UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS

INVESTIGACION Y DISEÑO DE UNA METODOLOGIA QUE PERMITA APLICAR EL RUTEO DE PAQUETES DE DATOS EN UN PROTOTIPO QUE IMPLEMENTE LA SUITE DE PROTOCOLOS IPV6.

PRESENTADO POR:

LUIS SALADOR BARRERA MANCÍA
ERICKA FABIOLA HENRÍQUEZ CAMPOS
DANIEL ERNESTO TUTILA HERNÁNDEZ

PARA OPTAR AL TÍTULO DE:

INGENIERO DE SISTEMAS INFORMÁTICOS

CIUDAD UNIVERSITARIA, DICIEMBRE DE 2007

UNIVERSIDAD DE EL SALVADOR

RECTOR :

ING. RUFINO ANTONIO QUEZADA SÁNCHEZ

SECRETARIO GENERAL :

LICDO. DOUGLAS VLADIMIR ALFARO CHÁVEZ

FACULTAD DE INGENIERÍA Y ARQUITECTURA

DECANO :

ING. MARIO ROBERTO NIETO LOVO

SECRETARIO :

ING. OSCAR EDUARDO MARROQUÍN HERNÁNDEZ

ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS

DIRECTOR :

ING. JULIO ALBERTO PORTILLO

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS

TRABAJO DE GRADUACIÓN PREVIO A LA OPCIÓN AL GRADO DE:

INGENIERO DE SISTEMAS INFORMÁTICOS

TÍTULO :

INVESTIGACION Y DISEÑO DE UNA METODOLOGIA QUE PERMITA APLICAR EL RUTEO DE PAQUETES DE DATOS EN UN PROTOTIPO QUE IMPLEMENTE LA SUITE DE PROTOCOLOS IPV6.

PRESENTADO POR :

LUIS SALVADOR BARRERA MANCÍA
ERICKA FABIOLA HENRÍQUEZ CAMPOS
DANIEL ERNESTO TUTILA HERNÁNDEZ

TRABAJO DE GRADUACIÓN APROBADO POR

DOCENTE DIRECTOR :

ING. PEDRO ELISEO PEÑATE

SAN SALVADOR, DICIEMBRE DE 2007

TRABAJO DE GRADUACIÓN APROBADO POR:

DOCENTE DIRECTOR :

ING. PEDRO ELISEO PEÑATE

AGRADECIMIENTOS

Durante estos años de estudio profesional, siempre soñé que un día escribiría los agradecimientos de mi tesis, lo que supondría que estaba parcialmente terminada. Ahora ese momento ha llegado y no se muy bien por donde empezar ya que han sido tantas las personas a las cuales debo parte de este triunfo, de lograr alcanzar mi culminación académica, la cual han apoyado durante todo este tiempo, de muy distinta forma, en momentos no pocos difíciles. Sin ellos este trabajo nunca habría visto la luz. A todos ustedes MUCHAS GRACIAS. Ahora se termina una etapa más de mi vida y comienza otra, del que espero también formen parte.

Gracias a mi Dios

Categóricamente, Dios Padre, Dios Hijo y Dios Espíritu Santo, mi Señor, mi Guía, mi Proveedor, mi Principio y mi Fin Ultimo; Quien me ha dado la oportunidad de existir, Fortaleza, Sabiduría, Ciencia y Conocimiento desde que lo deje morar en mi vida y mi corazón; por estar conmigo en cada paso que doy, por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio, Quien sabe lo esencial que ha sido en mi posición constante de alcanzar esta meta, esta alegría, que si pudiera hacerla material, la hiciera para entregársela, pero a través de esta meta, podré siempre de su mano alcanzar otras que espero sean parte del cumplimiento de Sus propósitos para mi vida y desde luego para Su Gloria y Honra. PADRE INFINITAS GRACIAS por ser parte de mi vida; eres lo mejor que me ha pasado.

Gracias a mi Mamá Linda

En primer lugar por encomendarme siempre a Dios para que saliera adelante. Yo se que sus oraciones fueron escuchadas. En segundo lugar por su cariño, comprensión, sacrificios y apoyo absoluto e ilimitado, por ser mi intermediaria aquí en la tierra, por guiarme sobre el camino de la educación y enseñarme a tener carácter. Creo ahora entender porque me obligaba a estudiar las clases a diario, a terminar mis tareas antes de salir a jugar y muchas otras sin fin de cosas más que no terminaría de mencionar. Su sacrificio, se convirtió en su triunfo y el mío. LE AMO MUCHO!

Gracias a mi Familia

Mis padres, mis hermanos, mis tíos y mis primos por darme la estabilidad emocional, sentimental y económica; porque a pesar de no estar cerca, se que procuraron siempre mi bienestar y esta claro que si no fuese por el esfuerzo realizado por ustedes para poder llegar alcanzar este logro, definitivamente no hubiese podido ser realidad. GRACIAS por darme la posibilidad de que de mi boca salga esa palabra…FAMILIA. En especial a mi padre, por su sacrificio en algún tiempo incomprendido, porque gracias a su cariño, guía y apoyo he llegado a realizar uno de los anhelos más grandes de la vida, fruto del inmenso apoyo, amor y confianza que en mí depositó. A mi

Madre, gracias porque nunca pensé que emanara tanta fuerza y entusiasmo para sacar adelante a alguien, aun con las adversidades y quebrantos de salud que se le ha presentado, será siempre mi inspiración para alcanzar mis metas, por enseñarme que todo se aprende y que todo esfuerzo es al final recompensado. Sus esfuerzos y luchas, se convirtieron en nuestro triunfo, con los cuales he logrado terminar mis estudios profesionales que constituyen el legado más grande que pudiera recibir y por lo cual les viviré eternamente agradecido a todos.

Gracias a mi familia postiza la Familia Zúniga

Por su ejemplo de superación incansable, por su comprensión y confianza; por su amor y amistad incondicional, porque sin su apoyo no hubiera sido posible la culminación de mi carrera profesional. Por lo que han sido y serán…MIL GRACIAS.

Gracias a todos mis Amigos

Que estuvieron conmigo compartiendo tantas mañanas, tardes y noches de estudio y experiencias, momentos de nerviosismo, donde compartimos conocimientos y alcanzamos triunfos, que me ayudaron a crecer y madurar como persona y como profesional. A mis amigos que están siempre conmigo apoyándome en todas las circunstancias posibles, que también son parte de esta alegría. Y a los que seguirán estando, brindándome cariño y soporte.

Gracias a mis Compañeros de Tesis

Ericka, Daniel e incluyo a la Sra. Rosa A. Henríquez, que si bien no fue parte del grupo legalmente, fue un pilar en los ánimos y desarrollo de esto. Gracias al dúo dinámico por permitirme ser parte del grupo de trabajo, porque fueron mi apoyo durante este agradable y difícil periodo académico, quienes me ayudaron a escalar este último peldaño de esta etapa para poder alcanzar este sueño, este MI SUEÑO, que ahora es una realidad.

Gracias a mis Asesores

Observador y Director que no sólo facilitaron el desarrollo de este trabajo, sino que hicieron un importantísimo aporte a la formación de este proyecto, en especial al Ing. Pedro Peñate sus asesorias, consejos, conocimientos, paciencia y opinión sirvieron para que me sienta satisfecho de mi participación dentro del proyecto de investigación.

Y a todos aquellos, que han quedado en los lugares más recónditos de mi memoria, pero que fueron participes en trabajar mi persona, GRACIAS, MUCHAS GRACIAS.

Luis Salvador Barrera Mancía

AGRADECIMIENTOS

Termina una etapa de mi vida donde se ha cumplido una de mis metas más importantes ya que esta me ayudará a enfrentar una nueva. Existen muchas personas que me ayudaron a enfrentar esta parte de mi vida.

Primero que todo le agradezco mucho a Dios y a la Virgen por todas las bendiciones recibidas en este transcurso del tiempo que estuve en la Universidad.

Le agradezco de todo corazón a las personas más importantes de mi vida mi papi, mi mami, y mi hermano ya que gracias a su cariño, guía y apoyo he logrado terminar mis estudios profesionales que constituye el legado más importante que he recibido, por todo muchas gracias y los quiero mucho.

A mi abuelita Rosa, a mi abuelo José que este año dejo de estar físicamente con nosotros les agradezco que siempre estaban pendiente de mi. A todos mis tíos, tías, primos, primas que estuvieron presentes en este paso por la universidad. Pero especialmente a la Familia Chávez Campos por apoyarme en esta etapa de mi vida.

A mis compañeros de tesis a Salvador pero especialmente a Daniel ya que has sido una persona muy importante en esta etapa de mi vida, además por aguantarme en mis momentos de locuras y enojos.

A mis compañeros y amigos Rafa, Claudia (Wawa), Sueco (Raúl), Gordo (Oscar), Ercilia, Julín que siempre estuvieron en los buenos y malos momentos que pasamos en la U, las desveladas que pasábamos porque teníamos que entregar un trabajo o teníamos parcial. Y a todos los compañeros con los que conviví en estos 5 años de estudio.

A Natalia por apoyarme en los buenos y malos momentos, ayudarme en la tesis y por todos esos ratos que pasamos platicando.

A mis asesores el Ing. Peñate e Ing. Chicas por ayudarnos en el desarrollo de este trabajo.

A Iris, Migdonia y a todas esas personas que siempre estuvieron presentes en el transcurso de esta etapa. Muchas gracias a todos.

Ericka Fabiola Henríquez Campos

AGRADECIMIENTOS

Antes que nada quiero agradecer a Dios, a la virgen María y a su hijo Jesús por todo el apoyo que recibí de ellos, especialmente en todas las noches de estudio en las que se mantuvieron a mi lado dándome fuerzas para continuar.

Agradezco a mi familia que siempre me dio su ayuda para poder concluir con éxito mi carrera, especialmente a mi papá y a mi madre que siempre me apoyaron en todo y que sin el ejemplo de ellos nunca hubiera podido alcanzar esta meta de convertirme en un profesional, a mi hermana y a mi hermano de quienes he aprendido mucho y que nunca han dejado de preocuparse por mi. A mi tía Silvia y a don Ricardo, quienes me acogieron dentro de su hogar como a un hijo, también le agradezco a mis primos Pablo y Ricardito por los momentos de diversión con los que escapaba de la monotonía del estudio. A mi tía Mayra y a mi tío Luis de quienes recibí mi primera computadora y siempre me ayudaron frente a cualquier necesidad que tuviera. A mis abuelos que siempre me brindaron sus sabios consejos y porque siempre estuvieron pendientes de mi a lo largo de toda mi carrera, y a toda mi familia que me ayudaron en todo momento.

A mis compañeros de tesis Luis y Ericka quienes me enseñaron mucho mientras desarrollábamos este proyecto, pero sobre todo a ti Ericka por haberte convertido en el apoyo que necesite en los momentos más difíciles y porque te convertiste en una persona muy valiosa para mí. Agradezco también a la Familia Henríquez Campos que siempre nos apoyaron y siempre nos brindaron una mano de ayuda para alcanzar con éxito la culminación e este proyecto.

A mis compañeros y amigos a Rolando por aquellas noches en vela para estudiar mate, a Rafa, Claudia, Raúl “el sueco”, Julio por todos los días que compartimos y especialmente por todas aquellas noches en vela que pasábamos entregando lo mejor de cada uno para entregar el mejor trabajo de todos, y a todos mis compañeros con quienes compartí clases. A las personas que conocí durante el tiempo que le dedique a la asociación de estudiantes y con quienes compartí grandes momentos a William, Rudy, Carlos Vásquez, Gustavo, Sofía, Robin y muchos otros con quienes me identifique en su búsqueda de la excelencia estudiantil y por la lucha de forjar una mejor universidad para todos, a Manuel, José David “el Gato”, Roger y a todos los que estuvieron involucrados en el grupo LinUes, especialmente a Carlos Marín por haber puesto la primera piedra para que este grupo se formara.

A nuestros asesores, el Ing. Pedro Peñate y el Ing. Rudy Chicas por brindarnos su apoyo, experiencia y porque siempre nos brindaron toda su confianza en el desarrollo de este proyecto.

Daniel Ernesto Tutila Hernández

INDICE

PARTE I

MANUAL DE REFERENCIA DE LOS PROTOCOLOS DE RUTEO RIPNG, OSPF Y BGP PARA IPV6

CAPITULO I

PROTOCOLO DE INFORMACIÓN DE RUTEO PARA PRÓXIMA GENERACIÓN

CAPITULO II

PROTOCOLO DE RUTEO OSPF PARA IPv6

CAPITULO III

PROTOCOLO DE RUTEO BGP4 PARA IPV6

PARTE II

METODOLOGÍA PARA LA CONSTRUCCIÓN DE UN PROTOTIPO DE RED QUE IMPLEMENTE RUTEO CON IPV6

CAPITULO I

METODOLOGÍA PARA LA CONSTRUCCIÓN DE UN PROTOTIPO DE RED QUE IMPLEMENTE RUTEO CON IPV6

ANEXOS

INTRODUCCIÓN

El ruteo de paquetes es la función más complicada pero a las vez la más importante en las redes de comunicación, ya que de dicha función depende si se tiene éxito en el acceso y comunicación de datos entre una computadora y otra que se encuentra alojada en una red diferente.

Dado que en una red pueden existir muchos caminos con los que una computadora puede establecer comunicación con dispositivo de red, se tiene la necesidad de contar con mecanismos que evalúen todos los posibles caminos que se tengan disponibles para establecer comunicación, y tomen la decisión de elegir un camino por el cual se establezca dicha comunicación, esta decisión es tomada por los router gracias a protocolos que estos utilizan para la evaluación de rutas.

Por tal razón, el proyecto que se presenta a continuación, pretende estructurar el conocimiento fundamental de la implementación de los protocolos de ruteo en IPv6, al mismo tiempo, se manejará como soporte para el contagio del conocimiento.

Debido a que la experiencia práctica es un factor importante para que el proyecto se enmarque dentro de un enfoque de ingeniería, se plantea el desarrollo de un prototipo funcional en el área propuesta.

El documento se divide en dos partes. En la primera parte se muestra el resultado de la investigación de la suite de protocolos de ruteo, la cual esta dividida en 3 capítulos que contienen las características de los protocolos RIPng, OSPFv3 y BGP+4.

En la segunda parte se desarrolla el diseño de la metodología para la construcción de un prototipo de red que implementa ruteo con IPv6. Esta segunda parte esta dividida en dos secciones, en la primera se describe de forma general la metodología propuesta para la construcción de un prototipo y en la segunda sección se muestra un ejemplo practico de esta metodología.

OBJETIVOS

OBJETIVO GENERAL

Realizar una investigación sobre las técnicas de ruteo utilizadas en el protocolo de Internet versión seis (IPv6), con el propósito de crear una metodología que permita la configuración de un prototipo funcional que aplique dichas técnicas, para que pueda ser utilizada por empresas u organizaciones.

OBJETIVOS ESPECÍFICOS

- Presentar una investigación acerca de los protocolos de ruteo en IPv6 y sus características esenciales con el objeto de documentar sobre estos.

- Diseñar un método que muestre la implementación de los protocolos de ruteo en IPv6, tomando en cuenta criterios tecnológicos y requerimientos de información.

- Aplicar la metodología desarrollada en la elaboración de un prototipo funcional, que utilice las técnicas de ruteo de IPv6.

ALCANCES

- La información técnica que aporta este documento, permitirá ser aplicada en cualquier empresa que utilice TIC.

- En el montaje del prototipo funcional se hará uso de un software especializado para la simulación de routers que muestren el funcionamiento de los protocolos investigados.

IMPORTANCIA

Con el desarrollo de la versión seis del protocolo de Internet y la adopción que algunos países están realizando en sus redes de comunicación, se mira cada vez más marcado el paso de adopción de este protocolo en las comunicaciones; es por esto que es importante contar con los recursos necesarios para llevar a cabo acciones que beneficien la utilización del protocolo de Internet versión seis en el país.

La Universidad de El Salvador, como un ente precursor de investigaciones tecnológicas y específicamente la Escuela de Ingeniería de Sistemas Informáticos, tiene como fin realizar investigaciones referentes a nuevas tecnologías que sean capaces de afectar de manera favorable al desarrollo del país, por tal razón esta investigación ayuda a alcanzar este objetivo institucional ya que impulsa el desarrollo tecnológico del país presentando recursos y herramientas para que se lleve a cabo una revolución tecnológica adoptando la ultima versión del protocolo de Internet y, más específicamente con esta investigación, la implementación de ruteo utilizando este mismo protocolo.

Tomando en cuenta el punto de vista técnico de la utilización de ruteo con IPv6 conlleva de forma implícita todas las ventajas de la utilización de IPv6, es decir se gana una mayor seguridad, escalabilidad, mayor número de direcciones, movilidad entre otros[1], con lo cual se dejan de lado todos los inconvenientes que presenta la utilización del protocolo de Internet versión cuatro.

En el ámbito académico, el desarrollo de esta investigación beneficiará a los estudiantes de la carrera de ingeniería de sistemas informáticos como a estudiantes de carreras afines a esta, ya que podrá ser usado como modelo para el desarrollo de investigaciones, permitiendo la realización de investigaciones que aporten un mayor conocimiento de las TIC's. Por otra parte el conocimiento y la experiencia resultante de la investigación podrían ser utilizadas como base para la creación de una nueva asignatura para la carrera en el área de las telecomunicaciones.

[1]Para mayor información referirse al trabajo de graduación: “DISEÑO DE UNA METODOLOGIA QUE PERMITA IMPLEMENTAR EL PROTOCOLO DE INTERNET VERSION 6 EN EMPRESAS O INSTITUCIONES CON APLICACIONES BASADAS EN EL PROTOCOLO TCP/IP VERSION 4”

JUSTIFICACIÓN

Al hablar de ruteo usando IPv6 es inevitable mencionar el uso del protocolo IPv6 y de las ventajas que este presenta frente a su predecesor IPv4, es por ello que con el uso de IPv6 en los router se reducirán las tablas de ruteo, mejorando así los tiempos de respuesta, además se contará con soporte nativo para permitir la Calidad de Servicio (QoS), Seguridad (IPsec) con lo que se alcanza un mejor rendimiento y seguridad en comunicación entre diferentes redes, estos beneficios se pueden alcanzar con IPv4, pero se tenia que implementar por medio de parches, lo que significa configuraciones adicionales para lograr dicha configuración.

Al presentar esta investigación se pretende incidir de forma directa a las micro, pequeña y medianas empresas que utilizan TIC, ya que estas presentan un gran interés en la adopción de TIC como herramienta empresarial, prueba de ello es el 71.5% de PYMES están dispuestas a incursionar en el comercio electrónico, y un 60% que desean tener su propio sitio Web[2], es a estas empresas a las que se les ayudaría en el proceso de adopción de IPv6, ya que se les presentará una herramienta para la configuración de sus router utilizando el protocolo IPv6.

Con la elaboración de esta investigación se dará un aporte académico a la comunidad estudiantil, el cual le ayudará en su formación como futuro profesional, entregando de manera ordenada y sistemática los resultados obtenidos y experiencias adquiridas durante la investigación y dejándolo estampado en una documentación escrita, además los estudiantes podrán utilizar los resultados de esta investigación como bases para una investigación más profunda.

[2]Datos obtenidos del documento "Situación y tendencia en el desarrollo de la E-MIPYME en El Salvador " elaborado por CONAMYPE para el "Seminario sobre Estrategias para el Desarrollo de la E-MIPYME", Panamá, octubre de 2006.

I. METODOLOGÍA PARA LA SOLUCIÓN DEL PROBLEMA

1. FORMULACIÓN DEL PROBLEMA

Necesidad de contar con una investigación que muestre de manera sistemática la utilización de ruteo con la suite de protocolos de IPv6, para desarrollar una metodología que permita su aplicación en las empresas u organizaciones.

Medio Ambiente: Tecnología de redes, equipo de computo y software especifico.

2. PLANTEAMIENTO DEL PROBLEMA

Estado A

Ruteo con suite IPv4

- Necesidad de documentación referente al tema de ruteo usando la suite de protocolos de IPv6.
- Adopción de la última versión del protocolo de Internet versión 6 para estar a la vanguardia de la tecnología mundial.
- Redes implementadas con IPv4 que serán migradas a IPv6.

Estado B

Ruteo con suite IPv6

- Documentación de referencia que contiene los resultados de la investigación acerca de la implementación de ruteo usando el protocolo IPv6.

- Metodología que facilité la implementación de ruteo con IPv6 en las empresas u organizaciones.
- Prototipo funcional aplicando la metodología diseñada para la implementación de ruteo con IPv6.

II. METODOLOGIA PARA EL DESARROLLO DEL PROYECTO

La metodología del desarrollo del proyecto se encuentra catalogada en dos tipos distintos, las cuales se mencionan a continuación:

- Metodología para desarrollo de la Investigación documental
- Metodología para la Implementación y Prueba experimental del Prototipo Funcional

En los siguientes apartados se formaliza y detalla cada una de estas metodologías.

1. METODOLOGÍA PARA EL DESARROLLO DE LA INVESTIGACIÓN DOCUMENTAL

A. Profundidad de la Metodología para la Primera Etapa

Se realizará la investigación con el propósito de destacar desde los aspectos y componentes fundamentales del ruteo de paquetes de datos en IPv6, pasando por conceptos, metodologías, procedimientos, técnicas, que permitan la inferencia teórica-técnica, hasta sus actualizaciones más recientes. Además de obtener un panorama general de la investigación y desarrollo de las TIC's en el área de las telecomunicaciones de las tecnologías de la suite de protocolo de ruteo en IPv6 en nuestro país y conocer las motivaciones para la iniciación del proyecto, creando procedimientos adecuados para hacer de esta, una promotora de otros tipos de investigaciones posteriores. Tomando en cuenta aspectos relacionados directa o indirectamente con el desarrollo de normativo del proyecto y sus antecedentes; valiéndose de diferentes tipos de fuentes documentales.

B. Fuentes Documentales para la Primera Etapa

Para la investigación se hará uso de dos tipos de fuentes documentales: primarias y secundarias. A continuación se detalla cada una de las fuentes especializadas en la tecnología a emplear y otras afines.

Fuentes primarias:

· Libros, normativas impresos y de Web

· Manuales Request For Comments (RFCs)

· Encuestas en la Web (datos estadísticos)

· Asesoría de experto

Fuentes secundarias:

· Publicaciones Web

· Foros en la Web

2. DESARROLLO DE LA METODOLOGÍA PARA PRIMERA ETAPA

· Orientación con asesor experto en el área de las telecomunicaciones para la localización de fuentes documentales en base a su experiencia.

· Exploración de la información vinculada íntimamente con el fondo del proyecto en todo tipo de fuentes documentales.

· Extracción y recopilación de la información, ideas, conceptos, metodologías, procedimientos, técnicas, que permitan la inferencia teórica-técnica.

· Selección y clasificación de la información en documentos y archivos digitales.

· Formulación, desarrollo y diseño, de la investigación documental desde la perspectiva teórica-técnica hacia el conocimiento tecnológico, que permita crear un supuesto concerniente a la implementación del prototipo funcional ligada al proyecto.

· Revisión de la información extraída, recopilada, seleccionada y clasificada para efectuar posibles modificaciones al producto final de la investigación.

3. METODOLOGÍA PARA LA IMPLEMENTACIÓN Y PRUEBA EXPERIMENTAL DEL PROTOTIPO FUNCIONAL

1. Profundidad de la Metodología para Segunda Etapa

Se realizará la investigación experimental con el propósito de diseñar y aplicar un método que demuestre la implementación y prueba de los protocolos y técnicas de ruteo en IPv6, en un prototipo funcional dentro de un laboratorio, que posteriormente se probará en otras redes de instituciones, tomando en cuenta criterios tecnológicos y requerimientos de información necesarios. Se planea realizar las pruebas experimentales de forma local.

El desarrollo de esta metodología tiene cuatro componentes, los cuales son: Investigación, Implementación, pruebas y documentación, las cuales se trabajarán en 10 fases. Esta se detalla en el apartado “Desarrollo de la Metodología para Segunda Etapa”.

2. Fuentes Documentales

Para la investigación experimental, al igual que la metodología anterior, se hace uso de dos tipos fuentes documentales, las primarias y las secundarias, y se catalogan de la siguiente manera:

Fuentes primarias:

· Manual Request For Comments (RFCs)
· Libros, estándares y normas impresos y de Web
· Asesoria de experto

Fuentes secundarias:

· Publicaciones Web

· Foros en la Web

· Guías de Prácticas de laboratorio

3. Desarrollo de la Metodología para Segunda Etapa

· **Manejo de las capas inferiores:** Se debe conocer el manejo de la capa que se utilizará, así como los pasos necesarios a seguir para establecer la conexión.

· **Lectura/algoritmo para suite de protocolos:** Se estudiarán el protocolo de compuerta de frontera (BGP), el protocolo de información de encaminamiento (RIP) y el camino abierto más corto primero (OSPF) y todos los componentes técnicos y actualizaciones, especificados en investigación y documentación técnica efectuada en la Primera Etapa de este proyecto, a partir de los cuales se escribirá un algoritmo o diagrama de flujo para la futura implementación.

· **Lectura/algoritmo IPv6:** Se leerán los RFCs más importantes relacionados con IPv6 (principalmente el 2460) y a partir de ellos escribir un algoritmo o diagrama de flujo para la futura implementación del ruteo con la suite de protocolos de IPv6.

· **Escoger/Aprender a utilizar:** a partir de los algoritmos realizados se tendrá una idea de las exigencias del hardware y software, tomando en cuenta la disponibilidad de las capas inferiores a utilizar y se decidirá lo que se utilizará (en caso que se efectúen ciertos cambios de hardware o software con la idea inicial), para luego aprender a manejar las herramientas necesarias para el desarrollo del prototipo.

· **Implementación/adquisición de hardware para la implementación de prototipo:** Esta fase se desarrollará en 2 etapas, la primera se realizará en paralelo a la fase 2 y 3, en esta se buscará implementaciones existentes y la forma de manejo. La segunda etapa se encargará de la utilización de esta para comunicarse y las aplicaciones a manejar, a partir del cual permitirá diseñar y establecer la red a implementar para el prototipo.

· **Implementación:** Al igual que en la fase anterior se realizará en 2 etapas, en la primera se hará el montaje de la red según requerimiento y diseño establecido en la fase anterior. La segunda etapa se encargará de la utilización de los algoritmos desarrollados en las fases 2 y 3, basado en el conocimiento del comportamiento de estas, adquirido en el desarrollo de las etapas anteriores.

· **Pruebas y ajustes:** Se realizarán pruebas y se definirán las condiciones de comunicación entre redes distintas, a partir de las cuales se harán los ajustes necesarios. Además de ello, en esta fase se presumirá el número de post-pruebas que se aplican en caso de fallo.

· **Manejo y desarrollo:** Para realizar el prototipo funcional es necesario conocer los comandos que puede recibir y enviar. Además, conocer la interfaz necesaria para la comunicación de forma local y remota, y confrontará los estados iniciales y finales de las mismas.

· **Pruebas y ajustes del prototipo:** Se definirá el número de usuarios para las redes y se les realizarán pruebas con el fin hacer los ajustes necesarios para su buen funcionamiento del prototipo.

· **Documentación**: Durante todo el proceso se realizará la documentación experimental del trabajo que se esta perpetrando. En él, se formalizarán y justificarán los elementos y componentes presentes antes, mientras y durante el desarrollo de las pruebas, con detalles minucioso de todo lo acontecido.

PARTE I

MANUAL DE REFERENCIA DE LOS PROTOCOLOS DE RUTEO RIPNG, OSPF Y BGP PARA IPV6.

CAPITULO I

PROTOCOLO DE INFORMACIÓN DE RUTEO PARA PRÓXIMA GENERACIÓN

1. ORIGINES DE RIPNG[3]

Uno de los protocolos de ruteo más antiguos es el Routing Information Protocol, este utiliza el algoritmo vector distancia para calcular sus rutas. Los algoritmos de vector distancia utilizados por RIP están basados en los algoritmos implementados por ARPANET en el año 1969. El algoritmo vector distancia fue descrito por R.E. Bellman, L.R. Ford Jr y D.R. Fulkerson[4].

La primera organización que implementó un protocolo de vector distancia fue la compañía Xerox en su protocolo GIP[5], este protocolo estaba incluido dentro de la arquitectura XNS[6]. GIP se utilizaba para intercambiar información de ruteo entre redes o sistemas autónomos no compatibles.

Poco después la Universidad de California en Berkeley creo una variante llamada “Routed”, esta variante del GIP introdujo novedades como la modificación del campo de direccionamiento, que logró hacerse más flexible[7]. También se añadió un temporizador que limitaba a 30 segundos el tiempo máximo de actualización, es decir, el tiempo máximo permitido sin saber la información de los vecinos.

El protocolo RIP, tal cual se conoce actualmente, fue descrito por primera vez en el RFC[8] 1058 por Chuck Hedrick de la Rutgers University en Junio de 1988, y posteriormente fue mejorado en el RFC 2453 por G.Malkin de la compañía Bay Networks en Noviembre de 1998. Mientras tanto, paralelo a este ultimo suceso, RIP para IPv6 daba sus primeros pasos en Enero 1997 atribuida esta última versión a G. Malkin y R.Minnear.

[3] RIPng - Del Inglés *Routing Information Protocol for Next Generation*
[4] Estos estudios sobre algoritmos de vector distancia fueron publicados por la Princeton University Press.
[5] GIP - Del Inglés *Gateway Information Protocol*
[6] XNS - Del Inglés *Xerox Network Systems*
[7] El campo de direccionamiento se podía utilizar por XNS y por IP.
[8] RFC: Request For Comments – Petición de Comentarios.

2. GENERALIDADES DE LA ARQUITECTURA RIPNG

RIPng es un protocolo de compuerta de enlace interna IGP[9], utilizado por routers que pueden actuar en equipos para intercambiar información con redes IP. Este protocolo tiene como trasfondo una serie de teorías y formulaciones matemáticas que serán tratadas brevemente en esta sección. La arquitectura de este protocolo ha sido diseñada con base a las versiones de RIPv1-RIPv2[10], además de la arquitectura funcional para IPv6. En la figura 1 se muestra la arquitectura para RIPng.

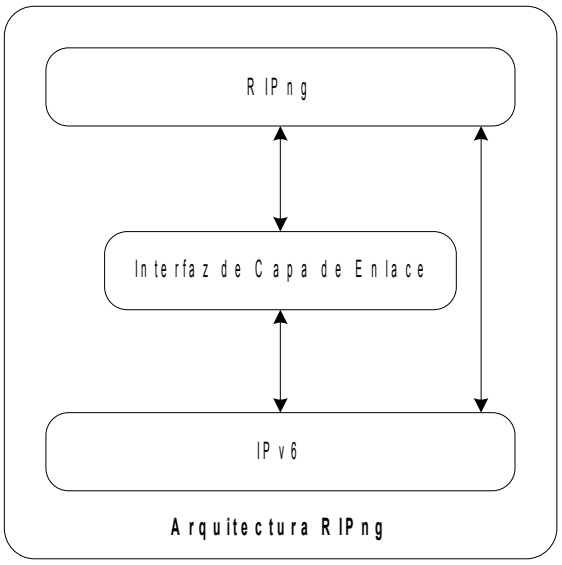

Figura 1: Arquitectura RIPng.

RIPng puede ser utilizado para manejar tecnologías y estándares de plataformas de servidores. Este es un software de control que puede también ser integrado dentro de un amplio rango de entornos de procesos que son previamente configurados para soportar diferentes sistemas operativos.

[9] IGP – Del Inglés *Internal Gateway Protocol, hace referencia a los protocolos usados dentro de un Sistema Autónomo.*

[10] Para las explicaciones detalladas respecto al algoritmo del vector distancia, ver RFC 1058 (RIPv1) y RFC 2453 (RIPv2).

3. ADAPTACIÓN DE RIP A RIPNG

En el protocolo RIPng se observan cambios sustanciales que han sido realizados con el propósito de añadir seguridad adicional y fiabilidad del servicio sobre algunas amenazas a los routers. Dentro de los cambios que encontramos para esta última versión, se destaca el de cabeceras de paquetes, que hacen que otras cabeceras sean opcionales utilizando cabeceras de extensión. Además, la dirección del enlace local de origen, la dirección de ámbito de enlace multicast destino, el próximo salto y el salto limitado son todas características de ámbito. La tabla 1 expone los cambios de RIP para IPv6.

Características	Descripción
Rutas anunciadas	RIPng anuncia las rutas IPv6 compuesto por: prefijo IPv6, tamaño del prefijo y métrica.
Próximo salto	Dirección del enlace local IPv6 conectado directamente con la interfaz física del router anunciado por el prefijo utilizado para alcanzar el próximo salto.
Protocolo de Transporte IP	IPv6 emplea el protocolo de transporte UDP para trasladar datagramas RIPng.
Origen de dirección IPv6	RIPng actualiza la dirección de origen IPv6 en la dirección de enlace local de la interfaz original del router, excepto cuando responde a un mensaje de petición unicast desde un puerto a otro que no sea el puerto RIPng, cuando la dirección de origen es una dirección global valida.
Destino de dirección IPv6	RIPng actualiza la dirección de origen IPv6 en ff02::9 a todas las direcciones multicast de los routers RIPng. Solo los routers RIPng escuchan la dirección multicast por el ámbito de enlace local de la dirección multicast, que no reenvían a otro enlace.
Salto limitado = 255	RIPng debe actualizar el paquete IPv6 fijando el Salto Limitado a 255 . Esto permite al router oyente verificar si las actualizaciones llegan desde los routers exteriores.
Puerto = 521	El puerto UDP es 521 en lugar de 520 para versiones anteriores.
Versión RIPng = 1	El número de la versión del paquete RIPng es 1, esto significa que es la primera versión de RIPng. Usado desde un puerto de transporte distinto, los routers oyentes pueden diferenciar los paquetes desde cualquier versión anterior inclusive a RIPng.
Tabla de Ruteo	La Tabla de Ruteo IPv6 es por defecto anunciada con ::/0
Autenticación	La Autenticación es colindante a la seguridad IPsec. Cualquier especificación de autenticación RIPng es eliminada.

Tabla 1: Características RIPng.

4. ALGORITMO DEL VECTOR DISTANCIA PARA RIPNG

Cada router conserva una tabla de ruteo listando y enumerando la mejor ruta para cada ruta IPv6. La figura 2 muestra un ejemplo de una tabla de ruteo de RIpng.

```
grupo24@debian3:~$ telnet ::1 ripngd
Trying ::1...
Connected to ::1.
Escape character is '^]'.
Hello, this is Quagga (version 0.99.5).
Copyright 1996-2005 Kunihiro Ishiguro, et al.
User Access Verification
Password:
debian17> en
debian17# show ipv6 ripng
Codes: R - RIPng, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes: (n) - normal, (s) - static, (d) - default, (r) - redistribute,
           (i) - interface, (a/S) - aggregated/Suppressed

   Network              Next Hop            Via     Metric Tag Time
R(n) 2010::/64  fe80::206:4fff:fe4b:4591    eth0       2    0  11:51
R(n) 2020::/64  fe80::206:4fff:fe4b:4591    eth0       2    0  11:51
R(n) 2030::/64  fe80::206:4fff:fe4b:4591    eth0       2    0  11:51
R(s) 2040::/64  ::                          self       1    0
R(n) 3050::/64  fe80::206:4fff:fe4b:4591    eth0       2    0  11:51
R(n) 3060::/64  fe80::206:4fff:fe4b:4591    eth0       2    0  11:51
R(n) 3070::/64  fe80::206:4fff:fe4b:4591    eth0       2    0  11:51
R(n) 3080::/64  fe80::206:4fff:fe4b:4591    eth0       2    0  11:51
R(n) 4010::/64  fe80::206:4fff:fe4b:4591    eth0       2    0  11:51
R(n) 4020::/64  fe80::206:4fff:fe4b:4591    eth0       2    0  11:51
R(n) 4030::/64  fe80::206:4fff:fe4b:4591    eth0       2    0  11:51
R(s) 4040::/64  ::                          self       1    0
```

Figura 2: Ejemplo de tabla de ruteo.

Para cada ruta, el router guarda las entradas en la Tabla de ruteo. En la tabla 2 se describe los campos que forman la tabla de ruteo.

Campos	Descripción
Ruta IPv6	El prefijo de dirección IPv6 y el tamaño del prefijo de la dirección de destino.
Dirección del próximo salto	La dirección IPv6, normalmente enlace-local del primer router a lo largo del recorrido de la ruta IPv6. Si la ruta está conectada directamente con el router, no hay necesidad de una dirección del próximo salto.
Interfaz del próximo salto	La interfaz física utilizada para alcanzar el próximo salto.
Métrica	Número que indica la distancia total de haber alcanzado el router destino. Las rutas directamente conectadas se asignan generalmente un valor métrico de 0. RIPng anuncia las rutas directamente conectadas con el valor métrico de origen, configurado desde el enlace (normalmente es 1).
Temporizador	La cantidad de tiempo desde que la información de la ruta fue instalada y actualizada en las tablas de ruteo.
Bandera de cambio de ruta[11]	Indica que la información de origen ha cambiado recientemente. Esta bandera es necesaria para el control de ruteo de activación de actualización[12].
Origen de ruta	Router que proporcionó la información acerca de la ruta. Por ejemplo, esto puede ser una entrada estática o conectado directamente, el origen puede ser RIP, OSPF, etc.

Tabla 2: Descripción de la Entrada de Tabla de Ruteo.

El router procesa las entradas de rutas recibidas usando el algoritmo de Bellman-Ford el funcionamiento del algoritmo se muestra en la figura 3.

[11] Bandera de cambio de ruta - del Inglés *route change flag*.
[12] Activación de actualización - del Inglés *triggered updates o activar actualización.*

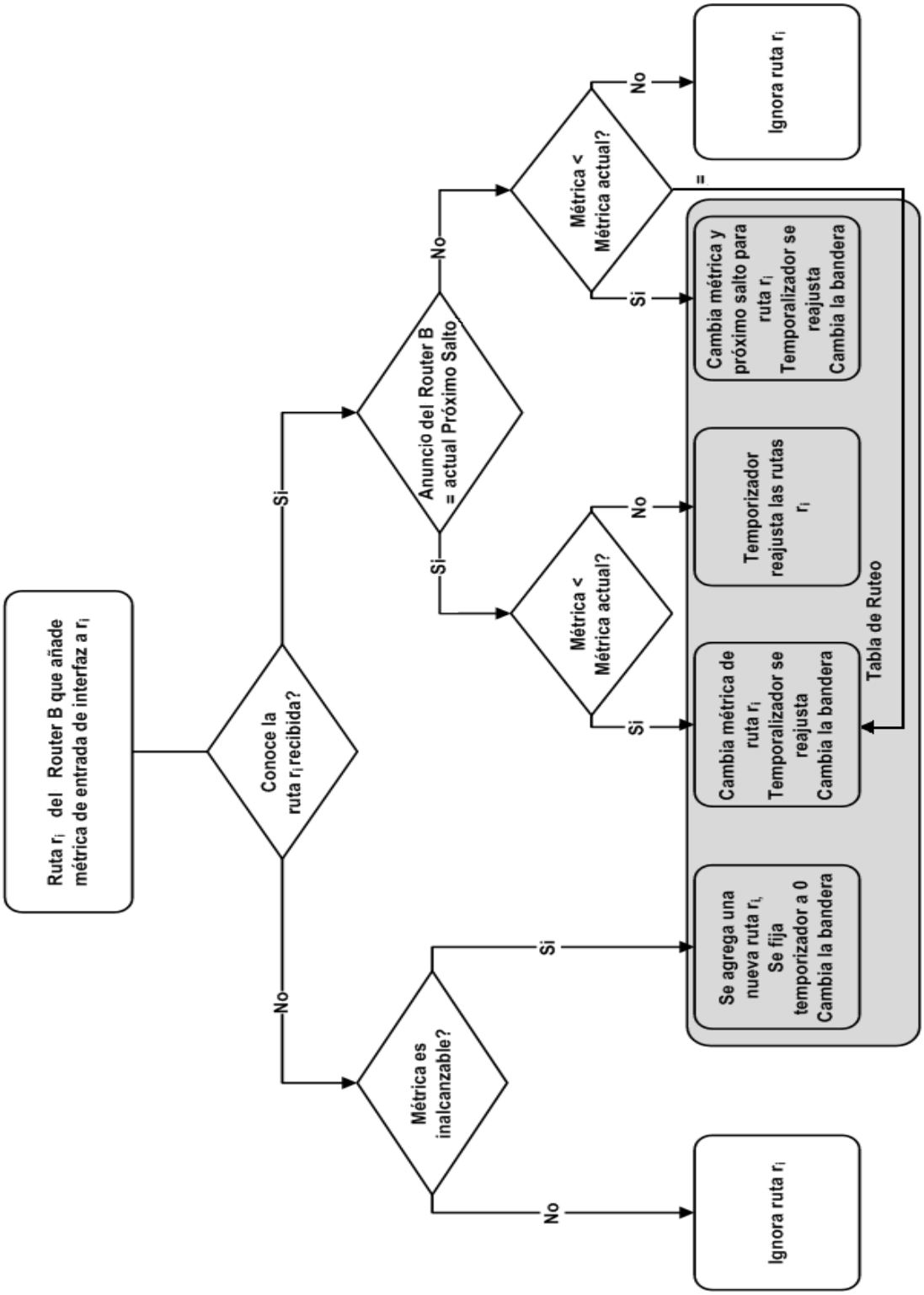

Figura 3: Algoritmo de Bellman-Ford.

A. Funcionamiento del Algoritmo de Bellman-Ford

El proceso inicia una vez que la entrada se ha validado, donde actualiza la métrica para agregarle el costo de red con que llegó el mensaje. Si el resultado es mayor que infinito (mayor que 16), utilizar el infinito. Es decir, utiliza la siguiente formula para ello:

Métrica = MIN (métrica + costo, infinito)

El algoritmo comprueba si ya existe una ruta para la dirección de destino. Si no existe tal ruta, suma a la tabla de ruteo esta ruta, a menos que la métrica sea infinita (no agrega una ruta inutilizable).

Sumarle una ruta a la tabla de ruteo consiste en:

- Fijar dirección destino a la dirección destino en la Entrada de Tabla de Ruta (RTE)
- Fijar métrica a la métrica nuevamente calculada.
- Inicializar temporizador de espera de ruta. Si el Temporizador de desecho está funcionando para esta ruta.
- Fijar la bandera de cambio de ruta.
- Señalar el proceso de salida para activación de actualización.

Si hay una ruta existente, el algoritmo compara la dirección del próximo salto con la dirección del router, desde cualquier llegada de datagrama. Si este datagrama llega desde el mismo router de la ruta existente, reinicializa el Temporizador, después compara las métricas, si el datagrama llega del mismo router de la ruta existente, y la nueva métrica es diferente a la anterior, o si la nueva métrica es menor que la anterior; realizar los siguientes pasos:

- Adoptar ruta del datagrama es decir, poner nueva métrica y ajustar la dirección del próximo salto, si es necesario.

- Fijar bandera de cambio de ruta y señalar el proceso de salida para activar actualización.

- Si la nueva métrica es infinito, comenzar el proceso de eliminación, si no, reiniciar temporizador de espera (Temporizador con más tiempo).
- Si hay alguna ruta de igual costo, entonces marcar todas las rutas anteriores que tengan rutas de igual costo para que sean eliminadas.

Si la nueva métrica es infinita, el proceso de eliminación inicia para la ruta que no ha sido utilizada para los paquetes de ruteo. Observar que el proceso de eliminación comienza solo cuando la métrica se fija al infinito. Si la métrica era infinita, entonces no se comienza con un nuevo proceso de eliminación.

Si la nueva métrica es igual que la anterior, esto se debe tratar como rutas de igual costo y una nueva ruta se debe instalar en la tabla de ruteo del router. En este caso, el router de reenvío puede balancear el tráfico. Cuando una ruta conoce su destino y tiene una métrica menor que la existente con rutas de igual costo, estas rutas, entonces se deben marcar para ser eliminadas.

Además, si la ruta destino es conocida y tiene una métrica mayor que la existente con rutas de igual costo, estas rutas se deben marcar para ser eliminadas.

B. Aplicación del Algoritmo de Bellman-Ford

Para ejemplificar un caso, un router A recibe una actualización de ruteo del router B y ha agregado ya la distancia de 1 a cada una de las rutas r_i anunciadas por el router B. Para cada ruta r_i, el router avanza como se presenta en el algoritmo en la figura 3. De acuerdo a la figura 3, la tabla de ruteo será actualizada si los criterios siguientes son verdaderos; si no, se desecha la ruta r_i:

Ruta r_i es nueva y es alcanzable

- La ruta r_i, las métricas, y el próximo salto se agregan como nueva entrada a la tabla de ruteo del router A. El temporizador se fija a cero y se incrementa la Bandera de Cambio de Ruta (Route Change Flag) del router A.

La ruta r_i existe en la tabla de ruteo y la dirección del próximo salto corresponde a una dirección de la tabla de ruteo:

- Si la métrica ha cambiado, se actualiza y se incrementa la Bandera de Cambio de Ruta. El temporizador se reajusta a cero en cualquier caso.

Ruta r_i es conocida, pero el próximo salto es diferente y la métrica es menor que la entrada en la tabla de ruteo.

- La métrica y el próximo salto son actualizados. El temporizador se fija a cero y la Bandera de Cambio de Ruta se incrementa.

Ruta r_i es conocida, pero el próximo salto es diferente y la métrica es igual a la que está en la tabla de ruteo

- Si el proceso de ruteo permite múltiples rutas r_i de igual costo al mismo destino en la tabla de ruteo, la ruta r_i se trata como una nueva entrada. Si el proceso de ruteo no permite múltiples rutas r_i de igual costo, se descarta la ruta r_i. Las múltiples rutas r_i de igual costo permiten compartir la carga de tráfico de IPv6 entre múltiples rutas r_i. El algoritmo para el tráfico que se distribuye entre estas rutas r_i, es el realizado por el proceso de ruteo, basado normalmente en direcciones de origen y destino IPv6.
- El próximo salto de la ruta r_i, se toma desde la información dentro del mensaje de actualización de ruteo o desde la dirección del origen IPv6 del paquete RIPng.

Cuando los routers son inicializados, primero solo conocen sus rutas r_i directamente conectadas. Esta información se extiende y se pasa a todos los routers vecinos, se procesa y se distribuye a los vecinos de los vecinos. Eventualmente, todas las rutas r_i IPv6 son conocidas por todos los routers. Los routers conservan y envían periódicamente los mensajes de actualización. Esto para evitar que las rutas r_i válidas caduquen y eviten que los routers contengan información errónea.

5. LIMITACIONES DEL PROTOCOLO RIPNG

Las limitaciones encontradas para las versiones 1 y 2 del RIP se aplican también a RIPng y se describen a continuación en la tabla 3:

Limitación	Descripción
El tamaño de la tabla ruta RIPng es limitado	La ruta más larga a cualquier ruta IPv6 se limita a una métrica de 15 saltos cuando está es propagada con RIPng. Normalmente, la métrica es igual a la cantidad de saltos, asumiendo que el costo de 1 está siendo utilizado para cada enlace encontrado. El protocolo permite que costos más grandes sean asignados a cualquier enlace, de tal forma que limita el número de saltos más lejanos.
Bucles de ruteo consecuencia de un tiempo de convergencia excesivo o cuenta al infinito	Cuando se produce un fallo en un enlace, la información que contienen las tablas de ruteo de todos los routers puede no ser coherente durante el intervalo de tiempo que transcurre desde que se produce el fallo hasta que se alcanza la convergencia, de tal forma que pueden producirse bucles en el proceso de ruteo de los paquetes. Cuando las rutas IPv6 que no son válidas se están propagando en un ambiente de bucle, RIPng depende de la "cuenta al infinito" para eliminar eventualmente estas rutas que son consecuencia de un tiempo de convergencia excesivo. Las actualizaciones erróneas continuarán generando bucles hasta que otro proceso lo detenga, de no ser así, los paquetes recorrerán la red en un bucle continuo. Los mecanismos[13] de solución de "cuenta al infinito" se explican más adelante en este capítulo y se da un ejemplo al respecto de este problema en la topología de red mostrada en la figura 4 de esta misma sección.
La métrica no refleja línea de velocidad	RIPng utiliza una métrica fija, normalmente con valor de 1, para cada enlace encontrado. Una ruta no se puede elegir porque no puede estar basada en el ancho de banda, en parámetros de tiempo real, en el medidor de retraso.

