DOCUMENTACIÓN, IMPLEMENTACIÓN Y ELABORACIÓN DE GUÍAS DE LABORATORIO SOBRE PROTOCOLOS DE ENRUTAMIENTO EN LA RED: RIP, IS-IS, OSPF Y BGP; BASADOS EN UN SOFTWARE DE SIMULACIÓN

ROBINSON ALVARADO CADENA

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE INGENIERÍA Y ADMINISTRACIÓN
PROGRAMA DE INGENIERÍA ELECTRÓNICA
2010

DOCUMENTACIÓN, IMPLEMENTACIÓN Y ELABORACIÓN DE GUÍAS DE LABORATORIO SOBRE PROTOCOLOS DE ENRUTAMIENTO EN LA RED: RIP, IS-IS, OSPF Y BGP; BASADOS EN UN SOFTWARE DE SIMULACIÓN

ROBINSON ALVARADO CADENA

Trabajo de grado presentado como requisito parcial para optar por el título de Ingeniero Electrónico

Director de tesis
PhD. JHON JAIRO PADILLA AGUILAR
Ingeniero Electrónico

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE INGENIERÍA Y ADMINISTRACIÓN
PROGRAMA DE INGENIERÍA ELECTRÓNICA
2010

Nota de Aceptación

_____

_____

_____

_____

Firma del jurado

Bucaramanga, Julio de 2010

DEDICATORIA

A mi familia.

Robinson Alvarado Cadena

AGRADECIMIENTOS

A Jhon Jairo Padilla Aguilar, nuestro director de proyecto por su apoyo y sabios aportes en el desarrollo de este proceso.

A la Universidad Pontificia Bolivariana, por brindar tan valiosas enseñanzas en el transcurso como estudiantes de ingeniería.

A los amigos, compañeros de clases y profesores quienes en su momento hicieron contribuciones en la formación.

TABLA DE CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

Ancho de banda: Medida de la capacidad de transmitir información.

Área: Conjunto de redes dentro de un sólo AS que se han agrupado juntas.

AS (Autonomous System): Un sistema autónomo es un conjunto de redes administradas por una misma organización que tiene definida una única política de encaminamiento.

Backbone: También denominado **área** cero, forma el núcleo de una red **OSPF.**

BGP: Es un protocolo de enrutamiento por vector de distancia usado comúnmente para enrutar paquetes entre dominios, estándar en Internet. BGP gestiona el enrutamiento entre dos o más routers que sirven como routers fronterizos para determinados Sistemas Autónomos.

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.

Interdomain: Este término se utiliza para describir la interacción entre dominios. Comúnmente se utiliza en los campos de enrutamiento entre internets, o AS.

Interfaz (fisica): Se conoce como **interfaz física** a los medios utilizados para la conexión de un computador con el medio de transporte de la **red.**

Intradomain: Es una interconexión de servidores dentro de un solo dominio.

IS-IS: Protocolo de enrutamiento de estado de enlace, que utiliza el algoritmo Dijkstra, para determinar camino más corto.

LSA: Los cambios en el estado de los enlaces de un *router* son notificados a la red mediante el envío de mensajes LSA (Link State Advertisment)).

Métrica: La métrica es el análisis, y en lo que se basa el algoritmo del protocolo de enrutamiento dinámico para elegir y preferir una ruta por sobre otra, basándose en eso el protocolo creará la tabla de enrutamiento en el router, publicando sólo las mejores rutas. Un protocolo de enrutamiento utiliza la métrica para determinar qué vía utilizar para transmitir un paquete a través de un Intercambio. La métrica incluye numero de saltos, ancho de banda, retraso,carga y fiabilidad.

Multicast: Es el envío de la información en una red a múltiples destinos simultáneamente, usando la estrategia más eficiente para el envío de los mensajes sobre cada enlace de la red sólo una vez.

NET: Especifica uno o más identificadores del router. Cada router debe tener al menos una entidad de red especificada (NET). Un router puede tener múltiples NETs, pero cada NET debe ser único dentro de la red.

OSPF: Es un protocolo universal basado en el algoritmo de estado de enlace, utiliza el algoritmo Dijkstra enlace-estado (LSA - *Link State Algorithm*) que le permite calcular la distancia más corta entre la fuente y el destino al determinar la ruta para un grupo específico de paquetes.

Paquete: Los paquetes pueden estar formados por una cabecera, una parte de datos y una cola. En la cabecera estarán los campos que pueda necesitar el protocolo de nivel de red, en la cola, si la hubiere, se ubica normalmente algún mecanismo de comprobación de errores.

RIP: RIP es un protocolo universal de enrutamiento por vector de distancia que utiliza el número de saltos como único sistema métrico.

Router: Dispositivo físico o lógico que permite encaminar la conexión entre redes TCP/IP, es el encargado de que los paquetes de información lleguen a su destino.

System Type: Hace referencia a la configuración de los routers IS-IS para establecer su función en una respectiva área. Puede ser Level 1, Level 2 o Level 1-2.

Tabla de enrutamiento: Es un documento electrónico que almacena las rutas a los diferentes nodos en una red informática. La Tabla de enrutamiento generalmente se almacena en un router o en red en forma de una base de datos. Cuando los datos deben ser enviados desde un nodo a otro de la red, se hace referencia a la tabla de enrutamiento con el fin de encontrar la mejor ruta para la transferencia de información.

Unicast: Unicast es el envío de información desde un único emisor a un único receptor.

RESUMEN GENERAL DE TRABAJO DE GRADO

TÍTULO: DOCUMENTACIÓN, IMPLEMENTACIÓN Y ELABORACIÓN DE GUÍAS DE LABORATORIO SOBRE PROTOCOLOS DE ENRUTAMIENTO EN LA RED: RIP, IS-IS, OSPF Y BGP; BASADOS EN UN SOFTWARE DE SIMULACIÓN[*]

AUTOR: ROBINSON ALVARADO CADENA[**]

FACULTAD: INGENIERIA ELECTRÓNICA
DIRECTOR: PhD. JHON JAIRO PADILLA AGUILAR

CONTENIDO:

Este proyecto de grado se realizó con el fin de implementar unas guías de laboratorio sobre los protocolos de enrutamiento en la red: RIP, OSPF, BGP e IS-IS; basados en un software de simulación (Opnet Modeler) para realizar todo un análisis sobre las características de cada uno de estos. La documentación previa de cada uno de los protocolos permitió una mejor comprensión y aplicabilidad para desarrollar Ingeniería de Tráfico garantizando calidad de servicio (QoS), teniendo en cuenta las ventajas y desventajas de cada uno.

PALABRAS CLAVES: RIP, OSPF, BGP, IS-IS, costo, ancho de banda, retardo, Ingeniería de Tráfico, Opnet Modeler, Protocolos de enrutamiento.

---

[*] PROYECTO DE GRADO

[*] ESCUELA DE INGENIERÍA Y ADMINISTRACIÓN. PROGRAMA DE INGENIERÍA ELECTRÓNICA. JHON JAIRO PADILLA AGUILAR

GENERAL SUMMARY OF WORK OF DEGREE

TITLE: DOCUMENTATION, IMPLEMENTATION AND DEVELOPMENT OF LAB MANUALS ON ROUTING PROTOCOLS OVER DATA NETWORKS: RIP, IS-IS, OSPF Y BGP; BASED ON A SIMULATION SOFTWARE [*]

AUTHOR: ROBINSON ALVARADO CADENA[**]

FACULTY: ELECTRONIC ENGINEERING
DIRECTOR: PhD. JHON JAIRO PADILLA AGUILAR

CONTENT:

This project was performed with the purpose to create some lab practices for the Networking laboratory. These practices are focused in network routing protocols; they are based on a simulation software (Opnet Modeler) that allows to perform several analysis about characteristics of each one. Also they allow a better comprehension and applicability of such protocols in developing Traffic Engineering and support of Quality of Service, taking into account advantages and disadvantages of each routing protocol.

KEY WORDS: RIP, OSPF, BGP, IS-IS, cost, bandwidth, delay, Traffic Engineer, Opnet Modeler, Routing Protocols.

VoBo DIRECTOR

---

[*] WORK PROJECT

[*] SCHOOLL OF ENGINEERING AND MANAGEMENT. ELECTRONICS ENGINEERING PROGRAM. JHON JAIRO PADILLA AGUILAR

1. INTRODUCCIÓN

En la década de 1980, se dió un gran auge en el crecimiento del enrutamiento (cantidad y tamaño de las redes): El enrutamiento de la Internet se desplegó bajo la arquitectura de protocolos TCP / IP; utilizando primero el protocolo RIP, la red telefónica comenzó a desplegar sistemas de llamadas de enrutamiento dinámico, mientras que la red de transporte de telecomunicaciones utilizó los mecanismos de transporte SONET.

El enrutamiento en la red puede dividirse en tres categorías básicas fundamentales: enrutamiento de paquetes, enrutamiento de conmutación de circuitos, y enrutamiento de transporte, aunque es posible una combinación entre ellos. La evolución durante el último cuarto de siglo ha traído al primer plano la necesidad de comprender y examinar dónde y cómo las diferentes dimensiones de enrutamiento, desde los algoritmos hasta los protocolos y las arquitecturas, pueden variar para los diferentes tipos de redes.

Teniendo en cuenta que el mecanismo de direccionamiento puede afectar las decisiones de enrutamiento, también se debe tener en cuenta la arquitectura de los routers, ya que la relación entre ingeniería de tráfico y el enrutamiento eficiente son complementos para establecer un mejor servicio en cuanto a transmisión, velocidad, retardo y costo.

Este proyecto permitirá que se tenga una mayor profundización sobre los Protocolos de Enrutamiento en la red y el problema que resuelve la Ingeniería de Tráfico en estas redes; obteniendo un conocimiento claro tanto teórico como práctico sobre sus aplicaciones.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

- Documentar y elaborar prácticas de laboratorio sobre los protocolos de enrutamiento: RIP, IS-IS, OSPF y BGP; basándose en un software de simulación.

2.2 OBJETIVOS ESPECÍFICOS

- Estudiar los conceptos básicos con que operan los protocolos de enrutamiento: RIP, IS-IS, OSPF y BGP.

