# MIGRACIÓN HACIA EL DIRECCIONAMIENTO IPV6 CON EL PROTOCOLO DE ENRUTAMIENTO RIPNG (PROTOCOLO DE ENCAMINAMIENTO DE INFORMACIÓN DE NUEVA GENERACIÓN)

AMPARO JAIMES CABALLERO

SANDRA MILENA VEGA SANABRIA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
ESCUELA DE INGENIERIA ELECTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES
ESPECIALIZACIÓN DE TELECOMUNICACIONES
BUCARAMANGA
2008

# MIGRACIÓN HACIA EL DIRECCIONAMIENTO IPV6 CON EL PROTOCOLO DE ENRUTAMIENTO RIPNG (PROTOCOLO DE ENCAMINAMIENTO DE INFORMACIÓN DE NUEVA GENERACIÓN)

AMPARO JAIMES CABALLERO

SANDRA MILENA VEGA SANABRIA

Monografía para optar al título de
Especialista en Telecomunicaciones

Director

RAUL BAREÑO GUTIERREZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER
ESCUELA DE INGENIERIA ELECTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES
ESPECIALIZACIÓN DE TELECOMUNICACIONES
BUCARAMANGA
2008

*A nuestros padres.*

*Primeros formadores de vida*

*y apoyo en todo momento*

*motivo por el cual, hoy somos*

*el fruto de sus sacrificios y*

*Esfuerzos.*

## AGRADECIMIENTOS

A mis padres que con su apoyo moral me ayudaron a culminar este proyecto.

Al ingeniero Cesar Duarte, que con su experiencia y colaboración nos orientó y nos ayudó en esta etapa de superación.

A mi esposo por el apoyo y la paciencia que tuvo para que pudiera terminar esta etapa mas en mi vida.

Amparo

Al gerente de operaciones y a la supervisora de la sala de grabación de SYC S.A. por sus consejos, apoyo y colaboración.

A Amparo Jaimes Caballero, amiga incondicional y motor de impulso para iniciar esta etapa de formación.

Y sobre todo a Dios, quien puso en mi camino a tan excelentes personas, docentes, compañeros y amigos, las herramientas y la fortaleza para iniciar, mantener y culminar este proyecto de superación profesional.

Sandra

**TABLA DE CONTENIDO**

**Pág.**

## LISTAS DE FIGURAS

## LISTA DE GRAFICOS

## LISTA DE TABLAS

**Pág.**

## RESUMEN

**TITULO:** **MIGRACIÓN HACIA EL DIRECCIONAMIENTO IPV6 CON EL PROTOCOLO DE ENRUTAMIENTO RIPNG (PROTOCOLO DE ENCAMINAMIENTO DE INFORMACIÓN DE NUEVA GENERACION)*

**AUTOR:** JAIMES CABALLERO, Amparo
VEGA SANABRIA, Sandra Milena**

**PALABRA CLAVES:** Tunelización, Ripng, Ipv4, Ipv6, Dual Stack, Enrutador, Traducción

.

**DESCRIPCIÓN:**

La presente monografía es el resultado de la investigación realizada por los autores, quienes en la búsqueda de nuevas tecnologías, encuentran la forma más orientada de realizar la migración hacia ipv6 en corto tiempo, sin causar traumatismos tecnológicos. Las opciones que se encuentran en la actualidad permiten facilitar la transición y escalar sin ningún problema entre versiones IP. Debido a que se manejan gran variedad de escenarios cuyos mecanismos facilitan esta acción a cualquier administrador de red.

Con el nuevo protocolo Ipv6 (Internet Protocol version 6) ha sido desarrollado recientemente para responder a las necesidades planteadas por los nuevos servicios de Internet. Sin embargo, aunque se trata de protocolos del nivel de red, las aplicaciones no son ajenas al cambio. Para completar la transición a Ipv6 es necesario revisar las aplicaciones. El proceso de migración no se puede hacer de forma instantánea y en consecuencia, durante el período de transición surgirán escenarios donde aplicaciones Ipv4 e Ipv6 tendrán que coexistir e incluso ínter operar. Los escenarios mas utilizados para realizar la migración de Ipv4 a Ipv6 son los siguientes:

- Dual Stack: es el mecanismo que implementa las 2 versiones de los protocolos en cada nodo de la red.

- Tunneling: es el proceso por medio del cual se encapsulan paquetes de Ipv6 dentro de paquetes de Ipv4 utilizando enrutadores.

- Traducción: proceso que realiza una traducción donde modifica la cabecera de Ipv4 por una cabecera Ipv6.


---

* Monografía

** F Facultad de Ingenierías Físico-Mecánicas. Especialización en Telecomunicaciones. Director: Ing. Raúl Bareño Gutiérrez.

## SUMMARY

**TITLE**: **MOVING TO IPV6 ADDRESS WITH RIPNG ROUTING PROTOCOL (PROTOCOL ROUTING INFORMATION AGAIN GENERATION)**[*]

**AUTHOR:** Jaimes Caballero, Amparo
Vega Sanabria, Sandra Milena [**]

**KEYWORD**: Tunneling, Ripng, Translation, IPv4, IPv6, Dual Stack, Routing, Traslation.

**DESCRIPTION:**

The present graduation work is the result of the research made by the authors, who in the quest for new technologies, find ways is more oriented towards the migration of ipv6 in short time, without causing injuries technological, The options that are currently permitted to facilitate the transition and climb without any problems between versions IP. Due to handle a variety of scenarios whose mechanisms facilitate this action to any network administrator.

With the new protocol IPv6 (Internet Protocol version 6) has been recently developed to meet the needs raised by the new Internet services. However, although this is the level of network protocols, applications are not alien to change. To complete the transition to IPv6 is necessary to review the applications. The process of migration can not be done instantly and in consequence, during the transition period will arise Scenarios where Ipv4 and IPv6 applications will have to coexist and even inter-operate. The scenarios used more for the migration of IPv4 to IPv6 are:

- Dual Stack: is the mechanism that implements the 2 versions of the protocols on each node on the network.

- Tunneling is the process through which encapsulate IPv6 packets within IPv4 packets using routers.

- Translation: the process that makes a translation which modifies the IPv4 header from a header by IPv6.


[*] Draft grade

[**] College Physics Mechanics - School Electric Engineering, Electronics and Telecommunications Director Raúl Bareño Gutiérrez.

# GLOSARIO

ACC (Advanced computer Comms), Equipo de comunicaciones avanzadas, empresa desarrolladora de equipo de telecomunicaciones como Amazon POP Router, Congo/Voice Router, y Danube también.

APPLETALK: Conjunto de protocolos desarrollados por Apple Inc. Para la conexión de redes. Fue incluido en un Macintosh en 1984 y actualmente está en desuso en los Macintosh a favor de las redes TCP/IP

ARPANET: (Advanced Research Projects Agency Network) se considera que fue el origen de Internet como lo conocemos hoy en día. Fue sustituida por la Red de la Fundación Nacional para la Ciencia (NSFNET, acrónimo en inglés) para conectar sus supercomputadoras.

GWINFO: protocolo de XEROX de donde se considera el origen de RIP.

BGPD: (Border Gateway Protocol), Protocolo de Pasarela Fronteriza.

BGP-4 Border Gateway Protocol versión4: Es un protocolo de enrutamiento específicamente desarrollado para administrar el intercambio de información de enrutamiento entre diferentes sistemas autónomos o dominios de enrutamiento. Ampliamente definido en la RFC 1105 4271. Soporta CIDR y sumarización de rutas.

BROADCAST: es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos o equipos.

BSD: son las siglas de “Berkeley Software Distribution”. Así se llamó a las distribuciones de código fuente que se hicieron en la Universidad de Berkeley en California y que en origen eran extensiones del sistema operativo UNIX de AT&T Research.

DATAGRAMA: Un datagrama es un fragmento de paquete que es enviado con la suficiente información como para que la red pueda encaminar el fragmento hacia el equipo terminal o de destino, de manera independiente a los fragmentos restantes.

DECNET: Es un grupo de productos de Comunicaciones, desarrollado por la firma Digital Equipment corporation. La primera versión de DECnet se realiza en 1975 y permitía la comunicación entre dos mini computadoras PDP-11 directamente. Se desarrollo en una de las primeras arquitecturas de la red Peer-to peer.

DISTANCIA ADMINISTRATIVA: Es la medida usada por los enrutadores para seleccionar la mejor ruta cuando hay dos o más rutas distintas hacia el mismo destino para dos protocolos de enrutamiento.

DNS (Domain Name System): Es un servidor que permite asignar los nombres a los equipos para que se puedan comunicar entre ellos bajo una misma red.

DSTM (Dual Stack Transition Mechanis) es un mecanismo de transición que se usa para hacer tunelización.

EGP: Exterior Gateway Protocol., protocolos de pasarela exterior, utilizado para el intercambio de información de encaminamiento entre pasarelas exteriores o entre SA (Sistema Autónomo) que no pertenezcan al mismo SA.

ENRUTADOR: dispositivo de trabajo para interconexión de redes de computadores que opera en capa tres. Es el encargado de realizar la selección de ruta con base en la información del protocolo enrutador (Ipv4-Ipv6).

ENRUTAMIENTO: es la búsqueda de un camino entre todos los posibles en una red de paquetes cuya topología parece una gran cantidad de nodos interconectados.

ETHERNET: Es un estándar para redes de área local con acceso al medio CSMA/CD, con características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI bien definidos.

FTP (File Transfer Protocol) Es un protocolo que permite transferir archivos de computador a otro, a través de una conexión TCP/IP.

HOST: es una maquina conectada a una red de datos y que tiene un nombre de equipo.

HTTP (HyperText Transfer Protocol) Es un protocolo que le permite acceder a la web y a su vez se encarga de procesar y dar respuesta a una petición.

ICMP: protocolo de control de mensajes de Internet. Se usa para enviar mensajes de error en Internet.

IGP: Interior Gateway Protocol, protocolos de pasarela interno, la cual hace referencia a los protocolos usados dentro de un SA (Sistema Autónomo). Utilizado para el intercambio de información de encaminamiento interno.

IGR: Interior Gateway Routing Protocol (IGRP) o Protocolo de Enrutamiento de Pasarela Interior, es un protocolo propietario patentado y desarrollado por Cisco que se emplea con el protocolo TCP/IP según el modelo (OSI) Internet comúnmente para el intercambio de datos dentro de sistemas Autónomos, aunque también es utilizado como Exterior Gateway Protocol (EGP) para el enrutamiento inter-dominio.

IP: Protocolo de Internet. Conjunto de reglas que regulan la transmisión de paquetes de datos a través de Internet. Se trata de una representación numérica de la localización de un computador dentro de una red.

IPV4: versión 4 del protocolo de Internet (IP) es estándar actual de Internet para identificar dispositivos conectados a la red. Se compone de 32 bits

IPV6: versión 6 del protocolo de Internet (IP) es el encargado de dirigir los paquetes a través de una red. Se compone de 128 bits

IPX (Netware de Novell): IPX es un protocolo de intercambio de paquetes entre Redes (IPX) es la implementación del protocolo IDP (Inter Datagram Protocol) de Xerox. Es un protocolo de datagramas rápido orientado a comunicaciones sin conexión que se encarga de transmitir datos a través de la red, incluyendo en cada paquete la dirección destino.

LAN: Red de Área Local. Red de datos para dar servicio a una determinada área geográfica con velocidades de transmisión de 1000 Mbps o mas (mega bits por segundo).

MULTICAST: Es la comunicación de un solo emisor y varios receptores dentro de una red.

MD5: (Message-Digest Algorithm 5). Algoritmo de Resumen del Mensaje 5, es un algoritmo de reducción criptográfico que se utiliza para encriptar las contraseñas con la función md5() se codifica el pass Word ingresado por un usuario, y luego se realiza una comparación de igualdad entre ambas contraseñas codificadas.

MÉTRICA: La métrica de enrutamiento es el método mediante el cual un algoritmo de enrutamiento determina que una ruta es mejor que otra. Esta información se guarda en tablas de enrutamiento. Las métricas incluyen ancho de banda, costo de la comunicación, retraso, número de saltos, carga, MTU, costo de la ruta y confiabilidad. A veces se denomina simplemente métrica.

MIT (Massachusetts Institute of Tecnology, Instituto Tecnológico de Massachusetts).

MTU: (Maximun Transfer Unit –MTU) Unidad Máxima de Transferencia es un término de redes que expresa el tamaño en bytes del datagrama mas grande que puede pasar por una capa de un protocolo de comunicaciones. Para Ethernet 1500 bytes, PPPoE: 1492 bytes, ATM(AAL5): 8190 bytes, FDDI: 4470 Bytes, PPP: 576 bytes.

NAT: Network Address Translation. Es un estándar de Internet que le permite a la red local LAN usar un grupo de direcciones IP privadas para su tráfico interno.

NETBEUI (NetBIOS Extended User Interface) - Interfaz extendida de usuario de NetBIOS): Es un protocolo que no mueve ficheros de gran tamaño.

NSFNet: National Science Foundation's Network. La NSFNET comenzó con una serie de redes dedicadas a la comunicación de la investigación de la educación. Fue creada por el gobierno de los Estados Unidos a través de la National Science fundation, y fue el reemplazo de ARPANET como backbone de Internet. Desde entonces ha sido reemplazada por las redes comerciales.

OPENBGPD: Es una implementación libre del Border Gateway Protocol, versión 4. Permite que las máquinas ordinarias puedan ser utilizadas como enrutadores intercambiando de rutas con otros sistemas.

OPENBS: Es un sistema operativo libre tipo Unix, multiplataforma, basado en 4.4 BSD. Es un descendiente de NetBSD, que ha integrado la seguridad y la criptografía.

OSPF: Open Shortest Path First, es un protocolo de enrutamiento jerárquico de pasarela interior o IGP, que usa el algoritmo DIjkstra, estado del enlace (LSA- Link State Algorithm) para calcular la ruta más corta posible. Usa como métrica el costo, construye una base de datos del estado del enlace idéntica en todos los enrutadores de la zona. Es utilizado en grandes redes.

PPTP (Protocolo de túnel punto a punto) Es un protocolo de capa 2 que utiliza las redes compatibles con las redes virtuales privadas.

PROTOCOLO: es el que permite la comunicación de datos, voz y video a través de una red de paquetes conmutados.

PROXY: Programa o dispositivo que realiza una representación de otro

PUP (Parc Universal Packet): Era un protocolo usado a nivel de red que luego evolucionaría hasta convertirse en el que luego fue XNS (Xerox Network System), antecesor a su vez de IPX (Netware de Novell)

RIPNG: es un protocolo de Internet que esta diseñado para habilitar la expansión de Internet hacia el direccionamiento ipv6

RFC: (Request For Comment- Petición de comentarios). Son documentos que se iniciaron en 1967 que describen los protocolos de Internet.

ROUTERS PROTEON: Enrutador original denominado PROTEON desarrollado por J. Noel Chiappa, cuya puerta de enlace es llamada MIT C, es el primer enrutador de código escrito en C, el código debe ser desarrollado en el MIT y escrito en C por las siglas MIT C

RTM: Real Time Messagin Protocol (RTMP) Protocolo de Mensajería en Tiempo Real, es de propiedad de Adobe System para el streaming de audio, vídeo y datos a través de la Internet, entre una versión de Flash Player y un servidor.

SA Sistema Autónomo: En Internet, un Sistema Autónomo es un conjunto de redes y dispositivos enrutador IP que se encuentran administrados por una sola entidad o en algunas ocasiones varias, que cuentan con una política en común de definición de trayectorias para Internet referenciado en el RFC 1930.

SERVIDOR: es el dispositivo que se encarga de proporcionar datos de modo que otros computadores puedan utilizar esos mismos datos.

SNA (System Network Architecture) Es el encargado de describir el protocolo aunque no lo es.

SISTEMAS XEROX (XNS): Serie de protocolos que la empresa Xerox Corporation desarrolló y publicó como estándar abierto llamado Especificación de Red Xerox (Xerox Network Specification, XNS). Define una serie de protocolos designados para la interconexión de propósito general, con énfasis en el uso de redes de área local.

SUMARIZACION: Es la capacidad del enrutador para manejar diversas redes.

TCP/IP: Familia de protocolos de Internet, es un conjunto de protocolos de red en la que se basa Internet y que permiten la transmisión de datos entre redes de computadoras.

TUNEL: Trayectoria virtual por la que viajan los paquetes de un punto a otro de Internet

TUNELIZACION: es usado para transportar tráfico de un protocolo sobre una red que no soporta ese protocolo directamente

UDP (User Datragram Protocol): Es u protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

VLSM (variable length subnet mask): Es una técnica que permite dividir subredes en redes más pequeñas que se ajusten a las necesidades reales de la red (los enrutadores que utilizan protocolos de enrutamiento sin clase como RIPV2 y OSPF pueden trabajar con un esquema de direccionamiento IP que contenga diferentes tamaños de mascara

# INTRODUCCIÓN

El direccionamiento IP es un componente fundamental de la pila de protocolos de TCP/IP, es la utilizada actualmente en redes de datos y su interconexión es lo que se conoce como Internet. El direccionamiento IP se divide en cuatro octetos de bits cada uno identifica de forma precisa y única la ubicación de cada computador en Internet.

Este sistema, esta en uso desde hace mas de 20 años (el actual IP v4 data de 1981), la organización Arin (American registry of Internet number) que administra la distribución de los recursos numéricos de Internet y su equivalente en Latinoamérica LACNIC (Registro de Direcciones de Internet para América Latina y el Caribe) creó un rango de direcciones basadas en cinco clases:

- Clase A tiene un rango de 1.0.0.0 a 126.0.0.0

- Clase B tiene un rango de 128.0.0.0 a 191.255.255.255.

- Clase C tiene un rango de 192.0.0.0 a 223.255.255.255

- Clase D tiene un rango de 224.0.0.0 a 239.255.255.255

- Clase E tiene un rango de 240.0.0.0 a 255.255.255.255 reservadas para uso futuro.

Actualmente se estima que el 81% del total de estas direcciones ya han sido asignadas y para finales del año pasado solo quedaban el 19% por asignar debido al amplio crecimiento de Internet, se prevé que en un futuro próximo no habría suficientes combinaciones de direcciones IP distintos para cada dispositivo conectado a la red.

Cuando IPV4 se diseño parecía inagotable, hoy en día se ve que no es así, las estadísticas que pronostican el tiempo que tardarían en terminarse se dice que lo más probable es que sea para antes del 2010 aunque es improbable definir la fecha exacta de su terminación ya que en Internet han aparecido noticias anunciando sobre esta escasez creando un ambiente de intranquilidad entre los usuarios lo cual conllevaría consecuentemente a la creciente demanda por adquisición de direcciones Ipv4, ocasionando que esta extinción fuera antes de lo pronosticado.

Como consecuencia a lo anterior y previniendo esta carencia se han creado nuevas tecnologías para alargar la vida de las direcciones Ipv4 incluidas en las redes classfull, direcciones CIDR (Classless Inter- Domain Routing por su traducción en ingles) y por supuesto NAT (Network Address Traslation – traducción de Direcciones de Red), algunas no recomendables a largo plazo, mientras que se implementan las direcciones Ipv6, sin sustituir totalmente a las Ipv4 logrando mantenerse ambas versiones siempre que las aplicaciones así lo requieran.

En la actualidad ya se encuentra en uso, esto implica el alto procesamiento que tendrían los routers para el envió de los datos.

La mayoría de los sistemas operativos de los dispositivos de capa tres solo enrutan direcciones de 32 bits pero la alta demanda de trafico a nivel mundial ya existen interconexiones a través de direcciones Ipv6 lo cual lleva a los ingenieros de redes a trabajar en nuevos protocolos de enrutamiento como Ripng (protocolo de encaminamiento de información de nueva generación), Este emplea direcciones ipv6 que son direcciones que pasan de 32 a 128 bits, o sea de $2^{32}$ direcciones que equivale a (4.294.967.296) a $2^{128}$ direcciones que equivale a (3.402823669 e38, o sea sobre 1.000 sixtillones) lo que equivaldría a que cada persona en el mundo tuviera una dirección IP e incluso se dice que cada célula de su cuerpo.

