ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería Eléctrica y Computación

"ANÁLISIS DEL DIRECCIONAMIENTO IPV6 Y ESTUDIO COMPARATIVO ENTRE LOS PROTOCOLOS DE ENRUTAMIENTO ORIENTADOS A IPV6"

INFORME DE PROYECTO DE GRADUACIÓN

Previo la obtención del Título de:

INGENIERO EN TELEMÁTICA

Presentada por:

ALEXANDER ABRAHAN AGUILAR ALVARADO

LUIS FELIPE CHÁVEZ CRUZ

Guayaquil – Ecuador
2014

AGRADECIMIENTO

Al Ing. Albert Espinal, el mismo que facilitó el uso del laboratorio de CISCO-ESPOL, para la realización de nuestras prácticas. A nuestro tutor Ing. José Patiño e Ing. Patricia Chávez, que con su constante apoyo y orientación, forjaron sólidos pilares para que este proyecto llegue a su culminación y posterior presentación.

DEDICATORIA

A Dios, porque todo está en él. A mis padres, quienes a lo largo de mi vida me ayudaron cumplir mis deberes y derechos. A cada una de las personas que desde mi concepción han contribuido en el desarrollo de mi aprendizaje a nivel profesional y personal.

Alexander Abrahan Aguilar Alvarado

A Dios, por darme sabiduría e iluminar mi camino día a día. A mis padres, quienes a lo largo de mi vida me han apoyado a seguir todos mis sueños y cumplir mis metas. A mi segundo padre, mi abuelo. A mi segunda madre, mi tía. A mis amigos, por brindarme su apoyo incondicional en todas las etapas de mi vida.

Luis Felipe Chávez Cruz

TRIBUNAL DE SUSTENTACIÓN

Ph.D. Boris Vintimilla
SUBDECANO DE LA FIEC
PRESIDENTE

Ing. José Patiño S., MSIG
DIRECTOR DEL PROYECTO DE GRADO

Ing. Patricia Chávez B., MSEE
MIEMBRO PRINCIPAL DEL TRIBUNAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Informe de Proyecto de Graduación nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL". (Reglamento de Exámenes y Títulos profesionales de la ESPOL).

_____

Alexander Abrahan Aguilar Alvarado

_____

Luis Felipe Chávez Cruz

RESUMEN

El presente proyecto tiene como objetivo realizar un análisis comparativo de los protocolos de enrutamiento orientados a IPv6 mediante pruebas experimentales, para las cuales se diseñaron topologías de red en base a los conocimientos obtenidos en el marco teórico. En dichas pruebas se midieron características como convergencia, confiabilidad, escalabilidad y latencia, además de comparar el hardware a utilizar para escoger los equipos idóneos para un ambiente de producción. Se describe el procedimiento que llevamos a cabo en nuestros laboratorios, identificando ventajas y desventajas de un IGP sobre otro, monitoreando el funcionamiento de la red y finalmente analizando los resultados obtenidos en las diferentes pruebas realizadas, tanto en protocolos de vector de distancia y estado de enlace. Adicionalmente se implementó un esquema multihoming, en el cual se utilizó el protocolo de enrutamiento BGP.

ÍNDICE GENERAL

ABREVIATURAS

ABR	Enrutador de borde
AFRINIC	Registros de Direcciones de Internet para África
AH	Cabecera de Autenticación
APNIC	Registros de Direcciones de Internet para Asia-Pacífico
ARIN	Registros de Direcciones de Internet para América anglosajona
AS	Sistema autónomo
ASBR	Enrutador de límite del sistema autónomo
ASN	Número de Sistema autónomo
BGP	Protocolo de entrada de frontera
CIDR	Enrutamiento entre dominios sin clase
DHCP	Protocolo de configuración de host dinámico
DHCPv6	Protocolo de configuración de host dinámico versión 6
DNS	Sistema de nombres de dominio

DUAL	Algoritmo de actualización por difusión
EGP	Protocolo de puerta de enlace exterior
EIGRP	Protocolo de enrutamiento de puerta de enlace interior mejorado
ESP	Cabecera de cifrado de seguridad
ESPOL	Escuela Superior Politécnica del Litoral
FTP	Protocolo de transferencia de archivos
IANA	Autoridad de asignación numérica de Internet
ICANN	Corporación de Internet para la asignación de dominios y direcciones
IEEE	Instituto de Ingenieros Eléctricos y Electrónicos
IETF	Grupo de Trabajo de Ingeniería de Internet
IGP	Protocolo de puerta de enlace interior
IOS	Sistema operativo de equipos de telecomunicaciones
IP	Protocolo de internet
IPSec	Protocolo de seguridad de internet

IPv4	Protocolo de internet versión 4
IPv6	Protocolo de internet versión 6
IS-IS	Protocolo de enrutamiento entre sistemas intermedios
ISO	Organización Internacional de Normalización
ISP	Proveedor de servicios de internet
KB	Kilobyte
Kbps	Kilobits por segundo
LACNIC	Registros de Direcciones de Internet para Latinoamérica y el Caribe
LAN	Red de área local
LSA	Respuesta de estado de enlace en IS-IS
LSP	Paquete de estado de enlace en OSPFv3
LSR	Petición de estado de enlace en IS-IS
LSU	Actualización de estado de enlace en IS-IS
MB	Megabyte

NAT	Traducción de Dirección de Red
NBMA	Redes de Multiacceso no Broadcast
ND	Descubrimiento de Vecinos
NET	Nombre de una entidad de red
NH	Siguiente cabecera
NSAP	Servicio de red de punto de acceso
NSEL	Selector de NSAP
OSI	Interconexión de Sistemas Abiertos
OSPF	Protocolo del primer camino más corto
OSPFv3	Protocolo del primer camino más corto versión 3
PC	Computador personal
RAM	Memoria de acceso aleatorio
RFC	Documentación de petición de comentarios
RIP	Protocolo de información de enrutamiento
RIPE-NCC	Centro de Coordinación de redes IP europeas

RIPng	Protocolo de información de enrutamiento de siguiente generación
RIR	Registro Regional de Internet
RTE	Cabecera de una entrada de enrutamiento
SEL	Selector
SNP	Paquete de número de secuencia en OSPFv3
SPF	Algoritmo de la primera ruta más corta
TCP	Protocolo de transmisión de control
TLV	Tipos, Longitud y Valor
VLSM	Máscara de subred de tamaño variable

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El exponencial crecimiento de usuarios en Internet causó el agotamiento de direcciones IPv4, la cual fue la pauta para la creación de IPv6, quien se espera sea implementando en todas las redes de datos a nivel mundial. Por esto es muy importante conocer las características de IPv6, pero principalmente saber el funcionamiento del enrutamiento estático y dinámico, diseñando topologías para realizar pruebas con los protocolos de enrutamiento: RIPng, EIGRP, OSPFv3 e IS-IS; comparándolos entre los del mismo tipo, vector distancia y estado de enlace, para así reconocer sus ventajas y desventajas entre sí.

CAPÍTULO 1

1. ANTECEDENTES

En esta sección se describirá la problemática que existe debido al agotamiento de direcciones IPv4, motivo por el cual fue creado IPv6, y que hoy en día ya es utilizado en organizaciones a nivel mundial. A su vez mencionamos los objetivos que nos hemos trazado, junto con la metodología para su cumplimiento.

1.1. Descripción del problema y presentación

IPv4 inicialmente fue ideado como un experimento en el cual se creía que 4300 millones de direcciones eran suficientes para abastecer el gran mercado que iba a abarcar, no se pensaba que se iban a ocupar este gran número de direcciones en tan poco tiempo y mucho menos la desenfrenada creación de nuevos equipos o dispositivos que iban a utilizar direcciones IP; en la actualidad artefactos de uso doméstico utilizan direcciones IP’s para comunicarse con los demás equipos del hogar y juntos poder formar lo que es llamado un hogar inteligente [1].

Se tomaron medidas para frenar el rápido agotamiento de direcciones IPv4 y así ayudar a que dicho modelo siga vigente. Esto dio tiempo para que las personas dedicadas a la investigación idearan una nueva versión de protocolo de internet, el cual fue llamado IPv6, en el que se corrigieron los errores de IPv4, se disminuyó la cantidad de campos en su cabecera, se aumentó el número de bytes del paquete, entre otros, todo esto pensado para que en un futuro no se agoten las direcciones IP, tanto así que se estima que cada usuario en el mundo posea poco más de 6 direcciones o incluso que cada uno pueda usar una dirección pública para cada uno de sus dispositivos electrónicos.

1.2. Descripción de la solución propuesta

Como parte del estudio analizaremos el direccionamiento IPv6, sus características principales, estructuras del paquete, formato de direcciones, enrutamiento estático IPv6, requerimientos de hardware y software que este necesita para su implementación. Realizaremos una revisión sobre cada uno de los IGP's, empezando por los de vector de distancia (RIPng y EIGRP) y continuando con los de estado de enlace (IS-IS y OSPFv3), revisando funcionamiento, configuración, análisis de actualizaciones y tablas de enrutamiento, y las características específicas

de cada uno de ellos. Adicionalmente revisaremos conceptos de EGP's, específicamente BGP y su implementación en multihoming.

1.3. Justificación

Debido al avance de nuevas tecnologías, día a día son diseñados nuevos equipos como ordenadores, teléfonos inteligentes, tabletas y cada usuario usa más de uno; ya que cada uno de ellos asocia una identificación para formar parte de una red ya sea intranet o internet, poco a poco estas identificaciones denominadas direcciones IP's comienzan a escasear, razón por la cual se dio la necesidad de crear direcciones que establezcan un dominio más amplio para asignar a cada dispositivo informático. Esta inmensa demanda, así como otros factores como son la seguridad, confiabilidad, escalabilidad, entre otros, crean la necesidad de la utilización de IPv6 para que las comunicaciones entre equipos de diferentes tipos sean más eficientes. Por lo cual creemos conveniente el análisis de los protocolos de enrutamiento en IPv6, sus diferentes usos, características, ventajas y desventajas.

1.4. Objetivos

A continuación se describirán los objetivos de este proyecto.

1.4.1. Objetivos Generales

- Establecer diferencias y semejanzas de protocolos de enrutamiento dinámico según la clasificación de Gateway Interior (Vector de Distancia y Estado de Enlace).

1.4.2. Objetivos Específicos

- Diseñar e implementar una red IPv6 mediante la utilización del protocolo EIGRP.
- Diseñar e implementar una red IPv6 mediante la utilización del protocolo RIPng.
- Diseñar e implementar una red IPv6 mediante la utilización del protocolo OSPFv3.
- Diseñar e implementar una red IPv6 mediante la utilización del protocolo IS-IS.
- Establecer diferencias y semejanzas entre protocolos de enrutamiento de Vector de Distancia IPv6 (EIGRP y RIPng).
- Establecer diferencias y semejanzas entre protocolos de enrutamiento de Estado de Enlace IPv6 (IS-IS y OSPFv3).

- Analizar las características y funcionamiento de una conexión básica entre Sistemas Autónomos aplicando Multihoming en direccionamiento IPv6.

1.5. Metodología

La metodología se llevará a cabo con el desarrollo de las siguientes ocho fases:

1.5.1. Fase 1

Revisar conceptos generales de IPv4.

1.5.2. Fase 2

Realizar una investigación sobre IPv6, características, direccionamiento, protocolos de enrutamiento y configuraciones.

1.5.3. Fase 3

Realizar un estudio de factibilidad y disponibilidad del hardware y software.

1.5.4. Fase 4

Estudiar más a fondo las características de los equipos seleccionados, como especificaciones técnicas y limitaciones.

1.5.5. Fase 5

Diseñar las diferentes topologías de red para los IGP’s en IPv6.

1.5.6. Fase 6

Implementar cada una de las topologías de red diseñadas, realizando las pruebas correspondientes para la obtención de resultados.

1.5.7. Fase 7

Elaborar nuestra matriz de comparación, diferenciando a los protocolos en base a parámetros como convergencia, confiabilidad, escalabilidad, entre otros.

1.5.8. Fase 8

Establecer claramente recomendaciones y observaciones para futuros usos y aplicaciones.

CAPÍTULO 2

2. MARCO TEÓRICO PREVIO AL ANÁLISIS COMPARATIVO DE LOS PROTOCOLOS DE ENRUTAMIENTO EN IPV6

Una vez descrito el problema en el capítulo uno y dividiéndolo en fases para su desarrollo, se describirán todos los conceptos necesarios para poder realizar un análisis comparativo entre los IGP's orientados a IPv6 y adicionalmente para la compresión de multihoming se añadieron conceptos de BGP.

2.1. Historia de las redes de datos

TCP, Protocolo de Control de Transmisión, es fundamental para el tráfico en Internet. Fue creado entre los años 1973 - 1974 por Vint Cerf y Robert Kahn. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron.

IPv4 es la versión 4 del Protocolo de Internet y constituye la primera versión de IP que es implementada de forma extensiva. IPv4 es el principal protocolo utilizado en el nivel de Red del modelo TCP/IP para Internet. Fue descrito inicialmente en el RFC 791 elaborado por la IETF en Septiembre de 1981, documento que dejó obsoleto al RFC 760 de Enero de 1980. Posteriormente se desarrolló el Protocolo de Internet versión 5 o IPv5, pero solo fue un protocolo experimental, ya que este protocolo fue orientado a mejorar el procesamiento de flujo de audio, voz y video. Desde 1992 se empezó a buscar mecanismos para mejorar e intentar suplir los defectos presentados en IPv4, la siguiente generación de Protocolos de Internet surgió del IETF, que ha culminado con la especificación de un nuevo protocolo IP, sucesor del actual IPv4, conocido formalmente como la versión 6 del Protocolo Internet o IPv6, el cual fue lanzado en el año 1999. IPv6 llega como la solución al agotamiento de direcciones IP dando así la facilidad de tener mayor número de dispositivos conectados a la red [2].

2.2. Direccionamiento IPv4

IPv4 utiliza direcciones de 32 bits (4 bytes) que limita el número de direcciones posibles a utilizar a cuatro mil trescientos millones de

direcciones únicas aproximadamente. Sin embargo, muchas de estas están reservadas para propósitos especiales como redes privadas, Multidifusión, etc. [2].

2.2.1. Características IPv4

Entre las características que se pueden resaltar de IPv4 tenemos [1]:

- El uso de IPsec es opcional.
- El direccionamiento de equipos debe configurarse manualmente o a través de DHCP.
- El encabezado incluye un campo llamado “Opciones” usado para pruebas, registrando información relacionada a seguridad, rutas desde el origen hasta el destino y los tiempos empleados.
- Se utilizan direcciones de multidifusión para enviar tráfico a todos los nodos de una subred.

2.2.2. Agotamiento de direcciones IPv4

El direccionamiento con clase fue aplicado en IPv4 en primera instancia, el cual tenía como principal característica que la máscara de subred podía determinarse con el valor de los primeros tres bits de la dirección, esto limitaba el enrutamiento a redes contiguas.

Debido al acelerado crecimiento del uso de direcciones IP, se diseñó el esquema al direccionamiento sin clase CIDR, en el que se usa VLSM para asignar direcciones IP a subredes de acuerdo con la necesidad individual en lugar de hacerlo por la clase. Uno de los métodos que se diseñó para mantener vigente el direccionamiento IPv4 fue NAT, que se presentó en 1994 (RFC 1631), el cual convierte direcciones de una red privada a una dirección pública [1].

2.2.3. Problemas existentes en IPv4

El principal problema que tiene IPv4 es que ya no existen direcciones IP's disponibles. Con la existencia de IPv6 nuevos problemas se han originado, esta vez por la operatividad en conjunto de IPv4 e IPv6, ya que manejan formatos de direcciones y estructuras de paquetes diferentes. Este problema actualmente se ha superado con la creación de mecanismos de transición que permiten funcionar a IPv6 e IPv4 en diferentes redes.

2.2.4. Factores Para El Cambio

El agotamiento de direcciones IPv4 fue la razón que motivó a diseñar un direccionamiento que cubra la demanda actual y futura de

usuarios conectados a Internet. IPv6 emplea 96 bits más que IPv4 para el direccionamiento IP, entre una serie de características adicionales.

2.2.5. Transición IPv4 – IPv6

Se han creado los siguientes mecanismos de transición que permiten interactuar IPv4 e IPv6: doble pila, túneles (6to4-RFC3056 y Teredo-RFC4213) y métodos de traducción (NAT64/DNS-RFC6144, RFC6145, RFC6146, RFC6052, RFC6147) [3].

2.3. IPv6

IPv6 se define en el documento RFC 2460, en este nuevo protocolo se mantuvo la base de IPv4, lo que era comúnmente usado por los usuarios se conservó y aquello que no se usaba con regularidad fue eliminado para así agregar nuevas características. La cantidad de direcciones IP que ofrece IPv6(2^{128}o 340 sextillones) nos hace pensar en cuán grande es dicho número y la infinitesimal probabilidad de que se agoten.

