Algoritmos de Enrutamiento Dinámico
Dynamic Routing Algorithms

Angely Yahayra Mendez Cruz
Escuela de Informática,
Universidad Nacional de Trujillo
La Libertad, Perú
t052701020@unitru.edu.pe

Ciara Solange Mendez Cruz
Escuela de Informática,
Universidad Nacional de Trujillo,
La Libertad, Perú
t022700920@unitru.edu.pe

Leslie Valentina Padilla Leyva
Escuela de Informática,
Universidad Nacional de Trujillo
La Libertad, Perú
t032700320@unitru.edu.pe

Carlos Marcial Pérez Horna
Escuela de Informática,
Universidad Nacional de Trujillo
La Libertad, Perú
t012701120@unitru.edu.pe

Angie Tatiana Recalde Monzon
Escuela de Informática,
Universidad Nacional de Trujillo,
La Libertad, Perú
t512700720@unitru.edu.pe

Alvaro Joao Rodriguez Celada
Escuela de Informática,
Universidad Nacional de Trujillo
La Libertad, Perú
t052700620@unitru.edu.pe

Resumen—**En nuestra vida cotidiana, interactuamos con diversas redes de datos, que parten desde pequeñas a grandes, es decir, de redes locales a globales. Estas redes pueden contar con múltiples enrutadores para satisfacer las necesidades de comunicación entre diversos computadores. En redes extensas con numerosas subredes, presenta dificultad en el caso de Mantenimiento e inserción,más que todo en enrutamiento estáticas resulta costoso en términos administrativos y operativos. Esta sobrecarga operativa se vuelve especialmente complicada cuando ocurren cambios en la red. Los protocolos de enrutamiento dinámico ayudan a disminuir dichas tareas mencionadas anteriormente y que la red presente. En este artículo, se lleva a cabo una revisión sistemática de los protocolos de enrutamiento dinámico basados en algoritmos tales como RIPV2, EIGRP, OSPF, IS-IS y BGP.**

Palabras Claves—***Enrutamiento dinámico, algoritmos, protocolos, redes.***

Abstract—**In our daily lives, we interact with various data networks, ranging from small to large, that is, from local to global networks. These networks can have multiple routers to satisfy the communication needs between different computers. In large networks with many subnets, it is difficult in the case of maintenance and insertion, especially in static routing it is expensive in administrative and operational terms. This operational overhead becomes especially complicated when changes occur in the network. Dynamic routing protocols help to reduce the aforementioned tasks and that the network presents. In this article, a systematic review of dynamic routing protocols based on algorithms such as RIPV2, EIGRP, OSPF, IS-IS, and BGP is carried out.**

Keywords—***Dynamic routing, algorithms, protocols, networks.***

I. Introducción

Sabemos que Internet es la red más extensa de todas y, antes de que la información se envíe a través de ella, se divide en numerosos paquetes. Estos paquetes son transmitidos entre redes por dispositivos intermedios (routers o enrutadores). Su objetivo principal es aprender las rutas para llegar y comunicarse con otras redes y así facilitar la transferencia de paquetes de datos entre ellas, en un proceso conocido como enrutamiento.

El enrutador, como dispositivo físico utilizado para el enrutamiento, no puede realizar esta tarea por sí solo; necesita recibir instrucciones sobre cómo hacerlo. En resumen, los enrutadores analizan la dirección IP de destino para decidir la ruta adecuada que permita que los paquetes lleguen a su red de destino. En caso de que no puedan encontrar una ruta válida, los paquetes son rechazados y no se envían.

El enrutamiento implica que los enrutadores aprendan acerca de redes remotas y encuentren todas las posibles rutas, luego seleccionan las mejores rutas, aquellas que permiten el intercambio de datos de manera más rápida y eficiente. Existen dos tipos de enrutamiento: enrutamiento con rutas estáticas, donde el enrutador debe ser configurado previamente con la información de las redes remotas; y el enrutamiento dinámico, donde los enrutadores intercambian información para aprender automáticamente sobre las redes disponibles.

II. Contexto

A. Enrutamiento Dinámico

Se basa en gran medida en los protocolos de enrutamiento, que se encargan de actualizar automáticamente las rutas. Según López (2018), estos protocolos utilizan la tabla de enrutamiento de cada enrutador para elegir la mejor ruta en redes extensas, siendo el enrutador el encargado tanto de crear, mantener y modificar dichas tablas. Además, que el enrutador también establece normas para que así la red se encuentre actualizada. Un ejemplo de enrutamiento dinámico es una empresa que selecciona nuevas rutas en casos específicos donde se presenten inconvenientes en la ruta original, buscando redes adyacentes.

Estos protocolos resaltan principalmente por su estructura de datos, lo cual es base para las diversas operaciones de las tablas; siendo los mensajes principal

enfoque para la comunicación sobre cambios en la red con routers vecinos y algoritmos, que son para informar los diversos caminos a presentarse y que el router pueda así , seleccionar la mejor ruta posible mediante esta información.

Además, el enrutamiento dinámico se distingue por su facilidad de configuración en redes amplias y por ser intuitivo tanto para seleccionar la mejor ruta como para detectar cambios en ella o descubrir redes remotas. Sin embargo, una desventaja es que los enrutadores comparten actualizaciones, lo que puede consumir un mayor ancho de banda en comparación con el estático. Cabe mencionar que el enrutamiento dinámico utiliza diversos algoritmos y protocolos, siendo los más populares el Routing Information Protocol (RIP) y el Open Shortest Path First (OSPF).

B. Enrutamiento dinámico versus el enrutamiento estático

El enrutamiento estático ocurre cuando el administrador de la red introduce las rutas de forma manual en cada enrutador configurado individualmente. Esto permite que los enrutadores aprendan y sigan las rutas establecidas. La simplicidad de este método se evidencia en el mantenimiento de las tablas de enrutamiento, especialmente en redes pequeñas. Sin embargo, a medida que el número de dispositivos en la red aumenta, configurar el enrutamiento estático se vuelve más complejo. Por otro lado, el enrutamiento dinámico no se ve afectado por la complejidad según el tamaño de la red, ya que las rutas se determinan automáticamente a través de protocolos de enrutamiento.

En términos de escalabilidad, el enrutamiento dinámico se emplea principalmente en redes que esperan un crecimiento futuro, mientras que el enrutamiento estático requiere un esfuerzo considerable y tiempo en la configuración individual de cada router. Es importante destacar que, una vez configurado, el enrutamiento estático puede propiciar errores, especialmente en redes extensas, y su mantenimiento se torna complicado y laborioso. En contraste, el enrutamiento dinámico tiene como objetivo principal obtener información de las redes remotas para adaptarse de manera rápida a los cambios en la topología de la red.

En el enrutamiento dinámico, el tiempo de convergencia aumenta en redes más grandes, pero esto viene acompañado de un mayor consumo de recursos, como memoria RAM, ciclos de CPU (del micro-procesador del enrutador) y un mayor uso del ancho de banda de la red.

III. Revisión sistemática

A. Protocolos de enrutamiento dinámico.

Los protocolos desempeñan un papel esencial en las redes y han sido utilizados desde principios de la década de los ochenta, con su primera versión lanzada en 1982, que incorporaba algoritmos elementales empleados en ARPANET en 1969.

Uno de los primeros protocolos, conocido como Routing Information Protocol (RIP), experimentó una evolución hacia su versión RIPv2, aunque aún no fue suficiente para adaptarse a redes de mayor envergadura. Por este motivo, surgieron dos nuevos protocolos destinados a abordar redes más extensas: el Open Shortest Path First (OSPF) y el Intermediate System-To-Intermediate System (IS-IS).

Estos protocolos representan algoritmos y directrices esenciales en las redes de computadoras, diseñados para determinar de manera automática las rutas óptimas con el fin de compartir paquetes de datos, considerando la topología de red y las condiciones de enlace. Además, facilitan el intercambio de información entre routers, permitiéndoles aprender sobre nuevas redes y hallar rutas alternativas en caso de fallas de enlace en la red actual.

Las funciones asociadas a este procedimiento podrían explicarse de la siguiente manera:

- El dispositivo de conexión transmite y recibe mensajes de dirección mediante sus interfaces.
- Se realiza un intercambio de datos de dirección e información de direccionamiento con otros dispositivos que emplean el mismo protocolo de direccionamiento.
- Los dispositivos de conexión comparten información de direccionamiento para obtener conocimientos sobre redes remotas.
- En caso de que un dispositivo de conexión identifique un cambio en la estructura de la red, el protocolo de direccionamiento puede notificar esta modificación a otros dispositivos.

En la representación gráfica presentada en la figura 1, se muestra una perspectiva jerárquica de la clasificación de los protocolos de direccionamiento dinámico.

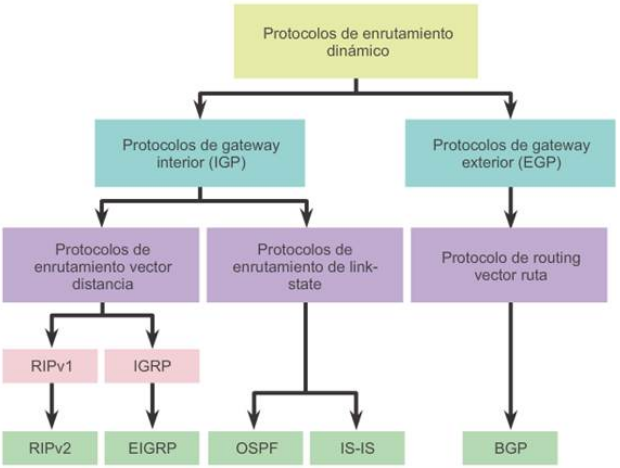

Fig. 1. Clasificación de los protocolos de routing dinámico por Cisco.

1) Protocolos de puerta de enlace interior(IGP):

A partir de 1992, el IETF inició el proceso de selección de un IGP común para Internet. El IGP común de facto, RIP, ya no se consideraba adecuado. dos candidatos a surgir el IGP común: OSPF e Integrated IS-IS [Gallon,R (1990)].

Se diseñó que los routers dentro de un sistema autónomo intercambian información mediante el protocolo IGP, el cual calcula rutas eficientemente y recalcula rápidamente en caso de que la red cambie basándose en métricas como distancia, ancho de banda o latencia, este se caracteriza por ser usados dentro de un dominio de enrutamiento interno o un red autónoma localizada en una ubicación geográfica específica, es decir, una empresa, una organización o institución.

Al romperse la regla del IGP único, esto debido a que varios sistemas autónomos ejecutaban al mismo tiempo varios IGP, tanto para RIP como para OSPF. Se le denominó Dominio de Enrutamiento a la colección de enrutadores que ejecutan IGP, por lo que en este caso un sistema autónomo puede consistir en múltiples dominios de enrutamiento.

1.1. Algoritmos de enrutamiento de vector de distancia:

Los protocolos de enrutamiento basados en vector de distancia constituyen algunos de los métodos de enrutamiento más antiguos aún utilizados en la actualidad. Estos protocolos son relativamente sencillos de comprender. Los enrutadores que emplean esta tecnología comparten información de enrutamiento con otros enrutadores de la red, transmitiendo sus tablas de enrutamiento completas a todos los vecinos conectados directamente.[13].

Sin embargo, se consideran algo ineficientes debido a que estas actualizaciones se envían periódicamente sin tener en cuenta el estado real de la red, independientemente de si hay cambios en la topología o no.