El principal beneficio del direccionamiento Ipv6 será la plena disponibilidad de direcciones IP, posibilitando que Internet vuelva a ser una red "entre extremos" ("end to end model") lo que quiere decir que no hay necesidad de utilizar tecnologías como NAT (Network Address Translation) para salir a Internet ya que cada equipo puede disponer de su propia dirección. En Ipv6 se hace necesaria la utilización del NAT (Traducción de direcciones de red) ya que existen direcciones suficientes, NAT tiene un direccionamiento privado que no se enrutan a Internet del cual comprende lo siguiente:

En la direcciones Clase A es todo el rango de 10.0.0.0/8

Clase B es el rango 172.16.0.0 hasta: 172.31.255.255/12

Clase C es el rango 192.168.0.0/16

Siendo estas las direcciones IP que son comprendidas para hacer redes privadas cuya salida a Internet no se puede realizar por si mismas por ser de carácter privado a no ser que se utilice un mecanismo de comprensión o de traducción de direcciones como NAT asociado con PAT para tener salida a Internet por medio de una dirección pública.

Esto es necesario debido a la escasez de direcciones provocada por el agotamiento anteriormente descrito. Otra razón de utilizar NAT es por seguridad, si no se utiliza cada computador queda expuesto a compartir sus recursos con Internet y se hace necesario entonces utilizar mas cantidad de ACL (Access Control List) para que la seguridad no sea un problema.

# PARTE I: FUNDAMENTOS

# 1. ASPECTOS GENERALES

## 1.1 MOTIVACION

La nueva versión del Protocolo Internet (IP) ha sido tema de conversación entre los profesionales e investigadores de redes desde hace tiempo, sin embargo nunca pareció ser de importancia. Las personas encargadas de planificar redes y negocios han estado escuchando a aquellos que defienden el protocolo de comunicaciones de nueva generación (Ripng) y a aquellos que lo ignoran elocuentemente, pero no han podido observar una tendencia, ni el surgimiento de una nueva ola, por lo menos, no de momento. Por lo tanto, año tras año se dieron cuenta que protocolo Ipv4 no era lo suficiente, hicieron un cálculo y notaron que para el 2010 no habría mas direcciones que asignar. Con la escasez que presentaba el Ipv4 se vieron en la necesidad de optar por una tecnología de nueva generación como lo es Ripng (Protocolo de Encaminamiento de Información de Nueva Generación) que trabaja de la mano con Ipv6 y que es un estándar que se encarga de encaminar paquetes a través de redes de computadores.

## 1.2 OBJETIVOS

### 1.2.1 OBJETIVO GENERAL

Analizar los escenarios y ventajas de migrar hacia el direccionamiento IPV6 mediante el protocolo de enrutamiento Ripng (Protocolo de encaminamiento de información de nueva generación).

### 1.2.2 OBJETIVOS ESPECIFICOS

- Analizar la tecnología RIPNG (Protocolo de Encaminamiento de Información de Nueva Generación).
- Examinar posibles escenarios para la introducción de este protocolo de nueva generación para proveedores de servicio y redes empresariales.
- Diseño e implementación de Ripng en tunelización de Ipv4 a Ipv6

## 1.3 DESCRIPCIÓN DEL DOCUMENTO

Este documento está compuesto en dos partes: la primera relacionada con los fundamentos, el estado del arte y el marco teórico que dan soporte a la investigación propuesta, la segunda es la implementación de uno de los mecanismos mas usados del Ripng (protocolo de encaminamiento de información de nueva generación), como es la tunelización.

**Parte I: FUNDAMENTOS**

**Capitulo 1. Aspectos Generales**

Describe la motivación de los autores para realizar la investigación y análisis del presente trabajo y define los objetivos que enmarcan su desarrollo.

**Capitulo 2. Estado del Arte**

Breve descripción del estado actual de las investigaciones y desarrollos que se han llevado a cabo en el área de las telecomunicaciones en cuanto a la evolución de las versiones IP hasta el momento por el incremento de demanda en direcciones IP.

**Capitulo 3. Análisis descriptivo concerniente al protocolo de información de Encaminamiento de Nueva Generación – RIPNG.**

Presenta la base teórica a tener en cuenta para conocer los orígenes, funcionamiento y modos de implementar el protocolo de información de encaminamiento de nueva generación –RIPNG. Y conocer las formas factibles de transición en el cual se pueda llegar a desarrollar.

**Parte II: PUESTA EN MARCHA**

**Capitulo 4. Diseño e implementación del protocolo de encaminamiento dinámico RIPNG mediante el mecanismo de transición denominado tunelización.**

En este capitulo se presenta el desarrollo del laboratorio en donde se muestran las actividades llevadas a cabo para la construcción de una topología diseñada, y de esta forma cumplir con los objetivos planteados al iniciar el proyecto, con el fin de obtener los resultados esperados.

El documento finaliza con las conclusiones de los autores sobre el trabajo desarrollado.

## 2. ESTADO DEL ARTE

La IANA (Internet Assigned Number Authority - Autoridad de Asignación de Números en Internet), en 1992 concluyó que se terminarían las direcciones que maneja Ipv4. Desde ese momento podríamos decir que se tomaron la tarea de adquirir formas de retardar el deceso de direcciones.

Esta crisis de direccionamiento viene del año 2000 a hoy, lo único que se ha hecho es retardar la implementación de Ipv6 mediante soluciones provisionales como son:

- Subredes
- NAT (**Network Address Translation**)
- PAT (**Port Address Translation)**
- VLSM **(variable length subnet mask)**
- DHCP (**Dynamic Host Configuration Protocol**)

Ipv6 sustituirá al estándar Ipv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, Pero, el nuevo estándar mejorará el servicio globalmente; por ejemplo, proporcionando a futuras celdas telefónicas y dispositivos móviles con sus direcciones propias y permanentes. Al día de hoy, se calcula que las dos terceras partes de las direcciones que ofrece Ipv4 están asignadas.

Ipv4 soporta 4.294.967.296 ($2^{32}$) direcciones de red diferentes, un número inadecuado para dar una dirección a cada persona del planeta, mientras que Ipv6

soporta 340.282.366.920.938.463.463.374.607.431.768.211.456 ($2^{128}$ ó 340 sextillones) direcciones —cerca de 4,3 × $10^{20}$ (430 trillones) direcciones por cada pulgada cuadrada (6,7 × $10^{17}$ ó 670 mil billones direcciones/$mm^2$) de la superficie de La Tierra.

Esto hace que:

- Desaparezcan los problemas de direccionamiento del Ipv4 actual.
- No sean necesarias técnicas como el NAT para proporcionar conectividad a todos los ordenadores/dispositivos de nuestra red.

**Tabla 1. Características y Diferencias de Ipv6 e Ipv4**

| | IPV6 | IPV4 | | IPV6 | IPV4 |
|---|---|---|---|---|---|
| CARACTERISTICAS | Tiene un espacio de direcciones infinito | Escasez de direcciones IP | DIFERENCIAS | Lanzada en 1999 | Lanzada en 1981 |
| | Arquitectura de jerarquía de direcciones | Soporte inadecuado de aplicaciones | | El tamaño de direcciones es de 128 bits | El tamaño de direcciones es de 32 bits |
| | Autoconfiguración de equipos | Difícil adecuar nuevas aplicaciones | | La formación de direcciones es hexagesima | La formación de direcciones es decimal |
| | Computación móvil | Necesita utilizar NAT | | La cantidad de direcciones es de $2^{128}$ esto equivale a 16 trillones de direcciones | La cantidad de direcciones es de $2^{32}$ esto equivale a 4 mil millones de direcciones |
| | Seguridad de datos<br>Calidad de servicios QoS<br>Soporte a trafico en tiempo real<br>Aplicaciones multicast y anycast | No es seguro | | | |

Hoy en día en las universidades ya se realizan experimentos de implementación de Ipv6 bajo protocolo de encaminamiento de información de nueva generación con el fin de preparar la llegada paulatina de esta versión, en universidades como los andes; la Universidad Industrial de Santander con proyectos de transición, las Unidades Tecnológicas de Santander entre otras. En Colombia se puede decir que ya se está realizando transiciones de este tipo, hay convocatorias para realizar conversiones de sus redes a este nuevo protocolo como en la Superintendencia Financiera de Colombia, las empresas municipales de Cali (Emcali), entre otras. Por lo que ya hay trazado antecedentes sobre esta etapa de implementación, lo que constituye un reto el dejarlo plasmado este estudio.

# 3. PROTOCOLO RIPNG - PROTOCOLO DE INFORMACIÓN DE ENCAMINAMIENTO, NUEVA GENERACIÓN

En este capítulo se presenta el estudio realizado al protocolo RIPng; donde se describe su origen, características, generalidades, modo de operación, ventajas y desventajas de su implementación.

## 3.1 ORIGEN

El origen de RIPng data desde el inicio del Protocolo de Información de Encaminamiento (RIP), de ahí que su historia inicie desde los principios del estándar RFC 1058.

Debido al incremento de muchos nodos en un grupo de redes y de tener enlaces con otros grupos con intereses parecidos la gestión de las rutas entre las diferentes redes se volvió muy compleja fue así que en junio de 1988 en la Universidad de Rutger, New Jersey, Charles Hedric crea un protocolo que permite a los enrutadores determinar con qué red pueden comunicarse y lo lejos que están esas redes. (ARPANET utilizó RIP como su algoritmo de encaminamiento inicial) y luego lo documentó en el RFC 1058, donde se describe un protocolo para el intercambio de información de enrutamiento entre puentes y otras máquinas.

Aunque su creación se considera que inicia mucho antes en el año 1969 cuando se utilizó el software basado en algoritmo vector distancia llamado Bellman-Ford

Algoritmo, donde Richard Bellman desarrolló la ecuación utilizada como base de programación dinámica y Lestor R. Ford Jr., el principio de trabajo en la zona. Este algoritmo es utilizado actualmente para realizar el enrutamiento por RIP en sus tres versiones. RIP ver 1; RIP ver 2; RIPNG.

En 1981 se considera que RIP evoluciona de un protocolo anterior desarrollado por Xerox (Red de Investigación y desarrollo) llamado protocolo GWINFO considerado el surgimiento de RIP y en 1982 se implementa como Routed en BSD donde RIP se basa en el programa de ordenador “Routed”, que se distribuyó ampliamente con el 4,3 Unix de Berkeley Software Distribution del sistema operativo de ahí sus siglas (BSD). Algunos creen RIP fue diseñado en la Universidad de Berkeley en California debido a que desde este momento se popularizó y se convirtió en la norma de hecho para el encaminamiento en laboratorios de investigación, apoyado por los proveedores de puentes debido a que viaja en UDP de la pila de protocolos TCP/IP, (inicialmente no fue diseñado para redes de área amplia).

El protocolo utilizado a nivel de red era PUP (Parc Universal Packet) que evolucionaría hasta convertirse en el que luego fue XNS (Xerox Network System) de Xerox PUP antecesor de IPX (Netware de Novell), son los dos protocolos de encaminamiento en los que RIP se basa para realizar sus rutas a demás es muy usado debido a que su código está añadido en el código de encaminamiento del BSD UNIX que constituye la base para muchas implementaciones de UNIX.

RIP hace parte de la familia de protocolos IGP (Interior Gateway Protocolos) protocolos de gateway interior para redes de área local y redes WAN, y proporciona gran estabilidad en la red, garantizando que si una conexión de red se cae la red puede adaptarse rápidamente a enviar paquetes a través de otra conexión.

El primer protocolo utilizado por RIP es el protocolo PUP (RIP v1- más adelante se describe), utiliza el Protocolo Portal de Información, para el intercambio de información de enrutamiento, y fue desarrollado por un equipo que incluía RM Metcalfe[1], quien más tarde desarrolló el Ethernet, capa física del protocolo de red. El protocolo PUP fue ascendido a apoyar la red de Sistemas Xerox (XNS), la arquitectura y hoy llamado RIP.

En 1986 NSFNet (Nacional Science Foundation Net) Router PDP-11[2] utilizó RIP como protocolo de encaminamiento de información. En 1988 Se abre el mercado de los routers Proteon, ACC y Cisco, en el 2004 Open BSD incorpora BGPD, 2005 Se crea el proyecto Open BGPD[3] por Federico Biancuzzi, 2006 Se optimiza RIPng es el soporte de RIP para IPV6 documentado en RFC 2080. Y en 2006 se anuncia Open RIPD.

En sus 3 principales versiones RIP evolucionó como el protocolo de enrutamiento más utilizado de Internet.

RIP v1- Routing Information Protocol version 1. Es un protocolo estándar su arquitectura se describe en la RFC 1058. Se basa en los protocolos de encaminamiento PUP y XNS de Xerox PUP. Esta versión no soporta subredes ni CIDR (Classless Inter-Domain Routing) Encaminamiento entre sin Clase, tampoco incluye ningún mecanismo de autenticación de los mensajes. Actualmente no es muy usado.

[1] Dr. Robert M. ("Bob"). contribuyó a que Internet diera sus primeros pasos, inventó Ethernet, el estándar internacional para redes de área local.
[2] La PDP-11 fabricado por la empresa Digital Equipment Corp., en las décadas de 1970 y 1980. Fue la primera minicomputadora en interconectar todos los elementos del sistema
[3] Border Gateway Protocol , Protocolo de Pasarela Fronteriza

RIP v2- Routing information Protocol versión 2. Es la actualización de RIP v1, se describe en la RFC1723 de Noviembre de 1994 realizada por Malkin G. Es fácil la implementación y de menores factores de carga que RIP v1 y soporta subredes, permitiendo una mayor flexibilidad al dividir rangos de direcciones IP y VLSM (variable length subnet mask) máscaras de subred de tamaño variable que representa una de las soluciones que se implementaron para el agotamiento de direcciones IP permitiendo la división en subredes.

Soporta autenticación utilizando uno de los siguientes mecanismos: autenticación mediante contraseña, autenticación mediante contraseña codificada mediante MD5 (desarrollado por Ronal Rivest).

RIPng - (Routing Information Protocol next generation). Es la última versión de RIP realizada para el protocolo de Internet versión 6 denominada protocolo de encaminamiento de información de nueva generación. Este protocolo le permite a los enrutadores intercambiar información para conmutar rutas a través de una red basada en IPV6. Cada enrutador que implementa RIPng tiene una tabla de enrutamiento con una entrada para cada destino IPV6 alcanzable. Cada entrada contiene: el prefijo ipv6 del destino, una medida que indica el costo total de obtener un datagrama desde el enrutador hasta el destino, la dirección Ipv6 del próximo enrutador en el camino al destino llamado siguiente salto (hop), una bandera de cambio enrutador que indica si la información acerca de esa ruta ha cambiado recientemente y timers o relojes que apunte la transmisión de la información de la tabla de enrutamiento a los enrutadores vecinos. Más adelante se amplía el funcionamiento de RIPng con mayor profundidad.

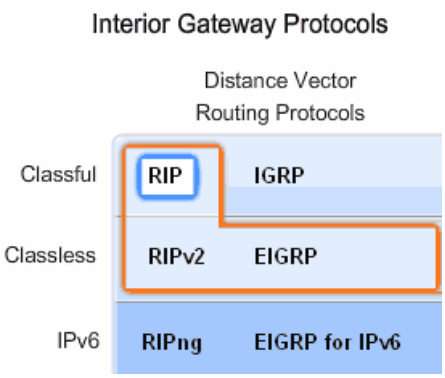



**Figura 1. Protocolos de Gateway Interior por Vector distancia**

Extraído de http://www.bitsfighter.com/2008_04_13_archive.html

En la figura 1 están graficados algunos de los protocolos de pasarela interior que utilizan el método vector distancia, a continuación se describen:

IGRP (Interior Gateway Routing Protocol), o Protocolo de enrutamiento de gateway interior basado en vector distancia y también tiene en cuenta el estado del enlace, al igual que RIP es un protocolo con clase (classfull), no se puede manipular las mascaras de la red. Desarrollado por CISCO System.

EIGRP (Enchaced Interior Gateway Routing Protocol), protocolo de enrutamiento de gateway interior mejorado es considerado un protocolo avanzado por lo que ofrece lo mejor de los algoritmos vector distancia y estado del enlace. Al igual que Ripv2 es un protocolo sin clase. También es de propiedad de CISCO System.

EIGRP para IPV6. (Enchaced Interior Gateway Routing Protocol), protocolo de enrutamiento de gateway interior mejorado para el Protocolo de Internet versión 6.

Otros protocolos que utilizan versiones modificadas de RIP, es el protocolo Apple Talk Routing Table Maintenance Protocol (RTMP)[4] y el Banyan VINES Routing Table Protocol (RTP)[5], están basados en una versión del protocolo de encaminamiento RIP.

La historia y desarrollo del protocolo de encaminamiento de información RIP ha dejado de manifiesto su evolución en el tiempo por sus autores en las siguientes referencias.

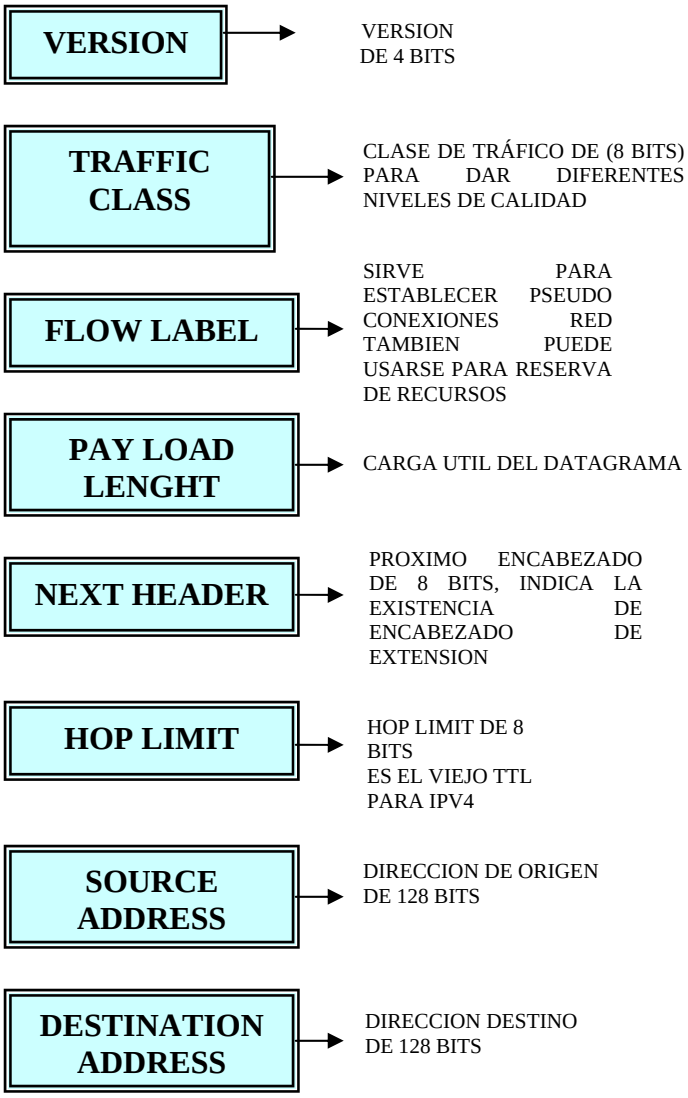
RFC 1058; Hedrick, C.; RIP; Junio 1988
RFC 1388; Malkin, G. RIP versión 2, con información adicional; Enero 1993
RFC 1723; Malkin, G. RIP versión 2, con información adicional; Noviembre 1994
RFC 2453; Malkin, G. RIP versión 2, de Noviembre de 1998, Internet Norma 56
RFC 2080; Grupo de Trabajo de la Red de G. Malkin, RIPng para Ipv6, Enero de 1997.

## 3.2 GENERALIDADES

En Ipv6 se adoptaron los mismos protocolos de enrutamiento ya existentes en las redes Ipv4 por lo cual los principios de funcionamiento son los mismos, la diferencia radica en los parámetros que se utilizan para soportar el protocolo de Internet versión 6. Lo que quiere decir que RIPng (Routing Information Protocol next generation) es el soporte del protocolo RIP para el protocolo de Internet versión 6 (Ipv6).

A continuación se grafica el manejo de las cabeceras Ipv6:

[4] RTMP (routing table maintenance protocol**):** un protocolo de comunicación usado por AppleTalk para garantizar que todos los routers de la red tengan información coherente de enrutamiento
[5] RTP (Real Time Transport Protocol) utilizado para transportar los datos multimedia (es el que realmente lleva "las imágenes del video")




Para entrar a comprender el funcionamiento del protocolo de enrutamiento de información de nueva generación hay que tener en cuenta algunas generalidades en donde se desarrolla RIP.