Tabla 3: Limitaciones de RIPng

Para el problema de la cuenta al infinito, considere la topología de la figura 4. En este caso el router B estima que la distancia hacia la Red 5 vale 2 a través del router D. Además los routers A y C estiman una distancia de 3 hacia la Red 5 a través del router B. Si el router D falla en algún momento, entonces el router B determina que la Red 5 ya no es alcanzable a través del router D. Al mismo tiempo que el router B actualiza su tabla y asigna una distancia de 4 para la Red 5, basándose en la información enviada por los routers A y C. En la siguiente actualización el router B envía su tabla a los routers A y C. Al mismo tiempo que a los routers A y C actualizan la distancia hasta la Red 5. Ahora vale 5 (4 desde B más 1 para alcanzar al router B) y el router B recibe de sus vecinos el valor 5 para la distancia hacia la Red 5 y asigna 6 a la distancia hasta la Red 5. Esto se repite

[13] Mecanismos descrito por primera vez por William Stallings en su libro "Comunicaciones y Redes de Computadoras".

hasta que la distancia llega al valor 16 (infinito), donde la ruta hacia la Red 5 tarda de 8 a 16 minutos en resolverse.

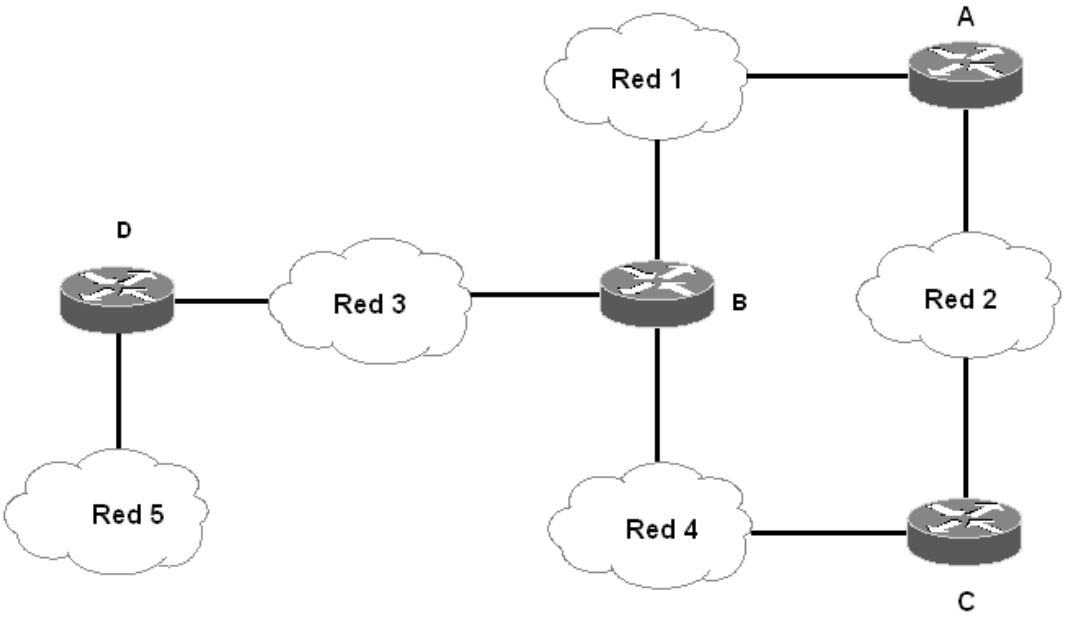

Figura 4: Ejemplo de problema de cuenta a infinito.

6. CRITERIOS PARA COMBATIR PROBLEMAS RIPNG

A. Cambios en la topología y Prevención de inestabilidad

Un cambio en la topología significa que nuevamente las rutas han sido agregadas o una ruta ha sido dada de baja(o esta caída). De tal forma que: las rutas recientemente agregadas: se anuncian con el próximo mensaje de actualización enviado por el router durante la conexión directa a esa ruta. Sus vecinos procesan la ruta y la pasan inmediatamente a sus vecinos. Eventualmente, todos los routers conocen la ruta nuevamente agregada.

¿Qué sucede si una ruta se cae o un router se desconecta repentinamente? Estas rutas eventualmente expirarán y no estarán disponibles para ser anunciadas. El tiempo que

toma para que todos los routers asimilen los cambios realizados a la topología es llamado tiempo de convergencia. Varias estrategias pueden ser introducidas para solucionar y mantener el tiempo de convergencia a su mínimo, las cuales se mencionan a continuación:

- **Envenenamiento de Actualización inversa y El Temporizador de desecho.**

Si una interfaz esta desconectada del router, el router no elimina la ruta o las rutas asociadas con esa interfaz inmediatamente. En lugar, el router mantiene la ruta en la tabla de ruteo y levanta la métrica a 16 (inalcanzable). Un Temporizador de desecho, también conocido como temporizador de sitio, determina cuánto tiempo el router mantiene esta ruta inalcanzable en la tabla de ruteo. La ruta ahora se anuncia a los vecinos con una métrica de 16. Los vecinos están funcionando con un temporizador de sitio, así como también mantienen la ruta de la tabla de ruteo para informar a sus vecinos respectivos de la ruta inválida. Es decir, que consiste en enviar actualizaciones hacia los vecinos con una métrica de 16 para todas las rutas anunciadas a través de esos vecinos. Si dos routers tienen rutas apuntando hacia cada uno, el anuncio de una ruta inversa con una métrica de 16 deshace el bucle inmediatamente. Este proceso se llama envenenamiento de ruta.

- **Horizonte Dividido**

La regla del horizonte dividido establece que no se debe enviar la información de la tabla de ruteo por el mismo enlace que ha llegado la ruta, sino que el router debe de enviar la información al router que este más cerca del destino y no del router que recibe la ruta errónea. Este se elimina en un periodo de 180 segundos y por consiguiente evita los bucles de ruteo disminuyendo el tiempo de convergencia.

- **Horizonte Dividido con o sin envenenamiento de actualización inversa**

Asumamos la ruta r_i está conectado directamente con el router A, según lo indica la figura 5. El router A anuncia r_i a su vecino, router B, con un costo de 1. El router B agrega el valor de 1 y enumera (lista) r_i en su tabla de ruteo usando el router A como el próximo salto. Ahora si r_i se desconecta. El router A envenena r_i y espera a que la actualización del Temporizador de Actualización de Rutas, termine antes de anunciar r_i a B con un costo de 16. Mientras tanto el router B anuncia r_i de nuevo a A con un costo de 2. Según Bellman-

Ford, el router A cambia la entrada para r_i, usando B como el próximo salto con una métrica de 3. Ahora el router A anuncia r_i con un costo de 3 (no 16) al router B.

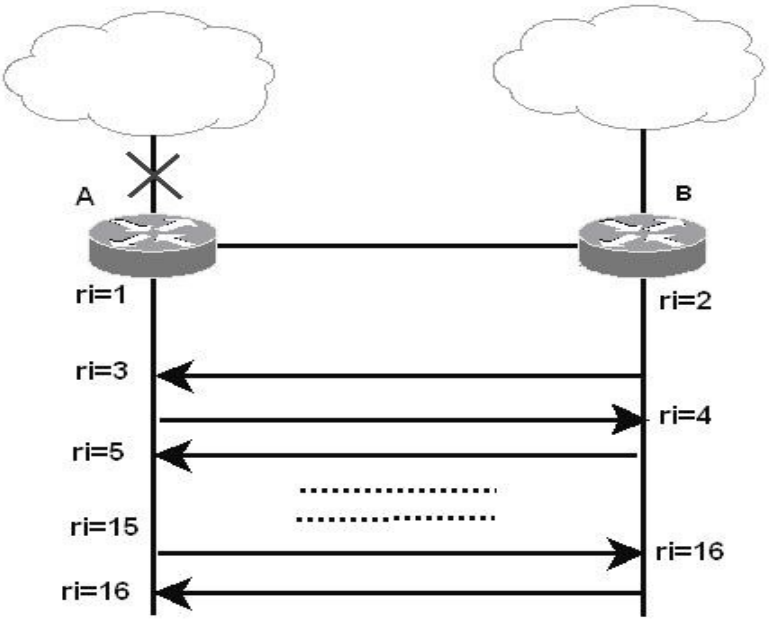

Figura 5: Convergencia de ruta r_i con Horizonte Dividido

El router B agrega 1 al costo y guarda la ruta r_i en su tabla de ruteo con un costo de 4. Los routers envían r_i de un lado a otro, cada vez que se incrementa el costo a 1 hasta contar al infinito y ambos alcanzan un costo de 16, declarando r_i invalida. Esto tomará cierto tiempo, sin embargo el problema principal es que el router B envía las rutas anunciadas de A regresando a A. El horizonte dividido del router A previene que esto suceda. Con el horizonte dividido, un router nunca anuncia una ruta de retorno durante el próximo salto. Una opción adicional es el horizonte dividido con envenenamiento de actualización inversa con esta opción un router anuncia una ruta de retorno durante el próximo salto con una métrica de 16. En la situación casi imposible que el router A y B tengan la misma ruta y el mismo temporizador de sitio y se apuntan entre ellos, los routers no tienen que esperar un tiempo para eliminar esta ruta porque el envenenamiento de actualización inversa invalida cada uno de ellas inmediatamente. El envenenamiento de actualización inversa puede tener la desventaja de incrementar el tamaño de los mensajes de ruteo

especialmente si muchos destinos tienen que ser nuevamente anunciados y envenenados.

- **Activación de la Actualización**[14]

Cualquier cambio en la tabla de ruteo tiene que esperar para ser anunciado hasta que el temporizador de actualización se actualice y termine. La activación de la actualización acelera el proceso permitiendo que la entrada de la ruta (que varia frecuentemente) sea anunciada casi de inmediato. Un temporizador de sitio muy pequeño se introduce antes de enviar la actualización, debido a que solamente se anuncian los cambios y las actualizaciones que periódicamente necesitan permanecer en su lugar.

Todas estas medidas aceleran la convergencia, pero no siempre se logran los resultados esperados. La información errónea siempre puede regresar y ser difundida especialmente dentro de una red de gran magnitud que contiene muchos bucles. El proceso de la cuenta al infinito prevalecerá siempre para eliminar la información errónea.

7. FORMATO DEL MENSAJE RIPNG

RIPng es un protocolo basado en UDP que usa el puerto número 521; el cual es llamado el puerto de RIPng. El proceso de ruteo de RIPng atiende siempre los mensajes que llegan por este puerto. Con la excepción de peticiones específicas, todos los mensajes RIPng fijan el puerto del origen y destino al puerto de RIPng.

El formato del mensaje RIPng se muestra en la figura 6 y en la tabla 4 se describen los campos del mensaje RIPng.

[14] Activación de la actualización – Del Inglés *Triggered updates*

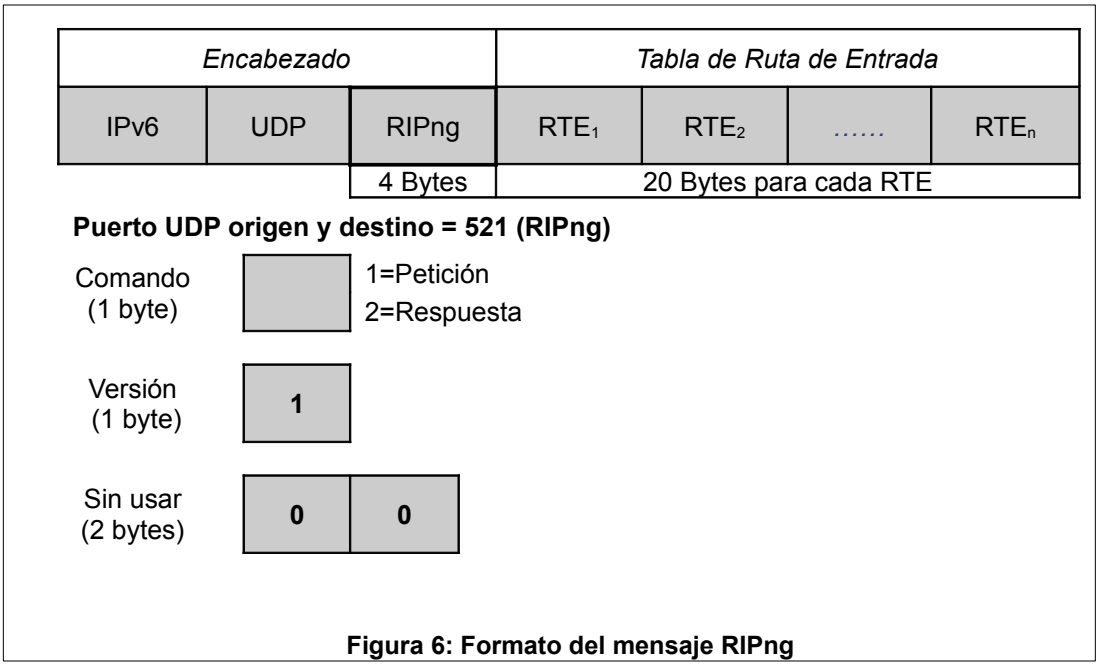

Figura 6: Formato del mensaje RIPng

Nombre del Campo	Byte Reservado	Descripción
Comando	1	El valor de 1 especifica el mensaje de petición que pide el mecanismo que atiende al envío de toda la tabla de ruteo o una parte de ella.
	1	El valor de 2 envía el mensaje de actualización que contiene toda o una parte de la tabla de ruteo del origen. Puede ser enviado en respuesta a una petición anterior o puede ser usada como una actualización periódica no solicitada o como un ruteo de activación de actualización.
Versión	1	El campo de la versión se fija a un valor de 1 por defecto.
RTE[15]	20 para c/u	El Encabezado RIPng es seguido por una o más RTE o Tabla de ruta de entrada, usando el formato representado en la figura 7.

Tabla 4: Campos del mensaje RIPng

8. FORMATO DE TABLA DE RUTA DE ENTRADA (RTE)

Cada RTE describe la ruta que se anunciará usando el campo prefijo IPv6 (16 bytes) y el campo tamaño del prefijo (1 byte). El campo de la métrica (1 byte) contiene la métrica

[15] RTE: Del Inglés *Route Table Entry*

usada por el origen para esta ruta. Una métrica válida tiene un valor entre 1 y 15. Una métrica de 16 describe la ruta como inalcanzable por el router origen.

Cada RTE contiene un campo de etiqueta de la ruta. También, puede ser utilizado para llevar información adicional acerca de la ruta anunciada de otro protocolo de ruteo tal como BGP. Un router que importa rutas externas en RIPng puede fijar esta etiqueta. RIPng preservará y redistribuirá esta etiqueta dentro de su ruteo de dominio. La información dentro de esta etiqueta se puede utilizar para redistribuir la salida de la ruta del dominio RIPng. RIPng por sí mismo no hace ningún uso de esta etiqueta.

El formato de una Tabla de Ruta de Entrada (RTE) se muestra en la figura 7 y la descripción de sus campos se describen en la tabla 5.

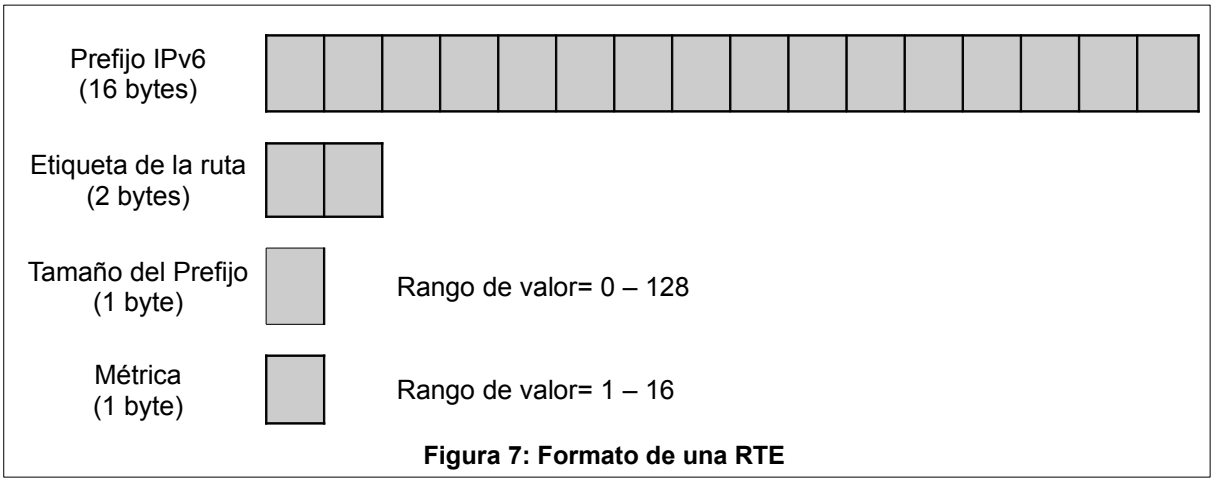

Figura 7: Formato de una RTE

Nombre	Byte Reservado	Descripción
Prefijo IPv6	16	Tamaño del Prefijo de IPv6 es de 128 bits
Etiqueta de la ruta	2	Atributo asignado a la ruta que debe preservarse y registrarse con la ruta. Permite separar las rutas de RIPng internas de las que son importadas de un EGP u otro IGP.
Tamaño del prefijo	1	Un valor entre el rango de 0 a 128
Métrica	1	Un valor entre el rango de 1 a 16

Tabla 5: Valores de los campos de una RTE

En la tabla 6 se definen las abreviaturas manejadas en la formula que sirve para calcular el número de RTEs dentro de una sola actualización, donde depende del MTU y del medio entre dos routers vecinos. La fórmula es:

$$\text{No. de RTEs} = \frac{\text{MTU} - \text{IPv6\_TamCab} - \text{UDP\_TamCab} - \text{RIPng\_TamCab}}{\text{Tam\_RTE}}$$

Abreviatura	Significado
No. de RTEs	Número de Tablas de Rutas de Entrada
MTU	Unidad de Transmisión Máxima
IPv6_TamCab	Tamaño de Cabecera IPv6
UDP_TamCab	Tamaño de Cabecera UDP
RIPng_TamCab	Tamaño de Cabecera RIPng
Tam_RTE	Tamaño de Tabla de Ruta de entrada

Tabla 6: Abreviaturas en la formula de número de RTE

9. FORMATO DEL PRÓXIMO SALTO

El próximo salto RTE es identificado por un valor de 0xFF en el campo de la métrica RTE. La dirección IPv6 dentro de la RTE ahora se identifica como la dirección del próximo salto IPv6 que se utilizará por la RTE adyacente. La etiqueta de la ruta y el tamaño del prefijo se fijan a cero para el momento de su envío, ignorando así la recepción del próximo salto.

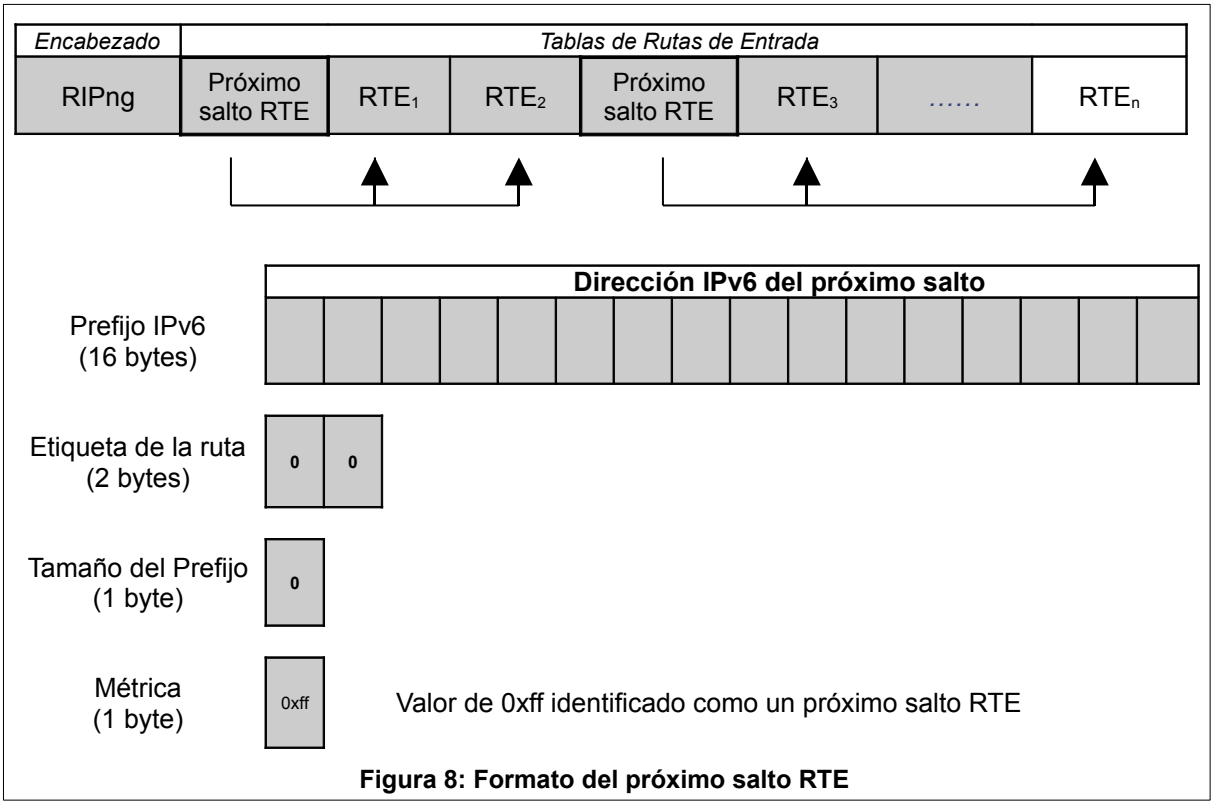

Figura 8: Formato del próximo salto RTE

Según el esquema que se muestra en la figura 8, un RTE típicamente llamado, el próximo salto RTE, se introduce para indicar la dirección del próximo salto IPv6. Todas las RTEs adyacentes utilizan el próximo salto IPv6 hasta alcanzar el otro extremo del mensaje u otro próximo salto RTE encontrado.

Al especificar un valor de 0:0:0:0:0:0:0:0 en el campo del prefijo del próximo salto RTE, indica que la dirección del próximo salto IPv6 se debe fijar a la dirección del origen IPv6 del mensaje de RIPng. El propósito de nombrar un próximo salto específico es eliminar saltos innecesarios en el ruteo. Por ejemplo, los routers A, B, y C están directamente conectados a una subred en común. El router C no funciona con RIPng. Asumimos que el router A sabe de alguna manera la ruta que esta utilizando el router C, por ser éste su próximo salto. El router A podría anunciar la ruta al router B con dirección del próximo salto del router C. El router B puede ahora reenviar el tráfico para la ruta directamente conectada con el router C, por lo tanto evita el salto innecesario a través del router A.

La dirección del próximo salto IPv6 debe ser siempre una dirección de enlace-local (comenzando con un prefijo de FE80). Si este no es el próximo salto RTE, o si la dirección recibida de la dirección del próximo salto no es enlace-local, debe ser considerado con un valor especifico de 0:0:0:0:0:0:0:0.

10. PARTICULARIDADES DE LA RUTA POR DEFECTO Y DE DIRECCIONAMIENTO

Se utiliza una ruta por defecto si la ruta de destino no se lista evidentemente en la tabla de ruteo. El próximo salto del router de la ruta por defecto se conoce como el router por defecto. Enviando el tráfico al router por defecto, se asume que este conoce todas las rutas o tiene un router por defecto para si mismo. Está es una peculiaridad del mecanismo para determinar si el recorrido de los routers por defecto debe ser implementado y de qué forma debe de realizarse.

El mecanismo de los routers por defecto se utiliza generalmente para conducir la salida del sistema autónomo o para conducir el tráfico desde sitios remotos hasta los sitios centrales. La ventaja de distribuir la ruta por defecto es reducir el número de actualizaciones de ruteo que se distribuirán a través del sistema. Las rutas por defecto no deben ser propagadas más allá del sistema autónomo, ni deben de abandonarlo. Una métrica se asigna a la ruta por defecto en su origen para establecer precedencia entre los

múltiples routers por defecto. RIPng maneja una ruta por defecto exactamente de la misma manera que cualquier otro destino.

11. TEMPORIZADORES

RIPng implementa diversos tipos de temporizadores para gestionar las actualizaciones de la información de ruteo. El tipo y el propósito de estos temporizadores se especifican en la tabla 7.

Tipo de Temporizador	Propósito
Temporizador de actualización[16]	Por defecto, cada 30 segundos el proceso de RIPng se activa en cada interfaz para enviar una respuesta no solicitada del ruteo a los routers vecinos. Los 30 segundos se compensan por un intervalo de tiempo aleatorio de 0 a 15 segundos en cuyo caso existe un desplazamiento que se deriva del 50% de un período de actualización de 30 segundos. Esta respuesta contiene la tabla de ruteo entera excepto las rutas que siguen la regla del horizonte dividido.
Temporizador de espera[17]	Cada vez que una ruta ingresa es actualizada, el período de espera para esta ruta ingresada se reajusta a cero. Si el ingreso de la ruta alcanza 180 segundos (valor por defecto) sin otra actualización, entonces se considera haber terminado la actualización. La métrica se fija a 16 y el proceso de colector de desecho se activa. Además, la bandera de cambio de ruta se activa para indicar un cambio. El proceso de salida utiliza esta bandera para activar la actualización.
Temporizador de desecho[18]	El temporizador se fija a 120 segundos para cada acceso de la ruta que ha medido el tiempo del origen (véase Temporizador de espera) o recibido con un valor de la métrica de 16. Solamente el vencimiento de este temporizador de desecho podrá ingresar a las rutas finalmente eliminadas de la tabla de ruteo. Si llega una nueva actualización a esta ruta antes de que termine el temporizador de desecho, se sustituye la ruta y el Temporizador de desecho es reiniciado y fijado a 0.

Tabla 7: Tipos de Temporizadores

[16] Temporizador de actualización: del Inglés *update timer.*
[17] Temporizador de espera: del Inglés *timeout timer*
[18] Temporizador de desecho: del Inglés *garbage collecion timer* también conocido como temporizador de sitio del Inglés hold-down timer.

12. PROCESAMIENTO DE PAQUETES RIPNG

A continuación se muestra cómo un router procesa los mensajes de origen y destino de los mensajes RIPng. Para que el paquete se procese con éxito encontramos 2 categorías de procesamientos de mensajes principales:

A. Procesamiento del Mensaje de Petición

Un mensaje de petición es solicitado por un router para responder con toda o una parte de su tabla de ruteo. La petición de origen se procesa de la siguiente manera:
Por ejemplo, si hay exactamente una RTE con un prefijo de cero, un tamaño del prefijo de cero, y una métrica de 16, la petición es para la tabla de ruteo de entrada, entonces el router responde enviando la tabla de ruteo de entrada; de lo contrario, el mensaje de petición se procesa como una RTE a la vez. Si el prefijo correspondiente de la RTE se encuentra en la tabla de ruteo, las métricas de la RTE se asignan al campo de la métrica de la RTE; de lo contrario, se le asigna una métrica de 16 al campo de la métrica, indicando que la ruta es desconocida. Una vez que se hayan procesado todas las RTEs, el campo del comando del encabezado de RIPng se cambia a respuesta y el mensaje de respuesta recién establecido se envía de nuevo al solicitante.

Existen dos tipos de mensajes de petición:

- General
- Específico

Ambos son manejados de forma distinta por el router destino. La tabla 8 explica estos dos tipos de mensajes de petición, y sus características son resumidas en la tabla 9.

Tipo de Mensaje de Petición	Proceso de envío
Mensaje de Petición General	Es enviado por un router que apenas se ha activado y desee llenar su tabla de ruteo rápidamente. El router envía un mensaje de petición general, pidiendo que todos los vecinos directamente conectados envíen su tabla de ruteo entera. Los vecinos en cada respuesta envían un mensaje que contiene la tabla de ruteo entera, usando la regla del horizonte dividido.
Mensaje De Petición Específica	Es enviado por un router administrador que pide toda o una parte de la tabla de ruteo. El router solicitante contesta enviando la información requerida de su tabla de ruteo. El horizonte dividido no se utiliza porque se asume que el solicitante está utilizando la información solicitada exclusivamente para los propósitos de diagnóstico.

Tabla 8: Tipos de Mensajes de Petición

Tipo de Peticiones	Dirección de origen IPv6	Dirección de destino IPv6	Puerto UDP origen	Puerto UDP destino	Usa Horizonte dividido en respuesta?
General	Enlace-local se envía a la interfaz del solicitante	FF02::9 (multicast)	RIPng - 521	RIPng – 521	Si
Específico	Global	Global	Cualquiera excepto el de RIPng	RIPng - 521	No
	Sitio-local unicast del solicitante	Sitio-local unicast del router solicitante			

Tabla 9: Características de los tipos de peticiones

B. Procesamiento del Mensaje de Respuesta[19]

Un mensaje de respuesta traslada la información de ruteo que se procesará por el router destino usando el algoritmo de Bellman-Ford y puede actualizar la tabla de ruteo de los routers.

Existen dos tipos de mensajes de respuesta:

[19] Ultimas actualizaciones publicadas en junio-27-2007 con fecha de vencimiento Diciembre-2007

- Respuesta No Solicitada que se clasifica en:
    - Actualización regular o Proceso periódico
    - Proceso de Activación de Actualización[20]
- Respuesta Solicitada o Respuesta a una pregunta especifica

Ambos son manejados de forma distinta por el router origen. La tabla 10 especifica la manera de procesar los diversos tipos de mensajes de respuesta. Las características de los mismos son resumidas en la tabla 11.

<table>
<tr><th>Tipos de Mensaje de Respuesta</th><th colspan="2">Proceso de envío</th></tr>
<tr><td rowspan="3">No solicitado</td><td>Periodo de actualización</td><td>Activación de Actualización</td></tr>
<tr><td>Se activa el Temporizador de Actualización para cualquier interfaz dada y se examina la última tabla de ruteo.</td><td>Se activa tan pronto como se incrementa la Bandera de Cambio de Ruta y examina solamente las rutas seleccionadas con la Bandera de Cambio de Ruta. Esto es causado por un cambio en la ruta.</td></tr>
<tr><td colspan="2">Enviar el mensaje de respuesta “no solicitada” a la dirección multicast asegurando que el mensaje de respuesta alcance todos los vecinos en cualquier red directamente conectada. Estos son los casos en los cuales éste no puede trabajar sobre una capa broadcast. Una lista estática de todos los vecinos de la red se puede proporcionar para enviar los mensajes directamente a cada vecino.

Ambos procesos entonces resuelven de la siguiente manera: si la entrada examinada de la ruta tiene una dirección de enlace local o no se utiliza debido al proceso de Horizonte Dividido se deberá ignorar; de lo contrario colocar el prefijo, el tamaño del prefijo, y la métrica en la RTE, y colocar la RTE en el mensaje de respuesta. Si se ha alcanzado el máximo MTU, se deberá enviar, construir y levantar un nuevo paquete.</td></tr>
<tr><td>Solicitado</td><td colspan="2">Se envía como una respuesta a un mensaje de petición.</td></tr>
</table>

Tabla 10: Tipos de Mensajes de Respuesta

[20] Activación de actualización: del Inglés *Triggered update*

Tipo Respuesta		Dirección de origen IPv6	Dirección de destino IPv6	Puerto origen UDP	Puerto destino UDP
No solicitado	**Actualización Periódica**	Enlace-local se envía a interfaz	FF02::9 (multicast)	RIPng - 521	RIPng puerto 521
	Activación de Actualización				
Solicitado (respuesta a petición)		Enlace-local (petición general)	Origen IPv6 del mensaje de petición	RIPng - 521	Origen UDP del mensaje de petición
		Global			
		Sitio-local o única (petición especifica)			

Tabla 11: Características de los tipos de respuesta

El procedimiento a realizarse para que el mensaje de respuesta sea aceptado solamente por un router si la dirección de origen del datagrama IPv6 es de un vecino válido, es decir, si esta directamente conectado con un vecino y es un enlace-local; y si los puertos UDP origen y destino se fijan al puerto de RIPng. Y además, la cantidad del salto se debe fijar a 255 para garantizar que la respuesta no ha sido enviada por ningún nodo intermedio.

Una vez que el mensaje de respuesta es aceptado, es decir que el datagrama haya sido totalmente valido, procesa cada RTE respondiendo uno a uno (comienza nuevamente la prueba de validación). Si un router procesa tanto sus propias salidas como las nuevas entradas, existe la posibilidad de una confusión, así que tales datagramas deben ser ignorados. También la respuesta debe ser ignorada sino es hecha por un puerto RIPng.

Las pruebas básicas de validación de una RTE incluye :

- El prefijo de la dirección unicast (no un multicast o una dirección enlace-local)
- El tamaño del prefijo unicast(entre 0 y 128)
- La métrica válida (entre 1 y 16).

Si se acepta la RTE, la métrica de la interfaz de entrada se agrega a la métrica de la RTE, esta RTE ahora pasa al proceso Bellman-Ford.

Las reglas previamente recibidas y validadas no son aceptables para responder a un

mensaje solicitado por una petición específica. El número del salto puede ser menor que 255, y la dirección origen IPv6 no es una dirección de enlace-local. El administrador de Redes utiliza la RTE recibida no para el ruteo, sino para proporcionar la entrada en su software de diagnóstico. Esto se implementa por un software que determina la validez de un mensaje de respuesta (manejados de forma distinta por el router).

13. FUNCIONES DE SEGURIDAD Y CONTROL

A. Seguridad RIPng

RIPng funciona en IPv6 y confía en el mecanismo de encabezado de autenticación IP y el mecanismo de seguridad y de encapsulamiento de certificación IP, utilizado por IPv6 para asegurar integridad y autenticación de intercambios de ruteo.

B. Control RIPng

RIPng no aporta especificaciones para el control de administración. Sin embargo, la experiencia con implementaciones y práctica existentes del RIP sugieren que tales controles puedan ser importantes. Los controles de administración son los filtros, que permiten o rechazan ciertas rutas que son anunciadas o recibidas. Además, una lista de vecinos válidos podría ser especificada, y un router aceptaría o notificaría las rutas solamente de o hacia los vecinos que se encuentran presentes en esta lista.

Los filtros se pueden utilizar para cambiar el comportamiento de actualizaciones con políticas de ruteo complicadas que se hallan fijadas dentro de un sistema autónomo. Aunque RIPng no necesita tales funciones de control, son frecuentemente recomendadas para que el administrador gestione tales controles. Cisco Systems, por ejemplo, implementa las listas de distribución RIPng y las herramientas RIPng de Nortel divulgan y aceptan estas políticas.

14. VENTAJAS Y DESVENTAJAS RIPNG

RIPng fue desarrollado para permitir a los routers, dentro de redes basadas en IPv6, intercambiar información de rutas. Aunque estos usan algoritmos, temporizadores y lógica como en sus versiones anteriores, existen ciertas ventajas y desventajas sobre estas. Al igual que al compararlos con otros protocolos de ruteo. En esta sección encontraremos tanto ventajas como desventajas que actualmente presenta RIPng.

A. Ventajas RIPng

En comparación con otros protocolos de ruteo y tomando en consideración las versiones anteriores de RIPng este protocolo establece el siguiente listado de mejoras que se presentan en la tabla 12:

Considerando	
Versiones anteriores	**Otros protocolos de ruteo**
Permite utilizar el mecanismo de direccionamiento de rutas por defecto, que distribuye la ruta por defecto para reducir el número de actualizaciones del ruteo que se distribuye a través del sistema.	Protocolo con un mecanismo totalmente independiente de instalación, configuración y actualización. (El más fácil de configurar).
Soporte nativo de enmascaramiento de subredes de longitud variable VLSM .	La implementación en plataformas independientes, es estable y robusto.
Soporta controles de eventos de forma manual cuando las Interfaces se conectan o se desconectan, las rutas se actualizan desde la tabla de reenvío y del cambio de prefijos de direcciones en la base de uso portátil BSD para conexiones APIs (interfaces con capa de enlace).	Conforma la arquitectura del software portable (FSAP), así asegura un código portable que use un intermediario y un administrador de temporizador. Es decir que soporta sistemas ENDIAN y sistema de operaciones múltiples con un mínimo de esfuerzo.
Permite el envío de actualizaciones de tablas de RIPng mediante direcciones multicast.	Es un protocolo abierto soportado por muchos fabricantes y tecnologías.
Puede permitir la utilización de arquitecturas de red discontinuas, utilizando máscaras de red en la elección del próximo salto.	Permitir la redistribución automática de rutas externas anunciadas por otros protocolos de ruteo.
Se actualiza los paquetes soportando mayor cantidad de bits (128 bit) para el formato de direcciones IPv6.	
Proporciona soporte para configuración del Horizonte dividido, envenenamiento de actualización inversa mediante interfaces, que ayudan a solventar las limitaciones del protocolo.	
Soluciona el problema para anunciar rutas de igual costo, con el “Horizonte Dividido con Envenenamiento de Actualización Inversa por destino”	
Proporciona un completo soporte del Protocolo Simple para Administración de Redes SNMP, basado en la gestión de propietarios MIB para la RIPng de datos IPv6.	
Soporta tablas de ruteo y operaciones de rutas usando TRIE (un modelo de estructura de datos con el árbol de PATRICIA)	

Tabla 12: Ventajas RIPng

B. Desventajas RIPng

RIPng por otra parte, tiene presente el siguiente listado de desventajas que se señalan en la tabla 13.

Considerando	
Versiones anteriores	**Otros protocolos de ruteo**
El envenenamiento de actualización inversa puede, incrementar el tamaño de los mensajes de ruteo, especialmente si muchos destinos tienen que ser anunciados y envenenados.	La limitación en el tamaño máximo de la red es de 15 saltos, lo cual implica que no se permite la utilización de RIPng en redes mucho más complejas.
	Para determinar la mejor métrica, únicamente toma en cuenta el número de saltos, es decir la cantidad de routers o equipos similares por los cuales es transferida la información (basándose en un sistema de costos que se incrementa en cada salto).
	Aunque existen técnicas externas al protocolo para la solución del conteo al infinito si se forman bucles, como el envenenamiento de actualización inversa y el horizonte dividido, métricas estáticas, no dan ninguna información del estado de la red únicamente puede ser cambiadas por el administrador de la red, pero el problema persiste.
	La convergencia es lenta para el vector distancia. Genera mucho tráfico al enviar toda la tabla de ruteo en cada actualización, con la carga de tráfico que ello conlleva.
	No incluye ningún soporte de autenticación nativo, sino se basa en las características de seguridad ofrecidas para IPv6. (Autenticación para la transmisión de información entre vecinos).

Tabla 13: Desventajas RIPng

15. ACTUALIZACIONES NACIENTES[21]

Las últimas actualizaciones del protocolo RIPng reflejan una mejora en lo que respecta a la utilización de mecanismos de rutas con igual costo para llegar al mismo destino a través de las diferentes rutas. Debido a que hoy en día en Internet existen muchas redes que poseen topologías donde existen más de un recorrido a un destino determinado. En esta sección se describen las modificaciones para el manejo y control de los distintos escenarios del protocolo RIPng, como son:

- "Horizonte dividido con envenenamiento de actualización inversa" para rutas de igual costo.

[21] Fuente: Equal cost routes support for RIP/RIPNG, IETF, Janardhan Naveen Anand, Publicado: Junio-27-2007

- “Horizonte dividido con envenenamiento de actualización inversa por destino” para anunciar rutas de igual costo.
- Peticiones de rutas anunciadas mediante puerto NON-RIPng.

A la vez, se describe como aplicar el Horizonte dividido y el envenenamiento de actualización inversa para tales rutas.

A. “Horizonte Dividido con Envenenamiento de Actualización Inversa” para rutas de igual costo.

El Horizonte Dividido Simple, según lo descrito en el RFC 2453, se define de la siguiente manera:

- El esquema del “Horizonte dividido Simple” omite las rutas anunciadas de un vecino a partir de las actualizaciones enviadas a ese vecino.
- El “Horizonte dividido con Envenenamiento de Actualización Inversa” incluye tales rutas en actualizaciones, pero fija sus métricas al infinito.

Cuando un router tiene 2 o más rutas para llegar al mismo destino, ¿cómo deben aplicar el Horizonte dividido a ellas? El Horizonte Dividido Simple según lo explicado en el RFC 2453 pide no enviar la ruta sobre un enlace desde que este fue anunciado. Pero en este caso, el router puede tener varias rutas para llegar al mismo destino, anunciándose en diferentes enlaces. Así pues, la aplicación del horizonte dividido según lo descrito en el RFC 2453, conducirá el anuncio de una ruta anunciada en un enlace, a otro enlace en el cual ha anunciado una topología diferente de una ruta de igual costo al mismo destino. Tal como se muestra en la topología de la figura 9.

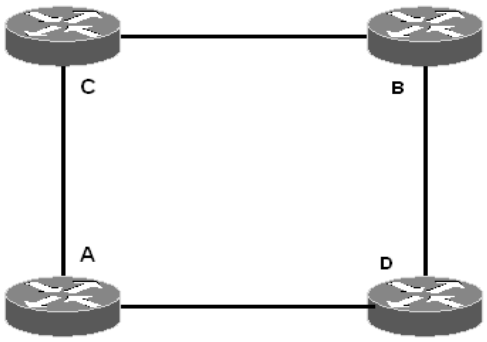

Figura 9: Topología diferentes rutas de igual costo al mismo destino

Considerar la topología de la figura 9. En este caso, el router C anunciará 2 rutas al destino D, una a través del router A y otra a través del B. Cuando C envía una actualización periódica en el enlace hacia B, incluirá la ruta anunciada a D a través de A. Pero esto no es correcto, porque esta ruta que se esta anunciando es la misma información que A ha anunciado de B hacia D.

Aún cuando la ruta se anuncia sobre diferentes interfaces con respecto al router C y B, para el router D es como si el router C no este haciendo Horizonte Dividido con Envenenamiento de Actualización Inversa, y simplemente anuncia la ruta que B que había enviado al router C. Esto conducirá obviamente a los mismos problemas que parten el horizonte dividido de rutas que desearon solucionar.

La solución no es anunciar tales rutas, sino, que nunca anuncie las rutas de igual costo sobre el enlace, si el router ha anunciado una ruta del destino de ese enlace. A esto se le llama, “horizonte dividido por destino”. El punto es, que el horizonte dividido no hace la ruta, sino que se hace por un destino. El nuevo Horizonte Dividido con Envenenamiento de Actualización Inversa puede indicar como hacer esto.

“Horizonte dividido por destino” omite todas las rutas de igual costo conocidas para un destino, si tiene una ruta a ese destino del mismo vecino a quien se envían las actualizaciones. “Horizonte Dividido con Envenenamiento de Actualización Inversa por destino" incluye solamente una ruta a ese destino, pero fija esta métrica al infinito.

Cuando se hace Envenenamiento de Actualización Inversa, sólo una ruta debe anunciarse con un costo de 16, sin importar que muchas rutas de igual costo son anunciadas. Tomando el ejemplo anterior, C anunciará una sola ruta con el costo de 16 en los enlaces hacia los routers A y B.

B. "Horizonte Dividido con Envenenamiento de Actualización Inversa por destino" para anunciar rutas de igual costo.

¿Cómo un router anuncia en general las rutas de igual costo? Cuando un router envía actualizaciones de ruteo en un enlace, tiene que hacer "Horizonte Dividido con Envenenamiento de Actualización Inversa" registrando las rutas como las que se describe en el ejemplo anterior. (Véase figura 9).

Si la ruta puede ser anunciada después de aplicar "Horizonte Dividido con Envenenamiento de Actualización Inversa por destino", entonces solamente una de las rutas debe ser anunciada. Para el envío de todas las rutas de igual costo, pero sirve nada más para el llenado de paquete.

Cuando una ruta antigua de igual costo entra o sale y es inalcanzable (el costo entrante es "infinito"), entonces el router puede enviar una "activación de actualización" de las otras rutas que se encuentran en el destino.

En algunos casos, las rutas de igual costo pueden tener próximos saltos para diferentes rutas anunciadas en la misma interfaz. En este panorama, puede anunciar más de una ruta a un router destino en un enlace.

C. Peticiones de Rutas Anunciadas Mediante Puerto NON-RIPng.

¿Cómo las rutas deben ser anunciadas cuando las peticiones de la ruta vienen de puerto NON-RIPng? El Mensaje de Petición desde el puerto NON-RIPng se dirige normalmente

hacia un router en particular y se utiliza normalmente para los propósitos administrativos y de depuración. Así pues, todas las rutas de igual costo pueden ser notificadas apropiadamente por el origen de llenado del “próximo salto”.

CAPITULO II
PROTOCOLO DE RUTEO OSPF PARA IPv6

1. GENERALIDADES

A. Introducción

Al ir de IPv4 a IPv6, los mecanismos básicos de OSPF no han sufrido cambios, aunque algunos de estos mecanismos ha sido necesarios acomodarlos, como el aumento del tamaño de la dirección de IPv6 y los cambios en la semántica del protocolo entre IPv4 e IPv6. El protocolo OSPF para IPv6 se define en el RFC 2740, en el cual se muestran las diferencias entre OSPF para IPv4 y OSPF para IPv6.

B. Características y limitaciones

El protocolo OSPF tiene algunas ventajas importantes sobre RIPng: Se recupera de fallos de la red en un plazo de algunos segundos en vez de varios minutos, ofrece una métrica de gran alcance, apoya redes con diámetros grandes y deja agregar prefijos de subred de comunicación en prefijos más grandes de ruteo.

OSPF tiene algunas desventajas: OSPF es un protocolo muy complicado y es por ello más susceptible a las implementaciones defectuosas. A diferencia de RIPng, OSPF necesita de una configuración antes que pueda funcionar como un router. Y aun cuando OSPF apoya redes con diámetros grandes, este no escala bien simplemente porque necesita más recursos que RIPng.

C. Conceptos básicos

OSPF es un protocolo de ruteo interno al igual que RIPng, así es que funciona dentro de una nube adyacente bien definida en la red; las especificaciones de OSPF frecuentemente suponen que funciona una sola instancia del OSPF a través de un Sistema Autónomo (AS). Todos los router con OSPF dentro de esta nube no pierden de vista la topología en-

tera de la red y el estado del enlace de todos los router dentro de la nube. En la terminología OSPF, un enlace no es una subred de comunicación así como lo es en la terminología IPv6, sino es una conexión entre dos router o un router y una subred unida. Tan pronto como un router se entera que un enlace ha cambiado, el puede rápidamente reconstruir su tabla de ruteo. Los cambios del estado del enlace son anunciados rápidamente a través de la inundación en la nube entera: Un router que aprende sobre un cambio del estado del enlace inmediatamente enviará un anuncio del estado del enlace (LSA) para todos los otros router que están directamente relacionados con él, excepto del que recibió el cambio. Para evitar una tormenta en la red, los router que reciben un cambio y ya saben de este cambio lo que hacen es ignorar ese cambio.

Estas dos características hacen a OSPF un protocolo de gran alcance: Un router OSPF siempre tiene información actualizada acerca del estado de la red entera y usa esta información para establecer una relación entre las tablas de ruteo.

D. Estructuras de datos del protocolo

Las estructuras de datos principales de OSPF son iguales para IPv4 e IPv6: áreas, interfaces, vecinos, la base de datos del estado de enlace y la tabla de ruteo. Las estructuras de datos a nivel superior para IPv6 siguen siendo la misma de IPv4[22].
Todos los LSAs con el LS (Estado del Enlace) conocido y el Sistema Autónomo (AS) al alcance de la inundación aparecen en la estructura de datos del nivel superior, en lugar de pertenecer a un área o enlace específico. AS-externo-LSAs es el único LSA que tiene un AS al alcance de la inundación. LSAs con el tipo de LS desconocido, pone a 1 el U-bit (inundación aun cuando es desconocido) y también el AS al alcance de la inundación aparece en la estructura de datos del nivel superior.