2.3.1. Características IPv6

Entre las características que se pueden resaltar de IPv6 tenemos [4]:

- Mayor capacidad en direccionamiento: se cambia el tamaño de la dirección IP de 32 bits a 128 bits.
- Simplificación del formato de la cabecera: se eliminaron varias opciones poco utilizadas.
- Autoconfiguración: cada host o interfaz puede obtener una dirección IP o parte de ella automáticamente.
- Seguridad: es compatible con IPSec permitiendo cifrado, autenticación e integridad de la información, ya que su uso es obligatorio.

2.3.2. Estructura del paquete IPv6

El paquete IPv6 se encuentra formado por dos partes, tal como se muestra en la figura 2.1, los primeros 40 bytes es donde se encuentra la cabecera y los siguientes 64KB corresponden a la carga útil o datos. En ocasiones el paquete IPv6 puede tener cabeceras adicionales las cuales tienen un tamaño máximo de 40 bytes por lo que el paquete se divide en tres partes principales: cabecera, cabeceras adicionales y datos. La gran mayoría de

mejoras que se han implementado en IPv6 son debido a los cambios en la cabecera.

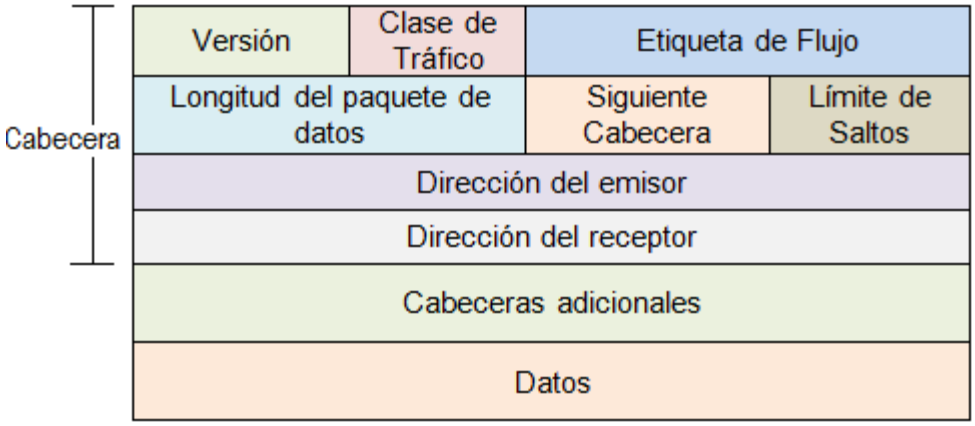


Figura 2.1 Estructura del paquete IPv6

2.3.3. Formato de la dirección IPv6

La dirección IPv6 está compuesta por 8 grupos de 16 bits cada uno separados por ":" en formato hexadecimal, haciendo un total de 128 bits. Se añadieron tres reglas principales para simplificar su escritura, las cuales se detallan a continuación:

- No existe distinción entre mayúsculas y minúsculas.
- Los 0's a la izquierda se pueden omitir.
- Una sucesión de 0's en varios grupos puede ser representado por "**::**", pero solo se podrá aplicar esta regla una sola vez.

Los bits principales en la dirección definen el tipo específico de la dirección IPv6. El campo de longitud variable que contiene estos bits principales se denomina un prefijo de formato y dividen una dirección de unidifusión de IPv6 en dos partes. La primera parte contiene el prefijo de dirección y la segunda parte contiene el identificador de interfaz. Una manera concisa de expresar una dirección IPv6 o una combinación de prefijo es la siguiente: dirección IPv6 /longitud de prefijo [5]. En IPv6 encontramos tres tipos de direcciones: unicast, anycast y multicast.

2.3.4. Mecanismos de configuración de direcciones

Existen tres métodos para la asignación de direcciones IPv6:

- Manual: se configura manualmente la dirección IPv6 y se asigna a la respectiva interfaz.
- Autoconfiguración sin estado: para este tipo de configuración se usa el Protocolo ND, el cual identifica los enrutadores conectados entre sí.
- DHCPv6: también llamado autoconfiguración con estado; el servidor DHCPv6 envía mensajes que contienen la dirección

IPv6, servidor DNS, entre otros parámetros que hayan sido configurados previamente para que los clientes lo reciban.

2.3.5. Enrutamiento IPv6

La configuración de rutas estáticas nos permite el envío y recepción de paquetes entre dos extremos de la red pero no existen actualizaciones automáticas cuando la topología sufre un cambio. En la figura 2.2 mostramos un ejemplo para el uso de rutas estáticas. Al no usar un protocolo de enrutamiento para poder realizar el envío de paquetes entre PC1 y PC2 se configura en cada uno de los enrutadores R1 y R2, rutas estáticas para poder alcanzar dichos destinos mediante el comando *ipv6 route.*

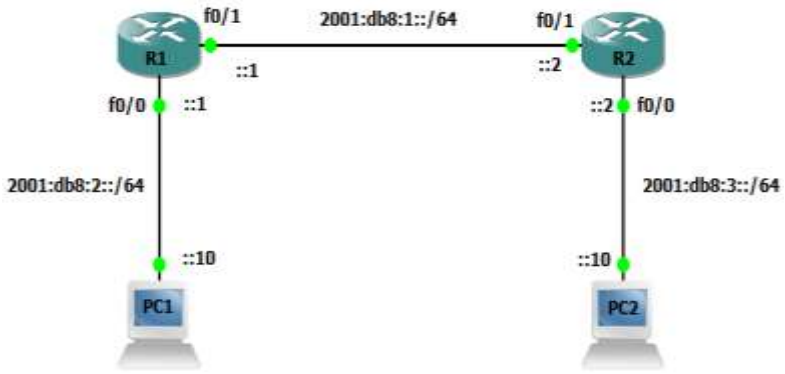


Figura 2.2 Topología básica para rutas estáticas

RIPng es un IGP que se limita a redes en las cuales el recorrido de sus paquetes no excede los 15 saltos. La publicación de RIPng se dio en 1997 gracias a la IETF en el RFC 2080 [6]. La figura 2.3 muestra el formato general de una actualización RIPng, cada entrada corresponde a un destino de red. Los campos de una RTE se muestran en la figura 2.4.

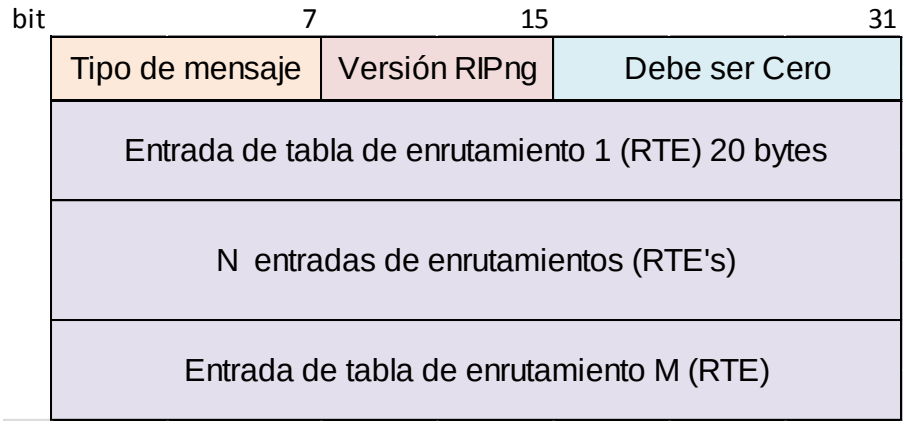


Figura 2.3 Formato general de un mensaje RIPng

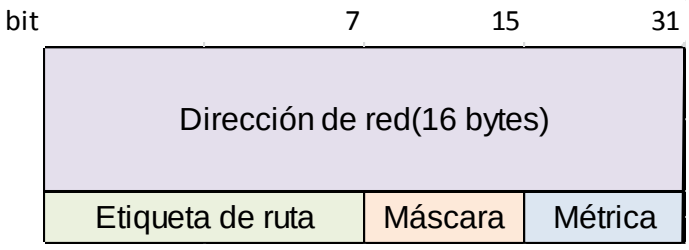


Figura 2.4 Cabecera de una entrada de enrutamiento (RTE)

EIGRP es un protocolo de enrutamiento dinámico que escoge la mejor ruta hacia un destino, basado en DUAL, que emplea las características de cada uno de los enlaces como ancho de banda, retraso, confiabilidad, carga y unidad máxima de transmisión [7]. Existen tres tipos de mensajes EIGRP:

- Mensaje de saludo: necesarios para descubrir a los nodos conectados directamente y conocer acerca de sus estados de enlace.
- Mensajes de actualización: incluyen información relacionada al enrutamiento; se envían cuando una red empieza a operar o sufre algún cambio.
- Mensajes de consulta y respuesta: usado para la búsqueda de redes y posterior análisis con el algoritmo DUAL; una consulta puede ser enviada como unicast o multicast, pero una respuesta solo como unicast al equipo solicitante.

Para el cálculo de la métrica EIGRP se utiliza: ancho de banda, retraso, confiabilidad y carga, aunque la métrica predeterminada solo utiliza los dos primeros. Para el balanceo de carga EIGRP distribuye el envío de datos por las rutas con igual costo, esto quiere decir que un paquete es dividido en partes y estas son enviadas por

diferentes vías, hasta encontrase en un determinado nodo. DUAL establece el concepto de sucesores, siendo un sucesor el mejor vecino para llegar a un destino, a este se encuentra ligada una distancia factible que es la métrica. Otro concepto utilizado es el de sucesor factible que es otro vecino alternativo para el mismo destino, a él está ligada una distancia notificada, la cual es la métrica del vecino hacia dicho destino. Un enrutador puede ser un sucesor factible si su distancia notificada es menor a la distancia factible [8]. DUAL proporciona rutas sin bucles, convergencia rápida y uso mínimo de ancho de banda y este se procesará cuando inicie EIGRP o cuando la topología sufra algún cambio.

OSPFv3 es un protocolo de enrutamiento de estado de enlace con soporte para IPv6, el cual está definido en el RFC 5340, usa el algoritmo Dijkstra SPF para seleccionar el mejor camino entre dos nodos. OSPFv3 es un protocolo usado a nivel de empresas como una solución para el enrutamiento en redes de gran tamaño, usa como métrica el costo de cada enlace, generalmente se emplea el ancho de banda. El tamaño de la cabecera es de 16 bytes. Los tipos de paquetes que maneja OSPFv3 son:

- Saludo: sirve para formar adyacencias entre enrutadores vecinos.
- Descripción de la base de datos: se envía la base de datos de estado de enlace del enrutador emisor para que el receptor la compare con la que posee y pueda construir su base de datos topológica.
- LSR: sirve para solicitar información adicional o faltante para que un enrutador arme su base de datos topológica.
- LSU: respuesta para los LSR y para comunicar cambios en la topología de red a sus enrutadores vecinos.
- LSA: confirmación de recepción de un LSU.

En el algoritmo SPF los enrutadores reciben las LSA por parte de sus vecinos, las cuales se almacenan en una base de datos que se actualiza periódicamente. Cuando un enrutador ya ha recibido todas las LSA's crea un árbol SPF usando el algoritmo Dijkstra, para así poder escoger las mejores rutas y completar su tabla de enrutamiento. OSPFv3 implementa el concepto de áreas que se refiere a un conjunto de enrutadores que comparten información, a dicho conjunto se lo identifica mediante un número entero que va desde 0 a 255. Comúnmente las áreas son usadas para segmentar

la topología y no sobrecargar la red con actualizaciones, ya que al aumentar el número de equipos el algoritmo SPF se ejecutará con mayor frecuencia consumiendo más recursos. En cada área se ejecuta su propio SPF por tanto el tiempo de convergencia no se ve afectado. Según su funcionalidad dentro de la red existen los siguientes tipos de áreas:

- Área de núcleo: conocida como área 0, a ella se conectan las demás áreas y contiene enrutadores con suficientes recursos tanto en memoria y CPU, ya que manejan el tráfico que fluye por toda la red.
- Área stub: no tiene conocimiento de las rutas externas, es usada para enrutadores con poca CPU para no sobrecargarlo con actualizaciones.
- Área Totally stubby: es usada en espacios con pocos usuarios que no necesitan conectarse constantemente con el exterior.
- Área NSSA (Not-So-Stubby-Area): son usadas para conectarse con un ISP o aun AS que ejecuta un protocolo de enrutamiento diferente.

Cada enrutador de la topología tiene una función determinada y son clasificados de la siguiente manera: enrutadores de núcleo, enrutadores internos, enrutadores de borde y enrutadores de límite de sistema autónomo. En la figura 2.5 se muestran los distintos tipos de enrutadores y áreas.

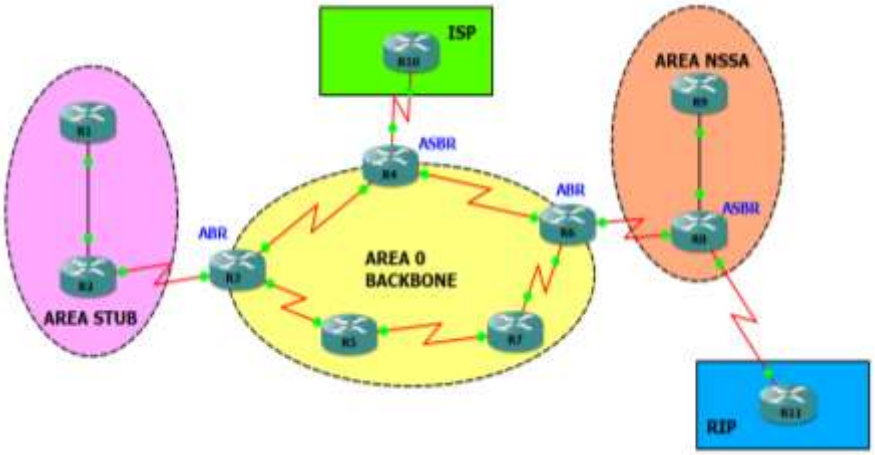


Figura 2.5 Topología con distintos tipos de áreas y enrutadores

OSPFv3 es un protocolo de estado de enlace, por tanto se anuncian todas sus conexiones y si un enlace deja de funcionar envían LSA's a sus vecinos, las cuales se propagan por toda la red para que se actualicen las tablas de topología que posee cada enrutador. Los enrutadores llegan a su punto de convergencia cuando todos poseen la misma tabla de topología y en ese instante comienza la función de SPF para calcular la mejor ruta hacia los destinos. Las

tablas de topologías son actualizadas mediante LSA's que envían los enrutadores dentro de una misma área. Para formar adyacencias, OSPFv3 envía periódicamente cada 10 segundos mensajes de tipo "hello" a todos sus vecinos conectados directamente para redes multiacceso y punto a punto, estos mensajes son enviados por la dirección multicast FF02::5.

IS-IS es un protocolo de estado de enlace creado para el modelo OSI y diseñado para competir con el protocolo TCP/IP pero no obtuvo la ventaja que se esperaba. IS-IS es usado en su mayoría por ISP's y en países desarrollados como EEUU es usado por el gobierno. En IS-IS los enrutadores pertenecen a una sola área y cada enrutador es configurado globalmente con la respectiva área. En este protocolo se manejan dos niveles, L1 que corresponde a los enrutadores que se encuentran agrupados en un área y solo conocen las rutas internas de dicha área, a su vez tenemos el nivel L2 donde se encuentran los enrutadores conectados al núcleo y manejan el tráfico entre áreas. También tenemos los enrutadores de nivel L1-L2 que son los encargados de conectar las áreas con el núcleo. Los enrutadores que participen dentro del proceso IS-IS se

les debe configurar una dirección ISO la cual tiene una longitud variable de 8 a 20 bytes y puede ser de dos tipos: NSAP o NET. Las direcciones ISO están conformadas por tres partes:

- Área: utilizado en el enrutamiento nivel 2 entre áreas. Su tamaño va desde 1 a 13 bytes.
- Identificador: utilizado en el enrutamiento nivel 1 para hosts. Su tamaño es de 6 bytes, generalmente se usan direcciones MAC o direcciones IP aumentándoles “0”.
- SEL: utilizado en el enrutamiento hacia una aplicación en un dispositivo final. Su tamaño es un byte.

Las direcciones ISO se diferencian principalmente por el valor del campo NSEL, si tiene el valor 0x00 corresponde al tipo NET caso contrario será NSAP. En figura 2.6 se muestra la estructura de las direcciones ISO.