- Estudiar y analizar el desempeño que proporcionan estos protocolos de enrutamiento al desarrollar ingeniería de tráfico.

- Diseñar y elaborar prácticas de laboratorio que muestren las características de operación que ofrecen los protocolos de enrutamiento en las redes.

3. MARCO TEÓRICO

3.1 PROTOCOLOS DE ENRUTAMIENTO E INGENIERIA DE TRÁFICO

En la actualidad las redes IP traen consigo una serie de nuevos conceptos que deben ser analizados y estudiados con el fin de contribuir a la convergencia de datos, voz y video bajo una misma arquitectura de red.

Uno de los grandes problemas que se presenta al enviar información usando redes IP, es mantener la integridad de los datos y garantizar una comunicación fluida, tanto en velocidad como en efectividad; es por esto que si se logra brindar Calidad de Servicio (QoS) en las aplicaciones que son ofrecidas a los usuarios finales, se logrará mejorar el Grado de Satisfacción (GoS) de ellos hacia las diferentes aplicaciones soportadas por la red.

Es necesario implementar todo un análisis a los diferentes procesos tecnológicos que permiten un buen flujo de la información a través de la red; y la búsqueda del mejor camino (enrutamiento) y deducir cual podría ser el que más garantiza la aplicación del concepto de Calidad del Servicio QoS para redes IP.

Para ello se hace necesario aplicar Ingeniería de Tráfico a estas redes, “la cual tiene como objetivo diseñar sistemas con un costo mínimo y con una capacidad tal que cumpla con un grado de servicio predefinido satisfaciendo la demanda de tráfico a futuro”.

De esta manera los protocolos de enrutamiento en la red desempeñan un papel muy importante. Hay que tener en cuenta las características y aplicaciones que comprende cada uno de estos, como por ejemplo; de la familia del vector distancia: Routing Information Protocol (RIP)[1], Interior GatewayRouting Protocolo (IGRP), y Enhanced Interior Gateway Routing Protocol (EIGRP). Otros dos protocolos que pertenecen a los protocolos de enrutamiento de estado de enlace: Open Shortest Path First (OSPF)[2] e Intermediate System to Intermediate System (IS-IS)[3], y también Border Gateway Protocol (BGP)[4] que es un protocolo de vector de ruta utilizado en la Internet.

Los protocolos de enrutamiento de estado de enlace fueron diseñados para superar las limitaciones de los protocolos de enrutamiento Vector Distancia. Estos últimos solo intercambian actualizaciones con sus vecinos inmediatos, mientras que los primeros tienen pleno conocimiento de los routers distantes y la forma como se interconectan, intercambiando información a través de un área más amplia; utilizan métricas de costo para seleccionar rutas a través de la red, utilizan inundación LSA para informar sobre cambios en la red convergiendo más rápidamente. En los protocolos Estado de Enlace cada router tiene una topología de su propia red, consumen menos ancho de banda, y se ejecuta el algoritmo Dijkstra-Primer camino más corto.

Todo este análisis tiene como propósito entender el funcionamiento del enrutamiento de las redes IP tanto a nivel interno como externo.

---

[1] HEDRICK, C. Routing Information Protocol (RIP): RFC 1058, Rutgers University. June 1988.Disponible en: http://www.freesoft.org/CIE/RFC/1058/index.htm

[2] MOY, J. Open Shortest Path First (OSPF): RFC 2328, Ascend Communications. June 1998.Disponible en: http://www.ietf.org/rfc/rfc2328.txt

[3] SMITH, H. Intermediate System to Intermediate System (IS-IS): RFC 3784, Procket Networks. June 2004.Disponible en: http://www.faqs.org/rfcs/rfc3784.html

[4] REKHTER, Y. Border Gateway Protocol (BGP):RFC 4271, June 2006.Disponible en : http://www.faqs.org/rfcs/rfc4271.html

De cierto modo las redes IP se auto gestionan por medio de estos protocolos, haciendo que la comunicación sea de la mejor calidad posible. Para ello se manejan diferentes métricas ó características de las rutas como son: ancho de banda, retardo, carga, confiabilidad, número de saltos, costo, etc. Donde además ante cualquier cambio en la configuración de la topología de red, los routers están en la capacidad de actualizar sus tablas de enrutamiento para proceder a seleccionar nuevos caminos posibles. Sin embargo, estos mecanismos no garantizan que la red sea lo más eficiente posible. Pues puede pasar que un enlace esté congestionado a pesar que existan enlaces subutilizados en otras partes de la red ó un servicio requerido puede viajar sobre una ruta con alto retardo de propagación cuando un camino de baja latencia está disponible. Es por eso que se requiere hacer más eficiente la administración y el uso de los recursos que se encuentran disponibles en la red, mejorando los tiempos de respuesta hacia los usuarios.

En pocas palabras aplicar Ingeniería de Tráfico a las actuales restricciones en la red, es posible lograr un mejor grado de servicio GoS y una mejor calidad del servicio QoS.[5]

3.2 ROUTING INFORMATION PROTOCOL (RIPv1)[6]

Es el protocolo de enrutamiento utilizado por primera vez en la arquitectura de protocolos TCP/IP, y opera en el dominio interno de una subred IP. Mientras la especificación del RIP fue descrita por primera vez en el RFC 1058 en 1988, sólo

[5] QUINTERO, Edison y ALVARO, Luis. ESTADO DEL ARTE EN LA APLICACIÓN DE INGENIERIA DE TRAFICO EN REDES IP. pdf. Universidad Pontificia Bolivariana.2010

[6] MEDHI, Deepankar y RAMASAMY, Karthikeyan. NETWORK ROUTING Algorithms, Protocols, and Architectures. Oxford, Elsevier: 2007. p. 147

estuvo disponible cuando RIP se editó con la versión 4.3 de Berkeley Software Distribution (BSD).

El nombre de RIP puede ser engañoso ya que todos los protocolos de enrutamiento necesitan intercambiar "información del enrutamiento." RIP debe ser entendido como una instancia de un protocolo de la familia del tipo vector distancia, independientemente de su nombre. Fue uno de los pocos protocolos para los cuales una aplicación fue disponible antes que una especificación fuera oficialmente completa. El RIP original ahora se conoce como RIP versión 1, ó RIPv1 en breve. Desde entonces, ha evolucionado para RIPv2, que es estándar en el RFC 2453.

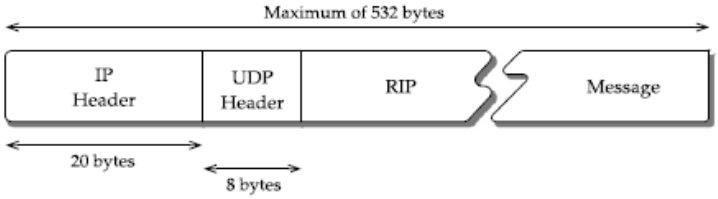
RIP sigue siendo uno de los protocolos de enrutamiento populares para un entorno de red pequeña. De hecho, la mayoría de routers DSL / cable módem como los de Linksys vienen junto con RIP.

3.2.1 Comunicación y formato del mensaje[7]

Dado que la información del vector distancia se obtiene de un router vecino, la comunicación de la información de enrutamiento es siempre entre dos routers vecinos en el caso de RIP. Además, dado que RIP está basado en el protocolo UDP, no hay garantía de que un mensaje de información de enrutamiento sea recibido por un router. Incluso, no se establece periodo de sesiones ya que cada paquete de enrutamiento es encapsulado y enviado al vecino, normalmente a través de radiodifusión. En la siguiente Figura 1 se puede apreciar un paquete de enrutamiento en la arquitectura TCP / IP.

[7] Ibíd., p. 147

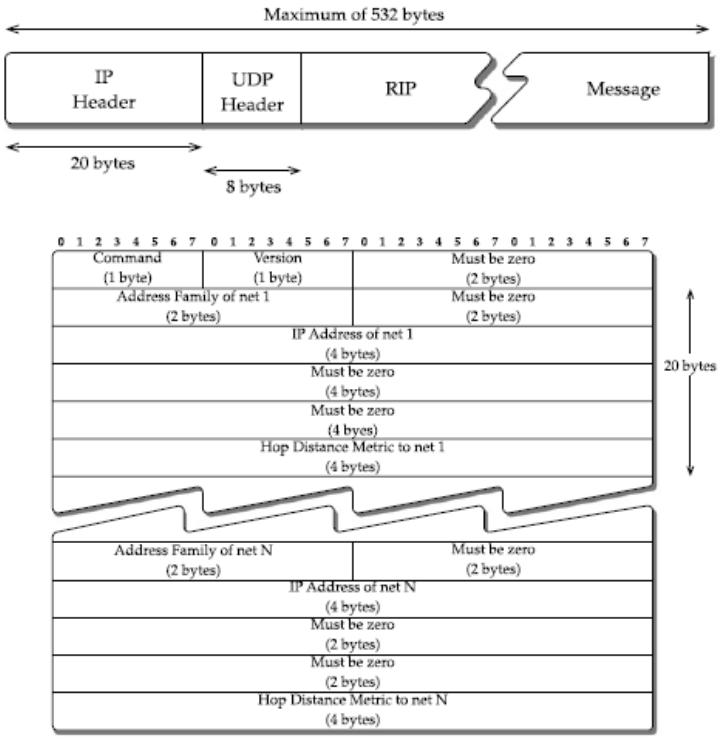
Figura 1. Estructura del mensaje RIP, con cabecera IP y UDP



Fuente: NETWORK ROUTING Algorithms, Protocols, and Architectures.

Ahora, consideremos el formato de un mensaje RIPv1, lo que se muestra en la Figura 2. El formato del paquete para RIPv1 se muestra en 32-bit (4-byte) límites. Un mensaje RIPv1 tiene una cabecera común de 4 bytes, seguido por un mensaje de 20 bytes para cada ruta por el cual el mensaje se está comunicando, hasta un máximo de 25 rutas / direcciones. Así, el tamaño máximo de un mensaje RIP (incluyendo IP / cabeceras UDP) es de $20 + 8 + 4 + 25 \times 20 = 532$ bytes, mientras que el mínimo es de 20 + 8 + 4 + 20 = 52 bytes. Es importante señalar que el tamaño del mensaje no limita el tamaño de la red en términos del número de routers, sino que es en términos del número de redes direccionadas o rutas.