Las redes están compuestas como una colección de Sistemas Autónomos (AS), los AS son modelos jerárquicos de enrutamiento, donde un conjunto de redes y dispositivos se encuentran administrados por una sola entidad o autoridad con una política común: definición de trayectorias para Internet. Los protocolos de

gateway están definidos dependiendo si éstos se usan dentro o fuera de los sistemas autónomos. Los protocolos de gateway interior permiten el intercambio de información dentro de los sistemas autónomos, y los protocolos de gateway exterior entre sistemas autónomos. Por ejemplo ver figura 2 donde se visualiza gráficamente la forma en que están divididos los protocolos de enrutamiento de gateway interior (IGP) y de gateway exterior (EGP) intercambiando el tráfico de Internet que va de una red a otra. Su función se basa en realizar gestión del tráfico que fluye en él SA1 y los demás sistemas autónomos que forman la gran red de redes Internet.

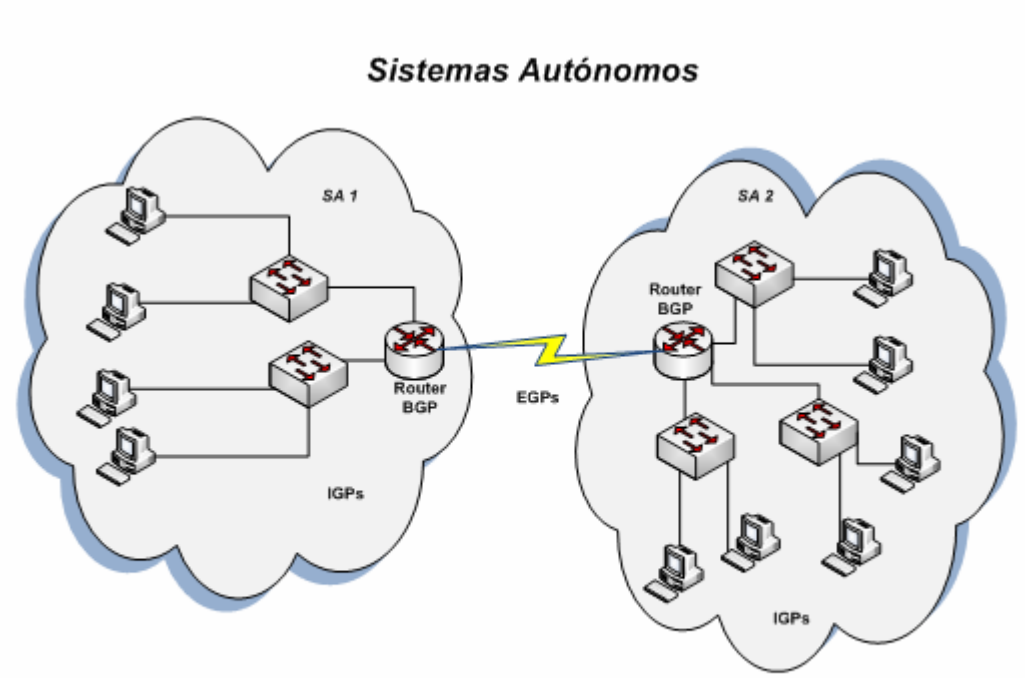



**Figura 2. Sistemas Autónomos – IGP - EGPs**

Los protocolos de enrutamiento dinámico se dividen en dos grupos: IGP protocolos de gateway interior los cuales encuentran entre otros y los más utilizados el Protocolo de Enrutamiento de Información RIP y el protocolo IGRP (interior Gateway Routing Protocol) es un protocolo de enrutamiento de gateway interior desarrollado por Cisco, en ambos se trabaja con el algoritmo vector

distancia. El otro protocolo utilizado en IGP es el protocolo Open Shortest Path First (OSPF) que es de estado de enlace y se caracteriza por primero la ruta más corta.

El segundo grupo de SA son los protocolos de enrutamiento EGP (Exterior Gateway Protocols) que traducido al español significa Protocolo de gateway Exterior, su función principal es la de intercambiar información de enrutamiento con otros sistemas autónomos, incluyendo los datos en la lista de los sistemas autónomos, el que más prevalece es BGP-4 Border Gateway Protocol versión4.

Ripv6 fue diseñado para trabajar como un Sistema Autónomo IGP o sea para redes pequeñas, el tipo de enrutamiento que puede utilizar es dinámico en donde las rutas van a ser aprendidas automáticamente por el router. Los elementos de enrutamiento que utiliza son; el router no conoce la topología de la red solo la ve desde la perspectiva de sus vecinos RIP, para determinar la ruta óptima y finalmente el paquete se coloca en la interfaz de salida de esa ruta.

### 3.2.1 CÓMO OPERA RIPng?

RIPng se basa en el intercambio de información entre Routers, de forma que puedan calcular las rutas más adecuadas, de forma automática.

Ripng sólo puede ser implementado en routers, donde requiera la métrica entre 1 y 15 saltos, lo que quiere decir que son 15 saltos los que cada paquete ha de emplear como límite para llegar a determinado destino. Cada salto supone un cambio de red, por lo general atravesando un nuevo router. Además de la métrica, cada red tendrá un prefijo de dirección destino y la longitud del propio prefijo. Estos parámetros han de ser configurados por el administrador de la red. Su distancia administrativa (DA) es de 120.

**Tabla 2. Distancia Administrativa**

| Protocolo | Distancia Administrativa |
|---|---|
| INTERFAZ | 0 |
| RUTA ESTATICA | 1 |
| EIGRP INTERNO | 90 |
| IGRP | 100 |
| OSPF | 110 |
| IS – IS | 115 |
| RIP | 120 |
| EIGRP EXTERNO | 170 |
| INALCANZABLE | 255 |

La distancia administrativa es la usada por los enrutadores Cisco para seleccionar la mejor ruta cuando hay dos o más rutas distintas hacia un mismo destino. Como se observa en la tabla 2, anteriormente descrita, rip no posee la mejor de las distancias administrativas, ya que a menor sea la distancia administrativa más fiable es la ruta, aun así rip sigue utilizándose por su sencillez.

Cada router que implementa RIPng asume tener una tabla de enrutamiento que tiene una entrada para cada destino ipv6 alcanzable. Cada entrada debe contener;

El prefijo ipv6 del destino

Una medida que indica el costo total de obtener un datagrama desde el router inicial hasta el router destino.

La dirección ipv6 del próximo router en el camino al destino, llamado el siguiente salto (hop).

Un Router Change Flag que indica si la información acerca de esa ruta ha cambiado recientemente.

Varios relojes (timers), como un reloj de 30 segundos que apunte la transmisión de la información de la tabla de enrutamiento a los routers vecinos.

### 3.2.1.1 FORMATO DE PAQUETE DE RIPng.

El paquete RIPng incluye 3 campos; Command (Request o Response), versión (1) y Route Table Entry (RTE). Ver figura 3-A.

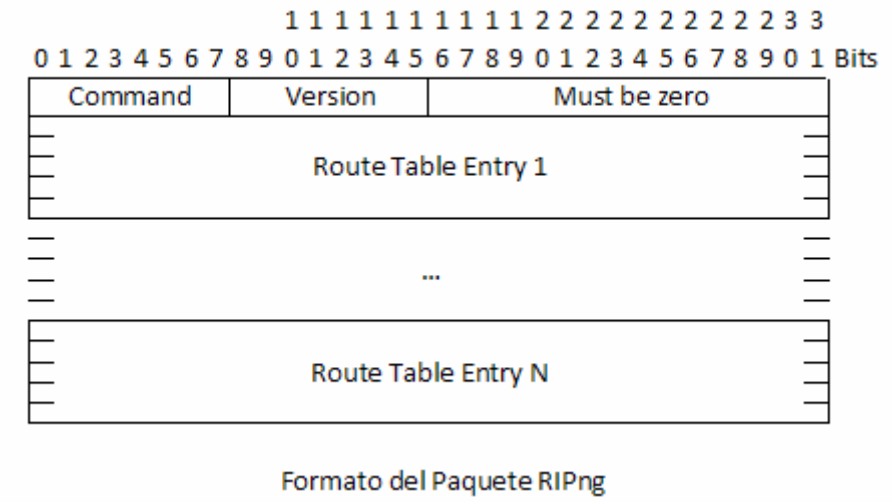



**Figura 3. Formato del paquete RIPng**

**El campo de command (comando):** Es de 8 Bits donde se presentan dos estados:

**1 es la solicitud.** A petición de la respuesta del sistema para enviar la totalidad o parte de su tabla de enrutamiento.

**2 es respuesta**. Es el mensaje que contiene la totalidad o parte del remitente de la tabla de enrutamiento. Este mensaje puede ser enviado en respuesta a una petición o actualización de enrutamiento no solicitado generado por el remitente.

**Campo versión: De** 8 bits

**Route Table Entry (RTE):** Ruta de entrada es de 20 bytes o número de registros. Son una serie de registros de entrada de la ruta. Cada RTE incluye el prefijo IPv6, el Route Tag o Ruta de etiquetas de 16 bits (para separar rutas internas de las externas), un campo Prefix Length, Longitud de prefijo, de 8 bits, para determinar el número de bits significantes en el prefijo, y Metric que es la métrica de 8 bits, para definir la medida corriente para el destino ver Figura 3-B

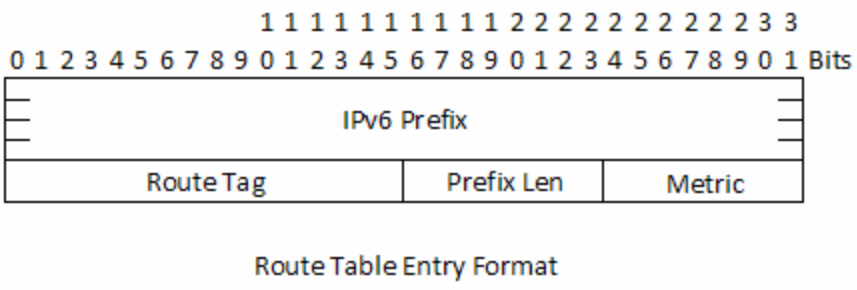



**Figura 4. Formato de la Tabla de Rutas de Entrada**

RIPng también puede especificar el próximo salto inmediato de dirección ipv6 para paquetes. El próximo salto está especificado por un RTE especial, The Next Hop Route Table Entry. Nex Hop RTE está identificado por el valor de FFH en el campo Metric. El campo Prefix especifica la dirección ipv6 del próximo salto M

Route Tag y Prefix Length son configurados a cero en la transmisión e ignorados en la recepción. Ver figura 3- C

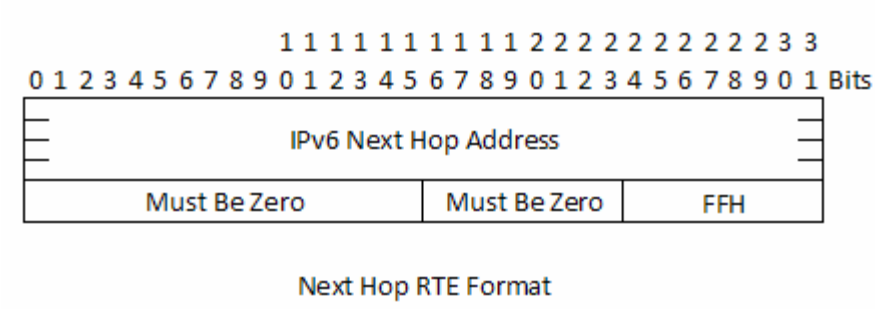



**Figura 5. Formato del Próximo Salto RTE**

En la mayoría de los casos, los Request son enviados como multicast desde el puerto RIPNG 521. Si la información para solo un router es necesitada, esa solicitud sería enviada directamente a ese router desde un puerto que no sea el puerto 521.

Hay tres (3) tipos de Response; una respuesta a un Query específico; una actualización regular, que es una respuesta no solicitada enviada cada 30 segundos a todos los routers vecinos; y una actualización accionada causada por un cambio de ruta.

En RFC 2080 se detalla específicamente lo concerniente al proceso de paquetes en Request Y Response.

### 3.2.1.2 ALGORITMO VECTOR DISTANCIA

El algoritmo de Vector Distancia es un método de encaminamiento basado en el algoritmo de Bellman-Ford para calcular o propagar las rutas y broadcasting para

la entrega de mensajes. Fue el algoritmo original de ARPANET, se usó en DECNET, IPX[6] y APPLETALK[7], y actualmente utilizado por el protocolo RIP (Routing Information Protocol) y hasta 1988 era el único utilizado en Internet, También se utiliza en los protocolos propietarios IGRP y EIGRP de Cisco.

El enrutamiento requiere que cada router informe a sus vecinos de los cambios en la topología periódicamente y en algunos casos cuando se detecta un cambio en la topología de la red.

Se basa en calcular la dirección y la distancia hasta cualquier enlace en la red. El costo de alcanzar un destino se lleva a cabo usando cálculos matemáticos como la métrica del camino. RIPng cuenta los saltos efectuados hasta llegar al destino mientas que IGRP utiliza otra información como el retardo y el ancho de banda.

Se debe mantener los cambios detectados periódicamente ya que la tabla de enrutamiento de cada router se envía a todos los vecinos que usan un mismo protocolo y una vez que el router tiene toda la información, actualiza su propia tabla reflejando los cambios y luego informa a sus vecinos de los mismos cambios. Este proceso se conoce como “enrutamiento por rumor” ya que los nodos utilizan la información de sus vecinos y no pueden comprobar a ciencia cierta si ésta es verdadera o no.

El algoritmo de vector distancia se adapta al modo de aprendizaje de los nodos que “nacen”, es decir, cuando se conectan a la red. A medida que el algoritmo progresa, el nuevo nodo va adquiriendo más información sobre el resto de nodos de la red. Este algoritmo converge rápidamente cuando se conectan nuevos nodos.

[6] Siglas de Internet Packet Exchange ( intercambio de paquetes interred)
[7] Appletalk es un conjunto de protocolos desarrollados por Apple Inc. Para la conexión de redes.

Este algoritmo implica que cada router mantenga en su tabla de enrutamiento la distancia, en saltos, que lo separa de cada destino. Cuando un router X recibe de un vecino Y su vector de distancias, actualiza la entrada de su tabla de enrutamiento correspondiente. A continuación en la gráfica 1. publicación de redes de los vecinos. Se explica la publicación de las redes existentes a los vecinos. Y en el gráfico 2 se gráfica la actualización de las tablas en los router cercanos o vecinos.

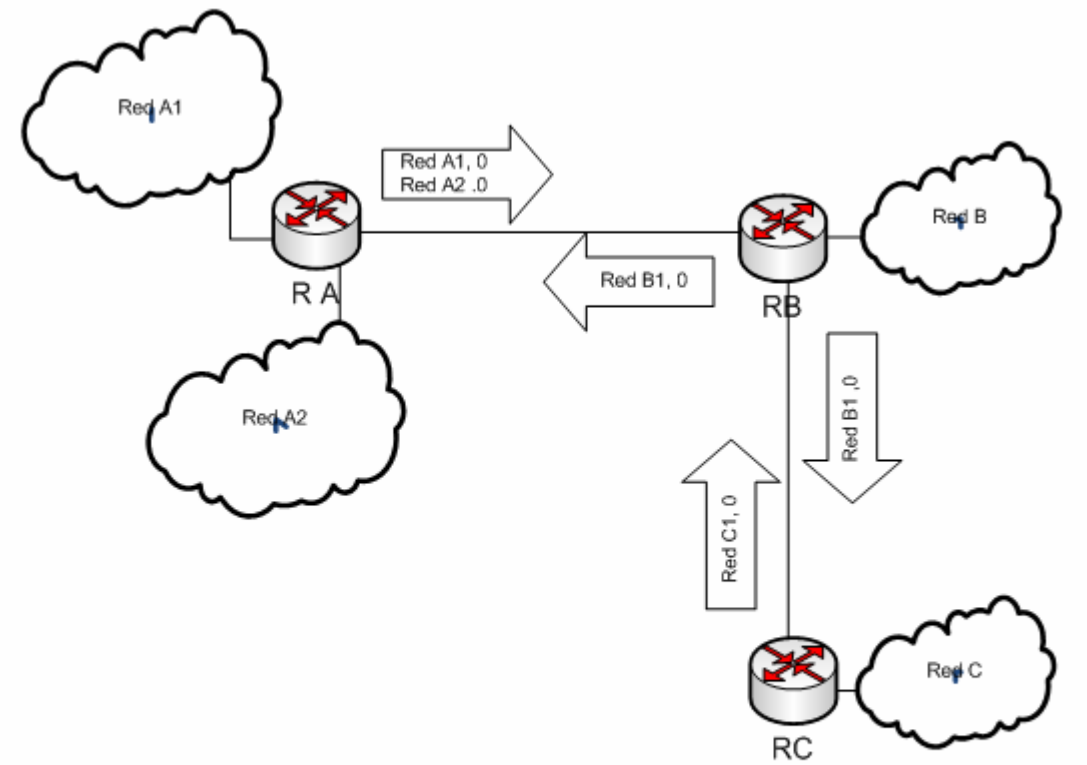



Grafico 1. Anunciación de Redes a los Vecinos

Cada entrutador de la red envía información sobre cada una de sus redes a sus vecinos.

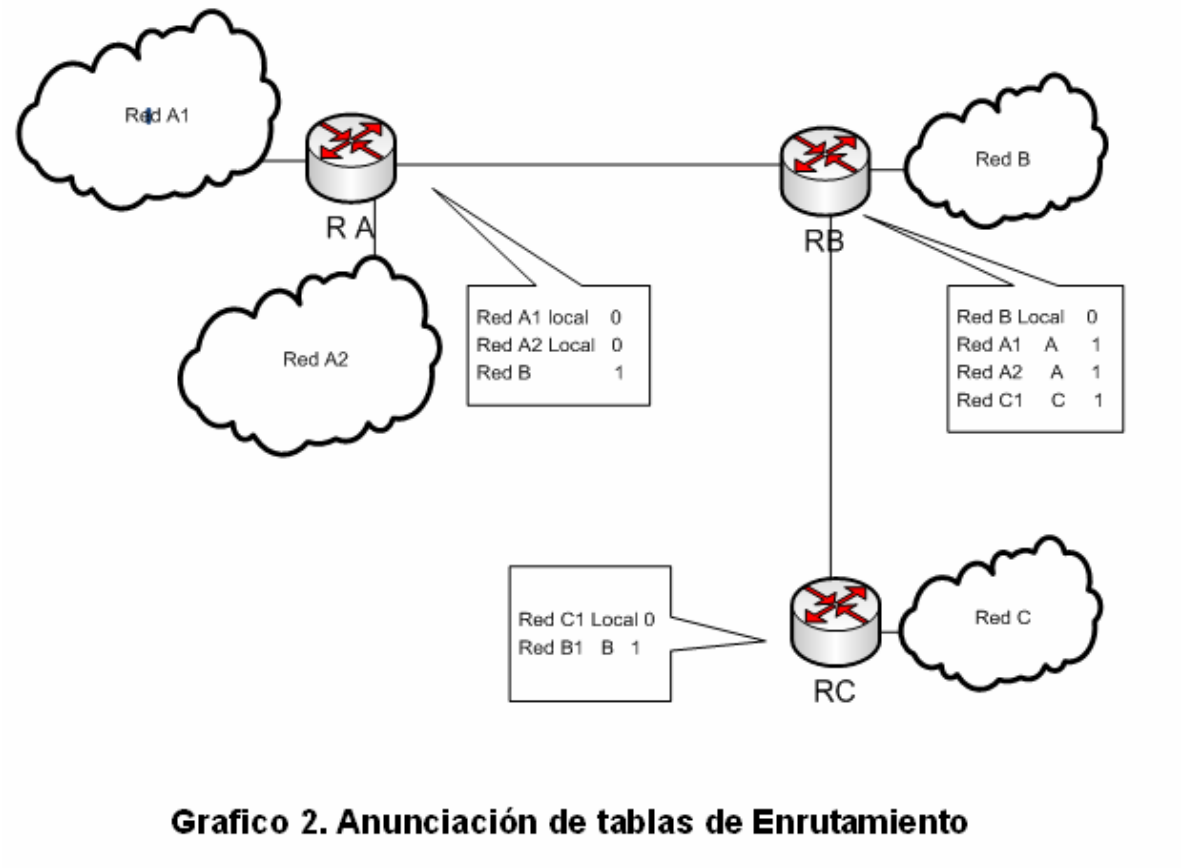



**Grafico 2. Anunciación de tablas de Enrutamiento**

Una vez recibida la información cada router actualiza su tabla de enrutamiento donde constan las redes propias de cada router y las redes de los router vecinos

### 3.3 CARACTERÍSTICAS.

RIPng es una implementación del algoritmo de enrutamiento por vector distancia para redes LAN con IPV6 y utiliza UDP (User Datragram Protocol) protocolo de transporte diseñado para redes de tamaño moderado, permite el envío de datagramas sin haber establecido previamente una conexión, debido a que el propio datagrama incorpora previamente suficiente información de

direccionamiento en su cabecera,  con el número de puerto UDP 520 como puerto de destino.