<table>
<tr><td colspan="2">IDP</td><td colspan="3">DSP</td></tr>
<tr><td>AFI</td><td>IDI</td><td>DSP de orden alto (HODSP)</td><td>ID del Sistema</td><td>NSEL</td></tr>
<tr><td colspan="2">Tamaño variable</td><td>6 Bytes</td><td>1 byte</td></tr>
<tr><td colspan="2">Area</td><td>ID del Enrutador</td><td>00</td></tr>
<tr><td colspan="2">49</td><td>001</td><td>222033304440</td><td>00</td></tr>
</table>

Figura 2.6 Estructura de una dirección ISO

Existen tres tipos de mensajes IS-IS:

- Saludo: sirven para formar adyacencias con los enrutadores vecinos.
- Estado de enlace: son enviados por enrutadores del mismo tipo, tanto nivel 1 y 2, contienen información de las redes que pueden alcanzar los enrutadores de nivel 2 y respectivos vecinos.
- Número de secuencia: su función es mantener la base de topología sincronizada entre vecinos, a su vez se encarga de los acuses de recibo de los LSP's y solicitándolos.

Cuando IS-IS entra en funcionamiento los enrutadores envían LSP's por sus interfaces y así distribuyen los prefijos, cada enrutador que recibe estas actualizaciones las reenvía excepto por donde la recibió. Si los LSP que se reciben son diferentes a los que ya tiene en su base de datos de estado de enlace son agregados, caso contrario se descartan. Una vez sincronizadas las bases de datos, SPF comienza a calcular las mejores rutas y la tabla de topología. En el momento en que un enrutador recibe un paquete con dirección de destino de otra red, se busca dicha red en la tabla de enrutamiento, mediante la dirección ISO el enrutador extrae la parte

que pertenece al área, de ser la misma área que el enrutador que la recibió, se usa la base de datos de nivel 1 y se reenvía el paquete hacia la red correcta. Por el contrario si el destino es un área diferente y el enrutador que recibió el paquete es de nivel 1, se reenvía hacia un enrutador de nivel 2 y en el caso en que el enrutador sea de nivel 2 usa la tabla de topología. Es importante que este procedimiento se base en la dirección ISO del paquete. IS-IS soporta cuatro valores para la métrica pero solo uno de ellos es soportado por equipos CISCO llamado costo, lo coloca en todas sus interfaces y el valor predeterminado es 10. Todos los enrutadores que utilicen IS-IS soportan esta métrica. Adicionalmente tenemos los tres parámetros restantes usados en equipos diferentes a CISCO: retraso en la transmisión, costo de la red y confiabilidad del enlace.

2.3.6. Extensiones adicionales IPv6

El uso de las cabeceras adicionales es opcional y van colocadas luego de la cabecera fija. Para organizar su aplicación se usa el campo “Siguiente Cabecera”. En caso de ser la última apuntan a una cabecera de transporte [9]. Los encabezados de extensión son los siguientes:

- Hop by Hop Options: es procesado por cada enrutador que reenvía el paquete a lo largo de su trayectoria. Su identificador es el 0NH y es de longitud variable.
- Routing: es de gran utilidad ya que le indica al paquete cual es el camino que debe atravesar y por cuales enrutadores pasar. Su identificador es el 43NH y es de longitud variable.
- Fragment: se usa cuando se envía un paquete que supera la unidad máxima de transferencia, este deberá ser fragmentado y así una vez que todas las partes del paquete lleguen al destino serán unidas para formar el paquete original. Su identificador es el 44 NH y es de longitud fija (64 bits).
- Destination Options: posee el campo “Opciones” en el que se especifica información que solo será analizada por el nodo de destino al que va dirigido el paquete. Su identificador es el 44 NH y es de longitud variable.
- Authentication Header (AH) y Encapsulating Security Payload (ESP): estos encabezados adicionales tienen como función cuidar la integridad y autenticación de los datos, por tanto será explicada en el capítulo 2.5 destinado a seguridad.

- Sin Cabecera Adicional: si el campo NH tiene como valor 59 indica que ya no existe una cabecera después de la actual.

2.3.7. Requerimientos de software y hardware

Para hacer un buen diseño de una red, entre los factores más relevantes tenemos el software y hardware, ya que en base a ellos y sus características deberán implementarse las funcionalidades que vayamos a necesitar. Para nuestro proyecto en cuanto a software podemos referirnos básicamente al IOS que se usará en los enrutadores y la aplicación que nos ha ayudado a emular todas las topologías, en este caso, GNS3. Lo necesario para que el IOS que utilizamos en las pruebas funcione correctamente en un entorno IPv6 es: BGP, BGP4, DHCP - DHCPv6, IPv6 Routing - EIGRP Support, IPv6 IS-IS, IPv6 BGP, IPv6 OSPF e IPv6 RIP.

2.4. Topología de Redes

Las topologías de redes según la conexión de sus equipos se clasifican en: Broadcast, Punto a Punto y NBMA, siendo esta última la que utilizaremos en nuestras pruebas.

2.5. Seguridad IPv6

IPv6 acoge al conjunto de métodos de seguridad con el nombre de IPsec. IPsec es el protocolo de seguridad de IP, en el caso de la versión 6 este es intrínseco.

2.5.1. Mecanismos de Seguridad

La sección de seguridad destinada a la autenticidad se denomina cabecera de autenticación. La AH es una de las características especiales de IPv6, ubicada entre la cabecera IPv6 y la parte de datos del datagrama, su identificador es 51 y su tamaño es de 12 bytes, la misma dispone de 5 campos designados para la autenticación de datos, los cuales se muestran en la figura 2.7. Para cifrar los datos IPv6 implementa ESP. Esta cabecera se muestra en la figura 2.8. La ESP siempre se encuentra al final, los datos que se encuentren posteriores a la ESP corresponderán a los autentificados y cifrados.

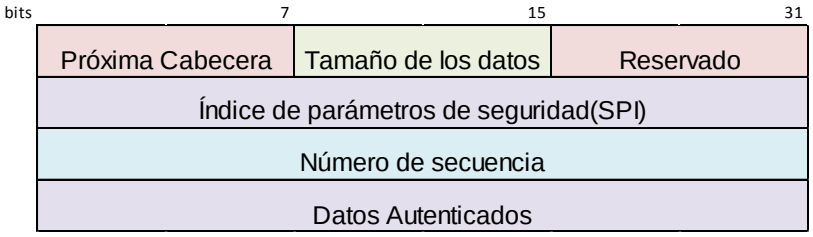


Figura 2.7 Esquema de la cabecera de autenticación

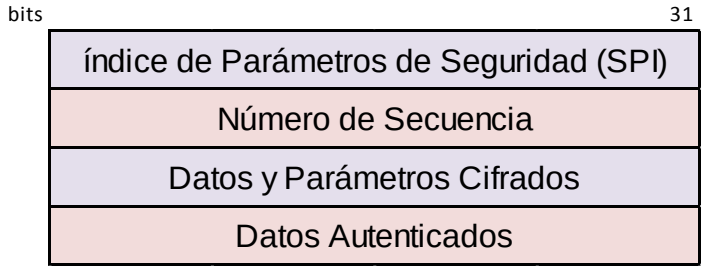


Figura 2.8 Esquema de cabecera de cifrado ESP

2.5.2. Administración de contraseñas

Se sugieren ciertos parámetros a la hora de creación de contraseñas, uno de ellos es la longitud (mínimo 10 y máximo 25 caracteres). También se recomienda la combinación de letras, números y caracteres especiales.

2.5.3. Aplicación

Las aplicaciones de seguridad en IPv6 tienen una gran variedad de utilidades gracias a IPsec, la designación de un nodo que actúe como la primera barrera de seguridad para los datos que provienen de destinos fuera de la red es un método muy empleado en IPv4 y se mantiene para redes IPv6, puesto que proporciona un alto nivel de seguridad.

2.6. Multihoming

Una organización no se pueden dar el lujo de estar incomunicada, ya sea con la intranet o hacia Internet, para lo cual se hace imprescindible tener un alto porcentaje de disponibilidad, la cual se da en resumen conectándonos a más de un ISP, a esto se le llama Multihoming.

2.6.1. ISP

Un ISP es una organización dedicada a brindar conexión hacia Internet para usuarios residenciales o corporativos, además ofrece servicios como asignación de dominios, IP públicas, enlaces dedicados, cuentas de correo electrónico y en algunos casos mantenimiento e instalación de equipos y servicios de telecomunicaciones [10].

2.6.2. BGP-4

BGP-4 es la versión del protocolo BGP con soporte para IPv6. Este es un EGP cuya función es enrutar el tráfico entre AS de diferentes dominios, es decir dirigir el tráfico hacia dicho AS para que luego el IGP sea el encargado de llevar hasta el destino específico los paquetes dentro del AS.

2.6.3. Multihoming

Multihoming es la conexión de un sistema autónomo u organización hacia dos o más ISP's con el fin de estar siempre conectado a Internet, ya que si uno de los proveedores falla, inmediatamente entra en funcionamiento otro, o a su vez ambos están en funcionamiento al mismo tiempo. Se debe contratar un número de sistema autónomo y a su vez un prefijo independiente de los ISP's, los cuales son otorgados por los RIR's.

2.7. Análisis para el Diseño

Para optimizar el rendimiento de los IGP's se sugiere aplicar interfaces pasivas, resumen de rutas y modificación de valores de temporizadores. En RIPng es recomendable mantener la relación entre los temporizadores la misma que se muestra en la tabla I.

Tabla I Múltiplos de temporizadores recomendados

Temporizador	Múltiplo	Tiempo por Omisión IP-RIPng(Segundos)
Actualización	Base	30
Invalidez	3*actualización	180
De Espera	3*actualización	180
Eliminación de Ruta	Mayor que el de invalidez	240

En EIGRP los enrutadores stub’s se utilizan para enviar información mínima hacia un solo vecino. Los candidatos para enrutadores Stub se muestran en la figura 2.9.

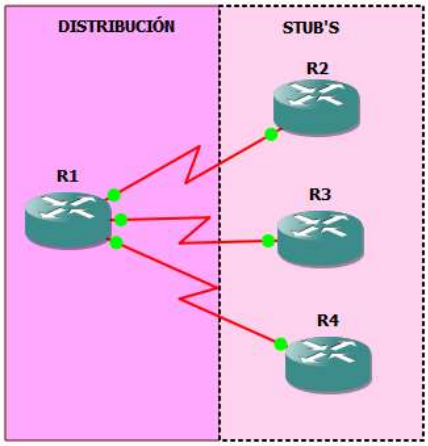


Figura 2.9 Representación de enrutadores STUB’s

Para OSPFv3 existen recomendaciones en cuanto al número de equipos que deben ser usados en cuanto a dispositivos CISCO se refiere:

- 40 - 50 enrutadores por Área
- 50 - 60 vecinos por enrutador
- 3 Áreas por enrutador

Para que IS-IS funcione de manera correcta, se deben tener en cuenta las siguientes reglas de resumen:

- Los enrutadores nivel 1-2 pueden resumir rutas dentro de su área. Las rutas resumidas se propagan a los enrutadores nivel 2.

- Si un enrutador nivel 1-2 tiene configurada el resumen de rutas, se tiene que configurar en los demás enrutadores nivel 1-2 para enviar las actualizaciones a los enrutadores nivel 2.
- Los enrutadores nivel 1 no pueden resumir rutas dentro del área porque el protocolo de enrutamiento no lo permite.

CAPÍTULO 3

3. DISEÑO DE LAS TOPOLOGÍAS DE RED

Luego de haber revisado el marco teórico estamos listos para el diseño de una topología estándar en todos los IGP's, la misma que guardará configuraciones idénticas a nivel general y similares para cada protocolo de enrutamiento en específico, de tal manera que se puede realizar una comparación en cuanto a características como convergencia, confiabilidad y escalabilidad.

3.1. Dispositivos Que Conforman La Red

Un enrutador conecta múltiples redes, razón por la cual posee varias interfaces, como lo son seriales o Ethernet. Esto permite que el enrutador recepte un paquete IP por una de sus interfaces, lo procese y elija cual es la mejor interfaz de salida, bien sea a su destino final o a otro enrutador, de ahí el nombre de enrutamiento o encaminamiento. En nuestro

proyecto utilizamos los conmutadores como simples mecanismos de distribución dentro del rango de direcciones LAN que se otorga. De igual forma los dispositivos terminales pueden ser equipos móviles u ordenadores.

3.2. Esquema lógico de la red

La topología que se muestra en la figura 3.1 será objeto de las configuraciones básicas generales previo a la configuración de cada uno de los protocolos de enrutamiento.

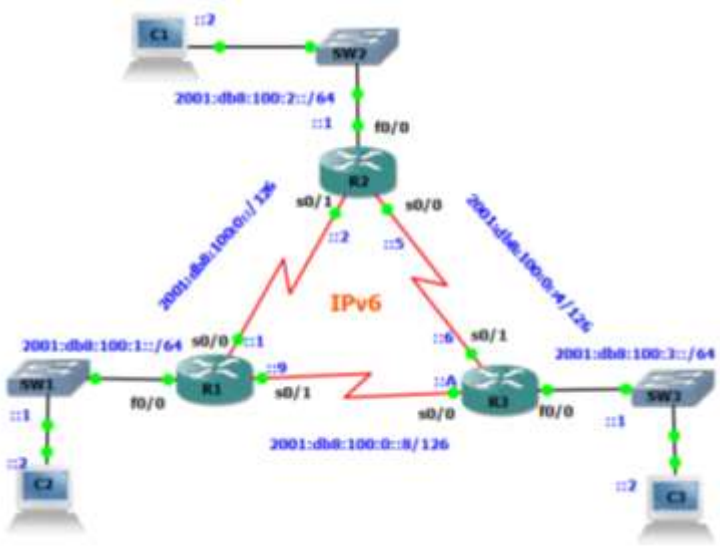


Figura 3.1 Topología de red para el esquema lógico de nuestra red

El direccionamiento IPv6 quedaría conformado como podemos apreciar en la tabla II. Los comandos necesarios para las configuraciones generales para cada IGP se encuentran en el anexo III.

Tabla II Direccionamiento IPv6

Disp.	Interfaz	Dirección IPv6	Puerta de enlace predeterminada
R1	Fa0/0	2001:db8:100:1::1/64	---
	S0/0	2001:db8:100:0::1/126	---
	S0/1	2001:db8:100:0::9/126	---
R2	Fa0/0	2001:db8:100:2::1/64	---
	S0/0	2001:db8:100:0::5/126	---
	S0/1	2001:db8:100:0::2/126	---
R3	Fa0/0	2001:db8:100:3::1/64	---
	S0/0	2001:db8:100:0::A/126	---
	S0/1	2001:db8:100:0::6/126	---
C1	---	2001:db8:100:2::2/64	2001:db8:100:2::1/64
C2	---	2001:db8:100:1::2/64	2001:db8:100:1::1/64
C3	---	2001:db8:100:3::2/64	2001:db8:100:3::1/64

3.3. Esquema físico de las conexiones de red

Se utilizó la misma topología en todos los IGP's para poder evaluar de mejor manera el funcionamiento de cada uno. El enrutador usado en las pruebas en GNS3 pertenece a la serie Cisco 3700, las características y especificaciones del enrutador se encuentran en el anexo II. También se utilizó un conmutador Ethernet de 8 puertos. El requisito indispensable en los ordenadores, ya sean de escritorio o portátiles, es que su tarjeta de red tenga soporte para IPv6.

3.4. Descripción de usos de protocolos de enrutamiento

La implementación de los protocolos de enrutamiento dependió de factores como escalabilidad, confiabilidad y convergencia, que sin duda están ligados a otros factores como los recursos monetarios que se dispone para la instalación, monitoreo y mantenimiento. La solución más económica para la implantación de un sistema de computadores conectados en red en IPv6 es RIPng. EIGRP es preferido por los ISP's para redes públicas y privadas, grandes o medianas organizaciones, a pesar de ser propiedad de CISCO. Por otra parte OSPFv3 e IS-IS al igual que RIPng son protocolos soportados por la mayoría de fabricantes. IS-IS se diferencia de OSPFv3 en aspectos de diseño.

3.5. Comandos para las configuraciones de los dispositivos

Los comandos utilizados en todas nuestras prácticas se han resumido en forma ordenada en el anexo III.

3.6. Diseño de pruebas

Para la comparación entre IGP's se diseñaron pruebas de convergencia, confiabilidad y escalabilidad, las mismas que se describen a continuación.

