivo de la implementación de IPv6.
FUNCIONES RESPONSABILIDADES		Diseñar y aprobar el proyecto de implementación de IPv6, equipo, presupuesto e inversión de infraestructura de TI necesaria. Dirigir el desarrollo de las actividades de adopción de IPv6 en el ISP. Controlar y revisar el cronograma de actividades del proyecto Controlar el cumplimiento de los planes de programas de implementación de IPv6 en el ISP. Dirigir y supervisar al personal técnico bajo su cargo. Analizar la información generada en el departamento de redes para la toma de decisiones. Comunicar e informar el estado y avance del proyecto de IPv6 a los accionistas. Cumplir y hacer cumplir las leyes y políticas establecidas por los entes que regulan el negocio.

REQUISITOS		Tener conocimientos en sistemas, redes, plataformas, comunicaciones, desarrollo de aplicaciones, manejo de redes y subredes. Conocimiento en diseño y ejecución de proyectos de TI. Capacidad de relacionamiento Orientación a resultados
PERSONAL REDES		
ÁREA	Redes	DESCRIPCIÓN DEL PUESTO
CARGO	Jefe redes	Persona con capacidad técnica y conocimientos específicos en la planificación, administración y gestión de redes de información y datos, capaz de asegurar el funcionamiento y trasmisión de la información y de servicios de comunicación a los clientes.
FUNCIONES RESPONSABILIDADES		Diseñar redes de datos y comunicaciones. Desarrollar actividades de configuración y administración de redes y datos. Diseñar la topología de red de IPv6. Controlar y revisar el cronograma de actividades del proyecto Implementar mecanismos de coexistencia entre los protocolos Ipv4 – Ipv6 Dirigir y supervisar al personal técnico bajo su cargo. Configurar el proceso de implementación de IPv6 en cada plataforma, hardware y aplicaciones que sean afectadas.

		Levantar un inventario del hardware, software, plataformas y aplicaciones que cuenta el ISP. Realizar las pruebas necesarias de funcionamiento de IPv6. Comunicar e informar el estado y avance del proyecto de IPv6 al Director de TI. Cumplir y hacer cumplir las leyes y políticas establecidas por los entes que regulan el negocio
REQUISITOS		Tener conocimientos en redes, plataformas, comunicaciones, manejo de redes y subredes, enrutamiento, direccionamiento, mecanismos de coexistencia. Conocimiento en diseño y ejecución de proyectos de redes de datos de TI. Certificación CISCO Capacidad de relacionamiento. Orientación a resultados.
Definir el equipo de técnicos para implementar Ipv6		
ÁREA	Redes	DESCRIPCIÓN DEL PUESTO
CARGO	Personal técnico y de soporte	Persona con capacidad técnica y conocimientos específicos en la planificación, administración y gestión de redes de información y datos, capaz de asegurar el funcionamiento y trasmisión de la información y de servicios de internet y comunicaciones a los clientes.
		Desarrollar actividades de configuración y administración de redes y datos. Diseñar la topología de red de ipv6.

FUNCIONES RESPONSABILIDADES	Implementar mecanismos de coexistencia entre los protocolos IPv4 – IPv6. Configurar el proceso de implementación de IPv6 en cada plataforma, hardware y aplicaciones que sean afectadas. Levantar un inventario del hardware, software, plataformas y aplicaciones que cuenta el ISP. Realizar las pruebas necesarias de funcionamiento de IPv6. Cumplir y hacer cumplir las leyes y políticas establecidas por los entes que regulan el negocio.
REQUISITOS	Tener conocimientos en redes, plataformas, comunicaciones, manejo de redes y subredes, enrutamiento, direccionamiento, mecanismos de coexistencia. Conocimiento en diseño y ejecución de proyectos de redes de datos de TI. Certificación CISCO. Capacidad de relacionamiento. Orientación a resultados.

Fuente: Propia

4.1.1 Plan de inversión

En el plan de inversión los IPS deben tomar en cuenta un costo estimado para la adopción de IPv6 con IPv4, ya que todo proyecto de tecnología requiere de una planificación de inversión económica la cual está orientada a la adquisición y al mejoramiento de la

infraestructura de tecnología que disponen los ISP's, con el fin de garantizar la continuidad del negocio y por ende el mejoramiento del servicio a los clientes.

Su objetivo principal es determinar si se debe adquirir nuevos equipos, el costo económico y beneficio para los ISP's, en la adopción del nuevo protocolo de IPv6.

Descripción: En esta etapa los IPS's deben de decidir y considerar de carácter económico financiero que en la adopción del nuevo protocolo se requiere de una inversión económica ya que es aconsejable la compra de nuevos equipos que soporten el nuevo IPv6, y por ende la capacitación requerida para el personal seleccionado y llevar acabo la adopción de Ipv6. Los ISP's, deben tener en cuanta un plan de inversión como se describe en la tabla 6.

Tabla: 6. Plan de Inversión

PLAN DE INVERSIÓN
1. Antes de realizar una inversión en tecnología, los ISP's deben realizar un análisis de la infraestructura de la red para el acoplamiento de la adopción al nuevo protocolo y la tecnología en las actividades de la organización. 2. Fijar un objetivo de lo que se quiere lograr. Qué se pretende obtener con la adopción al nuevo protocolo. 3. Crear un plan de cómo conseguir los objetivos hacia el nuevo IPv6, una vez fijado los objetivos, cómo se piensa alcanzarlos, que procedimiento se va a seguir, quién o quiénes serán los responsables. 4. Realizar un plan para ver los recursos que serán necesarios en la aplicación de la tecnología. 5. Prever que puede fallar. Realizar revisiones en el proceso de integración de tecnología para obtener alertas de posibles fallas en el mismo.

Fuente: Propia

- Para el desarrollo del proyecto de adopción de tecnologías y la implementación del protocolo IPv6 se requieren los siguientes recursos como; personal capacitado, equipos de comunicación, materiales, entrenamiento y capacitación para la adopción de IPv6 en el ISP. En la siguiente tabla se describe un costo estimado para la compra y capacitación necesaria que requiere la adopción de IPv6. Tabla 7

Tabla 7. Presupuesto Estimado

RECURSOS	CANTIDAD	VALOR UNITARIO	PRESUPUESTO
1. Humanos			
Personal administrativo	80 h	30,00	2400,00
Personal redes	80 h	30,00	2400,00
Personal técnico y de soporte	80 h	30,00	2400,00
TOTAL A			7200,00
2. Equipos			
Cisco SG300-28 28-Port Gigabit Switch gestionab	5	500,00	2500,00
Cisco switch cisco 2960	5	1500,00	7500,00
Smart cart IOS 15	5	500,00	2500,00
Cisco 1800 Serie (1841) Equipos cliente	15	150,00	2250,00
TOTAL B			14750,00
3. Materiales			
Cable	10	150,00	1500,00
Laptop	1	00,00	00,00
Sub-Total			23450,00
15 + % DE IMPREVISTOS			3518,00
TOTAL			26968,00

Fuente: Propia

Financiamiento: Propios (100%) Auspicio (0%) Entidades Financieras (0%)

Todos los gastos económicos que interfieren en el desarrollo del presente proyecto son costeados por los accionistas del Proveedor de Servicios ISP, que necesitan para poner en marcha y mantener el funcionamiento y así garantizar el servicio continuo a los proveedores.

Nota: Los costos y equipos pueden variar según el portafolio de clientes que maneje cada ISP, los equipos con los que se realiza el presupuesto son de marca **CISCO**.

4.1.2 Capacitación y entrenamiento

En el etapa de capacitación los ISP's deben considerar un factor importante para capacitar al personal de gestión de infraestructura de tecnología y obtener un mejor desempeño para el manejo de nuevas tecnologías y formas de comunicación entre dispositivos hardware, software y comunicaciones, con esta actividad permite cambiar la forma de trabajar y mejorar el desempeño del personal aportando ventajas competitivas en adopción e integración de nuevas tecnologías al negocio.

Su objetivo principal es proporcionar los conocimientos, habilidades y entrenamiento necesario para el personal técnico que desempeñe su trabajo dentro de la empresa para la implementación del protocolo IPv6.

Descripción. El propósito básico de la etapa de capacitación y entrenamiento es que el personal mejore su desempeño en el trabajo, y así identificar al personal y designarles sus funciones en cada área con sus habilidades y conocimientos necesarios para adoptar el protocolo IPv6 en los ISP's.

- Los ISP's deben tener en cuenta que la capacitación no se debe realizar una sola vez ya que es un proceso continuo para el mejoramiento de los conocimientos y habilidades del personal y así ellos estar preparados y aportar su conocimiento para resultados favorecidos a los ISP's, en la tabla 8 se describe al personal para la capacitación.

Tabla 8. Plan de capacitación

CAPACITACION		
Capacitación / entrenamiento	Director TI	Servicios de internet. Capacitación para dar soporte del protocolo IPv6 en la red CORE. Soporte para evaluar y adoptar mecanismos de transición para los clientes. Soporte para configurar nodos finales con mecanismos de transición IPv4 e IPv6. Soporte para instalar, actualizar y configurar plataformas, aplicaciones de los equipos de los clientes. Capacitación para evaluar la red, equipos y versiones de software Posibles nuevas adquisiciones, fabricantes y modelos. Evaluación de OS

		Evalaur aplicaciones de tercero
	Jefe redes	Capacitación para dar soporte del protocolo IPv6 en la red CORE. Soporte para evaluar y adoptar mecanismos de transición para los clientes. Soporte para configurar nodos finales con mecanismos de transición IPv4 e IPv6. Soporte para instalar, actualizar y configurar plataformas, aplicaciones de los equipos de los clientes. Evaluar la red, equipos y versiones de software Evaluación de Sistemas Operativos Evalaur aplicaciones de tercero
	Personal técnico soporte	Soporte para evaluar y adoptar mecanismos de transición para los clientes. Soporte para instalar, actualizar y configurar plataformas, aplicaciones de los equipos de los clientes. Evaluar red, elementos equipos y versiones de OS. Evaluar red, elementos equipos y versiones de software Evaluación de aplicaciones propias y de terceros.

Fuente: Propia

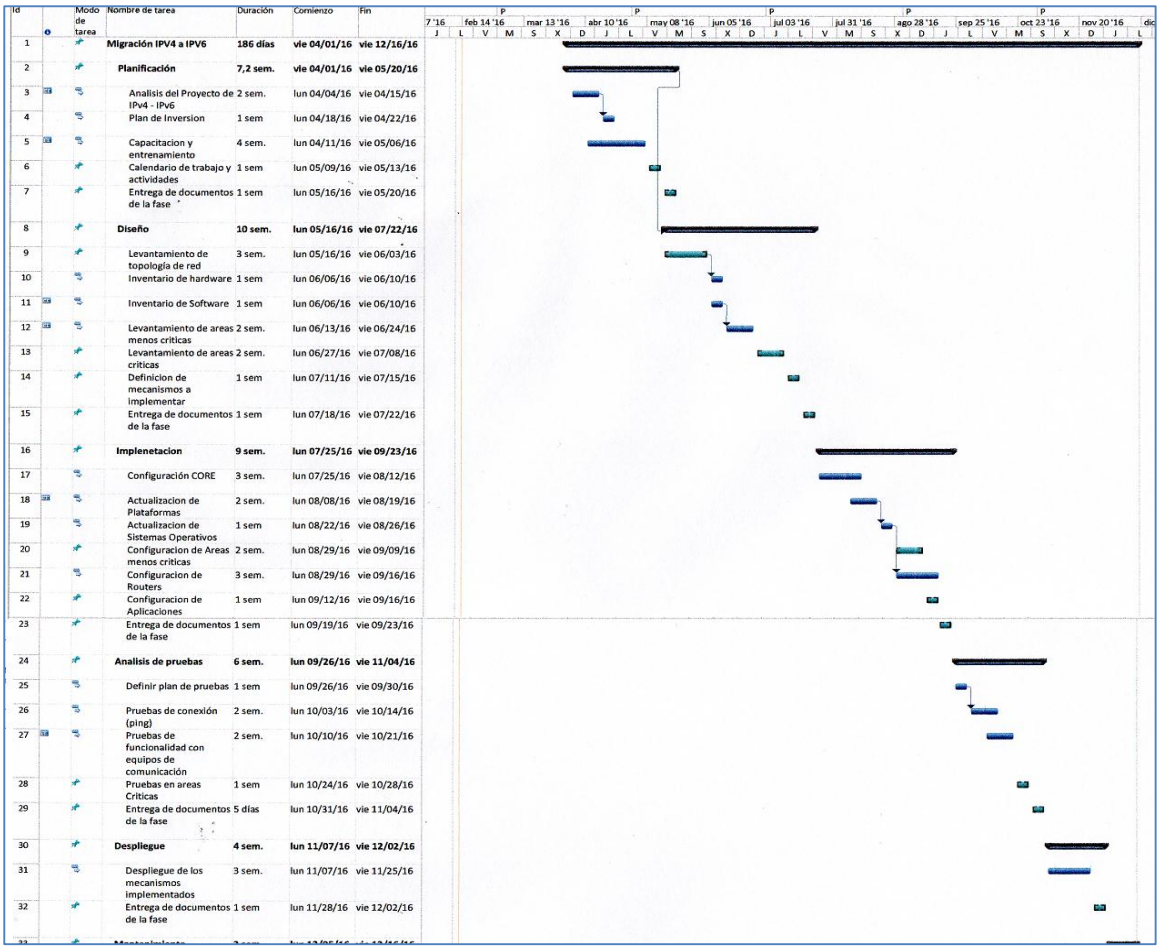
En este aspecto se debe tomar en cuenta que la capacitación y entrenamiento del personal involucrado para la implementación del nuevo protocolo debe ser entrenado en el área asignada de la infraestructura tecnológica, la propuesta está definida con tecnología CISCO, en el aspecto de hardware de comunicaciones y plataformas Windows.