Figura 2. Formato del paquete RIP



Fuente: NETWORK ROUTING Algorithms, Protocols, and Architectures.

Una práctica común de muchos protocolos es tener algunos espacios para futuras mejoras en el protocolo, a menudo, estos espacios están marcados con Must Be Zero. Como puede verse en la Figura 2, hay muchos lugares donde esto ocurre en el formato de mensaje RIPv1; algunos de ellos son utilizados en el formato de mensaje RIPv2.

Así, un mensaje RIPv1 posee los siguientes 5 campos: command, version, address family identifier, IPaddrss, y metric. Estos se describen a continuación:

- **Version (1 byte):** Este campo indica la versión del protocolo RIP. Se establece en 1 para RIPv1.Si este campo pasa a ser cero, el mensaje debe ser ignorado.

- **Address family identifier (2 bytes):** Este campo identifica la familia de direcciones. Se establece en 2 para la familia de direcciones IP. Originariamente, la intención era proporcionar RIP a otras familias de direcciones, aunque en la práctica este formato de paquete RIP no se ha utilizado para cualquier otra familia de direcciones. Hay un caso especial que se usa cuando este campo se establece a cero; vea el campo *command* a continuación.

- **IP Address (4 bytes):** Este es el destino de la red, identificado por la subred o un host.

- **Metric (4 bytes):** Esta basado en el número de saltos; es un número entre 1 y 16, donde 16 significa inalcanzable o infinito.

- **Command (1 byte):** Este campo es utilizado para ajustar diferentes comandos de un mensaje RIPv1. Mientras habían cinco diferentes comandos originalmente definidos, sólo dos se utilizan: *request* y *response*, los otros son obsoletos. El comando de petición puede ser utilizado por un router para solicitarle a un router vecino la información del vector distancia. Si se desea obtener la tabla de enrutamiento completa, un mensaje de solicitud (denominado "request-full") es enviado donde el identificador de la familia de direcciones se establece en 0 y la infinidad de métricas. Sin embargo, si se buscan las respuestas para un conjunto de bloques de direcciones

(denominado "request-partial"), la bandera de solicitud se establece, el identificador de la familia de direcciones se establece en IP, y las direcciones son enumeradas; el router responde enviando una respuesta a todas las direcciones enumeradas. Entendiendo que esta última es una petición especial y no una petición normal. Cabe señalar que la actualización periódica del mensaje del vector distancia también se envía con un comando establecido en modo respuesta. Ya que no hay un campo de identificación para un mensaje RIPv1 (a diferencia, del formato de un mensaje DNS), un router receptor no tiene manera directa de determinar si la respuesta fue una respuesta periódica o una respuesta a su “request-full” o “request-partial”.

3.2.2 Funcionamiento general[8]

Las siguientes son las consideraciones principales de un funcionamiento en lo que respecta al protocolo RIP:

- **Manipulación general de los paquetes:** si algunos de los campos de *must be zero* tiene un valor distinto de *cero* en cualquier lugar o si la versión del campo es *cero*, el paquete es descartado.

- **Inicio:** cuando un router es activado y se determina que todas las interfaces están en funcionamiento, se difunde un mensaje de solicitud que va a todas las interfaces en el modo "request-full".

  Los routers vecinos manejan respuestas siguiendo la regla de *Split horizon*. Una vez que las respuestas son recibidas, la tabla de enrutamiento es actualizada con rutas nuevas que el router ha obtenido.

[8] Ibíd., p. 149

- **Actualizaciones del enrutamiento:** por defecto esto se hace aproximadamente cada 30 segundos (“Autoupdate timer”) donde las actualizaciones son emitidas con los campos de *command* fijados en modo respuesta.

- **Recepción normal de respuesta:** la tabla de enrutamiento es actualizada por hacer la distribución de Bellman Ford, sólo la mejor ruta es guardada para cada destino.

- **Accionado de actualizaciones:** Si la métrica de una red direccionable cambia, un mensaje de actualización se genera sólo con las redes afectadas.

- **Caducidad de ruta:** Si una red direccionable no se ha actualizado durante 3 minutos (“expiration timer”) por defecto, su métrica se ajusta a infinito y es un candidato para ser eliminado. Sin embargo, se mantiene en la tabla de enrutamiento por otros 60 segundos, esta ventana de tiempo extra se refiere como a una colección de basura o como un temporizador de descarga.

3.3 ROUTING INFORMATION PROTOCOL (RIPV2)[9]

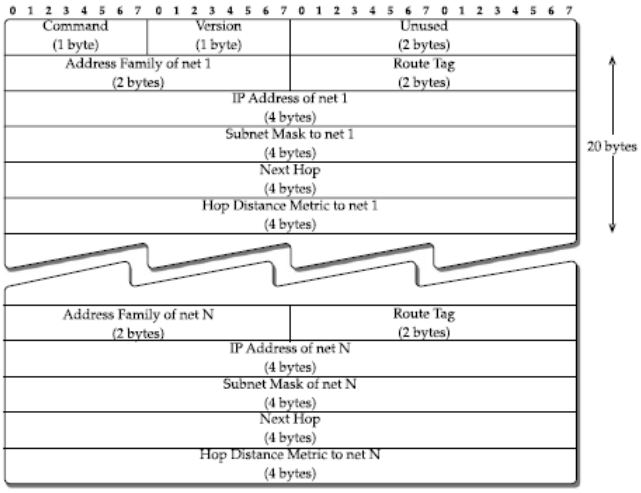
RIPv2 extiende a RIPv1 de varias maneras. La más importante, es que permite enmascarar explícitamente; pero también se introduce la *autenticación*. Autenticación se refiere al uso de algún mecanismo para autenticar el mensaje y / o de su contenido cuando un router lo recibe de tal manera que se sabe que el dato es confiable. Para ello, se introdujeron cambios en el formato del mensaje

[9] Ibíd., p. 150

RIP v1, manteniendo similar el formato general y así aprovechar los campos marcados previamente como *must be zero*.
Esto también demuestra por qué en el diseño de un protocolo, es bueno dejar algunos espacios para futuras mejoras.

En la figura 3 se puede apreciar el formato del paquete para RIPv2, el cual la cabecera común, es decir, los primeros 4 bytes, es el mismo que en RIPv1, en el campo de *version* este se establece en 2, y el campo *must be zero* es etiquetado como: *unused* (sin uso), mientras que *command* puede ser también una petición o una respuesta.

Figura 3. Formato del paquete RIPv2



Fuente: NETWORK ROUTING Algorithms, Protocols, and Architectures.

Esto es lo nuevo a diferencia de RIPv1:

- **Route Tag (2 bytes):** Este campo se presta para diferenciar las rutas internas dentro de un dominio de enrutamiento RIP de las rutas externas. Para las rutas internas, este campo se ajusta en cero. Si una ruta se obtiene de un protocolo de enrutamiento externo, entonces un valor arbitrario o preferiblemente el número del sistema autónomo de la ruta externa se incluye para diferenciarla de las rutas internas.

- **Subnet Mask(4 bytes):** Este campo permite el enrutamiento basado sobre la subred en lugar de hacer clases de enrutamiento, eliminando así una importante limitación de RIPv1. En particular, la variable longitud de la máscara de subred (VLSM) se puede utilizar.

- **Next hop (4 bytes):** Típicamente, un router anunciador es el mejor siguiente salto desde su propio punto de vista sólo cuando permite que sus vecinos conozcan la ruta.

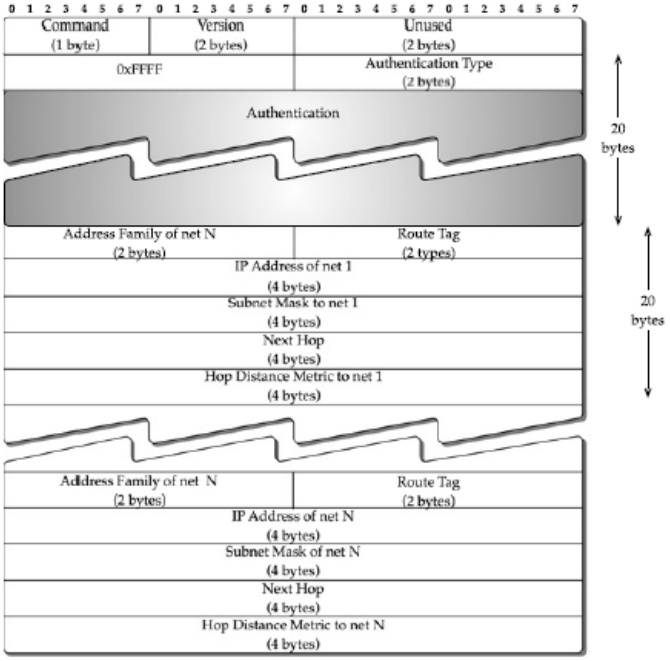
3.3.1 Autenticación[10]

A diferencia de RIPv1, RIPv2 permite una sencilla forma de autenticación. Para la propuesta de autenticación, un primer bloque de entrada de 20 bytes puede ser asignado para la autenticación en lugar de ser una ruta de entrada. Es decir, cuando la autenticación es invocada, un mensaje RIPv2 puede contener sólo un máximo de 24 rutas ya que una ruta de entrada de la tabla se utiliza para la autenticación. El identificador de la familia de direcciones para la parte de autenticación se ha marcado como 0xFFFF(escrito en hexagesimal), y el tipo de autenticación es establecido a 2 para indicar que es una contraseña en texto

[10] Ibíd., p. 151

claro, recordando los 16 bytes que contiene el password. El formato del paquete con autenticación se muestra en la figura 4. Verdaderamente, un password de texto claro no es una muy buena forma de autenticación. Por eso en la práctica no es muy usado.

Figura 4. Formato del paquete RIPv2



Fuente: NETWORK ROUTING Algorithms, Protocols, and Architectures.