3.6.1. Pruebas de convergencia

Para medir tiempo de convergencia probaremos con los siguientes escenarios:

- *Convergencia luego de la caída de un enlace:* simulamos la caída de un enlace, utilizando el comando “shutdown” en la interfaz y luego comenzamos a verificar mediante las depuraciones el tiempo que se tardó el equipo en actualizar por última vez la tabla de enrutamiento.
- *Convergencia luego de la subida de un enlace:* utilizamos el comando “no shutdown” para levantar nuevamente la interfaz y simular la subida del enlace.
- *Convergencia inicial:* realizamos pruebas simulando el inicio de la ejecución del protocolo de enrutamiento para conocer el tiempo que toma en iniciar y estabilizarse, para esto utilizaremos los comandos clear de cada IGP.

Nosotros utilizamos las depuraciones propias de IPv6 para obtener los tiempos de convergencia para cada uno de los protocolos. Tomando como datos el tiempo desde que la interfaz cambio de estado o se reinició el protocolo y la última actualización en la tabla de enrutamiento, la diferencia de estos tiempos nos otorga el tiempo

de convergencia. En la tabla III se listan los comandos relacionados a las depuraciones que usaremos en las pruebas de convergencia.

Tabla III Comandos de depuraciones enrutamiento IPv6

Comando	Función
debug ipv6 routing	Depuración de eventos de tabla de enrutamiento
debug ipv6 interface	Depuración de eventos en la interfaz
debug ipv6 rip	Depuración de eventos RIPng
debug ipv6 eigrp	Depuración de eventos EIGRP
debug ipv6 ospf events	Depuración de eventos OSPFv3
debug isis adj-packets	Depuración de eventos ISIS

Para medir la convergencia de una red utilizamos dos depuraciones básicas, la primera utilizando el comando *debug ipv6 interface*, el cual nos indica el tiempo exacto en que falló un enlace. Habilitando la depuración de los eventos afines a la tabla de enrutamiento podemos determinar el tiempo en que ésta se ha completado mediante el comando *debug ipv6 routing.* Mediante la topología de la figura 3.1 mediremos la convergencia para los IGP's y el direccionamiento estará dado según la tabla II.

3.6.2. Pruebas de confiabilidad

Las pruebas de confiabilidad que realizamos buscan medir el porcentaje de paquetes enviados versus los recibidos y así tener un

valor real de la confiabilidad en cada uno de los protocolos. En todas las topologías que vamos a diseñar para realizar pruebas de confiabilidad tenemos redundancia en los enlaces, es decir, si algún enlace sufre una caída durante la transmisión de datos existirá otro camino por el cual puedan viajar los datos restantes, teniendo así pérdidas de paquetes hasta que el protocolo actualice este cambio en sus tablas luego que transcurra el tiempo de convergencia. Esta prueba consiste en enviar un ping de gran tamaño entre dos dispositivos finales, en este caso serán dos ordenadores y durante la transmisión deshabilitar una interfaz mediante el comando “shutdown” y al final de la transmisión obtener el número de paquetes enviados, recibidos y perdidos, obteniendo así un porcentaje de confiabilidad. Para estas pruebas se diseñaron topologías específicas según la clasificación de los IGP’s, es decir, por vector distancia y estado de enlace, las mismas que se muestran en el anexo III junto con los comandos necesarios para las configuraciones específicas de cada protocolo de enrutamiento.

3.6.3. Pruebas de transferencia de datos

Utilizamos por cada tipo de protocolo las mismas topologías usadas en las pruebas de confiabilidad, figuras 3.2 y 3.3 para vector de distancia y estado de enlace respectivamente. Procedimos a enviar un archivo de aproximadamente 10 MB entre dos dispositivos finales en cada una de las dos topologías para tomar el tiempo de descarga y su tasa de transferencia, para esto nos ayudamos con el software FILEZILLA el cual es un servidor FTP. En todas nuestras topologías tenemos dos ordenadores como dispositivos finales, en uno instalaremos Filezilla Server y en el otro Filezilla Cliente. Los mensajes obtenidos que nos registró el cliente una vez que ha finalizado la descarga fueron usados para calcular la tasa de transferencia en base a la ecuación 1. Este procedimiento lo seguiremos para el cálculo de la tasa de transferencia de cada archivo en todos los IGP's.

$$\boldsymbol{Tasa\ de\ transferencia} = \frac{Tamaño\ del\ archivo}{Tiempo\ de\ descarga}\left[\frac{bytes}{segundos}\right] \qquad (1)$$

3.6.4. Pruebas de escalabilidad

Por motivos de limitante de recursos estas pruebas se realizaron solo con el emulador GNS3 y el objetivo principal fue comprobar el tope máximo de escalabilidad en RIPng. Para los protocolos EIGRP,

OSPFv3 e IS-IS se llegó a realizar la prueba hasta con 20 enrutadores ya que al ser una emulación dependíamos del consumo de recursos del software usado. En la figura 3.4 se muestra la topología que se usó para demostrar las limitaciones de RIPng.

Figura 3.2 Topología para medir escalabilidad en RIPng

3.6.5. Pruebas estadísticas

Los datos que arrojen cada una de las pruebas de convergencia y confiabilidad serán tabulados para poder comparar los IGP's y obtener resultados que sustenten por qué un protocolo de enrutamiento prevalece sobre otro. La ecuación 2 nos permite calcular el número mínimo de observaciones que deben efectuarse;

dónde n es el número mínimo de observaciones, W el rendimiento mínimo esperado, Z_β poder estadístico y Z_α nivel de confianza asignado.

$$n = \frac{W - W^2[Z_\beta + 1.4\,(Z_\alpha)]^2}{W^2} \qquad (2)$$

Para nuestro proyecto hemos decidido tomar los siguientes valores: nivel de confianza (1-α) 99%, diferencia mínimo observable (W) 30% y Poder estadístico (1-β) 80%. Usando estos valores, la ecuación 2 queda de la siguiente manera:

Z_α = 2,576 **Z_β =** 0,842 **W =** 0,30

$$n = \frac{0{,}30 - 0{,}30^2[0{,}842 + 1.4\,(2{,}576)]^2}{0{,}30^2} = 47$$

Tenemos como resultado que el número mínimo de observaciones debe ser 47 por tanto éste será aplicado para cada una de las pruebas y posterior tabulación de datos. Una vez que hemos tomado el número de observaciones suficientes procedemos a la aplicación de estadística descriptiva.

CAPÍTULO 4

4. IMPLEMENTACIÓN, PRUEBAS Y ANÁLISIS DE RESULTADOS

Una vez hecho el diseño de cada una de las topologías para las respectivas pruebas, en este capítulo procedimos a su implementación, obtención de resultados y la valoración de los mismos para realizar la comparación entre los tipos de protocolo de enrutamiento.

4.1. Comparación de alternativas de equipamientos

Tenemos marcas como CISCO, de origen estadounidense, se dice que el 50% del tráfico de datos a nivel mundial pasa por equipos de esta marca. Una de las competencias más fuertes de CISCO en Europa es JUNIPER, de nacionalidad estadounidense con sede en California, también dedicada a la venta de equipos de telecomunicaciones con una gran variedad en todos los equipos. Para este estudio comparamos las marcas

CISCO y JUNIPER, ya que son las más influyentes en el mercado mundial de redes de datos. Nosotros estudiamos las características de la serie M7i de JUNIPER ya que será comparado con el enrutador CISCO de la serie 3700, los cuales ofrecen características similares.

4.2. Análisis de costos de implementación y soporte

Se debe mencionar que el equipo CISCO 3725 es un enrutador que tiene bastante tiempo en el mercado, lo que hace que su precio no sea el mismo cuando apareció, como no ocurre con el enrutador JUNIPER M7i, el cual tiene poco tiempo lanzado al mercado. Se trató en la medida de lo posible obtener los precios más cercanos a lo real cuando ambos equipos salieron a la venta. Los precios del equipo JUNIPER supera en más del 100% el precio del equipo CISCO, lo cual otorga ventajas al equipo CISCO en caso de que se requiera la compra del mismo.

4.3. Justificación de selección de equipos

Una vez analizado ambos equipos, tanto en la parte de infraestructura, software y demás funcionalidades, hemos decido que el equipo para ser usado en nuestro proyecto sería el CISCO 3725. Entre los motivos más fuertes para decidirnos se encuentran los conocimientos previos de su

uso en nuestra carrera universitaria tanto físicamente como en su configuración, mayores funcionalidades que requerimos, entre esas EIGRP por ser un protocolo propietario de CISCO. Contamos con disponibilidad del equipo, ya que actualmente tenemos la facilidad de su uso en los laboratorios de ESPOL. Una comparación más detallada se puede apreciar en el anexo II.

4.4. Instalación y configuración de dispositivos

La instalación de equipos consistirá en reconocer el hardware que disponemos en los laboratorios para cada una de las prácticas que realicemos, así como el software que alojan los mismos (IOS).El Laboratorio CISCO ubicado en ESPOL-Peñas fue donde realizamos nuestras prácticas. En promedio estos salones cuentan con 20 ordenadores con sistema operativo Windows 7 de 32 bits, procesador Dual Core, disco duro de 500 gigabytes y memoria RAM de 2 gigabytes. Tenemos también 4 armarios de conmutación y enrutamiento que cuentan con 3 enrutadores, 3 conmutadores y un equipo Firewall. Estos enrutadores pertenecen a la familia 2800 y 1800, cuyas especificaciones técnicas las podremos consultar en el anexo II.

4.5. Análisis de envío y recepción de paquetes IPv6

En la topología básica que se muestra en la figura 3.1 se realizó un ping hacia la red 2001:db8:100:3::/64 desde R1, dicho ping tendrá de tamaño 1000 bytes y se repetirá 500 veces y el mismo se realizará para los cuatro protocolos de enrutamiento estudiados, RIPng, EIGRP, OSPFv3 e IS-IS. Mediante el uso del comando *tclsh* podremos ejecutar pings hacia más de un destino, uno a la vez en el orden que colocamos las direcciones IPv6. El ping realizado quedó de la siguiente manera:

ping 2001:db8:100:3::2 size 1000 repeat 500

4.6. Verificación de funcionamiento de la red

Una vez que hemos comprobado la conectividad entre todos los dispositivos que conforman la red, verificamos que el protocolo de enrutamiento esté realizando correctamente sus funciones, para estar seguros que no existirán fallos más adelante que pueden afectar el tráfico de datos. Entre los puntos más importantes a tomar en cuenta para verificar el correcto funcionamiento de un IGP revisamos tablas de enrutamiento, tablas de adyacencias o vecindades, distribución de áreas y conexiones físicas.

4.7. Identificación de ventajas y desventajas

Una de las mayores ventajas de IPv6 es la responsabilidad en la seguridad y por ende de las diversas categorías que esta propiedad encierra, entre ellas la confidencialidad e integridad de datos, a través del método de cabeceras adicionales se pueden implementar protocolos que protegen a un paquete cuando se transporta de un sitio a otro. Otra muy notoria es la cantidad de direcciones disponibles, es una de las principales razones del surgimiento de IPv6. Por último tenemos la característica de fragmentación del paquete en el nodo donde se origina y su unión en el nodo de destino, esta singular característica es denominada Fragmentación end-to-end.

En contrapartida tenemos las desventajas, la principal de ellas es todo el proceso de migración que se debe realizar de IPv4 a IPv6 basados en aspectos como la adquisición de nuevos equipos, así como de software, capacitación de personal, tiempo empleado en este proceso, impacto que causaría en el rendimiento del negocio que se esté llevando, este último uno de los más importantes, debido a que no se puede frenar la operativa de un negocio en un proceso de migración.

4.8. Comparación entre protocolos de enrutamiento de vector distancia

En las pruebas de convergencia luego de la caída de un enlace se obtuvieron los resultados mostrados en la tabla IV. Un valor importante es la media, la cual se ubica en 13,5 segundos. Vemos también que la moda es 7,6 segundos ya que es el valor que más se repitió en la muestra demostrándonos que es el patrón en el tiempo de convergencia. En la figura 4.1 podemos notar que la mayoría de las muestras que se tomaron luego de la caída de un enlace varían dentro de un intervalo de 24,5 segundos.

Tabla IV Estadística Descriptiva de los tiempos de convergencia luego de la caída de un enlace en RIPng

Tiempo de convergencia [s]	
Media	00:00:13,459
Moda	00:00:04,996
Desviación estándar	0,000
Varianza de la muestra	0,000
Mínimo	00:00:02,008
Máximo	00:00:26,684
Cuenta	53

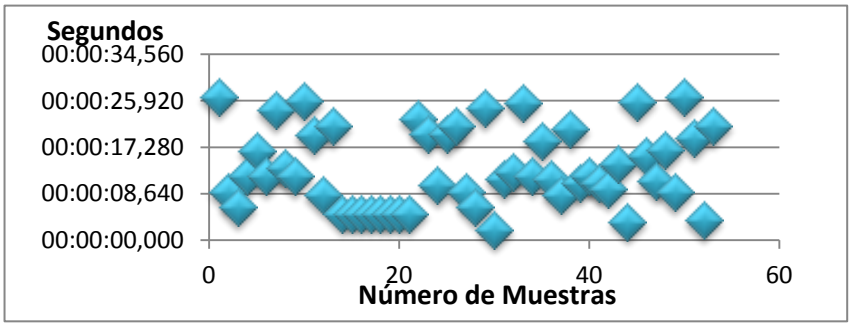


Figura 4.1 Dispersión de los tiempos de convergencia luego de la caída de un enlace en RIPng

En la prueba de convergencia luego de la subida de un enlace obtuvimos los resultados mostrados en la tabla V. La mayoría de las observaciones se encuentran bastante cercanas a la media, razón por la cual junto a la moda bordean los 5 segundos, esto se muestra en la figura 4.2.

Tabla V Estadística descriptiva de los tiempos de convergencia luego de la subida de un enlace en RIPng

Tiempo de convergencia [s]	
Media	00:00:05,012
Moda	00:00:05,004
Desviación estándar	0,000
Varianza de la muestra	0,000
Mínimo	00:00:04,045
Máximo	00:00:05,497
Cuenta	54

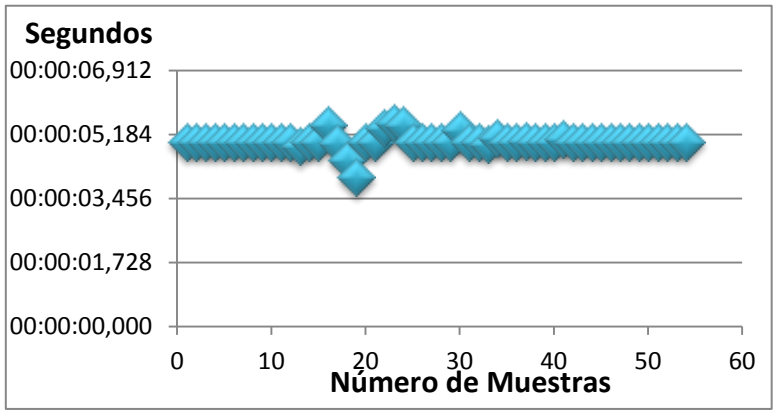


Figura 4.2 Dispersión de los tiempos de convergencia luego de la subida de un enlace en RIPng

Para la prueba de convergencia luego de reiniciar el protocolo se obtuvieron los datos mostrados en la tabla VI. En los tiempos de RIPng para estas pruebas tenemos una media de 17,088 segundos y algunas muestras incluso llegaron a no superar los 10 segundos. La dispersión de los datos se muestra en la figura 4.3.

Tabla VI Estadística de descriptiva de los tiempos de convergencia luego de reiniciar el proceso RIPng

Tiempo de convergencia [s]	
Media	00:00:17,088
Moda	-
Desviación estándar	0,00
Varianza de la muestra	0,00
Mínimo	00:00:03,200
Máximo	00:00:29,572
Cuenta	51

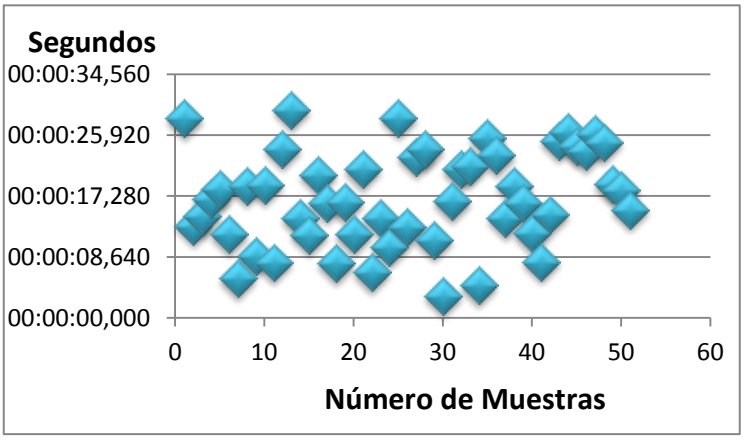


Figura 4.3 Dispersión de los tiempos de convergencia luego de reiniciar el proceso RIPng

Los datos estadísticos del tiempo de convergencia luego de la caída de un enlace para EIGRP se presentan en la tabla VII y su respectiva dispersión en la figura 4.4. Podemos notar que el tiempo de convergencia medio es de 2,057 segundos.