Un aspecto clave a tener en cuenta es que estos solo se comunican con sus vecinos directamente conectados. Por lo tanto, cada enrutador no dispone de información de primera mano sobre todas las rutas en su tabla de enrutamiento. De hecho, la mayoría de las rutas en la tabla de enrutamiento se basarán en información indirecta.

Para ilustrarlo con un ejemplo, en una red similar a la representada en la Figura 2, el enrutador 1 aprenderá acerca de las redes conectadas a los enrutadores 3 y 4 a través del enrutador 2. De manera similar, el enrutador 3 obtendrá información sobre las redes conectadas al enrutador 1 a través del enrutador 2. En resumen, los enrutadores no se comunican directamente con todos los demás enrutadores en la red.

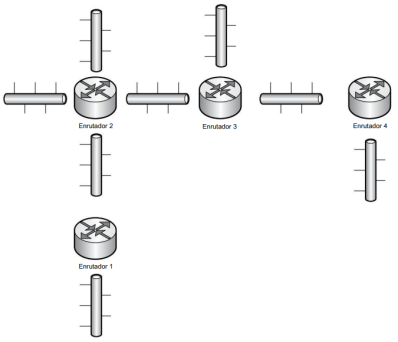

Fig. 2. Ejemplo de diagrama de red de enrutamiento por vector de distancia.

1.1.1. RIP

El Protocolo de Información de Enrutamiento (RIP), también conocido como Routing Information Protocol, representa una de las formas más elementales y sencillas de protocolo de enrutamiento basado en vector de distancia que está en uso en la actualidad. Existen dos variantes disponibles de este protocolo: RIPV1 (RFC 1058) y RIPv2 (RFC 1723)[1]. Para esta investigación, nos centraremos en la versión más actualizada (RIPv2), ya que la versión anterior no es compatible con enrutamiento sin clases y no admite máscaras de subred de longitud variable (VLSM) para las entradas de red, tal como se muestra en la Tabla 1, donde se realiza una comparación entre RIPV1 y RIPV2 [4].

El funcionamiento del RIP se basa en medir sus métricas mediante el conteo de saltos entre los nodos de origen y destino, seleccionando la ruta con el mínimo número de saltos para llegar a un destino específico. RIP permite un máximo de 15 saltos en una ruta; si la cantidad de saltos supera este límite para alcanzar una red de destino, se considera que dicha red es inalcanzable. Cada 30 segundos, el RIP actualiza su tabla de enrutamiento completa con los vecinos más cercanos, y su distancia administrativa es de 120 [20].

TABLA 1.
COMPARACIÓN ENTRE RIP-V1 Y RIP-V2

Características	Protocolos Comparación	
	RIPv1	***RIPv2***
Tipo	Vector Distancia	Vector Distancia
Algoritmo	Bellanfor[a]	Bellanford[a]
Clase	Clase llena	Sin Clase
Autenticación	No	Sí
Soporte VLSM	No	Sí
Métrica	Número de saltos	Número de saltos

[a]. Bellman-Ford: Un algoritmo de enrutamiento basado en vector distancia que realiza iteraciones en la cantidad de saltos de una ruta para determinar un árbol de expansión con la ruta más corta..

a) RIPv2

Diez años después del lanzamiento de la versión 1 de RIP, G. Malkin de Bay Networks lanzó la versión 2 en RFC 2453 en noviembre de 1998. RIPv2 no es un protocolo nuevo, sino una extensión del protocolo de enrutamiento original. Incluye todas las funciones disponibles en RIPv1 y algunas funciones adicionales como actualización de autenticación, multidifusión, etc., así como compatibilidad con versiones anteriores[5]. La razón para mejorar RIP fue que tiene ventajas muy importantes, como un pequeño encabezado adicional para los mensajes (que no afecta el uso del ancho de banda), fácil configuración y capacidad manejable[2]. RIPV2 realiza una serie de mejoras significativas con respecto a su predecesor, que incluyen:

- Autenticación utilizada para la transferencia de datos RIP entre vecinos.
- Implementación de máscaras de red con capacidad para VLSM (Variable Length Subnet Masking).
- Uso de máscaras de red para determinar el siguiente salto, permitiendo arquitecturas de red discontinuas.
- Envío de actualizaciones de la tabla RIP mediante la dirección de multidifusión 224.0.0.9.
- Inclusión de RIPv2 en Management Information Blocks (MIB) para gestión y monitoreo.

RIP y sus versiones RIPv1 y RIPv2 funcionan según el principio del algoritmo Bellman-Ford, que se caracteriza por la iteración, la asincronía y la descentralización.

- La distribución ocurre debido a que cada nodo recibe datos de otros nodos conectados directamente a él, realiza sus propios cálculos y después envía los resultados a sus nodos vecinos.

- Iterativo, porque el proceso continúa hasta que finaliza el intercambio de información con los vecinos. Los nodos no funcionan juntos y de forma sistemática, por lo que es asíncrono.

Una forma de expresar este algoritmo es: "encontrar los caminos más cortos desde un punto de partida dado, siempre que contengan como máximo un enlace; luego encontrar los caminos más cortos siempre que contengan como máximo dos enlaces, y así sucesivamente"[12].

El algoritmo Bellman-Ford es un algoritmo de búsqueda de gráficos para hallar la ruta más corta. El algoritmo puede encontrar pesos negativos de cada borde. En la Figura 3 se muestra el ***ejemplo 1***, donde hay 5 vértices, es decir, A, B, C, D y E. Cada borde tiene un valor de peso, dirigido el borde A hacia B es -3 y el otro borde es uno. N vértices Iteraciones de búsqueda N – 1, 5 vértices 4 iteraciones, pero si hay un ciclo vegetativo o pesos de valor son negativos, entonces debería ser en iteración nuevamente llamado Nth

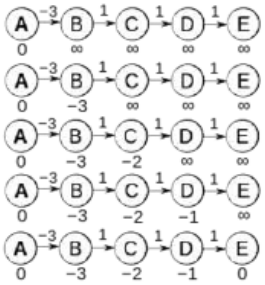

Fig. 3. Ejemplo de algoritmo de Bellman-Ford.

En la investigación [12], utiliza la topología de red,como se muestra en la Figura 4,de ensayos para el algoritmo de bellman-ford mediante el programa de simulación cisco, rastreador de paquetes. El ejemplo se basa en el uso de 3 routers como vértice, es decir, R1, R2 y R3, la ruta de búsqueda inicial es u = 1. Cada borde tiene un valor.

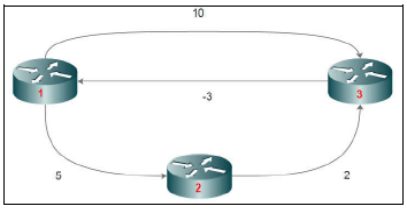

Fig. 4. Diseño de Topología (vértices y pesos) para ejemplo 1 de algoritmo Bellman-Ford.

Después de aplicar el algoritmo Bellman-Ford, el camino más corto, es el recorrido desde el vértice 1 es el valor de ponderación 5 y 2.

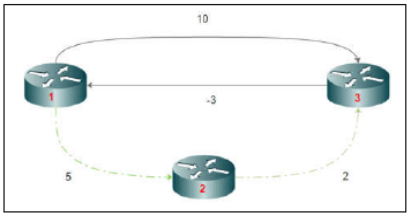

Fig. 5. Camino más corto para ejemplo del algoritmo Bellman-Ford.

El ***ejemplo 2,*** de la investigación[16]., explica también para un conjunto de routers siguiendo el algoritmo Bellman-Ford.

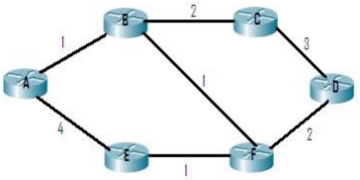

Fig. 6. Diseño de Topología (vértices y pesos) para ejemplo 2 de algoritmo Bellman-Ford.

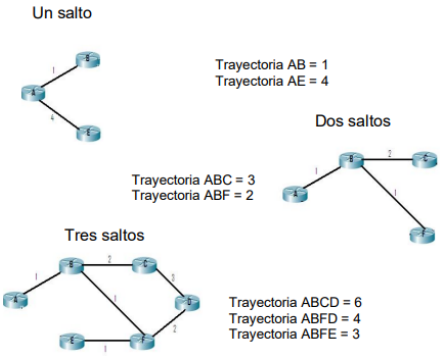

Fig. 7. Saltos para ejemplo 2 del algoritmo Bellman-Ford.

Se evalúan los gastos de todas las rutas que conectan el punto A con cada enrutador, considerando un enlace a la vez. Se selecciona la ruta que requiere menos enlaces para alcanzar el destino. Si solo se necesita un enlace, se escoge la ruta AB; para dos enlaces, la ruta ABF; y para tres enlaces, se eligen dos rutas: ABFD y ABFE, tal como se muestra en la Figura 7.

En el último paso (tres enlaces), se eligen dos rutas. La primera, ABFD, representa la opción de menor costo desde A hasta D, tomando en cuenta la métrica de enlaces. La segunda ruta, ABFE, es seleccionada porque representa el camino de menor costo desde A hasta E.

El resultado final representa el costo mínimo desde el enrutador origen o fuente hasta todos los enrutadores de la red. Resultados similares podrían generarse para cada enrutador de la red. El resultado de menor costo para el enrutador A en este ejemplo se muestra en la Figura 8.

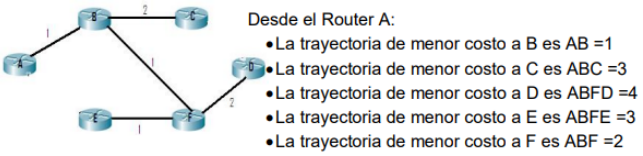

Fig. 8. RIP Resultado Menor costo para ejemplo 2 de algoritmo Bellman-Ford.

1.1.2. IGRP

Interior Gateway Routing Protocol (IGRP), en español "Protocolo de enrutamiento de puerta de enlace interior" es un protocolo de enrutamiento desarrollado por Cisco. IGRP solo está disponible en dispositivos Cisco. Si desea utilizar IGRP como su único protocolo de enrutamiento, todos los enrutadores de su red deben ser dispositivos Cisco [13].

IGRP es un protocolo de enrutamiento de vector de distancia, al igual que RIP, pero es un poco más avanzado y supera algunas de las limitaciones del uso de RIP. Fue desarrollado principalmente para superar el límite de conteo de saltos y la métrica de conteo de saltos de RIPV1[15].IGRP tiene un conteo máximo de saltos de 255. Esto permite que IGRP se use en redes mucho más grandes. Además, IGRP tiene una distancia administrativa de 100. Por lo tanto, sus rutas se consideran más confiables que las rutas proporcionadas por RIP.

EIGRP incluye las siguientes características [13].

- **Métrica de enrutamiento:** IGRP usa *métrica compuesta*, una métrica más avanzada que usa una combinación de múltiples factores en su cálculo, para determinar la ruta más eficiente a un destino.
- **Actualizaciones de enrutamiento:** IGRP no envía información de máscara de subred, sino que envía toda su tabla de enrutamiento cuando envía actualizaciones de enrutamiento. Sin embargo, estas actualizaciones solo se envían cada 90 s en lugar del tiempo de actualización de 30 s utilizado por RIP.
- **Sistemas Autónomos:** Cuando configura IGRP en un enrutador, debe configurar un número de sistema autónomo (AS). Un AS designa un grupo de enrutadores que compartirán información. Este número de AS debe coincidir en todos los enrutadores que compartirán información de enrutamiento. Se utilizan varios AS en redes más grandes para ayudar a segmentarlos. En una red grande, sin segmentación, podría terminar con tablas de enrutamiento muy grandes y complejas en sus enrutadores. Cuanto más grandes y complejas sean las tablas de enrutamiento, más tardará la convergencia.