4.1.3 Calendario de actividades

En esta etapa es importante que los ISP's establezcan un cronograma de actividades para el proceso de gestión y control, es decir el tiempo que se va a llevar a cabo la consecución del proyecto de la coexistencia entre IPv4 – Ipv6, tomando en cuenta que la migración a IPv6 no se puede realizar de la noche a la mañana ya que los dos protocolos coexistirán durante algunos años.

Además permite controlar cada una de las fases, actividades a desarrollar permitiendo verificar el cumplimiento de cada uno de los factores que crean cambios en el cronograma y tomar las respectivas acciones correctivas o preventivas mientras dure el proyecto. El calendario de actividades permite distribuir y organizar las funcionalidades de cada personal capacitado.

Su objetivo principal es elaborar el cronograma de actividades asociada a cada uno de las actividades a desarrollar para preparar la infraestructura de red que adoptara IPv6.



Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin
1		**Migración IPV4 a IPV6**	**186 días**	**vie 04/01/16**	**vie 12/16/16**
2		**Planificación**	**7,2 sem.**	**vie 04/01/16**	**vie 05/20/16**
3		Analisis del Proyecto de IPv4 - IPv6	2 sem.	lun 04/04/16	vie 04/15/16
4		Plan de Inversion	1 sem	lun 04/18/16	vie 04/22/16
5		Capacitacion y entrenamiento	4 sem.	lun 04/11/16	vie 05/06/16
6		Calendario de trabajo y actividades	1 sem	lun 05/09/16	vie 05/13/16
7		Entrega de documentos de la fase	1 sem	lun 05/16/16	vie 05/20/16
8		**Diseño**	**10 sem.**	**lun 05/16/16**	**vie 07/22/16**
9		Levantamiento de topología de red	3 sem.	lun 05/16/16	vie 06/03/16
10		Inventario de hardware	1 sem	lun 06/06/16	vie 06/10/16
11		Inventario de Software	1 sem	lun 06/06/16	vie 06/10/16
12		Levantamiento de areas menos criticas	2 sem.	lun 06/13/16	vie 06/24/16
13		Levantamiento de areas criticas	2 sem.	lun 06/27/16	vie 07/08/16
14		Definicion de mecanismos a implementar	1 sem	lun 07/11/16	vie 07/15/16
15		Entrega de documentos de la fase	1 sem	lun 07/18/16	vie 07/22/16
16		**Implenetacion**	**9 sem.**	**lun 07/25/16**	**vie 09/23/16**
17		Configuración CORE	3 sem.	lun 07/25/16	vie 08/12/16
18		Actualizacion de Plataformas	2 sem.	lun 08/08/16	vie 08/19/16
19		Actualizacion de Sistemas Operativos	1 sem	lun 08/22/16	vie 08/26/16
20		Configuracion de Areas menos criticas	2 sem.	lun 08/29/16	vie 09/09/16
21		Configuracion de Routers	3 sem.	lun 08/29/16	vie 09/16/16
22		Configuracion de Aplicaciones	1 sem	lun 09/12/16	vie 09/16/16
23		Entrega de documentos de la fase	1 sem	lun 09/19/16	vie 09/23/16
24		**Analisis de pruebas**	**6 sem.**	**lun 09/26/16**	**vie 11/04/16**
25		Definir plan de pruebas	1 sem	lun 09/26/16	vie 09/30/16
26		Pruebas de conexión (ping)	2 sem.	lun 10/03/16	vie 10/14/16
27		Pruebas de funcionalidad con equipos de comunicación	2 sem.	lun 10/10/16	vie 10/21/16
28		Pruebas en areas Criticas	1 sem	lun 10/24/16	vie 10/28/16
29		Entrega de documentos de la fase	5 días	lun 10/31/16	vie 11/04/16
30		**Despliegue**	**4 sem.**	**lun 11/07/16**	**vie 12/02/16**
31		Despliegue de los mecanismos implementados	3 sem.	lun 11/07/16	vie 11/25/16
32		Entrega de documentos de la fase	1 sem	lun 11/28/16	vie 12/02/16

Figura: 21. Calendario de trabajo
Fuente: Propia

Las actividades del cronograma deben estar definidas en un tiempo considerado, para supervisar y controlar el avance de la migración de todas las actividades asignadas al personal y así lograr y llevar a cabo el proyecto de adopción del nuevo protocolo, estabilización la red y las aplicaciones que sean afectadas con el nuevo protocolo IPv6.

4.2 Etapa de Diseño

4.2.1 Inventarios de Hardware y Software

Al disponer de una infraestructura tecnológica y de la red que se encuentra funcionando sobre protocolo IPv4, es necesario realizar el inventario tecnológico del hardware para administrar y realizar un seguimiento para la adquisición de nuevos equipos con porte y soporte de IPv6 que no disponen los ISP.

4.2.2 Inventario hardware de servidores

Con el inventario de Hardware los ISP's analizaran que servidores soportan y no el protocolo IPv6 juntamente con IPv4. En la tabla 9 se muestra los servidores que posee el escenario del ISP tomado como ejemplo.

Tabla 9. Inventario de Hardware de Servidores

MARCA	ÁREA	SERIE	SERIES	OBSERVACIONES
HP	DMZ	HP CORE 7500	CN1AD5709S	Soporte IPv6
HP	CORREO	HP CORE 7500	CN1AD5709S	Soporte IPv6
HP	WEB	HP CORE 7500	CN1AD5709S	Soporte IPv6
HP	AD	HP CORE 7500	CN1AD5709S	Soporte IPv6

Fuente: Propia

En el anexo 1, se presenta una plantilla como modelo de ejemplo para el inventario, Ver anexo1

4.2.3 Inventario hardware de comunicaciones

Con el inventario de Hardware de comunicaciones los ISP's analizaran que equipos de comunicación soportan y no el protocolo IPv6, para la coexistencia con IPv4. En la tabla 10 se muestran los equipos de comunicación que posee el escenario del ISP tomado como ejemplo.

Tabla: 10. Inventario de hardware de Comunicaciones

MARCA	ÁREA	SERIE	OBSERVACIONES
Cisco SG300	RED CORE	SG300	Soporte IPv6
Cisco switch	Zona Centro Zona Sur	cisco 2960	Soporte IPv6
Cisco 1800	Zona Norte	Serie (1841)	Soporte IPv6

Fuente: Propia

Nota: El escenario propuesto corresponde a que los equipos de comunicación son nuevos de marca CISCO y que traen soporte y activación por defecto para soportar el protocolo IPv6. Por lo tanto no se requiere configuraciones para aceptar IPv6.

Para los equipos que el proveedor de servicios de internet cuente y que no tengan activada por defecto el porte de IPv6 se debe activar o actualizar el equipo, para ello se deben seguir las siguientes actividades.

- Activar el equipo para porte de IPv6, en este sentido se debe verificar que la interfaz del equipo tenga **IOS versión 15,** de no tenerlo se debe contactar con el

fabricante del equipo para solicitar la nueva actualización del sistema operativo del equipo de comunicación mediante la compra de la actualización.

- Si se utiliza equipos de cualquier maraca debe comparar la actualización al proveedor del equipo, si se tiene equipos marca CISCO se puede contactarse con el proveedor y solicitar la actualización del equipo a IOS 15, para ello debe de comprar una Smar Card de actualización.

- Una vez comprado la actualización del IOS 15, el fabricante debe solicitar una serie de requisitos para la actualización del equipo, ejemplo:

- Un servidor del Trivial File Transfer Protocol (TFTP) o una aplicación del servidor del (RCP) Remote Copy Protocol se debe instalar en una estación de trabajo lista para TCP/IP.

Una vez que la aplicación está instalada, la configuración debe ser realizada:

- En primer lugar, la aplicación TFTP se debe configurar para actuar como un servidor TFTP y no cliente TFTP.

- En segundo lugar, debe especificarse el directorio de archivos de salida. Éste es el directorio en el que las imágenes de Cisco IOS se almacenan.

- Para mayor información ingresar a la siguiente dirección electónica del fabricante quien dispone de la información y el procesamiento necesario para llevar a cabo la actualización.

  http://www.cisco.com/cisco/web/support/LA/102/1023/1023840_IOSupgrade_800.pdf

Nota: Se debe tener en cuenta que dependiendo del tipo y serie de equipos, no todos pueden ser actualizados por lo tanto se debe analizar la compra de equipos nuevos en función de los requerimientos y necesidades de adopción del nuevo protocolo dentro del proveedor de servicios de internet.

4.2.4 Inventario software

En este inventario se debe detallar las características del software en cada uno de los equipos como: la versión, año de fabricación, licencias, sistema operativo y marca, ver tabla 11.

Tabla: 11. Inventario de Software

MARCA	ÁREA	VERSIÓN	OBSERVACIONES
Linux	DMZ	Centos 6.3	Soporte IPv6 nativo
Windows	CORREO	Server 2012	Soporte IPv6 nativo
Windows	WEB	Server 2012	Soporte IPv6 nativo
Windows	AD	Server 2012	Soporte IPv6 nativo

Fuente: Propia

Nota: En este sentido se debe considera las tecnologías libres o comerciales en las cuales se tenga las plataformas (Sistemas Operativos de equipos, clientes, servidores).

En el anexo 2, se presenta una plantilla como modelo de ejemplo para el inventario de software, Ver anexo2.

4.2.5 Definición de áreas de adopción de IPv6

En el proceso de adopción del nuevo protocolo es necesario definir qué áreas y portafolios de clientes son menos críticos para la implementación del nuevo protocolo IPv6, con el fin de que si se presentan fallos en la implementación del nuevo protocolo el impacto sea mínimo por lo tanto se debe tener las siguientes consideraciones, ver en la tabla 12.

Su objetivo principal es establecer las áreas no críticas que se van implementar IPv6 primero y antes de la adopción para el despliegue final en el proveedor de servicio.

Tabla: 12. Determinacion de Zonas de cobertura de servicios

Área	Zona de servicio norte	(Clientes residenciales) (Clientes domésticos)
	Zona de servicio sur	(Clientes residenciales) (Clientes domésticos) (Clientes Cybert) (Clientes domésticos)
	Zona de servicio centro	(Clientes residenciales) (Clientes Bancos) (Clientes Empresas) (Clientes corporaciones)

Fuente: Propia

Para determinar qué áreas de servicio son menos críticas en necesario que el Director de TI, en conjunto con el Jefe de redes, equipo técnico y de soporten evalúen cuál de las zonas de cobertura de servicio sean las que no se tenga portafolio de clientes importantes en términos de impacto de dejar sin servicio a las actividades de los clientes para ello se debe tener en cuenta que el impacto de una zona de clientes domésticos o comerciales es mínima ya que las actividades que estas realizan se limitan a ocio, entretenimiento, mientras que las de una < *zona centro*> hay clientes bancarios, empresas, corporaciones que realizan y se basan en actividades de términos al acceso a la red e internet.

4.2.6 Definición de Mecanismos de coexistencia para la implementación

En la actualidad existen muchos mecanismos para la transición o coexistencia entre los dos protocolos IPv4 e IPv6, que se han desarrollado para manejar redes con los dos protocolos. Es por ello que para llevar a cabo la adopción de IPv6 es recomendable ejecutar una transición sistemática de forma gradual en base a mecanismos de transición. Si bien existen varios mecanismos de coexistencia en los países desarrollados tecnológicamente como Estados Unidos, Europa, Asia,… ya se han evaluado ciertos mecanismos que permiten la coexistencia entre ambos protocolos lo que ha permitido en el Ecuador tener una referencia significativa de los mecanismos que han tenido éxito para llevar a cabo una migración progresiva.

Los mecanismos de transición probados y recomendados para la adopción y coexistencia de los dos protocolos se describen a continuación:

- Dual Stack
- Túneles

Su objetivo principal es elaborar el plan de coexistencia para los elementos de red, nodos finales, host y aplicaciones para garantizar la comunicación y conectividad entre IPv4 e IPv6.

4.2.7 La dualidad como opción para los ISPs

Conocido como dual Stack o como doble capa IP, este mecanismo provee que el host y routers soporten los dos protocolos IPv4 e IPv6, es decir que los dispositivos con ambas pilas pueden recibir y enviar tráfico a nodos de cualquiera de los dos protocolos IPv4 e IPv6 a la vez, como se muestra en la figura 22.

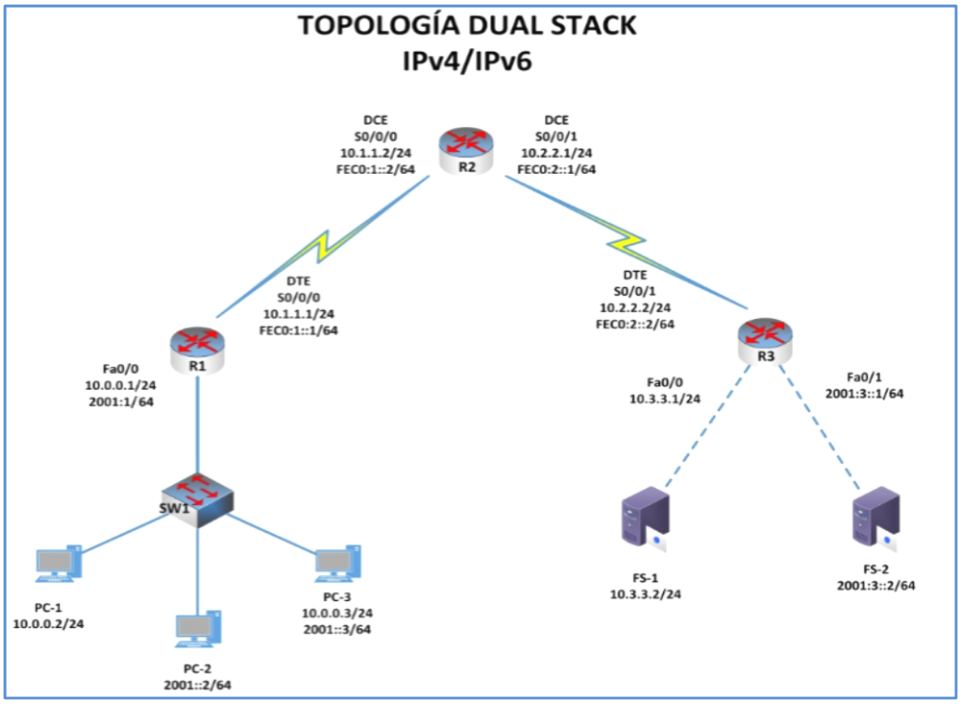


Figura: 22 Mecanismo Dual Stack
Fuente: Propia

4.2.8 El mecanismo por medio de túneles

Mientras que el mecanismo de Túneles conocido también como encapsulación. Es un proceso mediante el cual encapsula información de un protocolo dentro del paquete del otro protocolo, permitiendo así a los datos originales ser prorrogados en el segundo protocolo.