Desde una consideración funcional, los mensajes RIPv2 son *multicast* en lugar de *broadcast* como se hizo en RIPv1. Sin embargo, una red puede ser configurada en donde las rutas puedan ser sobre una red *non-broadcast;* un ejemplo de una *red non-broadcast* es una red ATM. Luego, una red *unicast* punto a punto puede ser utilizada para enviar información de enrutamiento. Podemos notar que la familia del identificador de direcciones puede tomar tres valores: 2 para un direccionamiento normal IP, todos los unos para autenticación, en el cual sólo se realiza en la primera ruta de entrada después de la cabecera común, y 0 para un

mensaje de petición para obtener un vector de distancia completa desde un vecino.

3.4 INTERIOR GATEWAY ROUTING PROTOCOL (IGRP)[11]

IGRP fue desarrollado por Cisco primeramente para superar el conteo límite de hop y el conteo métrico de hop para RIPv1. En general, IGRP difiere de RIPv1 de la siguiente manera:

- IGRP se ejecuta directamente sobre IP con el tipo de protocolo establecido en 9.
- El sistema autónomo es aparte de los campos del mensaje.
- Las actualizaciones del vector de distancia incluyen cinco valores de métricas diferentes para cada ruta, aunque una no se utiliza en el cálculo de la métrica compuesta.
- Rutas externas pueden ser anunciadas.
- Permite múltiples caminos de una ruta para la propuesta de balanceo de carga; esto requiere modificación del cálculo de Bellman-Ford para que en lugar de la ruta más sencilla al destino, múltiples “casi” caminos de igual costo puedan ser almacenados.

3.4.1 Formato del paquete

[11] Ibíd., p. 153

El paquete IGRP es bastante compacto, formado por 12 bytes en el campo de la cabecera seguido de 14 bytes para cada entrada de la ruta (ver figura 5). El campo de la cabecera se compone de los siguientes campos:

- **Version (4 bits):** Este campo se establece en 1.
- **Opcode (4 bits):** Este campo es equivalente al código del comando en RIP. 1 es una petición y 2 es una respuesta.

- **Edition (1 byte):** Un contador que es incrementado por el remitente; ayuda a evitar a un router receptor el uso de una vieja actualización (respuesta).

- **Autonomous system number (2 bytes):** Número de identificación de un proceso IGRP.

- **Number of interior routes (2 bytes):** Este campo es para indicar el número de entradas de enrutamiento en un mensaje de actualización en el que las subredes están directamente conectadas a la red.

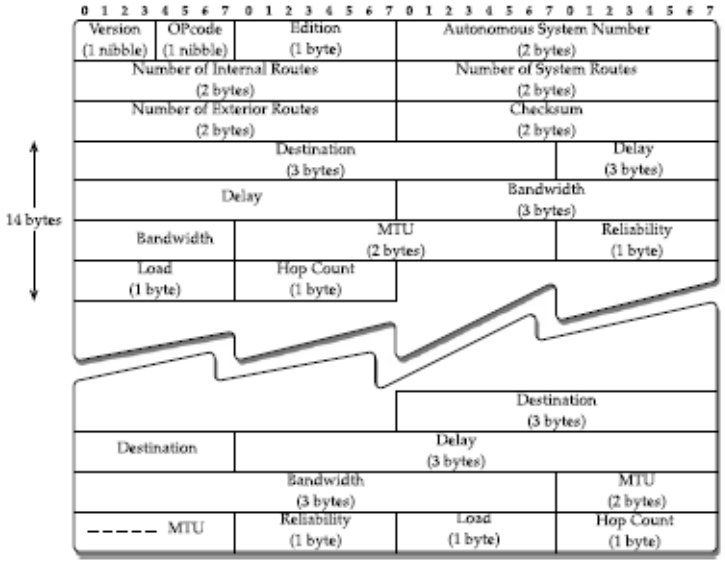
- **Number of system routes (2 bytes):** Esta es una contraparte del número interior de rutas, este campo se utiliza para indicar el número de rutas de entrada que no están directamente conectadas.

- **Number of exterior routes (2 bytes):** Es el número de rutas de entrada que por defecto son las redes. Este y otros dos campos previos, el numero interior de rutas y el número de rutas del sistema, ambos conforman el número total de 14-byte de rutas de entrada.

- **Checksum (3 bytes):** Este valor se calcula sobre el paquete completo IGRP (header + entries).

Para cada ruta de entrada, hay 9 campos que ocupan 14 bytes

Figura 5. Formato del paquete IGRP



Fuente: NETWORK ROUTING Algorithms, Protocols, and Architectures.

- **Destination (3 bytes):** Esta es la red de destino por el cual el vector distancia es generado.

- **Hop count (1 byte):** Un número entre 0 y 255 se usa para indicar el número de hops de destino.

- **MTU (2 bytes):** Es el valor MTU más pequeño de cualquier enlace a lo largo de la ruta hasta el destino.

3.4.2 Cálculo de la métrica compuesta[12]

Un aspecto interesante de IGRP es el método de elaboración que utiliza para calcular la métrica compuesta para representar el costo del enlace; fue incluido para proporcionar la flexibilidad necesaria de un costo del enlace en lugar de sólo usar un número de saltos como un costo del enlace (RIPv1 o RIPv2). La métrica compuesta en IGRP está basada en 4 factores: ancho de banda (B), retardo (D), fiabilidad (R), y carga (L), junto con cinco coeficientes no negativos (K1, K2, K3, K4, K5) para el peso de estos factores.

$$C = \begin{cases} \left(K_1 \times B + K_2 \times \frac{B}{256-L} + K_3 \times D\right) \times \left(\frac{K_5}{R+K_4}\right), & \text{if } K_5 \neq 0 \\ K_1 \times B + K_2 \times \frac{B}{256-L} + K_3 \times D, & \text{if } K_5 = 0. \end{cases}$$

(Ecuación 1).

Este costo métrico compuesto es utilizado en el cálculo de la tabla de enrutamiento. Aquí, el caso especial para K5 = 0 significa que la última parte, K5 / (R + K4), que considera que la fiabilidad de un enlace, no está incluido; en otras palabras, esto significa que si K5 = 0, todos los enlaces tienen el mismo nivel de fiabilidad. En el caso por defecto, K1 = K3 = 1 y K2 = K4 = K5 = 0. Así, la métrica compuesta se reduce a:

$$C_{\text{default}} = B + D.$$

(Ecuación 2).

[12] Ibíd., p. 154

Esto muestra que la compuesta métrica predeterminada es la suma del ancho de banda y del retardo.

3.5 ENHANCED INTERIROR GATEWAY ROUTING PROTOCOL (EIGRP)[13]

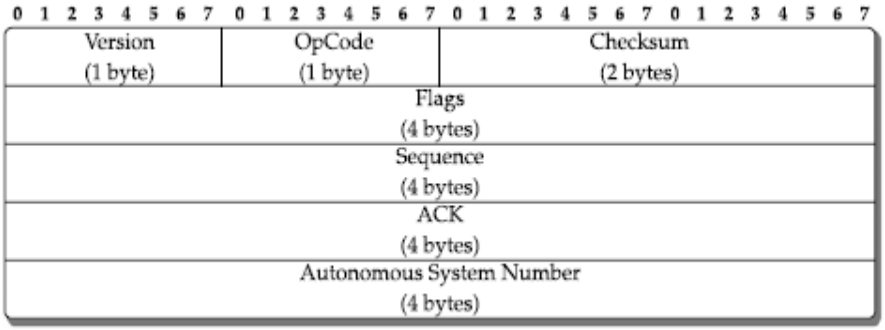
EIGRP es otro protocolo de enrutamiento de Cisco; es, sin embargo, más que una simple mejora de IGRP. Lo único en común entre IGRP y EIGRP es la métrica compuesta. Aunque EIGRP también es de la familia del protocolo de vector distancia, en muchos sentidos; es completamente diferente de los protocolos RIP e IGRP. Una diferencia importante es que EIGRP proporciona enrutamiento *loop-free*, lo que se logra a través de la difusión del cálculo, lo que también demuestra que no todos los protocolos de vector distancia utilizan un sencillo Bellman-Ford para el cálculo del camino de enrutamiento más corto. Hay una coordinación activa de fase antes del cálculo de enrutamiento cuando falla un enlace o el costo de este mismo cambia; para ello, solicita información adicional para que el algoritmo de actualización de difusión (DUAL) mantenga los estados. DUAL le permite a EIGRP lograr una convergencia más rápida. Además, EIGRP incluye el protocolo Hello para el descubrimiento y recuperación de vecinos, y un mecanismo de transferencia fiable para el intercambio de datos de vector distancia.

3.5.1 Formato del paquete[14]

El paquete EIGRP está dividido en dos partes: una parte la cabecera EIGRP, 20 bytes de longitud, seguido por varias entidades que están codificadas usando una variable longitud TLV (Type-Length-Value).

[13] Ibíd., p. 157
[14] Ibíd., p. 158

Figura 6. Formato del paquete EIGRP



Fuente: NETWORK ROUTING Algorithms, Protocols, and Architectures.

En la cabecera EIGRP, existen siete campos (ver figura 6), y se describen a continuación:

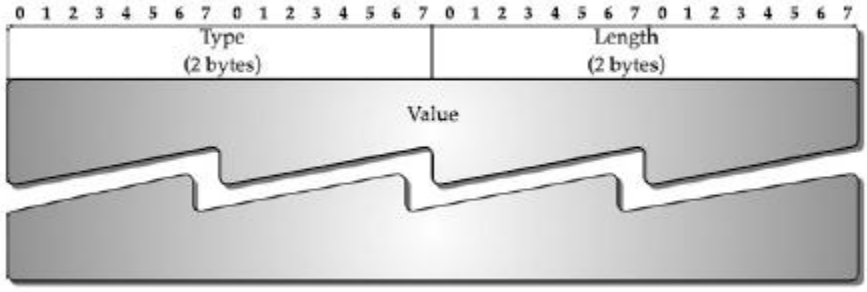
- **Version (1 byte):** Este campo se establece en 1.
- **OpCode (1 byte):** Este campo se utiliza para especificar el tipo de paquete EIGRP. Hay 4 tipos claves para redes IP: update, query, reply, y hello.
- **Checksum (2 bytes):** Checksum se calcula sobre todo el paquete EIGRP.
- **Flags:** Si este valor es 1, indica una nueva relación de vecindad. Este valor se establece en 2 para indicar el recibimiento de un bit condicional.
- **Sequence:** Este es un número de secuencia de 32–bit utilizado por el mecanismo de entrega fiable.
- **ACK:** Este campo enumera la secuencia de números desde el último aviso de un vecino. Para un paquete inicial Hello, este campo se ajusta en cero. Un tipo de paquete hello con un valor ACK diferente de cero es reconocido para un mensaje inicial hello.