Tabla VII Estadística Descriptiva de los tiempos de convergencia luego de la caída de un enlace en EIGRP

Tiempo de convergencia [s]	
Media	00:00:02,057
Moda	00:00:02,044
Desviación estándar	0,000
Varianza de la muestra	0,000
Mínimo	00:00:00,999
Máximo	00:00:03,414
Cuenta	48

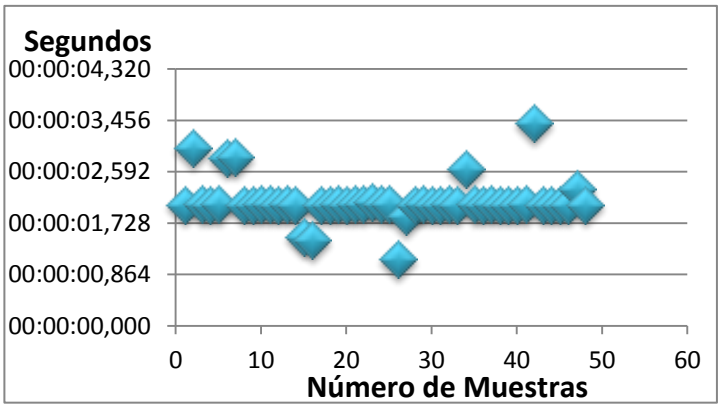


Figura 4.4 Dispersión de los tiempos de convergencia luego de la caída de un enlace en EIGRP

Los resultados de la prueba luego de la subida de un enlace se muestran en la tabla VIII. El valor medio de convergencia es 5,457 segundos. La dispersión de datos se los muestra en la figura 4.5.

Tabla VIII Estadística Descriptiva de los tiempos de convergencia luego de la subida de un enlace en EIGRP

Tiempo de convergencia [s]	
Media	00:00:05,457
Moda	00:00:06,208
Desviación estándar	0,00
Varianza de la muestra	0,00
Mínimo	00:00:04,295
Máximo	00:00:06,371
Cuenta	48

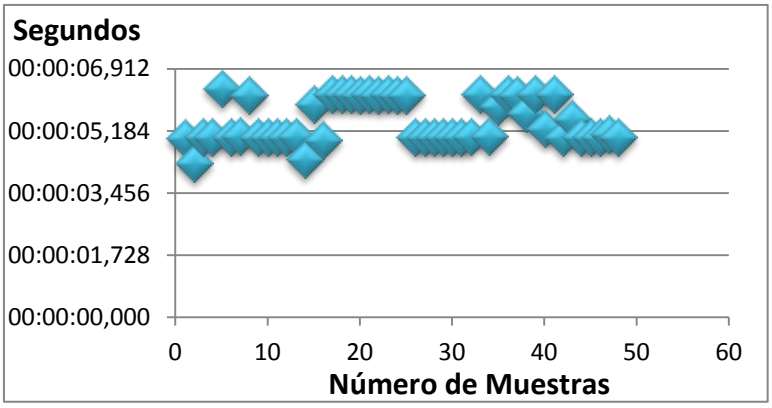


Figura 4.5 Dispersión de los tiempos de convergencia luego de la subida de un enlace en EIGRP

Los resultados al reiniciar un proceso EIGRP se muestran en la tabla XI y su respectiva dispersión en la figura 4.6. En líneas generales la tendencia fue a obtener valores menores que RIPng, tanto así que la media disminuye en aproximadamente 4 segundos.

Tabla IX Estadística Descriptiva de los tiempos de convergencia luego de reiniciar el proceso EIGRP

Tiempo de convergencia [s]	
Media	00:00:13,313
Moda	-
Desviación estándar	0,00
Varianza de la muestra	0,00
Mínimo	00:00:01,260
Máximo	00:00:29,572
Cuenta	51

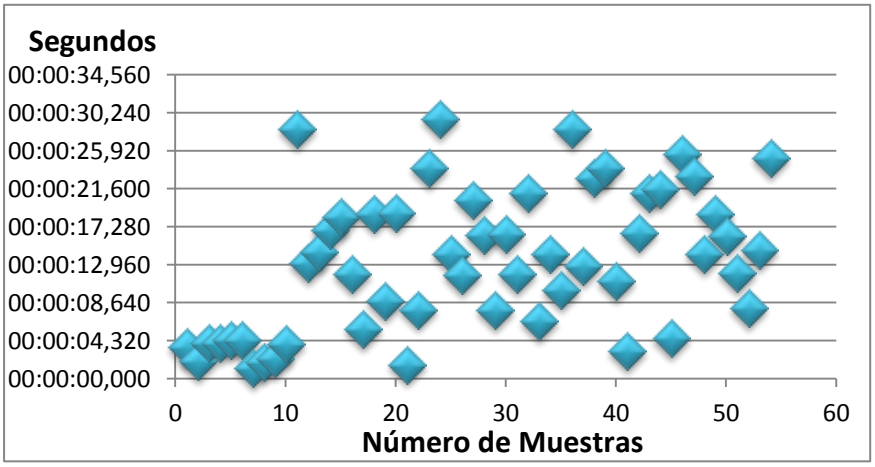


Figura 4.6 Dispersión de los tiempos de convergencia luego de reiniciar el proceso EIGRP

Entre los aspectos importantes para hacer una comparación completa e identificando cada una de las ventajas y desventajas de los protocolos, tenemos los siguientes:

- Tiempo de convergencia: la superioridad de EIGRP se mantiene en nuestras pruebas, en las cuales podemos ver que el tiempo

promedio de convergencia luego de la caída en un enlace es 6 veces menor a RIPng.

- Confiabilidad: para RIPng se obtuvo un porcentaje de confiabilidad del 88%, el cual fue superado en 11 puntos por EIGRP.
- Transferencia de datos: para RIPng y EIGRP la tasa de bits promedio cuando los dos archivos están siendo transferidos es 7,3 y 128,08 Kb/s respectivamente, pero esta tasa varía de acuerdo a la cantidad de tráfico que circulen por los enlaces activos de la red. Dicha tasa para cada uno de los archivos la podemos apreciar en la figura 4.7.

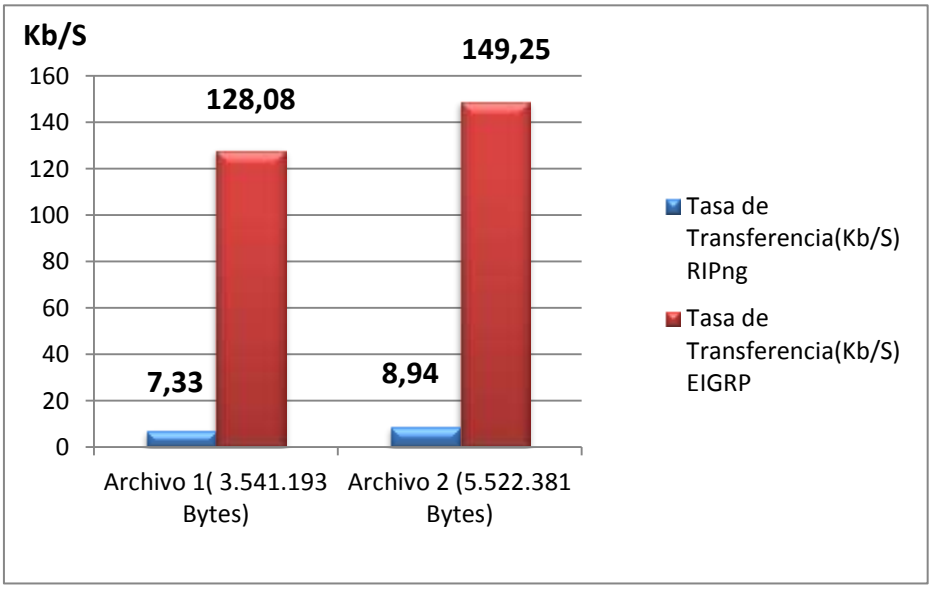


Figura 4.7 Comparación de tasas de transferencia RIPng y EIGRP

- Escalabilidad: RIPng claramente establece un destino ubicado a más de 15 saltos como inalcanzable, por el contrario EIGRP no establece ninguna restricción en cuanto a este parámetro, lo que si se sugiere es no exceder un número mayor a 60 enrutadores en un sistema autónomo EIGRP.
- Complejidad de la configuración: La configuración básica de estos dos protocolos de enrutamiento se asemeja mucho, en ambos casos es sencilla.
- Licenciamiento: EIGRP es un protocolo exclusivo para equipos CISCO, en cambio RIPng es libre de ser usado por los equipos de cualquier fabricante, esto podría marcar una de las pocas ventajas que tiene RIPng sobre EIGRP.
- Soporte en IOS: como podemos notar algunos parámetros de comparación se relacionan, no obstante podemos concluir en otra ventaja de RIPng sobre EIGRP, ya que el primero es soportado en casi todas las marcas de equipos.
- Métrica: RIPng mantiene su sencillez en utilizar el número de saltos, EIGRP añade mayor detalle y utiliza una relación basada en parámetros configurables como ancho de banda, retraso, carga y confiabilidad. Cabe mencionar que ambos protocolos ofrecen

flexibilidad para priorizar unas rutas sobre otras, ya que se pueden modificar los valores de todas las variables antes mencionadas e incluso el costo de un enlace en RIPng que predeterminadamente es la unidad.

- Resumen de rutas: ambos protocolos tienen deshabilitada esta característica predeterminada y la implementan de igual manera, lo que sí destaca a EIGRP sobre RIPng es que una vez aplicada esta característica, realiza este proceso con mayor rapidez.
- Consumo de Recursos: debido a la similitud en algunas características de EIGRP con protocolos de estado de enlace y al algoritmo que utiliza para alimentar las tablas que este administra, emplea mayores recursos de hardware como memoria y CPU, esto hace que RIPng sea preferido si se tiene limitantes en cuanto hardware y software.

Todos los parámetros de comparación mencionados anteriormente se consolidan en la tabla X.

Tabla X Comparación de protocolos de enrutamiento de vector distancia

	RIPng	**EIGRP**
Tiempo de convergencia	Alto	Bajo
Confiabilidad	88%	99%
Escalabilidad	Media	Alta
Complejidad de configuración	Media	Alta
Popularidad	Alta	Alta
Licenciamiento	Libre uso	Exclusivo CISCO
Características especiales	Pocas	Variadas
Soporte en IOS CISCO	Alto	Bajo
Métrica	Número de Saltos	Ancho de Banda, Retraso
Resumen de rutas	Si	Si
Consumo de recursos	Bajo	Alto
Consumo de ancho de banda	Ineficiente	Eficiente
Interfaces Pasivas	No	Si
Compatibilidad	Alta	Baja
Algoritmo de enrutamiento	Bellman - Ford	Dual

4.9. Comparación entre protocolos de enrutamiento de estado de enlace

Para la prueba de convergencia luego de la caída de un enlace en IS-IS los resultados se muestran en la tabla XI. Un valor importante es la media, la cual se ubica en 7,8 segundos lo que es un tiempo aceptable en un protocolo tan escalable como IS-IS. La figura 4.8 nos muestra la uniformidad en los tiempos de convergencia.

Tabla XI Estadística descriptiva de los tiempos de convergencia luego de la caída de un enlace en IS-IS

Tiempo de convergencia [s]	
Media	0:00:07,800
Moda	0:00:07,608
Desviación estándar	0,00001078119
Varianza de la muestra	0,00000000012
Mínimo	0:00:05,560
Máximo	0:00:12,928
Cuenta	47

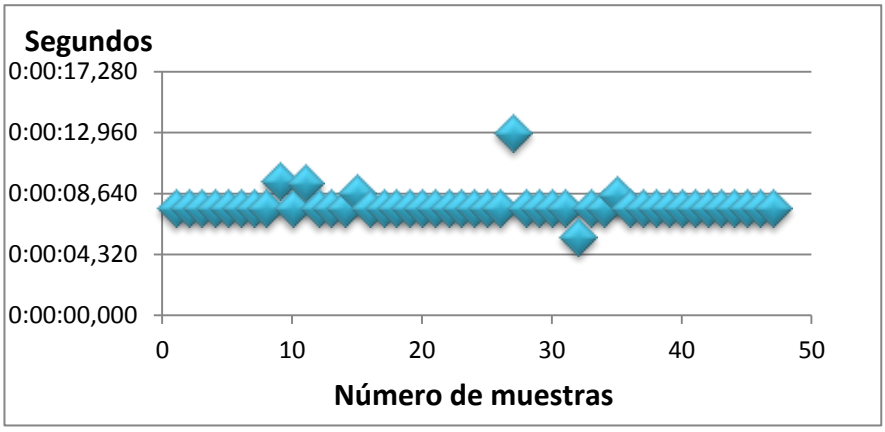


Figura 4.8 Dispersión de los tiempos de convergencia luego de la caída de un enlace en IS-IS

De igual manera se realizó la prueba simulando la operatividad del enlace luego de haber sufrido una caída en IS-IS, los datos se muestran en la tabla XII. El tiempo que toma la convergencia prácticamente se ha duplicado ya que se encuentra en una media de 14,7 segundos con una moda de 13,6 segundos. En la figura 4.9 se muestra que existen grandes

diferencias en los tiempos de convergencia en casi el doble cuando sube el enlace que cuando cae.

Tabla XII Estadística descriptiva de los tiempos de convergencia luego de la subida de un enlace en IS-IS

Tiempo de convergencia [s]	
Media	0:00:14,697
Moda	0:00:13,556
Desviación estándar	0,0000000001
Varianza de la muestra	0,00
Mínimo	0:00:09,556
Máximo	0:00:19,548
Cuenta	47

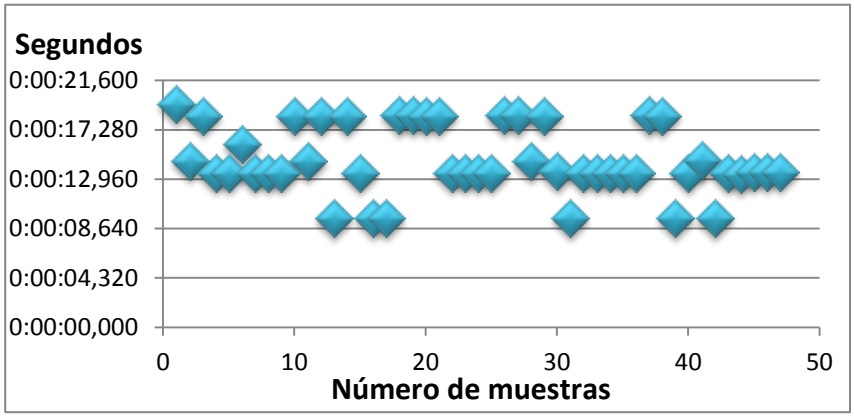


Figura 4.9 Dispersión de los tiempos de convergencia luego de la subida de un enlace en IS-IS

Podemos verificar en la tabla XIII que la media del tiempo de convergencia es de aproximadamente 12 segundos, que comparada con las obtenidas luego de la caída y subida de un enlace se encontraría entre ambas. Al percatarnos de la separación entre los datos como se muestra en la figura 4.10, en primera instancia creímos que se estaba

recopilando erróneamente los datos pero se la realizó por segunda vez donde se constató la gran diferencia en los tiempos.

Tabla XIII Estadística descriptiva de los tiempos de convergencia luego del reinicio del protocolo IS-IS

Tiempo de convergencia [s]	
Media	0:00:11,992
Moda	0:00:05,512
Desviación estándar	0,0000698602
Varianza de la muestra	0,0000000049
Mínimo	0:00:05,312
Máximo	0:00:22,052
Cuenta	48

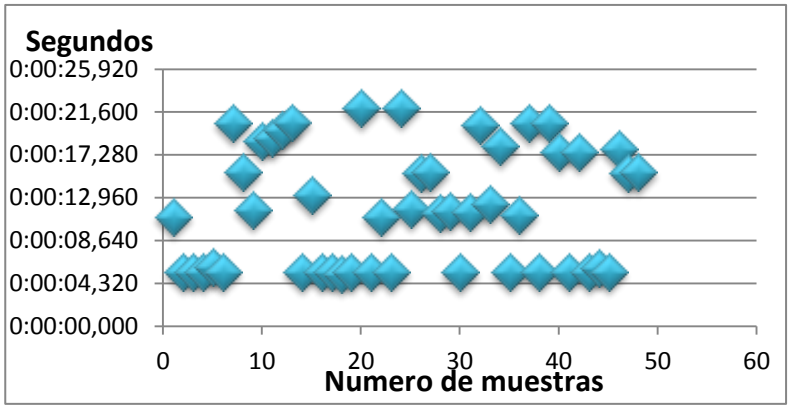


Figura 4.10 Dispersión de los tiempos de convergencia luego de reiniciar el protocolo IS-IS

Se muestra en la tabla XIV que el tiempo de convergencia medio luego de la caída de un enlace en OSPFv3 es de 5,174 segundos. La dispersión de los tiempos de convergencia se muestra en la figura 4.11,

demostrando que los tiempos son similares dándonos una seguridad y haciendo sobresalir su estabilidad en el enrutamiento.