Este mecanismo puede utilizarse cuando dos nodos o redes que utilizan el mismo protocolo quieren comunicarse a través de una red que utiliza otro protocolo de red. El proceso de construcción de túneles implica tres pasos:

- Encapsulación
- Des encapsulación
- Administración del túnel

Requiere dos extremos de túnel, que en el caso general son los nodos doble pila IPv4/IPv6 (generalmente enrutadores), para manejar la encapsulación y desencapsulación. Ver figura 23.

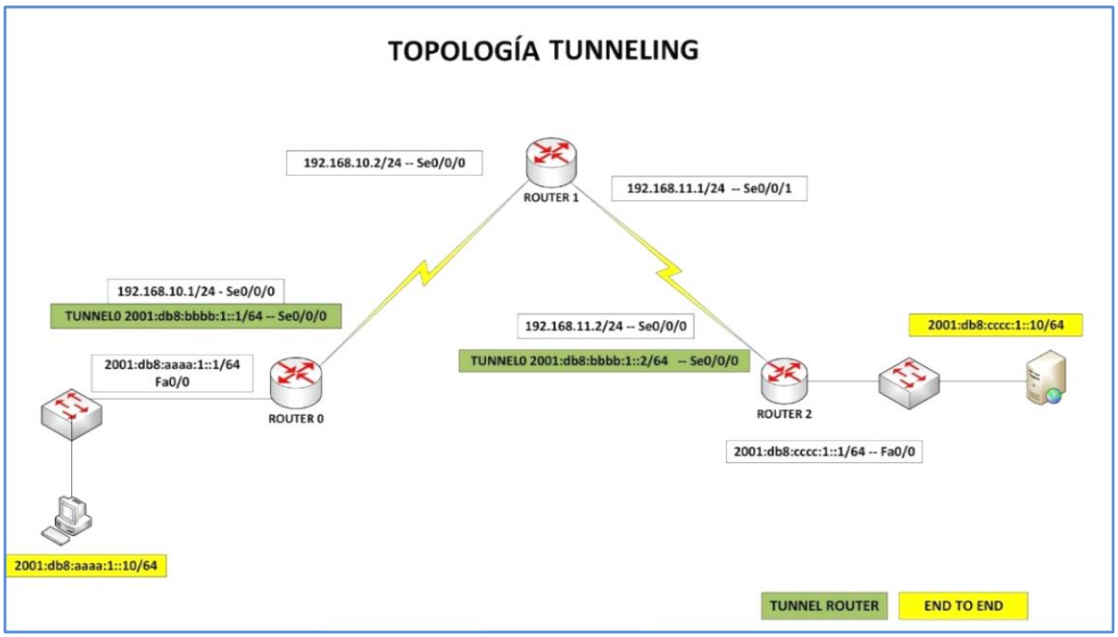


Figura: 23 Mecanismo Tenneling
Fuente: Propia

En la configuración de túneles de ruteador a ruteador es decir ruteadores IPv6/IPv4 conectan dos infraestructuras de IPv4 e IPv6 sobre una infraestructura IPv4 expandiendo los puntos finales del túnel un enlace lógico entre el camino origen y destino.

Puede configurarse un túnel de cuatro maneras diferentes:

- **Router a router.-** Abarca un segmento de trazado entre dos host **end-to-end,** Entre los proveedores de servicio de internet es el método más utilizado.

- **Host a router.-** Comprende el primer tramo de la ruta end-to-end entre los dos hosts.

- **Host a host**.- Atraviesa la ruta completa de end-to-end entre los dos hosts.

- **Router a host.-** Comprende el último segmento del trazado end-to-end entre los dos hosts.

Dependiendo de qué tipo de configuración se utiliza, puede ser un túnel "configurado" los proveedores de servicios de internet deben estar configurados en consecuencia, "semi configurado", es decir solamente un lado tiene que estar configurado, al otro lado actúa como una puerta de entrada, donde casi nada debe ser hecho por los dos anfitriones para comunicarse a través de un túnel

4.2.9 Seguridades en la Coexistencia de los dos protocolos

En el aspecto de seguridad de IPv6 los ISP's deben considerar las implicaciones al desplegar el nuevo protocolo ya que al tener un número ilimitado de direcciones se hace

imposible rastrear y escanear las direcciones, para esto se recomiendan las siguientes consideraciones de seguridad a implementar.

A continuación se sugieren algunas técnicas de mitigaciones de ataques que se pueden presentar en las redes.

- Desplegar SEND (SEcure Neighbor Discovery)
- Monitorear el tráfico de Neighbor Discovery)
- Usar entradas estáticas en el Neighbor Cache
- Restringir el acceso a la red.

Los Jefes de Red deben estar atentos al monitoreo de las redes ya que pueden ser vulnerables debido a que:

- SEND es difícil de desplegar
- Las herramientas de monitoreo son posibles de evadir
- El uso de entradas estáticas “no escala” para el caso general
- No siempre es posible restringir el uso a una red

En este sentido el proveedor de servicios debe configurar una Zona Desmilitarizada (DMZ), permitiendo restringir los servidores de acceso público a los demás segmentos de la red del ISP, bloqueando la comunicación con los demás segmentos de la red interna

y demás consideraciones de seguridad que el Jefe de redes deba implementar (proxy, Firewall, segmentación de red, directorio activo…) en el proveedor.

4.3 Implementación

Una vez que ya se han cumplido las fases anteriores el primer paso para implementar IPv6 consiste en configurar los nodos principales de la red del proveedor de servicios (Nodos CORE), ya que definida la topología en muchos casos no se modifica la estructura de la red actual es decir (cables, enrutadores, host). Para ello se debe verificar que el hardware de red admite el protocolo IPv6 y que se puede configurar (Ver actualización IOS de enrutadores).

Su principal objetivo es implementar el nuevo protocolo IPv6 en el proveedor de servicios de internet para que los usuarios finales y servicios admitan IPv4 e IPv6.

En el siguiente escenario se presenta la configuración básica de cada uno de los Router en la herramienta de Packet Tracer, donde nos permite configurar y mostrar la funcionalidad de cada uno de los métodos mencionados y recomendados anteriormente para el proceso de coexistencia de los dos protocolos. Escenario en la figura 24.

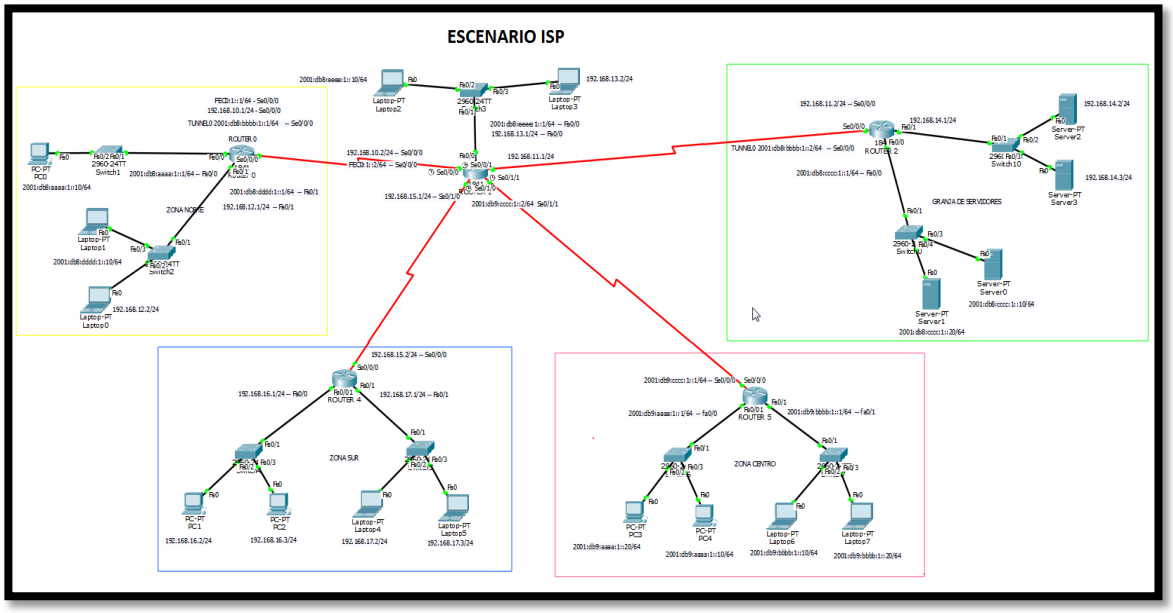


Figura: 24. Escenario en Packet Tracer de un ISP
Fuente: Propia

4.3.1 Asignación de Direcciones IPv6

Los ISP's deben solicitar un bloque de direcciones para la adopción del nuevo protocolo y debe ser solicitada a la entidad que otorga para la región de Latinoamérica, que es LACNIC, Para solicitar un bloque IPv6 los ISP's deben realizar el siguiente proceso.

- Ingresar a la siguiente dirección electrónica http://portalipv6.lacnic.net/como-obtener-un-bloque-de-direcciones-ipv6/

Para quienes estén interesados en obtener una asignación de direcciones IPv6, podrán encontrar políticas y formularios en:

- IPv6 para Proveedores: http://www.lacnic.net/web/lacnic/ipv6-isp.

- Además, ayudará en su tarea de solicitud de direcciones, informarse acerca de los servicios de registro: http://www.lacnic.net/web/lacnic/servicios-registro (LACNIC, 2015)

Una vez que se registre o se requiera los prefijos de IPv6, se deberá llenar el formulario a través del sistema de solicitud de recursos de LACNIC, en la siguiente dirección electrónica, ver Figura 25.

Figura: 25. Solicitud de Recursos
Fuente: (LACNIC, 2015)

En la figura 25, el Director de TI o el Jede de Redes autorizado, debe ingresar su usuario y clave para el registro de solicitud de recursos para solicitar los bloques de direcciones IPv6, para la adopción y coexistencia de los dos protocolos.

4.3.2 Tabla de Direcciones

En la tabla 13 se presenta las direcciones que se configuro en el escenario y simulador de Packet Tracer.

Tabla: 13. Direcciones IP

Tabla de Direccionamiento				
Dispositivo	**Interfaz**	**Dirección IP**	**Mascara de Subred**	**Gateway por defecto**
Router 1	Fa0/0	192.168.13.1	255.255.255.0	N/C
	Se0/0/0	192.168.10.2	255.255.255.0	N/C
		FEC0:1::2	/64	N/C
	Se0/0/1	192.168.11.1	255.255.255.0	N/C
	Se0/1/0	192.168.15.1	255.255.255.0	N/C
	Se0/1/1	2001:db9:cccc:1::2	/64	N/C
Router 0 Zona Norte	Fa0/0	2001:db8:aaaa:1::1	/64	N/C
	Fa0/1	2001:db8:dddd:1::1	/64	N/C
	Se0/0/0	FEC0:1::1	/64	N/C
		192.168.10.1	255.255.255.0	N/C
	Tunnel0	2001:db8:bbbb:1::1	/64	N/C
Router 2 Granja de Servidores	Fa0/0	2001:db8:cccc:1::1	/64	N/C
	Fa0/1	192.168.14.1	255.255.255.0	N/C
	Se0/0/0	192.168.11.2	255.255.255.0	N/C
	Tunnel0	2001:db8:bbbb:1::2	/64	N/C
Router 4 Zona Sur	Fa0/0	192.168.16.1	255.255.255.0	N/C
	Fa0/1	192.168.17.1	255.255.255.0	N/C
	Se0/0/0	192.168.15.2	255.255.255.0	N/C

Router 5 Zona Centro	Fa0/0	2001:db9:aaaa:1::1	/64	N/C
	Fa0/1	2001:db9:bbbb:1::1	/64	N/C
	Se0/0/0	2001:db9:cccc:1::1	/64	N/C
Servidor 0	NIC	2001:db8:cccc:1::10	/64	2001:DB8:CCCC:1::1
Servidor 1	NIC	2001:db8:cccc:1::20	/64	2001:DB8:CCCC:1::1
Servidor 2	NIC	192.168.14.2	255.255.255.0	192.168.14.1
Servidor 3	NIC	192.168.14.3	255.255.255.0	192.168.14.1
PC0	NIC	2001:db8:aaaa:1::10	/64	2001:DB8:AAAA:1::1
LAPTO0	NIC	192.168.12.2	255.255.255.0	192.168.12.1
LAPTO1	NIC	2001:db8:dddd:1::10	/64	2001:DB8:DDDD:1::1
PC1	NIC	192.168.16.2	255.255.255.0	192.168.16.1
PC2	NIC	192.168.16.3	255.255.255.0	192.168.16.1
LAPTO4	NIC	192.168.17.2	255.255.255.0	192.168.17.1
LAPTO5	NIC	192.168.17.3	255.255.255.0	192.168.17.1
PC3	NIC	2001:db8:aaaa:1::20	/64	2001:DB9:AAAA:1::1
PC4	NIC	2001:db8:aaaa:1::10	/64	2001:DB9:AAAA:1::1
LAPTO6	NIC	2001:db8:bbbb:1::10	/64	2001:DB9:BBBB:1::1
LAPTO7	NIC	2001:db8:bbbb:1::20	/64	2001:DB9:BBBB:1::1

Fuente : Porpia

4.3.3 Configuración de los routers del modelo ISP

En la tabla 14 se describe la configuración del router Núcleo y de los nodos finales para cada proveedor y zonas

Tabla: 14. Configuracion de equipos y dispositivos

Configuración	RPUTER 0

ROUTER0#show r

Building configuration...