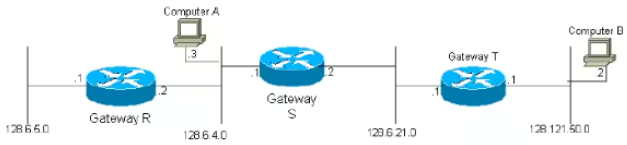

Fig. 9. Protocolo IGRP

Por ejemplo, en la Figura 9, el Gateway S está conectado a las redes 2 y 3 a través de las interfaces correspondientes. Inicialmente, Gateway 2 solo sabe que puede llegar a cualquier computadora de destino en las redes 2 y 3. Todas las puertas de enlace están programadas para transmitir periódicamente información a las puertas de enlace vecinas que han iniciado y que han recibido de otras puertas de enlace. La puerta de enlace S recibirá actualizaciones de las puertas de enlace R y T y sabrá que puede llegar a las computadoras de la red 1 a través de la puerta de enlace R y a las computadoras de la red 4 a través de la puerta de enlace T. Dado que la puerta de enlace S envió toda su tabla de enrutamiento, en el próximo ciclo la puerta de enlace T sabrá que puede llegar a la red 1 a través de la puerta de enlace S. No es difícil ver que mientras la red esté completamente conectada, la información sobre cada red en el sistema finalmente llegará a todas las puertas de enlace del sistema.

El soporte para IGRP ha quedado obsoleto y ya no es compatible con la mayoría de los enrutadores Cisco. Ha sido reemplazado por EIGRP [13].

a) EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP), en español "Protocolo de enrutamiento de puerta de enlace interior mejorado" es una mejora del estándar IRGP original.

EIGRP es híbrido o vector de distancia. Además es considerado uno de los protocolos más usados en la actualidad. Esto por la robustez y eficiencia que presenta[13].

EIGRP admite una variedad de protocolos de red. Puede proporcionar soporte de enrutamiento para IPv4, IPv6, Intercambio de paquetes entre redes (IPX) y AppleTalk.

Similar a su predecesor IGRP, EIGRP tiene un conteo de saltos máximo de 224 y un conteo de saltos máximo predeterminado de 100. EIGRP tiene una distancia administrativa de 90. Esto significa que sus rutas son un poco más confiables que las rutas IGRP y mucho más confiables que las rutas RIP que tienen una distancia administrativa de 120.

EIGRP reemplazó a IGRP en 1992. EIGRP incluye las siguientes características(Ver Tabla 2):

- **Actualizaciones activadas limitadas:** envía actualizaciones solo a los enrutadores que las necesitan.
- **Mecanismo de mantenimiento de saludo:** los mensajes de saludo se intercambian periódicamente para mantener las adyacencias.

TABLA 2.
COMPARACIÓN ENTRE IGRP Y EIGRP

Características y Funciones	Protocolos Comparación	
	IGRP	***EIGRP***
Métrica	Ambos usan una métrica compuesta que consta de ancho de banda y retraso. La confiabilidad y la carga también se pueden incluir en el cálculo métrico.	
Actualizaciones reenviadas a la dirección	255.255.255.255	224.0.0.10
Soporte VLSM	No	Sí
Soporte Summarization	No	Sí
Soporte Authentication	No	Sí

EIGRP emplea el ***Algoritmo de Actualización Difusa (DUAL)*** para calcular las rutas óptimas hacia un destino. Esta técnica de enrutamiento permite la operación sin restricciones de clases. Así, al enviar actualizaciones de enrutamiento, EIGRP incorpora datos sobre la máscara de subred. De esta forma, se habilita el uso de Máscaras de Longitud Variable (VLSM) y la configuración de redes no adyacentes.

Al usar DUAL, EIGRP realiza un seguimiento de tres tablas:

1. **Tabla de vecinos:** contiene una lista de todos los enrutadores con los que EIGRP ha establecido una vecindad.
2. **Tabla de topología:** realiza un seguimiento de toda la topología de la red. Almacena toda la información sobre todas las rutas que el enrutador ha recibido de sus vecinos, incluso rutas duplicadas.

3. **Tabla de rutas:** es la tabla que almacena información sobre las mejores rutas a un destino en particular.

A continuación se presenta un ejemplo DUAL:

La representación gráfica en la Figura 10 ilustra el proceso de convergencia del protocolo DUAL. En este ejemplo, se enfoca únicamente en el destino N, mostrando el costo de cada nodo para alcanzarlo (número de saltos). Las flechas indican el sucesor elegido por cada nodo para llegar a N. Por ejemplo, el nodo C utiliza el nodo A como sucesor para llegar a N, con un costo de 2.

Cuando se produce una falla en el enlace entre A y B, el nodo B envía una consulta a sus vecinos para informarles que ha perdido su sucesor válido. En este caso, el nodo D recibe la consulta y verifica si tiene algún otro sucesor posible. Si no encuentra sucesores válidos, debe iniciar un cálculo de ruta e ingresar al estado activo. No obstante, en esta situación, el nodo C es un sucesor válido ya que su costo (2) es menor que el costo actual de D (3) para alcanzar el destino N. En consecuencia, D puede cambiar a C como su nuevo sucesor. Es importante destacar que los nodos A y C no se ven afectados por este cambio y no participan en el proceso debido a que no están relacionados con el enlace fallido.

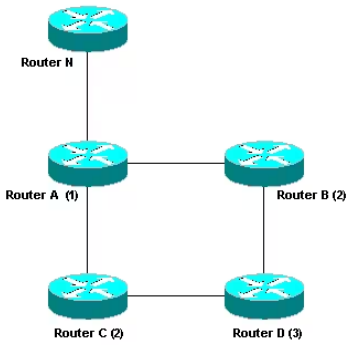

Fig. 10. Ejemplo de Algoritmo de Actualización Difusa (DUAL)

El funcionamiento de EIGRP se basa en los siguientes cuatro componentes básicos[10].

- **El proceso de detección o recuperación de vecinos** es una función esencial para los routers, ya que les permite aprender dinámicamente de otros routers conectados directamente a sus redes. Este procedimiento se realiza de manera eficiente mediante el envío de pequeños paquetes de saludo, lo que permite determinar si un vecino está activo y operativo al recibir dichos paquetes.
- **El transporte confiable** es una función responsable de asegurar que los paquetes EIGRP sean entregados de manera ordenada y garantizada a todos los vecinos. Para ello, se admiten tanto transmisiones unidifusión como multidifusión. Por ejemplo, en redes de acceso múltiple como Ethernet, donde se puede utilizar la multidifusión, no es necesario enviar saludos confiables de manera individual a cada vecino. En su lugar, EIGRP envía un único saludo de multidifusión y los receptores son informados de que no necesitan enviar un reconocimiento para dicho paquete.
- **La máquina de estados finitos DUAL** juega un papel crucial en los cálculos de rutas. Es responsable de rastrear y evaluar todas las rutas anunciadas por los vecinos. Utilizando la información de distancia o métrica, DUAL selecciona los caminos más eficientes sin formar bucles.
- **Los módulos que dependen del protocolo** EIGRP asumen responsabilidades específicas en la capa de red.

1.2. Algoritmos de enrutamiento de estado de enlace:

a) OSPF

Los routers utilizan la información de estado de sus routers vecinos para calcular y compartir la información de enrutamiento en la red. En una red OSPF, cada router tiene conocimiento completo de la topología de la red y utiliza esta información para encontrar la mejor ruta posible para el tráfico dentro del ancho de banda disponible. A diferencia de otros protocolos de enrutamiento que dependen del número de saltos para calcular la distancia,

OSPF utiliza una métrica basada en costos, la cual puede ser ajustada según la capacidad y prioridad de las distintas rutas. El cálculo de la ruta más corta se realiza utilizando el algoritmo de Dijkstra. En la Figura 11, la ruta más corta desde R2 hasta la LAN conectada a R3 se muestra como 27, y cada ruta se encuentra etiquetada con un valor de costo arbitrario. Por ejemplo, el costo de R2 a R1 es 20, más R1 a R3 (5), y finalmente R3 a la LAN (2). Cada enrutador establece su propio costo para cada unidad de topología.

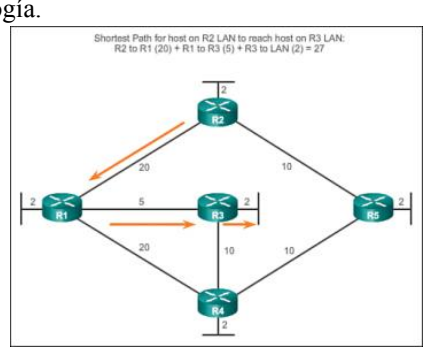

Fig. 11. Ruta más corta de R2 a R3

Proceso de enrutamiento de estado de enlace

- ***Enlace y estado de enlace***

En la Figura 12, R1 adquiere conocimiento sobre las redes a las que está directamente conectado, es decir, las redes a las que se encuentra físicamente enlazado. Estas redes conectadas se convierten en entradas en la tabla de enrutamiento de R1.

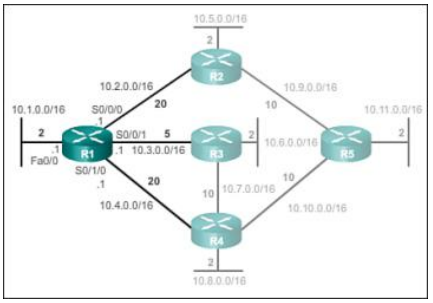

Fig. 12. Enlaces R1

Cómo se observa en la *Figura 13*, la información del estado de enlace incluye:

- ➢ Dirección IPv4 y la máscara de subred.
- ➢ Tipo de red.
- ➢ El costo del enlace.
- ➢ Cualquier router vecino en este enlace.

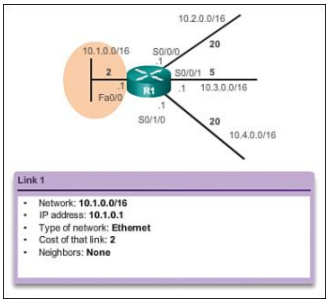

Fig. 13. Enlace- Enlace de la interfaz Fa 0/0

- ***Say hello***

En la siguiente etapa, denominada el proceso de enrutamiento de estado de enlace, cada router se encarga de identificar a sus vecinos en las redes a las que está directamente conectado. En este contexto, un vecino se refiere a cualquier otro router que también está configurado con igual protocolo de enrutamiento de estado de enlace.

En la Figura 14, R1 inicia el envío de paquetes Hello a través de sus interfaces con el fin de descubrir si hay vecinos de enlace en la red.

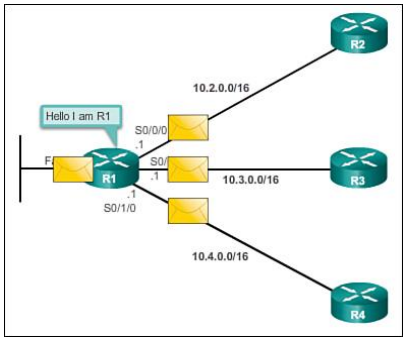

Fig. 14. R1 envía paquetes Hello

En la Figura 15, los routers R2, R3 y R4 responden al paquete "Hello" con sus propios paquetes "Hello" porque están configurados con el mismo protocolo de enrutamiento de estado de enlace. Sin embargo, en la interfaz FastEthernet 0/0, no se detectan vecinos. Como resultado, R1 no sigue con los pasos subsiguientes del proceso de enrutamiento de estado de enlace para esa interfaz en particular.