Tabla XIV Análisis estadístico de los tiempos de convergencia luego de la caída de un enlace en OSPFv3

Tiempo de convergencia [s]	
Media	0:00:05,174
Moda	0:00:05,012
Desviación estándar	0,0000109982
Varianza de la muestra	0,0000000001
Mínimo	0:00:04,569
Máximo	0:00:11,496
Cuenta	50

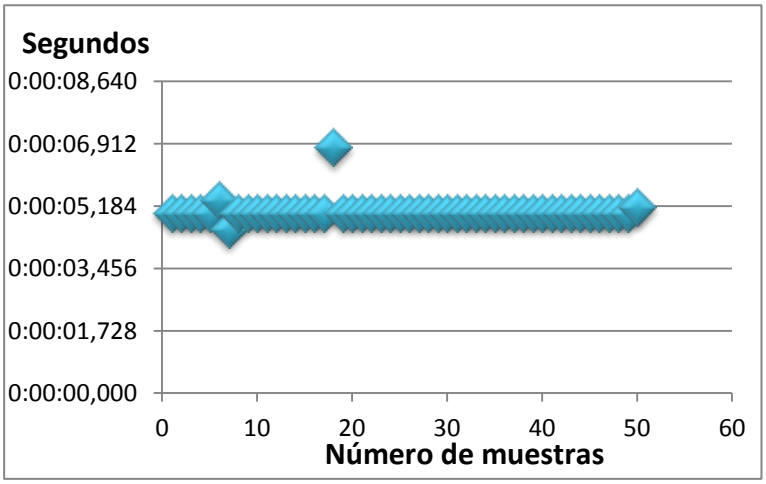


Figura 4.11 Dispersión de los tiempos de convergencia luego de la caída de un enlace en OSPFv3

La tabla XV muestra los datos estadísticos luego de la subida de un enlace y en la figura 4.12 observamos que los valores de los tiempos de convergencia se encuentran más dispersos, comparados con IS-IS

ambos presentan un patrón parecido, esto se debe a que ambos usan SPF.

Tabla XV Estadística descriptiva de los tiempos de convergencia luego de la subida de un enlace en OSPFv3

Tiempo de convergencia [s]	
Media	0:00:19,422
Moda	0:00:19,008
Desviación estándar	0,0000323510
Varianza de la muestra	0,0000000010
Coeficiente de asimetría	7,06
Mínimo	0:00:19,004
Máximo	0:00:38,780
Cuenta	50

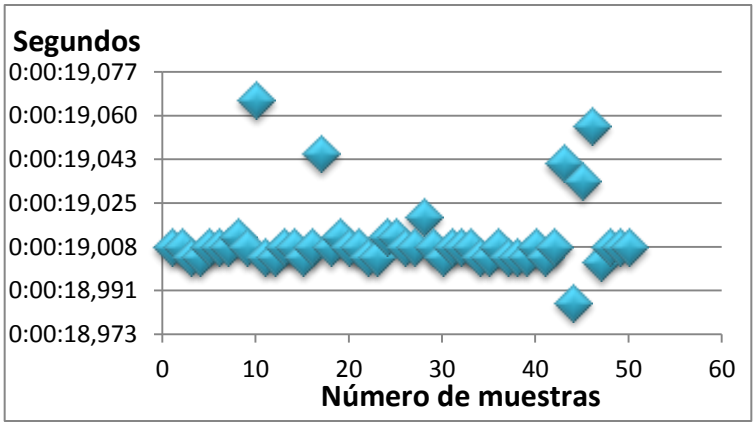


Figura 4.12 Dispersión de los tiempos de convergencia luego de la subida de un enlace en OSPFv3

En la tabla XVI se muestra la estadística descriptiva para la prueba de convergencia luego de reiniciar el protocolo, comparado con el de IS-IS este tiempo es mayor por 4 segundos, esto se puede apreciar en la figura

4.13, ya que en la prueba solo se contaba con tres enrutadores, lo cual nos indica que es una red pequeña.

Tabla XVI Análisis estadístico de los tiempos de convergencia luego del reinicio del proceso OSPFv3

Tiempo de convergencia [s]	
Media	0:00:15,008
Moda	0:00:15,008
Desviación estándar	0,00
Varianza de la muestra	0,00
Mínimo	0:00:15,008
Máximo	0:00:15,008
Cuenta	47

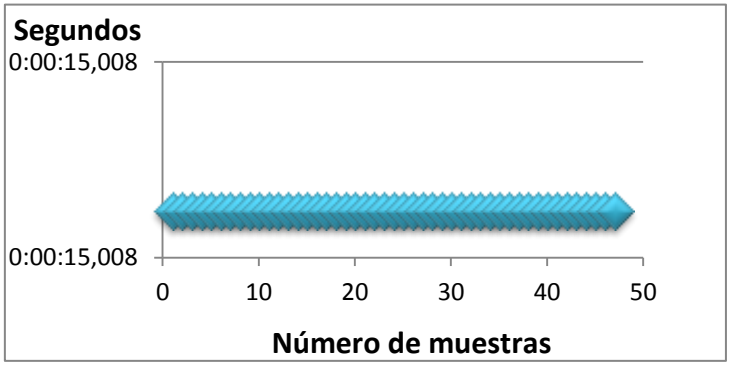


Figura 4.13 Dispersión de los tiempos de convergencia luego del reinicio del proceso OSPFv3

Entre los aspectos importantes para hacer una comparación completa e identificando cada una de las ventajas y desventajas de los protocolos, tenemos los siguientes:

- Tiempo de convergencia: comparando los tiempos de convergencia entre OSPFv3 e IS-IS, las diferencias son

mínimas, en cuanto a la caída del enlace no tenemos una diferencia mayor a 2 segundos, estando cada uno de ellos cercanos a los 5 y 8 segundos respectivamente.

- Confiabilidad: tanto en OSPFv3 e IS-IS existió un porcentaje de confiabilidad del 98%.
- Transferencia de datos: en cada uno de los envíos de archivos no se superó más allá de un 15% entre ambos protocolos, siendo OSPFv3 el que mantuvo las mayores tasas de transferencias como se muestra en la figura 4.14.

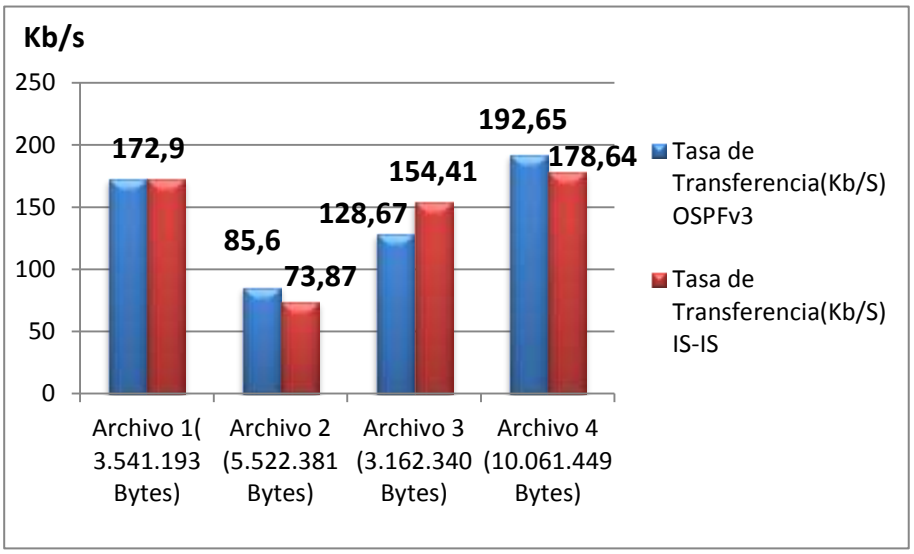


Figura 4.14 Comparación de tasas de transferencia OSPFv3 e IS-IS

- Escalabilidad: tanto OSPFv3 e IS-IS se destacan por ser altamente escalables por lo cual no existe una superioridad entre ellos.
- Licenciamiento: una gran ventaja que poseen los protocolos de estado de enlace es que son de libre uso por tanto no solo los vamos a encontrar en equipos de la marca CISCO sino a nivel mundial.
- Complejidad de la configuración: ambos protocolos tienen alto grado de complejidad para la configuración ya que se implementa el uso de áreas lo que aumenta las configuraciones.
- Soporte en IOS: ambos protocolos de estado de enlace se encuentran en todos los IOS que hemos utilizados tanto para las prácticas realizadas en el emulador como en los equipos reales.
- Métrica: en OSPFv3 la métrica es calculada en base al ancho de banda del enlace, pero para IS-IS los enlaces tienen el valor de 10 predeterminado, ya que estamos trabajando con equipos CISCO.

- Resumen de rutas: ambos protocolos de estado de enlace lo permiten con la diferencia que se debe configurar en los enrutadores de borde para OSPFv3 y para IS-IS en los de nivel 1-2.
- Consumo de Recursos: los protocolos de estado de enlace están hechos para soportar un alto número de enrutadores y gran tráfico de paquetes y por ende ambos protocolos consumen altos porcentajes de memoria y CPU.
- Compatibilidad: en equipos con soporte para IPv6 se admiten en todo tipo de enrutadores, tanto OSPFv3 e IS-IS.
- Algoritmo de enrutamiento: ambos protocolos para encontrar la mejor ruta entre dos dispositivos ejecutan el algoritmo SPF o Dijkstra.

Todos estos aspectos han sido resumidos en la tabla XVII para su mejor comprensión y visualización.

Tabla XVII Comparación de protocolos de enrutamiento de estado de enlace

	OSPFv3	**IS-IS**
Tiempo de convergencia	Bajo	Bajo
Confiabilidad	98%	98%
Escalabilidad	Media	Alta
Complejidad de configuración	Media	Alta
Popularidad	Alta	Baja
Licenciamiento	Libre uso	Libre uso
Características especiales	Variadas	Pocas
Soporte en IOS CISCO	Alto	Alto
Métrica	Ancho de banda	Valor predeterminado
Resumen de rutas	Si	Si
Consumo de recursos	Alto	Alto
Consumo de ancho de banda	Eficiente, bajo	Alto
Áreas	Si	Si
Compatibilidad	Alta	Alta
Algoritmo de enrutamiento	SPF	SPF

4.10. Comparación entre Multihoming IPv4 y Multihoming IPv6

Para implementar multihoming debemos adquirir un bloque de direcciones o prefijos por parte de un RIR pero también estos pueden ser otorgados por un ISP, que puede ser el mismo que está siendo usado en la organización. Los escenarios posibles para la implementación de multihoming en IPv4 son:

- Modelo con prefijos independientes del proveedor: en este esquema el bloque de direcciones se obtuvo junto con el número

de sistema autónomo, por parte de un RIR. Cada uno de los bloques de direcciones debe ser anunciado hacia Internet, para poder lograrlo se debe configurar BGP en los enrutadores de frontera del sistema autónomo.

- Modelo con prefijos asignados por el proveedor: cuando una organización no puede adquirir un bloque de direcciones independientes de su proveedor, existe otra forma de implementar multihoming. Si la organización adquiere un bloque de direcciones de parte de uno de los ISP's, que a su vez forma parte de la conexión multihoming, este bloque de direcciones toma el nombre de Provider Aggregatable (PA), a parte de dicho bloque de direcciones también deberá publicar el prefijo que fue asignado en primera instancia y que es usado por el sistema autónomo para conectarse hacia el exterior.
- NAT: también es un tipo de multihoming ya que dentro de un sistema autónomo se puede estar utilizando direcciones privadas y cuando necesiten salir hacia Internet se traducen a direcciones públicas por los enrutadores.

Dada la arquitectura del protocolo IPv6, veremos muchos cambios en la implementación de multihoming pero el funcionamiento será el mismo

que el mostrado en IPv4. Tomando como ejemplo el esquema con prefijos asignados por el proveedor, en IPv6 sucede algo similar, pero en este caso el direccionamiento es el que se maneja de manera diferente ya que la dirección IPv6 tiene varias partes que la identifican según la interfaz, subred y el identificador que otorgan los RIR's o ISP's. Suponemos una organización conectada a dos ISP's , del ISP A recibe el prefijo 2001:100:10::/48 y del ISP B recibe 2001:200:20::/48, a su vez un host del sitio posee dos direcciones globales, 2001:100:10:15::25 y 2001:200:20:15::25 y dicho host puede enviar tráfico por ambos ISP's. Cada proveedor por parte del RIR respectivo recibió el bloque de prefijos pero /35 y estos son anunciados hacia internet, estos prefijos engloban a los que se les asignaron al sitio.

Los métodos que se utilizan en Multihoming IPv4 funcionan correctamente, pero viéndolo a futuro existen inconvenientes tales como el anuncio de redes hacia el sistema global de rutas lo que limita en cuanto a escalabilidad del sitio. Si bien el uso de direcciones PA asignadas por los ISP's ayuda en gran medida al ahorro de recursos pero también tiene desventajas como la compatibilidad con los filtros de ingreso, tolerancia a fallos e ingeniería de tráfico. Dichas desventajas no

son radicales ya que en su mayoría pueden ser prevenidas mediante la creación de buenas políticas a la hora de la selección de rutas predeterminadas y ayudándose con los registros en los DNS. Al comparar las configuraciones del protocolo BGP en IPv4 e IPv6 nos damos cuenta que no existen grandes diferencias. Tanto el direccionamiento como en el anuncio de redes internas no ha cambiado, pero en su configuración para IPv6 se debe acceder a la familia de direcciones de su mismo nombre para activar el tráfico de información entre vecinos y dentro de esta misma sección, agregar las redes que serán anunciadas vía BGP. Las configuraciones tanto para Multihoming en IPv4 e IPv6 se puede revisar en el anexo IV. En IPv6 tenemos un alto grado de seguridad e integridad de los paquetes, dando mayor tolerancia a fallos ya que en las nuevas implementaciones de BGP se mejora el inicio y el mantenimiento de nuevas comunicaciones luego de un fallo.

CONCLUSIONES

A continuación se presentan las conclusiones obtenidas en base a los resultados de las pruebas que se realizaron a lo largo de nuestro proyecto.

1. Los resultados en nuestras pruebas de RIPng y EIGRP fueron los esperados, para el caso de convergencia se analizaron en tres escenarios, el primero de ellos luego de la caída de un enlace en donde el tiempo promedio de RIPng fue 14.5 segundos, una cifra 6 veces superior que en EIGRP. Sin embargo, en la subida del enlace ambos tiempos son similares, los mismos están ligeramente por encima de los 4 segundos. Y por último cuando se reinicia el proceso para ambos IGP's, este tiempo en RIPng es de 17 segundos aproximadamente, 4 segundos más que EIGRP. Por el lado de la confiabilidad los resultandos también fueron razonables, ya que las pruebas le dieron a RIPng un 88% de confianza en la transmisión de datos y a EIGRP un 99%. En escalabilidad se obtuvo un resultado más que evidente, el cual establece la limitación que RIPng tiene en redes cuyas distancias entre destino y origen superen los 15 saltos, por el contrario en EIGRP se llegó a probar hasta con 20 enrutadores sin problema alguno. Finalizamos con las pruebas de transferencia de datos en donde las diferencias son bastante acentuadas,

para RIPng y EIGRP se obtuvieron tasas promedios de 7,3 y 128,08 Kb/s, en ese orden. El análisis de estos resultados nos llevan claramente a concluir en la superioridad que EIGRP tiene sobre RIPng, fundamentada por ventajas y desventajas de un IGP respecto al otro, como algoritmo de enrutamiento, limitaciones, funcionamiento, recursos de hardware y software, costos, entre otros.

2. Una vez obtenidos los resultados en la figura 4.14, comparando los valores de las tasas de transferencia tanto en las implementaciones para OSPFv3 e IS-IS, se notó claramente una superioridad de OSPFv3 de hasta un 15% en la transferencia de archivos lo que nos inclina a pensar que a pesar que es un protocolo de enrutamiento ideado para redes de gran tamaño, posee un mejor rendimiento en el tráfico de datos comparado a IS-IS.