Current configuration : 1291 bytes

!

version 12.4

!

hostname ROUTER0

!

!

no ip cef

ipv6 unicast-routing

!

no ipv6 cef

!

!

spanning-tree mode pvst

!

!

interface Tunnel0

 no ip address

 mtu 1476

 ipv6 address 2001:DB8:BBBB:1::1/64

 tunnel source Serial0/0/0

 tunnel destination 192.168.11.2

 tunnel mode ipv6ip

!

!

interface FastEthernet0/0

```
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:AAAA:1::1/64
!
interface FastEthernet0/1
 ip address 192.168.12.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2001:DB8:DDDD:1::1/64
 ipv6 rip PUCE enable
!
interface Serial0/0/0
 ip address 192.168.10.1 255.255.255.0
 ipv6 address FEC0:1::1/64
 ipv6 rip PUCE enable
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/1/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/1/1
 no ip address
```

```
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 network 192.168.10.0
 network 192.168.12.0
!
ipv6 router rip PUCE
!
ip classless
!
ip flow-export version 9
!
ipv6 route 2001:DB8:CCCC:1::/64 2001:DB8:BBBB:1::2
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
End
```

Configuración	ROUTER 1

```
ROUTER1#show r
Building configuration...
Current configuration : 1188 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ROUTER1
!
!
no ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
!
spanning-tree mode pvst
!
!
interface FastEthernet0/0
 ip address 192.168.13.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2001:DB8:EEEE:1::1/64
 ipv6 rip PUCE enable
!
```

```
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 192.168.10.2 255.255.255.0
 ipv6 address FEC0:1::2/64
 ipv6 rip PUCE enable
 clock rate 128000
!
interface Serial0/0/1
 ip address 192.168.11.1 255.255.255.0
 clock rate 128000
!
interface Serial0/1/0
 ip address 192.168.15.1 255.255.255.0
 clock rate 128000
!
interface Serial0/1/1
 no ip address
 ipv6 address 2001:DB9:CCCC:1::2/64
 ipv6 rip PUCE enable
 clock rate 128000
!
interface Vlan1
 no ip address
 shutdown
```

```
!
router rip
 network 192.168.10.0
 network 192.168.11.0
 network 192.168.13.0
 network 192.168.15.0
!
ipv6 router rip PUCE
!
ip classless
!
ip flow-export version 9
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
End
```

Configuración	ROUTER 2
ROUTER2#show r Building configuration... Current configuration : 1181 bytes !	

```
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ROUTER2
!
!
no ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
!
spanning-tree mode pvst
!
!
interface Tunnel0
 no ip address
 mtu 1476
 ipv6 address 2001:DB8:BBBB:1::2/64
 tunnel source Serial0/0/0
 tunnel destination 192.168.10.1
 tunnel mode ipv6ip
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
```

```
 speed auto
 ipv6 address 2001:DB8:CCCC:1::1/64
!
interface FastEthernet0/1
 ip address 192.168.14.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 192.168.11.2 255.255.255.0
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/1/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/1/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
```

```
!
router rip
 network 192.168.11.0
 network 192.168.13.0
 network 192.168.14.0
!
ip classless
!
ip flow-export version 9
!
ipv6 route 2001:DB8:AAAA:1::/64 2001:DB8:BBBB:1::1
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
End
```

Configuración	ROUTER 4

```
ROUTER4#show r
Building configuration...
Current configuration : 932 bytes
!
version 12.4
```

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ROUTER4
!
!
no ip cef
no ipv6 cef
!
!
spanning-tree mode pvst
!
!
interface FastEthernet0/0
 ip address 192.168.16.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.17.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 192.168.15.2 255.255.255.0
!
interface Serial0/0/1
 no ip address
```

```
 clock rate 2000000
 shutdown
!
interface Serial0/1/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/1/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 network 192.168.15.0
 network 192.168.16.0
 network 192.168.17.0
!
ip classless
!
ip flow-export version 9
!
!
line con 0
!
```

line aux 0
!
line vty 0 4
 login
!
!
End

Configuración	ROUTER 5

ROUTER5#sh r
Building configuration...
Current configuration : 1004 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ROUTER5
!
!
no ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
!
spanning-tree mode pvst
!

```
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB9:AAAA:1::1/64
 ipv6 rip PUCE enable
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB9:BBBB:1::1/64
 ipv6 rip PUCE enable
!
interface Serial0/0/0
 no ip address
 ipv6 address 2001:DB9:CCCC:1::1/64
 ipv6 rip PUCE enable
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/1/0
 no ip address
 clock rate 2000000
 shutdown
```