RIPng específica tres tipos de paquetes: de petición y respuesta y Router Table Entry (RTE). Un paquete de petición, es enviado por los enrutadores a sus vecinos solicitándoles que envíen sus tablas de vector distancia, se dividen en dos (2);

- Mensajes de información de enrutamiento.
- Mensajes utilizados para solicitar información.

El paquete de respuesta, es enviado por los enrutadores para anunciar su tabla; esto se hace en las siguientes condiciones:

- Mensajes ordinarios: Cada 30 segundos indicando que el enlace sigue activo.
- Mensajes de respuesta: Corresponden a la respuesta a una petición
- Mensajes si cambió algún costo: Emitidos cuando las tablas de vector distancia cambian, ya sea un cambio en la métrica del enlace o si las rutas han cambiado.

Como es un protocolo diseñado para redes de tamaño moderado sólo puede ser implementado en enrutadores, donde requiera como métrica o número de saltos entre 1 a 15 saltos.

Depende de un proceso llamado “conteo hacia el infinito” para resolver ciertas situaciones, como loops de enrutamiento. Puede consumir una gran cantidad de ancho de banda de red cuando realiza este proceso antes de resolverlo.

El protocolo depende de medidas fijas para comparar rutas alternas, sin importar los parámetros en tiempo real como tardanza, confiabilidad o carga.

RIPng permite a los routers intercambiar información para computar rutas a través de una red basada en ipv6.

Las rutas que RIP aprende de otros enrutadores expiran a menos que se vuelvan a difundir en 180 segundos (6 ciclos broadcast). Cuando una ruta expira, su métrica se pone a infinito, la invalidación de la ruta se difunde a los vecinos, y 60 segundos más tarde, se borra de la tabla.

## 3.4 VENTAJAS Y DESVENTAJAS

RIPNG presenta las mismas ventajas y desventajas que sus antecesores propios de la implementación con UDP.

### VENTAJAS

Es un protocolo de fácil implementación esto quiere decir que es más fácil de configurar, es abierto, estándar y es soportado por la mayoría de fabricantes.

Por otra parte permite que el cliente envíe peticiones a puertas de enlace remotas, es decir, puerta de enlace que no está conectado a la misma red del cliente.

### DESVENTAJAS

Las desventajas de RIPNG son expuestas en RFC 2080 en el numeral 1.2 Limitaciones del protocolo. En resumen contempla la posibilidad de pérdida de paquetes, duplicación de paquetes, retrasos de mensajes o entrega en desorden de los paquetes, pérdida de conectividad, a razón de que los mensajes de actualización de enrutamiento se difunden lentamente a través de la red debido a

un problema del algoritmo denominado “convergencia lenta” o conteo al infinito, por tal motivo se ha seleccionado el salto 16 como tope máximo de saltos para ayudar a limitar la convergencia lenta pero esto no significa que no se presente. Aunque se considera que su gran inconveniente es su métrica fija, no varía a razón de otros parámetros como ancho de banda, velocidad, tiempo, retardo, etc, por tal motivo se recomienda para redes pequeñas.

# 4. ANÀLISIS DE ESCENARIOS DE IPV6

Debido a que Ipv6 es la evolución o sucesor de Ipv4, trae consigo algunas incompatibilidades con respecto a la longitud, cambio de formato de la cabecera IP y el modo en que se procesa la información, el motivo de pasar de Ipv4 a Ipv6 no es sencillo, estableciendo en la creación de mecanismos que permitieran la coexistencia entre ellas y la transición entre las dos versiones.

La migración al nuevo IP en corto tiempo y sin un mecanismo de transición requeriría la redefinición de un plan de direccionamiento Ipv6 mundial, la instalación del protocolo en cada router y host del mundo, y la modificación de las aplicaciones actuales para que puedan soportarlo, sin duda requiere de un proceso costoso, y podría causar interrupciones del servicio, por supuesto inaceptables, y sin tener necesidad de pasar por este trance ya que muchas de las aplicaciones hoy por hoy son operativas.

Dentro de las razones por las cuales el grupo NGTrans Trans Workin Group ha propuesto los mecanismos de transición que permitan interconectar redes Ipv4 e Ipv6, es para asegurar la interoperatividad gradual debido a que las empresas y los Prestadores de Servicios de Internet (ISP) no están dispuestos a perder las grandes inversiones realizadas en redes Ipv4 ni mucho menos sus infraestructuras de red actuales. La transición entre ambos es un proceso que debe garantizar la compactibilidad entre ellas, sin generar traumatismo tecnológico, es así que la IETF (Internet Engineering Task Force, en castellano Grupo de Trabajo en Ingeniería de Internet) ha creado este grupo NGT Trans Workin Group. Y este a su vez ha definido las técnicas de transición, debido a que no hay una regla universal que pueda ser aplicada al proceso de transición de Ipv4 a IP v6.

## 4.1 ESCENARIOS DE TRANSICIÓN

### 4.1.1 Doble Pila (Dual Stack)

También denominada la doble pila de protocolos es la forma más lógica de transición debido a que implica el uso simultáneo de ambos protocolos, en pilas separadas y es así como un dispositivo con ambas pilas pueden recibir y enviar tráfico a nodos que sólo soportan uno de los dos protocolos, implicando que el dispositivo tenga una dirección en cada pila, con direcciones IPV4 e Ipv6 relacionadas o sin estar relacionadas. Los DNS (servidor de Nombre de Dominio) tendrán la capacidad de devolver la dirección Ipv4, la dirección Ipv6 o ambas si se requiere. Si se emplea direcciones Ipv4 de 32 bits, se le anteponen 80 bits con valor cero (0) y 16 bits con valor 1, para crear una dirección Ipv6 mapeada desde Ipv4.

Requiere que los hosts y los routers soporten ambas versiones de IP y, por tanto, servicios y aplicaciones en Ipv4 como en Ipv6, siendo un mecanismo fundamental para introducir Ipv6 en las arquitecturas Ipv4 actuales. Su punto débil es que obliga a que cada máquina retenga una dirección Ipv4, de manera que se difunda Ipv6. La técnica de doble pila tendrá que ser aplicada donde específicamente ayuda al proceso de transición, por ejemplo en routers y servidores. Un servidor de doble pila puede soportar clientes sólo Ipv4 convencionales, nuevos clientes Ipv6, y por supuesto clientes de doble pila. Para aquellos casos en que haya insuficientes direcciones Ipv4 se ha definido una combinación modelo de conversión y de doble pila de protocolos, conocida como DSTM (Dual Stack Transition Mechanism), se basa en el uso de Ipv4 mediante túneles 4in6 en la intranet, con un punto final del túnel conocido; proporcionando un método para

asignar temporalmente direcciones Ipv4 dual. Es también una manera de evitar el uso de NAT (Network Address Traslation).

La función de Dual Stack es asegurar la compatibilidad entre nodos al pasar de ipv4 a ipv6 teniendo la habilidad de enviar y recibir paquetes de forma transparente sin tener ningún tipo de problema en su transmisión. Unas de las características importantes de esta técnica es que provee soporte completo para los dos protocolos donde la aplicación debe saber que hay doble pila y de esta forma conocer uso de los registros A y AAAA/A6.

Los registros A son aquellas direcciones de 32 bits utilizadas en Ipv4 por lo que se optó por agregar registros que toleren direcciones de 128 bits, dando origen a los registros AAAA con características idénticas al de los registros A, también fueron creados los A6 con mejores características como registros Ipv6 encadenados.

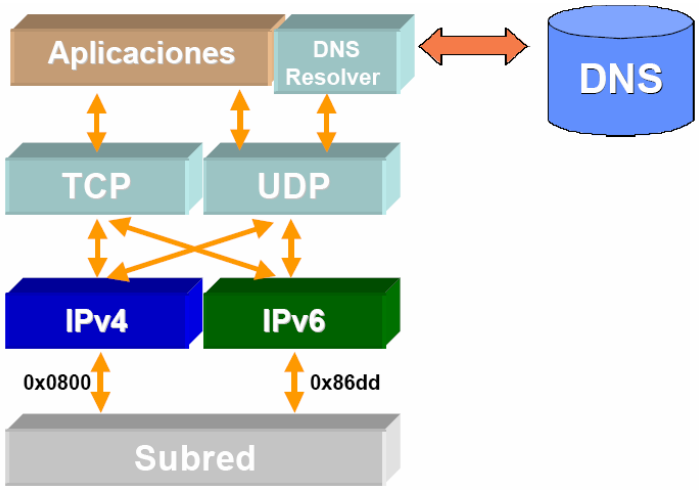



**Figura 6. Nodos Duales**

La figura 6. Visualiza el modo de operación del mecanismo de doble pila [8] . En primera instancia se consulta al Servidor de Nombres de Dominio (DNS) sobre un nombre, en segunda instancia el DNS puede devolver un registro A, un registro AAAA o ambos según se requiera, la aplicación debe saber que hay doble pila, en tercera instancia el resolver del DNS devuelve las respuestas a la aplicación Conecta la dirección v4 o la v6 y en cuarta la aplicación utiliza Ipv6 o Ipv4 dependiendo de las respuesta arrojada. Los nodos duales son como tener doble nivel 3.

En la figura 7. Muestra un escenario Dual Stack que nos permite visualizar el funcionamiento que se presenta en esta técnica.

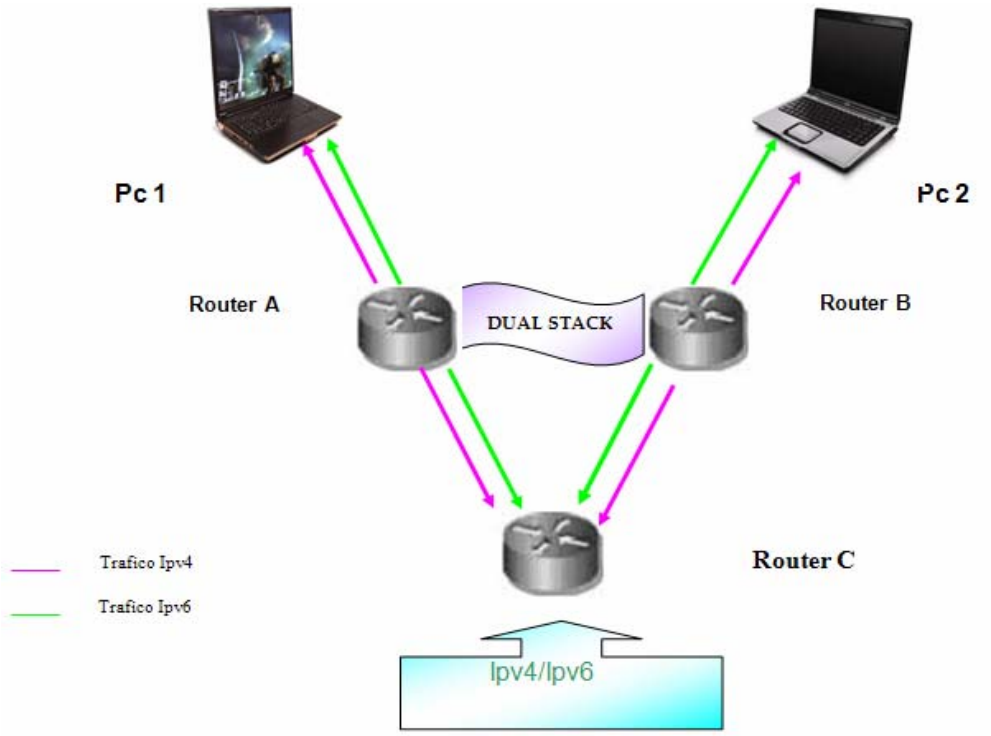



**Figura 7. Dual Stack**

[8] (http://internetng.dit.upm.es/ponencias-jing/2002/fernandez/Evolucion-IPv4-IPv6-David-Fernandez.PDF)

### 4.1.2 Túneles

La tunelización es una forma que se usa para transferir información de un extremo a otro, este se hace encapsulando la información que contiene Ipv6 sobre otro que contiene Ipv4, esta utiliza una red Ipv4 con un nodo de la misma versión cuando llega se encarga de extraerla utilizando el Ipv6, este se maneja a nivel de capa 2, el cual permite conectar plataformas similares a IP, IPX, NETBEUI, estas conexiones son discadas o dedicadas esto permiten al usuario autenticarse.

Veamos como se realiza los tunelización para la transferencia de la información.

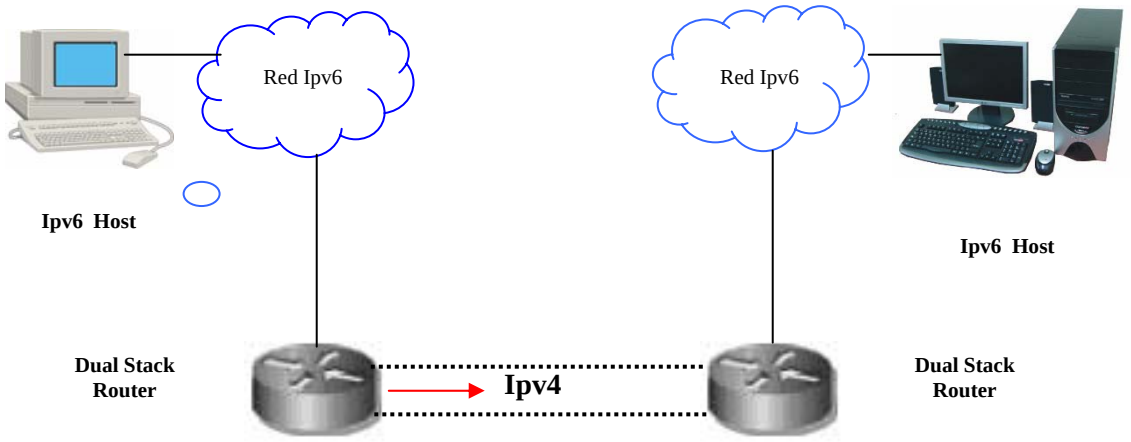



**Figura 8. Tunelización**

Entre la tunelización se manejan los túneles que utiliza el tunneling que es una técnica que facilita el enviar y recibir paquetes y de esta manera aprovecha ciertas propiedades que tienen esta información, el propósito es que el mensaje sea utilizado como si hubiese sido encapsulado.

Los protocolos que manejan los túneles son SNA sobre IP, IPX sobre IP, PPTP, L2TP e IPSEC, pero el más importante es el protocolo SSH (**Secure Shell**) por que es el que se utiliza para tunelizar trafico confidencial sobre Internet de manera segura

El protocolo SSH proporciona las siguientes protecciones:

- Tiene un medio seguro para utilizar aplicaciones graficas sobre una red
- La conexión es segura por que tiene encriptación fuerte, el cual lo hace difícil que se pueda desencriptar cualquier tipo de mensaje que se reciba o se envié.
- Contiene un formato cifrado en cual permite que el cliente se autentique sin tener ningún problema que le puedan cifrar el mensaje.

Es importante mencionar que existen 5 técnicas de tunelización que son las siguientes:

#### 4.1.2.1 Túnel Manual

Es cuando su configuración la hacen los usuarios de forma directa, la función de este Túnel es conectar islas Ipv6 a través de Ipv4, una de las características principales es que cada extremo de un nodo dual se configura las direcciones Ip4 e Ipv6 de forma local o remota.

Ventajas de este sistema:

- Disponible en multitud de plataformas (Cisco, Telebit, Linux, Windows NT, etc)
- Es un nivel totalmente transparente respecto al nivel Ipv6 y superiores, con lo cual no afecta a las aplicaciones.
- No consume excesivos recursos, la MTU se reduce en 20 bytes que es el tamaño típico de una cabecera Ipv4.

- Aplicación Principal: Conexión con ISP Ipv6 remoto a través de Internet.
- Método muy usado para el acceso a redes Ipv6 ya establecidas como 6bone.

Desventajas:

- No son dinámicos, sino que se establecen manualmente o de forma semiautomática.
- Si se unen N islas y la topología no considera unos nodos centrales o intercambiados, el número de túneles a establecer en cada sitio asciende a N-1. En el caso de pensar en la conexión entre sí de miles de islas IPv6 distribuidas por la Internet actual, este método carece de sentido.[3]

En la figura 9. Muestra el funcionamiento de la información utilizando el túnel manual.

.

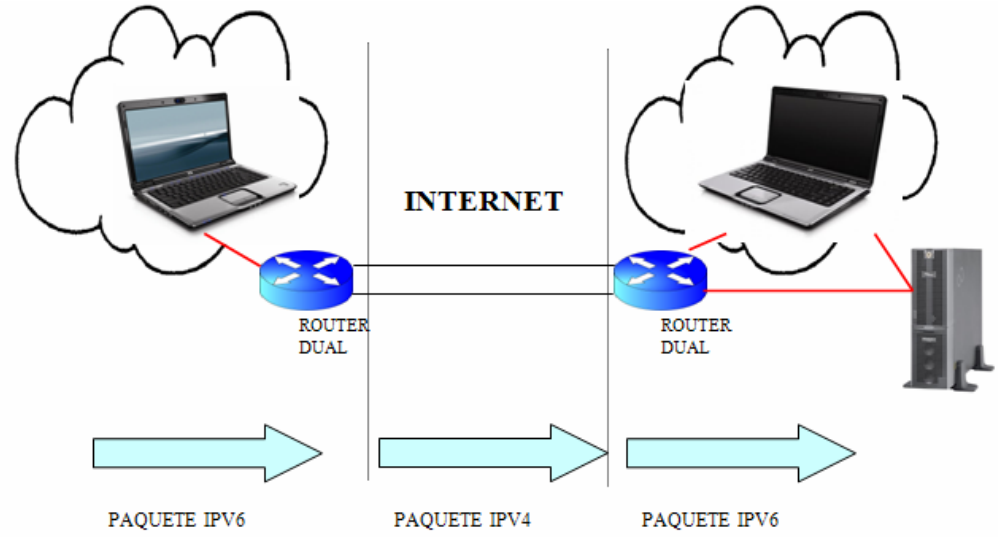



**Figura 9. Túnel Manual**

[3] www.depeca.uah.es/wwwnueva/docencia/ING-TELECO/proyectos/trabajos/grupo4/Ipv6_archivos/image004.gif&imgrefurl=http://www.depeca.uah.es/wwwnueva/docencia/ING-TELECO/proyectos/trabajos/grupo4/Ipv6.htm

#### 4.1.2.2 Túnel Automático 6 to 4

Estos túneles nos permiten ubicar Ipv6 que están aislados, admitiendo una comunicación con el túnel automático a través de la red Ipv4 que no soporta la versión Ipv6.

Las características mas importantes de esta técnica es que tiene direcciones asignadas de Ipv4 que es de forma: a.b.c.d, se establece un túnel automático si es compatible con Ipv4, otra característica es el reenvió de la direcciones ::/96 en una tabla de enrutamiento

Ventajas del Sistema:

- Este túnel es transparentes a nivel de Ipv6, por consiguiente no va tener ningún problema con estas aplicaciones.
- No necesita de ninguna configuración dado que no tiene ningún problema para su implementación.

Desventaja:

- Si se tiene un proveedor de servicios de Internet remoto solo es necesario colocar un único túnel, si es así se puede utilizar la técnica del túnel manual lo cual puede que se deseche la posibilidad de utilizar la técnica del túnel 6to4.

En la figura siguiente nos muestra como proporciona una conectividad entre sitios 6to4.