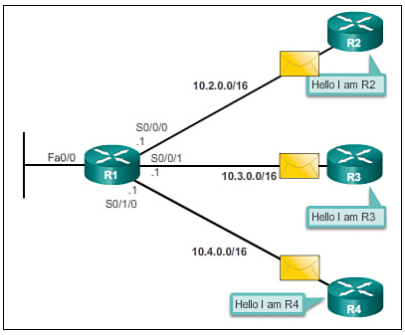

Fig. 15. R2, R3 y R4 Responder con Hello Packets

Cuando dos routers de enrutamiento de estado de enlace se reconocen como vecinos, establecen un vínculo llamado "vecindario". Estos routers intercambian pequeños paquetes de saludo (Hello) de forma continua entre ellos, lo cual sirve como un mecanismo de monitoreo del estado del vecino. Si un router deja de recibir paquetes Hello de su vecino, lo considera inalcanzable y, en consecuencia, el vecino se considera inactivo.

- ***Construcción del paquete Link-State***

El tercer paso es el E. estado de enlace donde cada enrutador genere un LSP (Link State Packet) que contiene la información del estado de cada enlace directamente conectado. Una vez que un enrutador ha identificado a sus vecinos, puede crear LSPs que contienen detalles sobre el estado de los enlaces que tiene con cada uno de ellos.

El LSP de R1 que se muestra en *Figura 16*.

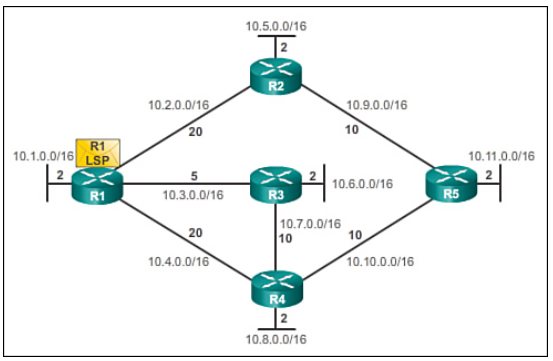

Fig. 16. Construyendo el LSP para R1

- ***Inundando el LSP***

Cuando un enrutador recibe un LSP (Link State Packet) de un vecino, lo retransmite de inmediato a todas las demás interfaces, excepto por aquella por la que recibió el LSP. Este proceso provoca un efecto de inundación, donde los LSP de todos los enrutadores se propagan a lo largo de todo el área de enrutamiento.

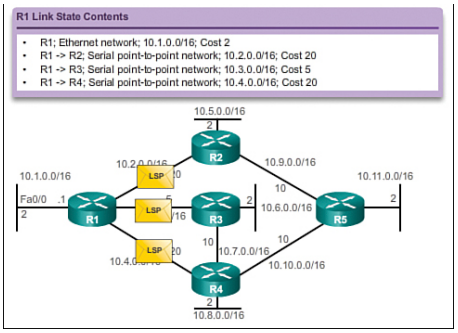

Fig. 17. R1 inunda su LSP

- ***Creación de la base de datos de estado de enlace***

En esta etapa, todos los routers reciben un "LSP" (Paquete de Estado de Enlace) de cualquier otro router que participe en el enrutamiento. Estos LSP se guardan en la base de datos, lo que permite que cada enrutador acceda a la información actualizada sobre la topología de la red y la utilice para calcular la ruta óptima hacia diversas redes de destino. De esta manera, los routers tienen acceso a datos actualizados sobre la red y pueden tomar decisiones precisas en el enrutamiento del tráfico hacia los destinos deseados.

Base de datos de estado de enlace
R1 Estados de enlace:
Conectado a la red 10.1.0.0/16, costo = 2
Conectado a R2 en la red 10.2.0.0/16, costo = 20
Conectado a R3 en la red 10.2.0.0/16, costo = 5
Conectado a R4 en la red 10.3.0.0/16, costo = 20
R2 Link-states:
Conectado a la red 10.5.0.0/16, costo = 2
Conectado a R1 en la red 10.2.0.0/16, costo = 20
Conectado a R5 en la red 10.9.0.0/16, costo = 10
R3 Link-states:
Conectado a la red 10.6.0.0/16, costo = 2
Conectado a R1 en la red 10.3.0.0/16, costo = 5
Conectado a R4 en la red 10.7.0.0/16, costo = 10
R4 Estados de enlace:
Conectado a la red 10.8.0.0/16, costo = 2
Conectado a R1 en la red 10.4.0.0/16, costo = 20
Conectado a R3 en la red 10.7.0.0/16, costo = 10
Conectado a R5 en la red 10.10.0.0/16, costo = 10
R5 Estados de enlace:
Conectado a la red 10.11.0.0/16, costo = 2
Conectado a R2 en la red 10.9.0.0/16, costo = 10
Conectado a R4 en la red 10.10.0.0/16, costo = 10

Después del proceso de inundación, R1 ha obtenido información del estado de todos los routers. Es relevante mencionar que R1 también incluye su propia información de estado de enlace en la base de datos correspondiente.

Con una base de datos completa del estado de enlace, R1 ahora tiene la capacidad de utilizar el algoritmo de ruta más corta primero (SPF) para calcular la ruta preferida y más corta hacia cada red, lo que conduce a la formación del árbol SPF. En este árbol se determinan las rutas óptimas desde R1 hacia cada destino en la red, tomando en cuenta la topología y el estado de los enlaces presentes en el área de enrutamiento.

- ***Construyendo el árbol SPF***

Cada enrutador dentro del área de enrutamiento utiliza la base de datos de estado de enlace junto con el algoritmo SPF para construir el Árbol SPF. Por ejemplo, R1, utilizando la información de estado de enlace proporcionada por todos los otros enrutadores, comienza a formar el Árbol SPF para la red. Para este propósito, el algoritmo SPF analiza los LSP de cada router para identificar las redes y sus costos asociados.

El algoritmo SPF procede a calcular las rutas más cortas hacia cada red individual, lo que da lugar a la creación del Árbol SPF, como se ilustra en la Figura 18. De esta manera, R1 obtiene una visión completa de la topología en el área de estado de enlace.

Destination	Shortest Path	Cost
10.5.0.0/16	R1→R2	22
10.6.0.0/16	R1→R3	7
10.7.0.0/16	R1→R3	15
10.8.0.0/16	R1→R3→R4	17
10.9.0.0/16	R1→R2	30
10.10.0.0/16	R1→R3→R4	25
10.11.0.0/16	R1→R3→R4→R5	27

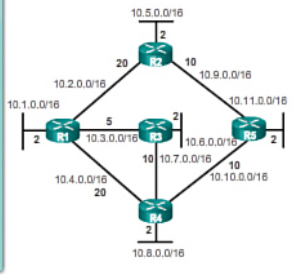

Fig. 18. Árbol SPF resultante de R1

b) IS-IS

IS-IS o su siglas en inglés "Intermediate System-to-Intermediate System" es un protocolo estandarizado de estado de enlace, que es conocido como el protocolo de enrutamiento principal para el Modelo OSI, desarrollado por la Organización Internacional de Normalización (ISO). En términos de similitudes, IS-IS comparte muchas características con OSPF. Aunque su diseño inicial se enfocó como un protocolo de puerta de enlace interna (IGP), su uso predominante se ha extendido a los proveedores de servicios de Internet debido a su excelente escalabilidad. IS-IS se rige por una serie de características propias del estado de enlace:

- El protocolo IS-IS permite la configuración de una estructura jerárquica de red mediante el uso de áreas.
- Para establecer conexiones con enrutadores adyacentes del mismo tipo de IS-IS, este protocolo establece relaciones de vecindad.
- En lugar de anunciar la distancia hacia las redes conectadas, IS-IS transmite información sobre el estado de los "enlaces" que están directamente conectados a través de Paquetes de Estado de Enlace (LSP). Solo se enviarán actualizaciones cuando se produzca un cambio en alguno de los enlaces, y dicha actualización contendrá únicamente la modificación realizada.
- La determinación de la ruta más corta se logra en IS-IS a través del uso del algoritmo de Dijkstra de Primer Camino más Corto.
- Al ser un protocolo sin clase, IS-IS es compatible con VLSM (Máscara de Longitud Variable).

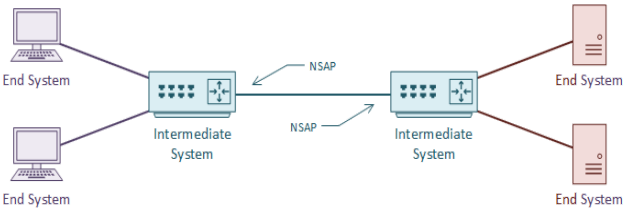

Fig. 19.. Intermediate System-to-Intermediate System.

IS-IS presenta diversas características adicionales, entre las cuales se encuentran las siguientes:

- IS-IS fue originalmente desarrollado para enrutamiento del espacio de direcciones ISO, y esto no se limita al enrutamiento IP.
- Las rutas de IS-IS tienen una distancia administrativa de 115.
- IS-IS utiliza un costo arbitrario para su métrica. Además, IS-IS tiene tres métricas opcionales: retardo, gasto y error. Cisco no admite estas métricas opcionales.
- IS-IS no tiene un límite de saltos.

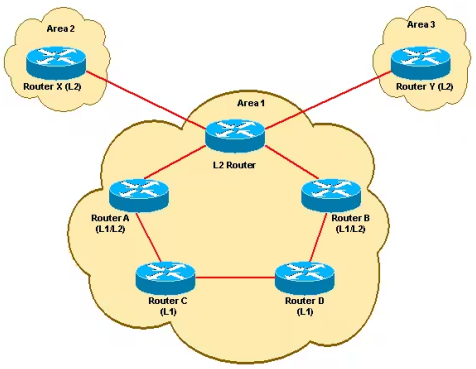

Fig. 20. IS-IS Route Leaking Overview.

Según el proceso de IS-IS, se generan y actualizan tres tablas distintas::

- *Tabla de vecinos: Esta tabla incluye un registro de todos los routers que son vecinos directos entre sí.*

- *Tabla de topología: Aquí se encuentran todas las posibles rutas hacia las diversas redes conocidas dentro de un área específica.*
- *Tabla de enrutamiento: En esta tabla se almacena la ruta óptima para alcanzar cada una de las redes conocidas.*

Es importante destacar que IS-IS sólo se encuentra disponible en las versiones empresariales del sistema operativo Cisco IOS.

1. Protocolos y direccionamiento de IS-IS

Los protocolos y direccionamiento de IS-IS están compuestos por tres subprotocolos que trabajan en conjunto con el propósito de lograr el enrutamiento de extremo a extremo, lo cual la ISO define como el Servicio de Red sin Conexión (CLNS, por sus siglas en inglés). Para ello, se emplean los siguientes subprotocolos:

- *CLNP (Protocolo de Red sin Conexión): Actúa como el protocolo de Capa 3 para IS-IS, y fue desarrollado por la ISO.*
- *ES-IS (Sistema Final a Sistema Intermedio): Se utiliza para el enrutamiento entre hosts y routers.*
- *IS-IS (Sistema Intermedio a Sistema Intermedio): Se emplea para el enrutamiento entre routers.*

IS-IS fue originalmente desarrollado para enrutamiento de direcciones CLNP de ISO *(descritas en RFC 1142)*. Sin embargo, el direccionamiento CLNP nunca se utilizó ampliamente. Por lo tanto, IS-IS se modificó para admitir además el enrutamiento IP y se convirtió en IS-IS Integrado (o Dual) *(descrito en RFC 1195)*.