3. En base a los resultados en las pruebas de confiabilidad, obteniendo ambos protocolos de enrutamiento estado de enlace, OSPFv3 e IS-IS un porcentaje del 98% podemos concluir que ambos ofrecen altas prestaciones en cuanto a la garantía en la transmisión de los datos y a su

vez que este aspecto al ser evaluado en ambos, no obtuvo una tendencia mayoritaria hacia alguno de ellos.

4. Los tiempos de convergencia luego de la caída y subida de un enlace siempre fueron menores en OSPFv3 comparados a los obtenidos en IS-IS, llegando a tener una diferencia aproximada de un 25% a favor de OSPFv3. La ventaja la mantiene OSPFv3 en la convergencia luego del reinicio del protocolo oscilando en un 20%.

5. Luego de la comparación realizada entre Multihoming IPv4 e IPv6 y haber puesto en práctica su configuración e implementación notamos que su complejidad en IPv6 es mayor, ya que requiere de nuevas configuraciones para la formación de adyacencias en cuanto al protocolo BGP y adicionalmente incluyen funcionalidades que deben ser revisadas con detenimiento para mejorar su funcionamiento.

RECOMENDACIONES

En base al estudio y las comparaciones realizadas entre los protocolos de enrutamiento orientados a IPv6, mencionamos las recomendaciones a tomarse en cuenta para un trabajo a futuro.

1. Para darse la migración de IPv4 a IPv6 en cualquier tipo de organización y sin distinción de tamaño, se sugiere realizarlo seccionalmente e ir evaluando y corrigiendo errores en la marcha, iniciando por sectores en que se ocasione el menor impacto posible y en base a una bitácora de pruebas y resultados ir pasando a las unidades de mayor relevancia en una organización. Este proceso puede ser posible gracias a los mecanismos de transición, los cuales nos permiten una coexistencia de segmentos de redes en IPv6 e IPv4.

2. Al momento de realizar pruebas de análisis y comparación de varias opciones de tecnología a utilizar (en nuestro caso protocolos de enrutamiento), se recomienda que estas sean lo mayormente equitativas posibles en todos los aspectos, tanto a nivel de hardware y software, como series y modelos de equipos, IOS, ya sea en ordenadores, enrutadores, conmutadores, entre otros equipos

importantes en una red de datos e incluso factores externos, como temperatura, humedad, alimentación eléctrica (voltaje y corriente), etc. Mientras más cercana sean las condiciones para evaluar el funcionamiento de varias tecnologías, obtendremos resultados con un muy alto nivel de confiabilidad, que nos ayudarán a tomar las mejores decisiones y explotarán al máximo los recursos dentro de una organización y por ende esta obtendrá mayor utilidad económica, que al fin y al cabo es uno de los más fuertes objetivos en una empresa.

3. Antes de empezar a diseñar e implementar una red en un entorno organizacional o experimental es primordial establecer la metodología de trabajo, esquemas de diseño, implementación, investigación, redacción, registro de bitácora, análisis de resultado y parámetros de decisiones, esto sin duda alguna agilitará el periodo que se tome para poner en marcha la operativa de una red de datos y el constante monitoreo y mantenimiento que se le debe dar a la misma. Sin olvidar que antes de pasar a un ambiente de producción es imperioso que este haya pasado por un alto control de calidad, principalmente para evaluación y corrección de errores en caso que amerite.

4. Para cada una de las pruebas que realizamos diseñamos topologías acorde a nuestros recursos pero si sería importante hacer las pruebas con topologías de gran tamaño para tener una idea más concreta del consumo de recursos de cada uno de los protocolos al estar funcionando con mayor tráfico y validar su desempeño a nivel empresarial. Todas las pruebas fueron realizadas en un ambiente de laboratorio donde los factores externos que suelen afectar las comunicaciones no intervinieron por tanto se podría decir que trabajamos bajo condiciones ideales, dada esta situación seria importante recrear un ambiente más real para las pruebas.

ANEXO I

DIRECCIONAMIENTO Y TOPOLOGÍAS USADAS EN LAS PRUEBAS DE CONFIABILIDAD Y TRANSFERENCIA DE ARCHIVOS

Para las pruebas de confiabilidad y transferencia de archivos se diseñaron dos topologías, una para cada tipo de protocolo de enrutamiento, vector distancia y estado de enlace. A continuación se muestran las tablas de direccionamiento y las topologías implementadas.

Topología implementada para los protocolos de enrutamiento RIPng y EIGRP

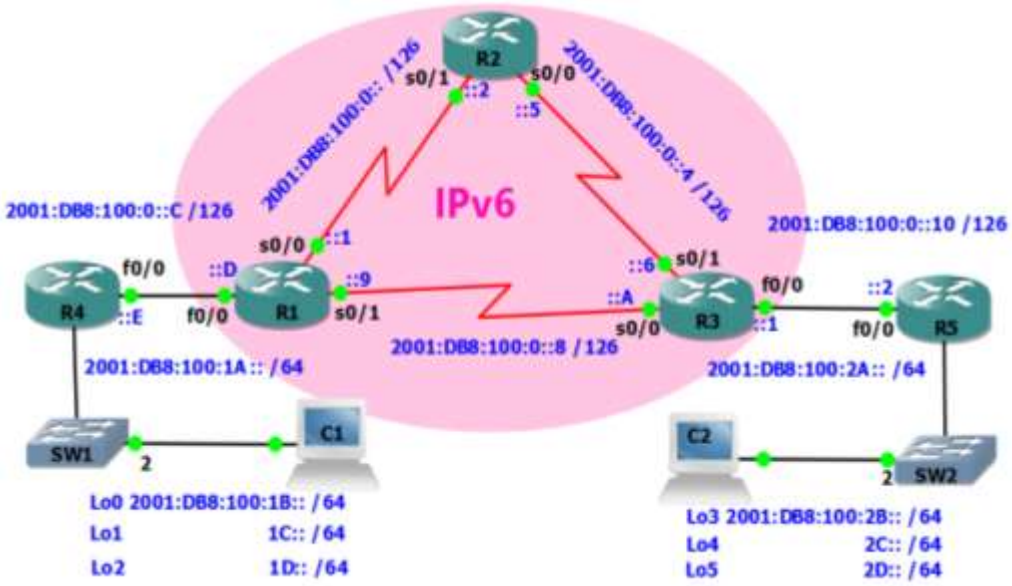


Tabla de direccionamiento para las pruebas de confiabilidad y transferencia de archivos para los protocolos RIPng y EIGRP

Disp.	Interfaz	Dirección IPv6	Puerta de enlace
R1	Fa0/0	2001:db8:100:0::D/126	---
	S0/0	2001:db8:100:0::1/126	---
	S0/1	2001:db8:100:0::9/126	---
R2	S0/0	2001:db8:100:0::5/126	---
	S0/1	2001:db8:100:0::2/126	---
R3	Fa0/0	2001:db8:100:0::11/126	---
	S0/0	2001:db8:100:0::A/122	---
	S0/1	2001:db8:100:0::6/122	---
R4	Fa0/0	2001:db8:100:0::D/126	---
	Fa0/1	2001:db8:100:1a::1/64	---
	Lo0	2001:db8:100:1B::1/64	---
	Lo1	2001:db8:100:1C::1/64	---
	Lo3	2001:db8:100:1D::1/64	---
R5	Fa0/0	2001:db8:100:0::12/126	---
	Fa0/1	2001:db8:100:2A::1/64	---
	Lo4	2001:db8:100:2B:1/64	---
	Lo5	2001:db8:100:2C::1/64	---
	Lo6	2001:db8:100:2D:1/64	---
C01	---	2001:db8:100:1A::2/64	2001:db8:100:1A::1/64
C02	---	2001:db8:100:2A:2/64	2001:db8:100:2A:1/64

Topología implementada para los protocolos de enrutamiento OSPFv3 e IS-IS

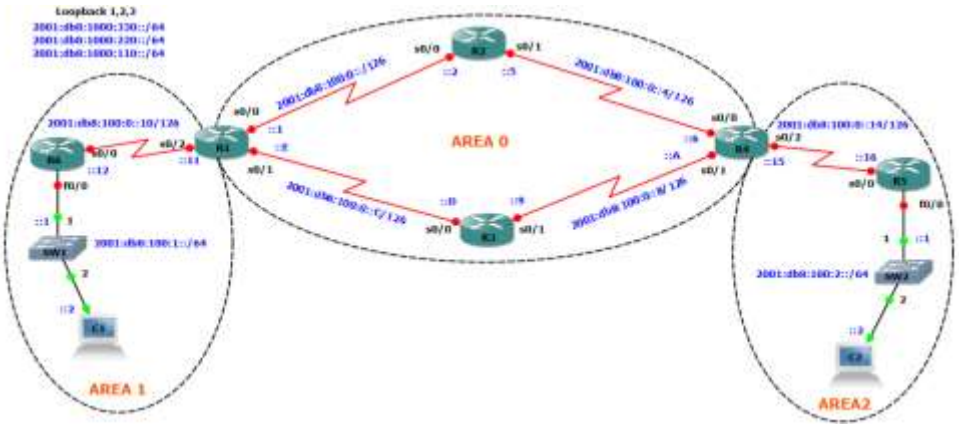


Tabla de direccionamiento para las pruebas de confiabilidad y transferencia de archivos para los protocolos OSPFv3 e IS-IS

Disp.	Interfaz	Dirección IPv6	Puerta de enlace
R1	S0/2	2001:db8:100:0::11/126	---
	S0/0	2001:db8:100:0::1/126	---
	S0/1	2001:db8:100:0::E/126	---
R2	S0/0	2001:db8:100:0::2/126	---
	S0/1	2001:db8:100:0::5/126	---
R3	S0/0	2001:db8:100:0::D/126	---
	S0/1	2001:db8:100:0::9/126	---
R4	S0/0	2001:db8:100:0::6/126	---
	S0/1	2001:db8:100:0::A/126	---
	S0/2	2001:db8:100:0::15/126	---
R5	S0/0	2001:db8:100:0::16/126	---
	Fa0/0	2001:db8:100:2::1/64	---
R6	S0/0	2001:db8:100:0::12/126	---
	Fa0/0	2001:db8:100:1::1/64	---
	Lo1	2001:db8:1000:330::1/64	---
	Lo2	2001:db8:1000:220::1/64	---
	Lo3	2001:db8:1000:110::1/64	---
C01	---	2001:db8:100:1::2/64	2001:db8:100:1::1/64
C02	---	2001:db8:100:2::2/64	2001:db8:100:2::1/64

ANEXO II

CARACTERÍSTICAS Y ESPECIFICACIONES DE LOS ENRUTADORES USADOS

Dado el número de enrutadores que se usó en cada una las prácticas, no existía el número necesario para realizar las pruebas usando el mismo modelo, por tal motivo se muestran las características de cada uno de ellos.

CISCO 3725

Características generales	
Factor de forma	Desktop - modular - 2U
Número de módulos instalados	1
Máximo número de módulos instalables	9
Dimensiones [cm]	43.4 x 8.9 x 37.3 cm
Peso [Kg]	6.4 Kg
Memoria RAM	256 MB
Memoria Flash	64 MB

CISCO 3725

Expansión / Conectividad	
Interfaces	2 x 10Base-T/100Base-TX - RJ-45, Administración : 1 x Consola, Serial: 1 x Entrada auxiliar
Total de ranuras de expansión	1 x Tarjeta CompactFlash / 4 x Ranuras de expansión, Memoria / 3 x WIC / 1 x AIM
Red	
Protocolo de enlace de datos	Ethernet, Fast Ethernet
Estándares	IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p
Software / Requisitos del sistema	
Sistema Operativo	Cisco IOS Advanced IP services

Información de Imagen del IOS utilizado

Nombre de la Imagen	c3725-adventerprisek9-mz.124-15.T14.bin
Número de versión (Release)	12.4(15)T14
Nombre de plataforma	3725
Características(NX-OS specific)	ADVANCED ENTERPRISE

CISCO 2800

Características generales	
Factor de forma	Externo - modular - 1U
Número de módulos instalados	1
Máximo número de módulos instalables	2
Dimensiones [cm]	43.8 x 4.5 x 41.7 cm
Peso [Kg]	6.4 Kg
Memoria RAM	256 MB /768 MB MAX
Memoria Flash	64 MB / 256 MB MAX
Expansión / Conectividad	
Interfaces	2 x 10Base-T/100Base-TX - RJ-45, Administración : 1 x Consola, Serial: 1 x Entrada auxiliar
Total de ranuras de expansión	1 x NM /4 x HWIC, WIC, VIC
Red	
Protocolo de enlace de datos	Ethernet, Fast Ethernet
Tecnología de conectividad	Cableado
Estándares	IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p

Información de Imagen del IOS utilizado

Nombre de Imagen	c2800nm-advipservicesk9-mz.124-25c.bin
Número de versión (Release)	12.4(25c)
Nombre de Plataforma	2811
Características (NX-OS specific)	ADVANCED IP SERVICES

CISCO 1800

Características generales	
Factor de forma	Desktop, 1-rack-unit (1-RU) high (4.75-cm high with rubber feet)
Número de módulos instalados	1
Máximo número de módulos instalables	2
Dimensiones [cm]	4,39 x 34,29 x 27,43cm
Peso [Kg]	2,72 kg
Memoria DRAM	256 MB / 384 MB
Memoria Flash	32 MB /384MB MAX
Expansión / Conectividad	
Interfaces	2 x RJ-45 10/100Base-TX 10/100Base-TX LAN, 1 x Consola Gestión, 1 x Auxiliar Gestión, 1 x USB
Red	
Protocolo de enlace de datos	Ethernet, Fast Ethernet
Tecnología de conectividad	Cableado
Protocolo de transporte	TCP/IP, SNMP
Estándares	IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p

Información de Imagen del IOS utilizado

Nombre de la Imagen	c1841-advipservicesk9-mz.151-4.M6.bin
Número de versión (Release)	15.1(4)M6
Nombre de plataforma	1841
Características(NX-OS specific)	ADVANCED IP SERVICES

Comparación de características de enrutadores CISCO 3725 y JUNIPER M7i

	CISCO 3725	JUNIPER M7i
Dimensiones	43.4 x 8.9 x 37.3 cm	44.5 x 8.9 x 45.7 [cm]
Peso	14.08 lbs	38.2 lbs
Montaje	Frontal o central	Frontal o central
Temperatura de Operación	0° - 40°C	0° - 40°C
% de Humedad	5% - 95%	5% - 90%
Alimentación	120 - 130 VAC	100 - 240 VAC
Dispositivos Instalados	1	1
Frecuencia	50 - 60 [Hz]	47 - 63 [Hz]
Memoria RAM	256 MB	512 MB
Interfaces	2 x 10Base-T/100Base-TX - RJ-45, Administración : 1 x Consola, Serial: 1 x Entrada auxiliar	1 x 1000Base-SX, Administración: 2 x RS-232 - 9 pin D-Sub (DB-9), Administración: 1 x 10Base-T/100Base-TX - RJ-45
Ranuras de expansión	1 x Tarjeta CompactFlash / 4 x Ranuras de expansión, Memoria / 3 x WIC / 1 x AIM	1 x Tarjeta PC , 4 x Ranuras de expansión
Sistema Operativo	IOS CISCO	JUNOS
Algoritmo de cifrado	DES, Triple DES, AES, MD5	DES, Triple DES, MD5, SHA-1
Estándares	IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p	IEEE 802.1Q
Soporte IPv6	SI	SI
Soporte RIPng	SI	SI
Soporte EIGRP	SI	NO
Soporte OSPFv3	SI	SI
Soporte IS-IS	SI	SI
Soporte BGP	SI	SI

ANEXO III

COMANDOS UTILIZADOS EN LOS PROTOCOLOS DE ENRUTAMIENTO

Hemos resumido todos los comandos utilizados en la configuración de los enrutadores para tener una mejor visión y comprensión de los mismos.