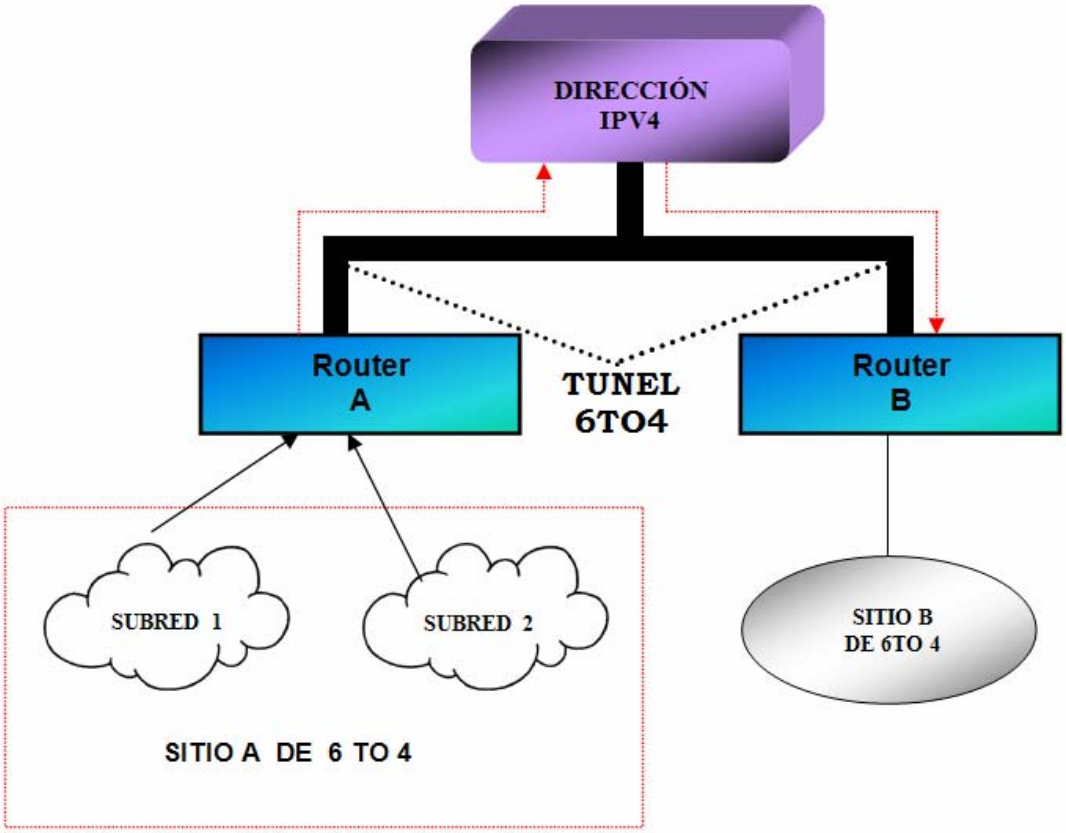



**Figura 10. Túnel Automático**

#### 4.1.2.3 Túnel 6 over 4

Es la forma de favorecer la técnica que maneja Ipv4 en cuanto a su conectividad a través de una infraestructura que soporte multicast utilizando la red Ipv4 como un enlace lógico, este túnel es también denominado túnel de multidifusión; para que esta técnica funcione correctamente tiene que tener una infraestructura Ipv4 habilitada para multidifunsion Ip4.

Unas de las características mas importantes de este túnel es que las direcciones multicast que este maneja se da por el trafico Ipv6 encapsulado entre nodos Ipv4, se forman LAN virtuales de Ipv6 debido a que los nodos se dispersan en las subredes de Ipv4.

Ventajas del sistema:

- En una red corporativa permite utilizar Ipv6 en algunos nodos de Ip4, sin tener ningún conflicto entre los routers internos.
- Conectando 6-Bone a un router Ipv6 proporciona información a toda la red sin tener ningún inconveniente con el tráfico.
- Este túnel tiene ventajas similares a los de los otros túneles.

Desventajas:

- Es una técnica que adecuada para redes finales.
- Esta en prueba de implementación ya que es una de las técnicas que no son usadas comúnmente.

La figura nos muestra el proceso de conectividad con el túnel 6over4.

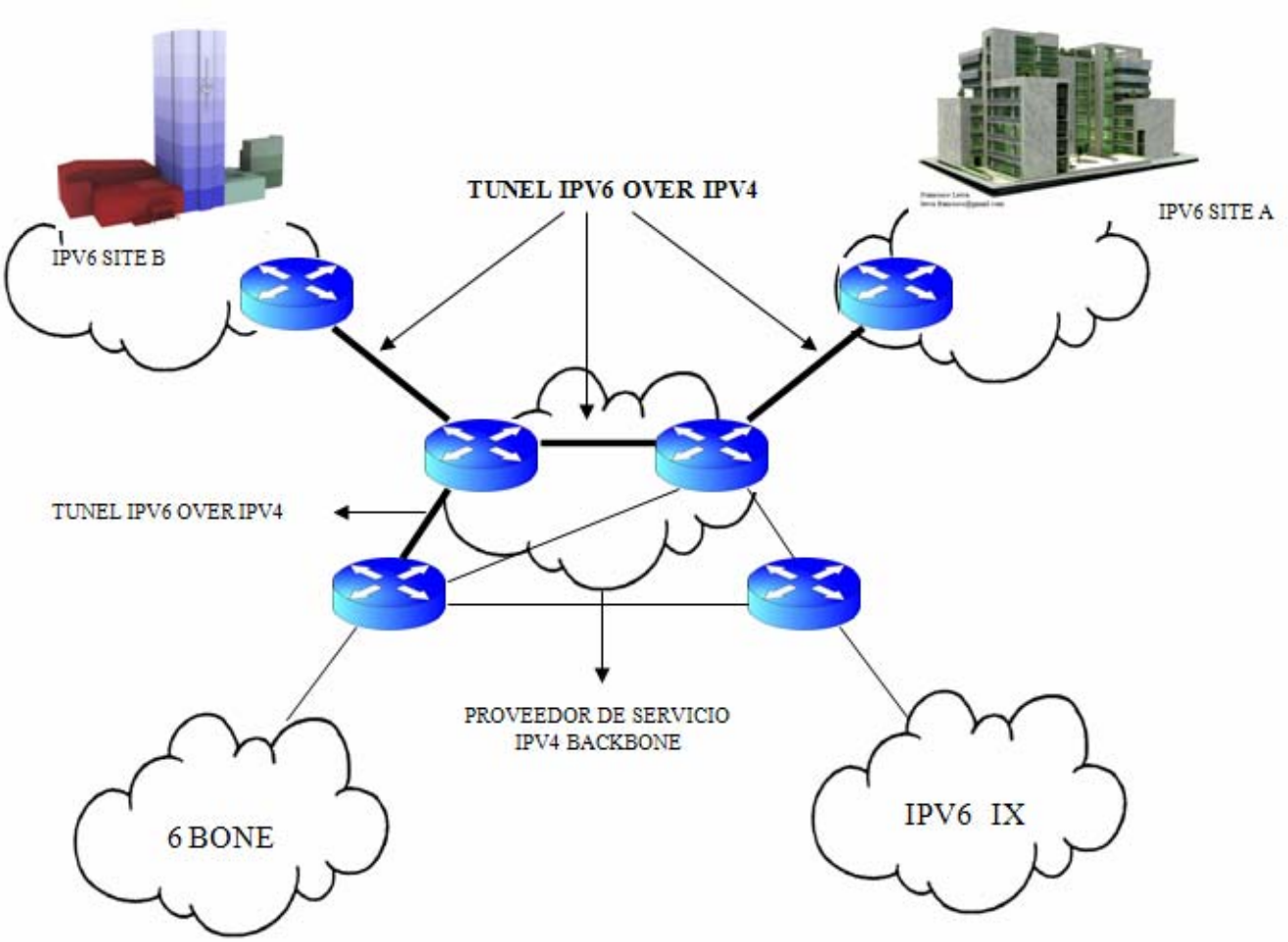



**Figura 11. Túnel 6over4**

#### 4.1.2.4 Túnel Broker

Es una técnica que el usuario tiene para configurar manualmente los extremos de los túneles, este túnel actúa como servidor por que recibe peticiones de otros nodos.

Una de las características más importantes es que en el servidor genera info. (Script) a clientes, donde el cliente se registra en el Tbroker es como decir que es el http. El Tbroker se comunica con Tserver el cual configura el lado del servidor y al Servidor de nombre de dominio, con esto el cliente configura el túnel el mismo.

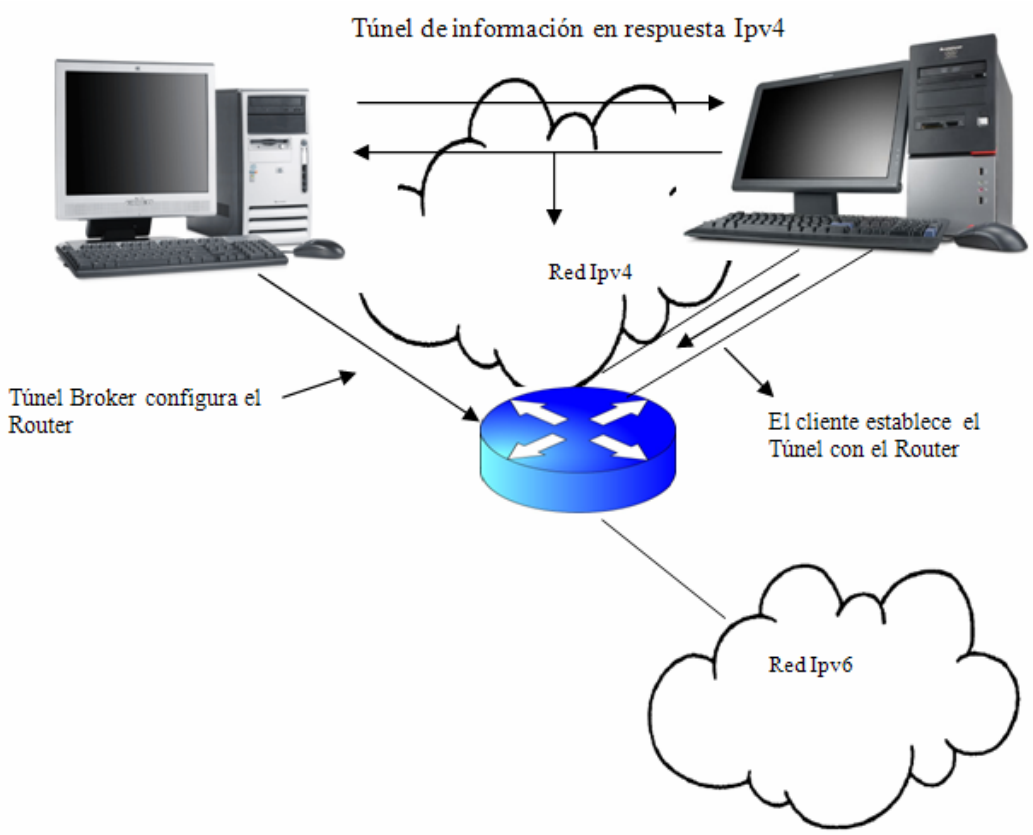



**Figura 12. Túnel Broker**

# 5. MECANISMO DE TRADUCCIÓN

Como su palabra lo indica es el que se encarga de traducir un sistema Ipv4 a un sistema Ipv6.

Existen 4 técnicas de traducción que son las siguientes:

## 5.1 SIIT (Stateless IP/ICMP Translation)

Es una técnica que nos permite tomar un paquete Ipv4 y pasarlo a un paquete Ipv6, el nodo Ipv6 se comunica con el otro nodo Ipv4 por medio de un traductor que asigna direcciones en pares.

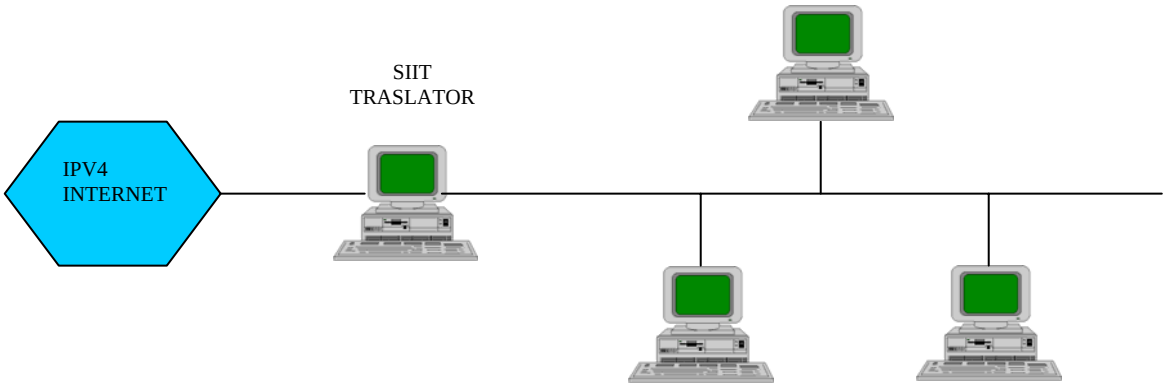



**Figura 13. Técnica De Traducción SIIT**

## 5.2 APLICATION LEVEL GATEWAY

Una aplicación de puerta de enlace proporciona características similares a la de un Proxy, éste realiza un análisis del paquete, el procedimiento de esta técnica es examinar y evaluar cuando el paquete llega, el maneja un sistema de seguridad que consiste en revisar las tramas y de esta manera permitir el paso a la red interna.

Unos de los protocolos que maneja la aplicación de puerta de enlace es el Telnet, FTP (File Transfer Protocol), HTTP (Hypertext Transfer Protocol) y SMTP (Simple Mail Transfer Protocol), cuando se trabaja a nivel de proxis la seguridad tiende a ser potente o flexible dependiendo del caso, los administradores son los encargados del manejos de los paquetes que llegan a red y a su vez son que permiten manejar los paquetes que llegan a la puerta de enlace.

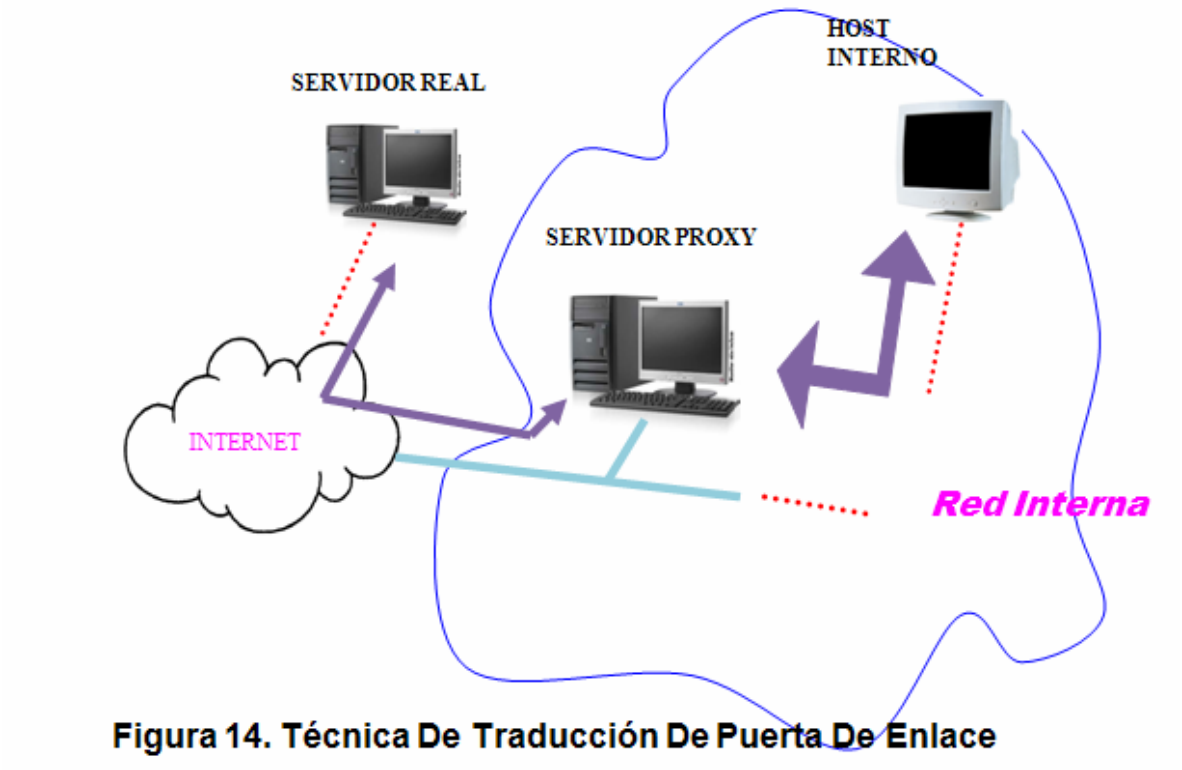



**Figura 14. Técnica De Traducción De Puerta De Enlace**

### 5.3 NAT-PT (Network Address Translation–Protocol Translation)

La comunicación se realiza mediante la utilización de un dispositivo dedicado que hace la traducción entre las direcciones de Ipv4 y Ipv6, se mantiene el estado durante el tiempo del período de sesiones.

La conversión se puede mantener mediante routers y host extremos, estas traducciones se hacen con la cabecera Ipv4 ⟺pv6.

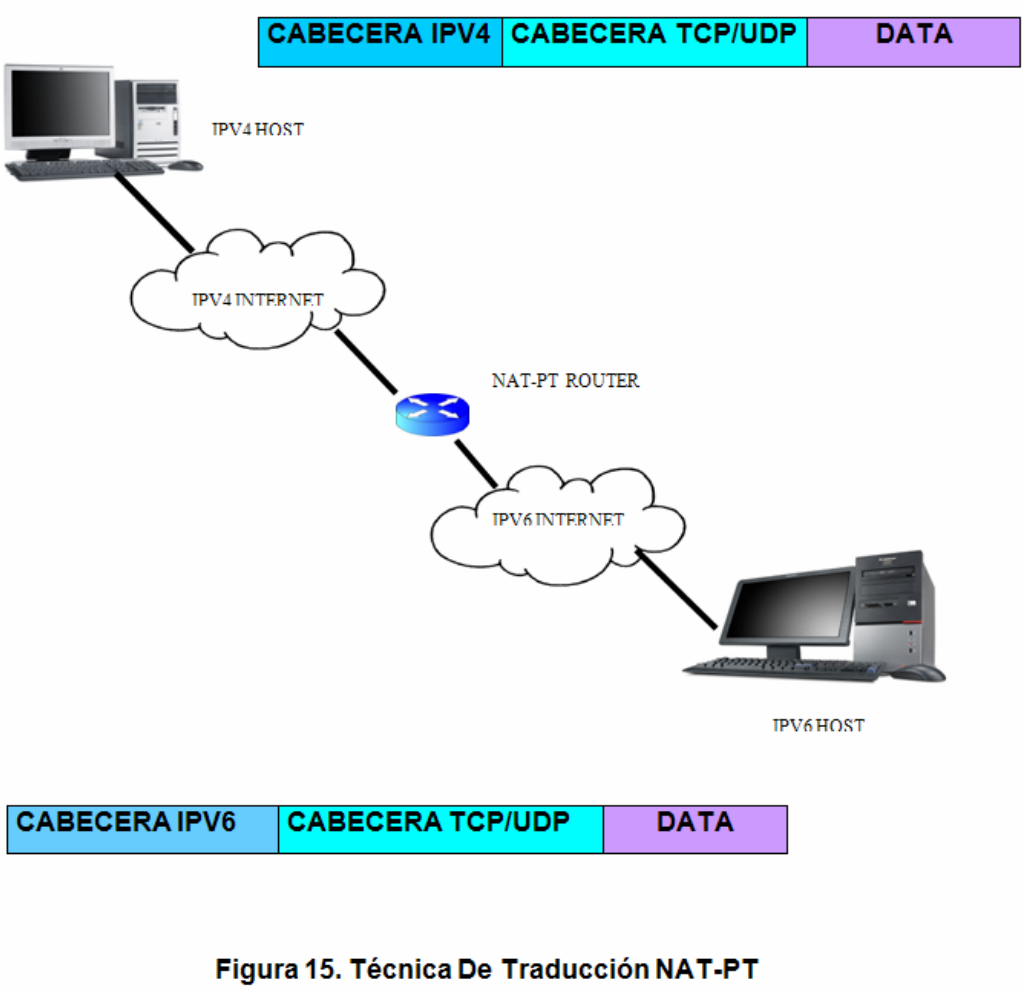



**Figura 15. Técnica De Traducción NAT-PT**

### 5.4 TRT (Transport Relay Translation)

Está definida en RFC 3142 se basa en la traducción entre DNS y registros AAAA-A6 conocida como DNS-ALG (Domain Name Service Aplication Level Gateway), Pasarela DNS de nivel de aplicación, su función es traducir las consultas DNS y está definida en RFC 2694.