```
!
interface Serial0/1/1
 no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
ipv6 router rip PUCE
!
ip classless
!
ip flow-export version 9
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
End
```

Fuente:Propia

4.3.4 Actualización y configuración de IPv6 en Windows

Para la implementación de IPv6, en las plataformas de Windows se debe tener en cuenta que a partir de las siguientes versiones de sistemas operativos ya traen soporte por parte del fabricante, así que antes de hablar de instalación lo que se debe hacer es la ***activación.*** Las plataformas que ya traen soporte del fabricante de Microsoft Windows y que solo requieren activación de IPv6 se describen a continuación.

- Windows XP SP1 y posteriores
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows 8
- Windows 10

El primer paso que se debe hacer dependiendo de la versión de la plataforma Microsoft Windows se debe ejecutar en la consola de comandos para verificar si está activado mediante la siguiente línea de comandos ***ping -6 -n 5 ::1*** y si el resultado es el siguiente: ver figura 26.

El sistema que utiliza ya trae activado por defecto el soporte para el tráfico de datos en la versión IPv6.

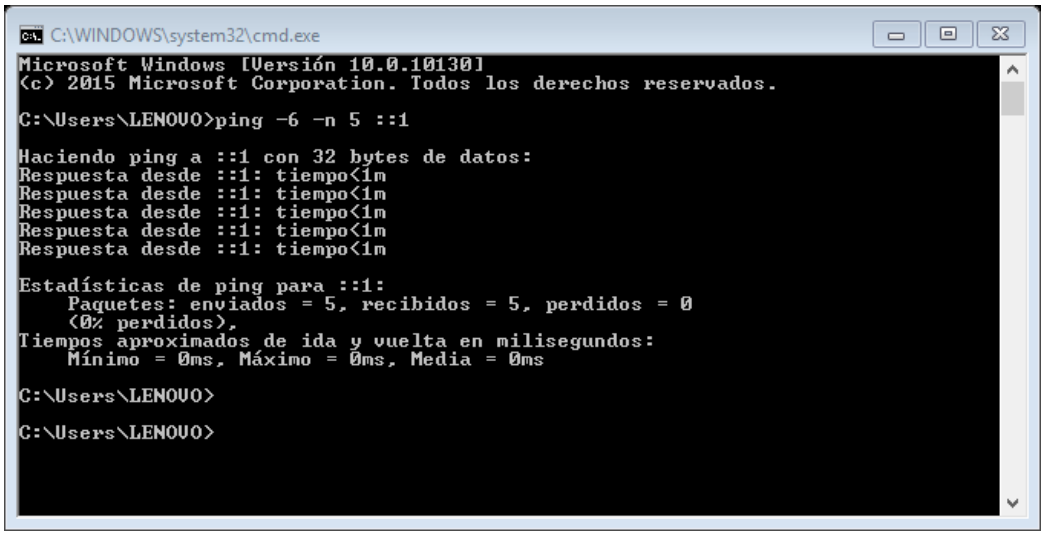


Figura: 26. Comando ping -6 –n 5::1
Fuente: propia

Ahora si no trae activado por defecto el soporte para IPv6, generalmente en versiones anteriores al 2006 como es el caso de versiones de Microsoft Windows XP SP1 se debe verificar ejecutando la línea de comandos ping ***-6 -n 5 ::1*** si el resultado es como el que se muestra en la siguiente pantalla: ver figura 27.

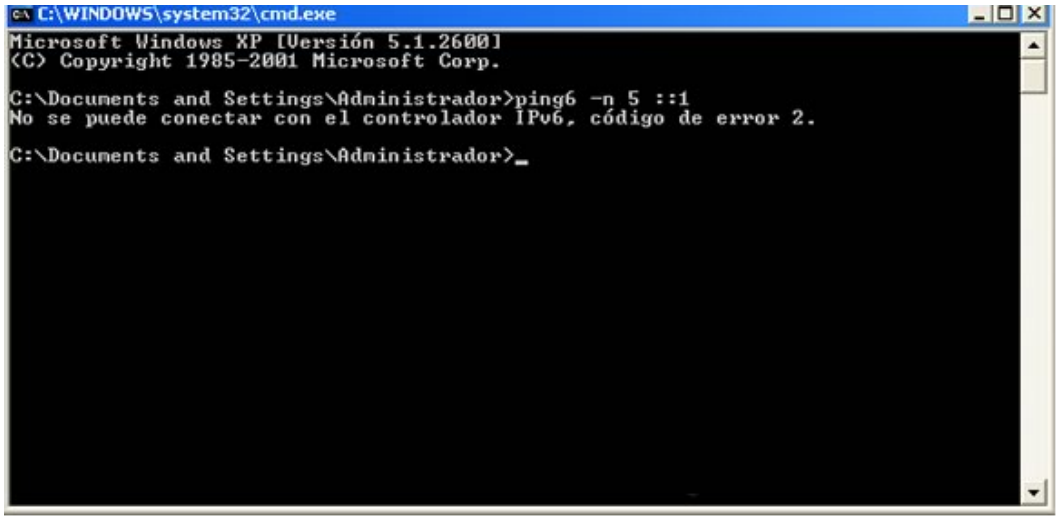


Figura: 27. Sin comando ping -6 –n 5::1
Fuente: Propia

Esto significa que no se encuentra activado el soporte para la versión IPv6, por lo tanto se debe ejecutar la siguiente línea de comandos, ***netsh interface ipv6 install*** desde la consola. Ver figura 28.

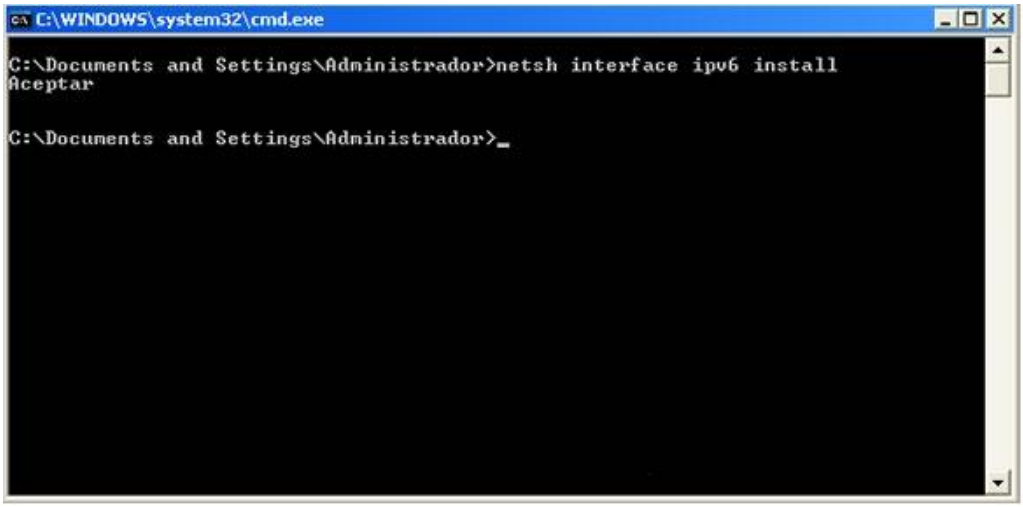


Figura: 28. Instalación de IPv6
Fuente: Propia

Para la comprobación de que se activado el soporte para IPv6 en el equipo solo vasta ejecutar la siguiente línea de comando ***ping -6 -n 5 ::1,*** confirmado que se activado correctamente el soporte. Ver figura 29.

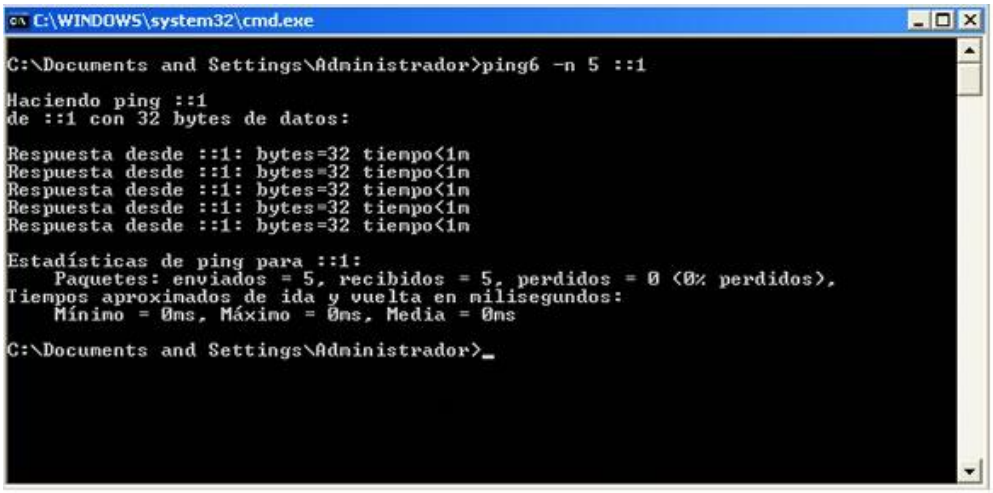


Figura: 29. Comprobación de Instalación IPv6
Fuente: Propia

Otra forma de activar el soporte de IPv6 en el equipo es de forma gráfica para ello se debe acceder a: Panel de control-> Conexión de red-> Red área local-> o red inalámbrica -> Propiedades -> Instalar protocolo -> TCP/IP versión 6, como se muestra en la siguiente ver figura 30.

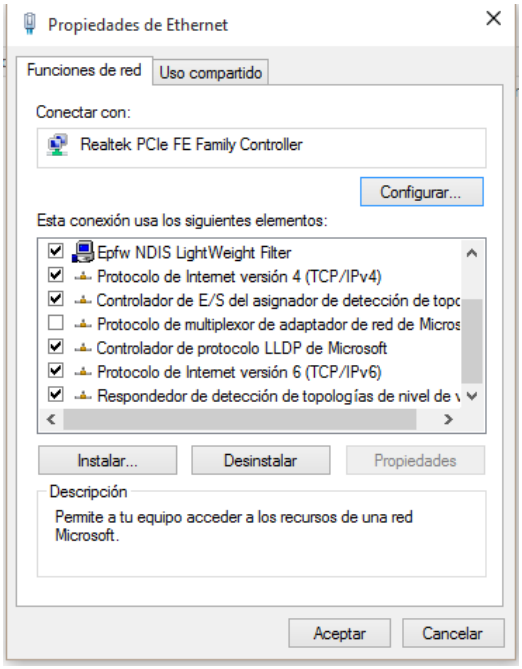


Figura: 30. Configuración Grafica para IPv6
Fuente: Propia

Para el proceso de instalación o activación en las demás versiones de plataformas de Windows, vista, server 2008 en adelante estos sistemas ya traen soporte de IPv6 instalado y habilitado por defecto. Por lo tanto no es necesario hacer ninguna configuración adicional si por alguna circunstancia se utilizara el procedimiento descrito en los párrafos anteriores con el comando ***netsh interface ipv6 install,***

4.3.5 Actualización y Configuración IPv6 en Mac OS X

Los fabricantes de Mac OS X han incluido compatibilidad con la nueva versión del protocolo IPv6 a partir de una versión específica **Mac Os X v10.1** y la activación por defecto a partir de la versión **Mac Os X v10.3.**

La forma de comprobación de que **Mac Os X,** tiene ya soporte para IPv6 en la terminal es digitar el siguiente comando ***ping -6 -c5 ::1,*** el resultado debe ser el siguiente. Ver figura 31.

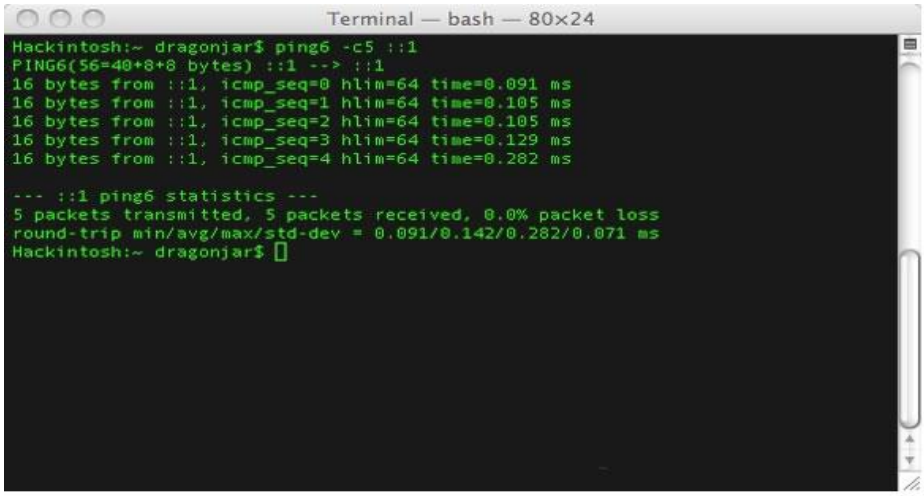


Figura: 31. Configuración MAC de IPv6
Fuente: Propia

Si la respuesta del terminal corresponde a la que se muestra en la figura significa que el equipo soporta IPv6, si no es el resultado similar se debe activar IPv6 en el equipo. Primero desde una terminal se debe ejecutar el comando ***/sbin/ifconfig –a***, para ver los adaptadores y dispositivos de red del equipo. Ver figura 32.

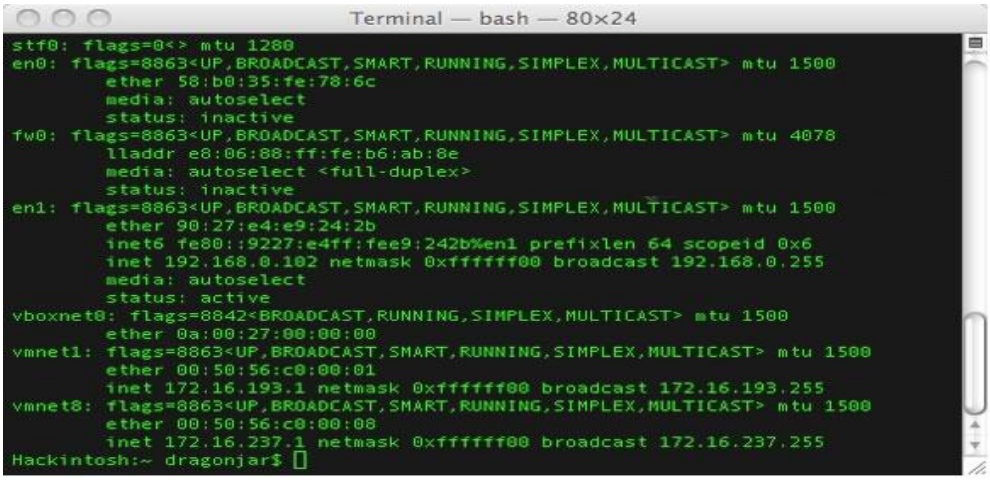


Figura 32. Instalación de IPv6 en MAC
Fuente: Propia

Una vez determinado los dispositivos activos en el equipo se debe buscar la interfaz con el **"satatus: active"**, que generalmente es la interfaz ***en0,*** y ejecutar el comando ***sudo ipv6config start-v6 en0; sudo ipv6config start-stf en0:*** ver figura 33.

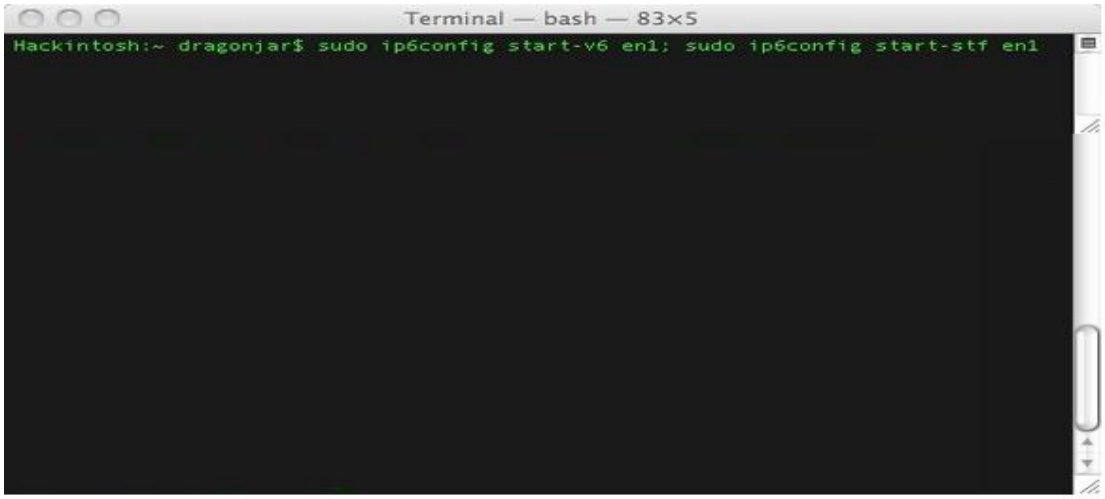


Figura: 33. Configuración de IPv6 en MAC
Fuente: Propia

Para verificar si se activó el soporte para IPv6, se debe ejecutar de la terminal el comando, ***ping -6 -c5 ::1,*** constatando de que el equipo ya tiene soporte IP versión 6. Para configurar de forma manual IPv6 en el equipo se deben seguir los siguientes paso para ejecutar se

debe tener permisos de administrador de red del proveedor de internet (ISP), para poder configurarlo.

- Elegir preferencias de sistema menú Apple.
- Acceder a la ventana de preferencias del sistema.
- Seleccionar servicio de red con IPv6 con Ethernet o Airport.
- Seleccionar avanzado y activar TCP/IP.
- Seleccionar del menú emergente configurar IPv6.
- Ingresar la dirección IPv6 en el router y la longitud del prefijo facilitado por el proveedor de internet.

4.3.6 Actualización y Configuración de IPv6 en Linux

Para la configuración en los equipos que utilizan distribuciones GNU/Linux con soporte para IPv6, se debe ejecutar desde la terminal el comando ***ping -6 -c5 ::1,*** ver figura 34

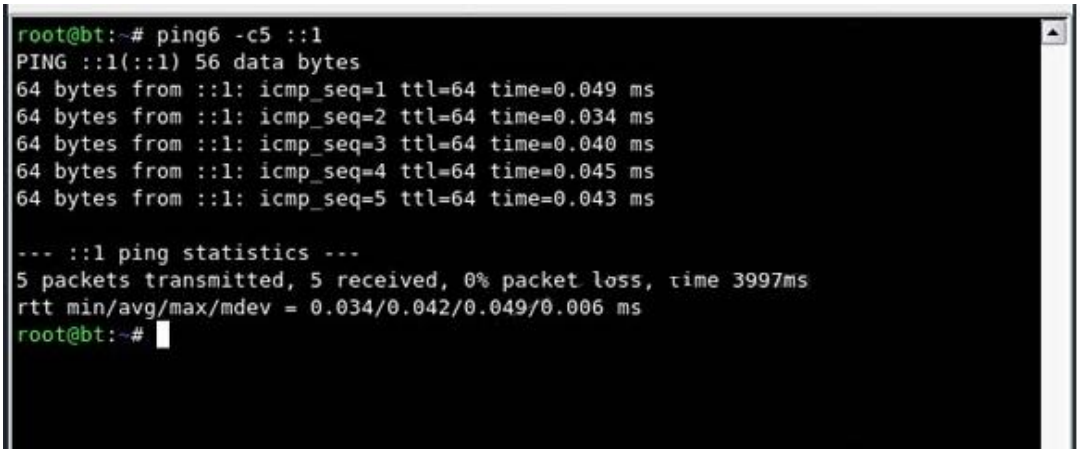


Figura 34. Configuración Linux de IPv6
Fuente: Propia

Si corresponde la gráfica significa que la distribución de GNU/Linux tiene soporte para IPv6 (desde el Kernel 2.4.x IPv6 trae soporte de fábrica), caso contrario se debe activar IPv6 en el equipo.

Para activar el soporte de IPv6 en el Kernel que está corriendo en el equipo se debe ejecutar desde la terminal el siguiente comando **–f /proc/net/if inet6 && echo,** lo que determina que el kernel está listo para soportar IPv6.

Una vez realizado este procedimiento se debe subir el módulo **modprobe ipv6.** Se vuelve a verificar si el kernel se cargó con l**smod | gree –w 'ipv6' && echo,** se reinicia el equipo y ejecutamos del terminal nuevamente el comando ***ping -6 -c5 ::1,*** ver figura 35.

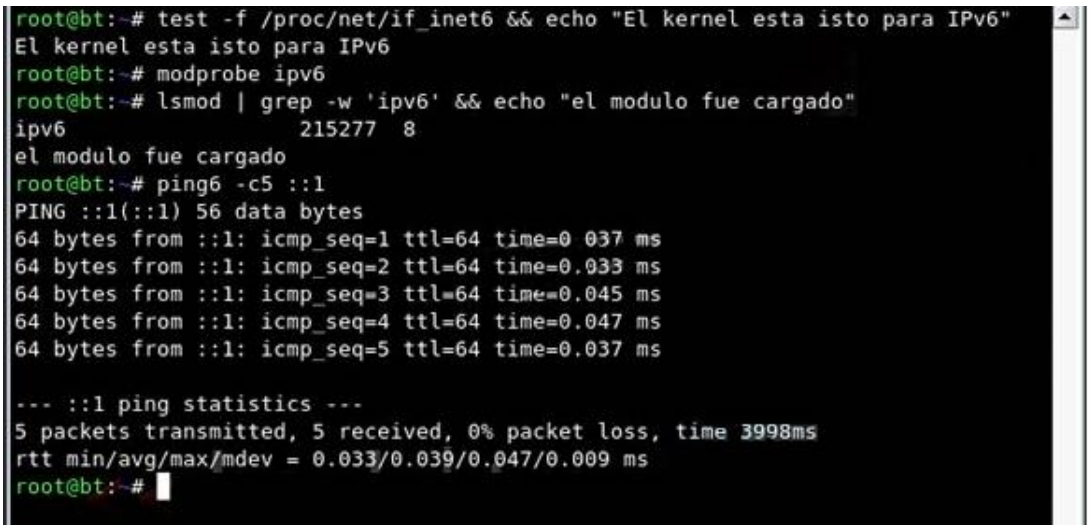


Figura 35.. Activacion de IPv6 Linux
Fuente: Propia

En general para el resto de sistemas operativos que dispongan las instituciones y de las derivaciones de estos sistemas como (Unix, distribuciones de Linux, BSD,….), se debe utilizar el comando ***ifconfig,*** que permite determinar si el equipo soporta el protocolo IPv6

o se requiere de la activación, también la mayoría de los sistemas traen incorporados entornos de interfaz gráfica de usuarios que son específicos para cada plataforma que permite el monitoreo del estado de la/s interfaces de red, y por lo tanto el protocolo de IPv6.

4.4 Análisis de pruebas

4.4.1 Pruebas de funcionamiento

Las pruebas de funcionamiento del nuevo protocolo así como de coexistencias de Ipv4 e IPv6, permiten determinar que cada elemento de red admita y soporte el nuevo protocolo de red versión IPv6, también que los mecanismos de coexistencia sean capaces de resolver tanto para IPv4 e IPv6, que se puede llegar a través de una red con los dos protocolos y a su vez exista conexión continua. Los encargados para realzar las pruebas deben realizar un plantilla de pruebas para que esto sea documentado ver plantillas en Anexo 3.