[22] "OSPF Version 2", RFC 2328

E. Estructura del Área de Datos

La estructura del área de datos de IPv6 contiene todos los elementos definidos para las áreas de IPv4[23]. Además, todos los LSAs de tipo conocido que tiene el área al alcance de la inundación pertenecen a la estructura del área de datos de IPv6. Esto siempre incluye los siguientes tipos de LSA: router-LSAs, red-LSAs, Inter-Área-prefijo-LSAs, Inter-Área-Router-LSAs e Intra-Área-Prefijo-LSAs. Los LSAs con el tipo desconocido de LS, ponen a 1 el U-bit (inundación aun cuando es desconocida) y el alcance del área también aparecen en la estructura del área de datos. Los router IPv6 que ponen el MOSPF (Protocolos de Estado de Enlace) en ejecución agregan al grupo de calidad de miembro[24] de los LSAs a la estructura del área de dato

F. Estructura de datos del interfaz

En OSPF para IPv6, una interfaz conecta a un router con un enlace. La estructura del interfaz para IPv6 modifica la estructura del interfaz para IPv4[25] de la siguiente manera:

- **ID de Interfaz:** Cada interfaz es asignada a un ID de interfaz, que identifica únicamente al interfaz con el router. El ID de interfaz aparece en los paquetes Hello enviados fuera del interfaz, en el enlace-local-LSA originado por el router para el enlace agregado, y en el router-LSA originado por el router-LSA para el área asociada. También servirá como ID del estado del enlace, para la red-LSA que el router originará, para el enlace si el router elige el router designado.
- **ID de instancia**: A cada interfaz se le asigna un ID de Instancia. Esto debería de tener por defecto el valor de cero, y será necesario asignar un valor diferente en los enlaces que contengan múltiples comunidades separadas de router. Por ejemplo, se supone que hay dos comunidades de router en un segmento dado de Ethernet y que se desean mantener separadas. La primera comunidad recibe un

[23] "OSPF Version 2", RFC 2328
[24] En Inglés *group-membership-LSAs*
[25] "OSPF Version 2", RFC 2328

ID de instancia de 0, asignándole 0 como el ID de instancia de todas las interfaces de sus router del segmento dado de Ethernet. El ID de instancia con valor de 1 es asignado a las interfaces de otros router para el segmento dado de Ethernet. OSPF transmite y recibe este proceso por lo que mantendrá a dos comunidades separadas.

- **Lista de LSAs con alcance de enlace-local:** Todos los LSAs con alcance de enlace-local que fueron originados/inundados en el enlace pertenece a la estructura del interfaz que conecta con el enlace. Esto incluye la colección de enlaces del enlace-LSAs.
- **Dirección IP del interfaz:** Para IPv6, la dirección IPv6 que aparece en el origen de los paquetes enviados fuera del interfaz es por lo general una dirección de enlace-local. La única excepción es para los enlaces virtuales, el cual debe usar una de las direcciones propias de los router locales o globales como dirección IP de la interfaz
- **Lista de LSAs con el tipo de LS desconocido:** Todos los LSAs con el tipo de LS desconocido y el U-bit en 0 (si es desconocido, se trata el LSA como si tuviera la inundación al alcance del enlace-local) se mantiene la estructura de datos para la interfaz que recibió el LSA.
- **Lista de prefijos del enlace:** Una lista de los prefijos de IPv6 puede ser configurada para el enlace unido. Éstos serán anunciados por el router en el enlace-LSAs a fin de que puedan ser anunciados por el router designado en la intra-área-prefijo-LSAs.

En OSPF para IPv6, cada interfaz del router tiene una sola métrica, que representa el costo de enviar los paquetes fuera de la interfaz. Además, OSPF para IPv6 confía en la autenticación de la cabecera IP ,además, el protocolo IP encapsula la carga útil para asegurar la integridad y la autentificación/confidencialidad de los intercambios del ruteo. Por esa razón, la llave de AuTipo y la autentificación no se asocia a las interfaces de OSPF para IPv6.

G. Estructura de Datos del Vecino

La estructura del vecino realiza la misma función en IPv6 e IPv4. Esta recolecta toda la información requerida para formar una adyacencia entre dos routers. Cada estructura del vecino está asociada con una sola interfaz OSPF. Las diferencias entre la estructura del vecino IPv6 y la estructura del vecino definidas para IPv4 son:

- **ID de interfaz del vecino:** El ID de interfaz que el vecino anuncia en sus paquetes HELLO debe ser registrado en la estructura del vecino. Los router incluirán el ID de interfaz del vecino en el router-LSA del router cuando se de cualquiera de estas acciones: a) cuando se anuncia un enlace punto-a-punto al vecino o b) se anuncia un enlace a una red donde el vecino tiene un router designado.
- **Dirección IP del vecino:** Excepto en enlaces virtuales, la dirección IP del vecino será una dirección IPv6 de enlace-local.
- **Router designado al vecino:** La elección del router designado al vecino es codificado como un ID de router, en lugar de como una dirección IP.
- **Router de respaldo designado al vecino:** La elección del router designado al vecino es codificado como un ID de router, en lugar de como una dirección IP.

2. ÁREAS DE OSPF Y RUTAS EXTERNAS

Dentro de un Sistema Autónomo, los router pueden ser agrupados para formar áreas. A cada área se le asigna un ID de área, un entero de 32-bit. No tiene ningún significado de direccionamiento aparte de ser el identificador de área. Un LSA tiene el alcance de de inundar un área, nunca será inundado fuera de esa área. Juntos, forman la estructura de datos del área, también conocido como el área LSDB. El Router-LSA y la red-LSA pertenecen a esta categoría. Los routers y las redes de un área están escondidas de otras áreas; es similar a dividir el mapa de la red en múltiples mapas, cada uno representa la topología de un área. Cada router dentro de un área calcula el árbol SPF (árbol con las trayectorias más cortas) para todas las rutas dentro de la misma área. Estas rutas son

llamadas rutas intra-área. Los routers con todas las interfaces pertenecientes a una sola área son llamados routers internos. Para encontrar las trayectorias de las rutas fuera del área, "los puntos de la salida" los proporcionan router al borde del área (ABR). Para proporcionar conectividad entre todas las áreas, cada área siempre debe estar directamente ligada a una sola área común llamada el área backbone. Esto es alcanzado por el ABR teniendo al menos una interfaz en el área backbone y una interfaz en el área local. El ABR anuncia todas las rutas del área local para el área backbone y todas las rutas del área backbone son anunciadas para el área local. Esto asegura que todas las rutas están distribuidas dentro del sistema autónomo. El área backbone recolecta y distribuye todas las rutas y áreas.

El proceso de ruteo dentro del AS ocurre en dos niveles. Si la fuente y la dirección IP de destino de un paquete pertenecen a la misma área, el paquete se remite solamente a la información obtenida del área LSDB, esto se llama ruteo intra-área. Si la dirección de destino está fuera del área, el paquete tendrá que ser remitido a lo largo de la trayectoria del ABR del área local. El ABR conoce todos los destinos y remite el paquete a través del backbone al ABR del área de destino o al área del backbone. A esto se le llama ruteo inter-área.

La ventaja de tener áreas, es la reducción de procesar gastos indirectos, ya que la topología de cada área es más pequeña que la del AS, el cálculo del árbol del SPF toma menos tiempo. Además, los cambios en la topología permanecen locales, y solo los router en el área local necesitarán recalcular el árbol del SPF. Los router en otras áreas se afectan menos porque la topología del área no se cambia. Los router internos se benefician más al pertenecer a áreas que al AS porque su LSDB es mucho más pequeño.

A. El Área Backbone

El área backbone es un área especial con un ID de área de 0. El área del backbone contiene todos los ABRs del AS. Si un AS no está dividido en áreas, el área del backbone es generalmente la única área configurada. Si el AS está dividido en áreas, el área del

backbone es la unión de todas las rutas de todas las áreas del nonbackbone. El área del backbone debe estar adyacente: cada router dentro de la misma área tiene por lo menos un enlace directo a otro router en la misma área, y ese enlace pertenece al área. Sin embargo, con la introducción de enlaces virtuales, un área del backbone no tiene que estar físicamente adyacente. Un área de tránsito se puede utilizar para crear un túnel (un enlace virtual) que pertenece al área del backbone.

B. Las áreas del Nonbackbone

Las áreas del Nonbackbone se le asignan los IDs de área con excepción del 0. Deben estar físicamente adyacentes. Cada área del nonbackbone debe tener un ABR conectado con el backbone usando un enlace físico o un enlace virtual. Un ABR anuncia todas las rutas del nonbackbone en el área del backbone, y viceversa, un ABR anuncia todas las rutas conocidas al área del backbone en el área del nonbackbone. Normalmente, el ABR utiliza un LSA (llamado el Inter-Área-Prefijo-LSA) para cada ruta anunciada. El ABR se puede configurar para resumir las rutas usando un prefijo más corto de IPv6 que representa algunas o todas las rutas que se anunciarán. Esto reduce el número de anuncios, así como la memoria y los requisitos del proceso.

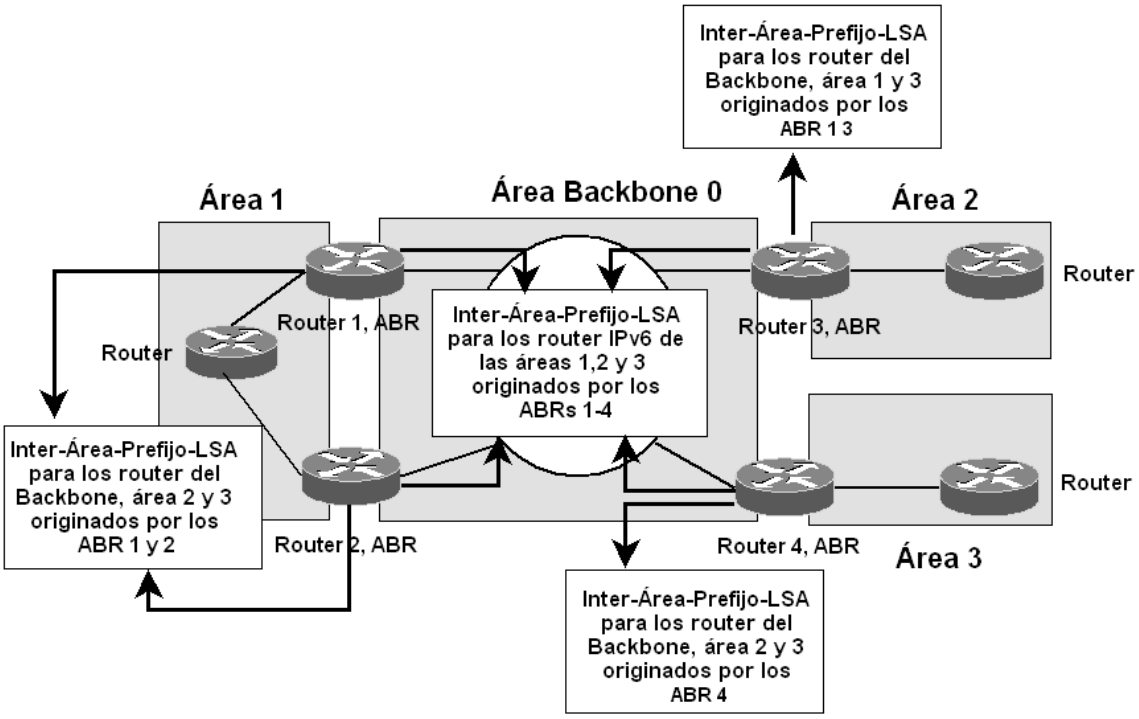

Figura 10: Áreas de OSPF y actualizaciones de rutas

Un área del nonbackbone puede tener ABRs múltiples. La figura 10 explica los ABRs que anuncian Inter-Área-Prefijo-LSAs.

C. Enlaces Virtuales

Un enlace virtual es un enlace lógico que hace un túnel a través del tráfico del backbone con un área del nonbackbone. Puede ser configurado entre dos ABRs usando un área común del nonbackbone llamada área de tránsito. Un enlace virtual pertenece al backbone y puede cruzar solamente una sola área de tránsito. El área de tránsito no debe ser un trozo de área. Un área apartada sin una interfaz física para el área del backbone puede estar relacionada al backbone usando enlaces virtuales. Los enlaces virtuales también se pueden utilizar para crear conexiones redundantes al backbone. OSPF considera un enlace virtual un enlace punto-punto. El camino más pequeño entre los ABRs a través del área de tránsito determina las direcciones reales del punto final del túnel. Estas direcciones deben ser globales o direcciones unicast de IPv6. La figura 11 muestra un ejemplo de enlaces virtuales.

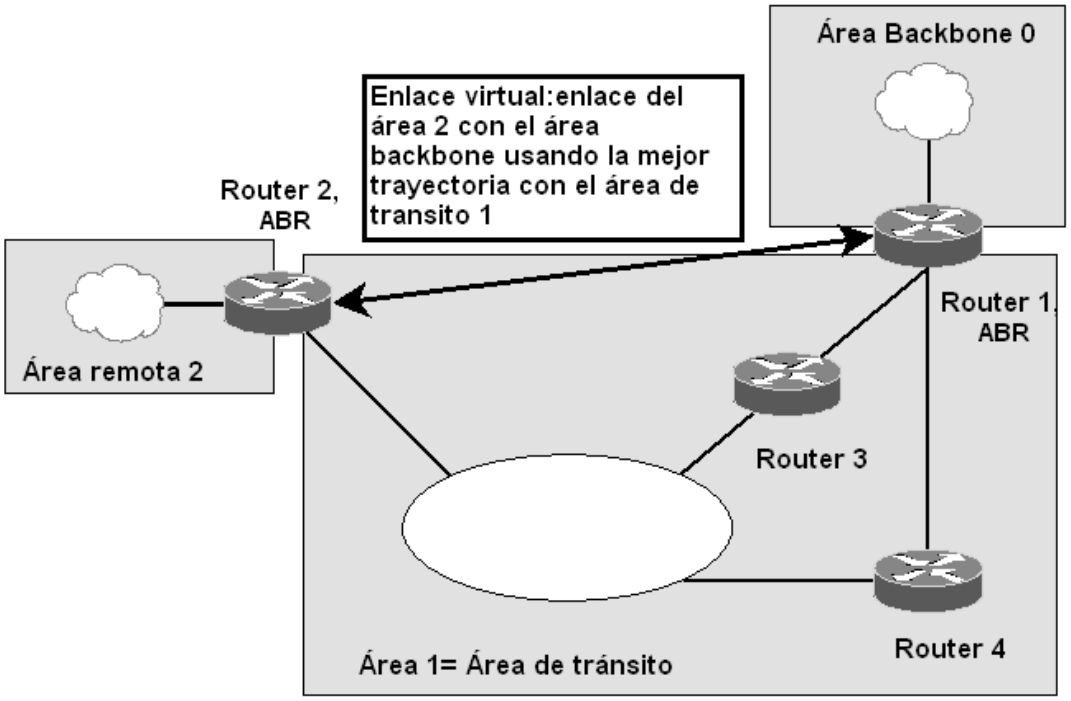

Figura 11: Enlace virtual conectando un área remota.

D. Rutas externas.

Un router puede aprender las rutas IPv6 de diversas fuentes, tales como RIPng, rutas estáticas, BGP, IS-IS, etc. Cada ruta de una fuente no-OSPF se considera una ruta externa a OSPF y se puede importar dentro de OSPF. Para importar las rutas externas en OSPF, un router debe tener por lo menos una interfaz configurada con OSPF y debe conocer al menos una red no-OSPF. Este router se llama router de frontera del Sistema Autónomo (ASBR). Se importan las rutas externas usando un solo AS-Externo-LSA para cada ruta externa. Dependiendo de la implementación, un ASBR puede resumir una gama de rutas externas a un solo LSA externo. La figura 12 explica cómo las rutas externas se importan en el OSPF.

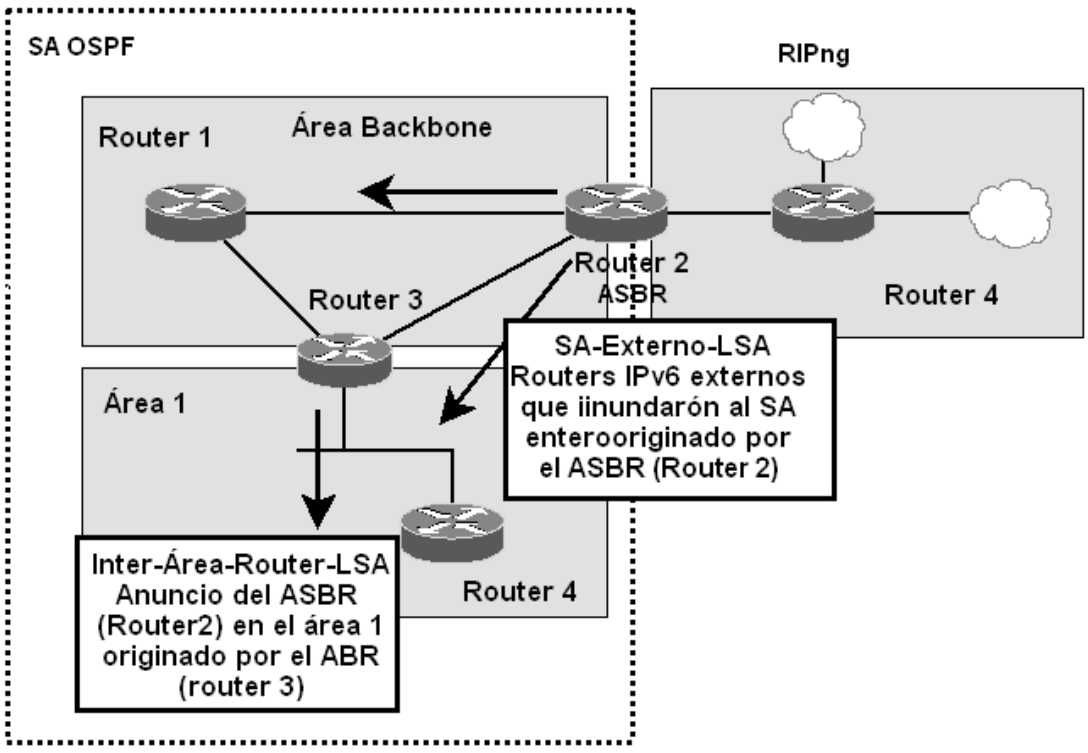

Figura 12: Rutas externas importadas en OSPF.

Un AS-Externo-LSAs debe ser inundado a través del AS. Cualquier router dentro del AS remite paquetes a las redes externas del ASBR o a una dirección de origen opcional especificada por el ASBR. Por lo tanto, debe haber una entrada al ASBR en el Área-LSDB, o la dirección de origen debe estar en la tabla de ruteo local. Si el ASBR no está dentro del área local, el ABR es responsable de anunciar la existencia del ASBR al área local. Se hace esto usando un Inter-Área-Router-LSA. La figura 12 muestra el uso de la Inter-Área-Router-LSA.

Las métricas de las rutas externas no son compatibles con la métrica del OSPF. Los ASBRs anuncian las rutas externas usando uno de los dos tipos de métricas: rutas externa-1 y externa-2. Las rutas externa-1 se consideran que están cerca del ASBR. Los router dentro del AS agregan el costo del OSPF para alcanzar el ASBR o la dirección de origen anunciada a la métrica de la ruta externa-1. Se asumen que las rutas externa-2 están más lejos del ASBR. Una métrica más grande que cualquier camino de intra-AS se le sumará la trayectoria a la métrica de la ruta externa-2.

Si se anuncia una ruta interna del OSPF al mismo tiempo que una ruta externa, la trayectoria de la ruta interna de OSPF se elige siempre por sobre la trayectoria de la ruta externa. Esto puede suceder si hay múltiples ASBRs conectados con la misma red externa. Un ASBR anuncia una ruta del OSPF al protocolo externo de ruteo, y el otro ASBR importa la misma ruta de regreso al OSPF.

3. FORMATO DEL MENSAJE OSPF PARA IPV6

A. Encapsulamiento de los datagramas IP

Los paquetes de OSPF se encapsulan directamente en IPv6. Esto quiere decir que OSPF no funciona para TCP o UDP.

El OSPF no utiliza la fragmentación, por lo tanto confía enteramente en la fragmentación del protocolo de Internet al enviar los paquetes más grandes que el MTU. La fragmentación debe ser evitada siempre que sea posible. Los paquetes OSPF potencialmente grandes tales como los paquetes de la descripción de la base de datos o paquetes de la actualización del estado del enlace se pueden partir fácilmente en los múltiples paquetes por OSPF.

Los mensajes del OSPF utilizan normalmente el enlace-local de la dirección IPv6 de la interfaz origen como sus direcciones fuente. Utilizan la dirección local o global del unicast del enlace virtual como su fuente. Dependiendo de la situación, los mensajes de OSPF se pueden enviar como unicast a un vecino específico o como multicast a los vecinos múltiples. Las siguientes dos direcciones multicast son descartadas con este propósito:

- **AllSPFRouters (FF02:: 5):** Todos los router que funcionan con OSPF deben escuchar esta dirección multicast. Los paquetes Hello se envían siempre a esta dirección. Esta dirección también se utiliza para algunos paquetes durante la inundación del LSA.

- **AllDRouters (FF02:: 6):** El DR y el BDR en un medio de multiacceso deben escuchar esta dirección multicast. Esta dirección se utiliza para algunos paquetes durante la inundación del LSA.

Los paquetes de OSPF enviados a la dirección multicast tienen un alcance de enlace-local, y el límite de salto se coloca en 1. Nunca serán enviados sobre saltos múltiples.

B. Cabecera OSPF

Hay cinco tipos de paquete usados por OSPF. Todos los paquetes de OSPF comienzan con un estándar de cabecera de 16 octetos, esto se muestra en la figura 13.

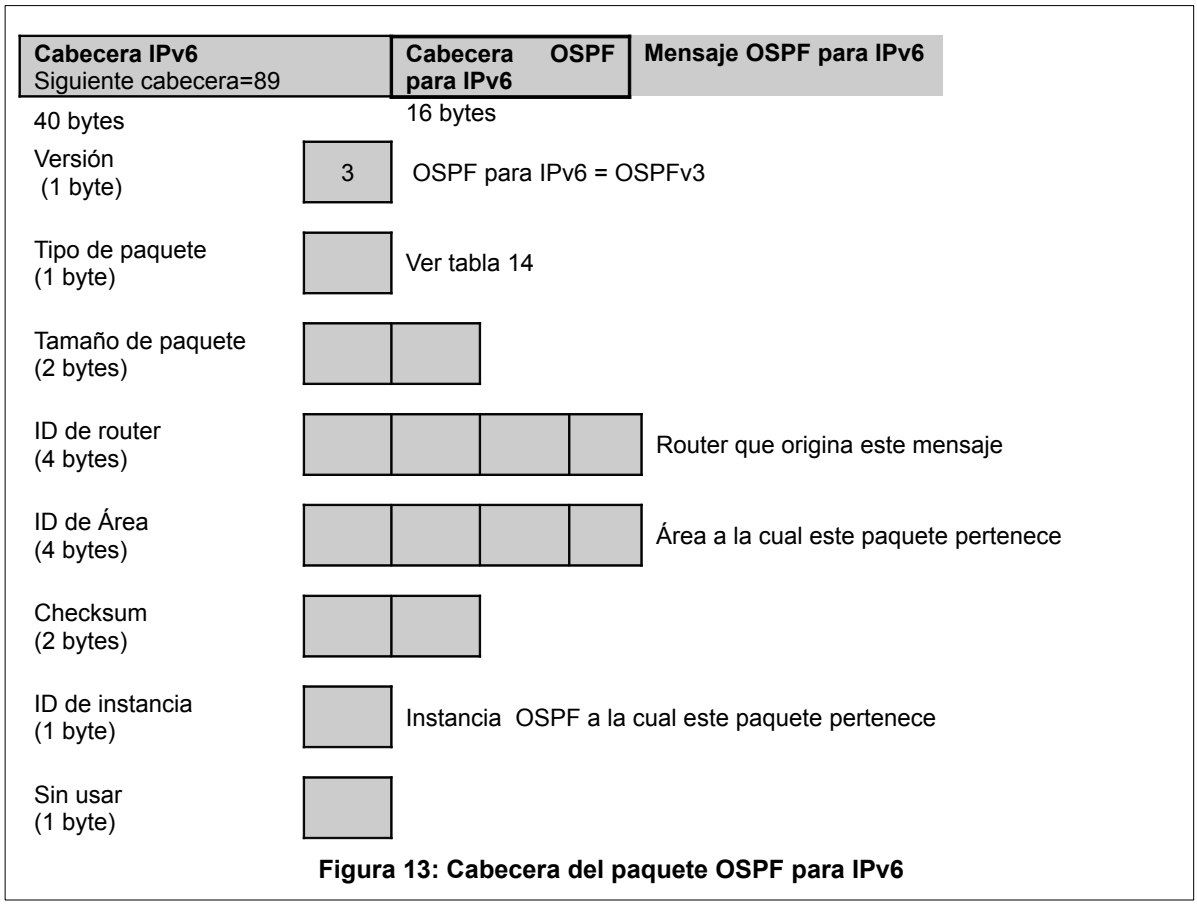

Figura 13: Cabecera del paquete OSPF para IPv6

Los campos de la cabecera OSPF se explican detalladamente a continuación:

- **Versión (1 byte):** OSPF para IPv6 utiliza la versión número 3.
- **Tipo (1 byte):** Define el tipo de mensajes de OSPF. La tabla 14 enumera todos los posibles tipos de mensajes OSPF.
- **Longitud del paquete (2 bytes):** Ésta es la longitud del paquete del protocolo OSPF en bytes, incluyendo la cabecera OSPF.
- **ID de Router (4 bytes):** Es el ID del router que origina el paquete. Cada router debe tener un único ID de router, un número de 32 bits representado normalmente en notación decimal. La identificación del router debe ser única dentro del AS.
- **ID de área (4 bytes):** El ID de área identifica el área a la cual pertenece el paquete OSPF. El área se basa normalmente en el área del interfaz origen del router. El ID de área es un número entero de 32 bits. El área 0 representa el área del backbone.
- **Checksum (2 bytes):** OSPF utiliza el cálculo estándar para el checksum en las aplicaciones IPv6. El checksum es computado usando los 16-bits de la suma del complemento sobre el paquete entero. Si la longitud del paquete no es un número entero de una palabra de 16-bits, el paquete se rellena con ceros antes del checksumming. Antes de computar el checksum, el campo del checksum en la cabecera del paquete OSPF se pone a 0.
- **ID de instancia (1 byte):** Identifica la instancia OSPF a la cual pertenece el paquete. El ID de instancia es un número de 8-bits asignado a cada interfaz del router. El valor por defecto es 0. El ID de instancia para el protocolo OSPF permite casos múltiples en un solo. Si el router destino no reconoce el ID de instancia, entonces desecha el paquete.

Tipo de Paquete	Nombre	Descripción
1	HELLO	Inicializa y mantiene adyacencias. También elige el DR y BDR.
2	Descripción de la Base de datos	Intercambia la descripción de la base de datos durante la formación de adyacencias.
3	Petición del estado del enlace	Peticiones que faltan o cambian de los LSAs
4	Actualización del estado del enlace	Transmite LSAs a cualquiera que responda a las peticiones al formar adyacencias o durante las inundaciones de los LSA.
5	Reconocimiento del estado del enlace	Reconoce la recepción de un LSA. Cada LSA debe ser reconocido

Tabla 14: Tipos de paquetes del OSPF para IPv6

C. Proceso de los paquetes OSPF

Cuando un router envía un paquete del protocolo OSPF, completa los campos de la cabecera según lo descrito en el apartado B de esta sección. EL ID de área y el ID de instancia son tomados de la estructura de datos del interfaz origen. Si se requiere la autentificación, es responsabilidad de IPv6 sumar las cabeceras necesarias.

Cuando un router recibe un paquete del protocolo OSPF, IPv6 primero lo valida comprobando las cabeceras IPv6 (direcciones IPv6, campo de siguiente cabecera, y la autentificación). Entonces el paquete es dado al proceso OSPF, este comprueba el número de versión (el cual para IPv6 debe ser 3), el checksum, el ID de área, y el ID de instancia. El ID de área debe concordar con el ID de área configurada en la interfaz destino. Si no son iguales, pero el ID de área es 0, la interfaz destino debe ser el punto final de un enlace virtual. El ID de instancia debe concordar con el ID de instancia del interfaz. Si la dirección IPv6 del destino del paquete es la dirección multicast AllDRouters, el router debe ser un DR o un BDR en este enlace. Si el paquete pasa todas estas pruebas, se pasa al proceso apropiado del OSPF para transformaciones futuras; de otra manera debe abandonarse.

4. FORMACIÓN DE ADYACENCIAS

Para intercambiar LSAs, los router deben crear canales confiables a sus vecinos los cuales se denominan adyacencias. Estos canales permiten que los router sincronicen el LSDB al darse la inicialización e inunden el LSA en caso de que exista un cambio.

Los vecinos necesitan primero ser descubiertos. Cada interfaz en un router OSPF se le asigna uno de los cuatro tipos de enlace: Punto-a-Punto, tránsito, trozo, o virtual.
En el Punto-a-Punto o enlaces virtuales, solo un vecino puede ser descubierto. El enlace de tránsito corresponde a las redes de multiacceso (Ejemplo Ethernet); los router múltiples pueden estar conectados con esta red, y por lo tanto más de un vecino podría ser descubierto. No es necesaria la formación de adyacencias con todos los router en un enlace de tránsito.

Cada enlace de tránsito elige un DR para formar adyacencias con todos los router en el enlace de tránsito. Esto garantiza que todos los router en este enlace tienen un LSDB sincronizado. Para asegurar la operación sin interrupciones, también se debe de elegir un BDR; este forma adyacencias con todos los router del enlace de tránsito. En la figura 14 se muestran adyacencias de enlace Punto-a-Punto y enlaces de tránsito. Si no se descubre a ningún vecino en ningún enlace dado, el enlace se declara un enlace de trozo, y no se está formando ninguna adyacencia en tal enlace.

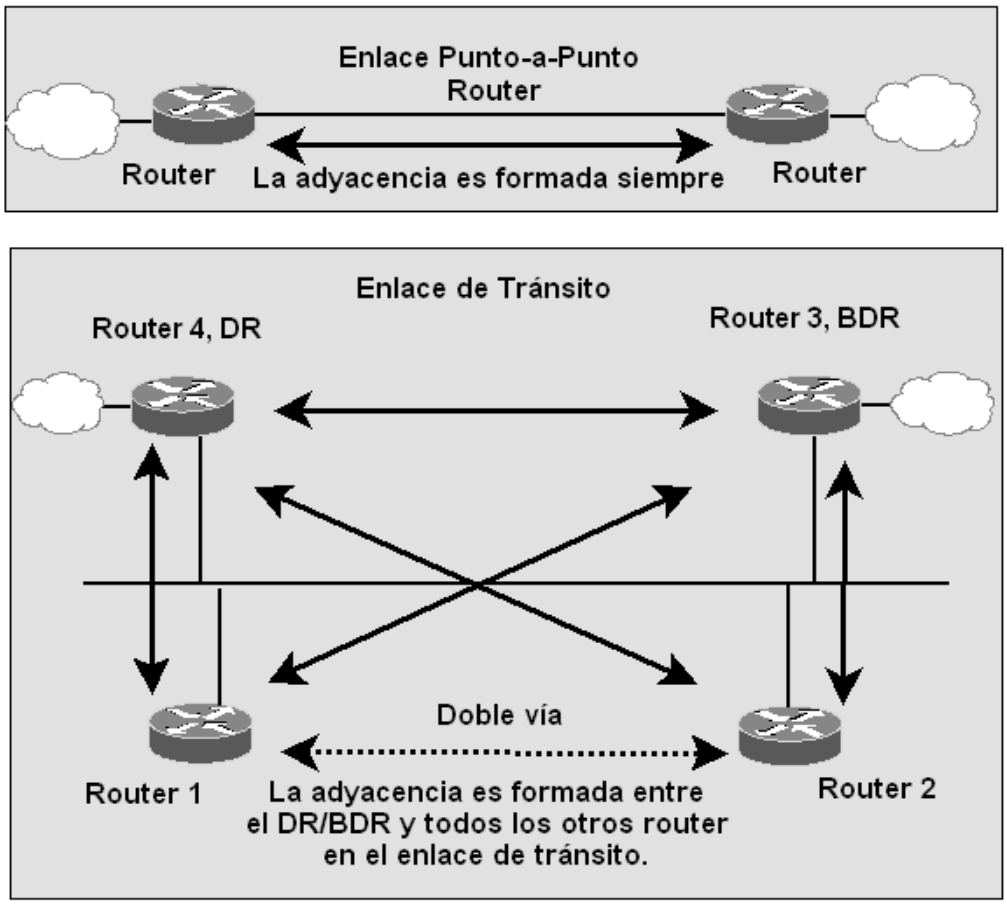

Figura 14: Adyacencias en un enlace de tránsito y en un enlace Punto-a Punto

A. El paquete Hello

El paquete Hello es responsable de inicializar y mantener adyacencias así como de elegir un DR/BDR. Este asegura que la comunicación entre dos routers sea bidireccional. Los paquetes Hello se envían a través de cada interfaz en los intervalos regulares. En el Punto-a-Punto o redes broadcast-capable de tránsito, los paquetes Hello del OSPF se envían a la dirección AllSPFRouters del multicast. Las redes multiacceso no son capaces de transmitir la difusión o los paquetes del multicast, a esto se le llama non-broadcast-multi-access networks (NBMA).

Las redes de NBMA se pueden configurar como enlace punto a múltiples puntos o enlaces de tránsito. Los enlaces Punto a múltiples puntos son realmente enlaces Punto-a-Punto como los enlaces lógicos creados para cada vecino. Como en el enlace Punto-a-Punto, no hay necesariamente un DR o BDR. Las redes NBMA configuradas con los enlace de tránsito tienen direcciones IPv6 creadas para cada vecino; se elige un DR y un BDR. Los mensajes OSPF se envían como unicast a estos vecinos configurados estáticamente.

La figura 15 muestra el formato del paquete Hello. El paquete OSPF es de tipo 1 según se muestra en la tabla 14.

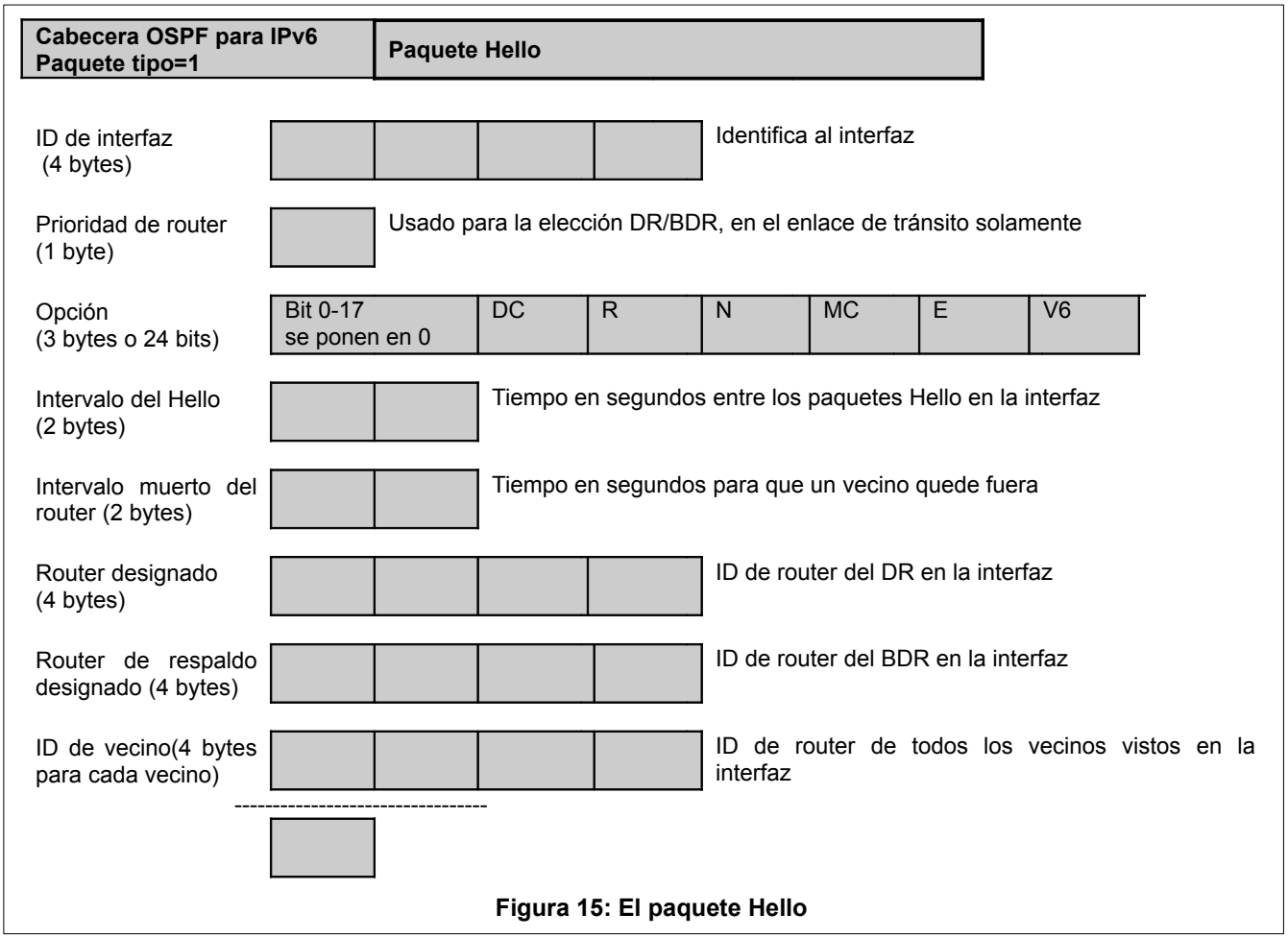

Figura 15: El paquete Hello

La siguiente lista explica todos los campos del paquete Hello:

- **ID de interfaz (4 bytes):** Identifica el interfaz del paquete Hello. A cada interfaz de un router OSPF se le asigna un ID de interfaz. El ID de interfaz debe ser único dentro del mismo router. Algunas implementaciones usan el MIB-II Índice de Interfaz que se encuentra especificado en el RFC 2863.
- **Prioridad del router (1 byte):** Identifica que número de prioridad que el router le asignó a la interfaz. Se utiliza para la elección del DR o BDR. Este campo es significativo solamente en el enlace de tránsito. El router con la prioridad más alta se convierte en el DR o BDR, pero solo si un DR o un BDR no se haya elegido. Si este campo se pone a 0, el router de la interfaz nunca puede ser un DR o BDR.
- **Opciones (3 byte):** Describe la capacidad de opción del router. Este campo está colocado en los paquetes Hello del OSPF, en los paquetes de la descripción de la base de datos, y en los LSAs siguiente: Router-LSA, Red-LSA, Inter-Área-Router-LSA, y enlace-LSA. La tabla 15 explica los bits usados en el campo Opciones. Solo 6-bits se utilizan actualmente.
- **Intervalo Hello (2 bytes):** Especifica el número de segundos entre los paquetes Hello enviados por el router en el enlace. Por defecto son 10 segundos.
- **Intervalo muerto del router (2 bytes):** Especifica el número de segundos antes de que el router declare un router silencioso por el enlace caído. (Un router silencioso ya no envía los paquetes Hello.) Por defecto son 40 segundos. En un enlace de tránsito, el intervalo muerto del router también determina el contador de tiempo que va a espera durante la elección del DR o BDR. En la inicialización de un enlace de tránsito, la interfaz entra en un estado de espera para determinar si un DR o BDR ya ha sido elegido.
- **ID de router designado (4 bytes):** Especifica el ID de router del DR desde la perspectiva del router en el enlace. Este campo es útil sólo en enlaces de tránsito. Por defecto esta en 0.0.0.0 cuando ningún DR ha sido elegido, o en un enlace Punto-a-Punto.
- **ID de router designado para reserva (4 bytes):** Especifica el ID de router del BDR desde la perspectiva del router en el enlace. Este campo es útil sólo en enla-

ces de tránsito. Por defecto esta en 0.0.0.0 cuando ningún BDR ha sido elegido, o en un enlace Punto-a-Punto.

- **ID del vecino (4 bytes):** Especifica el ID de router de cada router vecino del cual el router local ha recibido los paquetes Hello válidos en el enlace del router pasado durante el intervalo muerto.

Bit	Nombre	Descripción
0-17	No se usa	Reservada para usos futuros.
18	DC	Dirección de los circuitos de la demanda, según lo descrito en RFC 1793.
19	R	Indica quien originó el paquete Hello es un router activo. Si este bit se coloca a 0, significa que quien lo originó ya no reenviará los paquetes.
20	N	Todas los router dentro de un NSSA deben poner este bit. Además, el bit de E se debe poner a 0 (ver RFC 3101).
21	MC	Capacidad del multicast, según lo definido en RFC 1584.
22	E	La capacidad de rutas externas del router. Todos los miembros de un área deben convenir en la capacidad externa. En un trozo del área, todas los router deben colocar este bit en 0 para lograr adyacencia. El bit E es significativo sólo en los paquetes Hello (similar para el bit N).
23	V6	Indica que el router soporta OSPF para IPv6. Si se pone a 0, este router/enlace se excluye del cálculo de ruteo IPv6.

Tabla 15: Bits usados en el campo Opciones.

B. Proceso de los paquetes Hello

Antes de que se acepte un paquete Hello, existe un número de criterios que se deben cumplir para que un paquete Hello sea aceptado, en la figura16 se muestra el proceso.

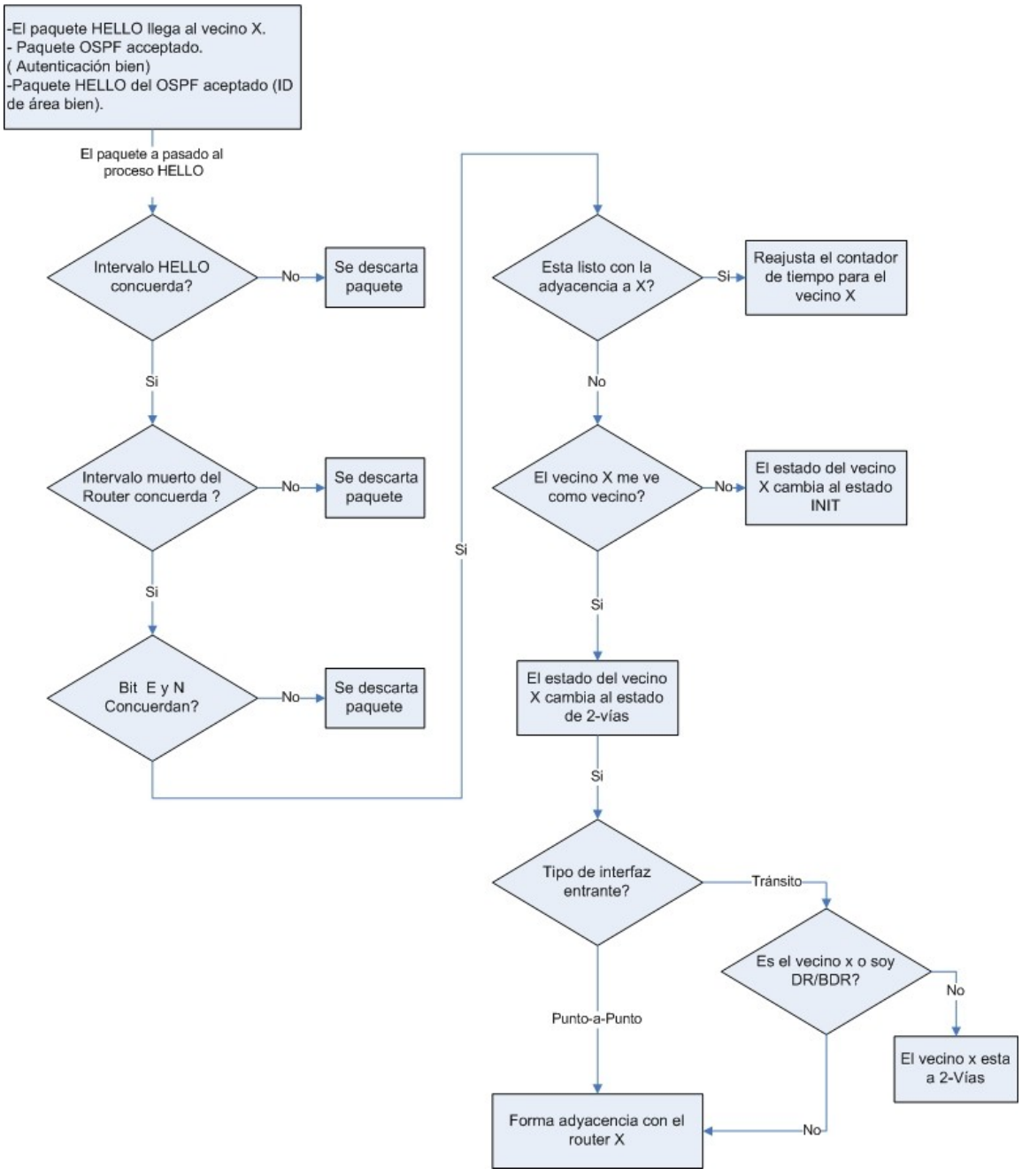

Figura 16: Proceso del paquete Hello.

El proceso de entrada del OSPF ha aceptado el paquete según lo descrito en la sección 3 de este capítulo. Ahora se comprueba el intervalo de los paquetes Hello y el intervalo muerto del router, los valores colocados en la interfaz de destino deben corresponder. Después, los bits E y N en el campo opciones se examinan. Los ajustes de estos bits deben corresponder al valor colocado en la interfaz destino.

En este punto, si todos los criterios concuerdan, el paquete es aceptado y el vecino es identificado por su ID de router. El router mantiene una tabla de estado del vecino por cada interfaz. Si hay ya una adyacencia completa con este vecino, el temporizador del paquete Hello simplemente vuelve a arrancar. Si no, el estado de este vecino cambia para inicializarse (Init). El router examina la lista de los vecinos proclamados en el paquete Hello recibido. Si el router identifica su ID de router en esa lista, la comunicación bidireccional esta establecida, y el estado del vecino cambia a dos vías. El router decide si forma una adyacencia con ese vecino. Si el estado del interfaz es Punto-a-Punto, una adyacencia se forma con es vecino. Si el router decide no formar una adyacencia, este vecino permanece en un estado de doble vía.

La figura 17 explica las diversas fases de formar una adyacencia y los estados de los vecinos correspondientes.

C. Estado del interfaz y elección de DR/BDR

Tan pronto como IPv6 en una interfaz OSPF hace conexión el proceso de los paquetes Hello comienza. Un enlace Punto-a-Punto cambia su estado y es inmediatamente activa-do.