La dirección CLNP de IS-IS es hexadecimal y de longitud variable, y puede tener una longitud de 64 a 160 bits. La dirección CLNP contiene tres "secciones", que incluyen:

- Campo de área *(de longitud variable)*.
- Campo de identificación *(ID de 8 a 64 bits, aunque generalmente 48 bits)*.
- Campo de selector *(SEL de 8 bits)*.

Se definen dos tipos de direcciones CLNP:

- *Dirección NET:* No contiene información de capa superior (es decir, el campo SEL siempre se establece en 0x00).
- *Dirección NSAP:* La dirección CLNP "completa", con los campos de Área, ID y SEL poblados.

Así, la dirección CLNP identifica el "área" en la que se encuentra un dispositivo, el "ID" real del host y la aplicación de destino en ese host, en forma del campo "SEL". La dirección CLNP está lógicamente segmentada aún más, como se indica a continuación en la siguiente tabla:

IDP		**DSP**		
AFI	*IDI*	*HO-DSP*	*System-ID*	*NSEL*
Area Field			**ID Field**	**SEL Field**

Figura 21. Segmentaciones de la dirección CLNP.

La figura previa presenta la fila superior que muestra cómo la dirección ISO CLNP (Protocolo de Red de Control de Enlace) brinda un control detallado al separar la información de enrutamiento interna y externa, de la siguiente manera:

- La porción IDP (Initial Domain Part) de la dirección tiene la función de identificar el Sistema Autónomo del dispositivo, facilitando así el enrutamiento hacia o entre Sistemas Autónomos. Esta parte de la dirección se divide en dos secciones:
  - *AFI (Authority and Format Identifier):* Es un campo de 8 bits que especifica la organización autorizada para asignar direcciones y también define el formato y longitud del resto de la dirección CLNP.
  - *IDI (Initial Domain Identifier):* Es el componente que identifica la "suborganización" dentro de la organización AFI padre. La longitud del IDI depende del AFI seleccionado.
- La parte DSP (Domain Specific Part) de la dirección se utiliza para el enrutamiento dentro del sistema autónomo.

Cabe mencionar que una dirección CLNP con un AFI de 0x49 corresponde a una dirección privada que no se puede enrutar a nivel global, similar a una dirección IPv4 privada. En contraste, un AFI de 0x47 se utiliza comúnmente para redes IS-IS globales, y la sección IDI dentro de esta dirección identifica organizaciones específicas. Es importante tener en cuenta que el AFI y el IDI combinados esencialmente identifican el sistema autónomo de la dirección, pero no debe confundirse con un número AS (Sistema Autónomo) de BGP (Protocolo de Puerta de Enlace de Borde), ya que no es compatible con BGP como protocolo de enrutamiento externo.

La parte DSP de la dirección se subdivide en tres secciones, que son las siguientes:

- *HO-DSP (High Order DSP): Sirve para identificar el área dentro del sistema autónomo.*
- *System ID: Es un campo de 48 bits (6 octetos) que se utiliza para identificar un host específico dentro del sistema autónomo, usualmente para acomodar direcciones MAC.*
- *NSEL: Se trata de un campo de 8 bits que identifica el protocolo de capa superior de destino del host.*

2. IS-IS Packet Types (Tipos de paquetes de IS-IS)

IS-IS define dos categorías de dispositivos de red:

- *ES (End System, sistema final):* Identifica un host final.
- *IS (Intermediate System, sistema intermedio):* Identifica un enrutador de Capa 3.

Además, IS-IS define cuatro categorías de tipos de paquetes:

a) *Hello (saludo):* Los paquetes Hello son utilizados en IS-IS para el descubrimiento de vecinos. En este protocolo, existen tres tipos de paquetes Hello:
- *IIH (IS-IS Hello): Estos paquetes son intercambiados entre routers (o sistemas IS) con el propósito de establecer conexiones vecinas.*
- *ESH (ES Hello): Se envía desde un Sistema de Extremo (ES) para descubrir un enrutador disponible en la red.*
- *ISH (IS Hello): Los routers IS envían estos paquetes para anunciar su presencia a los Sistemas de Extremo (ES) de la red.*

b) *LSP (Link State Packet, paquete de estado de enlace):* Se utilizan para compartir información topológica entre routers. En este sentido, se crean LSP separados para el enrutamiento de Nivel 1 y el enrutamiento de Nivel 2. Los detalles específicos acerca de los LSP serán abordados más adelante en este documento.

c) *CSNP (Complete Sequence Number PDU, PDU de número de secuencia completa):* Son actualizaciones que

contienen la base de datos completa del estado de enlace. En el contexto de IS-IS, los enrutadores actualizan esta base de datos completa cada 15 minutos.

d) *PSNP (Partial Sequence Number PDU, PDU de número de secuencia parcial): S*on utilizados por los routers de IS-IS para solicitar y confirmar una actualización del estado de enlace de manera parcial.

3. IS-IS Neighbors (Vecinos de IS-IS)

Los enrutadores de IS-IS establecen relaciones de proximidad denominadas "vecindades adyacentes" mediante el intercambio de paquetes conocidos como "Hello", también referidos como "IS-IS Hellos" o "IIH". Estos paquetes Hello son transmitidos cada 10 segundos, a parte del tipo de medio de comunicación utilizado que es independiente. Una vez que la vecindad ha sido establecida, los enrutadores pueden compartir información de enrutamiento. Cabe destacar que IS-IS admite tres formatos de paquetes IIH: uno para enlaces punto a punto, y dos para enlaces de difusión (o LAN) conocidos como "Hellos de difusión de Nivel 1 y Nivel 2".

A diferencia de OSPF, en IS-IS los vecinos no necesitan compartir una subred IP común para formar una vecindad. Estas vecindades se establecen a través de conexiones CLNP (Protocolo de Número de Conexión en Modo Orientado a la Conexión) en lugar de conexiones IP, incluso cuando se utiliza IS-IS Integrado. Por lo tanto, IS-IS no requiere de conectividad IP entre los enrutadores para llevar a cabo el enrutamiento de tráfico IP. Existen dos tipos de vecindades en IS-IS:

- *Vecindad de Nivel 1:* Se utiliza cuando el enrutamiento se da dentro de un área, también conocido como "enrutamiento intra área".
- *Vecindad de Nivel 2:* Se utiliza cuando el enrutamiento se da entre áreas, es decir, el "enrutamiento inter área".

Para que los enrutadores de IS-IS se conviertan en vecinos, es necesario que compartan un enlace físico común, y el "System-ID" debe ser único en cada enrutador. Además, ciertos parámetros deben ser idénticos en todos los enrutadores, como el formato del paquete Hello (punto a punto o difusión), los temporizadores Hello, el "Nivel" del enrutador, el área (aplicable solo para vecindades de Nivel 1), los parámetros de autenticación (con autenticación de texto sin formato para IS-IS) y la MTU (Unidad Máxima de Transmisión).

En los enlaces de difusión, los vecinos seleccionarán un "DIS" (Sistema Intermedio Designado), equivalente al "DR" (Router Designado) en el protocolo OSPF. Sin embargo, a diferencia de OSPF, no existe un respaldo para el DIS, lo que significa que se realizará una nueva elección inmediatamente si el DIS falla. Además, la elección del DIS es preemptiva, y el enrutador de IS-IS con la mayor prioridad se convertirá en el DIS (la prioridad predeterminada es 64). En caso de empate en la prioridad, se utilizará la dirección SNPA (generalmente la dirección MAC) más alta para determinar el DIS. Cabe mencionar que el DIS envía paquetes Hello cada 3.3 segundos, en lugar de los 10 segundos en el caso regular.

4. The IS-IS Hierarchy (La jerarquía IS-IS)

IS-IS define tres categorías distintas de routers:

- *Router de Nivel 1:* Estos routers se encuentran dentro de una única área y su tabla de topología está restringida a su área local, conocida como la base de datos del nivel 1.
- *Router de Nivel 2:* Los routers de este tipo actúan como enrutadores principales o backbone y son responsables de dirigir el tráfico entre áreas, manteniendo una base de datos del nivel 2.
- *Router de Nivel 1-2:* Estos routers se asemejan a los routers de borde de área, ya que interconectan un área local con el área del backbone, construyendo una base de datos de nivel 1 y de nivel 2.

El backbone de IS-IS está compuesto por varios routers de Nivel 2 que son contiguos, cada uno de los cuales puede existir en un área separada.

Para construir sus tablas de topología, los vecinos intercambian LSP (Link-State Packets), que son equivalentes a los LSA de OSPF. Dependiendo del tipo de proximidad, un router enviará un LSP de Nivel 1 o de Nivel 2.

Los routers de Nivel 1 comparten LSP de Nivel 1 y crean una tabla de topología de Nivel 1 que abarca únicamente su propia área, equivalente a un área totalmente sumarizada en OSPF.

- Si un router de Nivel 1 tiene un paquete previamente destinado al área local, simplemente lo enruta al ID del sistema utilizando la tabla de topología local (base de datos de Nivel 1).
- Si un router de Nivel 1 tiene un paquete previamente destinado a un área remota, lo envía al router de Nivel 1-2 más cercano. Los routers de Nivel 1-2 establecen un bit de Attach (ATT) en sus LSP de Nivel 1, informando a otros routers de Nivel 1 que están conectados a otra área.

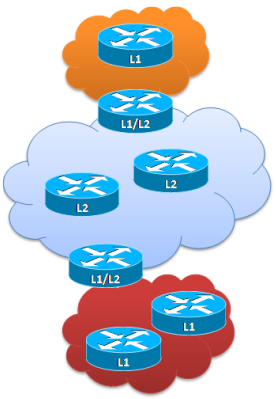

Fig. 21. IS-IS Hierarchy

Los routers de Nivel 2 intercambian Protocolos de Estado de Enlace (LSP, por sus siglas en inglés) a nivel 2, y con base en esta información, construyen una tabla de topología a nivel 2 que contiene una lista de áreas accesibles en todo el dominio del protocolo IS-IS.

Los routers que operan en el nivel 1-2 comparten tanto los LSP de Nivel 1 como de Nivel 2 con sus vecinos correspondientes. Además, mantienen tablas de topología separadas para el Nivel 1 y el Nivel 2.

En el caso de rutas de Nivel 1 que se originan localmente, estas siempre tienen prioridad sobre las rutas de Nivel 2 que se originan desde otra área del dominio. Los routers que utilizan el protocolo IS-IS actualizan la tabla de topología del Estado de Enlace cada 15 minutos, en contraste con los 30 minutos que emplea OSPF para llevar a cabo esta actualización.

5. Basic IS-IS Configuration

2) *Protocolos de puerta de enlace exterior(EGP):*

El protocolo EGP presenta su primera versión en RFC 827, el cual es un documento titulado "Exterior Gateway Protocol (EGP)", posteriormente la versión 2, propuesta en RFC888 y la especificación formal de EGPv2 propuesta en RFC 904.

El protocolo se emplea en la transferencia de datos entre sistemas independientes en Internet, facilitando una comunicación e intercambio eficiente de información entre diversas redes y proveedores. Los mensajes EGP se comparten entre vecinos o pares EGP, en caso estén en diferentes sistemas autónomos, son vecinos exteriores. El protocolo EGP No tiene ninguna función que descubra automáticamente a sus vecinos; las direcciones de estos se configuran manualmente y los mensajes que intercambian son unicast a las direcciones configuradas.