Su objetivo es realizar pruebas de conexión a través de los distintos enrutadores, nodos CORE, nodos finales, mecanismos y demás elementos que fueron intervenidos con la implementación de IPv6.

En este caso las pruebas serán demostradas con la funcionalidad y la configuración en la herramienta de Packet Tracer, donde se realizó la configuración de los mecanismos.

4.4.2 Escenarios de pruebas - Conexión

En la figura 36, se prueba la conexión desde la Zona Norte configurada con direcciones IPv4 e IPv6 hacia a la Granja de servidores, donde se aplica el mecanismo de Dual Stack y Tuneling

.

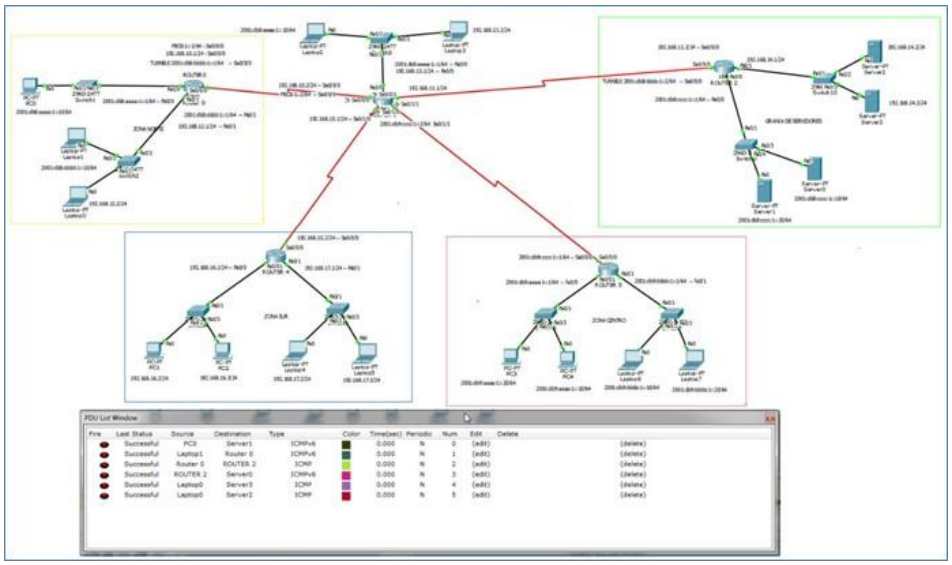


Figura: 36. Configuracion Zona Norte IPv4-IPv6 a Granja de Servidores
Fuente: Propia

En la figura 37, se prueba la conexión desde la Zona Sur, se configura con direcciones IPv4 con el mecanimos Dual Stack.

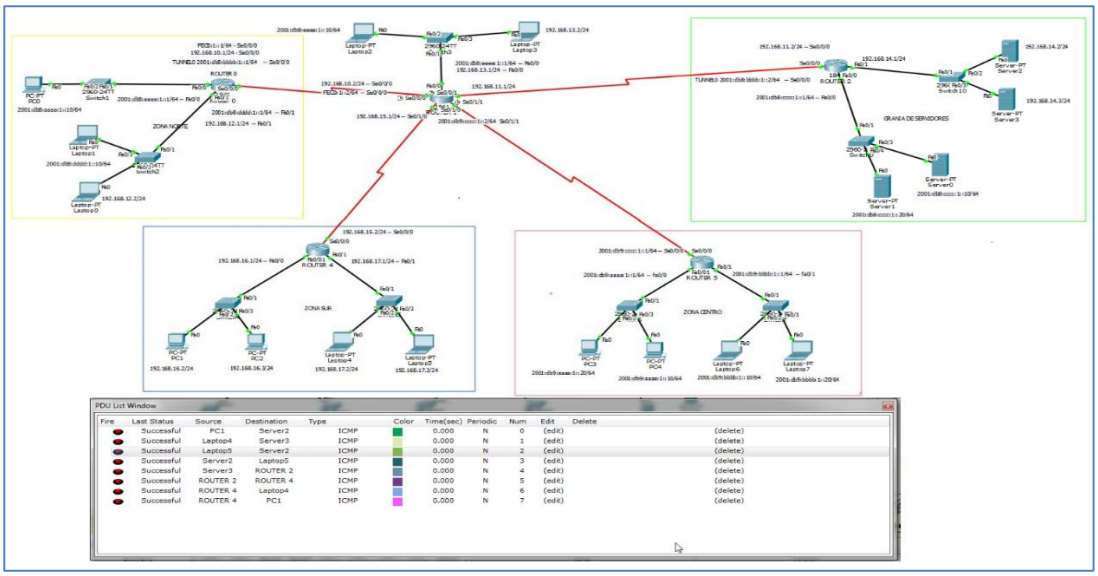


Figura: 37. Conexión de zona Sur con direcciones IPv4
Fuente: Propia

En la figura 38, se prueba la conexión desde la Zona Centro, se configura direcciones IPv6, con el mecanimo Dual Stack.

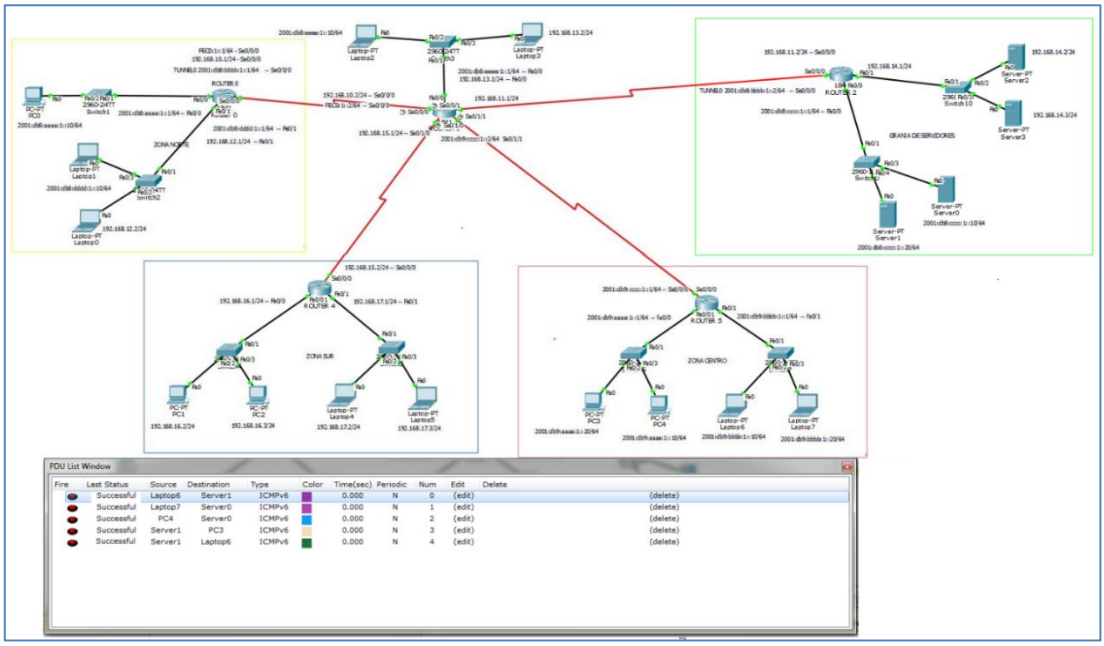


Figura 38. Configuracion Zona Centro con direcciones IPv6.
Fuente: Propia

En la figura 39, se prueba la conexión entre Zonas configuradas con direcciones IPv4-IPv6

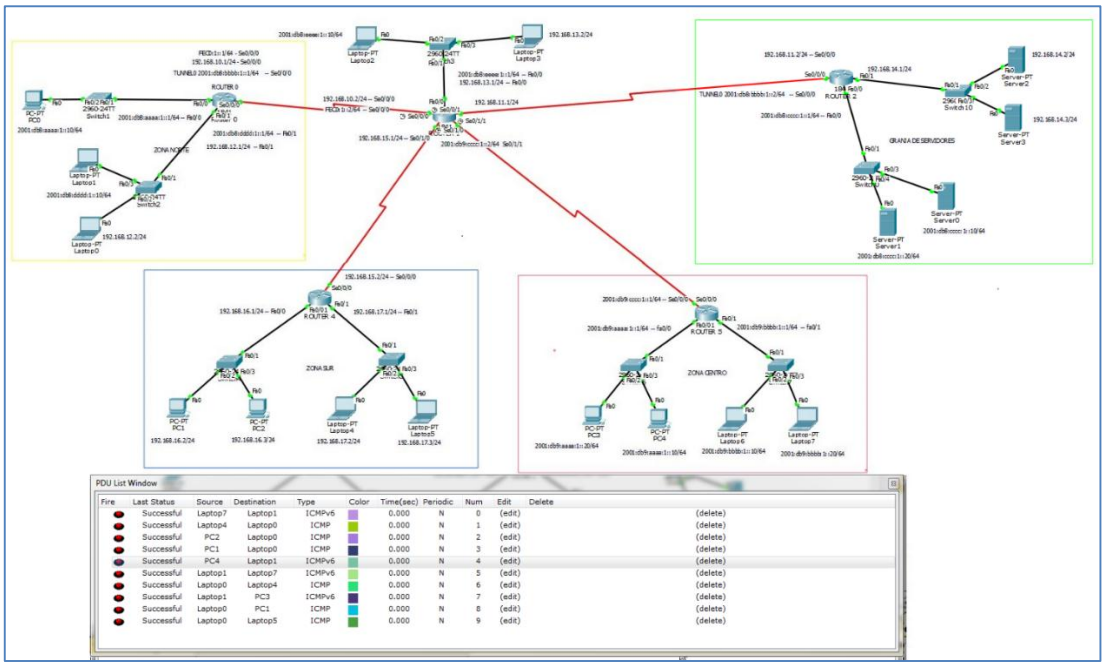


Figura: 39. Conexión entre Zonas IPv4-IPv6
Fuente: Propia

4.4.3 Funcionalidad del mecanismo Dual stack

Pruebas de conectividad del funcionamiento del mecanismo Dual Stack, ver configuración en anexo 4.

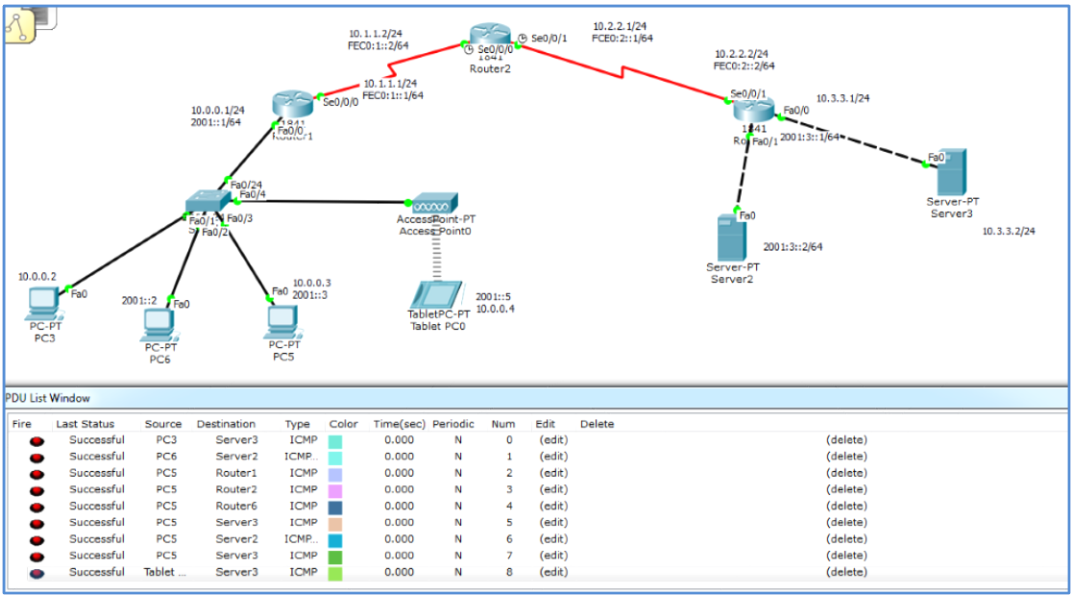


Figura 40. Funcionalidad del mecanismo Dual Stack
Fuente: Propia

4.4.4 Funcionalidad del mecanismo Tunel

Pruebas de conectividad del funcionamiento del mecanismo Tunel, ver configuración en anexo 5.

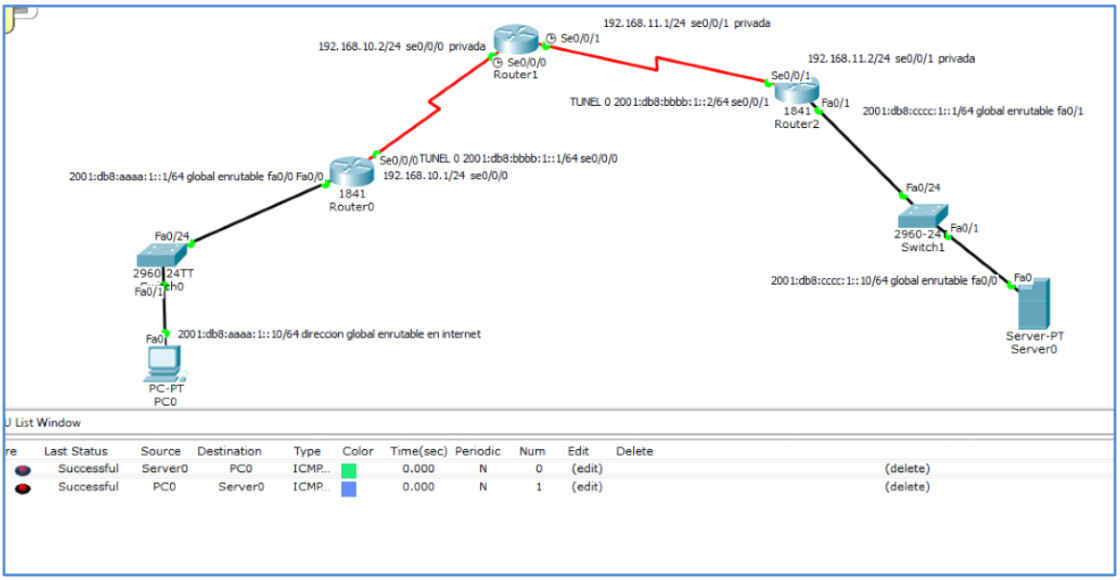


Figura 41. Funcionalidad del mecanismo Tunel
Fuente: Propia

4.4.5 Funcionalidad del mecanismo Dual stack –Tunel

Pruebas de conectividad del funcionamiento del mecanismo Dual Stack -Tunel, ver o de configuración en anexo 6.

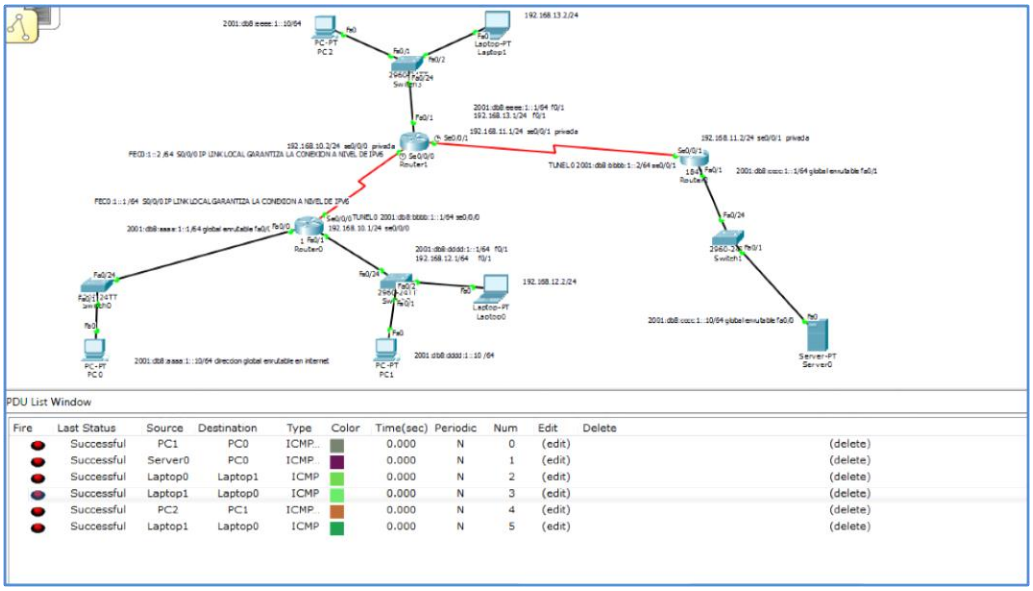


Figura 42. Funcionalidad del mecanismo Dual Stack - Tunel
Fuente: Propia

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Introducción

En este capítulo se redacta las conclusiones más importantes de la investigación, de cómo los ISP's deben actuar ante la migración y coexistencia de los protocolos IPv4 e IPv6 y ofrecer la continuidad del servicio a los usuarios, de igual manera se presenta las principales recomendaciones a futuro para la implementación de estos protocolos.

En este proyecto se propuso a los ISP's la información necesaria para la coexistencia de dos protocolos, la capacitación de personal, la realización de inventarios de software y hardware, el análisis de áreas menos críticas y críticas para la implantación, el levantamientos de la estructura de los ISP, la actualización de sistemas operativos, las configuraciones técnicas y definiciones de los mejores mecanismos de transición para la coexistencia

.

5.2.Conclusiones

- En conclusión la migración y coexistencia de los dos protocolos es un proceso muy lento que tardara muchos años, y por lo tanto los proveedores deben de contar con la información y funcionalidad necesaria de los mecanismos y su comportamiento para la implementación.

- Los proveedores no migran hacia el nuevo protocolo IPv6 por miedo al fracaso en la perdida y fallas de conexión durante la implementación.

- El uso y la descripción de los mecanismos de transición como: Dual Stack y Túnel son los más recomendados a nivel internacional por su funcionalidad que permite convivir a los dos protocolos durante algunos años.

- Con el nuevo protocolo IPv6 y el cambio de la infraestructura que realizan los ISP, estos pueden brindar numerosas combinaciones de direcciones IP a miles de usuarios para que se puedan conectar a la red.

- Mediante el estudio de este proyecto los proveedores deben tomar en cuenta antes de la migración con un inventario de software y hardware que soporten IPv6, y dependiendo del mismo deben contar con un presupuesto económico para la

compra necesaria de equipos con soporte IPv4-IPv6 y así brindar un mejor servicio de conexión.

- En Americalatina el despliegue de ipv6 aún se encuentra retrasado, a pesar de que algunos proveedores ya cuentan con la infraestructura para la adopción, son ellos los que deben impulsar y ofrecer el direccionamiento de IPv6, ya que existen muchos usuarios que se conectan a la red con más de un dispositivo.

- Las redes TOR no protegen el anonimato si no se toman medidas apropiadas, TOR no es usada únicamente por delincuentes o los llamados hackers, si bien es utilizada por familias, periodistas, militares, para planificaciones seguras, para proteger y preservar seguridad y para investigaciones seguras, permitiendo mantener un anonimato de forma transparente entre el emisor y el receptor.

5.3.Recomendaciones

- Se recomienda y es importante que los proveedores y el personal especializado en redes deban contar con información necesaria del funcionamiento y configuración de cada uno de los mecanismos a utilizar para la implementación y coexistencia de los dos protocolos.

- Es importante contar con personal especializado en redes de telecomuniciones o personal certificado en redes para el desarrollo de este proceso de migración y de igual manera contar con una capacitación permanente, es decir antes durante y después de la migración y coexistencia de los dos protocolos, para evitar fallas y estar en alerta con la funcionalidad y comportamiento de los dos protocolos.

- Se debe realizar el levantamiento de la infraestructura de la red que cada proveedor posee y realizar inventarios de software y hardware donde describa que equipos soporten los dos protocolos para la coexistencia de los mismos. Y a su vez definir qué áreas son menos críticas para realizar el proceso de migración con los mecanismos seleccionados.

- El mecanismo dual stack es uno de los mecanismos más recomendados debido que ofrece una convivencia flexible con los dos protocolos y cada uno actúa de forma independiente, los cuales son configurados en nodos finales permitiendo una transición eficiente, directa y su configuración no es compleja.

- Túnel es otro de los mecanismos recomendados debido a su funcionalidad ya que es un proceso de encapsulamiento de paquetes IPv6 dentro de paquetes IPv4 para posteriormente ser enviados a un nodo destino IPv4 y este a su vez desencapsular para extraer a IPv6. Este método es una técnica de integración y transición intermedia para los dos protocolos.

BIBLIOGRAFÍA

APLE. (Febrero de 2015). *¿Qué es IPv6?* Obtenido de https://support.apple.com/es-es/HT202236

AppleInc. (2007). *IPV6.* Obtenido de https://support.apple.com/es-mx/HT202236

Bellovin, S. (1996). *Problem Areas for the IP Security Protocols.* Obtenido de http://studies.ac.upc.edu/FIB/PIAM/Transici%F3%20IPv4-IPv6.pdf

Canal Tecnológico . (05 de Junio de 2012). *Ecuador se adelanta con protocolo IPv6 para instituciones públicas*. Recuperado el 11 de Septiembre de 2015, de http://www.canal-tecnologico.com/index.php?option=com_content&view=article&id=1429:ecuador-se-adelanta-con-protocolo-ipv6-para-instituciones-publicas&catid=30&Itemid=125