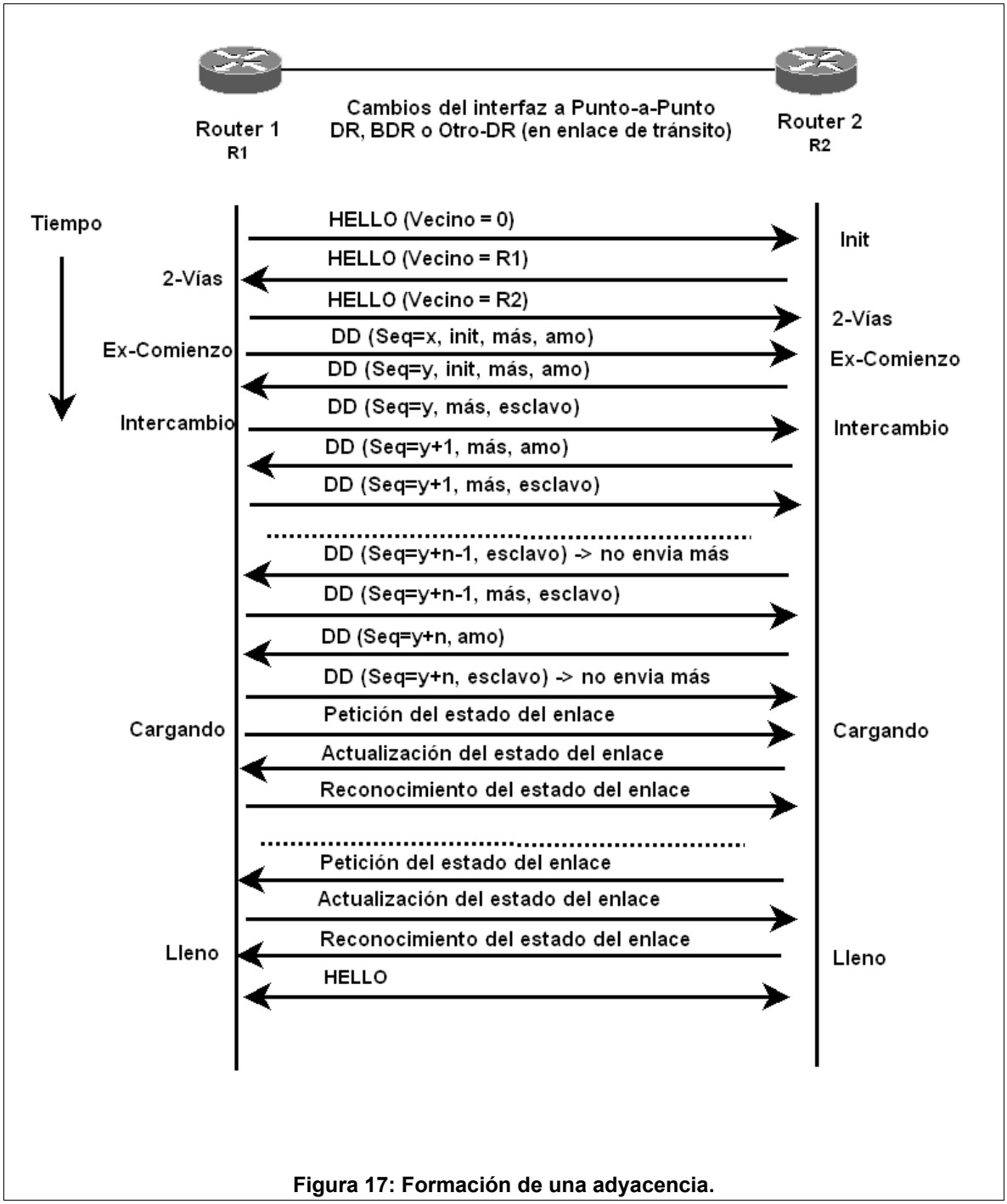

Figura 17: Formación de una adyacencia.

Un enlace de tránsito primero entra en el estado de espera para descubrir el DR/BDR. Cada enlace de tránsito necesita un DR y un BDR, el cuál forma adyacencias con todos los router en ese enlace de tránsito en particular. Para cada enlace del router hace lo siguiente: Durante el período de espera, el router escucha los paquetes Hello para determinar si un DR/BDR ya existe. También envía los paquetes Hello con el DR/BDR con el campo puesto en 0 para señalar que está en modo de descubrimiento. Si un router reclama ser el DR, ninguna elección de un DR ocurre. Si ningún router se declara a sí mismo como el DR (todos los paquetes Hello contienen un 0 en su campo DR), el router con la prioridad más alta se declara por sí mismo el router DR. Si las prioridades son iguales, el router con el más alto ID de router gana la elección. El BDR se elige exactamente de la misma manera. Los router que no fueron elegidos como DR/BDR se llaman otros-DR. El estado de la interfaz cambia ya sea para DR, BDR, u otros-DR y llega a ser activo. Los router con una prioridad de 0 nunca se convierten en DR/BDR. El estado de la interfaz cambia inmediatamente para otro-DR sin entrar al estado de espera.

Si el DR se vuelve silencioso (no envía paquetes Hello al router), el BDR se convierte en el DR, y un BDR nuevo es elegido porque el BDR ya ha formado todas las adyacencias, no hay interrupción del LSDB sincronizado en ese enlace de tránsito. Si el DR original regresa en línea, reconoce que hay ya un DR y un BDR, y entra en el estado de otro-DR. Si el BDR se vuelve silencioso, un BDR nuevo es elegido.

D. Intercambio de la descripción de la base de datos

Los router cambian su estado de vecino a comenzar-intercambiar y envían un paquete inicial de la descripción de la base de datos sin datos. Establecen una relación amo-esclavo para alcanzar un intercambio ordenado. Cada router se declara como el amo en el paquete inicial de la descripción de la base de datos. La única información relevante dentro del paquete inicial de la descripción de la base de datos es el número de serie de la descripción de la base de datos (DD) publicado por cada lado. El router con el ID de router más alto permanece como amo durante toda la fase del intercambio de la DD.

Ahora los vecinos incorporan el estado de intercambio. Comenzando con el esclavo, una serie de paquetes que describen el contenido de su LSDB se intercambian. El amo siempre incrementa el número de serie y el esclavo siempre usa el número de serie del amo en su paquete. Cada router indica que tiene más datos a enviar colocando el bit-más (ver la figura 18). Si un router ha enviado su descripción entera de la base de datos pero el otro no lo ha hecho aún, el primer router tiene la obligación de enviar los paquetes vacíos para mantener los números de serie emparejados. Para describir al LSDB, el router sólo envía las cabeceras de la base de datos (las cabeceras LSA[26]) según lo descritos en la figura 18. Todos los paquetes de la descripción de la base de datos se envían al vecino como unicast. Las direcciones del unicast son descubiertas mirando la dirección origen del paquete Hello enviado por el vecino. Tan pronto como ambos router no tengan nada más que enviar, los router se incorporan a la fase de carga.

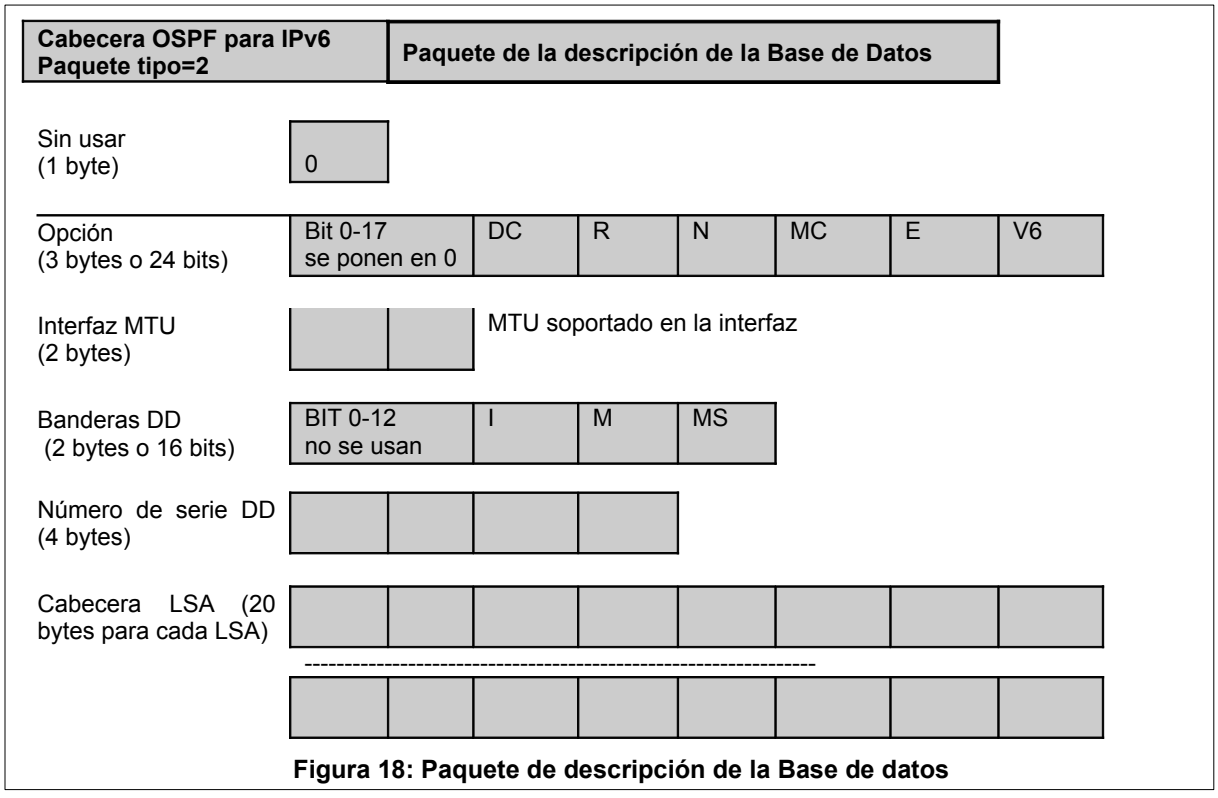

Figura 18: Paquete de descripción de la Base de datos

[26] Ver sección 6 de este capítulo

La siguiente lista explica todos los campos del paquete de Descripción de la Base de Datos:

- **Opciones (3 bytes):** Es la capacidad opcional soportada por el router según lo que muestra la tabla 15. Estas deberían ser las mismas opciones anunciadas en el paquete Hello. Los cambios en el campo opciones durante el intercambio de la DD pararán el intercambio, y los router vuelven a comenzar-intercambiar.
- **MTU del interfaz (2 bytes):** Es el tamaño más grande del marco que se puede enviar a través del interfaz sin que se de la fragmentación. Si el router recibe un paquete DD que indica un MTU más grande que puede manipular en la interfaz destino, se rechaza el paquete. En enlaces virtuales, esto se debe poner a 0.
- **Init bit (I bit):** Cuando se pone a 1, este bit indica el primer paquete de la Descripción de la Base de Datos enviado por el router. Este paquete no contiene ningún dato y comienza el proceso de intercambio.
- **bit-más (M bit):** Cuando se pone a 1, este bit indica que hay más paquetes de la Descripción de la Base de Datos. Cuando se pone a 0, indica que se han entregado todas las descripciones de la base de datos.
- **bit amo/esclavo (M/S bit):** Cuando se pone a 1, este bit indica que ese router es el amo; si no, es esclavo.
- **Número de serie DD (4 bytes):** Este número hace el intercambio confiable. El amo incrementa el número de serie por uno para cada paquete de la descripción de la base de datos enviada. El esclavo siempre evalúa el último número de serie recibido por el amo. Una incompatibilidad en el número de serie causa que el cambio DD fracase y los router vuelven a realizar el proceso comenzar-intercambiar.
- **Lista de cabeceras LSA (20 bytes para cada cabecera):** Esta lista describe la entrada en el LSDB[27].

[27] Ver sección 6 de este capituló

5. BASE DE DATOS DEL ESTADO DEL ENLACE (LSDB)

La base de datos del estado del enlace (LSDB) es el componente más importante del OSPF. La figura 19 ilustra los componentes del LSDB.

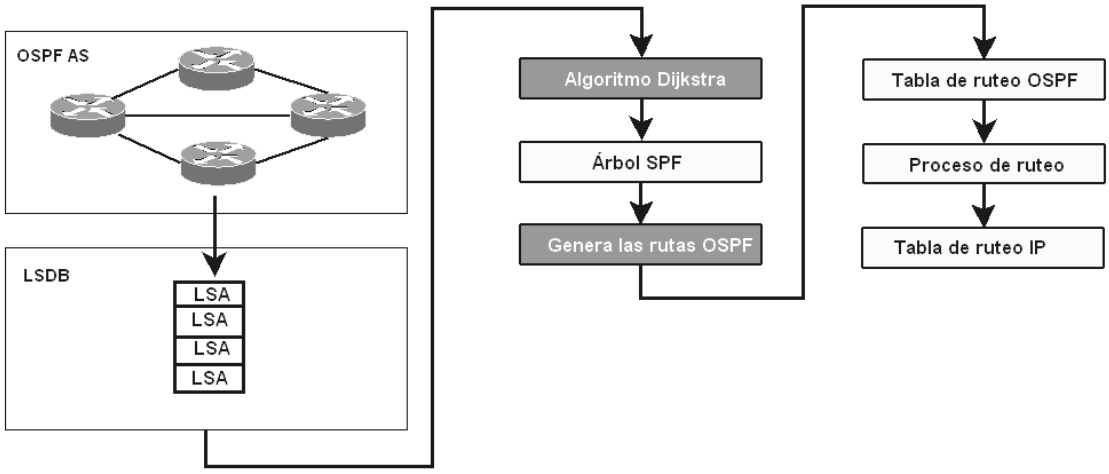

Figura 19: Componentes del LSDB

El LSDB es una estructura de datos que consiste de LSAs que han sido intercambiados en el AS. La información del estado del enlace se estructura para permitir la estructura de un árbol con ramas y hojas que representan las trayectorias más cortas a todas las rutas dentro del AS. Cada router construye su árbol desde su punto de vista. Lo más común es que los router utilizan el algoritmo de Dijkstra para construir este árbol con las trayectorias más cortas (árbol del SPF). Primero, el router construye el árbol del Intra-área a todos los destinos dentro de su propia área. El Inter-área y las rutas externas se unen a la rama que representa un ABR o un ASBR. En el extremo, cada ruta dentro del árbol se agrega a una de cuatro secciones de la tabla de ruteo del OSPF: las rutas del Intra-área, rutas del Inter-área, rutas externa-1, y finalmente, rutas externa-2. El siguiente salto es siempre la dirección de enlace-local del primer router con la trayectoria más corta.

A. Contenido del LSDB

El RFC 2328 describe el SPF como sistema de gráficos dirigidos usando vértices para construir un árbol. Esto describe básicamente la topología de la red como una colección de indicadores que construyen un árbol. Hay tres indicadores básicos dentro del árbol:

- **Router-a-Router:** Describe la interfaz Punto-a-Punto de un router, identifica el ID de router del Router vecino en un enlace Punto-a-Punto. En la terminología de LSDB, eso señala un Router-LSA para otro Router-LSA.
- **Enlace de tránsito a un router:** Describe el interfaz de un router en un enlace de tránsito identificando el ID de interfaz del DR para este enlace de tránsito. En la terminología de LSDB, eso señala de un Router-LSA a una Red-LSA.
- **Enlace de tránsito a routers:** Describe un enlace de tránsito y señala todos sus router unidos. En la terminología LSDB, eso señala de una Red-LSA para uno o muchos Router-LSAs.

Existen también elementos informativos los cuales proporcionan información complementaria asociada a las ramas particulares. Es como añadirle las hojas a las ramas. A diferencia de los tres indicadores anteriores, que construyen el árbol real, el elemento informativo sólo le añade la información al árbol. Los LSAs que representa un elemento informativo son Inter-Área-Prefijo-LSA, Inter-Área-Router-LSA, AS-Externo-LSA, Tipo-7-LSA, Enlace-LSA, e Intra-Área-Prefijo-LSA.

La figura 20 muestra los indicadores básicos y el elemento informativo en una estructura del árbol.

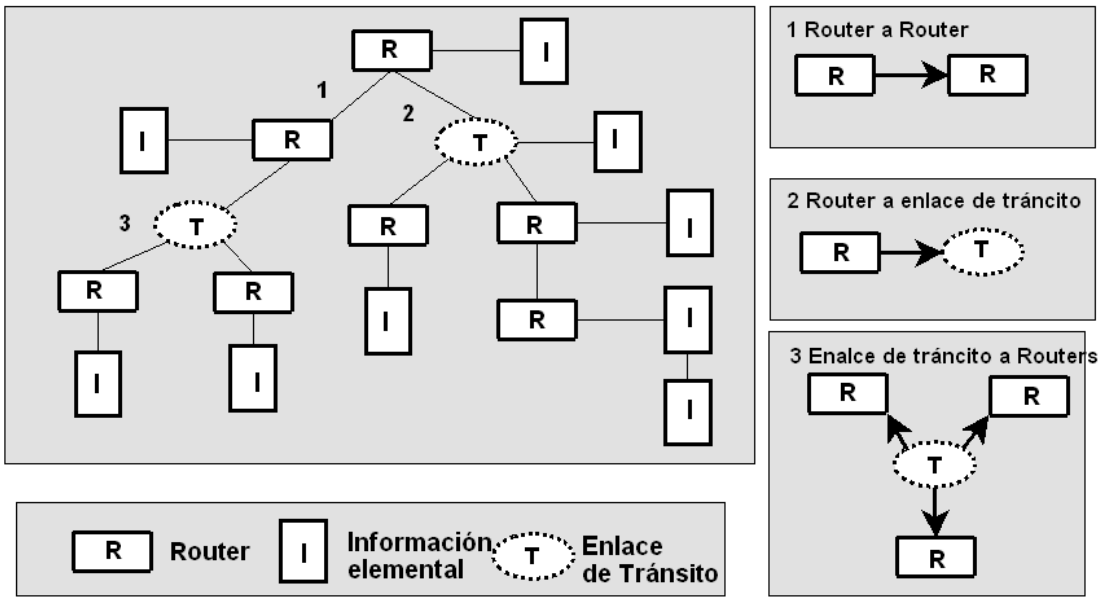

Figura 20: Indicadores de la estructura del LSBD

6. LSAS (ANUNCIOS DEL ESTADO DEL ENLACE)

Cada LSA dentro del LSDB incorpora uno o más de los indicadores previamente mencionados[28] o de los elementos informativos. Consiste en una cabecera LSA y un cuerpo LSA. La cabecera LSA identifica cada LSA individualmente.

A. Cabecera LSA

Cada LSA comienza con un campo común la cabecera de 20 bytes. La figura 21 muestra los detalles de esta cabecera. El tipo del estado del enlace (LS), el ID-LS, y el router designado, juntos identifican únicamente el LSA.

[28] Ver sección 5 de este capituló

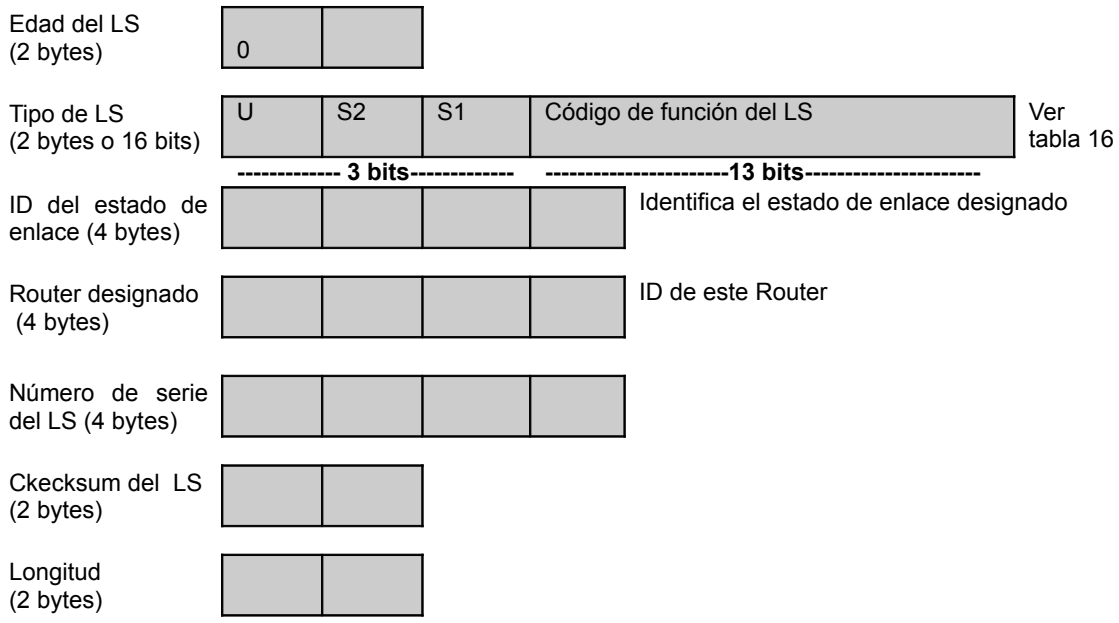

Figura 21: Cabecera LSA

Los campos de la cabecera LSA se detallan en la siguiente lista:

- **Edad del LS (2 bytes):** La edad del LS es el tiempo en segundos desde que la LSA fue originada. Si ha alcanzado la máxima edad (3,600 segundos), el LSA no se considera más para el cálculo del árbol del SPF. EL router que origina este LSA debe renovar el LSA e incrementar el número de serie antes de que se alcance la edad máxima, para evitar que el LSA envejezca. Es recomendado renovar un LSA tras darse la máxima edad dividida entre dos.
- **Tipo del LS (2 bytes):** Éste es el tipo de LSA anunciado. Los primeros tres bit del campo Tipo del LSA indican las características especiales del LSA. Los tipos de LS se explican en la tabla 16.
    - **U bit (dirección del tipo desconocido del LS):** Identifica la dirección de los tipos desconocidos de LSA por los routers. Si el bit está colocado con valor de 1, el LSA debe ser almacenado y ser inundado como si el tipo fuera comprendido. Si no, si el bit es 0, el LSA tiene que ser tratado como si tuviera el enlace-local al alcance de la inundación.

- **Bit S2 y S1 (al alcance de la inundación):** Los cuatro valores para definir el alcance de la inundación de los LSA son:

  00 = enlace-local, se inunda solamente en el enlace en el cual se originó.

  01 = el área, se inundan todos los router en el área que se originó.

  10 = AS, se inundan todos los router en el AS.

  11 = reservado.

  Los últimos 13 bits representan el código real de la función del LSA. Ver la tabla 16 para los tipos del estado del enlace. El tipo del LS se representa en la notación hexadecimal para reflejar el alcance de la inundación.

- **ID del estado del enlace (4 bytes):** El ID del estado del enlace es parte de la identificación del estado del enlace. Con el Router-LSA y Red-LSA, los servicios del ID del estado del enlace se usan como un indicador en el árbol para identificar un router o una red. Para el resto del LSAs, el router que origina utiliza un ID local único.
- **Router designado (4 bytes):** El router designado es el ID de router del router que origina este LSA.
- **Número de serie del LS (4 bytes):** El número de serie del LS identifica la instancia de este LSA. Se utiliza para determinarse qué LSA es más nuevo en caso de ocurrieren múltiples LSA del mismo. Cuanto más alto es el número de serie, más nuevo es el LSA. El número de serie que comienza es siempre 0x80000000. El número de serie más alto posible es 0x7FFFFFFF. Si se ha alcanzado este número, el LSA se envejece (la edad del LS es igual a la máxima edad) y se inunda antes de que una instancia nueva de la LSA (ahora utilizando 0x80000000) sea editado.
- **Checksum (2 bytes):** Ésta es la suma de comprobación del Fletcher del contenido completo del LSA, incluyendo la cabecera del LSA pero excluyendo el campo de la edad del LS.
- **Longitud (2 bytes):** Ésta es la longitud entera del LSA en bytes.

Tipo de Ls	Nombre	Alcance de la inundación	Anunciado por	ID del estado de enlace
0X2001	Router-LSA	Área	Cada Router	ID de router
0X2002	Red-LSA	Área	DR	ID de la interfaz del DR del enlace de tránsito
0X2003	Inter-Área-Prefijo-LSA	Área	ABR	Un ID local único puesto por el ABR
0X2004	Inter-Área-Router-LSA	Área	ABR	Un ID local único puesto por el ABR
0X2005	AS-Externo-LSA	AS	ASBR	Un ID local único puesto por el ASBR
0X2006	Grupo-Membership-LSA	Área	Ver RFC 1584	Ver RFC 1584
0X2007	Type-7-LSA	Área	Ver RFC 3101	Ver RFC 3101
0X2008	Enlace-LSA	Enlace	Cada router para cada enlace	ID de interfaz local única
0X2009	Intra-Área-Prefijo-LSA	Área	Cada router	Un ID local único puesto por el router

Tabla 16: Tipos del Estado de Enlace (LS)

- **Router-LSA (tipo 0x2001)**

Los enlaces del router describen los enlaces Punto-a-Punto, virtuales, o de tránsito del router. Básicamente, incluye todos los enlaces que tienen por lo menos un vecino. A diferencia de OSPF para IPv4, los enlaces del trozo se anuncian solamente dentro de un enlace de router. Un ABR debe originar los enlaces separados para cada área unida, conteniendo solamente los enlaces que pertenecen a esa área en particular. Los enlaces virtuales pertenecen al área 0 y son anunciados siempre por ABR.

- **Red-LSA (tipo 0x2002)**

El router designado para cada enlace de tránsito en el área origina una Red-LSA. El ID de estado del enlace se pone para el ID del interfaz del DR para el enlace de tránsito. Contiene el campo opciones seguido por una lista de los IDs de router que identifican todas los router unidos a este enlace de tránsito en particular. Esto representa un indicador a todos los router unidos a este enlace de tránsito.

o Inter-Área-Prefijo-LSA (type 0x2003)

El Inter-Área-Prefijo-LSAs es originado por el ABR para anunciar los prefijos IPv6 de otras áreas en el área de este LSA. Un Inter-Área-Prefijo-LSA se origina para cada ruta. Un ABR podría resumir un alcance íntimo de prefijos IPv6 en un solo anuncio. Para un área del trozo, el ABR anuncia la ruta predeterminada utilizando a este LSA. El Inter-Área-Prefijo-LSA es el equivalente al Resumen-LSA en OSPFv2.

o AS-External-LSA (type 0x2005)

Los AS-Externo-LSAs son anunciados por ASBRs para importar los prefijos externos IPv6 en el AS. Cada AS-Externo-LSA representa un prefijo IPv6 externo a OSPF, aprendido de RIP, BGP, estáticas, etc. Son inundados a todo lo largo del AS y por lo tanto se sabe que es conocido por cada router excepto los routers en el área del trozo.

o Enlace-LSA (type 0x2008)

El Enlace-LSAs es originado por cada router, uno para cada enlace del router. Nunca se inundan más allá de este enlace. El ID del estado de enlace está listo para el ID de interfaz de este enlace. El Enlace-LSA sirve para tres propósitos, y provee:

- La dirección enlace-local del router para todos los otros routers que corresponde a este enlace.
- Una lista de los prefijos IPv6 que se asociaron a este enlace.
- Una lista de las opciones que se utilizarán por el router designado para este enlace.

o Intra-Área-Prefijo-LSA (type 0x2009)

Un router utiliza el Intra-Área-Prefijo-LSA para anunciar uno o más prefijos IPv6 asociados al router o a una Red-LSA. Como OSPF para IPv6 ha quitado toda la semántica de dirección del Router-LSAs y de la Red-LSAs, el Intra-Área-Prefijo-LSA proporciona esta información. Cada prefijo de la dirección anunciada se asocia a un Router-LSA o a una Red-LSA.

7. INUNDACIÓN DE LSA

Cualquier cambio en la red causa que cierta información del estado del enlace cambie. Los ejemplos de tales cambios incluyen lo siguiente:

- El estado de la interfaz OSPF de un router cambia.
- Un vecino efectúa una transición para un estado completo.
- Un vecino pierde adyacencia completa.
- El DR en un enlace de tránsito cambia.
- Un prefijo nuevo del IPv6 es agregado o suprimido en cualquier interfaz.
- Una interfaz configurada para el OSPF es agregada o suprimida en un router.
- La información sumaria de un área cambia.
- Una ruta externa es agregada o retirada en el ASBR.
- El temporizador de renovación (Edad máxima/2) de un LSA requiere a un LSA actualizado.

El router que detecta el cambio reescribe el LSA por consiguiente, aumenta el número de serie, y le da al LSA el proceso de inundación. Según la tabla 16, el LSA inunda a un vecino solamente (alcance del enlace), a todos los vecinos en la misma área (alcance del área), o a todos los vecinos (alcance del AS).

El inundar significa que el LSA pasa del router anunciado a sus vecinos adyacentes. Dependiendo del alcance de la inundación del LSA, los vecinos lo pasan a sus vecinos, y así sucesivamente. Cada router que recibe un LSA primero evalúa si el LSA es nuevo o tiene un número de serie más alto que el que está instalado ya en el LSDB. Si cualquiera de estas dos condiciones es verdad, el LSA se agrega o se substituye en el LSDB. Ahora el router considerará que las interfaces sean utilizadas para futuras inundaciones. No inundar el LSA fuera del interfaz entrante da una excepción: si el router es un DR para el interfaz entrante del LSA y el LSA no fue enviado por el BDR, debe ser inundado de regreso fuera de la misma interfaz. El DR es responsable de enviar LSAs a todos sus vecinos. Otra razón de no inundar el LSA es, si el LSA es más viejo o tiene la misma edad que la

que está instalada ya. Esto evita que LSAs se coloquen en la red. Los LSAs son normalmente enviados a la dirección multicast de AllSPFRouters con las siguientes excepciones:

- En redes de tránsito, los router en el estado Otro-DR le envían los LSAs a la dirección AllDRouters. La actualización alcanza al DR/BDR, lo cual a su vez le devuelve al resto de routers en este enlace de tránsito, usando la dirección del multicast de AllSPFRouter.
- Si un router pide una actualización del estado del enlace enviando un paquete de petición del estado del enlace, el LSA usa la dirección unicast del router que realizo la petición.
- En NBMA, a todos los LSAs les es enviada la dirección unicast para todos los vecinos configurados estáticamente.
- Las retransmisiones LSA (LSAs no reconocidas) son enviadas a la dirección unicast del vecino.

La figura 21 muestra el proceso de un DR que recibe LSAs nuevos o cambiantes y que inundan a todos los router.

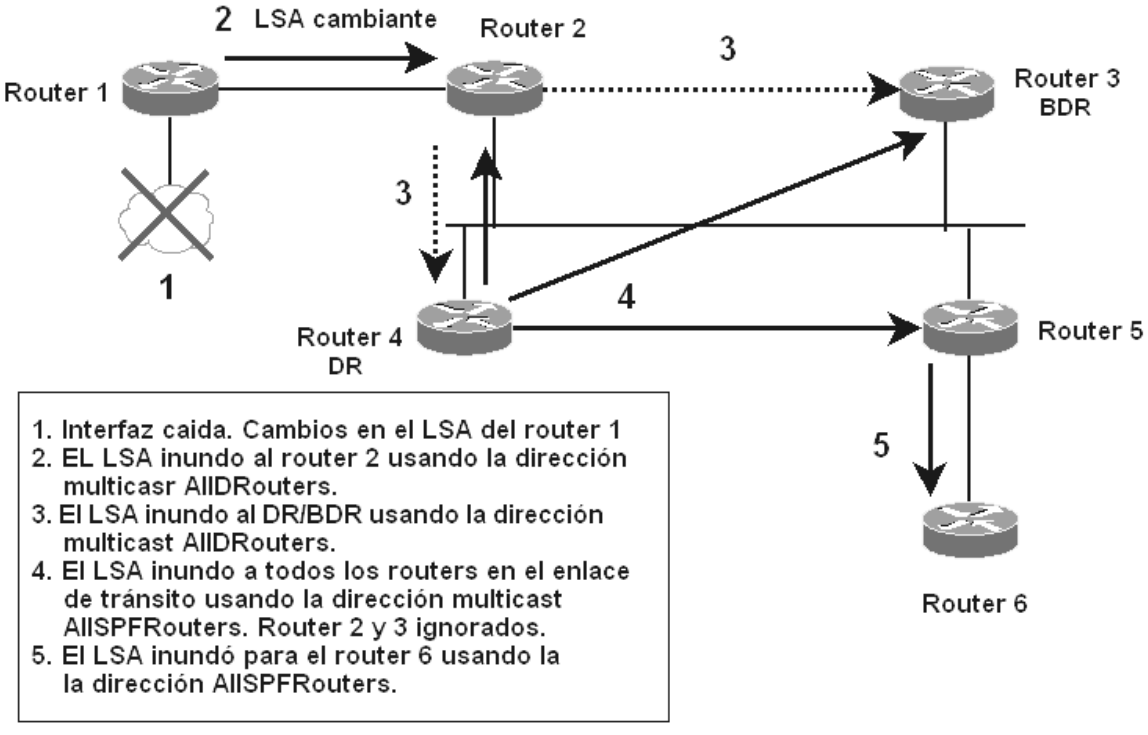

Figura 22: Inundación del LSA

Cada router que recibe un LSA nuevo o cambiante tiene que reconocer este LSA. Enviar un paquete de reconocimiento del estado de enlace logra generalmente esto. Podría también ser reconocida enviando de regreso el LSA si el LSA recibido es más viejo o de la misma edad que la que está ya instalada en el LSDB. En ese caso, el número de serie es el que esta instalado. Los LSAs no reconocidos tienen que ser retransmitidos. Cada router le sigue la pista, cuál vecino ha reconocido a cuál LSA. Las retransmisiones se envían siempre a la dirección del unicast del router vecino.

Un número de serie es asignado al LSA por el router anunciado para no perder de vista el caso más reciente de este LSA en particular. El número de serie es incrementado por el router anunciado cada vez que se cambia el LSA. Cuando se recibe y se acepta un nuevo o cambio de Router-LSA o Red-LSA, el router lo instala en el LSDB. Entonces volver a calcular el árbol del SPF. Si se recibe un LSA nuevo o ha cambiado de tipo, no es nece-

sario calcular nuevamente el árbol del SPF, porque este LSAs representa solamente elementos informativos. Substituyen o quitan la información existente. La nueva información se utiliza para evaluar la mejor trayectoria para el Intra-área, el Inter-área, o los router externos.

CAPITULO III
PROTOCOLO DE RUTEO
BGP4 PARA IPV6

1. GENERALIDADES

A. Introducción

El Protocolo de Compuerta de Frontera, BGP por sus siglas en Inglés, es un protocolo de ruteo utilizado en el borde o frontera de un sistema autónomo (AS). Es un Protocolo de Compuerta Exterior (EGP) y es el protocolo que se usa, generalmente por Proveedores de Servicio de Internet (ISP), para seleccionar rutas sin bucles en Internet. Utiliza el algoritmo de vector de rutas, esto quiere decir que busca las rutas considerando los AS que atraviesa.

La versión actual de BGP[29] es la cuatro, BGP4[30], esta versión cuenta con el respaldo de la mayoría de fabricantes de router como Cisco, Lucent Bay, Juniper y muchos otros, así como también la soportan software para ruteo como lo es Zebra.

Cabe mencionar que el protocolo BGP-4 es un protocolo de ruteo que se utiliza ampliamente con el protocolo de Internet versión 4 y que para poder hacer uso de este protocolo de ruteo en IPv6 es necesario hacer uso de extensiones del protocolo BGP.

Tres trozos de información son transmitidos por BGP-4, es información propia de Ipv4:

- El atributo NEXT_HOP, que es expresado como una dirección IPv4
- El atributo AGGREGATOR, que contiene una dirección IPv4
- El NLRI, que es expresada como un prefijo de dirección.

Por consiguiente, para habilitar a BGP-4 para que pueda utilizar IPv6 lo único que se tienen que hacer es:

[29] Cuando en este documento se mencione al protocolo BGP sin nombrar su versión, se debe entender que se esta haciendo refiriendo al protocolo BGP-4
[30] BGP-4 esta definido en el RFC4271

- Agregar la habilidad para asociar IPv6 con la información del atributo NEXT_HOP (próximo salto)
- Agregar la habilidad para asociar IPv6 con NLRI.

Para lograr que IPv6 pueda ser asociado con el atributo NEXT_HOP y la semántica de NLRI se utiliza el identificador de la familia de dirección (Addres Family).

Aunque BGP se considera como un protocolo de ruteo dinámico, este depende de entradas estáticas, como las declaraciones de vecinos, y la comunicación entre sistemas autónomos

B. Visión General de Ruteo

Los routers son dispositivos que conducen el tráfico entre distintos clientes (hosts), los routers construyen tablas que contienen información de los mejores caminos para las redes que pueden alcanzar estas tablas, estas son llamadas tablas de ruteo.

Los pasos básicos para la determinación de rutas son los siguientes:

Paso 1. Los routers hacen uso de diversos procesos para enviar y recibir información de rutas desde otros routers en la red.
Paso 2. Los routers usan está información para llenar las tablas de ruteo.
Paso 3. Los routers realizan búsquedas en las tablas de ruteo para determinar el mejor camino para alcanzar un destino determinado.
Paso 4. Los routers asocian: la dirección del próximo salto para llegar al destino y la interfaz local de salida, con el propósito de usarlos cuando se reenvíen paquetes a dicho destino.
Paso 5. La información de reenvío para el dispositivo del siguiente de salto, la dirección de red y el nombre de la interfaz asociada, es guardada en la tabla de ruteo del router.
Paso 6. Cuando un router recibe un paquete, el router examina el encabezado del paquete para determinar la dirección del destino.

Paso 7. El router consulta la tabla de reenvío para obtener la interfaz de salida y la dirección del próximo salto para alcanzar el destino.
Paso 8. El router realiza algunos procesos adicionales como el decremento de tiempo de vida del paquete de red y después envía el paquete al dispositivo de salida.
Paso 9. El proceso continúa hasta que el destino sea alcanzado. Este comportamiento refleja el paradigma de ruteo de salto a salto (hop by hop) que es generalmente usado en redes de conmutación de paquetes.

C. Vecinos BGP

Se conoce como vecinos a dos BGP speakers que intercambian información de ruteo, los vecinos BGP pueden ser de dos tipos;

- **Internos:** si se encuentran dentro del mismo AS.
- **Externos:** si no forman parte del mismo AS.

De allí que las declaraciones de vecinos especifican el Sistema Autónomo al que pertenece el vecino así como también su dirección IP. Estas declaraciones del vecino son el corazón del protocolo BGP. Es importante hacer ver que una conexión IP debe existir entre ambos vecinos, ya sea esta conexión por medio de rutas estática, conexión directa o a través del uso de un protocolo de compuerta interna (IGP). BGP no puede encontrar dinámicamente por si mismo la red de un destino dado. Las relaciones del vecino son configuradas a través del uso de la *dirección IPv6.*

D. ¿Qué es un Sistema Autónomo?[31]

Un Sistema Autónomo (AS por sus siglas en Inglés) es definido como una red, o un conjunto de redes, que se encuentran bajo una misma administración o autoridad administrativa. Es decir, que un Sistema Autónomo es una red que esta bajo un único control administrativo. Un Sistema Autónomo podría ser el conjunto de todas las redes de

[31] En el Anexo 1 se puede encontrar más información sobre los AS del país

computadoras de una empresa o de alguna entidad educativa como es el caso de una universidad. Las empresas u organizaciones podrían poseer más de un Sistema Autónomo, pero siempre manteniendo la idea que cada Sistema Autónomo sea administrado independientemente uno del otro.

Los números de Sistema Autónomos son números enteros que identifican a los AS, la Oficina Americana para Registro de Números de Internet[32] define los números de Sistema Autónomos de la manera siguiente:

" *Los números de sistemas autónomos son números únicos que se usan para identificar a los sistemas autónomos y que les permiten intercambiar información de ruteo entre sistemas autónomos vecinos. Un sistema autónomo es un grupo de redes IP, y que siguen una determinada política de ruteo ".*

La IANA[33] ha reservado los números AS de 64512 para 65535 para uso privado. El RFC 1930 provee un conjunto de líneas para la creación, selección y registro de números de sistemas autónomos.

Lo que se ha logrado al utilizar Sistemas Autónomos es dividir al mundo en administraciones independientes entre si, alcanzando la capacidad para tener una red grande dividida en redes más pequeñas y más fáciles de dar mantenimiento. Cada AS puede ejecutar su propio conjunto de políticas de ruteo, independientemente del conjunto de políticas de los demás AS.

La figura 23 muestra gráficamente un ejemplo de Sistemas Autónomos.

[32] ARIN por sus siglas en Inglés, http://www.arin.net
[33] IANA: Autoridad de Asignación de Números de Internet

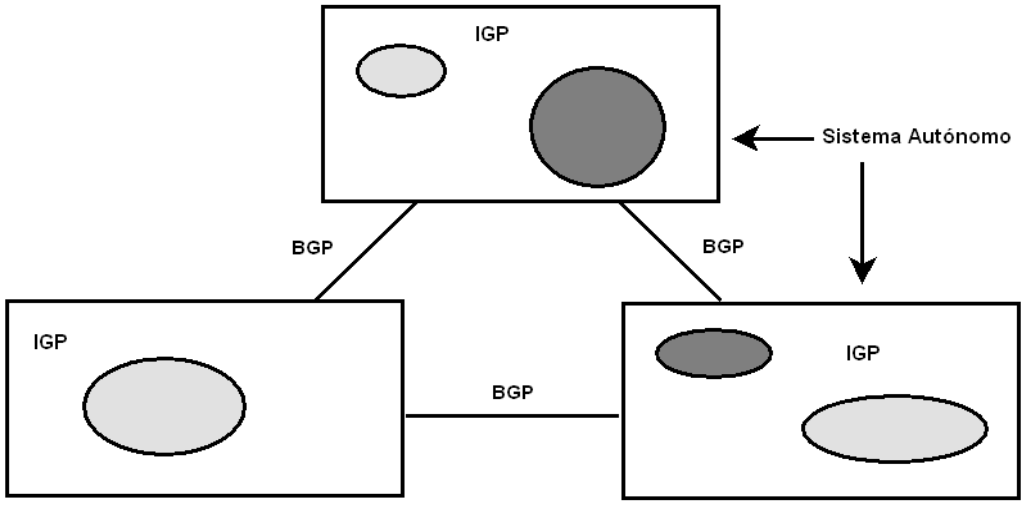

Figura 23: Representación de Sistemas Autónomos.

E. Métrica usada por BGP

Los protocolos de ruteo dinámicos incorporan métricas para hacer los cálculos de selección de la mejor ruta para poder hacer una mejor decisión de asignación de ruta, BGP no es excepción para esta regla, ya que se basa en diez criterios para el proceso de toma de decisión.

La métrica que BGP utiliza es la siguiente:

- Origen
- Ruta del AS
- El Próximo Salto
- Discriminador Multi-Salida
- Preferencia Local
- Agregación Atómica
- Agregación

- Comunidad
- ID de Origen
- Lista de Cluster

F. Multihoming

El concepto de multihomind se refiere al hecho de tener al menos dos caminos distintos para alcanzar un destino en Internet.

Teniendo conexiones para dos o más ISPs y ejecutando BGP de manera que todo el mundo coopere en la determinación del recorrido de interdominio. Está es la única manera de asegurar que una dirección de red sea alcanzable al mundo cuando la conexión a un ISP fracasa o cuándo el ISP mismo deja de operar.

La figura 24 ilustra un estado multihoming para IPv6, supongamos que dos IPS con números de sistema autónomo AS10 y AS20, le provee conexión al sistema autónomo AS65001, cada proveedor asigna un prefijo a AS65001, siendo respectivamente 2001:10:1::/48 y 2001:20:1::/48, ambos prefijos son anunciados al exterior por los router RA y RB para cada cliente dentro de AS65001, estos prefijos son usados para deducir la dirección IPv6 del proveedor para cada interfaz cliente. En este ejemplo AS65001 anuncia únicamente al prefijo 2001:10:1::/48 a AS10, el ISP ASP10 a su vez, anuncia la el prefijo 2001:10::/32 hacia Internet.

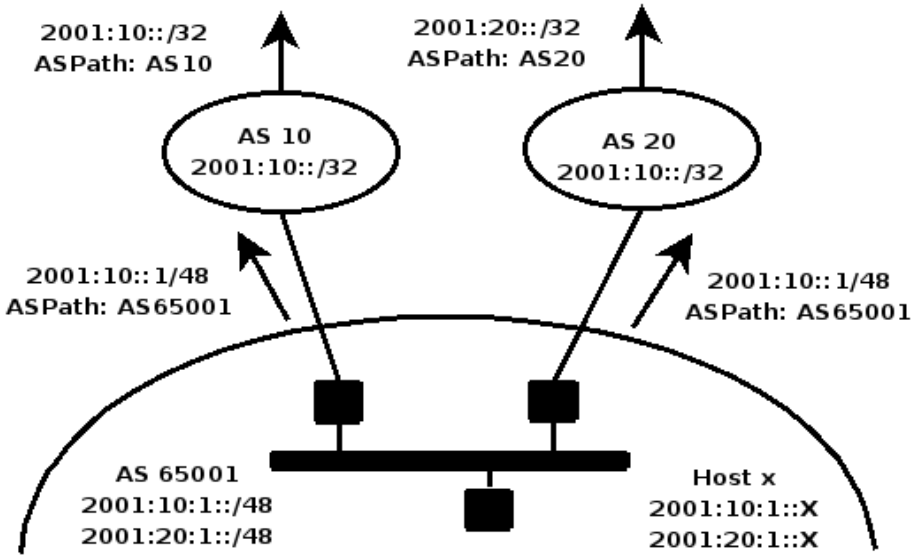

Figura 24: Ejemplo de Multihoming

2. MODO DE OPERACIÓN DE BPG

BGP usa TCP como protocolo de transporte sobre el puerto 179. Esto hace que la responsabilidad del transporte de los paquetes caiga sobre el protocolo TCP y por tanto no es necesaria implementarla en BGP, en consecuencia esto simplifica la complejidad del diseño del protocolo.

Como ya se mencionó, BGP es un protocolo de vector de rutas, usado para llevar información de ruteo entre Sistemas Autónomos, el término vector de rutas proviene de la información de ruteo, ya que acarrea una secuencia de números que identifica la ruta de los AS que el paquete ha atravesado. La información de la ruta en asociación con el prefijo se usan para descubrir la presencia de bucles, un bucle es causado por un conjunto de routers de los cuales uno de ellos cree que puede alcanzar un AS al cual ninguno de ellos está conectado, es decir, piensa que puede alcanzar un destino cuando en realidad esta fuera de su alcance.

Los routers que ejecutan un proceso BGP son llamados "BGP *speakers*" (routers que hablan BGP). Dos BGP speakers que realizan una conexión TCP entre ambos con el objetivo de intercambiar información de ruteo son llamados vecinos o *peers.* Cuando los vecinos BGP establecen una sesión TCP, comienzan a intercambiar información BGP en forma de mensajes. Cada mensaje comienza con un encabezado, seguido por el contenido del mensaje. La figura 25 muestra a dos vecinos BGP.

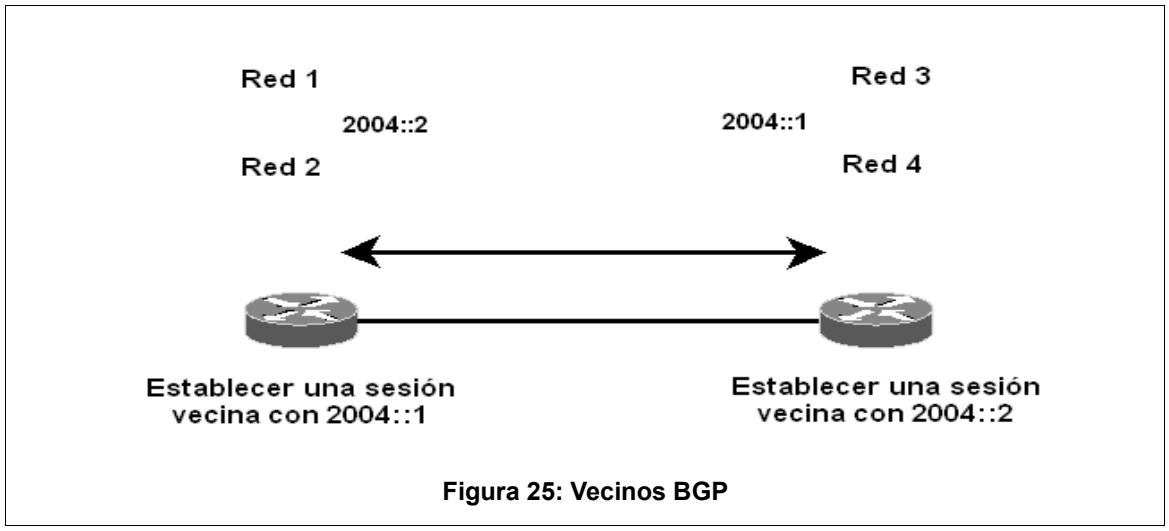

Figura 25: Vecinos BGP

Los routers vecinos intercambian "mensajes abiertos" (OPEN MESSAGES) para determinar los parámetros de conexión. Estos mensajes se usan para informar valores como el número de versión del protocolo BGP a cada router

BGP también provee un mecanismo para terminar con una conexión establecida con algún vecino. En otras palabras, en caso de un desacuerdo entre los vecinos, ya sea como resultado una configuración diferente, una incompatibilidad, o por intervención del administrador de redes o cualquier otra circunstancia, se envía un mensaje de notificación de error (NOTIFICACIÓN) y la conexión con ese vecino no es establecida o es cerrada en caso de haberse establecido.