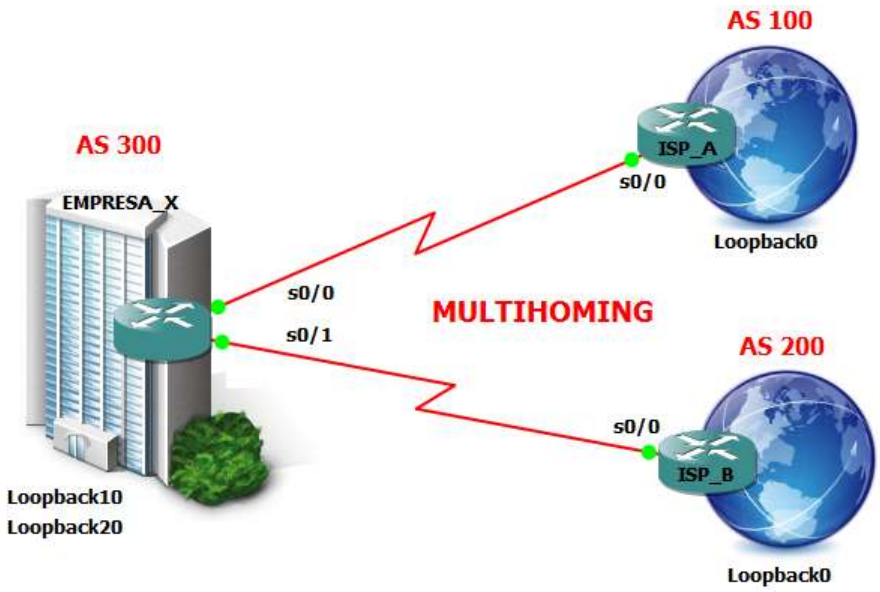
Comando	Función
Generales	
ipv6 unicast-routing	Habilita el direccionamiento IPv6 por unidifusión
ipv6 multicast-routing	Habilita el direccionamiento IPv6 por multidifusión
ipv6 address [dirección_IPv6] /[máscara]	Asigna dirección IPv6 a interfaz
RIPng	
ipv6 router rip [nombre_proceso]	Habilita e instancia proceso de enrutamiento RIPng
ipv6 rip [nombre_proceso] enable	Habilita proceso RIPng en la interfaz
ipv6 prefix-list [nombre_lista] seq [#_secuencia] deny [dirección_red_IPv6] /[máscara]	
ipv6 prefix-list [nombre_lista]	Crea una lista de direcciones de red
seq [#_secuencia]	Crea una entrada de la lista en una posición específica
deny [dirección_red_IPv6] /[máscara]	Deniega todo el tráfico que proviene de un segmento de red
distribute-listprefix-list [nombre_lista] in [interfaz]	
distribute-listprefix-list [nombre_lista]	Crea una lista de distribución
in [interfaz]	Tráfico de entrada de una interfaz
out [interfaz]	Tráfico de salida de una interfaz
timers [ta] [ti] [te] [td]	Modifica los valores de los temporizadores RIP
maximum-paths [#]	Establece máximo número de rutas para balanceo de carga
ipv6 rip [nombre_proceso] summary-address [X:X:X:X::X/<0-128>]	Resumen de rutas para proceso RIPng

EIGRP	
ipv6 router eigrp [#_Sistema_Autónomo]	Declara sistema autónomo(AS) EIGRP
router-id [dirección_ipv4]	Identificador del enrutador(Deber ser dirección IPv4)
no shutdown	Habilita sistema autónomo(AS) EIGRP
ipv6 eigrp [#_Sistema_Autónomo]	Habilita AS EIGRP dentro de una interfaz
passive-interface [interfaz]	Declara a una interfaz como pasiva
ipv6 summary-address eigrp [#_AS] [X:X:X:X::X/<0-128>]	Sumarización de rutas para sistema autónomo EIGRP
eigrp stub	Define a un enrutador como Stub
ipv6 hello-intervaleigrp [#_AS] [#_segundos]	Establece intervalo de mensajes de saludo para AS EIGRP
ipv6 hold-time eigrp [#_AS] [#_segundos]	Establece intervalo de mensajes de sostenimiento para AS EIGRP
bandwidth [#_ancho_banda]	Establece el ancho de banda en interfaz (Kbps)
OSPFv3	
ipv6 ospf [#_proceso] area [#_area]	Habilita el proceso OSPFv3 en la interfaz
ipv6 router ospf [#_proceso]	Crea el proceso OSPFv3 en el enrutador
router-id [dirección_ipv4]	Configura el identificador del enrutador en el proceso OSPFv3
ipv6 ospf cost [#_coste]	Configura el costo <1-65535>
auto-cost reference-bandwith [#_bandwith_referencia]	Configura el ancho de banda de referencia <1-4294967>
area [#número_del_área] range [X:X:X:X::X/<0-128>]	Configura el rango de direcciones IPv6 para el resumen de rutas
IS-IS	
ipv6 router isis [nombre_del_proceso]	Habilita el proceso IS-IS en la interfaz
router isis [nombre_del_proceso]	Crea el proceso IS-IS en el enrutador
net [direccion_NET]	Configura la dirección NET del enrutador
is-type [level-1 | level-1-2 | level-2]	Configura el nivel del enrutador
isis circuit-type [level-1 |level-1-2 | level-2-only]	Configura el tipo de adyacencia de cada interfaz
isis metric [métrica_predeterminada]	Cambia el valor de la métrica predterminada
BGP	
router bgp [#_Sistema_Autónomo]	Crea el proceso BGP en el enrutador
bgp router-id [dirección_ipv4]	Configura el identificador del enrutador en el proceso BGP
no bgp default ipv4-unicast	Deshabilita la familia de direcciones unicast IPv4 en todos los vecinos
neighbor [dirección_IPv6] remote-as [[#_Sistema_Autónomo]	Configurar un peer con un vecino
address-family ipv6	lngresa al modo de configuración de la familia de direcciones IPv6
network [X:X:X:X::X/<0-128>]	Indica que direcciones serán anunciadas hacia los vecinos

ANEXO IV

CONFIGURACIONES BÁSICAS PARA LA IMPLEMENTACIÓN DE MULTIHOMING IPV4 E IPV6

Para poder realizar la comparación entre la implementación de Multihoming en IPv4 versus IPv6 aplicamos los conocimientos asimilados de BGP explicados en el Capítulo 2, los mismos que fueron puestos en práctica para emular un entorno Multihoming como se muestra en la siguiente figura.



Configuración básica Multihoming IPv4

```
EMPRESAX #configure terminal
EMPRESAX(config-line)#interface Loopback 10
EMPRESAX(config-if)#ip address 192.168.0.1 255.255.255.0
EMPRESAX(config-if)#interface Loopback 20
EMPRESAX(config-if)#ip address 192.168.1.1 255.255.255.0
EMPRESAX(config-if)#interface s0/0
EMPRESAX(config-if)#ip address 10.0.0.2 255.255.255.252
EMPRESAX(config-if)#no shutdown
EMPRESAX(config-if)#interface s0/1
EMPRESAX(config-if)#ip address 172.16.0.2 255.255.255.252
EMPRESAX(config-if)#no shutdown
EMPRESAX(config-if)#exit
EMPRESAX(config)#router bgp 300
EMPRESAX(config-router)#bgp router-id 3.3.3.3
EMPRESAX(config-router)#neighbor 10.0.0.1 remote-as 100
EMPRESAX(config-router)#neighbor 172.16.0.1 remote-as 200
EMPRESAX(config-router)#network 192.168.0.0
EMPRESAX(config-router)#network 192.168.1.0
EMPRESAX(config-router)#end

ISPA #configure terminal
ISPA(config)#interface s0/0
ISPA(config-if)#ip address 10.0.0.1 255.255.255.252
ISPA(config-if)#ipv6 enable
ISPA(config-if)#no shutdown
ISPA(config-if)#interface Loopback 0
ISPA(config-if)#ip address 12.0.1.1 255.255.255.0
ISPA(config-if)#exit
ISPA(config)#router bgp 100
ISPA(config-router)#bgp router-id 1.1.1.1
ISPA(config-router)#neighbor 10.0.0.2 remote-as 300
ISPA(config-router)#network 12.0.1.0 mask 255.255.255.0
ISPA(config-router)#end
```

De igual manera como se realizó la configuración en el primer ISP, se lo hará para el segundo, con las únicas diferencias en el direccionamiento.

Configuración básica Multihoming IPv6

A continuación mostraremos una configuración básica de un entorno multihoming, en el que una organización se encuentra conectada hacia dos proveedores de servicio de Internet al mismo tiempo con el fin de tener redundancia en su conexión. Para su configuración usamos el protocolo BGP para IPv6, en este caso eBGP dado que tanto la organización como los ISP's son sistemas autónomos diferentes.

```
EMPRESAX#configure terminal
EMPRESAX(config)#ipv6 unicast-routing
EMPRESAX(config-line)#interface Loopback10
EMPRESAX(config-if)#ipv6 address 2010:ABCD::1/64
EMPRESAX(config-if)#ipv6 enable
EMPRESAX(config-if)#interface Loopback20
EMPRESAX(config-if)#ipv6 address 2020:ABCD::1/64
EMPRESAX(config-if)#ipv6 enable
EMPRESAX(config-if)#interface s0/0
EMPRESAX(config-if)#ipv6 address 2001:100::4/64
EMPRESAX(config-if)#ipv6 enable
EMPRESAX(config-if)#no shutdown
EMPRESAX(config-if)#interface s0/1
EMPRESAX(config-if)#ipv6 address 2002:200::4/64
EMPRESAX(config-if)#ipv6 enable
EMPRESAX(config-if)#no shutdown
EMPRESAX(config-if)#exit
EMPRESAX(config)#router bgp 300
EMPRESAX(config-router)#bgp router-id 3.3.3.3
EMPRESAX(config-router)#no bgp default ipv4-unicast
EMPRESAX(config-router)#neighbor 2001:100::5 remote-as 100
EMPRESAX(config-router)#neighbor 2001:100::5 ebgp-multihop 2
EMPRESAX(config-router)#neighbor 2002:200::5 remote-as 200
EMPRESAX(config-router)#address-family ipv6
EMPRESAX(config-router-af)#neighbor 2001:100::5 activate
EMPRESAX(config-router-af)#neighbor 2002:200::5 activate
```

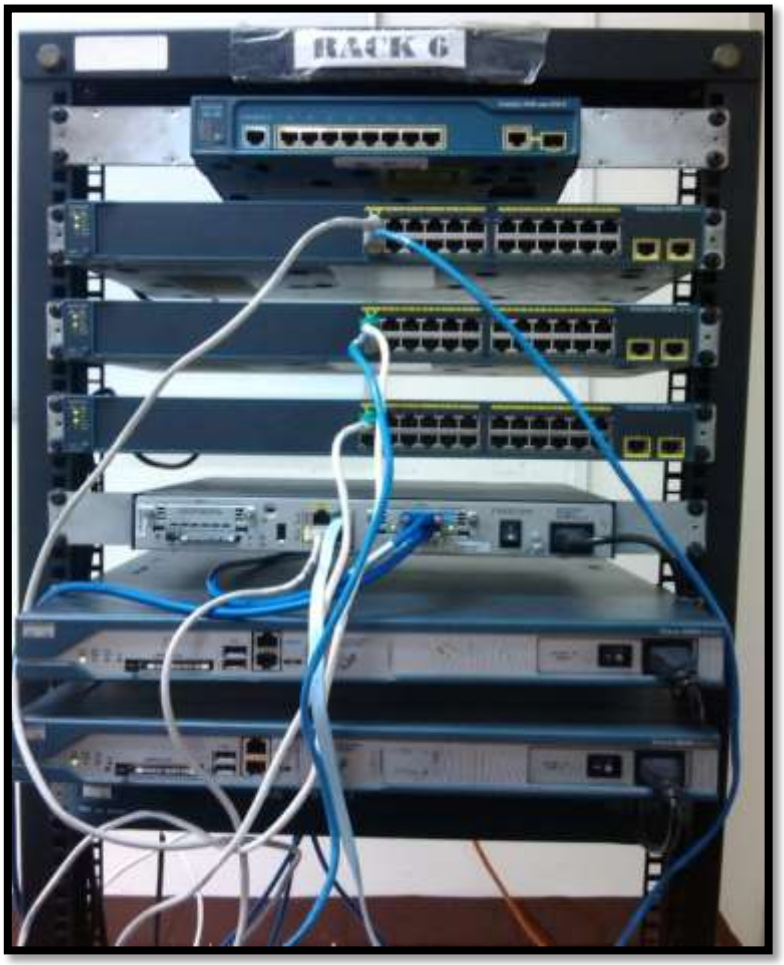
```
EMPRESAX(config-router-af)#network 2010:ABCD::/64
EMPRESAX(config-router-af)#network 2020:ABCD::/64
EMPRESAX(config-router-af)#exit-address-family
EMPRESAX(config-router)#end

ISPA#enable
ISPA#configure terminal
ISPA(config)#ipv6 unicast-routing
ISPA(config-line)#interface s0/0
ISPA(config-if)#ipv6 address 2001:100::5/64
ISPA(config-if)#ipv6 enable
ISPA(config-if)#no shutdown
ISPA(config-if)#exit
ISPA(config)#router bgp 100
ISPA(config-router)#bgp router-id 1.1.1.1
ISPA(config-router)#no bgp default ipv4-unicast
ISPA(config-router)#neighbor 2001:100::4 remote-as 300
ISPA(config-router)#address-family ipv6
ISPA(config-router-af)#neighbor 2001:100::4 activate
ISPA(config-router-af)#network 1000:1000::/64
ISPA(config-router-af)#exit-address-family
ISPA(config-router)#end
```

Tal como se hizo con el ISP A, se repite la configuración para el ISP B.

ANEXO V

FOTOGRAFÍAS TOMADAS DURANTE PRÁCTICAS REALIZADAS EN EL LABORATORIO DE CISCO-ESPOL PEÑAS



ANEXO VI

TABLA COMPARATIVA CONSOLIDADA DE LOS PROTOCOLOS DE ENRUTAMIENTO ORIENTADOS A IPV6, TANTO VECTOR DISTANCIA COMO ESTADO DE ENLACE EN BASE A LAS PRUEBAS REALIZADAS.

	RIPng	**EIGRP**	**OSPFv3**	**IS-IS**
Tiempo promedio de convergencia luego de la caída de un enlace	13,459 [s]	2,057 [s]	5,174 [s]	7,800 [s]
Tiempo promedio de convergencia luego de la subida de un enlace	5,012 [s]	5,457 [s]	19,422 [s]	14,697 [s]
Tiempo promedio de convergencia luego del reinicio del protocolo	17,088 [s]	13,313 [s]	15,008 [s]	11,992 [s]
Confiabilidad	88%	99%	98%	98%
Escalabilidad	BAJA	ALTA	ALTA	ALTA
Tasa de transferencia 3.541.193 Bytes	7,33 [Kb/s]	128,08 [Kb/s]	172,9 [Kb/s]	172,9 [Kb/s]
Tasa de transferencia 5.522.381 Bytes	8,94 [Kb/s]	149,25 [Kb/s]	85,6 [Kb/s]	73,87 [Kb/s]

BIBLIOGRAFÍA

[1] M. Canales. (2009, Octubre). *Protocolo de Internet IPv4*. [En línea]. Disponible en FTP: unizar.es Directorio: docencia_it/Protocolos de Comunicaciones/transparencias de clase/B1T1.1_IPv4_0910.pdf

[2] M. Peredos. (2013, Abril). *Historia del protocolo TCP/IP y IPv4 - IPv6*. [En línea]. Disponible en: www.redesiuv.blogspot.com/2013/04/historia-del-protocolo-tcpip-y-ipv4-ipv6.html

[3] G. L. Ahuatzin. (Octubre, 2005). *Teoría y métodos de transición IPv4 e IPv6*. [En línea]. Disponible en: www.catarina.udlap.mx/u_dl_a/tales/documentos/lis/ahuatzin_s_gl/capitulo2.pdf

[4] S. Ramírez, M. Cervantes. (2005, Noviembre). *Introducción al IPv6*. [En línea]. Disponible en: http://www.rau.edu.uy/ipv6/queesipv6.htm

[5] 6DEPLOY. (Junio, 2008). *IPv6 Addressing*. [En línea]. Disponible en: www.6deploy.org/tutorials2/0306deploy_ipv6_addressing_20120207_v2_0.pdf

[6] IETF. (1997, Enero). *RFC 2080 RIPng for IPv6* [En línea]. Disponible en: www.tools.ietf.org/html/rfc2080

[7] K. P. Singh, P. K. Gupta, G. Singh. (2013, Mayo). *Performance Evaluation of Enhanced Interior Gateway Routing Protocol in IPv6 Network*. [En línea]. Disponible en: www.arxiv.org/ftp/arxiv/papers/1305/1305.4311.pdf

[8] A. Hinds, A. Atojoko, S. Y.Zhu. (2013, Agosto). *Evaluation of OSPF and EIGRP Routing Protocols for IPv6.* [En línea]. Disponible en: www.ijfcc.org/papers/169-C005.pdf

[9] E. C. Cabeza. (2009, Mayo). *Cabeceras de extensión de IPv6*. [En línea]. Disponible en: www.eduangi.com/2009/05/25/cabeceras-de-extension-de-ipv6

[10] A. Pérez. (2002, Julio). *Infraestructura de un ISP*. [En línea]. Disponible en: www.dit.upm.es/david/TAR/trabajos2002/10-Infraestructura-ISP-Andoni-Perez-res.pdf