En la Figura X, se observa que los vecinos de EGP no están conectados a la misma red.

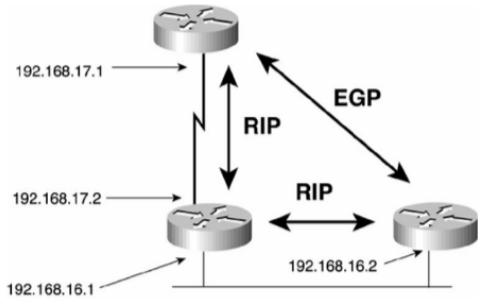

Fig. 22. Ruta más corta de R2 a R3

2.1. Protocolo de enrutamiento de vector de ruta:

a) BGP

El Protocolo de Puerta de Enlace Fronteriza (Border Gateway Protocol, BGP) es ampliamente conocido como el protocolo de enrutamiento utilizado en Internet. Su función principal consiste en facilitar la transmisión de datos entre diferentes Sistemas Autónomos (AS) y dentro de un mismo Sistema Autónomo. Este protocolo juega un papel crucial como mecanismo de enrutamiento de puerta de enlace exterior, y su uso es muy extendido en la actualidad.

Cada AS contiene múltiples enrutadores y cada AS se empareja con otros AS en base a un acuerdo firmado y políticas compartidas. Existen múltiples rutas entre el AS de origen y el AS de destino, pero el protocolo BGP selecciona solo una mejor ruta para propagar el tráfico utilizando el algoritmo de mejor ruta.

Hay dos modos diferentes en los que opera BGP: *eBGP (BGP externo) e iBGP (BGP interno)*. El eBGP intercambia información de enrutamiento entre diferentes ISP (proveedores de servicios de Internet) y el iBGP intercambia información de enrutamiento dentro del mismo ISP entre los enrutadores. Ambas configuraciones son importantes ya que comparten políticas comerciales con otros ISP. BGP siempre ha sido un tema interesante para la comunidad de investigación, principalmente debido a diversas preocupaciones relacionadas con su convergencia, su flujo, sus limitaciones en términos de ingeniería de tráfico, anomalías documentadas y otros problemas, pero las recientes interrupciones a gran escala en Internet actuaron como un catalizador para revivir el enfoque de investigación hacia su enrutamiento.

El protocolo de Gateway de Borde no satura la red con información de enrutamiento de manera periódica, sino que transmite mensajes de forma incremental. Se trata de un protocolo de tipo punto a punto (peer-to-peer) que distribuye información de enrutamiento y mantiene actualizada la tabla de enrutamiento. Los mensajes o actualizaciones de enrutamiento únicamente se envían cuando se identifica una nueva ruta o cuando se retira una ruta previa. A diferencia de los protocolos de enrutamiento interno (IGP), que emplean el algoritmo de vector de distancia y el algoritmo de estado de enlace, BGP utiliza el algoritmo de vector de camino para descubrir las rutas. Las decisiones de enrutamiento se fundamentan en:

- ❖ Ruta
- ❖ Políticas de red
- ❖ Reglas.

Para el uso de BGP se implementan determinadas políticas para el manejo de las rutas entrantes y salientes hacia Internet. Dentro de BGP, se prioriza únicamente una ruta óptima para ser propagada hacia el prefijo de destino. El proceso de selección de la ruta en BGP se compone de diversas etapas, durante las cuales un enrutador realiza comparaciones entre los atributos de las rutas de BGP disponibles y elige aquella que sigue las siguientes preferencias:

- Mayor preferencia local,
- Menor camino de AS,
- Menor valor de origen,
- Menor discriminador de salida múltiple (MED),
- Ruta eBGP sobre ruta iBGP,
- Menor costo interno del siguiente salto de BGP,
- Menor ID de BGP y
- Menor dirección IP del par.

Aunque existen múltiples rutas entre la misma fuente y destino, solo se selecciona una ruta para la transmisión y las rutas restantes no se utilizan en absoluto. El enrutador de origen de BGP tiene toda la información sobre los múltiples caminos disponibles para la transmisión. No sólo transmite, sino que también anuncia solo la mejor ruta única a todos sus pares. Hay algunos problemas asociados con la selección de una sola ruta. Tomemos un escenario en el que en una red existen múltiples rutas, pero el BGP tradicional selecciona solo la mejor ruta. Podemos ver esto en el siguiente diagrama:

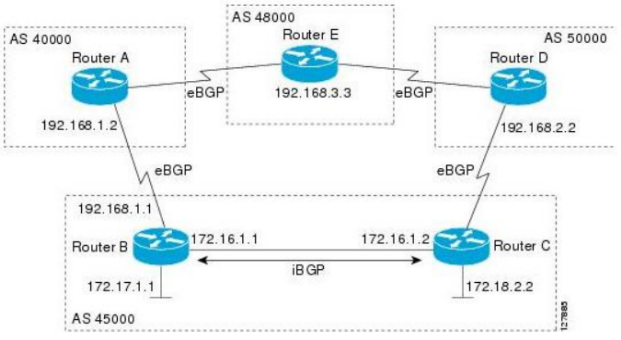

Fig. 23. Advertisement of routes in BGP protocol.

Según lo ilustrado en la figura 23, se asume que el Router A es el destinatario y el Router C es el remitente. El Router B y el Router C pertenecen al mismo Sistema Autónomo, identificado como AS 45000, lo que implicaría que la comunicación entre estos enrutadores sería de tipo iBGP (Border Gateway Protocol interno). Por otro lado, los

demás Sistemas Autónomos se consideran pares, debido a que cuentan con un acuerdo conjunto y políticas compartidas. En la red presentada, se identifican dos rutas disponibles.

1. RouterC >>> RouterD >>> RouterE >>> RouterA

2. Router C >>> Router B >>> Router A.

Según los criterios de selección de ruta en BGP mencionados anteriormente, se selecciona la ruta 2 y también se anuncia en toda la red. Aunque hay otra forma posible en la que el tráfico puede propagarse, simplemente se ignora. Si un enlace en la ruta falla, se envía un anuncio de retiro de ruta a todos los routers. Nuevamente, el proceso de selección de ruta comienza y busca la siguiente mejor ruta y luego propaga el tráfico a través de la siguiente mejor ruta. Si esta ruta también falla, debe seguir el mismo procedimiento desde cero. Este mensaje de falla se envía a través del mensaje UPDATE en la red. Veamos qué tipo de mensajes se propagan en el protocolo BGP.

1. Formato de mensajes BGP

En una red, si los routers utilizan BGP, intercambian mensajes para compartir su información de enrutamiento y para informar cualquier incidente en la red. Los incidentes pueden ser cambios de ruta, fallas de red o fallas de configuración. BGP tiene diferentes formatos de mensaje para cada uno de estos incidentes. Básicamente, hay 4 tipos principales de mensajes:

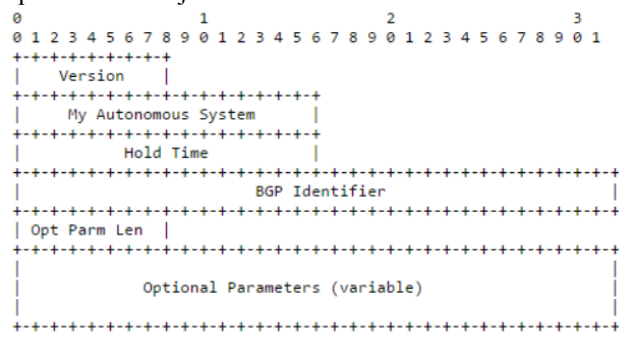

Fig. 24. BGP Open Message Format.

1.1 Open:

Cuando se configura BGP en el router, se envía este mensaje para establecer la conexión con el vecino.

Este es el primer mensaje que se intercambia entre los pares de BGP después de que se establece la conexión. Cada par de BGP intercambia este mensaje para presentar e introducir sus parámetros a los vecinos. Comparan sus parámetros operativos y mantienen un acuerdo para que su interconexión sea exitosa. El mensaje OPEN tiene los siguientes parámetros como se observa en la figura 24.

- *Versión:* Se especifica la versión de BGP que se está implementando, siendo la versión 4 la predeterminada. Es importante que las versiones de BGP coincidan entre los pares que se comunican. En caso de que las versiones sean diferentes, el orador BGP con la versión más alta podría reducir sus capacidades de versión para cumplir con la política de interconexión o, de lo contrario, cerrar la conexión.
- *Sistema Autónomo:* Este campo indica en qué Sistema Autónomo (AS) se encuentra el par de BGP emisor. Cada Sistema Autónomo se identifica con un Número de Sistema Autónomo (ASN) único asignado por la IANA, con un rango de 0 a 65535. Por lo tanto, el campo "Mi Sistema Autónomo" en el mensaje OPEN proporciona el número de sistema autónomo al vecino. Cada enrutador en la red anuncia su ASN a los demás vecinos mediante un mensaje de apertura.
- *Tiempo de espera:* El campo de tiempo de espera en el mensaje de apertura indica el tiempo máximo requerido para que transcurran los mensajes de ACTUALIZACIÓN o KEEPALIVE recibidos sucesivamente. Cada orador de BGP debe configurar su tiempo de espera después de la interconexión. De forma predeterminada, se establece en cero.
- *Identificador de BGP:* El identificador de BGP es el campo que indica la dirección IP de ese enrutador en particular.
- *Parámetros opcionales y longitud:* Los parámetros opcionales se pueden establecer mediante acuerdo. La longitud de este campo se establece en cero de forma predeterminada. Este campo se activa si los vecinos acuerdan compartir algunos parámetros adicionales.

1.2 Update: Tras establecer la conexión, se emite este mensaje de actualización con el propósito de intercambiar información de enrutamiento entre los nodos cercanos.

Los mensajes de actualización son los mensajes que llevan información de enrutamiento entre los pares de BGP. Un mensaje de actualización contiene cierta información con la cual podemos construir un grafo que describe la relación entre los diversos Sistemas Autónomos. Este mensaje de actualización se puede utilizar para detectar bucles de enrutamiento y otros defectos y luego eliminarlos del enrutamiento entre sistemas autónomos.

Un mensaje de actualización contiene toda la información sobre la publicación de una ruta factible a un par o para retirar múltiples rutas del servicio. Un mensaje de actualización puede tanto publicar una ruta factible como retirar múltiples rutas no confiables del servicio simultáneamente. Se profundizará en el contenido del mensaje de actualización en la sección de Publicación de Rutas, puesto que juega un rol fundamental en el proceso de difusión de las rutas

1.3 Notification: Este mensaje se envía para notificar si hay algún problema en la red. Por lo general, se utiliza para cerrar una conexión.

Este mensaje se envía cuando hay alguna condición de error en la red. Cuando se recibe este mensaje, se cierra la conexión de BGP. Podemos ver su formato en la figura a continuación.

1.4 Keepalive: Este mensaje se intercambia para realizar un seguimiento del estado de la sesión.

BGP utiliza el mensaje keepalive para evitar que el temporizador de espera expire. Este mensaje se intercambia entre los pares para mantener la accesibilidad. El intervalo de tiempo entre estos mensajes es de 1/3 del intervalo de tiempo de espera. Si el temporizador de espera se establece en cero, no se enviará ningún mensaje keepalive.

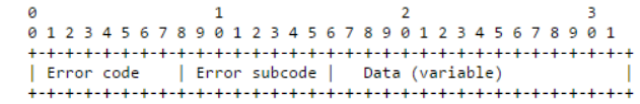

Fig. 25. Notification Message Format.