- **Autonomous system number:** Este identifica el dominio EIGRP.

3.5.2 Formato TLV (TYPE LENGTH VALUE)[15]

Más allá de la cabecera, las distintas entidades están separadas utilizando el formato TLV en un paquete EIGRP (ver Figura 7). Cada entidad TLV es de longitud variable donde campo type se ajusta en 1 byte, el campo length se fija en 1 byte, mientras que el valor del campo es de longitud variable; la longitud del valor del campo se indica a través del campo length.

Figura 7. Codificación de datos en paquetes. Formato genérico TLV



Fuente: NETWORK ROUTING Algorithms, Protocols, and Architectures.

Ciertamente, a través del campo type, el paquete se identifica; este campo no se puede confundir con el OpCode en el campo de cabecera utilizado para el tipo de mensaje.

[15] Ibíd., p. 159

3.6. OPEN SHORTEST PATH FIRST (OSPF)[16]

El protocolo del primer camino más corto disponible es un protocolo de ennrutamiento de estado de enlace que inicialmente fue desarrollado en 1987 por Internet Engineering Task Force (IETF) grupo de trabajo de OSPF. En el RFC 1131, la especificación de OSPFv1 fue publicada en 1989. La segunda versión de OSPF fue desarrollada en 1998 y publicada en el RFC 2328. La tercera versión de OSPF fue publicada en 1999 y destinadas principalmente para la compatibilidad con IPv6.

Como ya se mencionó, OSPF es un ejemplo de un protocolo de estado de enlace basado en la comunicación hop- by–hop del enrutamiento de la información, específicamente designado para el enrutamiento de dominio interno de una red IP. Un protocolo de enrutamiento requiere información sobre el estado (costo) de enlace, y la habilidad de anunciar la fiabilidad de este estado de enlace a través de la comunicación en la red. Además un protocolo de estado de enlace utiliza dos sub-protocolos, uno para establecer una relación de vecinos a través del protocolo hello, y otro para la sincronización de bases de datos.

Consideremos los siguientes ejemplos/escenarios:

- La inundación del anuncio del estado de enlace (LSA) no siempre es necesaria ya que una red puede tener diversos tipos de medios de transmisión. Por ejemplo, si hay N routers en una red, por decir, en la misma área local (LAN), se crea innecesariamente N (N -1) enlaces mientras que la definición de un solo

[16] Ibíd., p. 167

enlace es suficiente, además, también resulta innecesario el cálculo de la ruta más corta en cada router sin ningún tipo de ganancia.

- Una red de dominio interno podría consistir en un gran número de routers, posiblemente expandidos geográficamente; por eso, la escalabilidad es una característica muy importante, es predecible tener la habilidad para dividir la red entera en varios sub-dominios y obtener una jerarquía. Esto, al contrario, plantea la posibilidad de que un LSA desde un subdominio a otro no necesite ser distribuido, especialmente si dos subdominios están conectados por un enlace.

3.6.1 Jerarquía de la red[17]

OSPF proporciona la funcionalidad de dividir una red intradomain (un sistema autónomo) en subdominios, comúnmente conocido como áreas. Cada red intradomain debe tener un área central, referida como área troncal; lo que se identifica con el Área ID 0. Las áreas se identifican a través de un campo de área de 32 bits; por lo que Area ID 0 es lo mismo que 0.0.0.0.

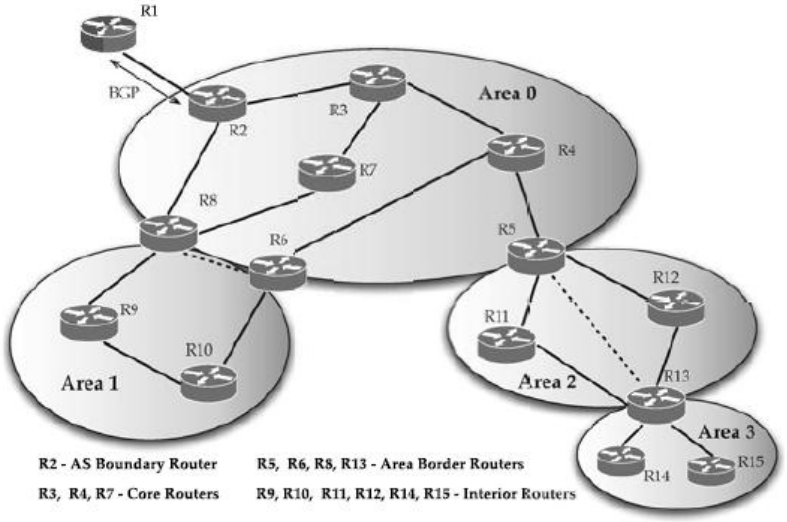
Por lo general, las áreas (aparte del área troncal) se numeran secuencialmente como Área 1 (es decir, 0.0.0.1), Área 2, y así sucesivamente. OSPF permite una configuración jerárquica con el área troncal como el nivel superior, mientras que todas las otras áreas, conectadas con el área troncal, se conocen como áreas de bajo nivel, lo que también significa que el área de red troncal es la encargada de resumir la topología de un área a otra área, y viceversa. En la figura 8, se ilustra la jerarquía de la red utilizando las áreas de bajo nivel.

[17] Ibíd., p. 168

3.6.2 Clasificación de los routers[18]

Con la funcionalidad proporcionada para dividir una red OSPF en áreas, los routers son clasificados en cuatro tipos diferentes:

Figura 8. Área troncal OSPF y áreas de bajo nivel



Fuente: NETWORK ROUTING Algorithms, Protocols, and Architectures.

- **Routers de borde de área:** Son routers que se sitúan entre el borde del área trocal y las áreas de bajo nivel. Cada router de borde de área debe tener al menos una interfaz al área troncal; también debe tener al menos una interfaz para cada área a la cual está conectada.

[18] Ibíd., p. 168

- **Routers internos:** Son routers ubicados en cada área de bajo nivel que sólo tienen interfaces para los routers internos en la misma área.
- **Routers del área troncal:** Son routers localizados en el Área 0 con al menos una interfaz que une a otro router en el área troncal.

- **Routers frontera AS:** Estos routers están localizados en el Área 0 con conectividad a otros AS; deben ser capaces de manejar más de un protocolo de enrutamiento. Por ejemplo, intercambiar información con otros AS, deben ser capaces de comunicar BGP. Estos routers también tienen interfaces internas para conectividad a otros routers del área troncal.

3.6.3 Tipos de redes[19]

OSPF está designado para direccionar 5 diferentes tipos de redes: (1) redes punto a punto, (2) redes de radiodifusión, (3) redes multiacceso sin radiodifusión (NBMA), (4) redes punto a multipunto, y (5) enlaces virtuales.

Las *redes punto a punto* hacen referencia a conectar un par de routers directamente por una interface/enlace como es el OC-3. Un router puede ser conectado a múltiples diferentes routers a través de interfaces punto a punto. Los enlaces punto a punto se utilizan típicamente cuando un dominio OSPF es expandido en una región distribuida geográficamente.

Las *redes de radio difusión* hacen referencia a las redes tales como las LANs, conectadas con una tecnología como Ethernet. Las redes de radiodifusión, por naturaleza, son multiaccesos donde todos los routers en una red de radiodifusión

[19] Ibíd., p. 169

pueden recibir un sólo paquete transmitido. En estas redes, un router es elegido como Designated Router (DR) y otro como Backup Designated Router (BDR).
Las redes *multi acceso sin-radiodifusión* utilizan tecnologías tales como ATM o frame relay donde más de dos routers pueden ser conectados sin capacidad de radio difusión. Así, un paquete OSPF es requerido para ser explícitamente transmitido a cada router de la red. Tales redes requieren una configuración extra para emular la operación de OSPF sobre una red de radio difusión. Como las redes de radio difusión, las redes NBMA elijen un DR y un BDR.

Las *redes multi punto a punto* son también redes sin radio difusión como las redes NBMA, sin embargo, el modo de operación de OSPF es diferente y de hecho similar a los enlaces punto a punto.

Los *enlaces virtuales* son utilizados para conectar un área con el área troncal utilizando un tránsito sin área troncal. Los enlaces virtuales se configuran entre dos routers de borde de área. Los enlaces virtuales pueden ser utilizados también si el área troncal está dividida en dos partes en caso de que un enlace falle; en tal caso, los enlaces virtuales son tuneliados a través del área (sin área troncal).

3.6.4 Sub-Protocolos[20]

Los mecanismos de sub-protocolos son también utilizados para el funcionamiento de un protocolo de estado de enlace además de la función de LSA a través de inundación. Dos sub-protocolos claves son el protocolo hello y el protocolo database synchronization protocol.

[20] Ibíd., p. 171

3.6.4.1 Protocolo hello[21]

El protocolo hello no sólo se utiliza para la inicialización, es mucho más que eso; recordando que el protocolo OSPF esta designado para diferentes tipos de redes. Primero, durante la inicialización/activación, el protocolo hello se utiliza para la búsqueda de vecinos así como muchos parámetros antes de establecer dos routers vecinos; esto significa que usar el protocolo hello, las adyacencias lógicas son establecidas; esto se hace para punto a punto, punto a multipunto, y redes de enlaces virtuales.

Para radio difusión y redes NBMA, no todos los routers se convierten en adyacencias lógicas; aquí, el protocolo hello se utiliza para elegir DRs y BDRs. Después de la inicialización, para todos los tipos de redes, el protocolo hello se utiliza para mantener viva la conectividad, que garantiza la comunicación bidireccional entre vecinos; esto significa, que si el mensaje hello de permanencia de conectividad no es recibido durante un intervalo de tiempo que se estableció durante la inicialización, el enlace/conectividad entre los routers se supone que no está disponible.