El beneficio de utilizar este mecanismo es que ambos vecinos se dan cuenta que la conexión no pudo ser o seguir establecida, de esta manera no se desperdician recursos que serían necesarios para mantener o intentar reestablecer la conexión. El mecanismo

de cierre se asegura que todos los mensajes salientes, primordialmente mensajes de notificación de error sean enviado antes que se cierre la sesión TCP.

Inicialmente, cuando una sesión BGP es establecida entre BGP speakers, todas las rutas BGP son intercambiadas, después que la sesión ha sido establecida y el primer intercambio de información de ruteo ha ocurrido, sólo se envían actualizaciones parciales como los cambios ocurridos en la red . Las actualizaciones incrementales han aportado una enorme mejora en el uso del CPU y en el uso de ancho de banda comparado con los protocolos previos, como EGP[34].

Las rutas son anunciadas en mensajes de actualización (UPDATE MESSAGE). El mensaje de actualización contiene una lista con formato <longitud, prefijo>, que indican la lista de destinos que pueden ser alcanzados por medio de un BGP speaker. El mensaje de actualización también contiene los atributos de ruta, los cuales incluyen información del grado de preferencia para una ruta en particular y la lista de ASs que la ruta ha recorrido.

En caso que una ruta se vuelva inalcanzable para un BGP speaker, este informa a sus vecinos de dicha ruta inválida y es retirada, el anuncio de rutas inválidas se hace por medio de los mensajes de actualización, ver figura 26. Si la información asociada a una ruta cambia, o se selecciona un camino nuevo para un prefijo dado, es necesario que la ruta se retire, entonces es necesario que el router envíe una ruta de reemplazo.

[34] Haciendo referencia al protocolo de ruteo EGP.

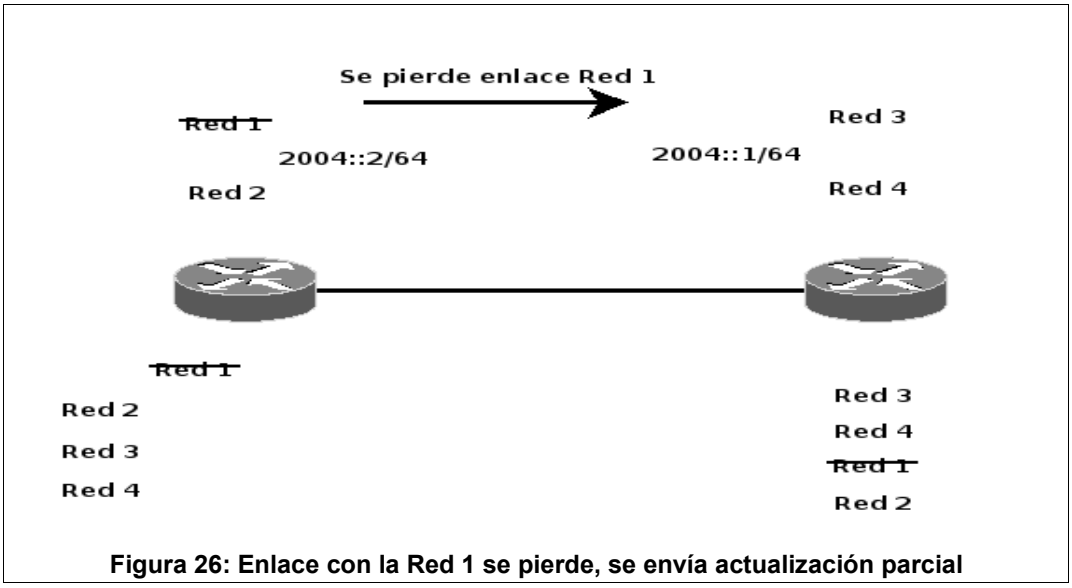

Figura 26: Enlace con la Red 1 se pierde, se envía actualización parcial

Si no ocurre algún cambio en las rutas, los routers intercambian sólo paquetes KEEPALIVE, esta situación se ve reflejada en la figura 27

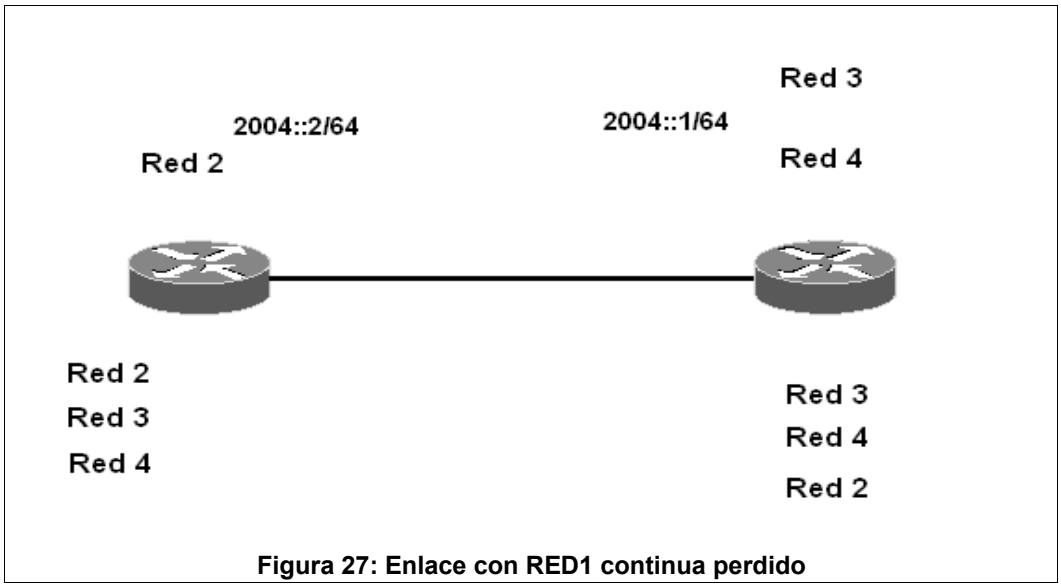

Figura 27: Enlace con RED1 continua perdido

Los mensajes KEEPALIVE son enviados periódicamente entre vecinos BGP para asegurar que la conexión siga establecida. Los paquetes KEEPALIVE no deberían producir ningún aumento en el ancho de banda de la red, porque consumen una cantidad mínima de ancho de banda.

BGP mantiene una tabla de números de versión la cual monitorea la instancia actual de la tabla de ruteo de BGP. Si dicha tabla cambia, BGP incrementa el número de versión de la tabla. Un incremento rápido de la tabla de versión generalmente es un indicador de inestabilidad en la red, cabe mencionar que ésta situación es común en redes de mayor escala, como las redes de algún proveedor de servicio de Internet, en este sentido las redes conectadas a Internet darán como resultado que el número de versión de la tabla sea incrementando en cada uno de los BGP speaker que tengan acceso a las tablas de ruteo de Internet.

3. FORMATO DE LOS MENSAJES BGP

A. Formato del Encabezado de Mensajes BGP

El formato del encabezado de mensaje BGP consta de un campo marcador (Marker) de 16 bytes, seguido por un campo Longitud (Length) de 2 bytes y un campo Tipo (Type) de 1 byte la figura 28 ilustra el formato de encabezado de mensaje de BGP.

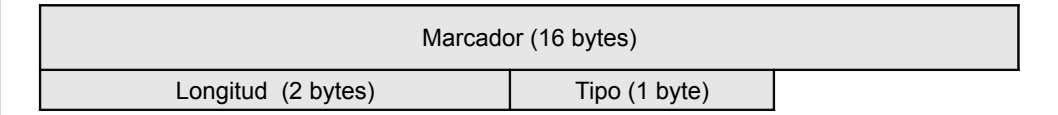

Figura 28: Formato del la cabecera de mensaje de BGP

Dependiendo del tipo de mensaje, puede o no adjuntarse datos después del encabezado, por ejemplo, los mensajes KEEPALIVE están compuestos únicamente por el encabezado de mensaje sin ningún dato después de el.

El campo Marcador (16 bytes), también se usa para autenticar mensajes entrantes de BGP o para detectar la pérdida de sincronización entre dos vecinos BGP. El campo

Marcador puede tener uno de los siguientes formatos:

- Si el tipo del mensaje es abierto (OPEN), o si el mensaje abierto no tiene información de autenticación, el campo Marcador debe ser rellenado con unos.
- Si el tipo del mensaje no es abierto, el campo del Marcador será procesado como parte del método de autenticación que se esta usado.

El campo Longitud (2 bytes) es utilizado para indicar la longitud total del mensaje BGP, incluyendo el encabezado. El mensaje más pequeño que puede enviar BGP es de 19 bytes (16 +2 +1) y los mensajes no pueden ser más grandes que 4,096 bytes.

El campo Tipo (1 byte), este campo indica el tipo de mensaje que se envía y este puede ser:

- Abierto (OPEN)
- Actualización (UPDATE)
- Notificación (NOTIFICATION)
- Mantener la sesión (KEEPALIVE)

B. Formato de Mensaje Abierto (OPEN)

La figura 29 ilustra el formato de un mensaje abierto

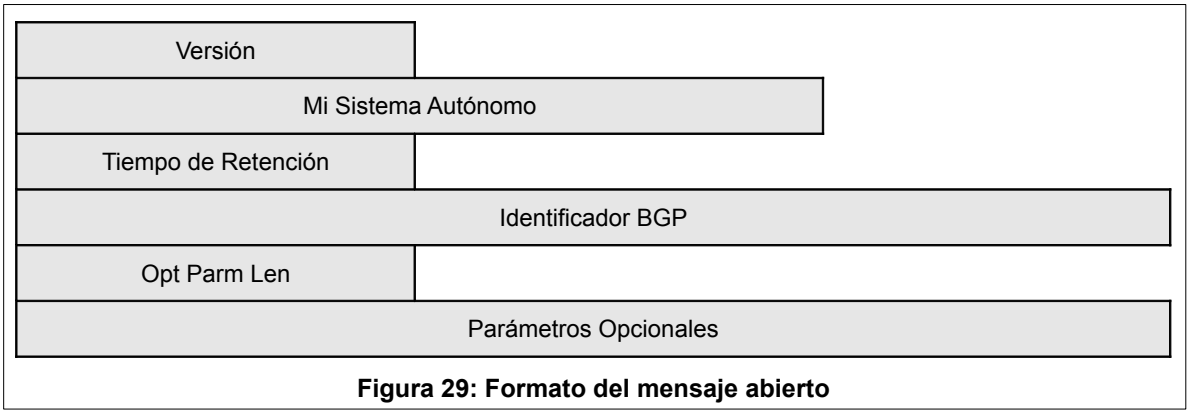

Figura 29: Formato del mensaje abierto

Las siguientes descripciones resumen cada uno de los campos del mensaje abierto:

- **Versión**

Indica la versión del protocolo BGP que se usará para las sesiones. La versión puede colocarse estáticamente cuando las versiones de los vecinos BGP son conocidas, la mayoría de implementaciones colocan por defecto la versión a BGP-4. Un entero sin signo del tamaño de 1 byte indica la versión del mensaje BGP, ya sea BGP-3 o BGP-4. Durante la negociación de vecinos, los vecinos se ponen de acuerdo sobre un número de versión de BGP. Los vecinos BGP intentan negociar la versión común más alta que ambos soportan. Los routers vuelven a establecer una sesión BGP y renegocian hasta que una versión que ambos puedan soportar sea determinada.

- **Mi Sistema Autónomo**

Un campo de 2 bytes que indica el número de AS del BGP speaker.

- **Temporizador de Retención (Hold Timer)**

El Temporizador de Retención es un entero sin signo de 2 bytes, el cual indica el tiempo máximo en segundos que puede transcurrir entre cada recepción sucesiva de mensajes KEEPALIVE o de mensajes de actualización. El Temporizador de Retención es un contador que incrementa de 0 hasta el valor de tiempo de retención. Recibir un mensaje KEEPALIVE o mensaje de actualización causa que el Temporizador de Retención vuelva a iniciarse a cero. Si el tiempo de retención para un vecino particular fuera excedido, el vecino sería considerado muerto, es decir, que ese destino se considera inalcanzable.

El router BGP hace negociaciones con su vecino para seleccionar el tiempo de retención. El Temporizador de Retención puede tener el valor de cero, en cuyo caso el Temporizador de retención y los temporizadores de los mensajes KEEPALIVE nunca se configuran. En otras palabras, estos temporizadores nunca caducan, y se considera que la conexión esta siempre activa.

Es de hacer notar que la negociación para establecer el Número de Versión y la negociación para el Temporizador de retención son muy diferentes una de la otra. En ambos casos, cada router sólo envía el mensaje abierto (OPEN).

- **Identificador BGP (BGP Identifier)**

Se trata de un entero sin signo de 4 bytes que indica el valor del identificador del router (RID)que envía el paquete BGP.

- **Longitud del Parámetro Opcional (Opt Parm Len)**

Es un entero sin signo de 1 byte, que indica la longitud total en bytes del campo Parámetros Opcionales.

- **Parámetros Opcionales**

Éste es un campo de longitud variable que hace referencia a una lista de parámetros opcionales que se utilizan al momento de la negociación de la sesión con los vecinos BGP. Este campo está representado por el valor de los parámetros de Tipo (1 byte), el Parámetro de Longitud (1 byte) y el Parámetro de longitud variable.

C. Mensaje de Notificación

Un mensaje de notificación siempre es enviado cada vez que un error es detectado. Después que el mensaje es enviado la conexión con el vecino es cerrada. Los administradores de red necesitan evaluar estos mensajes de notificación para determinar la naturaleza de los errores que aparecen en el protocolo de ruteo. La figura 30 muestra el formato de un mensaje de notificación.

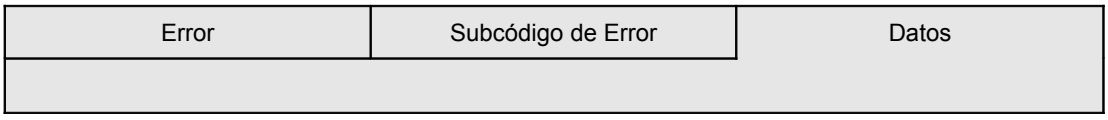

Figura 30: Formato de mensaje de notificación.

El mensaje de notificación está compuesto por los campos: Código de Error (1 byte), Subcódigo de Error (1 byte), y el campo de Datos (de longitud variable). El Código de Error indica el tipo de la notificación, y el Subcódigo de Error provee información

específica acerca de la naturaleza del error. El campo de Datos contiene información pertinente del error específico, por ejemplo un encabezado malo o un número de AS no válido.

D. Formato del Mensaje KEEPALIVE

Los mensajes KEEPALIVE son mensajes que se intercambian periódicamente entre vecinos para determinar si pueden ser alcanzados entre si. Como se dijo anteriormente, el valor del parámetro de tiempo de retención es la máxima cantidad de tiempo que puede transcurrir entre entradas de mensajes KEEPALIVE o de mensajes de actualización. Un valor recomendado para los mensajes KEEPALIVE es la tercera parte del valor de Tiempo de Retención.

El formato de un mensaje KEEPALIVE consiste únicamente en el encabezado del mensaje BGP.

E. Formato del Mensaje de actualización (UPDATE)

Un proceso importante en BGP es la actualización de la información de ruteo (routing update). El routing update le brinda al protocolo BGP la información necesaria para construir una fotografía, excluyendo las rutas con bucles de la red. El proceso de actualización de los routers es realizado gracias al envío de mensajes de actualización entre vecinos BGP.

Lo siguientes son los componentes básicos de un mensaje de actualización:

- Información de Accesibilidad de capa de red (NLRI)
- Los Atributos de la Ruta
- Rutas Inalcanzables

La figura 31 muestra el formato de un mensaje de actualización.

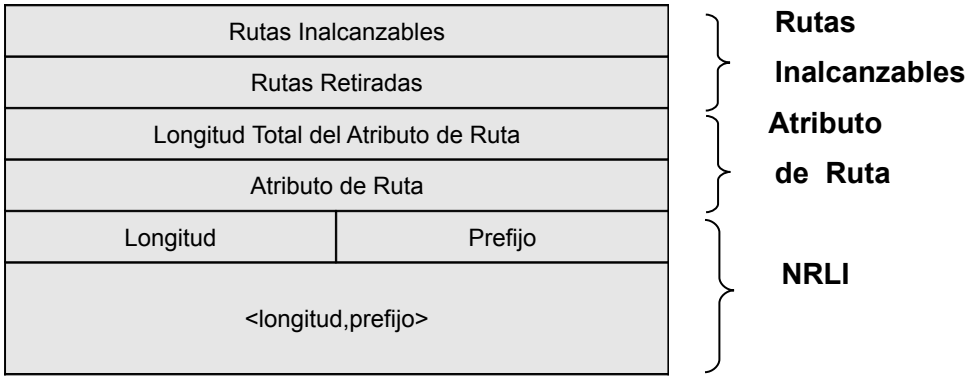

Figura 31: Formato de mensaje de actualización

El NLRI indica las redes que están siendo anunciadas. El Atributo de ruta le permite a BGP detectar rutas que contienen bucles y le da la flexibilidad para implementar políticas de ruteo locales y globales para la determinación del mejor camino. Un ejemplo de un Atributo de ruta BGP es el atributo AS_PATH, el cual consiste en una secuencia de números de AS que el paquete ha atravesado antes de alcanzar un router BGP, el mensaje de actualización también provee una lista de las rutas que se han vuelto inalcanzables. A continuación se describe cada uno de los campos del mensaje de actualización[35]:

- **Información de Accesibilidad de la capa de Red NLRI**

El NLRI es la parte del mensaje de ACTUALIZACIÓN BGP que lista el conjunto de destinos que BGP quiere informar a su otro vecino BGP. El NLRI consiste en uno o más instancias que contienen la tupla < longitud, prefijo >, donde la longitud es el número de bits del prefijo red.

- **Rutas Retiradas**

Las rutas retiradas proveen una actualización de rutas que no son alcanzables es decir que ya no se encuentran activas y tienen que ser retiradas de la tabla de ruteo de BGP. Las rutas retiradas también son representadas por la combinación < longitud, prefijo

[35] El Atributo de rutas se estudiará más adelante.

- **Rutas Inalcanzables (Unfeasible Routes)**

El campo de rutas Inalcanzables representa la longitud en bytes del total de rutas que serán descartadas de la tabla de ruteo. Un mensaje de ACTUALIZACIÓN puede listar ninguna o varias rutas para ser retiradas. Una longitud cero indica que ninguna ruta debe ser retirada.

4. ATRIBUTO DE RUTAS

Los atributos BGP son un conjunto de parámetros usados para dar a conocer información específica en la ruta, esta información puede ser el grado de preferencia de una ruta, el valor de NEXT_HOP de una ruta, y la información de agregación. Estos parámetros son usados para el filtrado de rutas y en el proceso de toma de decisión de camino. Cada mensaje de actualización tiene una secuencia de atributos de rutas de longitud variable .

A. Formato del Atributo de rutas

El campo de atributo de ruta se divide en: tipo de atributo de ruta (2 bits del atributo de banderas), atributo de banderas (1 byte) y código de tipo de atributo (1 byte). La figura 32 muestra un campo de atributo de ruta.

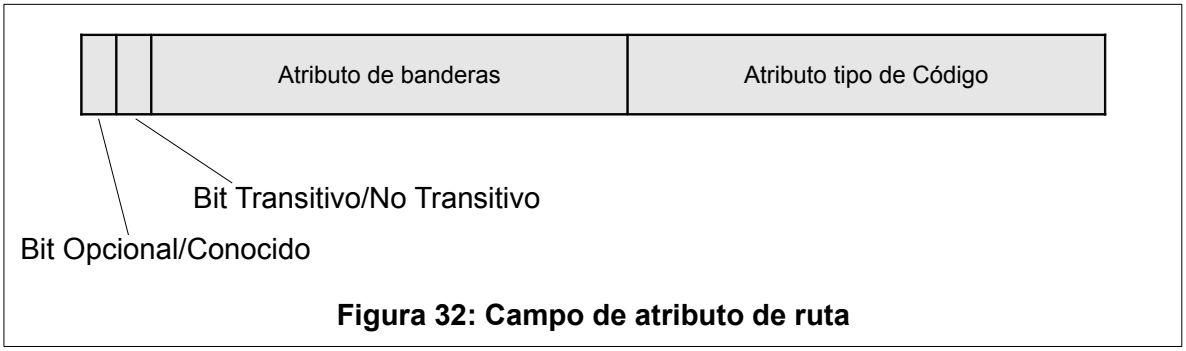

Figura 32: Campo de atributo de ruta

Los atributos de ruta se clasifican en cuatro categorías:

- Conocido obligatorio
- Conocido discrecional
- Opcional transitivo
- Opcional no transitivo.

Estas cuatro categorías están descritas por los primeros dos bits del campo atributo de Banderas:

a) El primer bit, el bit 0 del Atributo de Banderas, indica si el atributo es conocido (0) u opcional (1).
b) El segundo bit, el bit 1 del Atributo de Banderas, indica si el atributo opcional es no transitivo (0) o transitivo (1). Los atributos conocidos son siempre transitivos, así es que para ellos el segundo bit está siempre colocado a 1.
c) El tercer bit, el bit 2 del Atributo de Banderas, indica si la información en el atributo transitivo optativo es completa (0) o parcial (1).
d) El cuarto bit, el bit 3 del Atributo te Banderas, define si la longitud de atributo es 1 byte (0) o 2 bytes (1).
e) Bits de orden inferior, del bit 4 al bit 7 del Atributo de Banderas, en el campo del Atributo Bandera actualmente no se usa y siempre esta puesto a cero.

Las siguientes descripciones explican en detalle el significado de cada categoría de atributo:

- **Conocido Obligatorio:** Es un atributo que siempre tiene que estar presente en el mensaje de actualización de BGP. Es reconocido por todas las versiones de BGP. Si un atributo conocido contiene un error o falla, se generará un mensaje de notificación de error y la sesión es cerrada. Esto se hace para asegurar que todas las implementaciones BGP sigan el mismo conjunto estándar de atributos. Un ejemplo de un atributo obligatorio conocido es el atributo AS_PATH.

- **Conocido discrecional:** Es un atributo reconocido por todas las versiones de BGP, pero eso no necesariamente significa que es obligatorio enviarlo en el mensaje de actualización de BGP. Un ejemplo de un atributo discrecional conocido es LOCAL_PREF.

Además de los atributos conocidos, una ruta puede contener uno o más atributos opcionales. Los atributos opcionales no son soportados por todas las implementaciones de BGP. Los atributos opcionales pueden ser transitivos o no transitivos:

- **Opcional transitivo:** Si un atributo opcional no es reconocido por una versión. BGP, esta implementación busca dentro del atributo de banderas si dicho atributo esta definido. Si el atributo esta definido, es decir la bandera esta puesta, indica que el atributo es transitivo, la implementación BGP acepta el atributo y lo envía a los demás vecinos BGP.

- **Opcional no transitivo:** Cuando un atributo opcional no es reconocido y la bandera transitiva no está colocada, quiere decir que el atributo es no transitivo, el atributo debe ser ignorado y no se debe enviar a otros vecinos BGP.

Los atributos conocidos deben poder ser reconocidos por todas las implementaciones BGP. Algunos de estos atributos son obligatorios y deben ser incluidos en cada mensaje de actualización. Los atributos que son discrecionales pueden o no ser enviados en un mensaje actualización. Todos los atributos que sean del tipo conocido deben ser enviados a los vecinos BGP.

Además de los atributos conocidos, las rutas pueden tener asociados uno o más atributos opcional. No es requerido que estos atributos opcionales sean soportados por todas las implementaciones del protocolo BGP. El manejo de un atributo opcional no conocido es determinado por la asignación del bit transitivo (Transitive) en el octeto del atributo de banderas. Los caminos con atributos opcionales transitivos no conocidos deberían ser siempre aceptados por los BGP speakers.

Si una ruta con atributo opcional transitivo no conocido es aceptada y enviada a otros vecinos BGP, entonces el atributo optativo transitivo no conocido de la ruta también debe ser enviado en el mensaje hacia otro vecino BGP con el bit Parcial (Partitial) del octeto de Atributo de Banderas puesto a 1.

Si una ruta con atributo opcional transitivo conocido es aceptada y enviada a otro vecino BGP y el bit Parcial en el octeto del Atributo Bandera esta puesto a 1 por alguno AS previo, no será puesto a 0 por el AS actual. Los atributos optativos no transitivos no conocidos no deben ser ignorados y enviados a otros vecinos BGP.

Nuevos atributos opcionales transitivos pueden ser asociados a las ruta por el router que origina el mensaje o por algún otro AS en el camino. Si es adjuntado por el router que origina el mensaje, el bit Parcial en el octeto de Atributo de Banderas es puesto a 1.

Las reglas para adjuntar atributos opcionales no transitivos nuevos dependerán de la naturaleza del atributo que se desea especificar, se espera que en la documentación de cada atributo opcional no transitivo nuevo se incluyan tales reglas. Todos los atributos optativos, transitivos y no transitivos, pueden ser actualizados o modificados por cualquier AS en el camino.

Los atributos que actualmente definidos para BGP son mencionados en la siguiente lista.

- **ORIGEN (**tipo de código 1**):** Un atributo obligatorio conocido que define el origen de la información del camino. El octeto de datos puede asumir los siguientes valores:

    - **0: IGP,** La información de Accesibilidad de nivel de red que es interior al AS originario.
    - **1: EGP,** Información de Accesibilidad de nivel de red aprendido por medio de EGP.
    - **2: INCOMPLETO,** Información de Accesibilidad de nivel de red aprendido de alguna otra manera.

- **AS_PATH (**tipo de código 2**):** Un atributo obligatorio conocido que está compuesto de una secuencia de segmentos de rutas de AS. Cada segmento de la ruta está representado por el formato de tipo < camino, longitud del segmento de camino, valor del segmento del camino>.
- **NEXT_HOP (**tipo de código 3**):** Un atributo obligatorio conocido que define la dirección IP del router de borde que debería ser utilizado como el siguiente salto a los destinos de la lista del campo de Accesibilidad de la capa de Red del mensaje de ACTUALIZACIÓN.
- **MULTI_EXIT_DISC (**tipo de código 4**):** Un atributo no transitivo optativo, es un entero no negativo de cuatro octetos. El valor de este atributo puede ser usado por el proceso de decisión de BGP speaker para discriminar entre puntos múltiples de la salida para un Sistema Autónomo vecino.
- **LOCAL_PREF (**tipo de código 5**):** Un atributo discrecional conocido el cual es un entero no negativo de cuatro octetos. Es usado por un BGP speaker para especificarle a otro BGP speaker de su propio Sistema Autónomo el grado de preferencia del BGP speaker para una ruta anunciada.
- **ATOMIC_AGGREGATE (**tipo de código 6**):** Es un atributo discrecional conocido cuya longitud es cero. Es usado por un BGP speaker para informar a otro BGP speaker que el sistema local seleccionó una ruta menos específica sin seleccionar una ruta más específica que la incluida en ella.
- **AGREGADOR (**tipo de código 7**):** Un atributo transitivo optativo de longitud 6. El atributo contiene el último número de AS que ha sido agregado a la ruta (codificado como dos octetos), seguida por la dirección IP del BGP speaker que forma la ruta del número de AS agregado (codificado como cuatro octetos).
- **COMMUNITY (**tipo de código 8**):** Un atributo transitivo optativo de longitud variable. El atributo consiste en un conjunto de cuatro valores del octeto, cada uno del cual específica una comunidad. Todas las rutas con este atributo pertenecen a las comunidades mencionadas en la lista el atributo.

B. Atributo AS_PATH

El atributo AS_PATH es un atributo obligatorio conocido (tipo de código 2) que contiene una secuencia de números de sistema autónomos que representan el camino que la ruta ha atravesado.

Para el intercambio de información de ruteo entre dos vecinos internos (IBGP) , la información del atributo AS_PATH se deja intacta, sin embargo, cuando las rutas se envían hacia un vecino BGP externo (EBGP) , El AS que origina la ruta agrega su número de AS. Después, cada AS que recibe la ruta y lo pasa a otros vecinos EBGP agregará al principio del la lista su número AS (*Prepending*). La lista final representa todos los AS que una ruta ha atravesado.

El número del AS que originó el mensaje está al final de la lista. Esta lista del atributo AS_PATH hace referencia *a un AS_SEQU*ENCE, ya todos los AS están numerados de forma secuencial.

C. Atributo MULTI_EXIT_DISC (MED)

El atributo BGP Multi_Exit_Discriminator es un atributo no transitivo opcional (Tipo de código 4). Indica a los vecinos externos sobre el camino preferido que un AS con diversos puntos de entrada. El MED también es conocido como la métrica externa de una ruta. Un valor menor del MED es preferido por sobre un valor mayor.

A diferencia del atributo LOCAL_PREF, el atributo MED es intercambiado entre AS, pero un atributo MED que es recibido por un AS no sale por completo de dicho AS, es guardado para usarlo en el proceso de decisión. Cuando una actualización entra en el AS con un cierto valor MED, ese valor sirve para tomar decisiones dentro del AS. Cuando BGP envía actualizaciones de rutas a otro AS, el MED es puesto a cero, a menos que el MED de salida se le coloque explícitamente un valor específico.

D. Atributo LOCAL_PREF

El atributo de preferencia local (LOCAL_PREF) es un atributo discrecional conocido (tipo de código 5). Específica un grado de preferencia que se da a una ruta cuando es comparada con otras rutas del mismo destino. Un valor de preferencia local más alto señala que la ruta es más preferida. EL campo preferencia local, como lo indica su nombre, se usa en el Sistema Autónomo local y es intercambiado entre vecinos IBGP.

La preferencia local se usa para colocar un punto común de salida en un AS para alcanzar cierto destino ya que este atributo es comunicado a todos los routers BGP dentro del AS, así todos los routers BGP tendrán en común la misma ruta de salida del AS.

E. Atributo COMMUNITY

En el contexto de BGP, *una comunidad* es un grupo de destinos que comparten una propiedad en común. Una comunidad no está restringida a una red o un Sistema Autónomo, una comunidad no tiene límites físicos. Un ejemplo una comunidad es un grupo de redes que le pertenecen a las entidades educativas o de un gobierno.

Las comunidades se usan para simplificar las políticas de ruteo identificando las rutas basándose en una propiedad lógica en vez de hacerlo con un prefijo de red o un número de AS. Un router BGP puede usar este atributo en conjunto con otros atributos para controlar cuáles rutas aceptará, cuales rutas preferirá, y cuales enviará a otros vecinos BGP.

El atributo COMMUNITY es un atributo transitivo opcional. Es de longitud variable y consiste en un conjunto de 4 bytes. Los valores para las comunidades comprendidos entre 0x00000000 y 0x0000FFFF y las comprendidas entre 0xFFFFFFFF y 0xFFFF0000

están reservadas, estos valores de comunidad tienen un significado global. Aquí hay algunos ejemplos de comunidades conocidas:

- **NO_EXPORT (0xFFFFFF01):** Una ruta que lleva este valor de comunidad no debe ser anunciada a los demás vecinos fuera del AS.
- **NO_ADVERTISE (0xFFFFFF02):** Una ruta que lleva este valor de comunidad no debe ser anunciado por ningún vecino.

Además de los atributos de comunidades conocidos, los atributos de comunidades privados pueden estar definidos para usos especiales. Así esta definido en el RFC 1998, el cual describe un mecanismo mediante el cual las comunidades pueden usarse para manipular el proceso de selección de la ruta BGP en redes del proveedor de servicios.

Es común usar los primeros 2 bytes del atributo COMMUNITY para el número de AS y los últimos 2 bytes para definir una relación con el AS. Por ejemplo, un proveedor con un número de sistema autónomo asignado de AS128, quiere definir a una comunidad privada llamada “Mi-Comunidad”, los routers pueden representar esa comunidad de la siguiente manera: 128:1, estando representada en sistema decimal. El valor de 128 señala que el proveedor tiene definida la comunidad y el valor 1 tiene sentido especial para el proveedor, es Mi-Comunidad.

Una ruta puede tener más que un atributo comunidad. Un vecino BPG que mira múltiples atributos de comunidad, puede tomar decisiones a uno o más atributos. Un router tiene la opción de agregar o modificar atributos comunidad antes de anunciar las rutas a otros vecinos internos o externos.

Un ejemplo sencillo del atributo de comunidad es el siguiente: La Red-X envía paquetes a la Red-Y, las rutas X y Y tienen configurado el atributo de comunidad con NO_EXPORT y la ruta Z tiene el atributo de comunidad sin modificación, el router en la Red-Y únicamente propagará la ruta Z a la Red-Z, las rutas X y Y no serán propagadas ya que tienen el atributo de comunidad con NO_EXPORT, La figura 33 muestra gráficamente este ejemplo.

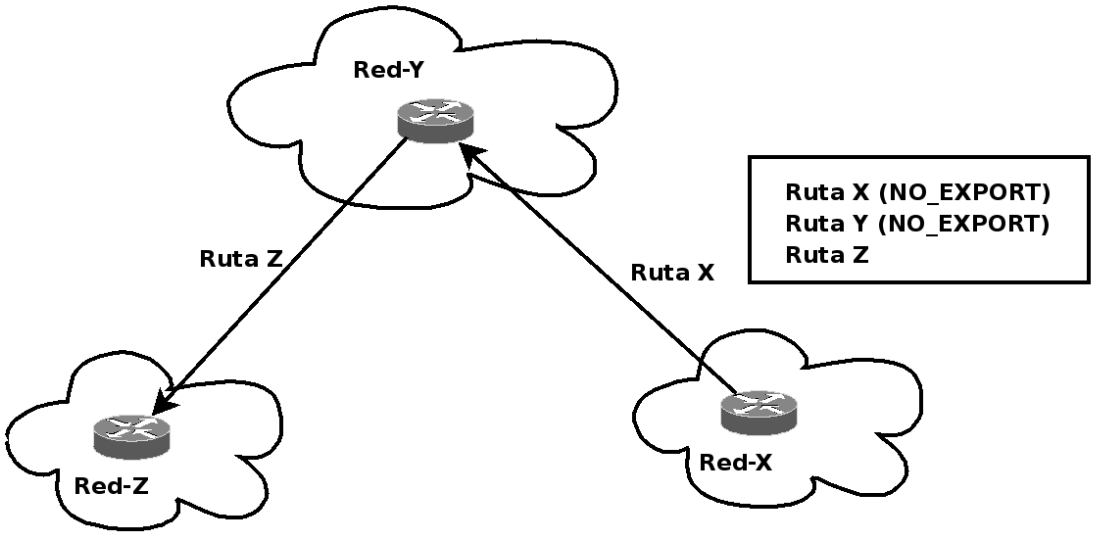

Figura 33: Ejemplo del atributo Comunidad

5. NEGOCIACIÓN DE VECINOS BGP

Uno de los pasos básicos del protocolo BGP es el establecer sesiones entre vecinos BGP. Si no se tiene éxito en el establecimiento de una sesión, el intercambio de actualizaciones no ocurrirá. La negociación de vecinos se basa en el establecimiento de una conexión de transporte TCP, el procesamiento exitoso del mensaje ABIERTO, y la detección periódica de mensajes de ACTUALIZACIÓN o de mensajes KEEPALIVE.

A. Máquina de Estados Finitos (FSM)

La negociación de vecinos BGP atraviesa diferentes etapas antes de que la conexión sea establecida, en la figura 34 se ilustra un FSM resaltando los acontecimientos principales durante el proceso, indicando los tipos de mensajes (OPEN, KEEPALIVE, NOTIFICATION) enviados al vecino en la transición de un estado al otro.

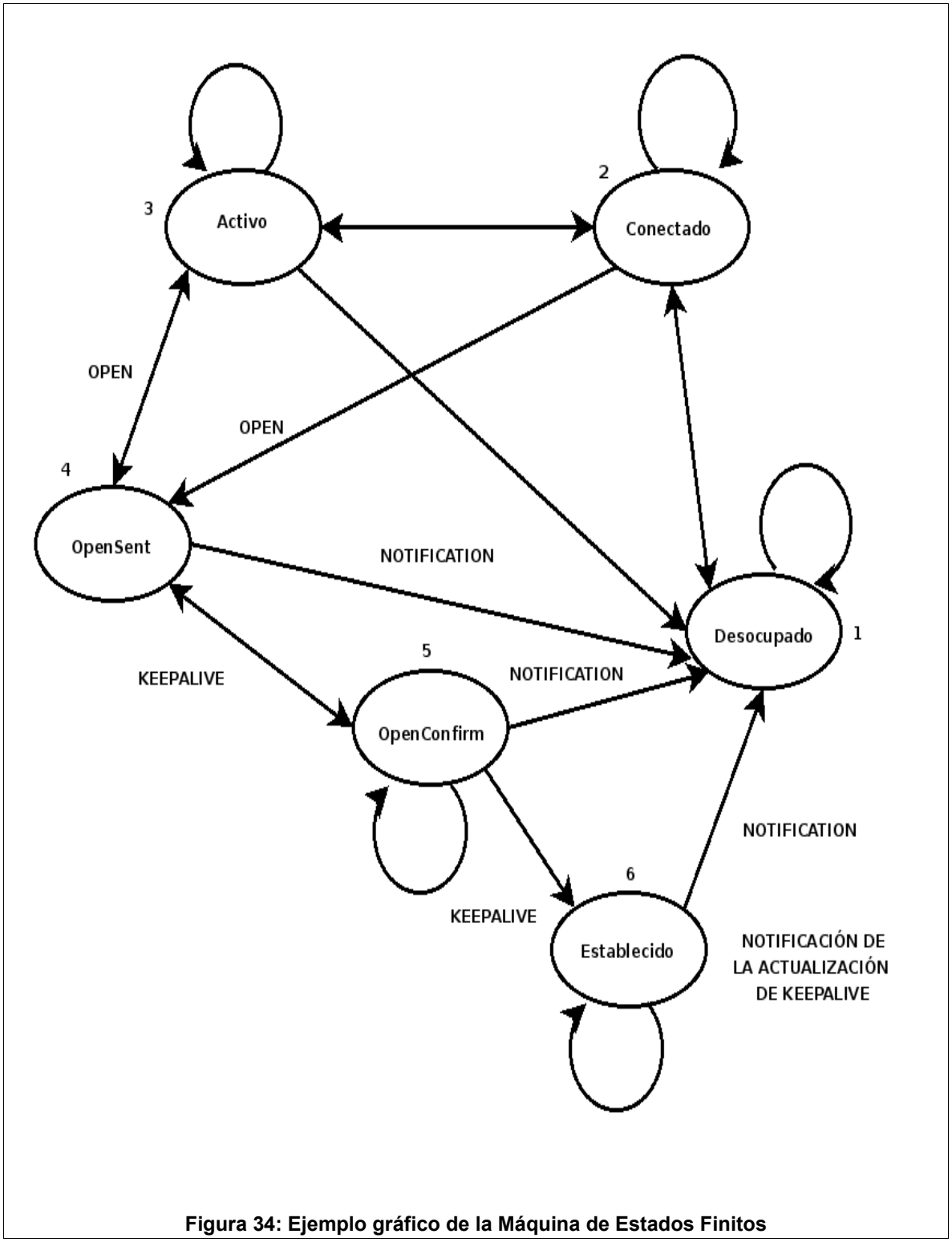

Figura 34: Ejemplo gráfico de la Máquina de Estados Finitos

A continuación se presenta una descripción de los estados de FSM:

1. Desocupado (idle)

Esta es la primera fase de la conexión, BGP está esperando un proceso de Inicio, el cual es iniciado por el administrador de red o por el mismo sistema BGP. Un administrador establece una sesión BGP a través de la configuración del router o reiniciando una sesión existente. Después del proceso de Inicio, BGP inicializa sus recursos, arranca el temporizador ConnectRetry, inicia una conexión de transporte TCP, y comienza a escuchar la conexión que se inició con el vecino. Es entonces cuando BGP entra al estado conectado. En caso de haber errores, BGP continúa en el estado Desocupado.

2. Conectado (connect) BGP está a la espera que la conexión TCP se complete. Si la conexión de transporte TCP tiene éxito, el estado cambia a OpenSent (un mensaje ABIERTO es enviado). Si la conexión de transporte no tiene éxito, el estado cambia a Activo. Si el temporizador ConnectRetry expira, el estado regresa a Conectado, el temporizador arranca nuevamente y una nueva conexión de transporte es iniciada. En caso de darse algún otro acontecimiento iniciado por el sistema o por el administrador, el estado regresa a desocupado.

3. Activo (Active)

BGP intenta hacer una conexión de protocolo de transporte con un vecino. Si la conexión de transporte es establecida, efectúa una transición al estado OpenSent. Si el temporizador ConnectRetry expira, el estado regresa a Conectado y temporizador ConnectRetry es reiniciado. El estado puede regresar a Desocupado si ocurren eventos iniciados por el administrador como el proceso de parada de la sesión. En general, un vecino que cambia de estado entre Conectado y Activo indica que algo anda mal con la conexión de transporte TCP.

4. OpenSent

BGP está esperando recibir un mensaje abierto de su vecino. El mensaje abierto es revisado en busca de errores. En caso de encontrar errores, como un número de versión malo o uno número de AS inaceptable, el sistema envía un mensaje de notificación de

error y vuelve al estado Desocupado. Si no se encuentran errores, BGP comienza a enviar mensajes KEEPALIVE e inicia el temporizador KEEPALIVE. En este punto, el tiempo de retención ya está negociado entre los vecinos. En caso que el tiempo de retención negociado se establezca a cero, el Temporizador de Retención y el temporizador KEEPALIVE no son vueltos a iniciar.

Para otros errores, como el de vencimiento del Temporizador de Retención, BGP envía un mensaje de notificación con el código correspondiente del error y regresa al estado Desocupado. Cuando una conexión de transporte TCP es eliminada, el estado vuelve al estado Activo.

5. OpenConfirm

BGP está a la espera de recibir un mensaje KEEPALIVE. Si un mensaje KEEPALIVE es recibido, el estado cambia a Establecido y la negociación del vecino se completa.

Cuando se recibe un mensaje KEEPALIVE, se inicia a cero el Temporizador de retención, suponiendo que el Tiempo de Retención negociado para la sesión no es cero.

Si un mensaje de notificación es recibido, el estado regresa a Desocupado. El sistema envía mensajes KEEPALIVE esperando el tiempo establecido por el temporizador KEEPALIVE. En caso de un mensaje de notificación de desconexión o en respuesta a cualquier proceso de parada iniciado por el sistema o el administrador, el estado regresa al estado Desocupado.

6. Establecido (Established)

Esta es la fase final en la negociación de vecinos. A estas alturas, BGP comienza a intercambiar paquetes de actualización (UPDATE) con sus vecinos. Suponiendo que el Temporizador de Retención no es cero, este vuelve a iniciarse cada vez que se recibe un mensaje de actualización o un mensaje KEEPALIVE. En respuesta cualquier otro evento, el sistema envía un mensaje de notificación con un código de error FSM y regresa al estado Desocupado.

B. BGP Interno y Externo (IBGP y EBGP)

Generalmente BGP es utilizado para proveer una topología de ruteo interdominio sin bucles , BGP también es usado al interior de un Sistema Autónomo (AS) para proveer a los routers internos la información externa sobre accesibilidad de algún destino. Una *conexión de vecino entre d*os routers*,* llamada también con*exión peer,* puede ser establecida dentro del mismo sistema autónomo, en cuyo caso BGP es llamado BGP Interno (IBGP). Asimismo, una conexión de vecino entre routers con AS diferente es llamado BGP Externo (EBGP). La figura 35 muestra de forma gráfica estas dos conexiones que se pueden llevar a cabo entre vecinos BGP.

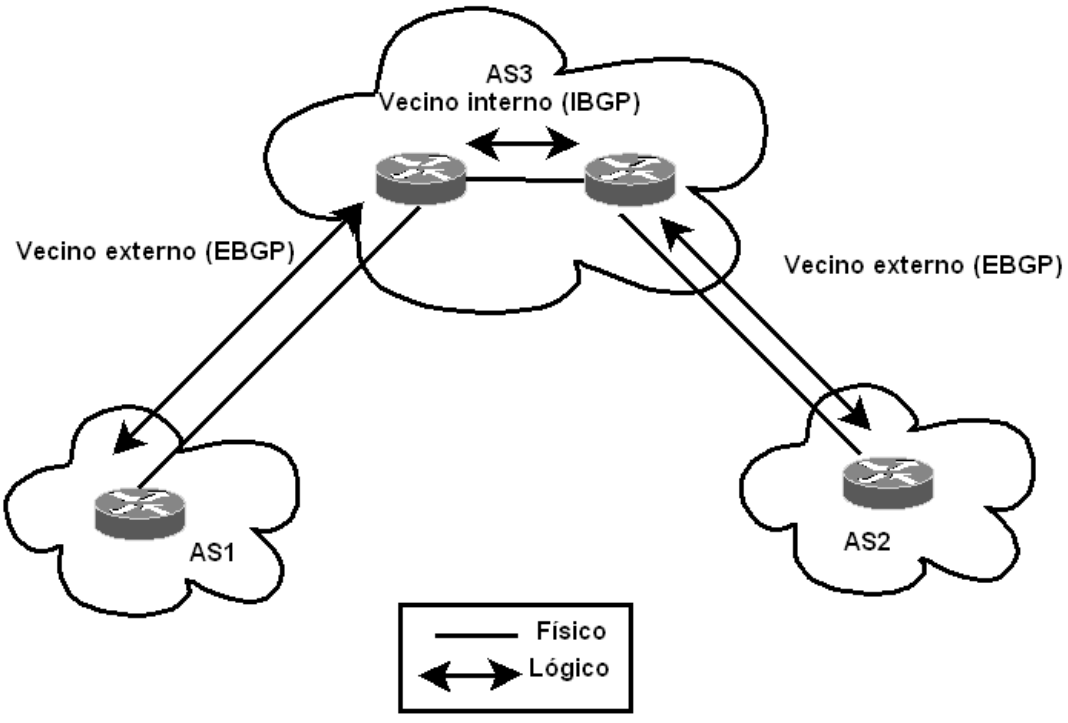

Figura 35: Vecinos BGP Internos y Externos

En el momento de establecimiento de la sesión de vecino y durante la negociación e intercambio de mensajes abiertos, los routers comparán números de AS y determinan si son vecinos dentro del mismo AS o si son vecinos de diferente AS.

La diferencia entre EBGP e IBGP radica en la manera en que cada vecino procesa las actualizaciones de rutas originadas por otro vecino y en la forma en que los diferentes atributos BGP son procesados tanto en conexiones externas como en conexiones internas.

El proceso de negociación del vecino es primordialmente lo mismo para vecinos internos y externos: establecer una conexión TCP en el nivel de transporte. Es imprescindible tener una conexión TCP entre los dos vecinos para que una sesión pueda ser establecida.

C. Negociación de Capacidades BGP

El propósito de este concepto es el de introducir nuevos parámetros opcionales a BGP añadiendo así nuevas capacidades. Con esto se espera facilitar la introducción de nuevas características BGP proveyendo esta capacidad de negociación.

Si un BGP speaker soporta negociación de capacidades, cuando envía un mensaje abierto a un BGP vecino, el mensaje puede incluir un parámetro opcional de capacidades. El vecino BGP examina la información contenida en el atributo de capacidades de un mensaje abierto para decidir cuáles capacidades soporta el vecino que envió el mensaje. Si un vecino BGP determina que un vecino soporta una capacidad dada, ambos vecinos pueden hacer uso de dicha capacidad.

Si un vecino BGP desea determinar si otro vecino soporta una nueva capacidad entonces envía un mensaje abierto que lleva consigo el nuevo parámetro opcional a este vecino, si dicho vecino no soporta la capacidad entonces genera un mensaje de notificación de error y lo envía como respuesta, el mensaje de notificación de error contiene un subcódigo de Error (ErrorSubcode) , si esto llegará a ocurrir el vecino BGP debería tratar de restablecer la conexión sin enviar el parámetro de capacidades opcionales que generó el mensaje de error al otro vecino.