Carrasco, L. d. (FEBRERO de 2012). *Redes TOR.* Obtenido de http://www.ieee.es/Galerias/fichero/docs_opinion/2012/DIEEEO16-2012_RedesAnonimizacionInternet_LdeSalvador.pdf

Castro, E. (Febrero de 2006). *Página del Ministerio de Ciencia y Tecnología dedicada.* Obtenido de http://www.6sos.org.

CISCO. (17 de Abril de 2014). *Tipos de direccionameinto IPv6.* Obtenido de http://blog.capacityacademy.com/2013/04/17/cisco-ccna-todo-sobre-ipv6-direcciones-global-unicast-55/

Dunmore, M. (2005). *6net an IPv6 Deployment Guide.* Javvin : Technologies Inc.Distribution.

Google. (2015). *Ipv6 ene l mundo*. Obtenido de http://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption

IANA. (04 de Mayo de 2012). *Direcciones IP.* Obtenido de Internet Assigned Numbers Authority: Internet Assigned Numbers Authority es la entidad que supervisa la

IETF. (2012). *Protocolo IPv6.*

IP&mx. (2011). *Fundamentos de IPv6.* Obtenido de http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6#

LACNIC. (2011). *Latin America & Caribbean Network Information Centre.* Obtenido de Latin America & Caribbean Network Information Centre

LACNIC. (2012). *No hay más direcciones IPv4 en América Latina y Caribe*. Recuperado el 09 de Septiembre de 2015, de http://www.lacnic.net/web/anuncios/2014-no-hay-mas-direcciones-ipv4-en-lac

LACNIC. (2015). *Servicios de Registro.* Obtenido de http://www.lacnic.net/web/lacnic/ipv6-isp

Mejía, F. (16 de Mayo de 2012). *IPv6 en el Ecuado.* Obtenido de http://ecuadoruniversitario.com/ciencia-y-tecnologia/ipv6-en-el-ecuador/

Ministerio de Industria Energia y Turismo. (2008). *IPv6 para proveedores de servicios de internet.* Obtenido de http://www.ipv6.es/es-ES/transicion/ISPs/Paginas/IPv6_ISPs.aspx

msdn. (2005). *Solucionar problemas de IPv6*. Recuperado el 22 de Septiembre de 2015, de https://msdn.microsoft.com/es-es/library/cc780623(v=ws.10).aspx#BKMK_10

Network Information Center México S.C. (2012). *Fundamentos de IPv6.* Obtenido de Fundamentos de IPv6: http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6#

ORACLE. (2010). *Tuneles IPv6.* Obtenido de https://docs.oracle.com/cd/E19957-01/820-2981/6nei0r1ac/index.html

ORACLE. (2012). *Servicios IPv6.* Obtenido de http://docs.oracle.com/cd/E26921_01/html/E25871/ipv6-troubleshoot-2.html

Ralli, C. (2007). *Macanismos de transicion de IPv4 a IPv6.* Obtenido de http://www.cu.ipv6tf.org/pdf/carlos_ralli_transitiontutorial.pdf

Ralli, C. (2012). *Mecanismos de Transicion* . Obtenido de www.cu.ipv6tf.org/pdf/carlos_ralli_transitiontutorial.pdf

SENATEL. (2012). *Acuerdo_No_007-2012.* Obtenido de http://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/07/02_14_Acuerdo_No_007-2012.pdf

Technologies, J. (2008). *IPv6 Deployment Guide.* Javvin Technologies Inc.

Vives, A. (2014). *Despliegue de IPv6.* Obtenido de http://www.6deploy.eu/workshops2/20111010_guayaquil_ecuador/DIA4-1-1-Consulintel_Curso-IPv6_WALC2011.pdf

ANEXOS

ANEXO 1

Inventario de Hardware							
Nombre Responsable:							
Cargo:							
Área/Departamento							
Fecha:							
Tipo de Inventario:					**Total artículos inventario**		
					0		
Equipo/descripción	**Marca**	**Modelo**	**Nº Identificación / Serie /Código / Referencia**	**Tiempo de Servicio**	**Sistema Operativo**	**Soporte IPv6**	**Soporte IPv4**
Observaciones:							

_____ _____

Firma del Director TI **Firma del responsable**

Anexo 2

Inventario de Software							
Nombre Responsable:							
Cargo:							
Área/Departamento							
Fecha:							
Tipo de Inventario:					**Total artículos inventario**		
					0		
Equipo/descripción	**Marca**	**Modelo**	**Nº Identificación / Serie /Código / Referencia**	**Tiempo de Servicio**	**Sistema Operativo**	**Soporte IPv6**	**Soporte IPv4**
Observaciones:							

Firma del Responsable **Firma del Director TI**

Anexo 3

Plantilla de Pruebas			
Nombre Responsable:			
Cargo:			
Área/Departamento			
Fecha:			
1/2			
Ciclo de Pruebas:			**Total pruebas realizadas**
			0

Id	Caso de Prueba	Descripción	Fecha	Área Funcional / Sub proceso	Funcionalidad / Característica	Datos / Acciones de Entrada	Resultado Esperado	Requerimientos de Ambiente de Pruebas	Procedimientos especiales requeridos	Dependencias con otros casos de Prueba

Información para el Seguimiento			
Resultado Obtenido	**Estado**	**Última Fecha de Estado**	**Observaciones**

Firma del Responsable **Firma del Director TI**

Anexo 4

Configuracion Basica **Dual stack**

R1	
configuración Nombre	Router>ena Router#configure terminal Router(config)#hostname R1
Configuración de IPv4-IPv6 a la interfaz f0/0	R1(config)#interface **f0/0** R1(config-if)#ip address 10.0.0.1 255.255.255.0 R1(config-if)#ipv6 address 2001::1/64
Habilitar la interfaz	R1(config-if)#no shutdown
Configuración de IPv4-IPv6 ala interfaz s/0/0/0	R1(config)#interface **s0/0/0** R1(config-if)#ip address 10.1.1.1 255.255.255.0 R1(config-if)#ipv6 address FEC0:1::1/64
Habilitar la interfaz	R1(config-if)#no shutdown
Configuración RIP ipv4	R1(config)#router rip R1(config-router)#network 10.0.0.0
Comando para reconocer paquetes IPv6	R1(config)#ipv6 unicast-routing
Configuración RIP ipv6	R1(config)#ipv6 router rip SEBAS
Configuración RIP ipv6 en las interfaces f0/0	R1(config)#interface **f0/0** R1(config-if)#ipv6 rip SEBAS enable
Configuración RIP ipv6 en las interfaces s0/0/0	R1(config)#interface **s0/0/0** R1(config-if)#ipv6 rip SEBAS enable
Guarda la configuración	R1(config)#^Z
R2	
Configuración Nombre	Router>enable Router#configure terminal Router(config)#hostname R2
Configuración de IPv4-IPv6 a la interfaz s0/0/0	R2(config)#interface **s0/0/0**

	R2(config-if)#ip address 10.1.1.2 255.255.255.0 R2(config-if)#ipv6 address FEC0:1::2/64
Configuración de la velocidad	R2(config-if)#clock rate 128000
Habilitar la interfaz	R2(config-if)#no shutdown
Configuración de IPv4-IPv6 a la interfaz s/0/0/1	R2(config)#interface **s0/0/1** R2(config-if)#ip address 10.2.2.1 255.255.255.0 R2(config-if)#ipv6 address FEC0:2::12/64
Configuración de la velocidad	R2(config-if)#clock rate 128000
Habilitar la interfaz	R2(config-if)#no shutdown
Configuración RIP ipv4	R2(config)#router rip R2(config-router)#network 10.0.0.0
Comando para reconocer paquetes IPv6	R2(config)#ipv6 unicast-routing
Configuración RIP ipv6	R2(config)#ipv6 router rip SEBAS
Configuración RIP ipv6 en las interfaz s0/0/0	R2(config)#interface **s0/0/0** R2(config-if)#ipv6 rip SEBAS enable
Configuración RIP ipv6 en las interfaz s0/0/1	R2(config)#interface **s0/0/1** R2(config-if)#ipv6 rip SEBAS enable
Guarda la configuración	R2(config)#^Z
R3	
Configuración Nombre	Router>ena Router#configure terminal Router(config)#hostname R3
Configuración Interface s0/0/1 (IPv4 e IPv6)	R3(config)#interface **s0/0/1** R3(config-if)#ip address 10.2.2.2 255.255.255.0 R3(config-if)#ipv6 address FEC0:2::2/64
Habilitar la interfaz	R3(config-if)#no shutdown
Configuración Interface f0/0 (IPv4)	R3(config)#interface **f0/0** R3(config-if)#ip address 10.3.3.1 255.255.255.0
Habilitar la interfaz	R3(config-if)#no shutdown

Configuración IPv6 a la Interfaz f0/1	R3(config)#interface **f0/1** R3(config-if)#ipv6 address 2001:3::1/64
Habilitar la interfaz	R3(config-if)#no shutdown
Configuración RIP ipv4	R3(config)#router rip R3(config-router)#network 10.0.0.0
Comando para reconocer paquetes IPv6	R3(config)#ipv6 unicast-routing
Configuración RIP ipv6	R3(config)#ipv6 router rip SEBAS
Configuración RIP ipv6 en las interfaz s0/0/1	R3(config)#interface **s0/0/1** R3(config-if)#ipv6 rip SEBAS enable