3.6.4.1 Database synchronization process[22]

Más allá de la inicialización básica para establecer vecinos, dos routers adyacentes necesitan construir adyacencia. Esto es más importante, que el fallo

[21] Ibíd., p. 171
[22] Ibíd., p. 172

de un enlace entre dos routers vecinos y que luego sea recuperado. Pues la base de datos del estado de enlace mantenida por estos dos routers puede convertirse fuera de sincronización durante el tiempo de fallo del enlace, es necesario sincronizarlos de nuevo. Mientras un completo LSA de todos los enlaces en la base de datos de cada router pueda ser intercambiado, un proceso de descripción especial de la base de datos se utiliza para optimizar este paso. Por ejemplo, durante la de descripción de la base de datos, sólo las cabeceras del LSA son intercambiadas; las cabeceras sirven como una información adecuada para comprobar si un lado tiene el último LSA. Ya que un proceso de sincronización puede requerir intercambio de información de la cabecera sobre muchos LSAs, el proceso de sincronización de la base de datos permite para tales intercambios dividir en múltiples pedazos. Estos pedazos son comunicados mediante la descripción de la base de datos de los paquetes indicando si es un pedazo de un paquete inicial (utilizando I-bit) o una continuación/más paquetes o el último paquete (con M-bit). Además, un lado necesita servir como maestro (MS-bit) mientras que el otro lado sirve como esclavo, esta negociación es permitida; típicamente, el router vecino con el ID más bajo será el esclavo.

3.6.5 Formato del paquete[23]

Cabecera común

La cabecera común posee los siguientes campos (ver figura 9):

- **Version:** Este campo representa el número de la versión de OSPF; la correspondiente versión es 2.

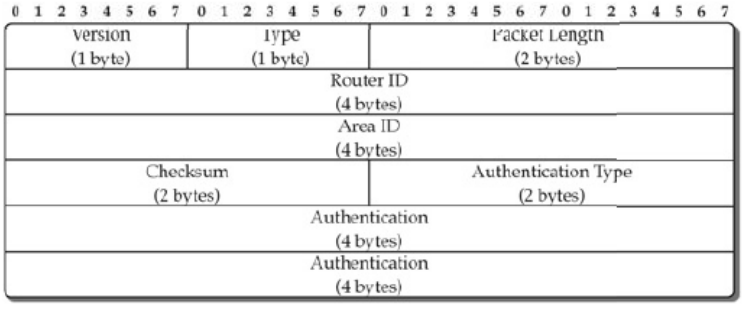
[23] Ibíd., p. 177

- **Type:** Este campo especifica el tipo del paquete. OSPF tiene 5 tipos de paquetes: hello (1), database description (2), link state request (3), link state update (4), y LSA (5).
- **Packet length:** Este indica la longitud del paquete OSPF

- **Router ID:** Este campo indica el ID del router origen. Ya que un router tiene múltiples interfaces, no hay un modo definitivo para determinar cual interface de dirección IP debería ser el ID del router. De acuerdo al RFC 2328, podría ser también la dirección IP más larga o más corta que pertenece a todas las interfaces. Cabe señalar que si un router es creado sin una interface de conexión, no tiene la habilidad para adquirir el ID del router. Para evitar este escenario, una interfaz de loopback, siendo una interface virtual, puede usarse para adquirir el ID de un router. En general, el ID de un router que es basado sobre una interface de loopback proporciona mucha más flexibilidad a las funciones de la red en términos de administración que una interface física basada en el direccionamiento.

- **Área ID:** Este es el ID del área donde el paquete OSPF es originado. El valor 0.0.0.0 está reservado para el área backbone (área troncal).

Figura 9. Cabecera común del paquete OSPF



Fuente: NETWORK ROUTING Algorithms, Protocols, and Architectures.

- **Checksum:** Este es el checksum IP sobre todo el paquete OSPF.

- **AuType and Authentication Field:** AuType trabaja con el campo de (Authentication field) para la autenticación. Existen tres tipos de autenticación: El valor 0 (sin autenticación), 1 (password de texto claro) y 2 (autenticación criptográfica MD5 de checksum).

3.6.6 Hello packet[24]

El propósito general del paquete hello (figura 10) es establecer y mantener adyacencias. Esto significa que mantiene un enlace con un vecino que es funcional. El paquete hello se utiliza también en el proceso de elección de DR y BDR en redes de radio difusión. El paquete hello también se utiliza para la negociación de capacidades opcionales.

- **Network Mask:** Esta es la dirección de la máscara de una interface del router desde el cual el paquete es enviado.

- **Hello Interval:** Este campo designa la diferencia de tiempo en segundos entre cualquiera de dos paquetes hello. Los routers transmisores y receptores son requeridos para mantener el mismo valor; si no, la relación de vecindad entre esos dos routers no se establece. Para redes punto a punto y redes radio

[24] Ibíd., p. 178

difusión, el valor por defecto es 10 segundos, mientras para una red sin radio difusión el valor por defecto es 30 segundos.

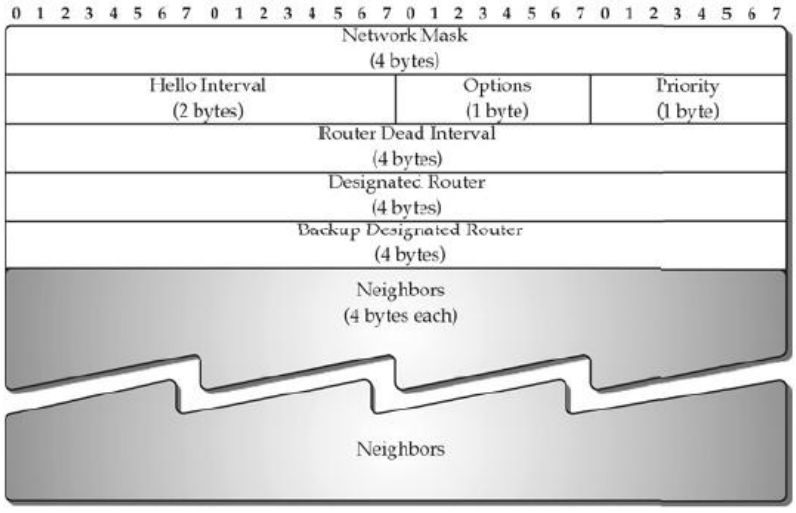
- **Options:** El campo options permite compatibilidad con un router vecino para ser revisado.

- **Priority:** Este campo se utiliza cuando se elige el router designado y el router de apoyo.

- **Router Dead Interval:** Esta es la longitud de tiempo en el cual un router declara a un vecino para ser eliminado si no recibe un paquete hello.

- **Designated Router (DR) (Backup Designated Router (BDR)**: El campo DR (BDR) enumera las direcciones IP de la interface del DR (BDR) sobre la red, pero no la identificación del router. Si el campo DR(BDR) es 0.0.0.0, esto significa que no hay DR (BDR).

Figura 10. Paquete hello OSPF



Fuente: NETWORK ROUTING Algorithms, Protocols, and Architectures.

3.6.7 Database description packet

El paquete de descripción de la base de datos OSPF tiene las siguientes características (figura 11).

- **Interface Maximun Transmission Unit (MTU):** Este campo indica el tamaño de la unidad de transmisión que la interface puede manejar sin fragmentación.

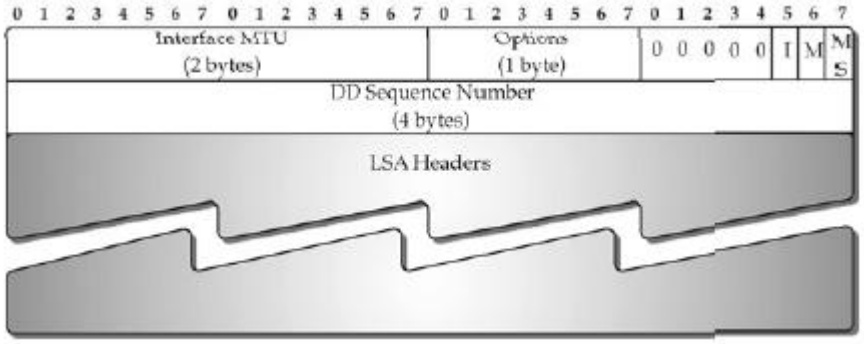
- **Options:** Los campos de opciones consisten de muchos bits de campos de nivel. El más crítico es el E-bit, el cual se establece cuando el área próxima es capaz de procesar AS – externos LSA.

- **I/M/MS bits:** I-bit (initial-bit) se inicializa en uno para un paquete inicial que empieza una sesión de la descripción de la base de datos; para otros paquetes en la misma sesión, este campo se establece en 0. M-bit (more bit) se utiliza para indicar que este paquete no es el último para la sesión de descripción de la base de datos. MS-bit (bit maestro-esclavo) se utiliza para indicar que el originador es el maestro y se estable este campo en 1, mientras el esclavo se establece en 0.

- **DD Sequence number:** Este campo se utiliza para incrementar el número de secuencias de los paquetes desde el lado del maestro durante la sesión de descripción de la base de datos; el maestro establece el valor inicial para el número de secuencia.

- **LSA Header:** Este campo enumera las cabeceras de los LSAs en el originador de la base de datos de estado de enlace; podría enumerar algunos o todos.

Figura 11. Paquete de descripción de la base de datos



Fuente: NETWORK ROUTING Algorithms, Protocols, and Architectures.

3.6.8 Soporte de múltiples métricas[25]

La tecnología actual hace que sea posible soportar varias métricas en paralelo. Evaluando el camino entre dos nodos en base a diferentes métricas es tener distintos mejores caminos según la métrica utilizada en cada caso, pero surge la duda de cuál es el mejor. Esta elección se realizara en base a los requisitos que existan en la comunicación.

[25] QUINTERO, Edison y ALVARO, Luis. ESTADO DEL ARTE EN LA APLICACIÓN DE INGENIERIA DE TRAFICO EN REDES IP. pdf. Universidad Pontificia Bolivariana.2010. p. 19

Diferentes métricas utilizadas pueden ser: Mayor rendimiento, Menor retardo, Menor costo, Mayor fiabilidad.

La posibilidad de utilizar varias métricas para el cálculo de una ruta, implica que OSPF provea de un mecanismo para que una vez elegida una métrica en un paquete para realizar su routing esta sea la misma siempre para ese paquete, esta característica dota a OSPF de un routing de servicio de tipo en base a la métrica.