Las Capacidades BGP son atributos de tipo 24 y tienen el formato: < código de Capacidad, Longitud de Capacidad, Valor de Capacidad >, la figura 36 ilustra el formato de las capacidades de BGP:

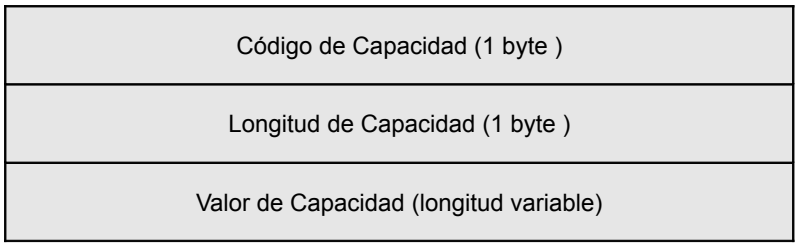

Figura 36: Formato de Capacidades de BGP

6. PROCESAMIENTO DE RUTAS

A. Proceso de Ruteo de BGP

Las rutas son intercambiadas entre vecinos BGP por medio de mensajes de actualización. Cuando los routers BGP reciben estos mensajes, ejecutan algunas políticas o filtros sobre las actualizaciones de rutas, y entonces le pasan las rutas a otros vecinos BGP. Un proceso BGP es requerido para guardar todas las actualizaciones recibidas en una tabla de rutas. En el caso que existan múltiples rutas para el mismo destino, BGP no inunda a sus vecinos con todas esas rutas; más bien, escoge la mejor ruta y la envía. Un router BGP puede originar actualizaciones de ruteo para anunciar redes internas que pertenecen a su Sistema Autónomo. Las rutas locales originadas en el sistema y las mejores rutas aprendidas de vecinos BGP son entonces almacenadas en la tabla de ruteo. La tabla de rutas es consultada para la tomar la decisión de ruteo y es usada para llenar la tabla de reenvío.

Para ejemplificar el proceso BGP, supongamos que cada BGP speaker tiene diferentes piscinas de rutas a las que se les aplicaron diferentes políticas, entonces se requiere:

- Una piscina de rutas que el router recibe de sus vecinos.
- Una política de entrada de rutas, que puede filtrar las rutas o puede manipular sus atributos.
- Un proceso de decisión, el cual decide qué caminos usará para encaminar
- Una piscina de rutas utilizada por el propio router.
- Una política de salida de rutas, que puede filtrar las rutas o puede manipular sus atributos.
- Una piscina de rutas que el router anuncia para otros vecinos.

B. Anuncio y Almacenamiento de rutas

Para BGP una ruta se define como una unidad de información que almacena y asocia un destino con sus respectivos atributos de ruta en pares ordenados. Las rutas son anunciadas entre BGP speaker en mensajes de actualización: el destino es el sistema cuyas direcciones IP se encuentran en el campo de Información de Accesibilidad de Capa de Red (NLRI), y la ruta es la información almacenada en el campo de Atributos de Ruta del mismo mensaje de actualización.

Las rutas se guardan en las Bases de Información de Ruteo (RIBs): el Adj-Rib-In, el Loc-RIB, y el Adj-Rib-Out. Las rutas que serán anunciadas a otros vecinos BGP deben estar presentes en el Adj-Rib-Out; las rutas que serán usadas por el BGPspeaker local debe estar almacenadas en el Loc-RIB, el próximo salto para estas rutas deben estar almacenados dentro de la Base de Información de reenvío (FIB) del BGPspeaker local; y las rutas que se reciben de otros BGP speakers se guardan en el Adj-Rib-In. Si un BGP speaker decide anunciar una ruta, puede agregar o puede modificar los atributos del camino de la ruta antes de anunciarlo al vecino.

C. Base de información de Ruteo (RIB)

Como se muestra en la figura 37, la tabla de ruteo de BGP consiste en tres partes distintas: Adj-RIB-In , Loc-RIB, y Adj-RIB-Out.

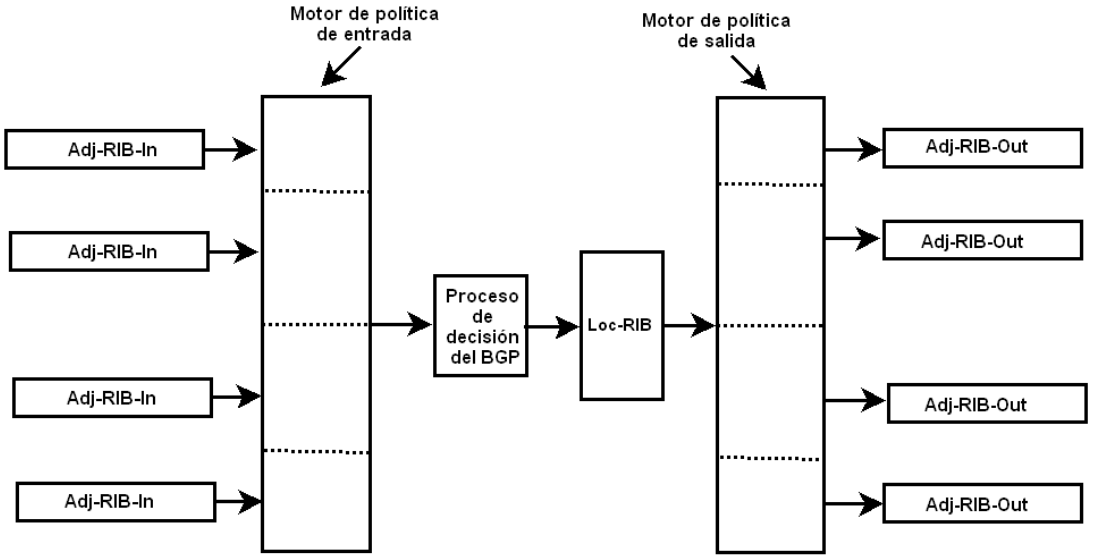

Figura 37: Representación lógica de la tabla de ruteo de BGP

Un Adj-RIB-In está asociado lógicamente a cada vecino individual de un BGP speaker. Adj-RIB-In almacena información de ruteo que ha sido aprendida a través de sus vecinos por medio de la entrada de mensajes de actualización. El contenido de todo el Adj-Rib-In está disponible como insumo para el proceso de decisión BGP, después pasa a ser manipulado o filtrado por el Motor de Política de Entrada asociado al vecino.

El Loc-RIB contiene las rutas que han sido seleccionadas como el mejor camino para cada destino disponible. Después que han sido aplicados los filtros de la Política de entrada se pasa a aplicar el proceso de selección, como resultado del proceso de selección se obtiene en Loc-RIB.

El Adj-RIB-Out esta asociado a cada vecino individual de un BGP speaker. Almacena información de ruteo que el BGP speaker ha seleccionado para ser anunciado a los

vecinos. El Adj-RIB-OUT contiene información del Loc-RIB que será anunciada a los vecinos después de ser aplicada la Política de Salida . Aunque este modelo conceptual distingue entre Adj-Rib-In, Loc-RIB, y Adj-RIB-Out, no es requisito que se almacenen tres copias separadas de la información de ruteo, la mayoría de implementaciones actuales almacenan una copia de la información con punteros para conservar memoria.

- **Las Rutas Recibidas de los Vecinos**

Un BGP speaker recibe rutas, y sus atributos asociados, de vecinos del exterior e internos por medio mensajes de actualización. De acuerdo a la configuración de la Política de entrada de rutas, algunas o todas esas rutas se almacenaran en el Loc-RIB.

- **Motor de Política de Entrada**

El Motor de Política de Entrada maneja el filtrando de rutas y la manipulación de atributos. El filtrado se hace basado en diferentes parámetros como prefijos de red, AS_PATH, y otros valores de atributos de BGP.

BGP también usa el Motor de Política de Entrada para manipular los atributos de la ruta y de esa manera influenciar en el proceso de decisión, por lo tanto afecta las rutas que se usarán para alcanzar un destino dado. Por ejemplo, si BGP elige filtrar un cierto prefijo de un vecino, esto indica que BGP no quiere alcanzar dicho destino por medio de ese camino, o si BGP le da a un cierto prefijo un valor mayor de LOCAL_PREFr, esto quiere decir que BGP prefiere el prefijo de un vecino específico al de otros vecinos. El Motor de Política de Entrada le aplica políticas a los paquetes entrantes que han sido definidos por el administrador de la red.

- **Rutas Usadas por el Router**

Las mejores rutas, que se han identificado por el proceso de decisión, son colocadas en el Loc-RIB. Estas rutas se convierten en rutas candidatas a ser anunciados a otros vecinos o guardadas en la tabla de rutas. Si una ruta no está colocada en el Loc-RIB, no puede ser guardada en el Adj-RIB-OUT ni anunciarse a otros vecinos. Además de las rutas recibidas de los vecinos, el router también puede generar actualizaciones sobre los cambios dentro de su Sistema Autónomo.

- **El Motor de Política de Salida**

Es semejante al Motor de Política de Entrada, pero aplicado en sentido contrario: el lado de salida. Las rutas usadas por el router junto a las rutas que el router genera localmente, son pasadas a este motor para que sean procesadas. El Motor de Política de Salida puede aplicar filtros y puede cambiar los valores de los atributos BGP antes de enviar una actualización, por ejemplo puede modificar el atributo AS_PATH antes de ser enviado. El Motor de Política de Salida hace diferencia entre vecinos internos y externos; por ejemplo las rutas aprendidas de un vecino interno no deben ser pasadas a otro vecino interno.

- **Rutas anunciadas a los Vecinos**

El conjunto de rutas anunciadas a los vecinos, consiste en rutas que atraviesan exitosamente los filtros del Motor de Política de Salida y son anunciadas a los vecinos BGP ya sean estos internos o externos.

D. Políticas de control de rutas con BGP

El tráfico que entra y sale de un AS siempre fluye de acuerdo al mapa de rutas diseñado por las rutas. Alterar las rutas se traduce en cambios en el comportamiento de tráfico. BGP provee los procesos y atributos de ruta necesarios para ocuparse del flujo de dicho tráfico.

- **Filtro de Rutas**

El concepto de filtrar rutas es franco. Un BGP speaker puede escoger a quien envía y que rutas recibe de cualquier vecino BGP. El filtrado de rutas es esencial para definir las políticas de ruteo. Un Sistema Autónomo puede identificar el tráfico de entrada que podría aceptar de otros vecinos especificando la lista de rutas anunciadas para sus vecinos. De manera inversa un AS puede controlar qué rutas de salida anuncia especificando las rutas que aceptan de sus vecinos.

El filtrado también es usado para limitar las actualizaciones de rutas que se intercambian de protocolo a otro. El filtrado de rutas es esencial ya que específica que información va a

enviar dentro del IGP y que información saldrá de este.

Las rutas permitidas a través de un filtro pueden tener manipulados sus atributos. Entonces al manipular los atributos afecta el proceso de decisión de la mejor ruta de BGP.

- **Filtro de Entrada y de Salida**

Ambos conceptos, el filtrado de entrada y salida pueden ser aplicados a los vecinos y niveles de protocolo. Desde la perspectiva del intercambio de rutas entre vecinos BGP, el filtrado de entrada indica que el BGP speaker filtra las actualizaciones de rutas recibidas de otros vecinos, considerando filtros de salida para las actualizaciones de rutas enviadas a otros vecinos. El comportamiento de filtrado es el mismo si los vecinos BGP son externos (EBGP) o internos (IBGP).

A nivel de protocolo, el filtrado de entrada limita las actualizaciones de rutas que son inyectadas desde la red dentro del protocolo. El filtrado de salida limita las actualizaciones de rutas que están siendo inyectadas desde el protocolo hacia la red. Con relación a BGP, por ejemplo, el filtrado de entrada limita las actualizaciones distribuidas por otros protocolos como el protocolo de compuerta interior y las rutas estáticas en BGP. El filtrado de salida limita las actualizaciones que son distribuidas por BGP al protocolo de compuerta interior.

E. Proceso de filtrado

Filtrar y manipular una ruta o un conjunto de rutas implica tres acciones: primero, identificar las rutas; segundo, permitir o denegar rutas; tercero, manipular los atributos.

- **Identificando Rutas**

La identificación de rutas es el proceso de establecer criterios para identificar una ruta a otra. Tales criterios podrían basarse en el prefijo IP de la ruta, el Sistema Autónomo del cual la ruta fue originada, una lista de ASs por la que la ruta ha pasado, un valor específico de atributo dentro de la ruta, entre otros.

Una lista de instancias de criterios contiene las reglas de filtrado, y la ruta es comparada con la primera instancia en la lista. Si la ruta no corresponde a la primera instancia, es chequeada con la siguiente instancia en la lista. Después de que una ruta es identificada ya no será comparada con otras instancias. Si la ruta es comparada contra la lista entera y no corresponde a ninguna instancia, la ruta es descartada.

Identificar Rutas Basado en AS_PATH

Identificar rutas basándose en la información AS_PATH es más complicado que usar NLRI. El AS_PATH es una lista de números de AS que la ruta ha atravesado antes de alcanzar un vecino BGP.

La lista en si es una cadena de caracteres que puede contener una combinación de:

• Números del 0 al 9
• Espacios
• Corchete izquierdo {
• Corchete derecho }
• Paréntesis izquierdo (
• Paréntesis derecho)
• Comienzo de la cadena de entrada
• Fin de la cadena de entrada
• Coma ,

Los caracteres ^ y $ son representaciones del comienzo y el fin de la cadena respectivamente. Una expresión normal es un patrón de caracteres representados por una fórmula como ^200 100$.

Expresiones de Carácter

Las Expresiones de carácter son combinaciones de letras, números, cualquier carácter del teclado, y cualquier carácter de sentidos especiales. Las expresiones de carácter pueden ser:

- **Expresiones Simples de carácter:** Una expresión simple de carácter corresponde a un solo carácter.

- **Expresiones múltiples de carácter:** Las expresiones múltiples de carácter son secuencias ordenadas de patrones simples de carácter.

- **Permitir o Negar Rutas**

Una vez la ruta haya sido identificada ya se pueden aplicar otros procesos sobre esta. La ruta es permitida o negada, dependiendo de las reglas de filtrado que se hayan establecido para esa ruta. Los criterios para permitir o negar rutas dependen de las políticas que posea el AS. Si la ruta es negada, esa ruta es descartada y no se le aplica ningún otro procesamiento en ella

Si una ruta es permitida, sus atributos pueden verse afectados como consecuencia del proceso de decisión.

El orden en el cual las rutas son comparadas con las diferentes instancias es muy importante. Por ejemplo, si es al comienzo de la lista, es colocada una instancia que le permite todas las rutas, esta instancia dejaría de lado a todas las otras instancias.

F. Política de Ruteo

Las políticas de ruteo son una forma de controlar la procedencia, el origen y el destino del tráfico que llega a los routers. La política de ruteo puede usarse para controlar el tráfico dentro de uno AS así como también entre diversos ASs.

Las políticas de ruteo son una forma de ruteo estático. Estas son usadas cuando se quiere obtener un comportamiento determinado para un paquete, diferente al que especifica el protocolo de ruteo.

La política de ruteo dirige el tráfico basándose en la fuente y el destino del tráfico o una combinación de fuente y destino o en otro conjunto de atributos.

7. EXTENSIONES DE MULTIPROTOCOLO DE BGP[36] (MBGP)

Las extensiones de multiprotocolo de BGP también suelen ser llamadas como “BGP4 +”, y se basan en las capacidades de BGP para proveer extensiones para otros protocolos de capa de red como: IPv6, IPX, L3VPN.

Como ya se había dicho BGP ha sido diseñada para la versión cuatro del protocolo de Internet, y es a través de uso de MBGP que BGP tiene soporte para IPv6.

Para añadir MBGP a BGP-4 fueron introducidos dos atributos nuevos: Multiprotocol Reachable NLRI (MP-REACH_NLRI) y Multiprotocol Unreachable NLRI (MP-UNREACH_NLRI).

A. Atributo Multiprotocol Reachable NLRI – MP_REACH_NLRI (Tipo de código 14)

Es un atributo opcional no transitivo que se usa para:

- Anunciar a los vecinos rutas que pueden ser alcanzadas.
- Permitir a un router poder anunciar la dirección de capa de Red, para nuestro caso se trata de una dirección IPv6, del router que será el próximo salto para los destinos listados en NLRI del atributo MP_NLRI.

El atributo está divido como se muestra en la figura 38:

[36] Basado en el contenido del RFC 4760

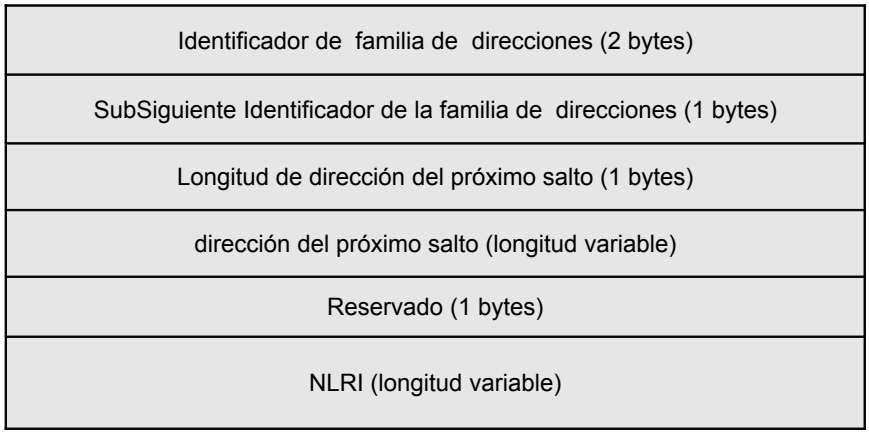

Figura 38: Formato de atributo MP_REACH_NLRI

Los campos del MP_REACH_NLRI se describen a continuación:

- **Identificador de familia de direcciones (AFI) y SubSiguiente Identificador de familia de direcciones (SAFI):** Estos campos en combinación identifican el protocolo de Nivel de Red al cual pertenece la dirección que se encuentra en el campo de próximo salto, la forma en la cual la dirección del próximo salto es codificada, y la semántica del NLRI. si el campo próximo salto permite direcciones de capa de red de distinto protocolo, la información de codificación debe proveer la forma de interpretar dicho protocolo.
- **Longitud de dirección del próximo salto:** este campo indica la longitud del campo de dirección del próximo salto.
- **dirección del próximo salto: es** la dirección del próximo router en la ruta que se debe recorrer hacia el destino, este campo tiene una longitud variable. El NRLI asociado con la dirección del próximo salto es identificada por la combinación <AFI, SAFI> que esta en el atributo.
- **Reservado:** este campo debe de tener un valor de cero y además debe ser ignorado al procesar el atributo.

- **NLRI:** Un campo de longitud variable que lista las rutas accesibles que son anunciadas en este atributo y formarán parte de NRLI. La semántica de NLRI es identificada por una combinación de < AFI, SAFI > del atributo.

La información del próximo salto que se encuentra guardada en el MP-REACH-NLRI del atributo de ruta, define el protocolo de capa de red que el router debe usar en las direcciones del próximo salto listadas en el atributo MP-NRLI del mensaje de actualización.

Un mensaje de actualización que lleve dentro el atributo MP_REACH_NLRI también debe llevar los atributos de origen y de ruta tanto en actualizaciones de EBGP como de IBGP.
Un mensaje de actualización que no tenga NLRI, además del que lleva en el atributo MP-REACH-NLRIm no debería de tener atributo NEXT_HOP

B. Multiprotocol Unreachable NLRI - MP_UNREACH_NLRI (código Tipo 15)

Este es un tipo de atributo opcional no transitivo que se usa para anunciar rutas que serán eliminadas porque no son accesibles. El formato de este atributo se muestra en la figura 39.

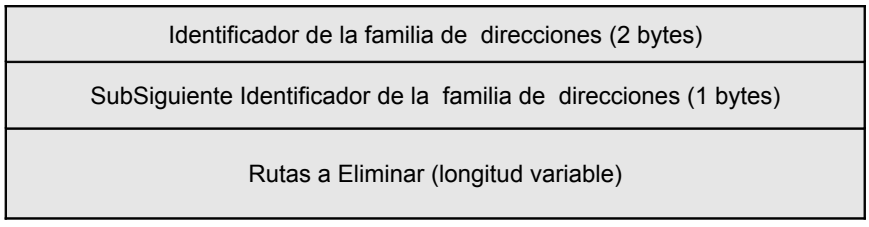

Figura 39: Formato del atributo MP_UNREACH_NLRI

Los campos de este atributo se describen a continuación:

- **Identificador de la familia de direcciones (AFI) y SubSiguiente Identificador de la familia de direcciones (SAFI):** Estos campos en combinación identifican el protocolo de Nivel de Red al que pertenece la dirección que se encuentra en el campo de próximo salto, la forma en la cual la dirección del próximo salto es codificada, y la semántica del NLRI. si el campo próximo salto permite direcciones de capa de red de distinto protocolo, la información de codificación debe proveer la forma de interpretar dicho protocolo

- **Rutas a Eliminar:** Un campo de longitud variable que lista a las rutas que serán retirados del NLRI. La semántica de NLRI se identificada por la combinación de < AFI, SAFI >.

PARTE II

METODOLOGÍA PARA LA CONSTRUCCIÓN DE UN PROTOTIPO DE RED QUE IMPLEMENTE RUTEO CON IPV6

CAPITULO I

METODOLOGÍA PARA LA CONSTRUCCIÓN DE UN PROTOTIPO DE RED QUE IMPLEMENTE RUTEO CON IPV6

FASE 1. DISEÑO DE RED PARA EL PROTOTIPO

El primer paso para el diseño del prototipo es la selección de los protocolos de ruteo que se utilizarán, para hacer esta selección se debe de tomar en cuenta lo siguiente:

El Protocolo de Información de Ruteo de próxima generación (RIPng) es un protocolo de ruteo que se utiliza para redes de pequeño y mediano tamaño. El diámetro máximo de interconexiones de redes RIPng es de 15 routers. Sin embargo, el router del servidor que ejecuta Ruteo y acceso remoto considera que todas las rutas aprendidas que no sean RIPng son de dos saltos.

Entre los casos que pueden constituir un entorno con una configuración en RIPng para IP se incluyen:

- Una empresa de tamaño de pequeño a mediano son las que se compone de 10 a 50 redes.
- Una sucursal u oficina auxiliar con varias redes.

OSPFv3 es un protocolo de ruteo mucho más avanzado que RIPng, ya que OSPF conserva mapas de toda la topología de la red. OSPF envía paquetes "HELLO" para verificar si los routers vecinos aun son alcanzables y para encontrar vecinos nuevos. Aparte de eso, OSPF sólo envía actualizaciones cuando hay cambios en la red. Todos los routers ejecutan el algoritmo de la primera ruta más corta, y el tráfico comienza a tomar el mejor camino. La rápida reacción a las interrupciones y los mecanismos para almacenar información de rutas de una porción o subconjunto de la red hacen adecuado a OSPF para poder ser utilizado en redes de todos los tamaños.

Entre los casos que pueden construir un entorno con una configuración en OSPF se incluyen:

- Un lugar institucional o corporativo que son las que tiene más de 50 redes.
- Una interconexión de redes institucional o corporativa.

- Cuando se desea una red que se recupere rápidamente después de un fallo.

A diferencia de los otros dos protocolos de ruteo, BGP es usado entre redes de diferentes organizaciones ya que es un protocolo para intercambiar información de ruteo entre hospedajes de portales (cada uno con su propio router) en una red de sistemas autónomos. Además, BGP hace posible que los paquetes encuentren el camino de un ISP a otro. BGP también es usado por organismos que se conectan a dos o más ISPs.

En conclusión, los criterios a tomar en cuenta para la construcción del prototipo de red, y en general para cualquier red que incorpore ruteo con IPv6 son el número de redes que componen el prototipo, el hardware con el que se cuenta para el desarrollo del prototipo, el tiempo de convergencia de la red y el tiempo de reponerse a los fallos ocurridos en la red.

Los protocolos utilizados para el prototipo tomando en cuenta lo anterior son: Dado que el prototipo es de carácter experimental se seleccionarán RIPng y OSPFv3 que son protocolos de ruteo de puerta de enlace interna (IGP) y BGP-4 que es un protocolo de puerta de enlace externo (EGP).

Como segundo paso para la construcción del prototipo, se deben realizar y responder las siguientes interrogantes con las cuales se obtendrá una visión clara del diseño del prototipo que se quiere construir y los requisitos que este debe de satisfacer :

- ¿Con que objetivo o propósito se usará el prototipo?
  El objetivo principal del prototipo es la implementación y experimentación de los protocolos de ruteo para IPv6 RIPng, OSPFv3 y BGP-4 dentro de una red.
- ¿Con que equipo se cuenta para la construcción del prototipo?
  Para la construcción del prototipo se cuenta con 16 computadoras de escritorio[37], las cuales cumplen las características siguientes:
  Para una computadora que funcione como Router:
    - Velocidad de procesador 700MHz o superior

[37] Ver Anexo 2 para ver una lista de dispositivos especializados de ruteo.

- Memoria RAM de 128 MB o superior
- Al menos dos interfaces de red
- CD-ROM.
- Sistema operativo con soporte para IPv6

Características para cliente:

- Velocidad de procesador 266MHz o superior
- Memoria RAM de 128 MB
- Una interfaz de red
- Sistema operativo con soporte para IPv6

- ¿Qué sistema operativo se usará para los routers?
  Dado que se implementarán computadoras que funcionan como routers, el sistema operativo de estas debe tener soporte para IPv6 y además deben de tener instalado un software de ruteo, para el prototipo se utilizara el sistema operativo GNU/Linux Debian 4 junto al software de ruteo Quagga 0.99.5.
- ¿Qué tipo de conexiones/cableado se usará?
  La conexiones de los prototipos se realizarán mediante interfaces FastEthernet y cableado UTP categoría 5.
- ¿Qué tipo de direccionamiento se utilizará en el prototipo?
  El direccionamiento para las computadoras que servirán de clientes se realizará de forma dinámica por medio de anuncios de routers (Routers Advertsiment), las direcciones para los routers serán asignadas estáticamente.
- ¿Cuantos routers necesitara el prototipo?
  Se hará uso de ocho routers, de los cuales cuatro implementarán el protocolo de ruteo BGP-4, dos el protocolo OSPF y los dos restantes RIPng.

El diseño de la red que se ha diseñado para el desarrollo de este prototipo se muestra en la figura 40:

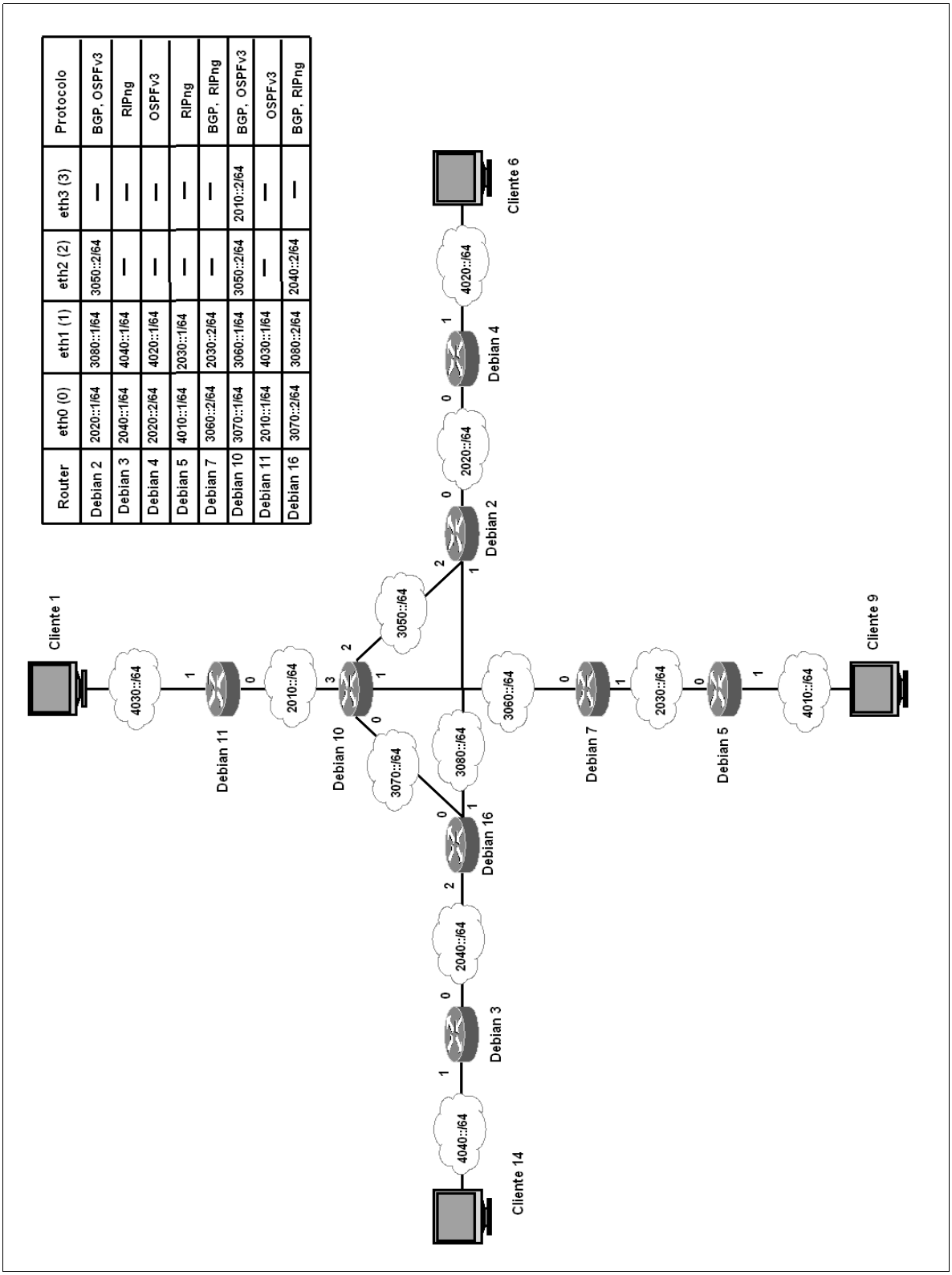

Figura 40: Diagrama de red del Prototipo

Para el prototipo se definen tres AS, la descripción de los routers y el AS al que pertenecen se detalla en la tabla 17:

Nombre del Router	Descripción
debian2	Router que posee tres interfaces de red y ejecuta los protocolos BGP y OSPFv6,pertenece al sistema autónomo AS300.
debian3	Router con dos interfaces de red, ejecuta el protocolo RIPng y esta dentro del sistema autónomo AS200, además envía Router Advertsiment a la red 4040::/64.
debian4	Router con dos interfaces de red, ejecuta el protocolo OSPFv3 y esta dentro del sistema autónomo AS300, además envía Router Advertsiment a la red 4020::/64.
debian5	Router con dos interfaces de red, ejecuta el protocolo RIPng y esta dentro del sistema autónomo AS100, además envía Router Advertsiment a la red 4010::/64.
debian7	Router que posee dos interfaces de red y ejecuta los protocolos BGP y RIPng,pertenece al sistema autónomo AS100.
debian10	Router que posee cuatro interfaces de red y ejecuta los protocolos BGP y OSPFv6,pertenece al sistema autónomo AS100.
debian11	Router con dos interfaces de red, ejecuta el protocolo OSPFv3 y esta dentro del sistema autónomo AS100, además envía Router Advertsiment a la red 4030::/64.
debian16	Router que posee tres interfaces de red y ejecuta los protocolos BGP y RIPng,pertenece al sistema autónomo AS200.

Tabla 17: Descripción de los Routers del prototipo.

FASE 2. CONSTRUCCIÓN DEL PROTOTIPO

En esta fase de la metodología se enfoca en la configuración del equipo que forma parte del prototipo.

A. Configuración del Software Quagga

Quagga esta dividido en diversos archivos, en los cuales es guardada cada configuración que se realiza para cada protocolo de ruteo que ejecuta Quaga, La tabla 18 muestra el listado de archivos de configuración que necesita Quagga para que ejecute los protocolos de ruteo RIPng, OSPFv6 y BGP-4.

Archivo	Descripción
daemons	Este archivo le indica a Quagga los demonios que debe iniciar.
debian.conf	Este archivo indica opciones para telnet
zebra.conf	Archivo de configuración de Zebra
ripng.conf	Archivo de configuración de RIPng
ospf6d.conf	Archivo de configuración de OSPFv3
bgpd.conf	Archivo de configuración de BBGP-4

Tabla 18: Archivos de configuración de Quagga.

A continuación se describen los archivos debian.conf y daemons de Quagga.

- **Archivo daemons**

Este archivo le especifica a Quagga que demonios arrancar, es decir que protocolos de ruteo ejecutará Quagga.

Ejemplo de archivo daemons:

```
# This file tells the quagga package which daemons to start.
#
# Entries are in the format: <daemon>=(yes|no|priority)
#   0, "no"  = disabled
#   1, "yes" = highest priority
#   2 .. 10  = lower priorities
# Read /usr/share/doc/quagga/README.Debian for details.
#
# Sample configurations for these daemons can be found in
# /usr/share/doc/quagga/examples/.
#
# ATTENTION:
```

```
#
# When activation a daemon at the first time, a config file, even if it is
# empty, has to be present *and* be owned by the user and group "quagga", else
# the daemon will not be started by /etc/init.d/quagga. The permissions should
# be u=rw,g=r,o=.
# When using "vtysh" such a config file is also needed. It should be owned by
# group "quaggavty" and set to ug=rw,o= though. Check /etc/pam.d/quagga, too.
#
zebra=yes
bgpd=yes
ospfd=no
ospf6d=yes
ripd=no
ripngd=no
isisd=no
```

En el ejemplo anterior del archivo daemons, se le indica a Quagga que ejecute los demonios para Zebra (zebra=yes), BGP-4 (bgpd=yes) y OSPFv3 (ospf6d=yes).

- **Archivo debian.conf**

Este archivo es especifico para el sistema operativo GNU/Linux Debian, en este archivo de configuración se especifica diferentes opciones para realizar una sesión telnet con las diferentes interfaces de comando de los protocolos de ruteo.

Ejemplo de archivo debian.conf:

```
#
#   If   this   option   is   set   the   /etc/init.d/quagga   script
automatically loads
# the config via "vtysh -b" when the servers are started.
# Check /etc/pam.d/quagga if you intend to use "vtysh"!
#
vtysh_enable=yes
zebra_options=" --daemon -A ::1"
bgpd_options="  --daemon -A ::1"
ospfd_options=" --daemon -A ::1"
ospf6d_options="--daemon -A ::1"
ripd_options="  --daemon -A ::1"
ripngd_options="--daemon -A ::1"
isisd_options=" --daemon -A ::1"
```

En este ejemplo se indica que para poder hacer una sesión telnet a cualquier interfaz de comando se debe de hacer a través de la dirección de loopbak de IPv6 (::1).

Interfaces de Comando

Cada demonio tiene su propio archivo de configuración e interfaz de terminal. Para evitar la incomodidad de configurar individualmente cada uno de estos demonios existe una interfaz shell integrada llamada vtysh. Las interfaces de comando de Quagga posen dos estados de configuración para el de usuario: modo *normal* y modo *enable* . El usuario de modo normal sólo puede ver el estado del sistema sin cambiar las configuraciones del sistema; el usuario de modo enable puede cambiar la configuración del sistema. Para entrar en las diferentes interfaces de comandos de los protocolos de ruteo que posee Quagga se utiliza telnet especificando el puerto al cual esta asociada la interfaz de comandos del protocolo de ruteo a la cual se quiere ingresar, la tabla 19 muestra los puertos a los que esta asociado cada interfaz de comando de Quagga.

Interfaz de Comando	Puerto	Descripción
zebra	2601	zebra vty
ripngd	2603	RIPngd vty
bgpd	2605	BGPd vty
ospf6d	2606	OSPF6d vty

Tabla 19: Puertos asociados a las interfaces de comando

B. Configuración de Zebra

El demonio Zebra se utiliza para darle una base de configuración común a los demás demonios de los protocolos de ruteo que se ejecutan en el router (RIPng, OSPFv3, BGP-4), además es el encargado de proveer las configuraciones de direccionamiento a las diferentes interfaces del router.

El demonio Zebra también es el encargado de configurar las interfaces que generan los Router Advertisement (RA), con lo cual se habilita la autoconfiguración (Stateless) de direcciones IPv6 para los Host que se encuentran conectados en la misma red a la que la interfaz del router esta conectada.

Los pasos para obtener una configuración básica de Zebra son los siguientes:

Paso 1. Entrar al modo privilegiado de la consola de Zebra. Para esto se utiliza el comando *enable*, dependiendo de la configuración que tenga el archivo zebra.conf es posible que se necesite ingresar una contraseña para entrar al modo privilegiado.

Sintaxis.

```
enable
```

Ejemplo.

```
debian1>enable
```

Paso 2. Entrar a modo de configuración global, usando el comando *configure terminal*.

Sintaxis.

```
configure terminal
```

Ejemplo.

```
debian1#configure terminal
```

Paso 3. Entrar al modo de configuración de la Interfaz, para esto se utiliza el comando *interface* seguido del nombre que identifica la interfaz que se quiere configurar.

Sintaxis.

```
interface IFNAME
```

Donde:

IFNAME Es el nombre de la interfaz que se quiere configurar.

Ejemplo.

```
debian1(config)# interface eth0
```

Paso 4. Asignamos la dirección IPv6 a la interfaz con el comando ipv6 address.

Sintaxis.

```
ipv6 address X:X::X:X/M
```

Donde:

X:X::X:X/M Es una dirección IPv6, M hace referencia al tamaño del prefijo de red.

Ejemplo.

```
debian1(config-if)# ipv6 address 3070::1/64
```

Paso 6. Activación del envío de Router Advertisement, este paso es opcional puesto que solo se tiene que habilitar si queremos que en nuestra red sea posible la autoconfiguración de direcciones. Por defecto Zebra tiene deshabilitada esta habilidad, entonces, para autorizar a una interfaz a enviar Router Advertisement es necesario el comando *no ipv6 nd suppress-ra*. Además este comando se complementa con el comando que se describe en el Paso 7.

Sintaxis.

```
no ipv6 nd suppress-ra
```

Ejemplo.

```
debian1(config-if)# no ipv6 nd suppress-ra
```

Paso 7. Configurar el prefijo que anuncia la interfaz, para que este comando sea de utilidad debe de estar activado el envío de Router Advertisement como se indica en el paso anterior. Para indicar el prefijo de red que los clientes utilizarán para la autoconfiguración de direcciones IPv6 se utiliza el comando ipv6 nd prefix seguido del valor del prefijo de red.

Sintaxis.

```
ipv6 nd prefix X:X::X:X/M
```

Donde:

X:X::X:X/M es el prefijo de red que se anunciará, M hace referencia al tamaño en bits del prefijo.

Ejemplo.

```
debian1(config-if)#ipv6 nd prefix 3050::/64
```

Paso 8. Salir del modo de configuración de la interfaz y del modo de configuración global con el comando *end* el cual nos lleva hasta el modo privilegiado de la consola de Zebra.

Sintaxis.

```
end
```

Ejemplo.

```
debian1(config-if)#end
```

Paso 9. Guardamos la configuración que se ha hecho, para esto se utiliza el comando write. Esta configuración se guarda en el archivo *zebra.conf*.

Sintaxis.

```
write
```

Ejemplo.

```
debian1#write
```

Siguiendo todos los pasos anteriores se obtiene una configuración del demonio Zebra capaz de proporcionar autoconfiguración de direcciones IPv6 para Host.

C. Configuración de los protocolos de ruteo

A continuación se muestra los pasos a seguir para configurar los routers del prototipo con los protocolos de ruteo RIPng, OSPFv3 y BGP-4.

Configuración del Router RIPng

A continuación se muestran los pasos para obtener una configuración básica para un router que implemente el protocolo de ruteo RIPng.

Paso 1. Entrar a modo privilegiado de la consola de RIPng. Para esto usamos el comando *enable*.

Sintaxis.

```
enable
```

Ejemplo.

```
debian1>enable
```

Nota: Es posible que solicite una contraseña para poder entrar en modo privilegiado, por lo tanto sera necesario ingresarla.

Paso 2. Entrar a modo de configuración global, usando el comando *configure terminal*.

Sintaxis

```
configure terminal
```

Ejemplo.

```
debian1#configure terminal
```

Paso 3. Entrar a modo de configuración de router RIPng, usando el comando *router ospf6.*

Sintaxis

```
router ripng
```

Ejemplo.

```
debian1(config)# router ripng
```

Paso 4. Se configura la dirección IPv6 de la interfaz. Lo cual permitirá que las interfaces que tienen las direcciones coincidentes con la red se encuentren habilitadas. Se usa el comando *network.*

Sintaxis

```
network red
```

Donde:

red Es una direction IPv6.

Ejemplo.

```
debian1(config-router)# network 4010::1/64
```

Paso 5. Se configura la interfaz de la Red definida. Se habilita tanto el envió como recepción de paquetes RIPng de la interfaz. Se usa el comando *network.*

Sintaxis.

```
network IFNAME
```

donde:

IFNAME *Es el nombre que identifica una interfaz de red*

Ejemplo.

```
debian1(config-router)# network eth1
```

Paso 6. Se crea una ruta estática sólo dentro de RIPng Se usa el comando *route.*

Sintaxis

```
route  X::X::X::/m
```

Donde X::x::X::/m es la dirección IPv6

Ejemplo.

```
debian1(config-router)# route 4010::/64
```

Paso 7. Redistribuimos los prefijos que almacena RIPng, especificando a que protocolo de ruteo queremos que haga la redistribución. Para esto se hace uso del comando *redistribute* seguido del protocolo al que queremos redistribuir la información de RIPNG.

Sintaxis.

```
redistribute (connected|kernel|ospf6|BGP|static)
```

Donde:

connected Se refiere a inyectar a RIPng los prefijos que tienen las interfaces activas del router local.

kernel Se refiere a inyectar a RIPng los prefijos IPv6 que están presentes en la tabla de ruteo del kernel.

ospf6	Se refiere a inyectar a RIPng los prefijos IPv6 que están presentes en OSPFv6
bgp	Se refiere a inyectar a RIPng los prefijos IPv6 que están presentes en BGP
static	Se refiere a inyectar a OSPF la tabla de rutas estática.

Ejemplo.

```
Debian1(config-router)# redistribute connected
```

Paso 8. Salir del modo de configuración del router RIPng usando el comando *end.*

Sintaxis.

```
end
```

Ejemplo.

```
debian1(config)# end
```

Paso 9. Guardar la configuración, para esto se utiliza el comando *write*.La configuración es guardada en el archivo *ripngd.conf*.

Sintaxis.

```
write
```

Ejemplo.

```
debian1# write
```

Configuración del Router OSPFv3

A continuación se muestran los pasos para obtener una configuración básica para un router que implemente el protocolo de ruteo OSPFv3.

Paso 1. Entrar a modo privilegiado de la consola de BGP. Para esto usamos el comando *enable*.

Sintaxis.

```
enable
```

Ejemplo.

```
debian9>enable
```

Nota: Es posible que solicite una contraseña para poder entrar en modo privilegiado, por lo tanto sera necesario ingresarla.

Paso 2. Entrar a modo de configuración global, usando el comando *configure terminal*.

Sintaxis

```
configure terminal
```

Ejemplo.

```
debian9#configure terminal
```

Paso 3. Entrar a modo de configuración de router OSPFv3, usando el comando *router ospf6.*

Sintaxis

```
router ospf6
```

Ejemplo.

```
debian9(config)# router ospf6
```

Paso 4. Configurar el router-ID del router, para lo cual usamos el comando *router-id* seguido del valor que deseamos poner al router, el router-ID esta expresado con la sintaxis de una dirección Ipv4.

Sintaxis.

```
router-id A.B.C.D
```

Donde:

A.B.C.D Es un número expresado con la sintaxis de una dirección Ipv4.

Ejemplo.

```
debian9(config-ospf6)# router-id 9.0.0.0
```

Paso 5. Configurar las interfaces que el router utilizará, designándoles su respectiva área, para lo cual utilizamos el comando *interface.*

Sintaxis.

```
interface interfaz area área
```

Donde:

interfaz Es el tipo de interfaz que se va a configurar.

área Es un número que representa al área

Ejemplo.

```
debian9(config-ospf6)# interface eth0 area 0.0.0.0
```

Paso6. Redistribuimos los prefijos que almacena OSPF, especificando a que protocolo de ruteo queremos que haga la redistribución. Para esto se hace uso del comando *redistribute* seguido del protocolo al que queremos redistribuir la información de OSPF.

Sintaxis.

```
redistribute (connected|kernel|BGP|ripng|static)
```

Donde:

connected Se refiere a inyectar a OSPF los prefijos que tienen las interfaces activas del router local.

kernel Se refiere a inyectar a OSPF los prefijos IPv6 que están presentes en la tabla de ruteo del kernel.

ripng Se refiere a inyectar a OSPF los prefijos IPv6 que están presentes en RIPng

bgp Se refiere a inyectar a OSPF los prefijos IPv6 que están presentes en BGP

static Se refiere a inyectar a OSPF la tabla de rutas estática.

Ejemplo.

```
debian9(config-ospf6)# redistribute connected
```

Paso 7. Salir del modo de configuración del router OSPFv3 usando el comando *end.*

Sintaxis.

```
end
```

Ejemplo.

```
debian9(config-ospf6)# end
```

Paso 8. Guardar la configuración, para esto se utiliza el comando *write*. Esta configuración se guarda en el archivo *ospf6d.conf*.

Sintaxis.

```
write
```

Ejemplo.

```
debian9# write
```

Configuración del Router BGP

A continuación se muestran los pasos para obtener una configuración básica para un router que implemente el protocolo de ruteo BGP-4.

Paso 1. Entrar a modo privilegiado de la consola de BGP. Para esto usamos el comando *enable*.

Sintaxis.

```
enable
```

Ejemplo.

```
debian10>enable
```

Nota: Es posible que solicite una contraseña para poder entrar en modo privilegiado, por lo tanto sera necesario ingresarla.

Paso 2. Entrar a modo de configuración global, usando el comando *configure terminal.*

Sintaxis.

```
configure terminal
```

Ejemplo.

```
debian10#configure terminal
```

Paso 3. Crear un nuevo proceso BGP, para esto se utiliza el comando *router bgp* seguido del número de Sistema Autónomo al que pertenece el router, este comando también sirve para entrar al modo de configuración de un proceso BGP especifico.

Sintaxis.

```
router bgp <1-65535>
```

Donde:

<1-65535> Es un número entero positivo mayor que 1 y menor que 65535.

Ejemplo.

```
debian10(config)# router bgp 100
```

Paso 4. Desactivamos la familia de direcciones para Ipv4 para el proceso bgp, el comando utilizado es *no bgp default ipv4-unicast.*

Sintaxis.

```
no bgp default ipv4-unicast
```

Ejemplo.

```
debian10(config-router)# no bgp default ipv4-unicast
```

Paso 5. Configuramos el router-ID del router, para lo cual usamos el comando *bgp router-id* seguido del valor que deseamos poner al router, el router-ID esta expresado con la sintaxis de una dirección Ipv4.

Sintaxis.

```
bgp router-id A.B.C.D
```

Donde:

A.B.C.D Es un número expresado con la sintaxis de una dirección Ipv4.

Ejemplo.

```
debian10(config-router)# bgp router-id 10.0.0.0
```

Paso 6. Agregamos los vecinos BGP del router local, especificando la dirección IPv6 junto al número de Sistema Autónomo al que pertenece con el comando *neighbor.*

Sintaxis.

```
neighbor (X:X::X:X|WORD) remote-as <1-65535>
```

Donde:

X:X::X:X Es una dirección IPv6.

WORD Es una etiqueta que identifica la dirección de un vecino BGP.

<1-65535> Es un número entero positivo mayor que 1 y menor que 65535.

Ejemplo.

```
debian10(config-router)# neighbor 3050::1 remote-as 200
```

Paso 7. Especificamos que se hará uso de la familia de direcciones de IPv6 y a la vez se ingresa al modo de configuración de la familia de direcciones de IPv6 con el comando *address-family ipv6*.

Sintaxis.

```
 address-family ipv6
```

Ejemplo.

```
debian10(config-router)# address-family ipv6
```

Paso 8. Habilitar a los vecinos BGP para que intercambien prefijos de direcciones IPv6 con el router local, para esto se utiliza el comando *neighbor* dentro del modo de configuración de la familia de direcciones IPv6 que se describió en el paso anterior.

Sintaxis.

```
neighbor (X:X::X:X|WORD) activate
```

Donde:

X:X::X:X es una dirección IPv6.

WORD es una etiqueta que identifica la dirección de un vecino BGP.