Configuración RIP ipv6 en las interfaz f0/1	R3(config)#interface **f0/1** R3(config-if)#ipv6 rip SEBAS enable
Guarda la configuración	R3(config)#^Z

Anexo 5
Configuración Basica **Tunneling**

ROUTER0	
Configuración Nombre	Router > enable Router # configure terminal Router (config) #hostname ROUTER0
Configuración de IPv6 a la interfaz f0/0	ROUTER0 (config) #interface **f0/0** ROUTER0 (config-if) #ipv6 address 2001:db8:aaaa:1::1/64
Habilitar la interfaz	ROUTER0 (config-if) #no show
Configuración de IPv4 a la interfaz s/0/0/0	ROUTER0 (config) #interface **s0/0/0** ROUTER0 (config-if) #ip address 192.168.10.1 255.255.255.0
Habilitar la interfaz	ROUTER0 (config-if) #no show
Configuración RIP ipv4	ROUTER0 (config) # Router RIP ROUTER0 (config-route) #network 192.168.10.0

Comando para reconocer paquetes IPv6	ROUTER0 (config) # ipv6 unicast-routing
Crea el Tunnel	ROUTER0 (config) # interface Tunnel0
No va tener IPv4	ROUTER0 (config-if) # no ip address
Crea IPv6 (tunnel) nombre y dirección	ROUTER0 (config-if) # ipv6 address 2001:db8:bbbb:1::1/64
Interface que se asocia – Interfaz fuente	ROUTER0 (config-if) # tunnel source **s0/0/0**
Destino de Tunnel (Llega a la dirección IPv4)	ROUTER0 (config-if) # tunnel destination 192.168.11.2
Tunnel IPv6 sobre IPv4	ROUTER0 (config-if) # tunnel mode ipv6ip
Habilitar la interfaz	ROUTER0 (config-if) # no show
Configuración de ruta estática IPv6 (Dirección IP destino y la interfaz de entrada)	ROUTER0 (config) # ipv6 route 2001:db8:cccc:1::/64 2001:db8:bbbb:1::2
Guarda la configuración	ROUTER0 (config)#^Z
ROUTER1	
Configuración Nombre	Router > enable Router # configure terminal Router (config) #hostname ROUTER1
Configuración de IPv4 a la interfaz s0/0/0 (IPv4)	ROUTER1 (config) #interface **S0/0/0** ROUTER1 (config-if) #ip address 192.168.10.2 255.255.255.0
Configuración de la velocidad	ROUTER1 (config-if) #clock rate 128.000
Habilitar la interfaz	ROUTER1 (config-if) #no show
Configuración de IPv5 a la Interfaz s0/0/1	ROUTER1 (config) #interface **S0/0/1** ROUTER1 (config-if) #ip address 192.168.11.2 255.255.255.0
Configuración de la velocidad	ROUTER1 (config-if) #clock rate 128.000
Habilitar la interfaz	ROUTER1 (config-if) #no show
Configuración RIP ipv4	ROUTER1 (config) #router RIP ROUTER1 (config-route) #ip address 192.168.10.0

	ROUTER1 (config-route) #ip address 192.168.11.0
Habilitar la interfaz	ROUTER1 (config-if) #no show
Guarda la configuración	ROUTER1 (config)#^Z
ROUTER2	
Configuración Nombre	Router > enable Router # configure terminal Router (config) #hostname ROUTER2
Configuración de IPv6 a la Interfaz f0/1	ROUTER2 (config) #interface f0/1 ROUTER2 (config-if) #ipv6 address 2001:db8:cccc:1::1/64
Habilitar la interfaz	ROUTER2 (config-if) #no show
Configuración de IPv4 a la Interfaz s0/0/0	ROUTER2 (config) #interface **s0/0/1** ROUTER2 (config-if) #ip address 192.168.11.2 255.255.255.0
Habilitar la interfaz	ROUTER2 (config-if) #no show
Configuración RIP IPv4	ROUTER2 (config) # Router RIP ROUTER2 (config-route) #network 192.168.11.0
Comando para reconocer paquetes IPv6	ROUTER2 (config) # ipv6 unicast-routing
Crea el Tunel	ROUTER2 (config) # interface Tunnel0
No va tener IPv4	ROUTER2 (config-if) # no ip address
Crea IPv6 (Tunnel) nombre y Dirección	ROUTER2 (config-if) # ipv6 address 2001:db8:bbbb:1::2/64
Interface que se asocia – Interfaz fuente	ROUTER2 (config-if) # tunnel source **s0/0/1**
Destino de Tunnel (Llega a la Dirección IPv4)	ROUTER2 (config-if) # tunnel destination 192.168.10.1
Tunnel IPv6 sobre IPv4	ROUTER2 (config-if) # tunnel mode ipv6ip
Habilitar la interfaz	ROUTER2 (config-if) # no show
Configuración de ruta estática IPv6 (Dirección IP destino y la interfaz de entrada)	ROUTER2 (config) # ipv6 route 2001:db8:aaaa:1::/64 2001:db8:bbbb:1::1

Guarda la configuración	ROUTER1 (config)#^Z

Anexo 6

Configuración básica de Dual Stack-Tunel

R2	
Configuración Nombre	Router>enable Router#configure terminal Router(config)#hostname R2
Configuración de IPv6-IPv4 a la interfaz s0/0/0	R2(config)#interface s0/0/0 R2(config-if)#ip address 10.1.1.2 255.255.255.0 R2(config-if)#ipv6 address FEC0:1::2/64
Configuración de la velocidad	R2(config-if)#clock rate 128000
Habilitar la interfaz	R2(config-if)#no sh R2(config-if)#exit
Configuración de IPv4 a la interfaz s/0/0/1	R2(config)#interface s0/0/1 R2(config-if)#ip address 10.2.2.1 255.255.255.0 R2(config-if)#ipv6 address FEC0:2::12/64
Configuración de la velocidad	R2(config-if)#clock rate 128000
Habilitar la interfaz	R2(config-if)#no sh R2(config-if)#exit
Configuración RIP ipv4	R2(config)#router rip R2(config-router)#network 10.0.0.0 R2(config-router)#exit
Comando para reconocer paquetes IPv6	R2(config)#ipv6 unicast-routing
Configuración RIP ipv6	R2(config)#ipv6 router rip SEBAS R2(config-rtr)#exit

Configuración RIP ipv6 en las interfaz S0/0/0	R2(config)#interface s0/0/0 R2(config-if)#ipv6 rip SEBAS enable R2(config-if)#exit
Configuración RIP ipv6 en las interfaz S0/0/0	R2(config)#interface s0/0/1 R2(config-if)#ipv6 rip SEBAS enable R2(config-if)#exit R2(config)#^Z
Guarda la configuracion	R2(config)#^Z
R1	
Configuración Nombre	Router>ena Router#configure terminal Router(config)#hostname R1
Configuracion IPv4 – Ipv6 en la interfaz f0/0	R1(config)#interface f0/0 R1(config-if)#ip address 10.0.0.1 255.255.255.0 R1(config-if)#ipv6 address 2001::1/64
Habilitar la interfaz	R1(config-if)#no sh R1(config-if)#exit
Configuracion IPv4 – Ipv6 en la interfaz s0/0/0	R1(config)#interface s0/0/0 R1(config-if)#ip address 10.1.1.1 255.255.255.0 R1(config-if)#ipv6 address FEC0:1::1/64
Habilitar la interfaz	R1(config-if)#no sh R2(config)#exit
Configuracion RIP ipv4	R1(config)#router rip R1(config-router)#network 10.0.0.0 R1(config-router)#exit
Comando para reconocer paquetes IPv6	R1(config)#ipv6 unicast-routing
Configuracion RIP ipv6	R1(config)#ipv6 router rip SEBAS R1(config-rtr)#exit
Configuración de IPv6 a la Interfaz f0/1	R1(config)#interface f0/0 R1(config-if)#ipv6 rip SEBAS enable R1(config-if)#exit

Configuración de IPv6 a la Interfaz f0/1	R1(config)#interface s0/0/0 R1(config-if)#ipv6 rip SEBAS enable R1(config-if)#exit
Guarda la configuración	R1(config)#^Z
R3	
Configuración Nombre	Router>ena Router#configure terminal Router(config)#hostname R3
Configuración de IPv4-IPv6 a la Interfaz s0/0/1	R3(config)#interface s0/0/1 R3(config-if)#ip address 10.2.2.2 255.255.255.0 R3(config-if)#ipv6 address FEC0:2::2/64
Habilitar la interfaz	R3(config-if)#no sh R3(config-if)#exit
Configuración de IPv4 a la Interfaz f/0/0	R3(config)#interface f0/0 R3(config-if)#ip address 10.3.3.1 255.255.255.0
Habilitar la interfaz	R3(config-if)#no sh R3(config-if)#exit
Configuración de IPv4 a la Interfaz f/0/1	R3(config)#interface f0/1 R3(config-if)#ipv6 address 2001:3::1/64
Habilitar la interfaz	R3(config-if)#no sh R3(config-if)#exit
Configuracion RIP ipv4	R3(config)#router rip R3(config-router)#network 10.0.0.0 R3(config-router)#exit
Comando para reconocer paquetes IPv6	R3(config)#ipv6 unicast-routing
Configuracion RIP ipv6	R3(config)#ipv6 router rip SEBAS R3(config-rtr)#EXIT R3(config)#
Configuracion RIP ipv6 en las interfaz s0/0/1	R3(config)#interface s0/0/1 R3(config-if)#ipv6 rip SEBAS enable R3(config-if)#exit

Configuracion RIP ipv6 en las interfaz s0/0/1	R3(config)#interface f0/1 R3(config-if)#ipv6 rip SEBAS enable R3(config-if)#exit R3(config)#^Z
Guarda la configuración	R3(config)#^Z