Contiene tres campos:

- Código de error.

- Subcódigo de error.
- Datos.

Al observar el código de error y el subcódigo, podemos identificar dónde está ocurriendo el problema. Hay alrededor de seis tipos de códigos de error, y cada uno tiene sus propios subcódigos. A continuación se muestra la clasificación de los códigos y subcódigos que nos indican el evento desencadenante:

Código de error 1: Error en el encabezado del mensaje
- ❖ Subcódigo de error:
  - ➔ Conexión no sincronizada
  - ➔ Longitud de mensaje incorrecta
  - ➔ Tipo de mensaje incorrecto

Código de error 2: Error en el mensaje open.
- ❖ Subcódigo de error:
  - ➔ Número de versión no admitido
  - ➔ AS de par incorrecto
  - ➔ Identificador de BGP incorrecto
  - ➔ Número de versión no admitido
  - ➔ Fallo de autenticación
  - ➔ Tiempo de espera no aceptable

Código de error 3: Error en el mensaje de actualización.
- ❖ Subcódigo de error:
  - ➔ Lista de atributos mal formada
  - ➔ Atributo bien conocido no reconocido
  - ➔ Error en las banderas del atributo
  - ➔ Error en la longitud del atributo
  - ➔ Error en la longitud del atributo
  - ➔ Atributo de origen inválido
  - ➔ Bucle de enrutamiento de AS
  - ➔ Atributo de siguiente salto inválido
  - ➔ Error en atributo opcional

Hemos analizado los formatos de los mensajes de BGP. De la misma manera, BGP tiene sus estados de vecino a través de los cuales cada sesión de BGP debe pasar. Estos estados nos indican qué está sucediendo exactamente con esa sesión en particular. Ahora veamos cada estado en detalle a través de su mecanismo llamado Mecanismo de Estado Finito de BGP.

También existe otro tipo de mensaje opcional llamado Route-Refresh. Esta capacidad debe estar habilitada en el enrutador que implementa BGP. Se utiliza este mensaje para actualizar las rutas en caso de cambios en las políticas u otros cambios.

2. Máquina de estados finitos de BGP

Existen un total de seis estados diferentes de BGP en los que podemos encontrar una sesión de BGP. Son los siguientes:

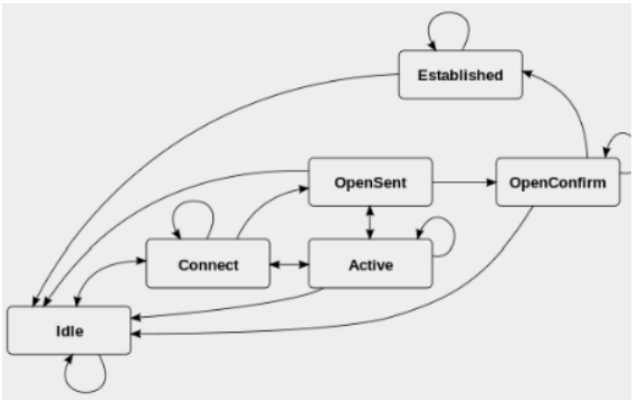

Fig. 26. BGP Finite State Machine

La siguiente figura 26 muestra el flujo en la Máquina de Estados Finitos de BGP. Cada vez que hay una sesión de BGP, el primer estado que aparece será el estado Idle. Analizaremos cada estado y su flujo en la siguiente sección.

- *Estado Idle*
  Este es el primer estado que se inicia cuando BGP se configura en el dispositivo. El estado Idle también se puede alcanzar cuando ocurre un error en cualquier otro estado. Los pares pierden su conexión y el enrutador pasa al estado Idle. BGP siempre comienza con un estado Idle y pasa al estado Connect para una conexión TCP.
- *Estado Connect*
  En este estado, BGP espera a que se establezca la conexión TCP entre los pares. Si la conexión TCP es exitosa, se envía un mensaje OPEN al vecino y se avanza al estado OpenSent. Si la conexión no va bien, entonces se pasa al estado Active para volver a intentar la conexión. Si hay algún problema en el enlace, entonces se vuelve al estado Idle.
- *Estado Active*
  Este estado significa que se está buscando activamente establecer la conexión. No debemos confundirnos con el nombre, ya que aún no está conectado. Cualquier conexión fallida resultará en el estado Active. Cuando expira el temporizador en este estado, se vuelve al estado Connect para reconectar. Si la conexión es exitosa sin problemas, entonces se procede al siguiente paso.
- *Estado OpenSent*
  En esta etapa, se produce cuando el vecino recibe el mensaje "OPEN" y aguarda su correspondiente respuesta. Si el vecino recibe de manera satisfactoria el mensaje "OPEN," entonces transita hacia el estado OpenConfirm. Sin embargo, si se detectara algún error en el mensaje "OPEN" recibido por el vecino, se procederá a enviar un mensaje de Notificación al mismo, volviendo así al estado Idle. Asimismo, si se presentara algún inconveniente en cuanto a la conectividad, se realizará la transición al estado Active con el fin de llevar a cabo el proceso de reconexión.
- *Estado OpenConfirm*
  En este estado, simplemente se espera un mensaje Keepalive o un mensaje de Notificación. Si se envía un mensaje Keepalive, entonces se pasa al estado Established; de lo contrario, si algo sale mal, se envía un mensaje de notificación y se vuelve al estado Idle.
- *Estado Established*
  Este estado se alcanza cuando la sesión de BGP está completamente establecida. Esto significa que los pares de BGP pueden intercambiar exitosamente sus actualizaciones. Si hay una falla en el enlace o algún error, entonces se sigue el mismo proceso anterior: se envía un mensaje de notificación que contiene un código de error y se devuelve al estado Idle.

IV. Aplicaciones

A. *Nivel Nacional*

La tesis para optar el grado de “Magíster en Ingeniería de las Telecomunicaciones” por la Pontificia Universidad Católica del Perú la cual se titula “Implementación de mecanismos de transición al protocolo IPv6 en VNUML y en una red Windows” realizada por Vivas,Jesús (2017) tras la problemática que el Organismo Supervisor de Inversión Privada en Telecomunicaciones ha propuesto un Reglamento sobre Neutralidad de Red que incluye un requisito relacionado con la adopción del protocolo IPv6. Según esta propuesta, la adopción de IPv6 no debe afectar ni restringir el acceso normal a Internet por parte de los usuarios, incluyendo el uso de aplicaciones, protocolos, servicios u otro tipo de tráfico. Sin embargo, algunos proveedores de servicios han retrasado la implementación de IPv6, lo que ha generado problemas y un aumento en los costos. Para abordar la creciente demanda de direcciones IP, se sugiere el uso de CG-NAT. Además, se proponen mecanismos de transición para facilitar la adopción de IPv6, como Túneles 6to4, Túneles 6RD y DNS64 + NAT64. Estos mecanismos pueden aplicarse en el Enrutamiento Dinámico IPv6 en un entorno Windows.

La Figura 26 muestra el sexto escenario, un túnel 6to4 en cada router frontera de las redes privadas IPv6. El tráfico de IPv6 destinado a la red IPv6 nativa es dirigido mediante un túnel IPv4 hacia uno de los router relays 6to4. Del mismo modo, el tráfico desde la red IPv6 nativa hacia los hosts IPv6 es enrutado a través de un túnel IPv4 hacia el router frontera de la red privada IPv6 y, finalmente, hacia el host de destino.

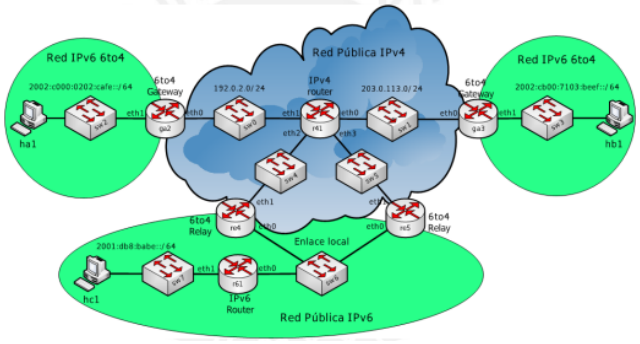

Fig 26. Topología del escenario 6to4.

En la Figura 27 se pueden observar túneles establecidos entre los relay de frontera.

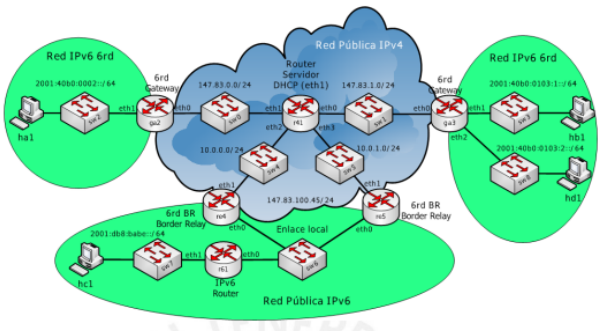

Fig 27. Topología

B. *Nivel Internacional*

La investigación titulada “An Evaluative Analysis of DUAL, SPF and Bellman-Ford” en español “Un análisis Evaluativo de DUAL, SPF y Bellman-Ford” de Tayeb, S., & Latifi, S. (2016) en el Departamento de Ingeniería Eléctrica e Informática, Universidad de Nevada, Estados Unidos. Su objetivo es analizar los protocolos de enrutamiento dinámico que se basan en algoritmos que calculan las rutas más cortas utilizando dígrafos ponderados y recorridos de árboles. En este documento, también se realiza un análisis en profundidad de las diversas características de los protocolos. Algunas de las características son abandonar la periodicidad de los mensajes de actualización y operar en función de los eventos con capacidad de conmutación por error automática. Parte de la novedad de este artículo radica en la representación matemática de los procesos de toma de decisiones y el cálculo de métricas. Uno de los hallazgos notables es un análisis evaluativo de los tiempos de convergencia logrados en una implementación típica de enrutamiento de un campus universitario, se muestra la topología lógica en la Figura 28. Donde concluyeron que EIGRP puede proporcionar tiempos de convergencia más cortos con un tráfico de red mínimo. Este protocolo solía denominarse híbrido; sin embargo, se basa únicamente en un algoritmo de vector de distancia y, por lo tanto, debe denominarse vector de distancia avanzado.

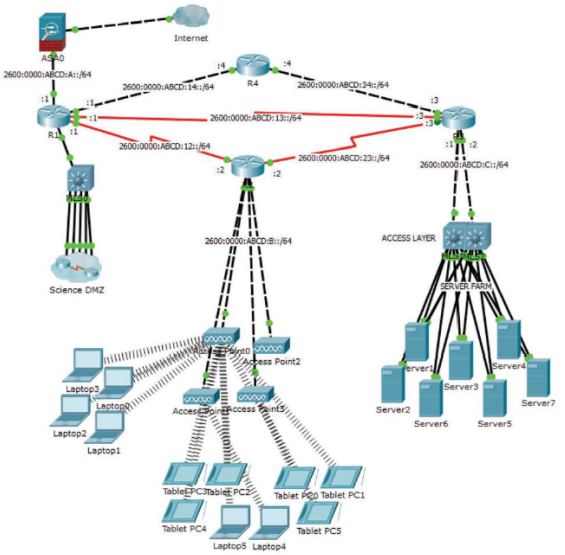

Fig. 28 . Topología lógica del experimento en Packet Tracer

V. Análisis e interpretación de los resultados de la revisión sistemática

En el artículo de título “Análisis Evaluativo de DUAL, SPF y Bellman-Ford”, también se evaluó la popularidad de los protocolos dinámicos que cambian con el tiempo. La popularidad de búsqueda en la web utilizados entre enero de 2004 y abril de 2016 se ilustra en la Figura 19. Estos números lo obtuvieron utilizando las tendencias de búsqueda de Google.