Ejemplo.

```
debian10(config-router)#neighbor 3050::1 activate
```

Paso 9. Redistribuimos los prefijos que almacena BGP, especificando a que protocolo de ruteo queremos que haga la redistribución. Para esto se hace uso del comando *redistribute* seguido del protocolo al que queremos redistribuir la información de BGP.

Sintaxis.

```
redistribute (connected|kernel|ospf6|ripng|static)
```

Donde:

connected Se refiere a inyectar a BGP los prefijos que tienen las interfaces activas del router local.

kernel Se refiere a inyectar a BGP los prefijos IPv6 que están presentes en la tabla de ruteo del kernel.

ospf6 Se refiere a inyectar a BGP los prefijos que provienen del protocolo OSPF para IPv6

ripng Se refiere a inyectar a BGP los prefijos que provienen del protocolo RIPng.

static Se refiere a inyectar a BGP la tabla de rutas estática.

Ejemplo.

```
debian10(config-router-af)# redistribute connected
```

Paso 10. Salir del modo de configuración de la familia de direcciones IPv6 con el comando e*xit.*

Sintaxis.

```
exit
```

Ejemplo.

```
debian10(config-router-af)# exit
```

Paso 11. Salir del modo de configuración del proceso BGP usando el comando *exit,* que es el paso anterior.

Sintaxis.

```
exit
```

Ejemplo.

```
debian10(config-router)# exit
```

Paso 12*. Salir del modo de configuración global, nuevamente se utiliza el comando* exit.

Paso 13. Guardar la configuración, para esto se utiliza el comando *write*. La configuración es guardada en el archivo *bgpd.conf*.

Sintaxis.

```
write
```

Ejemplo.

```
debian10# write
```

Archivos de configuración de los Protocolo

Archivo de configuración de Zebra:

```
!
! Zebra configuration saved from vty
!   2007/07/11 15:33:55
!
hostname debian2
password zebra
enable password zebra
!
interface eth0
 ipv6 address 2020::1/64
 ipv6 nd suppress-ra
!
interface eth1
 ipv6 address 3080::1/64
 ipv6 nd suppress-ra
!
interface eth2
 ipv6 address 3050::1/64
 ipv6 nd suppress-ra
!
interface lo
!
interface sit0
 ipv6 nd suppress-ra
!
!
line vty
```

Archivo de configuración de RIPng:

```
!
! Zebra configuration saved from vty
!   2007/09/17 07:34:37
!
hostname debian3
password zebra
log stdout
!
router ripng
 network 2040::1/64
 network 4040::1/64
 network eth0
 network eth1
 redistribute connected
 redistribute bgp
 route 2040::/64
 route 4040::/64
!
line vty
!
```

Archivo de configuración de OSPFv3:

```
!
! Zebra configuration saved from vty
!   2007/09/17 07:49:45
!
hostname debian2
password zebra
log stdout
service advanced-vty
!
debug ospf6 lsa unknown
!
interface eth0
 ipv6 ospf6 cost 1
 ipv6 ospf6 hello-interval 10
 ipv6 ospf6 dead-interval 40
 ipv6 ospf6 retransmit-interval 5
 ipv6 ospf6 priority 1
 ipv6 ospf6 transmit-delay 1
 ipv6 ospf6 instance-id 0
!
!
router ospf6
 router-id 2.0.0.0
 redistribute kernel
 redistribute connected
 redistribute static
 redistribute bgp
 interface eth0 area 0.0.0.0
line vty
!
```

Archivo de configuración de BGP:

```
!
! Zebra configuration saved from vty
!   2007/09/17 07:48:04
!
hostname debian2
password zebra
log stdout
!
router bgp 200
 bgp router-id 2.0.0.0
 neighbor 3050::2 remote-as 100
 neighbor 3080::2 remote-as 300
!
 address-family ipv6
 redistribute connected
 redistribute ospf6
 neighbor 3050::2 activate
 neighbor 3080::2 activate
 exit-address-family
!
line vty
!
```

Configuración de los clientes

Los clientes del prototipo no necesitan de mayor configuración, únicamente es necesario que el sistema operativo tenga soporte para IPv6. Para pruebas de conexión y depurado de la red es necesario que el sistema operativo posea los comandos tracepath, traceroute y que posea algún programa de captura de paquetes de red para que facilite dichos procesos.

D. Información del estado de los protocolos de ruteo

Los comandos que se presentan en las siguientes tablas muestran la información general para el demonio Zebra en la tabla 20 y de los protocolos de ruteo RIPng en la tabla 21 OSPFv6 en la tabla 22, BGP-4 en la tabla 23.

Comando	Propósito
show ipv6 route	Muestra las rutas conocidas por el router, donde se observan los prefijos de red con sus respectivas interfaces
show zebra	Muestra la información de Zebra, donde se observa cuantos protocolos redistribuye por defecto, cuales protocolos redistribuye y en que modo de configuración se encuentra.

Tabla 20: Comandos de información para Zebra.

Comando	Propósito
show ipv6 ripng	Despliega todas las rutas de la tabla de ruteo RIPng, el tiempo que tardo el paquete que se envió en llegar a su destino junto con la interfaz por la cual llega y la información de la etiqueta. Esto solo para rutas que han sido recibidas a través de RIPng y las rutas redistribuidas de los vecinos RIPng, si los hay.
show ipv6 ripng status	Muestra el estado actual de RIPng, donde incluye temporizador, versión, interfaz habilitada y la información de los vecinos, si los hay.
show memory ripng	Muestra las estadísticas y la información de los objetos alojados en el router configurado con el protocolo RIPng.
show running-config	Muestra el archivo de configuración de RIPng que esta corriendo en ese instante.
show ipv6 route *dirección*	Despliega la información de entrada de la ruta, interfaz, métrica, distancia, y la fecha de la última actualización de la ruta especificada.

Tabla 21: Comandos de información para RIPng.

Comando	Propósito
show ipv6 ospf6	Muestra el estado actual de OSPFv3, donde se observa el número de áreas, la identificación de las áreas, el identificador de router, el número de AS al alcance de LSAs y las interfaces con OSPFv3 activas en el router.
show ipv6 ospf6 spf tree	Muestra como esta construido el árbol SPF de OSPFv3 con los ID de router.
show ipv6 ospf6 database	Muestra el contenido de la base de datos del LSA del router OSPFv3, donde se observa el tipo de LSA, el ID del LS, el Router designado, la edad del LS, Número de serie del LS, el Checksum del LS, la longitud del LS y la duración.
show ipv6 ospf6 redistribute	Muestra las rutas que tiene el router y el tipo de distribución que se realiza en cada ruta.
show ipv6 ospf6 route	Muestra todas las rutas que conoce el router y la interfaz por la que tiene el acceso.
show ipv6 ospf6 interface	Muestra la información de estado de las interfaces que tiene el router configurado con el protocolo OSPFv3.
Show memory	Muestra las estadísticas y la información de los objetos alojados en el router configurado con el protocolo OSPFv3.
show ipv6 ospf6 neighbor	Muestra la información de los vecinos que tiene el router configurado con OSPFv3.

Tabla 22: Comandos de información para OSPFv3.

Comando	Propósito
sh ipv6 bgp summary	Muestra la información de los atributos de la tabla de ruteo de BGP-4, así como el estado de los vecinos con los cuales el router ha estableció una sesión.
show ipv6 bgp neighbors 3070::2 routes	Muestra la información de ruteo asociada a un vecino en particular, este comando muestra las rutas que BGP-4 ha recibido desde el vecino.
show bgp ipv6 neighbors 3070::2 advertised-routes	Muestra las rutas que el router anuncia a un vecino especifico, es decir que este comando despliega el conjunto de prefijos que el router BGP-4 anuncia a un vecino,
show memory bgp	Muestra las estadísticas del uso de memoria de BGP, despliega los diferentes objetos que se encuentran alojados en memoria.
show bgp memory	Muestra las estadísticas del uso de memoria de BGP, este comando, al igual que show memory bgp, despliega la información de los objetos que se encuentran en memoria y la cantidad de memoria que ocupan, es decir, la cantidad que de memoria en bytes que se utiliza para guardarlos en memoria.

Tabla 23: Comandos de información para BGP.

- **Información de estado del demonio zebra**

Comando *show zebra* ejecutado en el router debian4

```
debian4# show zebra
Zebra Infomation
  enable: 1 fail: 0
  redistribute default: 7
        redistribute: kernel connected static ospf6 bgp
```

Comando *show ipv6 route* ejecutado en el router debian4

```
debian4# show ipv6 route
Codes: K - kernel route, C - connected, S - static, R - RIPng, O -
OSPFv3,
       I - ISIS, B - BGP, * - FIB route.

C>* ::1/128 is directly connected, lo
O>* 2010::/64 [110/1] via fe80::214:22ff:fe3f:b446, eth0, 00:20:11
O   2020::/64 [110/1] is directly connected, eth0, 00:43:10
K * 2020::/64 is directly connected, eth0
C>* 2020::/64 is directly connected, eth0
O>* 2030::/64 [110/1] via fe80::214:22ff:fe3f:b446, eth0, 00:20:11
O>* 2040::/64 [110/1] via fe80::214:22ff:fe3f:b446, eth0, 00:43:10
O>* 3050::/64 [110/1] via fe80::214:22ff:fe3f:b446, eth0, 00:43:10
O>* 3060::/64 [110/1] via fe80::214:22ff:fe3f:b446, eth0, 00:20:11
O>* 3070::/64 [110/1] via fe80::214:22ff:fe3f:b446, eth0, 00:20:11
O>* 3080::/64 [110/1] via fe80::214:22ff:fe3f:b446, eth0, 00:43:10
O>* 4010::/64 [110/1] via fe80::214:22ff:fe3f:b446, eth0, 00:20:11
O   4020::/64 [110/1] via ::1, lo, 00:43:10
K * 4020::/64 is directly connected, eth1
C>* 4020::/64 is directly connected, eth1
O>* 4030::/64 [110/1] via fe80::214:22ff:fe3f:b446, eth0, 00:14:27
O>* 4040::/64 [110/1] via fe80::214:22ff:fe3f:b446, eth0, 00:43:10
K * fe80::/64 is directly connected, eth1
C * fe80::/64 is directly connected, ra0
C * fe80::/64 is directly connected, eth1
C>* fe80::/64 is directly connected, eth0
O   ff00::/8 [110/1] via fe80::214:22ff:fe3f:b446, eth0, 00:43:10
K>* ff00::/8 is directly connected, eth1
```

- **Información de estado del router configurado con el protocolo RIPng**

Comando *show ipv6 ripng status* ejecutado en el router debian5

```
debian5# show ipv6 ripng status
Routing Protocol is "RIPng"
  Sending updates every 30 seconds with +/-50%, next due in-1190195436
seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:    connected    bgp
  Default version control: send version 1, receive version 1
    Interface        Send  Recv
    eth0             1     1
    eth1             1     1
  Routing for Networks:
    2030::2/64
    4010::2/64
    eth1
    eth0
  Routing Information Sources:
    Gateway          BadPackets BadRoutes  Distance Last Update
    fe80::206:4fff:fe4b:4591
                           0          0        120      00:00:12
```

Comando *show memory ripng* ejecutado en el router debian5

```
debian5# show memory ripng
RIPng structure               :          1
RIPng route info              :         12
RIPng peer                    :          1
```

Comando *show ipv6 ripng* ejecutado en el router debian5

```
debian5# show ipv6 ripng
Codes: R - RIPng, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
      (n) - normal, (s) - static, (d) - default, (r) - redistribute,
      (i) - interface, (a/S) - aggregated/Suppressed

   Network      Next Hop                         Via     Metric Tag Time
R(n) 2010::/64  fe80::206:4fff:fe4b:4591    eth0       2    0  11:57
R(n) 2020::/64  fe80::206:4fff:fe4b:4591    eth0       2    0  11:57
R(n) 2030::/64  fe80::206:4fff:fe4b:4591    eth0       2    0  11:57
R(s) 2040::/64  ::                          self       1    0
R(n) 3050::/64  fe80::206:4fff:fe4b:4591    eth0       2    0  11:57
R(n) 3060::/64  fe80::206:4fff:fe4b:4591    eth0       2    0  11:57
R(n) 3070::/64  fe80::206:4fff:fe4b:4591    eth0       2    0  11:57
R(n) 3080::/64  fe80::206:4fff:fe4b:4591    eth0       2    0  11:57
R(n) 4010::/64  fe80::206:4fff:fe4b:4591    eth0       2    0  11:57
R(n) 4020::/64  fe80::206:4fff:fe4b:4591    eth0       2    0  11:57
R(n) 4030::/64  fe80::206:4fff:fe4b:4591    eth0       2    0  11:57
R(s) 4040::/64  ::                          self       1    0
```

Comando *show ipv6 ripng route 2030::2* ejecutado en el router debian5

```
debian5# show ipv6 route 2030::2
Routing entry for 2030::/64
  Known via "kernel", distance 0, metric 0
  * directly connected, eth0

Routing entry for 2030::/64
  Known via "connected", distance 0, metric 1, best
  * directly connected, eth1
```

- **Información de estado del router configurado con el protocolo OSPFv3**

Comando *show ipv6 ripng status* ejecutado en el router debian4

```
debian4# show ipv6 ospf6
 OSPFv3 Routing Process (0) with Router-ID 4.0.0.0
 Running 00:50:49
 Number of AS scoped LSAs is 25
 Number of areas in this router is 1
 Area 0.0.0.0
     Number of Area scoped LSAs is 6
           Interface attached to this area: eth0 eth1
```

Comando *show ipv6 ospf6 spf tree* ejecutado en el router debian4

```
debian4# show ipv6 ospf6 spf tree
+-4.0.0.0 [0]
   +-2.0.0.0 Net-ID: 0.0.0.2 [1]
             +-2.0.0.0 [1]
```

Comando *show ipv6 ospf6 database* ejecutado en el router debian4

```
debian4# show ipv6 ospf6 database

        Area Scoped Link State Database (Area 0.0.0.0)

Type         LSId            AdvRouter        Age   SeqNum Cksm  Len Duration
Router       0.0.0.0         2.0.0.0         1195 80000002 be55   40 00:19:54
Router       0.0.0.0         4.0.0.0         1195 80000008 8e7b   40 00:19:54
Network      0.0.0.2         2.0.0.0         1195 80000002 58c3   32 00:19:54
Intra-Prefix 0.0.0.0         2.0.0.0         2999 80000001 dca4   44 00:49:54
Intra-Prefix 0.0.0.2         2.0.0.0         1195 80000002 cead   44 00:19:54
Intra-Prefix 0.0.0.0         4.0.0.0         1195 80000006 3d17   44 00:19:54

        I/F Scoped Link State Database (I/F eth0 in Area 0.0.0.0)

Type         LSId            AdvRouter        Age   SeqNum Cksm  Len Duration
Link         0.0.0.2         2.0.0.0          436 80000004 e8c7   56 00:07:15
Link         0.0.0.2         4.0.0.0         1195 80000007 8e06   56 00:19:54

        I/F Scoped Link State Database (I/F eth1 in Area 0.0.0.0)

Type         LSId            AdvRouter        Age   SeqNum Cksm  Len Duration
Link         0.0.0.3         4.0.0.0         1198 80000002 de60   56 00:19:58

        AS Scoped Link State Database

Type         LSId            AdvRouter        Age   SeqNum Cksm  Len Duration
AS-External  0.0.0.0         2.0.0.0          436 80000004 d13a   32 00:07:15
AS-External  0.0.0.1         2.0.0.0          436 80000004 3c52   36 00:07:15
AS-External  0.0.0.2         2.0.0.0          436 80000004 2528   36 00:07:15
AS-External  0.0.0.3         2.0.0.0          436 80000004 5dbe   36 00:07:15
AS-External  0.0.0.18        2.0.0.0         3600 80000002 d4ba   36 00:26:56
AS-External  0.0.0.19        2.0.0.0         3600 80000002 4c22   36 00:26:56
AS-External  0.0.0.20        2.0.0.0         3600 80000002 35f7   36 00:26:56
AS-External  0.0.0.21        2.0.0.0         3600 80000002 1854   36 00:26:56
AS-External  0.0.0.22        2.0.0.0         3600 80000001 e338   36 00:26:56
AS-External  0.0.0.24        2.0.0.0         1203 80000002 da7e   36 00:20:01
AS-External  0.0.0.25        2.0.0.0         1203 80000002 3206   36 00:20:01
AS-External  0.0.0.26        2.0.0.0         1617 80000001 8602   36 00:26:56
AS-External  0.0.0.27        2.0.0.0         1617 80000001 fd69   36 00:26:56
AS-External  0.0.0.28        2.0.0.0         1617 80000001 e63f   36 00:26:56
AS-External  0.0.0.29        2.0.0.0         1617 80000001 9d77   36 00:26:56
AS-External  0.0.0.30        2.0.0.0         1617 80000001 bfa4   36 00:26:56
AS-External  0.0.0.31        2.0.0.0         1603 80000001 542f   36 00:26:42
AS-External  0.0.0.32        2.0.0.0         1603 80000001 cb96   36 00:26:42
AS-External  0.0.0.33        2.0.0.0         1603 80000001 b46c   36 00:26:42
AS-External  0.0.0.34        2.0.0.0         1603 80000001 97c8   36 00:26:42
AS-External  0.0.0.35        2.0.0.0         3600 80000001 0f30   36 00:26:38
AS-External  0.0.0.36        2.0.0.0         1273 80000001 0539   36 00:21:12
AS-External  0.0.0.0         4.0.0.0         1198 80000002 b158   32 00:19:58
AS-External  0.0.0.1         4.0.0.0         1198 80000002 1c70   36 00:19:58
AS-External  0.0.0.2         4.0.0.0         1198 80000002 73f7   36 00:19:58
```

Comando *show ipv6 ospf6 redistribute* ejecutado en el router debian4

```
debian4# show ipv6 ospf6 redistribute
Redistributing External Routes from:
    1: kernel
    2: connected
    0: static
    0: bgp
Total 3 routes
C 2020::/64           0.0.0.1         type-0     0 :: (ifindex 2)
C 4020::/64           0.0.0.2         type-0     0 :: (ifindex 3)
K ff00::/8            0.0.0.0         type-0     0 :: (ifindex 3)
```

Comando *show ipv6 ospf6 route* ejecutado en el router debian4

```
debian4# show ipv6 ospf6 route
*N E1 2010::/64                fe80::214:22ff:fe3f:b446    eth0 00:22:30
 N E1 2010::/64                fe80::214:22ff:fe3f:b446    eth0 00:22:16
*N IA 2020::/64                ::                          eth0 00:45:29
 N IA 2020::/64                fe80::214:22ff:fe3f:b446    eth0 00:45:29
 N E1 2020::/64                fe80::214:22ff:fe3f:b446    eth0 00:45:29
*N E1 2030::/64                fe80::214:22ff:fe3f:b446    eth0 00:22:30
 N E1 2030::/64                fe80::214:22ff:fe3f:b446    eth0 00:22:16
*N E1 2040::/64                fe80::214:22ff:fe3f:b446    eth0 00:45:29
*N E1 3050::/64                fe80::214:22ff:fe3f:b446    eth0 00:45:29
*N E1 3060::/64                fe80::214:22ff:fe3f:b446    eth0 00:22:30
 N E1 3060::/64                fe80::214:22ff:fe3f:b446    eth0 00:22:16
*N E1 3070::/64                fe80::214:22ff:fe3f:b446    eth0 00:22:30
*N E1 3080::/64                fe80::214:22ff:fe3f:b446    eth0 00:45:29
*N E1 4010::/64                fe80::214:22ff:fe3f:b446    eth0 00:22:30
 N E1 4010::/64                fe80::214:22ff:fe3f:b446    eth0 00:22:16
*N IA 4020::/64                ::1                            0 00:45:29
*N E1 4030::/64                fe80::214:22ff:fe3f:b446    eth0 00:16:46
*N E1 4040::/64                fe80::214:22ff:fe3f:b446    eth0 00:45:29
      *N E1 ff00::/8                    fe80::214:22ff:fe3f:b446    eth0
      00:45:29
```

Comando *show ipv6 ospf6 interface* ejecutado en el router debian4

```
debian4# show ipv6 ospf6 interface
eth0 is up, type BROADCAST
  Interface ID: 2
  Internet Address:
    inet : 169.254.5.173/16
    inet6: 2020::2/64
    inet6: fe80::214:22ff:fe3f:b45b/64
  Instance ID 0, Interface MTU 1500 (autodetect: 1500)
  Area ID 0.0.0.0, Cost 1
  State BDR, Transmit Delay 1 sec, Priority 1
  Timer intervals configured:
   Hello 10, Dead 40, Retransmit 5
  DR: 2.0.0.0 BDR: 4.0.0.0
  Number of I/F scoped LSAs is 2
    0 Pending LSAs for LSUpdate in Time 00:00:00 [thread off]
    0 Pending LSAs for LSAck in Time 00:00:00 [thread off]
eth1 is up, type BROADCAST
  Interface ID: 3
  Internet Address:
    inet6: 4020::1/64
    inet6: fe80::208:54ff:fe1f:c082/64
  Instance ID 0, Interface MTU 1500 (autodetect: 1500)
  Area ID 0.0.0.0, Cost 1
  State DR, Transmit Delay 1 sec, Priority 1
  Timer intervals configured:
   Hello 10, Dead 40, Retransmit 5
  DR: 4.0.0.0 BDR: 0.0.0.0
  Number of I/F scoped LSAs is 1
    0 Pending LSAs for LSUpdate in Time 00:00:00 [thread off]
    0 Pending LSAs for LSAck in Time 00:00:00 [thread off]
lo is up, type LOOPBACK
  Interface ID: 1
   OSPF not enabled on this interface
ra0 is up, type BROADCAST
  Interface ID: 4
   OSPF not enabled on this interface
```

Comando *show memory* ejecutado en el router debian4

```
debian4# show memory
System allocator statistics:
  Total heap allocated:  528 KiB
  Holding block headers: 0 bytes
  Used small blocks:     0 bytes
  Used ordinary blocks:  426 KiB
  Free small blocks:     24 bytes
  Free ordinary blocks:  102 KiB
  Ordinary blocks:       18
  Small blocks:          1
  Holding blocks:        0
(see system documentation for 'mallinfo' for meaning)
----------------------------
Temporary memory              :          2
String vector                 :       6950
Vector                        :       3298
Vector index                  :       3298
Link List                     :         12
Link Node                     :         18
Thread                        :         45
Thread master                 :          1
Thread stats                  :         32
Thread function name          :         77
VTY                           :          2
Interface                     :          4
Connected                     :          8
Buffer                        :          2
Buffer data                   :          1
Stream                        :          2
Stream data                   :          2
Prefix                        :          9
Hash                          :          1
Hash Bucket                   :         32
Hash Index                    :          1
Route table                   :         30
Route node                    :        281
Command desc                  :       3485
Privilege information         :          2
Logging                       :          1
Zclient                       :          1
Priority queue                :          2
Priority queue data           :          2
Host config                   :          3
----------------------------
OSPF6 top                     :          1
OSPF6 area                    :          1
OSPF6 interface               :          2
OSPF6 neighbor                :          1
OSPF6 route                   :         53
OSPF6 message                 :          2
OSPF6 LSA                     :         82
OSPF6 LSA database            :         19
OSPF6 vertex                  :          3
OSPF6 ext. info               :          3
```

Comando *show ipv6 ospf6 neighbor* ejecutado en el router debian4

```
debian4# show  ipv6 ospf6 neighbor
Neighbor ID     Pri    DeadTime  State/IfState         Duration
I/F[State]
      2.0.0.0         1 -331362:-5:-41   Full/DR          00:44:30
      eth0[BDR]
```

- **Información del estado del router configurado con el protocolo BGP-4**

Comando *show ipv6 bgp summary* ejecutado en el router debian10

```
debian10# show ipv6 bgp summary
BGP router identifier 10.0.0.0, local AS number 100
RIB entries 23, using 1472 bytes of memory
Peers 3, using 7536 bytes of memory

Neighbor   V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd

3050::1    4   200      22      32        0    0    0 00:13:17        7
3060::2    4  1001      18      26        0    0    0 00:13:22        3
3070::2    4   300      26      25        0    0    0 00:13:22        7

Total number of neighbors 3
```

Comando *show ipv6 bgp neighbors 3070::2 routes* ejecutado en el router debian10

```
debian10# show ipv6 bgp neighbors 3070::2 routes
BGP table version is 0, local router ID is 10.0.0.0
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal,   r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop       Metric LocPrf Weight Path
*  2020::/64        3070::2                             0 300 200 ?
*> 2040::/64        3070::2              1              0 300 ?
*  3050::/64        3070::2                             0 300 200 ?
*  3070::/64        3070::2              1              0 300 ?
*  3080::/64        3070::2              1              0 300 ?
*  4020::/64        3070::2                             0 300 200 ?
*> 4040::/64        3070::2              2              0 300 ?

Total number of prefixes 7
```

Comando *show bgp ipv6 neighbors 3070::2 advertised-routes* ejecutado en el router debian10

```
debian10# show bgp ipv6 neighbors 3070::2 advertised-routes
BGP table version is 0, local router ID is 10.0.0.0
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal,  r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 2010::/64        3070::1                  1         32768  ?
*> 2020::/64        3070::1                               0 200 ?
*> 2030::/64        3070::1                               0 1001 ?
*> 3050::/64        3070::1                  1         32768  ?
*> 3060::/64        3070::1                  1         32768  ?
*> 3070::/64        3070::1                  1         32768  ?
*> 4010::/64        3070::1                               0 1001 ?
*> 4020::/64        3070::1                               0 200 ?
*> 4030::/64        3070::1                  2         32768  ?

Total number of prefixes 9
```

Comando *show memory bgp* ejecutado en el router debian10

```
debian10# show memory bgp
BGP instance                   :          1
BGP peer                       :          4
BGP peer hostname              :          3
BGP attribute                  :         28
BGP aspath                     :          6
BGP aspath seg                 :          5
BGP aspath segment data        :          5
BGP aspath str                 :          6

-----------------------------

BGP table                      :         31
BGP node                       :         30
BGP route                      :         22
BGP synchronise                :         32
BGP adj out                    :         29

-----------------------------

community-list handler         :          1

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

FASE 3. PRUEBAS DE CONFIGURACIÓN PARA EL PROTOTIPO

Pruebas de la configuración de los clientes

Para probar las configuraciones de los routers se realiza pruebas de conexión con los clientes, esto se hace usando el comando ping6 y traceroute6, con lo cual se comprueba la conectividad entre los diferentes clientes, redes o subredes del prototipo. El comando ping6[38] realiza una petición de echo hacia otra dirección, si esta dirección puede ser alcanzada esta responde la petición. El comando traceroute6 muestra los diferentes saltos que ha realizado un paquete para llegar a su destino.

```
debian14:/home/grupo24# ping6 4010::211:9ff:fe2c:faf4
PING 4010::211:9ff:fe2c:faf4(4010::211:9ff:fe2c:faf4) 56 data bytes
64 bytes from 4010::211:9ff:fe2c:faf4: icmp_seq=1 ttl=59 time=0.528 ms
64 bytes from 4010::211:9ff:fe2c:faf4: icmp_seq=2 ttl=59 time=0.518 ms
64 bytes from 4010::211:9ff:fe2c:faf4: icmp_seq=3 ttl=59 time=0.515 ms
64 bytes from 4010::211:9ff:fe2c:faf4: icmp_seq=4 ttl=59 time=0.520 ms

--- 4010::211:9ff:fe2c:faf4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 0.515/0.520/0.528/0.016 ms
```