Es un sistema que localiza Host Ipv6 - Host Ipv4 y los traduce en TCP-UDP y viceversa, solo para el intercambio de hosts, una maquina haciendo TRT tendrá un rango de direcciones Ipv6 que traducirá a un rango de direcciones Ipv4. Cuando se haga una conexión TCP a alguna dirección, la maquina TRT hará una conexión TCP a la dirección Ipv4 correspondiente en el mismo puerto. Luego los paquetes TCP sean recibidos, la data será redireccionada, de igual manera para UDP.

Las ventajas de TRT es que no requieren modificaciones de los protocolos a comparación de los otros sí requieren modificaciones lo que limita la posibilidad de despliegue. Una de las desventajas está en que solo tiene tráfico bidireccional.

Este mecanismo de traducción entre redes Ipv6 e Ipv4 tiene los siguientes componentes:

- Uno o más servidores TRT dependiendo del tamaño de la subred
- Un DNS-ALG a favor de la capa de aplicación DNS puerta de enlace
- Un servidor de DNS que es accesible por DNS-ALG
- Al menos una dirección Ipv4 para cada uno de doble pila TRT servidor

En la figura 16. TRT Apoyado en Ipv6, se reconocen los anteriores componentes como un sistema para instalación de TRT.

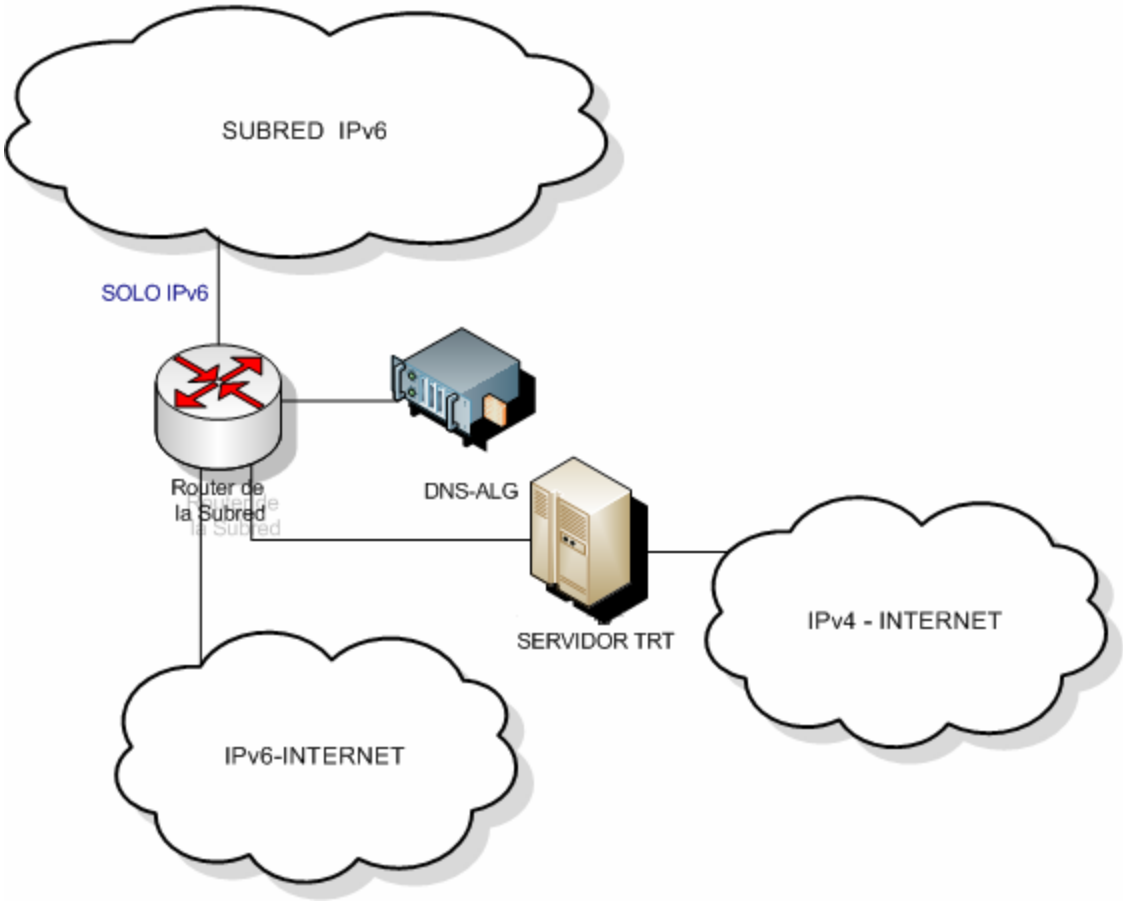



**Figura16. TRT apoyado en Ipv6**

# PARTE II: PUESTA EN MARCHA

# 6. IMPLEMENTACION DEL PROTOCOLO RIPNG

Para el desarrollo del presente capítulo se tiene en cuenta el software libre GNS-3 como herramienta principal para la ejecución del diseño propuesto y antes de realizar la descripción de la implementación y configuración del protocolo de enrutamiento RIPNG sobre Ipv6 - Ipv4, primero se hace referencia a las características de esta herramienta, utilizada para la realización de la emulación sobre IOS reales de enrutadores CISCO 7200.

## 6.1 DESCRIPCION DEL SOFTWARE UTILIZADO GNS-3 V0.5

Es un emulador virtual creado bajo Linux, permite imitar routers CISCO 7200, 3600 (Modelos 3620, 3640 Y 3660), 3700 (modelos 3725.3745) y 2600 ( desde el 2610 al 2650xm, y el 2691), se ejecuta en modo de hipervisor, de ésta forma se tienen varios dispositivos comunicándose unos con otros en una red virtual, ejecutando máquinas virtuales de routers simultáneamente, haciendo posible crear una red que emule una LAN o una WAN según la necesidad, todo dentro de un computador o si se desea entre un computador y redes reales.

GNS-3 es la parte gráfica del proyecto denominado Dynamips/Dynagen. Dynamips, desarrollado por Chistophe Fillot; actúa como emulador de routers CISCO ejecutando imágenes de IOS reales. La parte front end del emulador es la denominada Dynagen escrito por Greg Anuzelli, utilizada para interactuar con

dynamips, y permite a los usuarios listar los dispositivos; integra la consola de administración utilizada por la aplicación de GNS3.

### 6.1.1 Características de instalación.

La instalación de GNS3 es muy sencilla sobre todo para ambientes Windows, pero también trabaja perfectamente en Linux Y Mac OS X en el instructivo de este emulador que se encuentra en la página Web de la aplicación [1] se explica claramente como realizarse, sin embargo a continuación se describe un pequeño resumen sobre las características presentadas allí.

Gracias a que GNS3 es la versión gráfica de Dinamips/Dynagen su instalador es un compendio que incluye:

Winpcap: Herramienta para acceder a la conexión entre capas de red en un entorno Windows, permitiendo a la aplicación capturar y trasmitir los paquetes de red puenteando la pila de protocolos.

Dynamips: Descrito anteriormente es el emulador de routers Cisco, emula plataformas de routers y corre imágenes IOS estándar.

Pemuwrapper y una versión compilada de GNS3: El PEMU es un emulador basado en código abierto QEMU. Este emulador permite correr el sistema operativo de Firewalls de la casa Cisco Pix Firewall Operating System.

A demás se puede descargar libremente de la página oficial de dynagen [2], o en la página oficial de GNS3 [3], sin embargo en Internet se encuentran un sinnúmero de páginas y tutoriales que facilitan esta tarea, en donde también remiten a la página oficial de descarga.

### 6.1.2 IOS - Imágenes de enrutadores CISCO.

Como los IOS son imágenes o software real de enrutadores o dispositivos Cisco, por obvias razones para conseguirse hay que ser un cliente Cisco y de esta forma es permitido descargarlos de la página oficial [4] sin ningún problema a demás permite descargar toda la información y software necesario para cualquier dispositivo que se desee. Ya que el software GNS3 se consigue gratuito en la red, pero los IOS con que trabaja no lo son.

Estas imágenes en realidad son archivos comprimidos, por lo cual es recomendado realizar una descompresión del mismo debido a que dynamips es el encargado de ejecutar las imágenes de Cisco IOS y el proceso de arranque se torna más lento debido a la descompresión, al igual pasa en los routers reales, mientras que descomprimidas no tiene que realizar esta tarea. Para ahorrar carga o gastos generados para la computadora personal en el momento del arranque de un router con el software IOS ya que lo asume como un dispositivo real aumentando el tiempo de arranque del enrutador emulado, mediante la descompresión se consigue disminuir este tiempo. A demás hay otros factores como consumo de recursos de CPU que también hay que mejorar y que más adelante se explica la forma de realizarse para optimizar el uso de la memoria.

### 6.1.3 Optimizando recursos.

El encargado de ejecutar las imágenes IOS de Cisco (dynamips) asume el equipo PC como suyo y hace uso total de la memoria RAM y CPU en aras de lograr la emulación real de un dispositivo. A continuación un ejemplo citado en la página 6 de la documentación del GNS3.

Por ejemplo: Si se ejecuta una imagen de IOS de un router 7200 real, que requiere 256 MB de RAM para inicializar el router virtual, entonces este utilizará 256 MB de memoria para funcionar, porque ese es su requerimiento como enrutador real. A demás el software dynamips también requiere utilizar por defecto 16 MB de RAM por cada instancia en ambientes Windows y dice que es para cachear las transacciones JIT. Esto es a que los archivos de dynamips trazan un mapa de la memoria virtual de los routers.

No solo se hace uso intensivo de la memoria, también de la CPU debido a que en el proceso emula la CPU de un router se dice que instrucción-por-instrucción. En un principio no hay manera de saber cuando el router virtual se encuentra en estado ocioso (idle), razón por la cual ejecuta diligentemente todas las instrucciones que constituyen las rutinas de idle del IOS al igual que las que conforman el real funcionamiento. Aunque una vez ejecutado el proceso de idle PC para una determinada imagen de IOS, la utilización de la CPU disminuye considerablemente.

Por lo que cuando se inicia GNS3 por primera vez, hay que registrar una imagen de IOS y configurarle el IDLE PC para disminuir la carga de CPU del PC, y se realiza de forma sencilla, dando click derecho sobre el router ya ubicado en el área de trabajo; al desplegarse el menú, se escoge la opción IDLE PC y este muestra la mejor opción para configurarle el idle al router. Solo es colocar el numero de la opción que dio mejor rendimiento para ese dispositivo y no hay que volver a configurarle a esa versión, el IDLE a trabajar.

## 6.2 DISEÑO DE UN ESQUEMA DE TUNEL IPV6 A TRAVÉS DE UNA RED IPV4 Y CONFIGURACIÓN MEDIANTE EL PROTOCOLO RIPNG

El objetivo a alcanzar en la presente sección, es la puesta en marcha de lo investigado anteriormente, en donde se interconectan cinco routers y uno de ellos, R2 solo posee ipv4 logrando que se vean los demás mediante el mecanismo de tunelización manual y configuración del protocolo de enrutamiento dinámico para IPV6 denominado RIPNG, de esta forma comprobar que existe conectividad entre ellas, registrando las tablas de enrutamiento arrojadas por cada uno de los enrutadores.

### 6.2.1 Esquema utilizado.

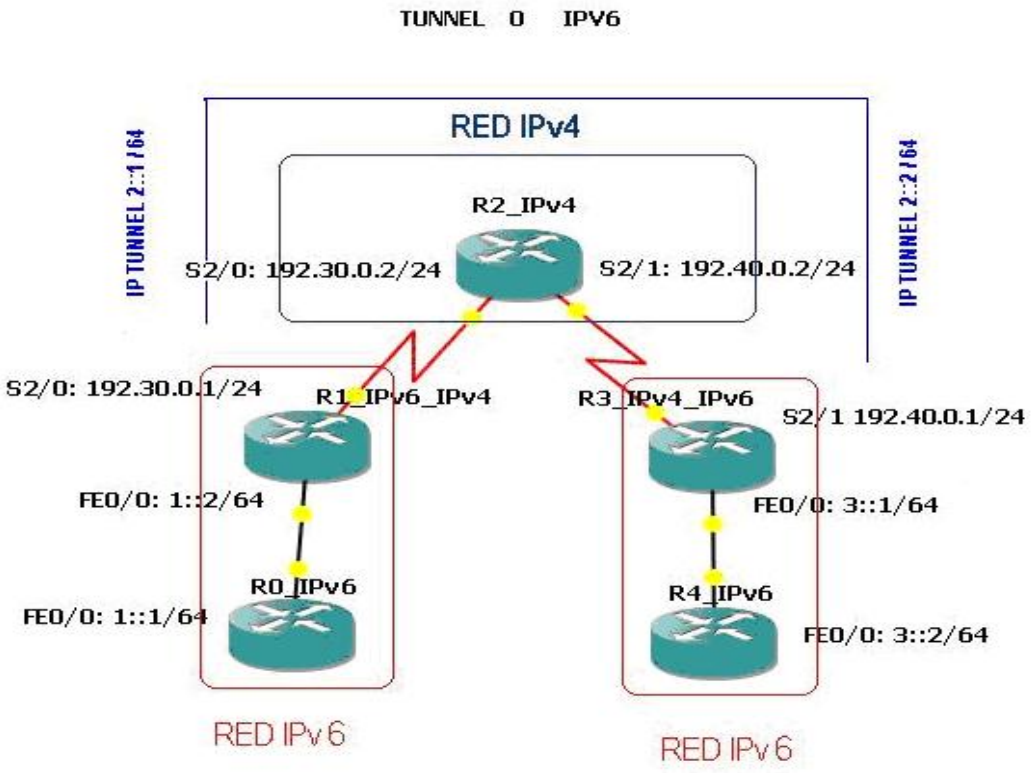



**GRAFICO 3. TOPOLOGIA DE RED**

El esquema planteado anteriormente en el grafico 3, se muestra la topología trabajada a continuación en el laboratorio; son 5 enrutadores planteados, en el cual dos redes ipv6 se encuentran separadas por medio de una red ipv4 lo cual los paquetes que se envíen y transiten entre enrutadores deben viajar de un extremo ipv6 (R0) a otro ipv6 (R4) a través del enrutador (R2) configurado con la tecnología ipv4 sin ningún problema mediante la técnica de tunelización y de modo manual.

### 6.2.2 Herramientas.

**Tabla 3. Descripción de las Herramientas**

| HERRAMIENTA | NOMBRE | DESCRIPCIÓN |
|---|---|---|
|   | GNS3 | Es el software que permite realizar conexiones virtuales. |
|  | IOS | Imagen del enrutador IOS CISCO c7200-js-mz.122-25.S8.bin |
|  | INTERFAZ SERIAL | Conexión entre dos dispositivos que permite intercambiar información de bit a bit enviando un solo bit a la vez. |
|  | INTERFAZ FastEthernet | Conexión entre dos dispositivos que permite intercambiar información o datos en forma de flujo en serie. De forma rápida. |

### 6.2.3 Configuración de los enrutadores

Para realizar la configuración en los enrutadores es necesario habilitar inicialmente el comando **ip cef** debido a que el IOS CISCO c7200-js-mz.122-25.S8.bin, empleado para el desarrollo del laboratorio lo requiere. Otros comandos utilizados como: **ipv6 unicast-routing**, permite habilitar el protocolo IP en su versión 6 en los enrutadores y así configurar el prefijo a la interfaz cuya dirección sea de 64 bits. El comando: **Interfase tunnel0** se requiere para realizar la tunelización y de esta forma versen las redes ipv6 que se encuentran en los extremos de la topología de red planteada. **Ipv6 rip ripng enable**, habilita el protocolo ripng como protocolo de enrutamiento en la interfaz en que se configure. **Router ospf 1**, activa el protocolo ospf a utilizar en el enrutador en que se configure, **network xx.xx.xx.xx 255.2555.255.0 área 0**, asigna a la red un área de trabajo.

A continuación se describe detalladamente la configuración en cada enrutador del esquema planteado (ver grafico 3 Topología De Red).

**Tabla 4. Configuración R0-ipv6**

| Paso | COMANDO | PROPOSITO |
|---|---|---|
| 1 | R0>enable | Cambia a modo privilegiado |
| 2 | R0# Configure Terminal | Modo de configuración global |
| 3 | R0(config)#hostname R0-ipv6 | Asigna nombre al enrutador |
| 4 | R0-ipv6(config)#ip cef | Se utiliza para definir a que interfaz enviar los paquetes, se encuentra deshabilitado en la mayoría de los dispositivos Cisco. |
| 5 | R0-ipv6(config)#ipv6 unicast-routing | Habilita ipv6, permite enrutamiento con ipv6 |
| 6 | R0-ipv6(config)#interface FastEthernet0/0 | Ingresar a la Fast Ethernet 0/0 |
| 7 | R0-ipv6(config-if)#ipv6 address | Asignación dirección IPv6 a la serial |

| | | |
|---|---|---|
| | 1::1/64 | Fa0/0 |
| **8** | R0-ipv6(config-if)#ipv6 rip ripng enable | Activa el protocolo de enrutamiento rip para IPv6 |
| **9** | R0-ipv6(config-if)#no clns route-cache | Desactiva cambio rápido de la caché de la interfaz |
| **10** | R0-ipv6(config-if)#no shutdown | Activa la interface Fast Ethernet |
| **11** | R0-ipv6#wr | Guarda la configuración |

R0-ipv6#**show run**

```
hostname R0
!
boot-start-marker
boot-end-marker
!
!
ip subnet-zero
!
!
!
ip cef
ipv6 unicast-routing
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync

interface FastEthernet0/0
 no ip address
 duplex half
 ipv6 address 1::1/64
 ipv6 rip ripng enable
 no clns route-cache

!
ip classless
!
no ip http server
```

```
!
!
!
ipv6 router rip ripng
!
!
!
!
-------------------
```

**Tabla 5. Configuración R1-ipv6-ipv4**

| Paso | COMANDO | PROPOSITO |
|---|---|---|
| **1** | R1>enable | Cambia a modo privilegiado |
| **2** | R1# Configure Terminal | Modo de configuración global |
| **3** | R1(config)# hostname R1-ipv6-ipv4 | Asignar nombre al enrutador |
| **4** | R1-ipv6-ipv4 (config)#ip cef | Se utiliza para definir a que interfaz enviar los paquetes, se encuentra deshabilitado en todos los dispositivos Cisco. |
| **5** | R1-ipv6-ipv4 (config)#ipv6 unicast-routing | Habilitar ipv6, permite enrutamiento con ipv6. |
| **6** | R1-ipv6-ipv4(config)#interface tunnel0 | Establece una interfaz túnel 0 |
| **7** | R1-ipv6-ipv4 (config-if)#ipv6 address 2::1/64 | Asignación dirección Ipv6 a esta interfaz del túnel |
| **8** | R1-ipv6-ipv4 (config-if)#ipv6 rip ripng enable | Activa el protocolo rip para ipv6 al túnel |
| **9** | R1-ipv6-ipv4 (config-if)#tunnel source serial2/0 | Establece la fuente u origen de la Interfaz serial del túnel (R1) |
| **10** | R1-ipv6-ipv4 (config-if)#tunnel destination 192.40.0.1 | Asigna dirección del destino (R3) al túnel. |
| **11** | R1-ipv6-ipv4 (config-if)#tunnel mode ipv6ip | Asigna modo de configuración del túnel, en este caso configuración de túnel manual, (túnel ipv6 a través de |

| | | |
|---|---|---|
| | | una red ipv4). |
| **12** | R1-ipv6-ipv4 (config-if)#no clns route-cache | Desactiva cambio rápido de la cache de la interfaz |
| **13** | R1-ipv6-ipv4 (config)#interface FastEthernet0/0 | Ingreso a la Fast Ethernet 0/0 |
| **14** | R1-ipv6-ipv4 (config-if)#ipv6 address 1::2/64 | Se asigna dirección ipv6 a la interfaz Fast Ethernet |
| **15** | R1-ipv6-ipv4 (config-if)#ipv6 rip ripng enable | Activa el protocolo de enrutamiento rip para ipv6 |
| **16** | R1-ipv6-ipv4 (config-if)#no clns route-cache | Desactiva cambio rápido de la cache de la interfaz |
| **17** | R1-ipv6-ipv4 (config-if)#no shutdown | Activa la Fast Ethernet |
| | | |
| **18** | R1-ipv6-ipv4 (config-if)#interface serial2/0 | Ingreso a la interfase serial 2/0 |
| **19** | R1-ipv6-ipv4 (config-if)#ip address 192.30.0.1 225.255.255.0 | Se asigna una dirección ipv4 con su correspondiente mascara |
| **20** | R1-ipv6-ipv4 (config-if)#clockrate 64000 | Temporizador para la interfaz serial |
| **21** | R1-ipv6-ipv4 (config-if)#no clns route-cache | Desactiva cambio rápido de la caché de la interfaz |
| **22** | R1-ipv6-ipv4 (config-if)#no shutdown | Activa la interfaz serial |
| **23** | R1-ipv6-ipv4 (config-if)#router ospf 1 | Configuración del protocolo ospf en R1 como protocolo de enrutamiento. |
| **24** | R1-ipv6-ipv4 (config-router)#network 192.30.0.0 0.0.0.255 area 0 | Asignación de la red 192.30.0.0 al R1 |
| **25** | R1-ipv6-ipv4 (config-router)#exit | Salir del modo de configuración del enrutador |
| **26** | R1-ipv6-ipv4 (config)#exit | Salir del modo de configuración global |
| **27** | R1-ipv6-ipv4 #wr | Guardar configuración actual |