Se utiliza una escala de popularidad que va desde 0 hasta 100 para evaluar los términos. Un valor de 100 indica el punto máximo de popularidad del término, mientras que un valor de 50 significa que el término es la mitad de popular en comparación con el máximo. Se observa que todos los protocolos de enrutamiento han perdido su popularidad significativamente entre 2004 y 2016, excepto

EIGRP, que sólo experimentó un declive a pesar de que ha sido un protocolo propietario y no se ha adoptado ampliamente.

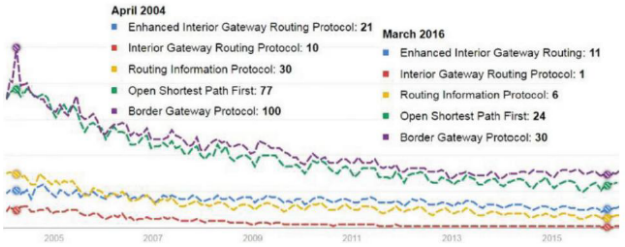

Fig 29. Tendencias de popularidad de los protocolos de enrutamiento dinámico 2004-2016.

Dentro de la evolución, los términos "standard" (estándar), "proprietary" (propio) y "in progress" (en progreso) se refieren al estado y la categoría de un protocolo en relación con su desarrollo y adopción. Como se muestra en la Figura 20, donde esta evolución según los autores, implica la aparición de nuevos protocolos, mejoras en los protocolos existentes y la adopción generalizada de los estándares más maduros. Los protocolos estándar tienden a ser preferidos debido a su interoperabilidad, documentación abierta y capacidad de implementación multiplataforma.

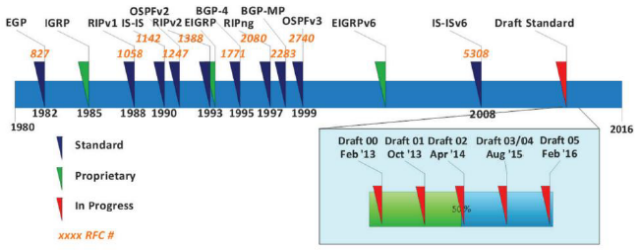

Fig 30. Evolución de los protocolos de enrutamiento dinámico.

En esta revisión sistemática, hemos llevado a cabo una comparación de los protocolos de enrutamiento dinámico utilizando también Google Trends, analizando los datos desde 2017 hasta el presente año 2023, cuyos resultados se encuentran en la Figura 20. El gráfico refleja que RIP ha mantenido valores constantes en el tiempo, situándose en 23 y 63. Sin embargo, se observa una leve disminución en el mismo periodo para los protocolos EIGRP y OSPF. Esta tendencia actual difiere de investigaciones anteriores realizadas en 2016.

En la actualidad, los protocolos de enrutamiento dinámico se enfocan en mejorar la escalabilidad, el rendimiento y la eficiencia de las redes, además de adaptarse a las nuevas demandas y tecnologías emergentes. Es por ello que BGP ha experimentado un incremento, posiblemente debido a su uso en el nivel de sistemas autónomos en Internet. BGP es esencial para el intercambio de información de enrutamiento entre proveedores de servicios de Internet (ISPs) y para el funcionamiento general de Internet. Asimismo, hemos representado esta información con un desglose comparativo por regiones del mundo a través de un mapa, como se muestra en la Figura 31.

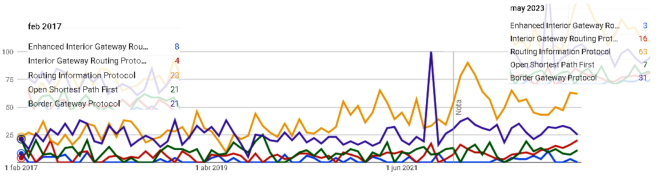

Fig 31. Tendencias de popularidad de los protocolos de enrutamiento dinámico 2017-2023.

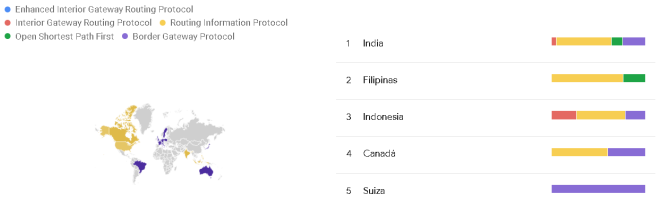

Fig 32. Comparación entre los cinco países a nivel mundial de Tendencias de popularidad de los protocolos de enrutamiento dinámico 2017-2023.

Los algoritmos de enrutamiento dinámico, como Bellman-Ford, DUAL (Diffusing Update Algorithm) y SPF (Shortest Path First), son fundamentales en la determinación de las mejores rutas de enrutamiento en redes. Una comparación de las características entre estos algoritmos se encuentra en la Tabla 3.

TABLA 3.

COMPARACIÓN ENTRE EIGRP, OSPFV2 Y RIPV2

Características y Funciones	**Protocolos Enrutamiento**		
	EIGRP	***OSPFv2***	***RIPv2***
Algoritmo	DUAL	SPF	Bellman-ford
Jerarquía	Área única, jerárquica mediante agregación.	Multiárea	Departamento
Tipo	Vector Distancia	Estado de Enlace	Vector Distancia
Métrica	Ecuación compuesta	Costo (ancho de banda) Número de saltos	
IGP / EGP	o IGP o EGP	Solo IGP	Solo IGP
CPU	Bajos Requisitos	Altos Requisitos	Muy Bajos Requisitos
Complejidad	Mediocre	Complicado	Simple
Multiprotocolo	IPv4/v6, IPX y AppleTalk	IPv4/v6	IPv4/v6

VI. CONCLUSIONES

En resumen, los protocolos de enrutamiento dinámico son esenciales para permitir la conectividad automática, la adaptabilidad a cambios en la topología de red, una rápida convergencia, el balance de carga y la eficiencia en las

redes. Estos protocolos brindan una gestión automatizada y eficiente de las rutas de enrutamiento, lo que facilita una comunicación fluida y confiable en entornos de red en constante cambio y expansión.

Los algoritmos de enrutamiento dinámico, como Bellman-Ford, DUAL (Diffusing Update Algorithm) y SPF (Shortest Path First), son fundamentales para determinar las mejores rutas de enrutamiento en redes de diversos tamaños y complejidades. Cada algoritmo tiene características específicas que los hacen eficientes, confiables y adaptables en diferentes entornos de red. Bellman-Ford es adecuado para manejar topologías complejas y bucles en redes pequeñas, DUAL ofrece convergencia rápida y estabilidad en redes grandes, mientras que SPF calcula las rutas más cortas basadas en costos y permite una selección eficiente de rutas. En conjunto, estos algoritmos son cruciales para un enrutamiento dinámico efectivo en redes.

Actualmente, los protocolos de enrutamiento más utilizados y populares incluyen OSPF, BGP, EIGRP y IS-IS. Estos protocolos son escalables, eficientes y se adaptan a entornos de red complejos. OSPF es ideal para redes internas, BGP se emplea para el enrutamiento entre sistemas autónomos en Internet, EIGRP es común en dispositivos Cisco y IS-IS es empleado por proveedores de servicios. Estos protocolos son esenciales para lograr un enrutamiento dinámico eficiente en redes de diferentes tamaños y necesidades.

Referencias

[1] Albaour, A., & Aburawi, Y. (2021). Performance Comparison of Routing Protocols. International Research Journal of Engineering and Technology (IRJET), 8(2), 1-5.

[2] Alemany, E. D., Gigena, C. E., & Giovanardi, G. W. E. (2018). RIP (Routing information Protocol) Análisis y simulación.

[3] Balchunas, A. (2020, octubre 1). IS-IS. Routeralley.com. https://www.routeralley.com/guides/isis.pdf

[4] Biradar, A. G. (2020, December). A comparative study on routing protocols: RIP, OSPF and EIGRP and their analysis using GNS-3. In 2020 5th IEEE international conference on recent advances and innovations in engineering (ICRAIE) (pp. 1-5). IEEE.

[5] Cabeza, E. C. (2009). Fundamentos de Routing. Eduardo Collado Cabeza.

[6] Comprender OSPF (ruta de acceso más corta primero): guía de diseño. (2022, 3 noviembre). Cisco. https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

[7] Doyle, J., & Carroll, J. D. (2001). Routing TCP/IP, Volume II: CCIE Professional Development. Cisco Press.

[8] Gallon R.(1990). Use of OSIIS-IS for Routing in TCP/IP and Dual Environments. RFC 1195

[9] Hu, Y.-C., Perrig, A., & Sirbu, M. (2004). SPV: Secure path vector routing for securing BGP. Ethz.ch. https://netsec.ethz.ch/publications/papers/spv.pdf

[10] Introducción a EIGRP. (2022). Cisco. https://www.cisco.com/c/es_mx/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/13669-1.html

[11] Introducción a IGRP. (2022). Cisco. https://www.cisco.com/c/es_mx/support/docs/ip/interior-gateway-routing-protocol-igrp/26825-5.html

[12] Kurose, J. F., & Ross, K. W. (2021). Computer networking: A top-down approach.(7th ed.). Pearson.

[13] Lara Castañón, A. (2011). Algoritmo de enrutamiento para IPv6. Licenciatura en Ingeniería en Sistemas Computacionales.

[14] Liu, D., Barber, B., & DiGrande, L. (2009). Routing Protocols. Cisco CCNA/CCENT Exam 640-802, 640-822, 640-816 Preparation Kit, 169–196. doi:10.1016/b978-1-59749-306-2.00009-9

[15] López Bulla, R. (2018). Enrutamiento y configuración de redes. Recuperado: https://digitk.areandina.edu.co/handle/areandina/1495

[16] Marcelo. (2020). Introducción a OSPF. CCNA Desde Cero. https://ccnadesdecero.com/curso/ospf/

[17] Medhi, D., & Ramasamy, K. (2007). IP Routing and Distance Vector Protocol Family. Network Routing, 142–164. doi:10.1016/b978-012088588-6/50009-7

[18] Mier Ruiz, E., & Mier Ruiz, G. (2008). Protocolos de enrutamiento rip, ospf y eigrp.

[19] Moy J.T .(1998). OSPF: Anatomy of an Internet Routing Protocol. Addison-Wesley Professional

[20] Parasa, S. K. (2016). BGP Routing Protocol. Suny.edu. https://dspace.sunyconnect.suny.edu/bitstream/handle/1951/68236/Sai-Parsa.pdf?sequence=1&isAllowed=y

[21] Prácticas de Redes. (2010). España: Julián Verón Piquero.Sulaiman, O. K., Siregar, A. M., Nasution, K., & Haramaini, T. (2018, April). Bellman Ford algorithm-In Routing Information Protocol (RIP). In Journal of Physics: Conference Series (Vol. 1007, No. 1, p. 012009). IOP Publishing.

[22] Tayeb, S., & Latifi, S. (2016). An Evaluative Analysis of DUAL, SPF, and Bellman-Ford.

[23] Wai, K. K. (2019). Analysis of RIP, EIGRP, and OSPF Routing Protocols in a Network. International Journal of Trend in Scientific Research and Development (IJTSRD), 219(3), 5.

[24] Vivas J.(2017). Implementación de mecanismos de transición al protocolo IPv6 en VNUML y en una red Windows.