3.6.9 Balanceado de carga en múltiples caminos[26]

Una característica importante del computo del enrutamiento para ambos protocolos (OSPF e IS-IS) es la opción de múltiples caminos de igual costo; de esta manera, si las rutas tienen el mismo camino de más bajo costo, el enlace de salida (siguiente hop) para ambos puede ser llamado en la tabla de enrutamiento y así la demanda de tráfico pueda ser divido, garantizando el balanceo de carga a través de múltiples rutas.

3.7. IS-IS (INTERMEDIATE SYSTEM TO INTERMEDIATE SYSTEM)[27]

Es un protocolo de encaminamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el estado de enlace para encontrar el camino más

[26] Ibíd., p. 34

[27] MEDHI, Deepankar y RAMASAMY, Karthikeyan. NETWORK ROUTING Algorithms, Protocols, and Architectures. Oxford, Elsevier: 2007. p. 185-186

corto mediante el algoritmo SPF (Shortest Path First). El protocolo está definido en el RFC 1142.

Este protocolo también se puede usar bajo la arquitectura TCP/IP. De tal manera que es capaz de encaminar paquetes IP y CLNP (ConnectionLess Network Protocol). No emplea encapsulación para los paquetes, ni ninguna diferencia relevante entre ellos, excepto que en IP añade información adicional.

El protocolo IS-IS tiene su propia terminología que la diferencia de OSPF. Por ejemplo, los routers son referidos como *intermediate systems* (sistemas intermedios)*;* por eso, el nombre de intermédiate systems - to - intermédiate systems. Los LSAs son llamados link state protocol data units, or LSPs, en resumen. Una red de radio difusión se conoce como *pseudonode*; un sistema intermedio designado se elige desde todos los ISs para representar una red de radio difusión. Una dirección para identificar un sistema intermedio es llamado *network service access point (NSAP)*. IS-IS se ejecuta directamente sobre la capa 2 de protocolos, a diferencia de OSPF que se ejecuta sobre IP. Similar a OSPF, IS-IS también ha sido extendido para proporcionar capacidades de ingeniería de tráfico.

3.7.1 Estructura del protocolo IS-IS[28]

En la figura 14 se puede apreciar la estructura del protocolo IS-IS

[28] SHEWANDAGN, Esuendale y ATHAR, Syed. Performance Comparison of EIGRP/ IS-IS and OSPF/ IS-IS. pdf. Blekinge Institute of Technology. 2009.p.50

- **Intradomain routing protocol discriminator:** Este campo indica el identificador del protocolo de la capa de red dado para el protocolo IS-IS.
- **Length indicator:** Describe la longitud de la cabecera fija en octetos.
- **Version/ protcol ID extensión:** Se establece en 1.
- **ID length:** Define la longitud del campo y el identificador NET que se utiliza en el dominio del enrutamiento.
- **R:** Es un bit de reserva.
- **PDU:** Describe el tipo de PDU, los bits 6,7 y 8 se reservan.
- **Version:** Se establece en 1.
- **Maximun area addresses:** Este campo indica el número de áreas de direcciones permitidas.

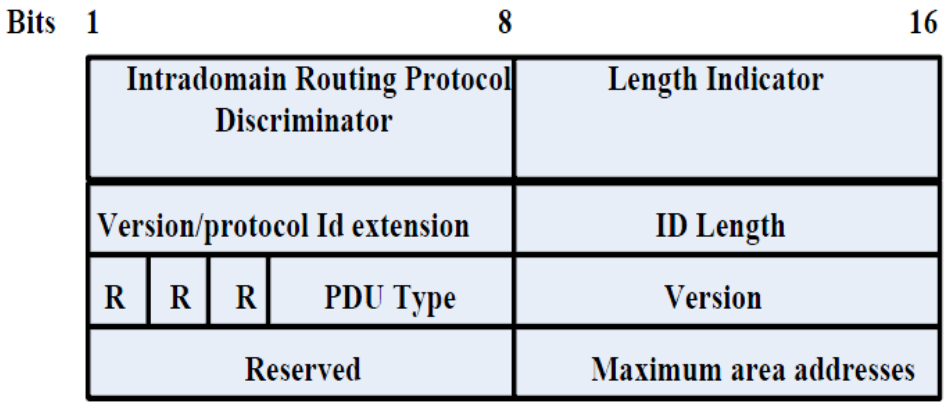
IS-IS tiene dos tipos de direcciones

- ***Network Service Access Point (NSAP):*** Las direcciones NSAP descubren los servicios de la capa de red.

- ***Network Entity Title (NET)*****:** Las direcciones NET descubren las entidades de la capa de red o procesos más que servicios.

Existe una posibilidad de que un dispositivo tenga más de un tipo de dirección, pero NET´s y el system ID del NSAP debe ser único para cada sistema.

Figura 12. Estructura del protocolo IS-IS



Fuente: NETWORK ROUTING Algorithms, Protocols, and Architectures.

3.7.2 Tipos de paquetes IS-IS[29]

Por lo general los tipos de paquetes son definidos para Level 1 o Level 2.

1. Intermediate System – Intermediate System HELLO

- Se utiliza para detectar vecinos y mantener adyacencia.
- Diferencia sobre enlaces punto a punto y LANs.

2. Link state packet (LSP):

- Consiste de pseudo node de nivel 1, sin pseudo node de nivel 1, pseudo node de nivel 2 y sin pseudo node de nivel 2.
- Un LSP por router y fragmento.
- Un LSP por una red LAN

3. Complete sequence number PDU (CSNP)

- Consiste de una lista de LSPs de la base de datos.
- Se utiliza para informar a otras rutas de LSPs, que podrían ser olvidadas. Esto es importante para los routers para tener la misma información.

4. Partial sequence number PDU (PSNP)

- Se utiliza para solicitar un LSP

[29] Ibíd., p. 51

- También se utiliza para reconocer la recepción de LSPs (o un LSP).

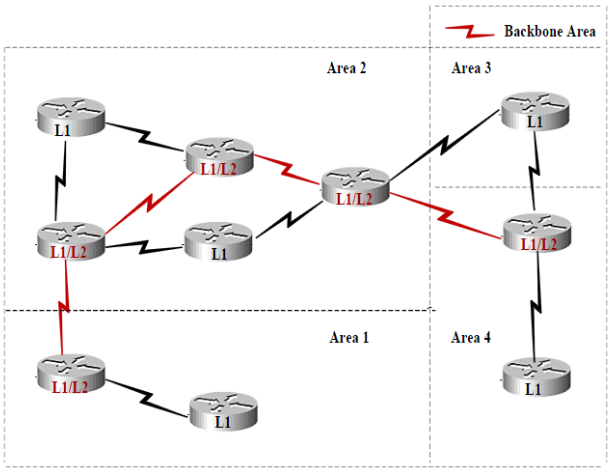
3.7.3 Dominios de enrutamiento y áreas IS-IS[30]

Un dominio de enrutamiento es una colección de áreas que implementan políticas de enrutamiento dentro de un dominio de un AS.

3.7.3.1 Área backbone[31]

IS-IS no incluye un área Backbone como lo hace OSPF Área 0. Una colección contigua de routers IS-IS de nivel 2 forman el área backbone donde cada uno de ellos puede estar en diferentes áreas. En la figura 13 se muestra el área backbone en color rojo lo cual los routers L1/L2 están posicionados en diferentes áreas.

Figura 13. Área Backbone



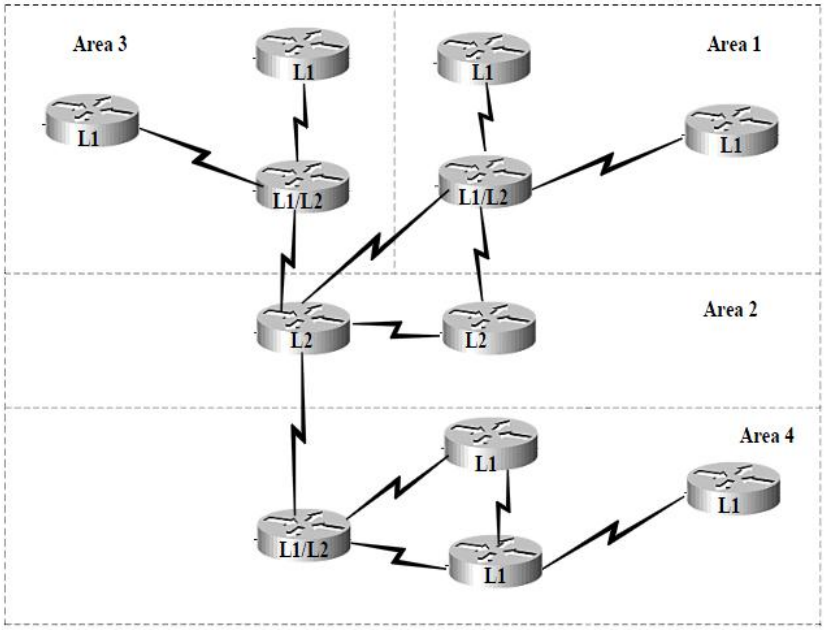
[30] Ibíd., p. 52
[31] Ibíd., p. 52

Fuente: NETWORK ROUTING Algorithms, Protocols, and Architectures.

3.7.3.2 Áreas[32]

En IS-IS, cada router es posicionado solo en un área en el cual el borde entre áreas esta sobre un enlace conectando los routers en diferente área. Esto lo hace diferente de OSPF. Un router habilitado con IS-IS tiene una dirección NSAP. En la figura 14 se puede apreciar la distribución de áreas.

Figura 14. Área Backbone



[32]Ibíd., p. 53

Fuente: NETWORK ROUTING Algorithms, Protocols, and Architectures.