R1-ipv6-ipv4 #**show run**

```
hostname R1-ipv6-ipv4
!
boot-start-marker
boot-end-marker
!
!
ip subnet-zero
!
!
!
ip cef
ipv6 unicast-routing
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync

interface Tunnel0
 no ip address
 ipv6 address 2::1/64
 ipv6 rip ripng enable
 tunnel source Serial2/0
 tunnel destination 192.40.0.1
 tunnel mode ipv6ip
 no clns route-cache
!
interface FastEthernet0/0
 no ip address
 duplex half
 ipv6 address 1::2/64
 ipv6 rip ripng enable
 no clns route-cache

!
interface FastEthernet1/0
 no ip address
```

```
 shutdown
 duplex half
 no clns route-cache
!
interface Serial2/0
 ip address 192.30.0.1 255.255.255.0
 serial restart-delay 0
 clockrate 64000
 no clns route-cache


!
router ospf 1
 log-adjacency-changes
 network 192.30.0.0 0.0.0.255 area 0
!
ip classless
!
no ip http server
!
!
!
ipv6 router rip ripng
!
!
!
!
control-plane

----------------
```

**Tabla 6. Configuración R2 -ipv4**

| Paso | COMANDO | PROPOSITO |
|---|---|---|
| **1** | R2>enable | Cambia a modo privilegiado |
| **2** | R2# Configure Terminal | Modo de configuración global |
| **3** | R2(config)#hostname R2-ipv4 | Asignar nombre al enrutador |
| **4** | R2-ipv4(config)#ip cef | Se utiliza para definir a que interfaz a enviar los paquetes, se encuentra deshabilitado en todos los dispositivos Cisco. |
| **5** | R2-ipv4(config)#ipv6 unicast-routing | Habilitar ipv6, permite enrutamiento con ipv6. |
| **6** | R2-ipv4(config)#interface Serial2/0 | Ingreso a la interfase serial 2/0 del R2 |
| **7** | R2-ipv4(config-if)#ip address 192.30.0.2 255.255.255.0 | Se asigna una dirección ipv4 con su correspondiente máscara a la serial |
| **8** | R2-ipv4(config-if)#no clns route-cache | Desactiva cambio rápido de la cache de la interfaz |
| **9** | R2-ipv4(config-if)#no shutdown | Activa la interfaz serial |
| | | |
| **10** | R2-ipv4(config-if)#interface serial2/1 | Ingreso a la interfase serial 2/1 del R2 |
| **11** | R2-ipv4(config-if)#ip address 192.40.0.2 255.255.255.0 | Asignación de la dirección ipv4 con su correspondiente máscara de red a la serial |
| **12** | R2-ipv4(config-if)#no clns route-cache | Desactiva cambio rápido de la cache de la interfaz |
| **13** | R2-ipv4(config-if)#no shutdown | Activa la interfaz serial |
| **14** | R2-ipv4(config-if)#router ospf 1 | Configuración del protocolo ospf en el enrutador R1 como protocolo de enrutamiento. |
| **15** | R2-ipv4(config-router)#network 192.30.0.0  0.0.0.255 area 0 | Asignación de la red 192.30.0.0 |
| **16** | R2-ipv4(config-router)#network 192.40.0.0   0.0.0.255 area 0 | Asignación de la red 192.40.0.0 |
| **17** | R2-ipv4#wr | Guarda la configuración |

R2-ipv4#**show run**

```
hostname R2-ipv4
!
boot-start-marker
boot-end-marker
!
!
ip subnet-zero
!
!
!
ip cef
ipv6 unicast-routing
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
 no clns route-cache
!

interface FastEthernet1/0
 no ip address
 shutdown
 duplex half
 no clns route-cache
```

```
!

interface Serial2/0
 ip address 192.30.0.2 255.255.255.0
 serial restart-delay 0
 no clns route-cache
!

interface Serial2/1
 ip address 192.40.0.2 255.255.255.0
 serial restart-delay 0
 no clns route-cache


router ospf 1
 log-adjacency-changes
 network 192.30.0.0 0.0.0.255 area 0
 network 192.40.0.0 0.0.0.255 area 0
!
ip classless
!
no ip http server
----------------------------
```

**Tabla 7. Configuración R3 -ipv4-ipv6**

| Paso | COMANDO | PROPOSITO |
|---|---|---|
| **1** | R3>enable | Cambia a modo privilegiado |
| **2** | R3# Configure Terminal | Modo de configuración global |
| **3** | R3(config)# hostname R3-ipv4-ipv6 | Asignar nombre al enrutador |
| **4** | R3-ipv4-ipv6 (config)#ip cef | Se utiliza para definir a que interfaz enviar los paquetes, se encuentra deshabilitado en todos los dispositivos Cisco. |
| **5** | R3-ipv4-ipv6 (config)#ipv6 unicast-routing | Habilitar ipv6, permite enrutamiento con ipv6. |
| **6** | R3-ipv4-ipv6(config)#interface tunnel 0 | Establece una interfaz túnel 0 |
| **7** | R3-ipv4-ipv6 (config-if)#ipv6 address 2::2/64 | Asignación dirección Ipv6 a la interfaz del túnel |
| **8** | R3-ipv4-ipv6 (config-if)#ipv6 rip ripng enable | Activa el protocolo rip para ipv6 al túnel |
| **9** | R3-ipv4-ipv6 (config-if)#tunnel source serial2/1 | Establece la fuente u origen de la Interfaz serial del túnel (R3) |
| **10** | R3-ipv4-ipv6 (config-if)#tunnel destination 192.30.0.1 | Asigna dirección del destino (R1) al túnel. |
| **11** | R3-ipv4-ipv6 (config-if)#tunnel mode ipv6ip | Asigna modo de configuración del túnel, en este caso configuración de túnel manual, (túnel ipv6 a través de una red ipv4). |
| **12** | R3-ipv4-ipv6 (config-if)#no clns route-cache | Desactiva cambio rápido de la cache de la interfaz |
| | | |
| **13** | R3-ipv4-ipv6 (config)#interface FastEthernet0/0 | Ingreso a la Fast Ethernet 0/0 |
| **14** | R3-ipv4-ipv6 (config-if)#ipv6 address 3::1/64 | Se asigna dirección ipv6 a la interfaz Fast Ethernet |
| **15** | R3-ipv4-ipv6 (config-if)#ipv6 rip ripng enable | Activa el protocolo de enrutamiento rip para ipv6 |

| | | |
|---|---|---|
| **16** | R3-ipv4-ipv6 (config-if)#no clns route-cache | Desactiva cambio rápido de la caché de la interfaz |
| **17** | R3-ipv4-ipv6 (config-if)#no shutdown | Activa la Fast Ethernet |
| **18** | R3-ipv4-ipv6 (config-if)#interface serial2/1 | Ingreso a la interfaz serial 2/1 |
| **19** | R3-ipv4-ipv6 (config-if)#ip address 192.40.0.1 225.255.255.0 | Se asigna una dirección ipv4 con su correspondiente máscara |
| **20** | R3-ipv4-ipv6 (config-if)#clockrate 64000 | Temporizador para la interfaz serial |
| **21** | R3-ipv4-ipv6 (config-if)#no clns route-cache | Desactiva cambio rápido de la cache de la interfaz |
| **22** | R3-ipv4-ipv6 (config-if)#no shutdown | Activa la interfaz serial 2/1 |
| | | |
| **23** | R3-ipv4-ipv6 (config-if)#router ospf1 | Configuración del protocolo ospf en el enrutador R3 como protocolo de enrutamiento. |
| **24** | R3-ipv4-ipv6 (config-router)#network 192.40.0.0 0.0.0.255 area 0 | Asignación de la red al R3 |
| **25** | R3-ipv4-ipv6 (config-router)#exit | Salir del modo de configuración del enrutador |
| **26** | R3-ipv4-ipv6 (config)#exit | Salir del modo de configuración global |
| **27** | R3-ipv4-ipv6 #wr | Guardar configuración actual |

R3-ipv4-ipv6 **show run**

```
hostname R3-ipv4-ipv6
!
boot-start-marker
boot-end-marker
!
!
ip subnet-zero
!
!
```

```
!
ip cef
ipv6 unicast-routing
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync
!
!
!
!
!
!
!
!
interface Tunnel0
 no ip address
 ipv6 address 2::2/64
 ipv6 rip ripng enable
 tunnel source Serial2/1
 tunnel destination 192.30.0.1
 tunnel mode ipv6ip
 no clns route-cache
!
interface FastEthernet0/0
 no ip address
 duplex half
 ipv6 address 3::1/64
 ipv6 rip ripng enable
 no clns route-cache
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex half
 no clns route-cache
!
```

```
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
 no clns route-cache
!
interface Serial2/1
 ip address 192.40.0.1 255.255.255.0
 serial restart-delay 0
 clockrate 64000
 no clns route-cache
!

router ospf 1
 log-adjacency-changes
 network 192.40.0.0 0.0.0.255 area 0
!
ip classless
!
no ip http server
!
!
!
ipv6 router rip ripng
!
!
!
!
control-plane
!
!
dial-peer cor custom
----------------------------
```

**Tabla 8. Configuración R4-ipv6**

| Paso | COMANDO | PROPOSITO |
|---|---|---|
| 1 | R4>enable | Cambia a modo privilegiado |
| 2 | R4# Configure Terminal | Modo de configuración global |
| 3 | R4(config)#hostname R4-ipv6 | Asigna nombre al enrutador |
| 4 | R4-ipv6(config)#ip cef | Se utiliza para definir a que interfaz enviar los paquetes, se encuentra deshabilitado en todos los dispositivos Cisco. |
| 5 | R4-ipv6(config)#ipv6 unicast-routing | Habilita ipv6, permite enrutamiento con ipv6 |
| 6 | R4-ipv6(config)#interface FastEthernet0/0 | Ingresar a la Fast Ethernet 0/0 |
| 7 | R4-ipv6(config-if)#ipv6 address 3::2/64 | Asignación dirección IPv6 a la serial Fa0/0 |
| 8 | R4-ipv6(config-if)#ipv6 rip ripng enable | Activa el protocolo de enrutamiento rip para IPv6 |
| 9 | R4-ipv6(config-if)#no clns route-cache | Desactiva cambio rápido de la caché de la interfaz |
| 10 | R4-ipv6(config-if)#no shutdown | Activa la interface Fast Ethernet |
| 11 | R4-ipv6#wr | Guarda la configuración |

**R4-ipv6# show run**

```
hostname R4-ipv6
!
boot-start-marker
boot-end-marker
!
!
ip subnet-zero
!
!
!
```

```
ip cef
ipv6 unicast-routing
ipv6 cef
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync
!
!
!
!
!
!
!
interface FastEthernet0/0
 no ip address
 duplex half
 ipv6 address 3::2/64
 ipv6 rip ripng enable
 no clns route-cache
!

no ip http server
!
!
!
ipv6 router rip ripng
!
!
!
!
control-plane
!
!
dial-peer cor custom
-------------------------
```

### 6.2.4 PRUEBAS DE CONECTIVIDAD

Para comprobar que el túnel está realizando su función de conectividad entre redes ipv6 e ipv4 se hace un ping en cada uno de los enrutadores que se encuentran en los extremos (R0-ipv6 y R4-ipv6) siendo los únicos configurados con ipv6.

En la imagen de la izquierda (gráfico 4) que se visualiza a continuación, muestran los resultados arrojados al hacer ping a la interfaz Fast Ethernet0/0 de dirección 3::2 del enrutador R4-ipv6 que se encuentra al otro extremo de la topología de red.

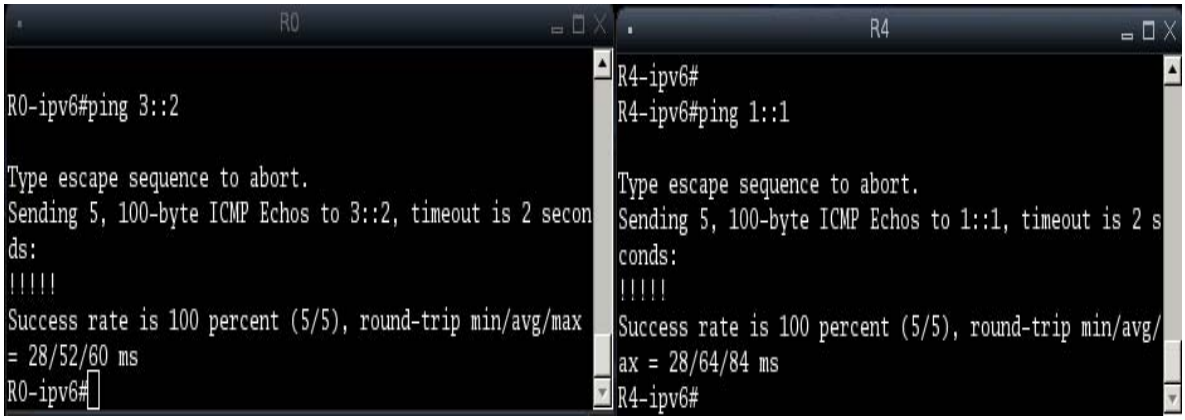



**Gráfico 4. Prueba de conectividad R0** **Gráfico 5. Prueba de conectividad R4**

Con los 5 signos de admiración arrojados y haciendo eco en 2 segundos ha demostrado que efectivamente hay conectividad entre este enrutador R0_ipv6 y el enrutador R4-ipv6.

Sin embargo también hay que mirar que desde el otro extremo se puedan ver los enrutadores, por lo que en la imagen de la derecha (gráfico 5) muestra el ping

realizado a la interfaz Fast Ethernet del enrutador R0-ipv6 desde el enrutador R4-ipv6.

Como se describió anteriormente también con los 5 signos de admiración y eco a la interfaz 1::1 del enrutador R0-ipv6 realizado en los mismos 2 segundos, revela que efectivamente también hay conectividad hacia el enrutador R0-ipv6. Lo cual demuestra que las interfaces están funcionando correctamente y por supuesto el túnel configurado está realizando la función de comunicar dos redes iguales a través de redes diferentes.

### 6.2.5 Tablas de rutas

Mediante el comando **show ip route o show ipv6 route** según corresponda a la versión 4 o 6 del protocolo de internet, se muestra la tabla de rutas que se han configurado en las interfaces de los enrutadores, permitiendo así visualizar la lista de redes que cada enrutador puede alcanzar, y la forma como puede acceder a ellas, como por ejemplo por medio de un túnel.

A continuación, se presentan en las imágenes la configuración de los enrutadores vistas mediante la tabla de rutas desplegadas en cada uno de los enrutadores del escenario propuesto.

### 6.2.5.1 Tabla de rutas para el enrutador R0-ipv6

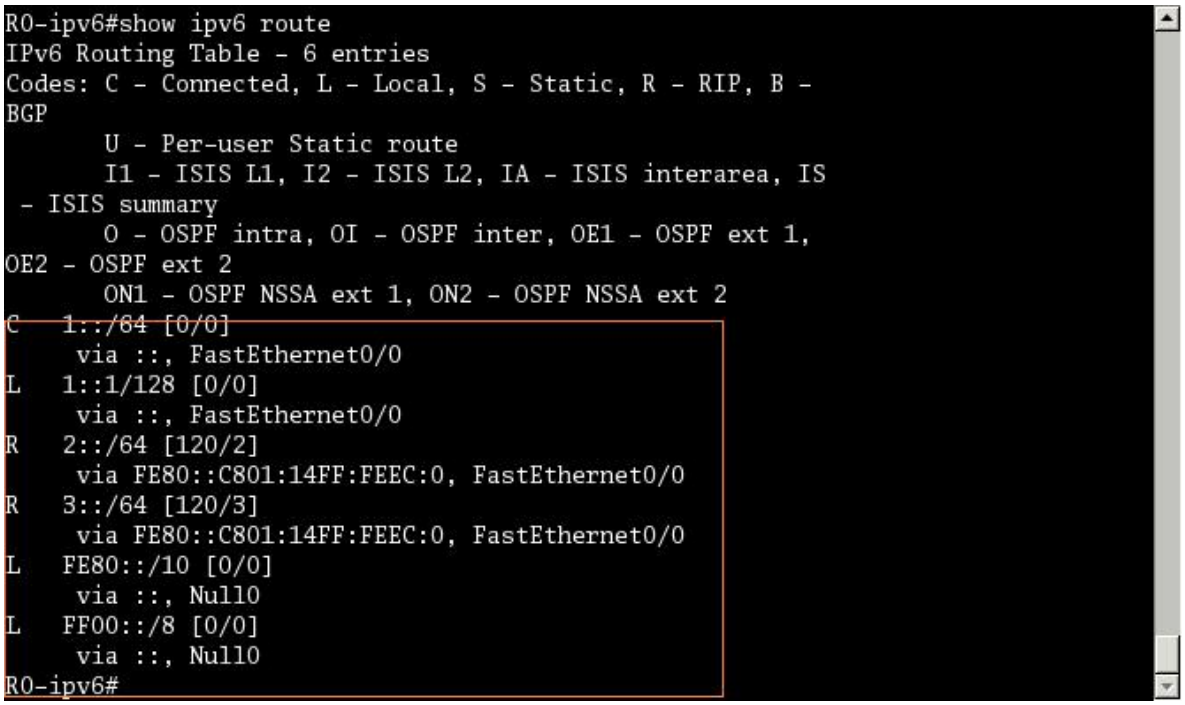



**Gráfico 6. Tabla de rutas enrutador R0-ipv6**

En el enrutador R0-ipv6, la tabla que arroja el comando **show ipv6 route**, muestra que el enrutador tiene conectada la interfaz Fast Ethernet 0/0 a una red ipv6 1::/64 y su dirección a nivel de red local es 1::1. También se observa que por medio del protocolo de enrutamiento ripng se puede conectar a la red ipv6 2::/64 (red configurada para uso del túnel) a dos saltos de distancia, y a su vez se comunica por medio del protocolo ripng a la red 3::/64 a tres saltos de distancia de este. (Arroja la distancia administrativa de ripng que es de 120).