```
debian14:/home/grupo24# traceroute6 4010::211:9ff:fe2c:faf4
traceroute to 4010::211:9ff:fe2c:faf4 (4010::211:9ff:fe2c:faf4) from
4040::206:4fff:fe4b:4431, 30 hops max, 16 byte packets
 1  4040::1 (4040::1)  4.688 ms  0.085 ms  0.08 ms
 2  2040::2 (2040::2)  0.164 ms  0.16 ms  0.16 ms
 3  3070::1 (3070::1)  0.246 ms  0.225 ms  0.22 ms
 4  3060::2 (3060::2)  0.318 ms  0.302 ms  0.332 ms
 5  2030::1 (2030::1)  0.399 ms  0.367 ms  0.365 ms
 6  4010::211:9ff:fe2c:faf4 (4010::211:9ff:fe2c:faf4)  3.825 ms  0.432
ms  0.433 ms
```

[38] El comando ping6 hace uso de los mensajes de ICMPv6, ver Anexo 3.

Además de las pruebas con los comandos ping y traceroute, en el prototipo se pueden realizar pruebas de captura de paquetes para el análisis de la información de ruteo que transporta, también se puede realizar pruebas de la estabilidad y recuperación de fallos de la red desconectando físicamente un enlace entre dos routers y analizar el cambio en las rutas que se producen.

Errores comunes de configuración y posibles soluciones

- **Problema:** El cliente no puede dar ping aun cliente dentro de su propia red.

  Posible Causa: Mal funcionamiento en la conexión de la capa física, falta de dirección IPv6 (dirección IPv6 global o de enlace).

  Posible Solución: Cambiar o revisar el medio físico de conexión a la red, solicitar la asignación de una nueva dirección para el cliente.

- **Problema:** El cliente no puede dar ping a un cliente fuera de la red a la cual que pertenece y la salida del comando ping indica que no existe ruta a dicha dirección (Destination unreachable: No route).

  Posible Causa: Mala configuración del router por defecto.

  Posible Solución: Revisar la política de ruteo del router para verificar las rutas a las que permite el acceso el router.

- **Problema:** El cliente no puede dar ping a un cliente fuera de la red a la cual que pertenece y la salida del comando ping indica que no puede alcanzar a red. (Destination unreachable: Address unreachable).

  Posible Causa: Errores de capa de enlace: falta de direcciones IPv6 global o de enlace, la dirección no esta asignada a ningun cliente .

  Posible Solución: Asignar las direcciones del cliente, verificar que la dirección a la que se hace ping exista.

- **Problema:** El cliente no puede dar ping a un cliente fuera de la red a la cual que pertenece y la salida del comando ping indica que la red no es alcanzable. (connect: Network is unreachable).

  Posible Causa: Falta de dirección IPv6 global o de enlace.

  Posible Solución: Asignación de una dirección IPv6.

CONCLUSIONES

La utilización de ruteo con IPv6 es inevitable, ya que a medida pasa el tiempo las empresas u organizaciones se enfrentan a una migración completa hacia IPv6, por lo que será beneficioso contar para este cambio con la ayuda de este documento el cual contiene una investigación y las características esenciales de los protocolos de ruteo.

La metodología muestra las fases a seguir para desarrollar un prototipo de red, con lo que se solventa la necesidad de un documento que facilite a las empresas u organizaciones la implementación de ruteo con IPv6. Además, con la utilización del manual de referencia estas empresas u organizaciones obtienen una reducción de tiempo y costo en la investigación necesaria para desarrollar un prototipo de red que implemente IPv6.

Como resultado de la investigación se concluye que los algoritmos de selección de rutas que utilizan los protocolos de ruteo de IPv4 siguen siendo aplicados en la selección de rutas en los protocolos de ruteo de IPv6, sin embargo, el ruteo con IPv6 a diferencia del ruteo con IPv4 es más eficiente, puesto que incorpora mejoras al formato de la cabecera IP lo que permite un mejor procesamiento de la misma en los routers favoreciendo a un ruteo de paquetes más rápido.

RECOMENDACIONES

Se recomienda que dentro de la universidad se promuevan y apoyen los trabajos de investigación, en la rama del conocimiento tecnológico, especialmente aquellas que promuevan la adopción de nuevas tecnologías, ya que esto conlleva a un crecimiento en el desarrollo tecnológico en el país, además de dar continuidad a las investigaciones ya realizadas.

Se recomienda desarrollar más investigaciones relacionadas a la última versión del protocolo de Internet ya que esto ayudará a la sociedad salvadoreña a desarrollar más aplicaciones de tecnología avanzada de redes de telecomunicaciones.

GLOSARIO

A

Access Control List (ACL) Las listas de control de acceso son listas de condiciones que se aplican al tráfico que viaja a través de la interfaz del router. Estas controlan el tráfico en una dirección por vez, en una interfaz. Se necesita crear una ACL por separado para cada dirección, una para el tráfico entrante y otra para el saliente. Finalmente, cada interfaz puede contar con varios protocolos y direcciones definidas. Las ACL permiten la administración del tráfico y aseguran el acceso hacia y desde una red estas filtran el tráfico de red, controlando si los paquetes son enrutados se envían o se bloquean en las interfaces del router. El router examina cada paquete y lo enviará o lo descartará, según las condiciones especificadas en la ACL. Algunos de los puntos de decisión de ACL son direcciones origen y destino, protocolos y números de puerto de capa superior.

Address Family Identifier (AFI) Especifica la dirección de familia utilizada. RIP esta diseñado para portar información de diferentes protocolos. Cada entrada tiene una dirección de identificación que indica cual es el tipo de direcciones especificadas. El valor del campo de AFI para IP es 2. Si la AFI para la primera entrada es 0xFFFF, significa que el resto de la entrada contiene información de autenticación. Actualmente, la información de autenticación es nada más simple que un password.

B

Backbone Se refiere a las principales conexiones troncales de Internet. Está compuesta de un gran número de routers comerciales, gubernamentales, universitarios y otros, de gran capacidad interconectados que trasladan los datos e información entre países, continentes y océanos del mundo.

Broadcast Es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

C

Cabecera de paquete Es la que contiene la información que intercambian nodos, de tal manera que siempre sean valores válidos. Se visualiza a través de un formato y se utiliza como expresión del conjunto de reglas que definen un protocolo.

Costo	Esta asociado a la métrica con un enlace o a un camino.
	D
Dirección del Nivel de enlace	Es la dirección física de una interfaz, como la dirección de control de acceso al medio (MAC) en los enlaces Ethernet. En IPv6 todo el direccionamiento es hacia la interfaz del nodo, no a los nodos.
Dominio de Ruteo	Es la división jerárquica de la red que contiene un conjunto de anfitriones (hosts) y routers; los routers comparten la misma información de ruteo, comprueban las tablas usando el mismo IGP, y son manejadas por una autoridad administrativa común.
Duplicate IP Address Detection (DAD)	La Detección de Duplicidad de dirección, permite que un nodo compruebe si una dirección propuesta esta funcionando. El DAD usa la dirección especificada como una dirección origen, el nivel-enlace del router debe ser usado en soluciones multicast y puede ser usado en soluciones unicast.
	E
Encapsulamiento IPv6	Es el proceso por el cual los datos que se deben enviar a través de una red se colocan en paquetes que se puedan administrar y rastrear. El encapsulado consiste entonces en ocultar los detalles de implementación de un objeto pero, a la vez, se provee una interfaz pública por medio de sus operaciones permitidas.Radica principalmente en el aprovechamiento máximo de las redes ya existentes.
ENDIAN	Se refiere a la forma en que los números binarios de bytes múltiples son guardados en la computadora.
Ethernet	Es el nombre de la capa de enlace más popular de una tecnología de redes LANs basada en tramas de datos usada actualmente y fue desarrollada principalmente por las empresas XEROX, Intel y Digital Equipment Company (DIX). El nombre viene del concepto físico de ether. Ethernet define las características de cableado y señalización de nivel físico y los formatos de trama del nivel de enlace de datos del modelo OSI. Ethernet se refiere a las redes de área local y dispositivos bajo el estándar IEEE 802.3 que define el protocolo CSMA/CD. Ethernet es popular porque permite un buen equilibrio entre velocidad, costo y facilidad de instalación. Estos puntos fuertes, combinados con la amplia aceptación en el mercado y la habilidad de soportar virtualmente todos los protocolos de red populares, hacen a Ethernet la tecnología ideal para la red de la mayoría de usuarios de la informática actual.

F

Fragmentación IP

Es la división de datagramas en pedazos muy pequeños para pasar sobre un enlace con un MTU más pequeño que el tamaño original del datagrama.

Hay dos decisiones que se pueden seguir para decidir al tamaño de datagramas IP que se enviarán sobre la red: El origen puede enviar un par de datagramas IP del mismo tamaño que la MTU de la fuente al primer salto del destino. El segundo es poner a funcionar “el algoritmo del descubrimiento del MTU de la trayectoria (PMTU)” para decidir cuál es el tamaño del datagrama IP a enviar al destino.

H

Host

Es un nodo que no reenvía paquetes o una máquina conectada a una red de computadoras y que tiene un nombre de equipo (en inglés, hostname). Es un nombre único que se le da a un dispositivo conectado a una red informática. Puede ser un computador, un servidor de archivos, un dispositivo de almacenamiento por red, una máquina de fax, impresora, etc. Este nombre ayuda al administrador de la red a identificar las máquinas sin tener que memorizar una dirección IP para cada una de ellas.

I

Institute of Electrical and Electronics Engineers (IEEE)

El Instituto de Ingenieros Eléctricos y Electrónicos, es una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros eléctricos, ingenieros en electrónica, científicos de la computación e ingenieros en telecomunicación, entre otros. Su creación se remonta al año 1884, contando entre sus fundadores a personalidades de la talla de Thomas Alva Edison, Alexander Graham Bell y Franklin Leonard Pope. En 1963 adoptó el nombre de IEEE al fusionarse asociaciones como el AIEE (American Institute of Electrical Engineers) y el IRE (Institute of Radio Engineers).

Interfaz

Es una interfaz es la conexión con un medio de transmisión por la que se envían los paquetes de IPv6. Aunque se realice una distinción entre routers y hosts, es posible, aunque poco probable, que un único nodo tenga varias interfaces y, potencialmente, reenvíe paquetes a direcciones de otros nodos o solamente a un subconjunto de sus interfaces. Es decir, este dispositivo actuaría como un host (en las interfaces que no reenvía) y como un router (en las interfaces que reenvía).

Internetworking Protocol (IP) Es un protocolo de interconexión, también conocido como protocolo de ruteo básico para capa 3 de Internet.

Internet Assigned Numbers Authority (**IANA**) La Agencia de Asignación de Números de Internet, es el antiguo registro central de los protocolos Internet, como puertos, números de protocolo y empresa, opciones y códigos. Fue sustituido en 1998 por ICANN.

Internet Control Message Protocol version 6 (ICMPv6) El Protocolo de control de mensajes Internet para IPv6, es un estándar de IPv6 necesario que está definido en el documento RFC 4443. Con ICMPv6, los hosts y los routers que se comunican mediante IPv6 pueden informar de errores y enviar mensajes de eco simples.

Internet Packet Exchange (IPX) El Intercambio de Paquetes en la red, es un protocolo de red utilizado por los sistemas operativos Novell Netware. Como TCP/IP e IPX. Este es un protocolo de datagramas usado para las comunicaciones no orientadas a conexión. Se derivan de los protocolos IDP y SPP de los servicios de red de Xerox.

Internet Service Provider (ISP) Una organización pública o privada que proporciona servicios de Internet. A menudo simplemente proporciona otros tipos de servicios relacionados con Telecomunicaciones.

L

Latin American and Caribbean Internet Addresses Registry (LACNIC) Es el Registro Regional de Internet para América Latina y el Caribe, que administran las Direcciones IP versión 4 y versión 6, Números de Sistemas Autónomos, DNS Reverso, y otros recursos de red para la región.

LACNIC se estableció en el año 2001. Sus oficinas administrativas se encuentran en Montevideo, Uruguay y el complejo tecnológico de asignación es provisto por Comité Gestor da Internet Brasil de São Paulo Brasil. Antes de su fundación, los registros de servicios IP para la región eran provistos por ARIN.

Local Area Network (LAN) La Red de Área Local, es la Interconexión de nodos y periféricos para formar una red dentro de una empresa u hogar, limitada generalmente a un espacio físico pequeño. Con esta se pueden intercambiar datos y compartir recursos entre los nodos que conforman la red.

M

Management Information Base (MIB) La Base de Información de Gestión, es un tipo de base de datos que contiene información jerárquica, estructurada en forma de árbol, de todos los dispositivos gestionados en una

	red de comunicaciones. Es parte de la gestión de red definida en el modelo OSI. Define las variables usadas por el protocolo SNMP para supervisar y controlar los componentes de una red. Está compuesta por una serie de objetos que representan los dispositivos (como routers y switch) en la red. Cada objeto manejado en un MIB tiene un identificador de objeto único e incluye el tipo de objeto, el nivel de acceso (tal como lectura y escritura), restricciones de tamaño, y la información del rango del objeto.
Maximum Transfer Unit (MTU)	Es la Unidad máxima de transferencia que expresa el tamaño en bytes del datagrama más grande que puede pasar por una capa de un protocolo de comunicaciones. Los datagramas pueden pasar por varios tipos de redes con diferentes protocolos antes de llegar a su destino. Por tanto, para que un datagrama llegue sin fragmentación al destino, ha de ser menor o igual que el mínimo MTU de las redes por las que pase.
Métrica	Es el número que indica la distancia total de haber alcanzado el router destino y se usa para rutear protocolos que incluye: Número de dispositivos de la capa de red a lo largo del camino (cuenta del salto), Anchura de banda, Retraso, Carga, MTU y Costo.
Multihomed	Una red que pertenece a dos o más dominios de ruteo.
	N
Nodo	Es cualquier dispositivo con IPv6. Es decir el espacio real o abstracto en el que convergen parte de las conexiones de otros espacios reales o abstractos que comparten sus mismas características y que a su vez también son nodos. Todos estos nodos se interrelacionan entre sí de una manera no jerárquica y conforman lo que en términos sociológicos o matemáticos se llama red.
	P
Paquete	Es todo tipo de información que es transferida por Internet que está dividida en paquetes pequeños de información. Cada paquete posee una estructura y tamaño diferente dependiendo del protocolo que lo utilice. También existen los paquetes multicast que se encuentran encapsulados como paquetes comunes y viajan por Internet a través de dispositivos que soportan protocolos unicast.
Ping	Es una utilidad que comprueba el estado de la conexión con uno o varios equipos remotos por medio de los paquetes de solicitud de eco y de respuesta de eco (definidos en el

protocolo de red ICMP) para determinar si un sistema IP específico es accesible en una red. Es útil para diagnosticar los errores en redes o routers IP.

Muchas veces se utiliza para medir la latencia o tiempo que tardan en comunicarse dos puntos remotos, y por ello, se utiliza entre los aficionados a los juegos en red el término PING para referirse a la latencia de su conexión.

Protocolo de ruteo

Es la puesta en práctica de un algoritmo del ruteo en software o hardware. Este utiliza métrica para determinarse qué trayectoria va utilizar para transmitir un paquete a través de una red interna. Los protocolos de ruteo almacenan los resultados de estas métricas en una tabla de ruteo. Esto se desarrolla en la capa de red donde son usados para resolver peticiones de servicios de envío de paquetes de datos a través de diferentes redes. En el mercado existen muchos protocolos, algunos incluso propietarios de los fabricantes de routers.

R

Request For Comment (RFC)

La Petición de Comentarios, son documentos que se iniciaron en 1967 que describen los protocolos de Internet cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet (originalmente de ARPANET), que se explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades. Cada RFC tiene un título y un número asignado, que no puede repertirse ni eliminarse aunque el documento se quede obsoleto. Antes de que un documento tenga la consideración de RFC, debe seguir un proceso muy estricto para asegurar su calidad y coherencia. Cuando lo consigue, prácticamente ya es un protocolo formal al que probablemente se interpondrán pocas objeciones, por lo que el sentido de su nombre como petición de cometarios ha quedado prácticamente obsoleto, dado que las críticas y sugerencias se producen en las fases anteriores. De todos modos, el nombre de RFC se mantiene por razones históricas.

Router de frontera de área

Es un router que conecta el área del backbone con una o más áreas. Estos routers se utilizan muchas veces con el algoritmo del OSPF para cada área directamente conectada y en caso para el backbone. Los routers de frontera de área recogen la información alcanzable desde las áreas a las cuales están conectadas y la redistribuyen en el backbone. El Backbone redistribuye esta información a otras áreas.

Router exterior

Un router que maneja conexiones entre diversos ASs.

Router interior

Un router que maneja conexiones solamente dentro de un AS. Es decir un router que conecta a todas las subredes que pertenecen a la misma área. Estos routers se usan solamente en el caso del algoritmo OSPF. Los routers tienen interfaces en el backbone que pertenecen a esta categoría.

T

Tabla de ruteo

Es una lista de rutas e interfaces conocidas. Una tabla de ruteo es también una base de datos en la cual un protocolo del ruteo almacena la información sobre la topología de la capa de red del intranetwork.

Traceroute

Es una herramienta de la red de nodos usada para determinar la ruta tomada por los paquetes a través de una red del IP. IPv6 una variante, traceroute6, está también extensamente disponible.

X

Xerox Network Services (XNS)

Es el protocolo usado para proveer de ruteo y entrega de paquetes para redes de área local, prácticamente copiados en cierto punto por todos los sistemas de redes usados en los 80 y los 90 por 3Com y (con algunas modificaciones) otros sistemas comerciales que se volvieron más comunes que el XNS en sí mismo, incluyendo Ungermann-Bass Net/One, Novell NetWare, y Banyan VINES.

BIBLIOGRAFÍA

TESIS:

Ardon Marvin; Noviembre 2006

Diseño de una metodología que permita implementar el protocolo de Internet versión 6 en empresas o instituciones con aplicaciones basadas en el protocolo TCP/IP versión 4.

Universidad de El Salvador

LIBROS:

Blanchet, Marc; Enero 2006

Migrating to IPv6: A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks.

John Wiley & Sons Ltd

Brown, Sam; Browne, Brian; Parenti, Edgar Jr.; Enero 2002

Configuring IPv6 for Cisco IOS

Syngress Publishing, Inc. – United Status America

Hagen, Silvia; Mayo 2006

IPv6 Essentials

O'Reilly

Benedikt Stockebrand, Marzo 2007

IPv6 in Practice

Springer

KnowlledgeNet , 2003

Border Gateway Protocol (BGP), Student Guide V3.0

KnowlledgeNet.com

SITIOS WEB:

IPv6 Práctico

http://www.rediris.es/red/reuniones/IPv6practico.pdf

Mayo 2006

Introducción al Protocolo IPv6

http://internetng.dit.upm.es/ponencias-jing/2001/david-fernandez.PDF.

Marzo 2006

Equal cost routes support for RIP/RIPNG

http://tools.ietf.org/id/draft-janardhan-naveen-rtgwg-equalcostroutes-rip-00.txt

Junio 2007

IP Routing Fundamentals

http://www.cisco.com/cpress/cc/td/cpress/fund/iprf/index.htm

Febrero 2001

Quagga Routing Suite

http://www.quagga.net/

Septiembre 2007

IPv6 Forum

http://www.consulintel.es/html/ForoIPv6/RFCs.htm

Enero 2004

Implementing OSPF for IPv6

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_ospf3.htm#wp1154380

Agosto 2007

Consideraciones de diseño de OSPF

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/ffe9f01f-26e8-4e44-8cce-6ccc7ff4b960.mspx?mfr=true

Enero 2005

Consideraciones de diseño de RIP para IP

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/058245cf-e977-4bbb-9c74-974fc7468c5b.mspx?mfr=true

Enero 2005

Routers Hitachi

http://www.hitachi.com/New/cnews/E/2000/001129B.html

Noviembre 2000

Switch

http://www.tigerdirect.com/applications/searchtools/item-Details.asp?EdpNo=2911656&sku=D700-5560

Septiembre 2007

OSPFv3 Commands on Cisco IOS XR Software

http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.0/routing/command/reference/rr3ospf3.html

Mayo 2005

BGP: the Border Gateway Protocol Advanced Internet Routing Resources

http://www.bgp4.as/

Julio 2007

BGP Commands on Cisco IOS XR Software

http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.0/routing/command/reference/rr3bgp.html

Mayo 2005

RFC's:

RFC 1584 - Multicast Extensions to OSPF

Marzo 1994

RFC 1793 - Extending OSPF to Support Demand Circuits

Abril 1995

RFC 1930 - Guidelines for creation, selection, and registration of an Autonomous System (AS)

Marzo 1996

RFC 1998 - An Application of the BGP Community Attribute in Multi-home Routing

Agosto 1996

RFC 2080- RIPng for IPv6

Enero 1997

RFC 2328 - OSPF Version 2

Abril 1998

RFC 2453 - RIP Version 2

Noviembre 1998

RFC 2740 - OSPF for IPv6

Diciembre 1999

RFC 2863 - The Interfaces Group MIB

Junio 2000

RFC 3101 - The OSPF Not-So-Stubby Area (NSSA) Option

Enero 2003

RFC 4443 – Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

Marzo 2006

ENTREVISTAS:

Ing. Rafael Antonio Ibarra Fernández

Director SVNet y RAICES

ribarra@di.uca.edu.sv

Septiembre 13 del 2007

ANEXOS

ANEXO 1
SISTEMAS AUTÓNOMOS DE LOS PROVEEDORES DE SERVICIO DE INTERNET[39] EN EL SALVADOR

Desde 1993 hasta antes del 2007 el ente regulador facultado en El salvador para la asignación y administración de bloques de Direcciones IP (Protocolo de Internet) y recursos relacionados (Números Autónomos y Resolución Inversa), a los Proveedores de Servicio de Internet (ISP) se conoce como SVnet. Ésta organización, requirió del Registro de Direcciones de Internet Para América Latina y Caribe (LACNIC), la concesión de 65,000 direcciones IP categoría "B" para nuestro país, las cuales fueron fragmentadas en bloques de direcciones categoría[40] "C" entre ISP's, gobierno, empresas y otros. A las vez estan administrados bajo los Números Autónomos. En la actualidad, los entes interesados en la concesión de más bloques de direcciones IP's han venido solicitando la asignación de nuevos bloques de direcciones IP de forma directa y sin intermediario a LACNIC. Por lo cual el país cuenta con más de 65,000 direcciones IP entre proveedores locales y SVNet.

Los encargados de generar las condiciones necesarias para el buen funcionamiento de la red global y los diferentes servicios afines a nivel nacional como es el uso del servicio de Traducción de Direcciones de Red (NAT) tiene cerca de 20 proveedores de servicios de Internet y telefonía. En la tabla 24 se proporcionan algunos de los proveedores de servicios de Internet con sus correspondientes Números de Sistemas Autónomos (AS), bloques de direcciones (Múltiplos de 256) y la cantidad de direcciones asignadas del bloque administrado por SVNet.

[39]Fuente: Ing. Rafael Antonio Ibarra Fernández, Director SVNet y RAICES, Septiembre 13 del 2007, Entrevista.

[40]Son múltiplos de categoría "C" aunque no empiezan con prefijo correspondiente, pero así lo ha definido SVnet.

ID	Proveedores de Servicio de Internet	Sistemas Autónomos	Bloques de Direcciones Categoría "C"	Direcciones 168.243.x.x IPv4
1	AMERICATEL	17086	8	2,048
2	GCA TELECOM	27008	8	2,048
3	SALNET	16906	8	2,048
4	TELECAM	25927	8	2,048
5	INTERCOM	16592	16	4,096
6	TELEMOVIL	17079	16	4,096
7	SALTEL	14111	24	6,144
8	TELEFONICA	12127	32	8,192
9	TELECOM	22833	136	34,816
TOTAL			256	65,536
10	AMNET[41]	29009	16	2,048

Tabla 24: Sistemas Autónomos, Bloques y direcciones asignadas a los ISPs

BACKBONE DE EL SALVADOR[42]

En El Salvador, el desarrollo de la infraestructura de TIC se ha visto impulsado por la apertura y modernización del mercado de las telecomunicaciones, que generó las condiciones para un desarrollo de la Internet, telefonía fija y la liberalización de la telefonía

[41]El último ISP que a comenzado a tener mayor auge en el país es AMNET, aunque esta no fue asignado por SVnet sino directamente por LACNIC.

[42]Fuente: http://www.epais.gob.sv/index.htm; Infraestructura de TIC Nacional y Regional

móvil. Los servicios de acceso a Internet que esta disponible en El Salvador se encuentra conectada dentro de una red con una cobertura bastante amplia a nivel nacional. Desafortunadamente el ancho de banda y la variedad de servicios disponibles a través de esta red es limitado (especialmente en las zonas más remotas del país).

CONECTIVIDAD NACIONAL

El nivel de conectividad nacional se muestra en la figura 41 a través de un Backbone nacional que proporcione una plataforma tecnológica y un ancho de banda adecuados según los requerimientos de la línea estratégica del Gobierno Electrónico. Este Backbone esta diseñado teniendo en mente ISP's, gobierno, empresas y otros. A la vez están administrados bajo los Números Autónomos (A.S) que se encuentran en la tabla 24, aunque se considera su disponibilidad a otras instituciones públicas y privadas para potencializar los esfuerzos de otras líneas estratégicas.

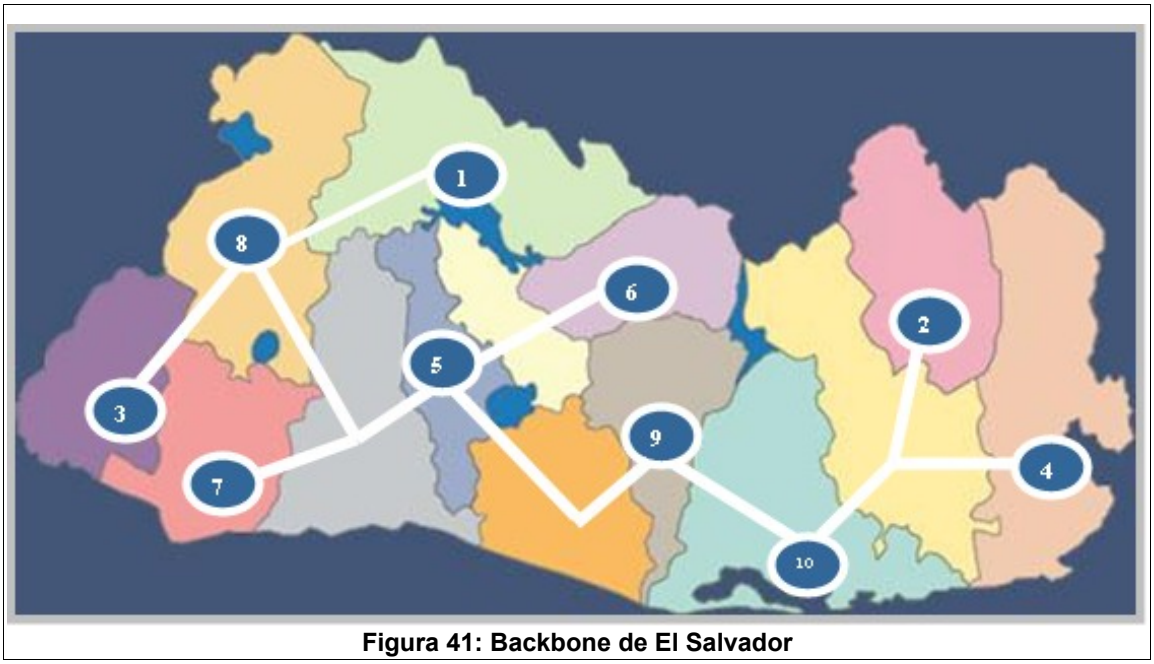

Figura 41: Backbone de El Salvador

Se estima que la operación y el acceso del Backbone funciona bajo un modelo similar al empleado en la red de cableado eléctrico o la red de telefonía fija. En este caso SVnet no tiene el control y administración del Backbone sino que cada proveedor de servicios de Internet, ofrece mejor servicio o mayor cobertura a sus clientes y hacen las inversiones necesarias en infraestructura.

El Salvador no cuenta con algún punto físico de encuentro (NAP) de los enlaces de los ISPs, en ningún sitio del territorio nacional, que sea favorable a los servicios que estos prestan, ni tampoco cuenta con una seguridad adecuada, para intercambiar por medio de los equipos el tráfico de Internet que va de la red de un ISP a la red de otro de los ISPs conectados. Sino que los paquetes de información (mensajes, archivos, respuestas de sitios Web, etc.) necesitan salir del país y volver a entrar, vía los enlaces dedicados, satelitales o de otro tipo, de estos ISPs, con el fin de llegar a la red de otro ISP.

CAPA DE DISTRIBUCIÓN

El modelo de la Red de Conectividad jerárquica considera que los servicios de comunicación son y seguirán siendo prestados por los operadores de telecomunicaciones, quienes funcionarán como Proveedores de Servicios de Internet de la Capa de Distribución.

En la actualidad los tipos de servicios brindados por las ISPs son:

- **Acceso Telefónico Inalámbricos:** Voz (CDMA, GSM, Trunking/Radio), Internet conmutado y dedicado.
- **Acceso Integrado por Cable:** Voz (Telefonía), Internet y Televisión.
- **xDSL:** Internet y Telefonía.
- **Servicios Wi-Fi** (Operando desde 2003): En Centros Comerciales, Aeropuerto

Internacional de El Salvador y en Hoteles.

Aunque estos servicios son muy variados los precios son muchas veces relativamente elevados y la gama total de los servicios ofrecidos en muchos casos está limitada a las zonas metropolitanas del país.

CAPA DE ACCESO

La Capa de Acceso abarca los elementos tecnológicos que manejan enlaces de telecomunicaciones entre los usuarios finales y el último nodo de la red. Sus principales componentes son los medios de comunicación de la última milla que coexisten: Par de cobre, Cable coaxial, Fibra óptica, Radio frecuencia e Inalámbricas.

Los medios conectados a ellos permiten el acceso con un grado de seguridad y estabilidad acorde al medio que se este ocupando. Así también, el ancho de banda depende de tecnologías de acceso como:

- Líneas de abonado digital (DSL)
- Sistemas de terminación de módem por cable (CMTS) o UMTS que fue concebido para servicios de voz y de datos.

ANEXO 2
DISPOSITIVOS QUE SOPORTAN IPV6

En la tabla 25 se muestran dispositivos (Router y Switch) que soportan IPv6, en la cual se especifica el modelo, marca y una descripción de lo que soportan.

Modelo	Marca	Descripción
Routers Serie GR2000	Hitachi	Protocolos que soporta: Interior: RIPv1/v2,RIPng, OSPFv2, OSPFv3 Exterior: BGP4, BGP4+
Routers series AX7800R	Alaxala	Los protocolos que soporta RIPng, OSPFv3, IS-IS y multicast teniendo en cuenta la construcción de una variedad amplia de las redes IPv6.
Router 4134	Nortel	Su diseño modular apoya una gama de los servicios de red avanzados - incluyendo el ruteo IPv4/IPv6, WAN de alto rendimiento, VoIP y seguridad - en una sola plataforma integrada.
Router 857w	CISCO	Posee soporte IPv6, protección firewall, soporte de DHCP, soporte de NAT, VPN, soporte para PAT, señal ascendente automática.
Router IMR 640 Multi-servicio	Foundry NetIron	Soporta Ruteo con apilados duales en IPv4/IPv6 con hasta 500 pares del BGP y 4 millones de rutas del BGP.
Switch serie 8800	3Com	Soporte para los protocolos de ruteo en IPv6: ruteo estático, RIPng, OSPFv3, BGP4+. Además soporta:PIM-SMv6, PIM-DMv6 , Dual Stack, IPv6 Neighbor Discovery, IPv6 Path MTU Discovery.
Switch serie DGS-3627	D-Link	Soporte para protocolos avanzados de Capa 3 RIP, OSPF, VRRP, IGMP, DVMRP, PIM-DM e PIM-SM. Enrutamiento completamente dinámico con soporte para IPv4 e IPv6.
Switch 9408sl	Hewlett-Packard	Permite a los gestores de red, construir redes de alto rendimiento, escalables y de alta disponibilidad que sean compatibles con las tecnologías emergentes como la velocidad del cable de 10 Gigabits e IPv6.

Tabla 25: Dispositivos que soportan IPv6

ANEXO 3
PROTOCOLO DE MENSAJE DE CONTROL DE INTERNET

1. INTRODUCCIÓN ICMPV6[43]

El Protocolo de Mensajes de Control y Error de Internet ICMP para IPv6, es la versión que ha sido adaptada de sus antecesores para el protocolo IPv6. Es de características similares a UDP (Protocolo de Datos de Usuario)[44], pero con un formato mucho más simple, cuyo provecho no está en el transporte de datos de usuario, sino en controlar si un paquete no puede alcanzar su destino, si su vida ha expirado, si el encabezado lleva un valor no permitido, si es un paquete de petición o respuesta eco, entre otras. Es decir, que su función radica en manejar e informar mensajes de error y de control necesarios para los sistemas de una red cualquiera, cuando un paquete no puede ser procesado apropiadamente informando con ellos a la fuente que lo origina para que evite o corrija el problema detectado. ICMP proporciona así una comunicación entre el software IP de un nodo y el mismo software en otro. Por ejemplo, si un router no puede enviar un paquete porqué este es muy grande se envía por otra red. Este envía de regreso un mensaje ICMP al router origen. El router origen puede usar este mensaje ICMP para determinar el mejor tamaño del paquete y luego reenviar los datos.

El protocolo ICMP solamente informa de incidencias en la entrega de paquetes o de errores en la red en general, pero no toma decisión al respecto. Esto es tarea de las capas superiores.

El ICMP además de basarse en funciones de diagnosticó, tal como PING, que utiliza los mensajes de Petición (Solicitud) y Respuesta de Eco ICMP, prueba la disponibilidad de un nodo.

[43] ICMPv6 – Del inglés Internet Control Message Protocol
[44] UDP – Del inglés User Datagram Protocol

2. GENERALIDADES ICMPV6

ICMPv6 es mucho más poderoso que su versión anterior y contiene nuevos funcionamientos. Por ejemplo, el Protocolo de gestión de grupos de Internet (IGMP)[45] que funciona como administrador de grupos multicast afiliado con IPv4 ya viene incorporado dentro de ICMPv6.

El Descubrimiento de Vecinos (ND[46]) esta presente; este se usa en los mensajes ICMPv6 en un orden determinado por la capa de enlace para las direcciones de sus vecinos fijados al mismo enlace, encontrar-routers, que conserva el camino o la ruta de sus vecinos que son alcanzables, y detecta los cambios de direcciones en la capa de enlace. ICMPv6 además soporta IPv6 móvil, debe ser implementado totalmente en cada nodo IPv6. Esto se encuentra detallado en el RFC 4443.

3. REGLAS QUE ADMINISTRAN EL PROCESAMIENTO ICMPV6

El procesamiento de paquetes ICMP esta gobernado por una serie de reglas. Estas pueden ser encontradas en el RFC 4443 y se resumen a continuación:

- Si un nodo recibe un mensaje de error ICMPv6 y desconoce su tipo, este debe pasar a la capa-superior.
- Si un nodo recibe un mensaje informativo ICMPv6 y desconoce su tipo, este debe ser descartado silenciosamente.
- El paquete de mensaje de error ICMPv6 puede ser causado por muchas razones y serán incluidas dentro del cuerpo del mensaje. El paquete ICMPv6 no puede exceder de un mínimo MTU.
- Si el error del mensaje tiene que ser pasado al protocolo de capa-superior, el tipo de protocolos es determinado por extraerse de un paquete original (presente en el cuerpo de mensaje de error ICMPv6). En el caso que el tipo de protocolo no pueda ser encontrar en el cuerpo del mensaje ICMPv6, el mensaje ICMPv6 es

[45] IGMP – Del inglés *Internet Group Management Protocol*
[46] ND – Del inglés *Neighbor discovery*

descartado silenciosamente.

Un mensaje ICMPv6 no debe ser enviado bajo ninguno de los siguientes casos:

- Como resultado de un mensaje de error ICMPv6
- Como resultado de un mensaje redireccionado ICMPv6
- Como resultado de un paquete enviado por una dirección multicast IPv6. Aquí encontramos dos excepciones :
  - El paquete de mensaje es demasiado grande y este es usado para el Descubrimiento de Rutas MTU (PMTU)[47].
  - El Problema de Parámetros con el valor del código de 2 para una reconocida opción IPv6.

Cada nodo IPv6 debe poner en ejecución tarifa-limitadora de funciones que limiten el índice de los mensajes ICMPv6 que envía, y deben ser configurables. Si esta función se pone en ejecución correctamente, protege contra la negación de los ataques del servicio.

4. FORMATO GENERAL DEL MENSAJE ICMPV6

Existen dos clases mensajes en ICMPv6:

- Mensajes de error del ICMPv6
- Mensajes informativos del ICMPv6

Todos los tipos de mensajes ICMPv6 tiene una estructura universal del encabezado. Tal y como se observa en la figura 42 los principales campos son Tipo, Código, Suma de Verificación (Checksum) y Cuerpo del Mensaje. A continuación en la tabla 26 se presenta la descripción de los campos del formato general del mensaje ICMPv6.

[47] PMTU – Del inglés Path Maximum Transfer Unit

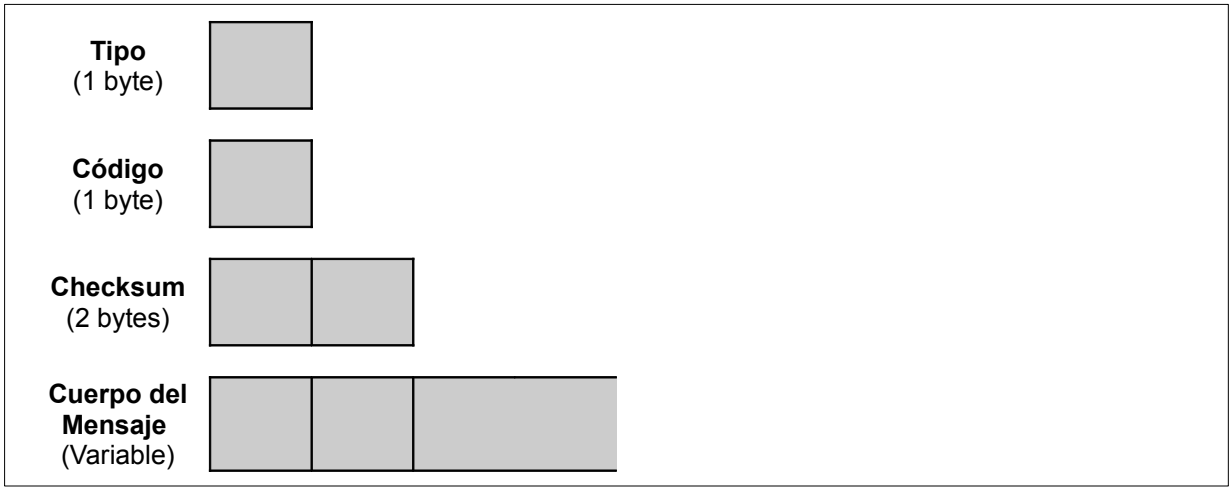

Figura 42: Formato Universal del mensaje ICMPv6

Campos del Formato General de Mensajes ICMPv6		
Nombre del Campo	**Byte Reservado**	**Descripción**
Tipo	1	Este campo especifica el tipo de mensaje y permite determinar el formato del resto del mensaje. Este tipo de mensaje se identifica por tener un campo con un valor ente 0-127 para los mensajes de error y de 128 -255 para los mensajes informativos.
Código	1	Este campo tiene una dependencia correspondiente al valor del campo Tipo de mensaje, añadiéndole otro tipo de información.
Suma de Verificación	2	Este campo es usado para detectar corrupción en los datos del encabezado ICMPv6 y en parte del encabezado IPv6. Para el cálculo de este, un nodo debe determinar la dirección origen y destino en el encabezado IPv6. Si el nodo posee más de una dirección unicast, ahí se escoge la regla de dirección.
Cuerpo del Mensaje	Variable	Este campo esta identificado por su dependencia sobre otros campos. Cual sea el Tipo y Código, el cuerpo del mensaje podrá llevar diferentes datos. Para el caso de un mensaje de error, podrá contener muchas posibilidades que el mensaje de paquete invocado auxilie en el problema. El tamaño total del paquete ICMPv6 no podrá exceder el mínimo de Unidad de Transmisión Máxima (MTU)[48] para IPv6, que es de 1280 bytes.

Tabla 26: Campos del formato general de mensajes ICMPv6

[48] MTU - Del inglés *Maximum Transfer Unit*

5. FUNCIONAMIENTO DE LOS TIPOS DE MENSAJES ICMPV6

Este protocolo define dos tipos de mensajes, a los cuales ICMPv6 recurre para ver la disponibilidad de un nodo. Estos mensajes se encuentran clasificados en 2 tipos:

- Mensajes de Error[49]
- Mensajes Informativos[50]

A. Mensajes de Error

Este ocurre cuando un nodo debe de resolver un paquete. El bit de capa-superior tiene un valor de cero dependiendo del campo Tipo de mensaje. Es decir, que un mensaje de error sucede cuando el bit más significativo del campo Tipo es cero. Los nodos que envían un mensaje de error ICMPv6 siempre incluyen en el datagrama original de carga el mensaje ICMP como se muestra en la figura 43. Sin embargo, la resolución del tamaño del datagrama ICMP es menor o igual al MTU IPv6, para garantizar que bajo cualquier circunstancia el mensaje de error alcanza el origen.

Al introducir el datagrama original IPv6 en el mensaje de error ICMP se permite que el nodo origen reciba el mensaje de error y halle el contexto del datagrama original (dirección origen, dirección destino y puertos), el proceso de corrección de error y la capa superior lo ponen a funcionar correctamente complementando el procedimiento en el nivel de aplicación tal y como se muestra en la figura 43.

[49] Mensajes de error – Del inglés *error messages*
[50] Mensajes Informativos – Del inglés *informational messages*

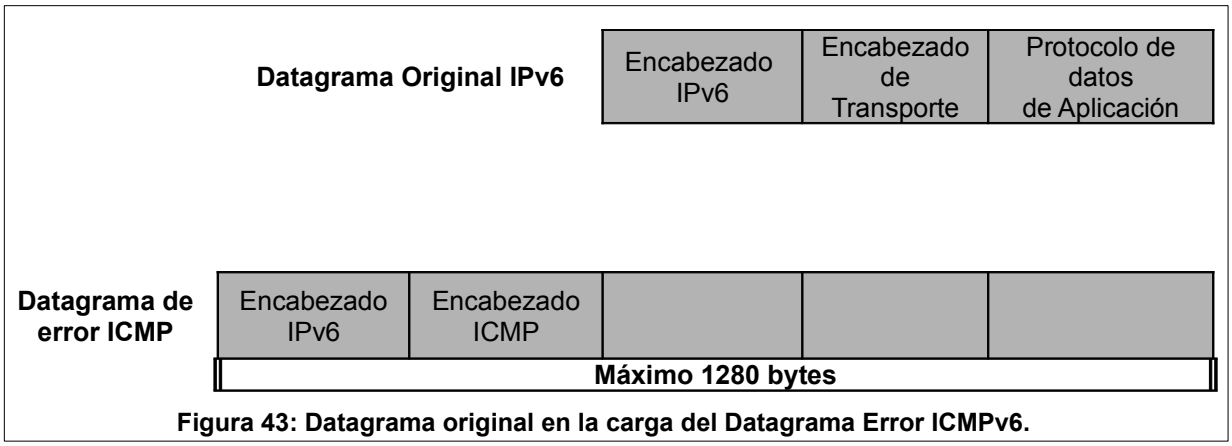

Figura 43: Datagrama original en la carga del Datagrama Error ICMPv6.

Un ejemplo de este tipo de mensaje lo encontramos ilustrado en la figura 44, en la cual el nodo A envía un datagrama a B (1). Pero en el router R no puede enviar el datagrama porque B es inalcanzable. (2)

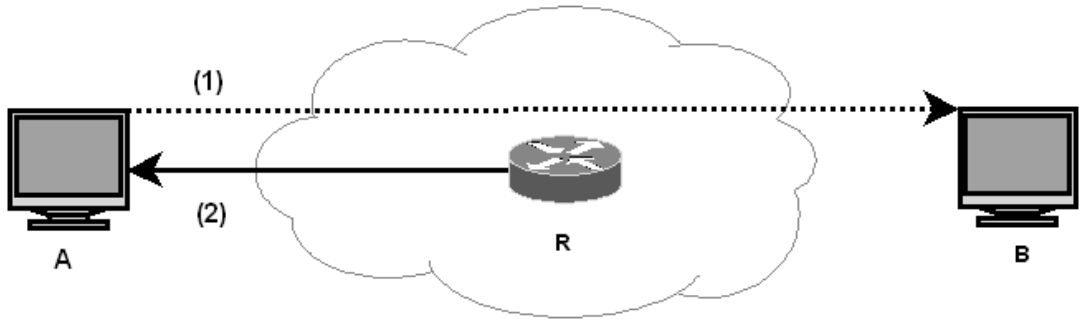

Figura 44: Mensaje ICMP enviado por un nodo intermedio

La figura 45 Muestra el funcionamiento de los tipos de mensajes de error ICMPv6. Para cada uno de estos tipos de mensaje de error se determina un valor del campo del encabezado ICMPv6 tal y como se muestra en la tabla 28

Mensajes de Error ICMPv6		
Tipo	**Definición**	**Funcionamiento**
1	**Destino inalcanzable** ***Destination Unreachabe***	Son enviados por nodos intermedios cuando estos no pueden alcanzar el destino del datagrama. Cuatro eventos son definidos para este y se explican en tabla 28
2	**Paquete demasiado grande** ***Packet Too Big***	Una máquina envía un paquete cuyo tamaño es la MTU de su nivel de enlace. Si un nodo intermedio está conectado a un medio con MTU menor, no puede reenviarlo y devolverá un paquete de error ICMPv6 con el valor de la MTU. Entonces la máquina realiza otro intento disminuyendo el tamaño del paquete al valor de MTU recibido. Este proceso continúa hasta que el paquete llega al destino y no se recibe ningún error.
3	**Tiempo excedido** ***Time Exceded***	Un nodo al recibir un mensaje de error ICMPv6 por tiempo excedido debe informar al proceso de nivel superior.
4	**Problema de parámetro** ***Parameter Problem***	Un nodo al recibir un mensaje de error ICMPv6 por problema de parámetros debe informar al proceso de nivel superior.

Figura 45: Tipos de Mensaje de error ICMPv6

B. Mensajes Informativos

Este ocurre cuando un nodo descarta o ignora un paquete. Al igual que los mensajes de error depende de su campo Tipo de mensaje, aunque el bit de nivel-superior tiene un valor de uno.

Este protocolo define 3 tipos de mensajes de mayor precedencia, a los cuales ICMPv6 recurre para ver la disponibilidad de un nodo. Estos mensajes se encuentran clasificados en 3 tipos de mensajes principales:

- Rastreador de paquetes en redes (PING)
- Descubrimiento de Vecinos (ND)
- Descubrimiento de Escuchas Multicast (MLD)

Otros mensajes informativos son usados por ICMPv6 pero generalmente los que con frecuencia usa ICMPv6 son los expuestos en esta sección. En la tabla 27 se exponen el funcionamiento de cada uno de estos mensajes.

Mensajes Informativos ICMPv6	
Tipo	**Funcionamiento**
Rastreador de paquetes en redes (Ping)[51]	Este permite comprobar si un nodo en particular está conectado a la misma red que cualquier otro nodo, el nodo origen utiliza un mensaje de Petición de Eco hacia un nodo destino específico. El nodo destino, si está disponible, responde con un mensaje de Respuesta de Eco. De tal manera que determina el tiempo que tarda un paquete enviado en llegar hasta el destino. Se utiliza como una herramienta de diagnóstico.
Descubrimiento de Escuchas Multicast (MLD)[52]	Este permite que cada router IPv6 descubra la presencia de escuchas multicast en los enlaces a los que están conectados directamente, utilizando mensajes ICMPv6. Es decir, que gestiona la pertenencia a un grupo multicast.
Descubrimiento de Vecinos (ND)[53]	Este permite que todos los nodos (host o routers) con IPv6 utilicen el descubrimiento de vecindario para determinar las direcciones de la capa de enlace de todos los otros nodos que se encuentran en la interfaz de red y verifiquen si estos nodos continúan siendo alcanzables. Es decir, que gestiona la comunicación nodo a nodo en un mismo enlace

Tabla 27: Tipos de Mensajes informativos ICMPv6

6. FORMATOS ESPECIFICOS PARA LOS TIPOS DE MENSAJES ICMPV6

Este protocolo tiene 2 tipos de mensajes para los cuales cada uno de ellos se precisa un formato similar al formato general del mensaje ICMPv6. Sus diferencias radican en la adición de ciertos campos con funcionalidades específicas, aunque la estructura del formato general del mensaje ICMPv6, en esencia se conserva. En esta sección se resumen ambas estructuras de los formatos de mensaje tanto de error como informativos, tomando en cuenta los cambios mínimos presentes en cada uno de ellos.

A. Formato de Mensajes de Error

Este apartado se centra en todos los mensajes de error existentes para ICMPv6. El formato de estos tipos de mensajes tienen igual estructura, no obstante se diferencian por

[51] PING – Del inglés *Packet Internet Groper*
[52] MLD – Del inglés *Multicast Listener Discovery*
[53] ND – Del inglés *Neighbor Discovery*

tener un funcionamiento distinto en los campo Tipo, Número Secuencial y el campo Datos tal como se muestran en la figura 46 y tabla 28

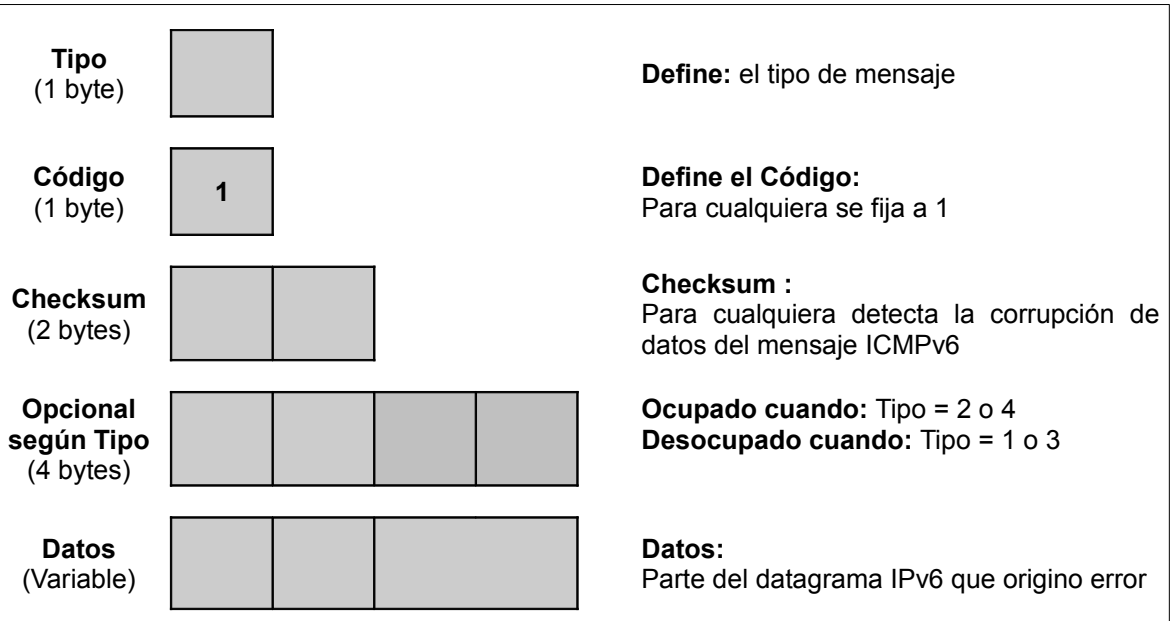

Figura 46: Formato de mensajes de error ICMPv6

Eventos del Tipo de Mensajes de error ICMPv6				
Tipo	Código	Definición	Cuerpo del Mensaje	
			Opcional	Datos
1	0	No hay ruta al destino	Sin usar. Puede ser 0. Ignora por destino.	Parte del datagrama IPv6 que origino Error
	1	Comunicación prohibida (firewall).		
	2	Sin usar		
	3	Dirección inalcanzable (nivel-enlace imposible resolver)		
	4	Puerto inalcanzable		
2	0	Excepción de regla RFC 4443 para ICMPv6	El MTU del enlace del próximo salto.	
3	0	Excedido el número de saltos.	Sin usar. Puede ser 0. Ignora por destino.	
	1	Tiempo excedido en el reensamblado de fragmentos (unos pocos minutos)		
4	0	Campo de cabecera erróneo	Apunta al octeto que ha provocado el error.	
	1	Campo siguiente cabecera desconocido		
	2	Opción de IPv6 desconocida		

Tabla 28: Eventos del los tipos de Mensajes de error ICMPv6

B. Formato de Mensajes Informativos

Esta sección se centra en los tipos de mensajes informativos que son los que frecuentemente se utilizan por ping. El formato de mensajes de Petición y Respuesta de Eco, tienen los mismos campos con funcionalidad diferente entre si. No obstante se diferencian por tener un funcionamiento distinto en los campos: Tipo, Identificador, Número Secuencial y el campo Datos tal como se muestran en la figura 47.

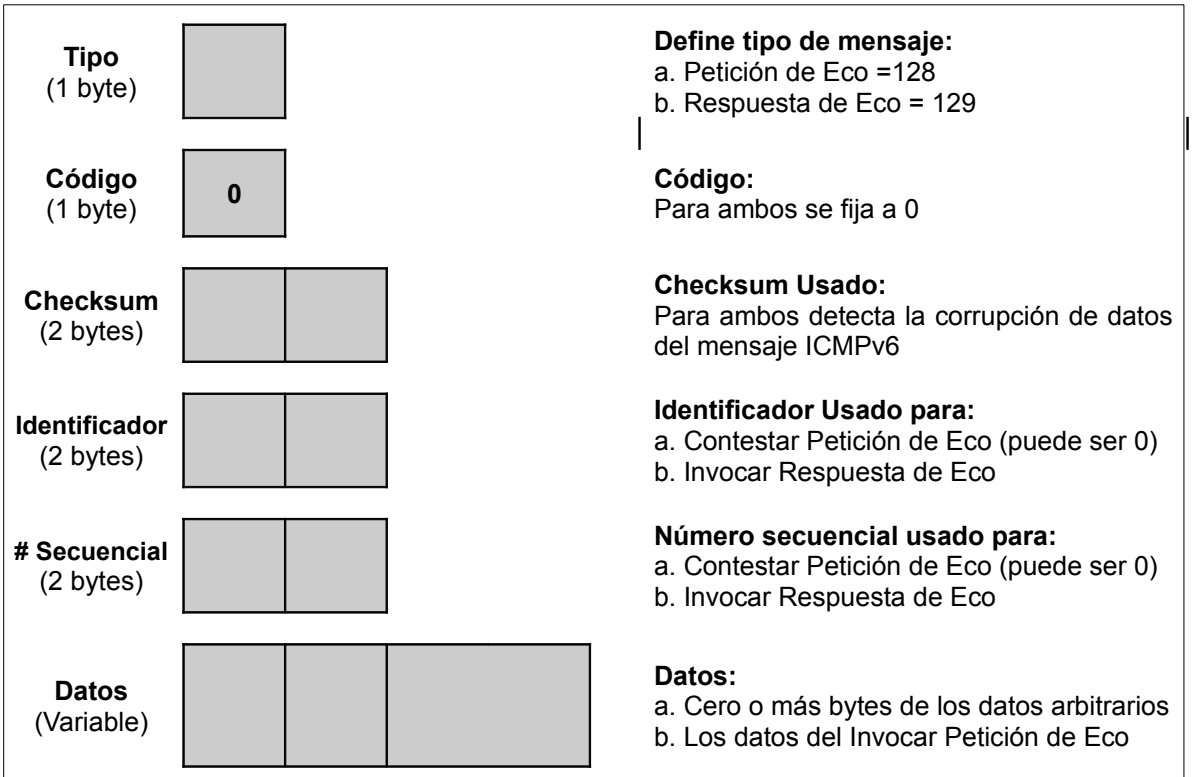

Figura 47: Formato de mensajes Informativos basados en Petición y Respuesta Eco.

Los campos adicionados al formato de mensajes informativos del formato general ICMPv6 son los campos Identificador y Número Secuencial. El campo Identificador, que consiste en enviar y recibir procesos ping de forma simultánea o no simultanea. Es decir, que es usado para contestar petición o invocar respuesta de eco. El campo de Número Secuencial que a diferencia del campo Identificador, se incrementa con cada mensaje que se envía, permitiendo saber si se han o no perdido mensajes. Además este maneja diferentes tipos de eventos aunque los que se aplican a menudo son los mostrados en tabla 29.

Eventos del Tipo de Mensajes de error ICMPv6			
Tipo[54]	**Código**	**Definición**	**RFC**
PING	128	Petición de eco	4443
	129	Respuesta de eco	
MLD	130	Consulta de escucha multicast	2710/`3810
	131	Reporte de Escucha Multicast	2710
	132	Escucha multicast realizada	
ND	133	Petición de Router	2461
	134	Anuncio de Router	
	135	Petición de Vecino	
	136	Anuncio de Vecino	
	137	Redirección de mensaje	

Tabla 29: Eventos del Tipo de Mensajes Informativos ICMPv6

7. RASTREADOR DE PAQUETES EN REDES (PING)

Hay dos tipos de mensajes informativos definidos para este, los cuales son Mensajes de Petición o de Respuesta de Eco. Ambas clases de mensajes informativos son los comandos más comúnmente utilizado para el protocolo TCP/IP como Ping. En la tabla 30 se describe el funcionamiento de cada uno de estos tipos de mensajes informativos PING.

[54] Este campo tipo se fija a cero para el caso de los mensajes informativos

Tipos de mensajes PING	
Tipo de Mensaje	**Funcionamiento**
Petición o solicitud de Eco	Cumple una función interlocutora, con propósitos de diagnóstico, emitiendo y recibiendo peticiones de eco.
	No hay limitación en la cantidad de datos que se puede poner en un mensaje de petición de eco y puede ser enviado a cualquier dirección IPv6 válida.
Respuesta de Eco	Al igual que la petición de eco tiene una función interlocutora, que trabaja también con propósitos de diagnóstico, recibiendo peticiones de eco y emitiendo respuestas de eco.
	No hay limitación en lo que se refiere a la cantidad de datos que se puede poner en un mensaje de respuesta de eco.
	La dirección de origen que deben incluir los mensajes respuesta de eco será, en el caso de un mensaje de petición de eco a una dirección unicast, la misma dirección destino de este mensaje. En el caso de un mensaje de petición de eco a una dirección multicast o anycast, la dirección destino del mensaje de respuesta de eco a enviar será una dirección unicast perteneciente a la interfaz en la cual dicho mensaje de petición de eco fue recibido.

Tabla 30: Tipos de mensajes informativos PING

Los mensajes de Respuesta y Petición ICMPv6 pueden ser autenticadas, usando un encabezado de autenticación IPv6. Esto significa que un nodo puede estar configurado, ignorado o no tener una autenticación ping ICMPv6, que a la vez proporcione protección contra ataques a ICMPv6.

8. DESCUBRIMIENTO DE VECINOS (ND)

Estos son especificados en RFC 2461. El nuevo funcionamiento de esta incluye la combinación de ARP y descubrimiento de Router y mensajes de redirección del router ICMP con IPv4, esto no significa detectar si un vecino es o no inalcanzable. Con el protocolo de descubrimiento de vecinos, un vecino inalcanzable detecta el mecanismo que tiene que ser definido. El Duplicado de direcciones destino (DAD)[55] tiene que implementar también, los nodos de descubrimiento de vecinos usados para IPv6 que tienen como propósito:

- Determinar el nivel 2 de direcciones de los nodos encontrados en el mismo enlace.

[55] DAD – del inglés *Duplicate IP Address Detection*

- Encontrar routers vecinos que puede enviar los paquetes.
- Cuidar de ataques de cualquier vecino que son y no son inalcanzables, y detectar cambios dentro de la capa-enlace de direcciones.

El Mecanismos que incluye el protocolo de descubrimiento de vecinos se basa en los siguientes 5 mensajes ICMPv6: dos mensajes de Petición y Anuncio de Routers, dos mensajes de Petición y Anuncio de Vecinos y un Redireccionamiento de mensaje ICMP. El funcionamiento de cada uno de estos tipos mensajes ICMPv6 se encuentran explicados en la tabla 31 y en la tabla 32 se muestra el mecanismo de descubrimiento de vecino.

Mensajes de descubrimiento de vecinos ICMPv6	
Mensajes	**Funcionamiento**
Petición de router (Router Solicitation)	Enviado por las máquinas para descubrir rápidamente los routers que hay en ese enlace, lo cuáles enviarán como respuesta un mensaje de anuncio de router. (Se envía al grupo multicast al que están conectados todos los routers en ese enlace de red).
Anuncio de router (Router Advertisement)	Enviado periódicamente por los routers (dirigido al grupo multicast de todas las máquinas de ese enlace) o como respuesta a un mensaje de solicitud (dirigido a la máquina que hizo la solicitud). Avisa de la existencia de un router, del prefijo de red (para autoconfiguración) y otros parámetros tales como límite de saltos y MTU del enlace.
Petición de vecino (Neighbor Solicitation)	Enviado a un vecino para verificar su existencia y solicitar que transmita un mensaje de anuncio de vecino.
Anuncio de vecino (Neighbor Advertisement)	Enviado por una máquina para indicar su existencia, en respuesta de un mensaje de anuncio de vecino y proporcionar información sobre esa máquina.
Mensaje de Redirección (Redirect)	Enviado por un router a un host para indicar un mejor método para encaminar paquetes hacia un destino determinado.

Tabla 31: Bases del Descubrimiento de Vecinos

Mecanismo del Descubrimiento de Vecinos		
Pasos		**Proceso**
1	**Descubrimiento de routers**	Las Máquinas localizan los routers de su enlace.
2	**Descubrimiento de prefijos**	Las máquinas descubren los prefijos de red de las máquinas que están conectadas a su mismo nivel de enlace con el propósito de poder distinguir entre máquinas directamente conectadas y máquinas que requieren el encaminamiento de un router para poder comunicarse.
3	**Descubrimiento de parámetros**	Descubrimiento de MTU de nivel de enlace y límite de saltos para la cabecera IP.
4	**Autoconfiguración de direcciones**	Configuración automática de una dirección
5	**Resolución de direcciones**	Descubrimiento de la dirección de nivel de enlace.
6	**Determinación del siguiente salto**	Algoritmo para determinar cuál es la dirección IP del vecino que se encargará de reenviar el paquete hacia el destino.
7	**Detección de desconexión de vecino**	El router sustancialmente mejora la entrega de paquetes en caso que falle la interfaz de enlace o algún router que cambio esa dirección de Capa-Enlace. este, al mismo tiempo detecta la falla de conectividad y de tráfico que no se envió al vecino inalcanzable. Además, detecta fallas de routers y swiches conectados, definiendo junto al retransmitido mensaje de solución de vecinos un tiempo en milésimas de segundos.
8	**Detección de direcciones duplicadas (DAD)**	Un router usa una dirección especificada como una dirección origen, el nivel-enlace del router debe ser usado en soluciones multicast y puede ser usado en soluciones unicast
9	**Redirección Redirect**	Un router informa a una máquina que existe otro router para ser utilizado como primer salto en el envío de un paquete hacia un destino.

Tabla 32: Mecanismo de Descubrimiento de Vecinos

9. GESTIÓN DE DIRECCIONES MULTICAST (MLD)

Grupo de Direcciones Multicast son usados como un grupo identificador para un grupo de nodos. Un protocolo requiere manejar la eficiencia de ruteo de paquetes con un grupo de direcciones multicast como un destino.

IPv6 utiliza mensajes ICMPv6 para tener el mismo funcionamiento que sus versiones anteriores; su desarrollo se baso en especificaciones IGMPv2. Esta es ahora llamada

Escucha de Descubriendo de Vecinos (MLD)[56] y se define en el RFC 2710.

Todos los mensajes MLD son enviados con un enlace-local de dirección origen IPv6 y un salto limitado de uno. Si el paquete tiene un Salto-por-Salto en el encabezado Opciones, este tiene activada la Bandera de Alerta del Router. Así, los routers no podrán ignorar el paquete, en particular si estos no están escuchando al grupo de direcciones multicast en cuestión. Los tres tipos de mensajes tienen igual formato, el cual se muestra en la figura 48.

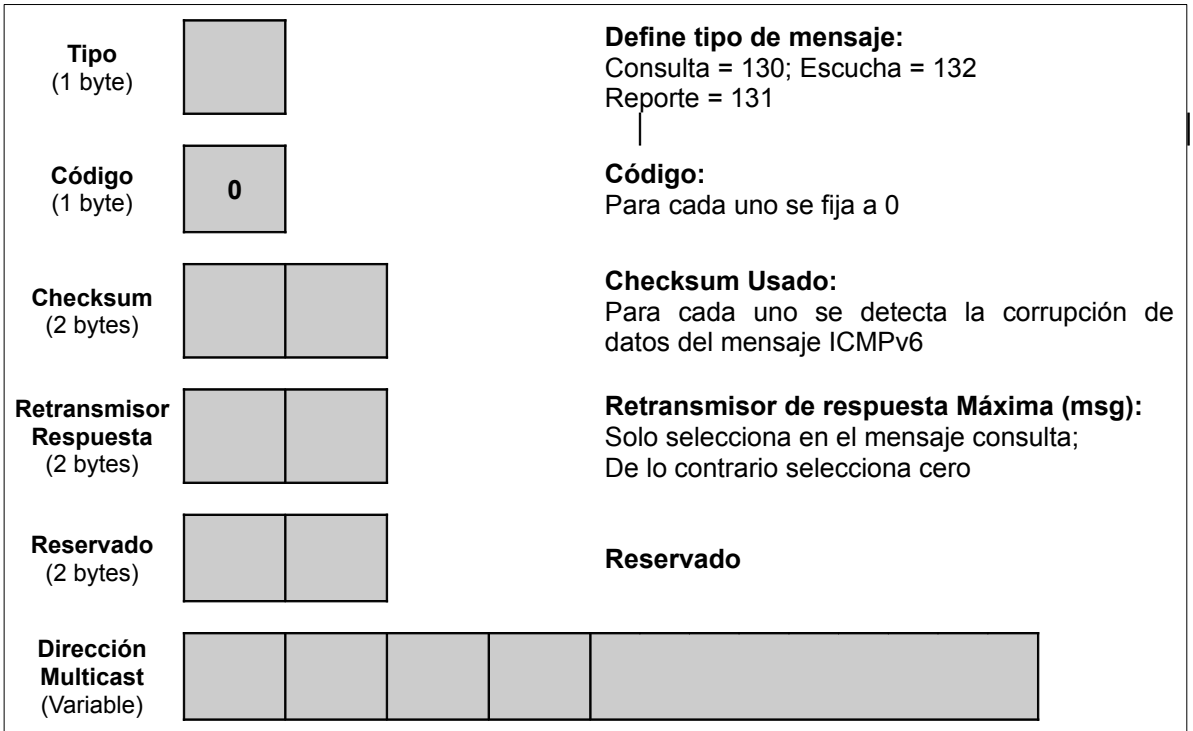

Figura 48: Formato del Mensaje MLD

Los routers usan MLD para descubrir cual dirección multicast tiene escuchas en cada uno de esos enlaces. Para cada enlace, el router mantiene una lista de direcciones escuchas.

Las consultas generales son enviadas al enlace-local para que alcance todos los nodos multicast de dirección FF02::1. Cualquier estación que quiera enviar un reporte en respuesta a una consulta iniciada, el temporalizador donde este recibe la consulta supone

[56] MLD – Del inglés *Multicast Listener Discovery*

esperé a un retransmisor (relay) aleatorio antes de enviar el reporte. Si dentro del retransmisor, la estación observa otras estaciones envía un reporte, este reporte detiene el proceso. Así, pueden ser evitados múltiples reportes para la misma dirección. El grupo de miembros responsables de reportes y terminaciones envían a la dirección en cuestión.

El enlace-local alcanza todos los nodos (FF02::1) si es una dirección especial. Esta nunca envía a sus miembros reportes o un mensaje de realizado. Si una dirección tiene un alcance de 1 (nodo-local), los mensajes MLD nunca son enviados. La tabla 33 resumen el tipo de mensaje, campo y direcciones destino multicast.

Tipo de Mensaje	Campo de Dirección Multicast	Dirección Destino IPv6
Consulta-General	Seleccionar 0	Enlace-local alcance todos los nodos (FF02::1)
Consulta especial	Grupo de direcciones Multicast Requeridas	Dirección multicast ha ser consultada
Reporte	Grupo Multicast (miembro escucha o grupo permitido)	Dirección multicast a ser reportada
Realizado (done)		Enlace-local enlace todos los routers (FF02::2)

Tabla 33: Tipo de mensaje, campos y destino multicast.