### 6.5.2.2 Tabla de rutas para el enrutador R1-ipv6-ipv4

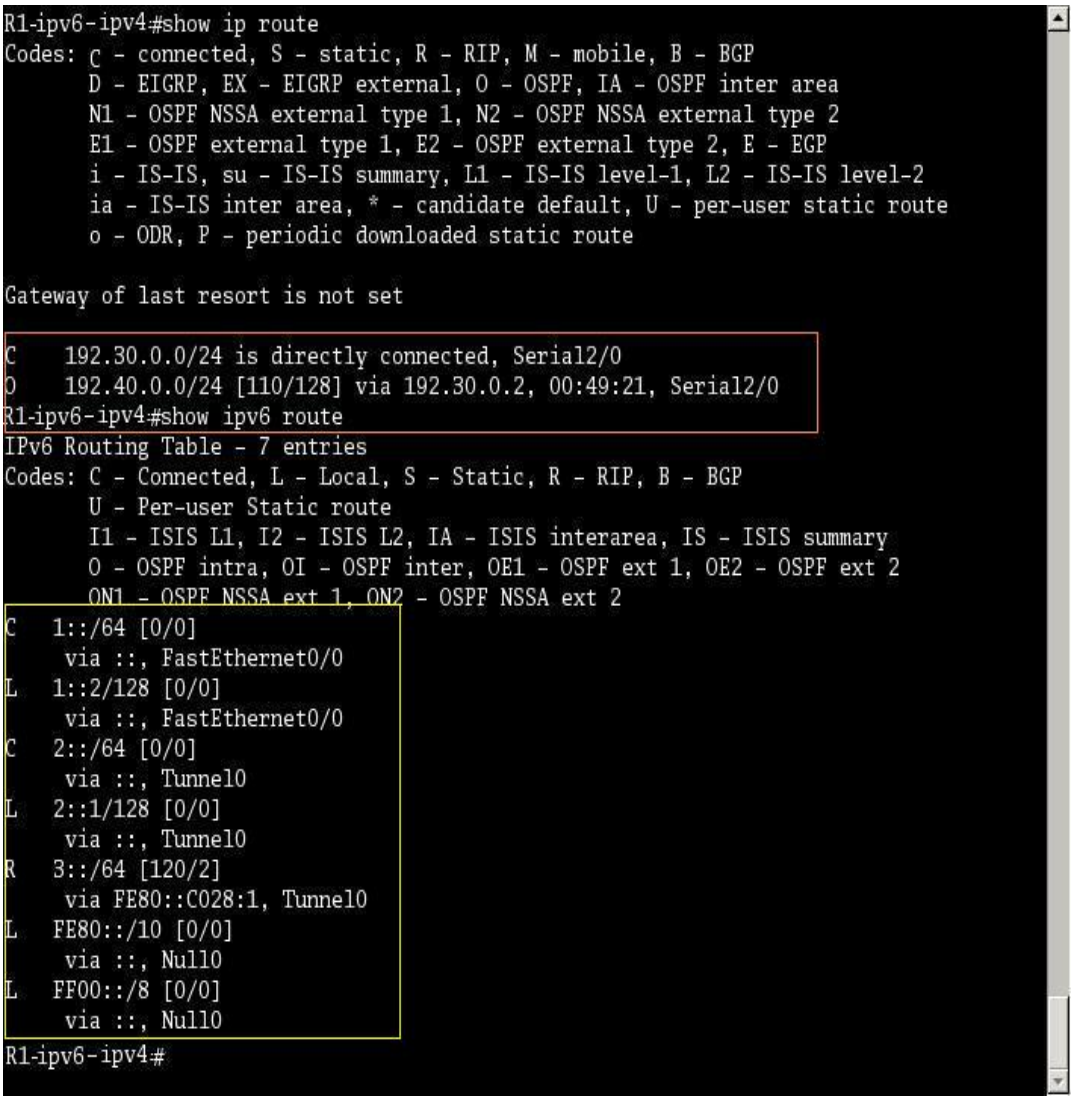



**Gráfico 7. Tabla de rutas enrutador R1-ipv6-ipv4**

En el enrutador R1-ipv6-ipv4 se ha configurado una interfaz serial para red ipv4 y otra interfaz Fast Ethernet para red ipv6, por esta razón hay que ejecutar el comando **show ip** tanto para la versión ipv4 como para la versión ipv6.

En la versión Ipv4

La tabla de rutas arrojada al ejecutar el comando show **ip route**, (ver recuadro naranja en la imagen grafico 6) muestra que el enrutador R1 tiene conectada la red 192.30.0.0/24 a la interfaz serial2/0 y que por el protocolo OSPF (con distancia administrativa de 110) puede ver la red 192.40.0.0/24 que se encuentra al otro extremo, ya que la interfaz serial 2/0 de este enrutador tiene la dirección 192.30.0.2 que es la dirección del puerto serial que conecta directamente con el siguiente enrutador R2 el cual tiene configuradas las dos redes: 192.30.0.0 y la 192.40.0.2 por tal motivo el protocolo de enrutamiento OSPF permite verla desde este enrutador.

En la versión Ipv6

Para visualizar la tabla de rutas en la versión 6 se ejecuta el comando **show ipv6 route**, con este se ven las conexiones directamente establecidas. En el recuadro amarillo se muestra la configuración de la interfaz Fast Ethernet 0/0 con la red 1::/64, y la otra red conectada es la 2::/64 que es la red establecida para la tunelización.

Es importante aclarar que por medio de esta interfaz se puede ver en qué red se encuentra configurado el túnel, claramente se visualiza que el **Tunel0 (**modo escogido **ipv6ip)** está conectado localmente a la dirección 2::1 y por medio del protocolo de enrutamiento Ripng puede ver la red 3::/64 que se encuentra a dos saltos de distancia de este [120/2] con distancia administrativa 120 que es la de rip.

### 6.2.5.3 Tabla de rutas para el enrutador R2-ipv4

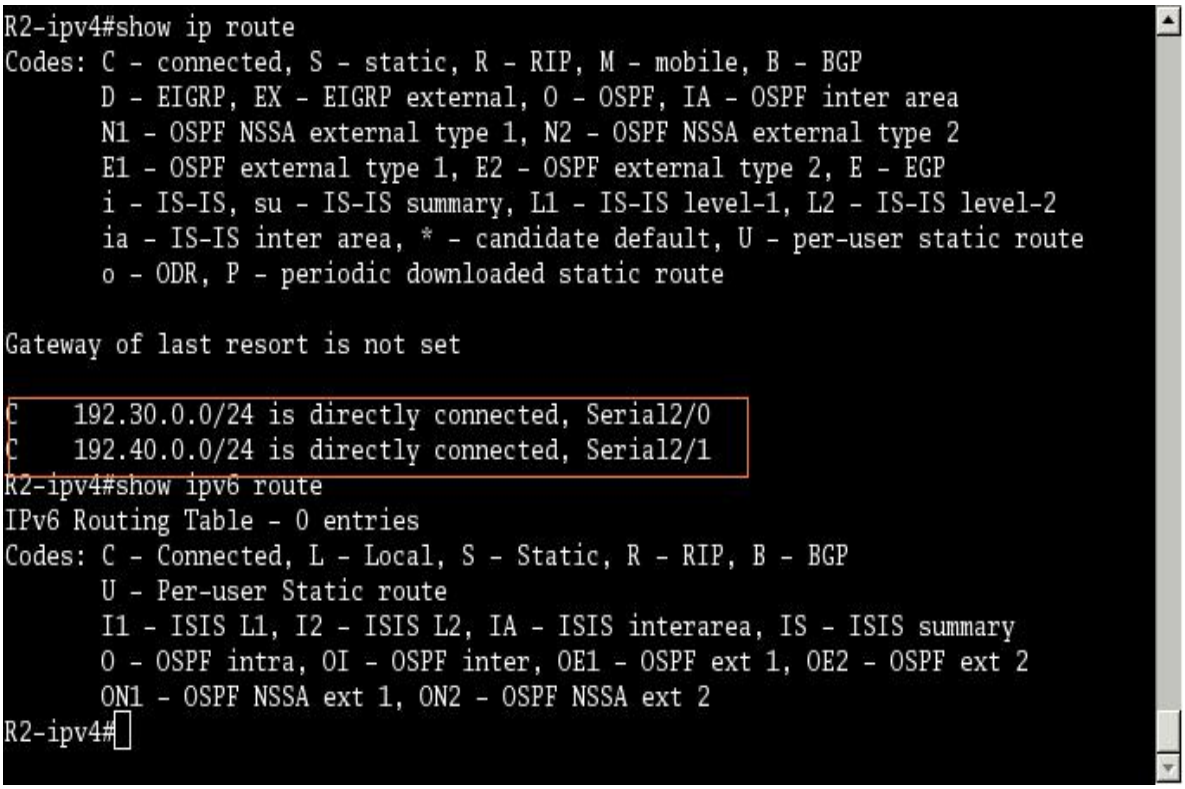



**Gráfico 8. Tabla de rutas enrutador R2-ipv4**

El enrutador R2 –ipv4 en donde solo se encuentra configurada la versión 4 de ip. La tabla de rutas permite ver que hay dos redes conectadas directamente a el, que son las redes 192.30.0.0/24 conectada por medio de la interfaz serial 2/0 y la red 192.40.0.0/24 conectada por medio de la serial2/1.

### 6.2.5.4 Tabla de rutas para el enrutador R3-ipv4-ipv6

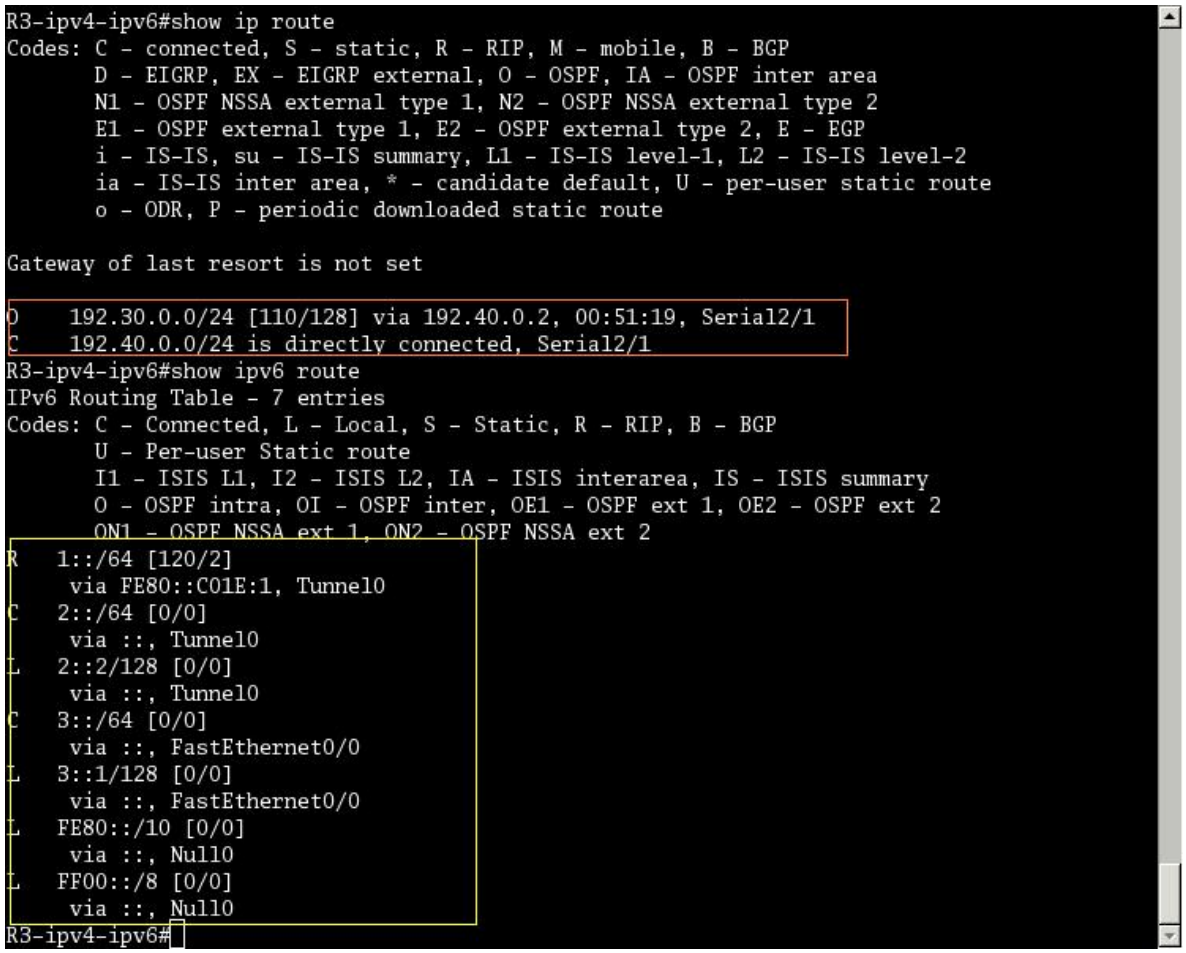



**Gráfico 9. Tabla de rutas enrutador R3-ipv4-ipv6**

La configuración del enrutador R3-ipv4-ipv6 es la misma configuración realizada al enrutador R1-ipv6-ipv4, ya que estos dos, son los encargados del túnel por estar en los extremos de la red ipv4, por eso en su configuración se observan semejanzas y la descripción de la tabla de rutas es muy parecida.

Al analizar primero la tabla de rutas arrojada para ipv4, se observa en ella que se encuentra configurada la red 192.40.0.0/24 conectada directamente a la interfaz serial 2/1 del enrutador que se está analizando (R3-ipv4-ipv6) y por medio de esta

misma serial se puede ver la red 192.30.0.0/24 que se encuentra al otro extremo en el enrutador R2-ipv4 gracias al protocolo de enrutamiento OSPF.

En cuanto para ipv6 se puede notar que en primera instancia aparece la red 1::/64 el cual se encuentra a dos saltos de distancia de este enrutador y que gracias al túnel y a la configuración ripng como protocolo de enrutamiento se pueden ver desde este enrutador. En seguida se observan conectadas directamente las redes ipv6 3::/64 en la interfaz Fast Ethernet con dirección local 3::1 y la red 2::/64, siendo esta última la red configurada para uso del túnel con dirección local 2::2.

### 6.2.5.5 Tabla de rutas para el enrutador R4

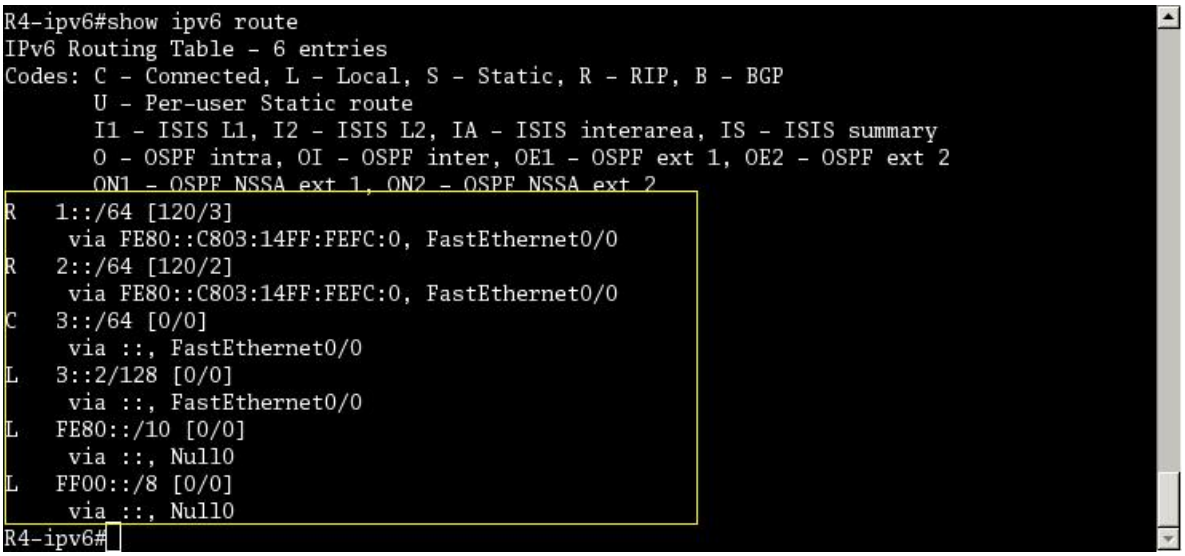



**Gráfico 10. Tabla de rutas enrutador R4-ipv6**

Como en el enrutador R4-ipv6 solo se configuró para uso de ipv6 solo se observan las redes con que se puede comunicar siempre y cuando sean de la misma versión. Por medio del protocolo ripng puede comunicarse con la red 1::/64 que se encuentra a tres saltos de distancia, gracias al túnel configurado en el enrutador

R3-ipv4-ipv6 que se encuentra a dos saltos de distancia en la red 2::/64. Este enrutador tiene conectada directamente la red ipv6 3::/64 en la interfaz Fast Ethernet0/0 con la dirección local 3::2.

# CONCLUSIONES

Mediante la investigación de los escenarios de transición se demuestra, que la forma más acertada de realizar la migración hacia ipv6 en corto tiempo sin causar caos tecnológico, es mediante la escalabilidad de una versión IP a otra, por lo tanto la mejor opción es la utilización de un mecanismo de transición. Se considera conveniente ya que no altera las infraestructuras complejas empleadas hoy día bajo redes ipv4.

Además, una de las grandes ventajas de los escenarios de transición contemplados en el capítulo 4 es la variedad. Esto permite que el administrador de cualquier red pueda adecuarse a la más apropiada para su propia topología, eso sí, teniendo en cuenta las características y configuración de las mismas. De esta forma se pueden adaptar a cualquier necesidad.

A la vez se confirmó que la implementación con RIP, aunque se realice mediante su nueva versión para ipv6 (ripng) sigue siendo la más sencilla de emplear, no obstante también el mecanismo de transición para redes ipv6, demostró ser viable para su utilización y dio pie para efectuar ágilmente la implementación, mediante la técnica de Tunelización, el cual se tomó como mecanismo para transferir la información de un extremo a otro. Además alígero el desarrollo del laboratorio contemplado en el último capítulo.

Aunque el modo empleado para su configuración es de forma manual, su complejidad fue mínima, por lo que resultó para este caso la más apropiada por su ligereza, sencillez y precisión al implementarse.

No obstante, rip a pesar de los cambios realizados para adaptarlo a la nueva versión de ipv6 (ripng), sigue siendo poco útil para redes grandes y complejas ya que posee las mismas limitaciones que sus versiones anteriores, restándole seguridad, versatilidad, precisión y por consiguiente confianza ante la toma de decisiones.

En las redes de área local pequeñas, la decisión más acertada es la utilización de la tunelización ya que permite un buen funcionamiento de la red y agiliza trabajo a la hora de configurar enrutadores CISCO reales.

## BIBLIOGRAFIA


- Jorge Villa, Art. "*Nuevo Estudio sobre agotamiento de direcciones IPv4*", extraído de*:* http://www.latinoamericann.org/modules.php?op=modload&name=News&file=article&sid=1113&mode=thread&order=0&thold=0 (recuperado el 30 de junio de 2008)

- *"El futuro de Internet (introducción a IPv6) Emezeta blog*", extraído de http://www.emezeta.com/articulos/el-futuro-de-internet-introduccion-a-ipv6 (recuperado el sábado 28 de junio de 2008)

- Ciprian Popoviciu PhD, CCIE , CIscoSystems, art. "*Una segunda oportunidad para obtener una fracción equitativa de IP- IPv6 consideraciones sobre su introducción",* extraído de: http://www.citel.oas.org/newsletter/2005/marzo/ipv6_e.asp ( recuperado el lunes 30 de junio de 2008 ).

- Alberto Roldán, Art. "Cómo hacer una monografía", extraído de: http://www.fiet.com.ar/articulo/monografia_roldan.doc (recuperado el 22 de junio de 2008)

- Jordi Palet Martínez, tutoría. "*Tutorial de IPv6*", extraído de: http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf (recuperado el 25 de junio de 2008)

- Joaquín Muñoz Lucavechi, documento sobre “Implementación de IPv6 para la red académica de centros de Investigación y Universidades Nacionales”, extraído de: http://www.nic.ve/view/docs/CNTI_IPv6.pdf (recuperado el 25 de junio de 2008).

- Gonzalo Paniagua Javier, “ RFC es, Grupo de Traducción al castellano de:

  RFC”, extraído de http://www.rfc-es.org/ (Recuperado 10 agosto de 2008)

- Pv6 forum, “RFC´S de IPv6”, extraído de :

  http://www.consulintel.es/html/ForoIPv6/RFCs.htm. (recuperado el 30 de septiembre de 2008)

- Jorge A. Flores Iturbe, art. “Tunelización de protocolos”, extraído de:

  http://www.mitecnologico.com/Main/TunelizacionDeProtocolos (Recuperado el 15 de Octubre del 2008).

- Arin (American Registry For Internet Number), art. “La transición hacia Ipv6”, extraído de:

  http://www.arin.net/about_us/media/fact_sheets/Spanish/IPv6_Transition_spanish_web.pdf. (Recuperado el 16 de Octubre del 2008).

- Sergio Ramírez, María Cervantes, Art “Introducción al Ipv6” extraído de:

  http://www.rau.edu.uy/ipv6/queesipv6.htm (Recuperado el 16 de Octubre del 2008).

- CISCO. Art. “About Cisco IOS and Cisco IOS XE software Doccumentation.” http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_4/ipv6_12_4_book.pdf. Pág. 621, (Recuperado el 4 de octubre de 2008).

- David Bombal. Art. “ Dynamips & Dynagen – how to run Cisco Routers on yor PC”. Extraído de: http://www.configureterminal.com/Dynamips.htm.

  (Recuperado 05 de octubre de 2008).

- Mike Fuszner. GNS3. “New tutorial for GNS3”, extraído de:

  http://www.gns3.net/news/new_tutorial_gns3. (Recuperado 30 de septiembre de 2008).

Páginas WEB referidas en el contenido

[1] http://www.gns3.net/news/new_tutorial_gns3
[2] http://dynagen.org
[3] http://www.gns3.net/
[4] http://www.cisco.com/