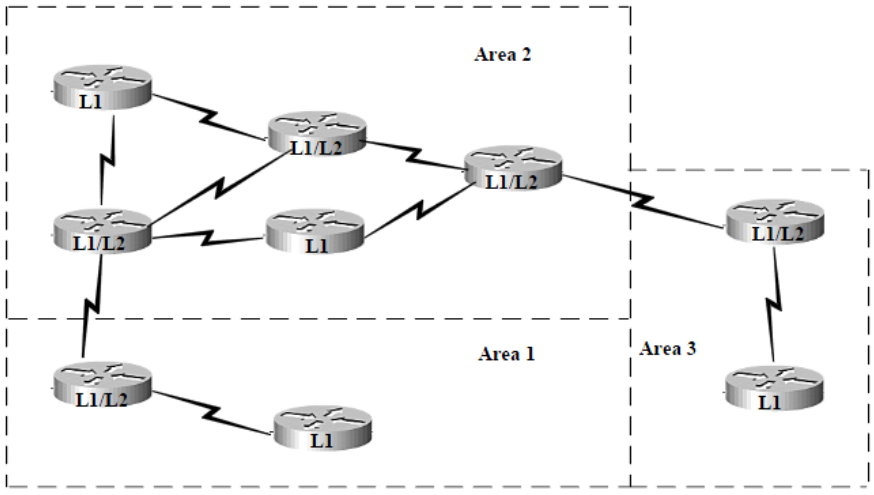
3.7.3.3 Tipos de routers IS-IS[33]

Existen tres tipos de routers en las redes IS-IS. En la figura 17 se muestra la topología de una red IS-IS.

- Level 1 (L1)
- Level 2 (L2)
- Both (L1/L2)

Router Nivel 1:

Figura 15. Topología de una red IS-IS



[33] Ibíd., p. 5

Fuente: NETWORK ROUTING Algorithms, Protocols, and Architectures.

Un router de configuración L1 sólo identifica los routers de su propia área y tiene vecinos de configuración L1 o L1/L2 en su área. Este incluye una base de datos del estado de enlace L1 con toda la información de enrutamiento del área interna. Para enviar paquetes fuera de su área, el router L1 utiliza el router L2 más cercano disponible en su área.

Router Nivel 2: Los routers de configuración L2 pueden incluir vecinos en la misma o diferente área y consiste de una base de datos del estado de enlace L2 con información para enrutamiento de área interna. Un router L2 sólo puede identificar otras áreas pero no tiene información de L1.

Router Nivel L1/L2: Un router de configuración L1/L2 puede incluir vecinos en cualquier área y consta de las siguientes dos bases de datos de estado de enlace.

- Una base de datos de estado de enlace L1 para entutamiento área interna.
- Una base de datos de estado de enlace L2 para entutamiento área externa

Un router L1/L2 ejecuta dos SPFs lo cual requiere más memoria y procesamiento.

3.7.4 Métrica de IS-IS[34]

[34] Ibíd., p. 55

Originalmente IS-IS define 4 tipos de métricas, llamada costo, retardo y error. El costo es usualmente una métrica arbitraria. Por defecto la métrica debería ser soportada sobre todos los routers. Las métricas opcionales son intencionadas para proporcionar enrutamiento QoS.

- Cost: El costo es la métrica por defecto. Esta métrica indica la velocidad delenlace. Un valor bajo del costo de un enlace indica más ancho de banda o un enlace de alta velocidad.
- Delay: Mide la transmisión del retardo de el enlace.
- Expense: Medida monetaria de la utilización del costo del enlace.
- Error: Mide la probabilidad del error residual encontrado en el enlace.

3.7.5 Funcionamiento general[35]

- En IS-IS, los routers envían paquetes HELLO a todas las interfaces habilitadas con IS-IS para identificar vecinos y crear adyacencias.
- Los routers podrían establecer un paquete de estado de enlace dependiendo de las interfaces locales configuradas con IS-IS y prefijadas desde otros routers adyacentes.
- Los routers inundan paquetes de estado de enlace a cada vecino adyacente excluyendo el vecino de donde se obtiene el paquete del estado de enlace. Hay diferentes tipos de inundación y dependiendo de los escenarios, la operación de inundación difiere.
- Cada router construye su base de datos de estado de enlace desde los paquetes de estado de enlace.

[35] Ibíd., p. 55

- Cada IS calculara el camino más corto; la tabla de enrutamiento será construida.

3.7.6 Diferencias y similitudes de ISIS y OSPF[36]

- Ambos protocolos proporcionan jerarquía en la red a través de dos niveles de área.
- Ambos protocolos utilizan el paquete Hello para inicializar de forma adyacente y luego continuar manteniéndolo.
- Ambos protocolos tienen la capacidad para resumir las direcciones entre áreas.
- Ambos protocolos mantienen una base de datos de estado del enlace, y el cálculo del camino más corto a cabo utilizando el algoritmo de Dijkstra.
- Ambos protocolos tienen la disposición para elegir un router designado para representar una red de difusión.

Entre las diferencias se encuentran:

- IS-IS se ejecuta directamente sobre la capa 2, es relativamente más seguro que OSPF.
- Mientras que los paquetes OSPF son encapsulados en datagramas IP, los paquetes en IS-IS son encapsulados directamente en el marco de la capa de enlace.
- Con OSPF, un router de borde de área puede situarse en la frontera entre el área de red troncal y un área de bajo nivel con algunas interfaces en el área, mientras que otras interfaces están en otra área. En IS-IS, los routers están totalmente dentro de una o la otra área, las fronteras de área están sobre los enlaces, no sobre los routers.

[36] MEDHI, Deepankar y RAMASAMY, Karthikeyan. NETWORK ROUTING Algorithms, Protocols, and Architectures. Oxford, Elsevier: 2007. p. 189

3.8 BORDER GATEWAY PROTOCOL (BGP)[37]

El protocolo BGP se utiliza para comunicar información sobre las redes que actualmente residen (o alojados) en un sistema autónomo a otros sistemas autónomos. El intercambio de información de la red se realiza mediante la creación de una sesión de comunicación entre sistemas autónomos de frontera. Para la entrega fiable de información, se establece una sesión de comunicación basado en el protocolo TCP entre sistemas autónomos de frontera utilizando el número de puerto TCP 179. Esta sesión de comunicación es requerida para estar conectado, y es utilizado por ambas partes para intercambiar y actualizar periódicamente la información. Cuando por alguna razón se rompe la conexión TCP, cada parte está obligada a dejar de utilizar la información que ha obtenido desde el otro lado. En otras palabras, la sesión TCP sirve como un enlace virtual entre los dos sistemas autónomos vecinos, y la falta de comunicación significa que este vínculo virtual esta caído. Ciertamente, este enlace virtual será más que un enlace físico que conecta los routers frontera entre dos sistemas autónomos; es importante señalar que si se rompe un enlace virtual, no significa necesariamente que la conexión física se ha roto.

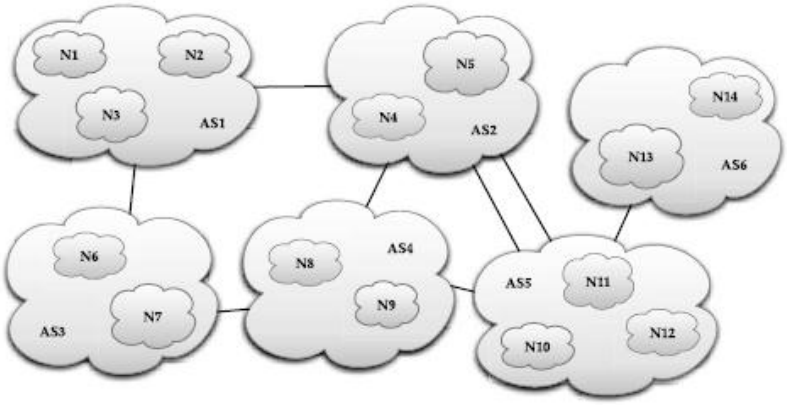
Ahora, considere que cada sistema autónomo es un *supernodo virtual*; incluso la totalidad de la Internet puede ser pensado como una conexión virtual de supernodos virtuales a través de enlaces virtuales.

3.8.1 Topología BGP[38]

[37] Ibíd., p. 239

En la Figura 16 se puede apreciar seis supernodos virtuales (sistemas autónomos) AS1 a AS6, conectados por enlaces virtuales, utilizando el protocolo TCP basado en sesiones BGP para la comunicación entre dos supernodos virtuales adyacentes. Cada supernodo virtual contiene una o más redes identificadas como N1, N2, N3 en AS1, y así sucesivamente. De la figura, podemos ver que hay más de un camino posible entre sistemas autónomos determinados. También es posible tener un supernodo en el borde de toda la red, tales como AS6. Además está permitido que existan múltiples enlaces virtuales entres dos sistemas autónomos vecinos, así como se puede apreciar entre AS2 y AS5, existen dos enlaces virtuales.

Figura 16. Internet: una visión de la concepción gráfica a través de nubes de sistemas autónomos (super nodos virtuales) conectados a través de sesiones BGP (enlaces virtuales)



Fuente: NETWORK ROUTING Algorithms, Protocols, and Architectures.

[38] Ibíd., p. 239

3.8.2 Funciones de BGP[39]

BGP se diseñó para permitir la cooperación en el intercambio de información de encaminamiento entre dispositivos de encaminamiento, llamados pasarelas, en sistemas autónomos diferentes. El protocolo opera en términos de mensajes, que se envían utilizando el protocolo TCP. El repertorio de mensajes es el siguiente:

1. OPEN
2. UPDATE
3. KEEPALIVE
4. NOTIFICACION

BGP supone tres procedimientos funcionales: Adquisición de vecino, detección de vecino alcanzable y detección de red alcanzable.

Dos dispositivos de encaminamiento se consideran que son vecinos si están en la misma subred. Si los dos dispositivos de encaminamiento están en sistemas autónomos, podrían desear intercambiar información de encaminamiento. Para este cometido es necesario realizar primero el proceso de adquisición de vecino. Se requiere un mecanismo formal de encaminamiento ya que alguno de los dos vecinos podría no querer participar. Existirán situaciones en las que un vecino no desee intercambiar información esto se puede deber a múltiples factores como por ejemplo que este sobresaturado y entonces no quiere ser responsable del tráfico que llega desde fuera del sistema.

En el protocolo de adquisición de vecino, un dispositivo envía un mensaje de petición al otro, el cual puede aceptar o rechazar el ofrecimiento. El protocolo no

[39] Ibíd., p. 243

indica cómo puede saber un dispositivo la dirección o incluso la existencia de otro dispositivo de encaminamiento. Estas cuestiones se tratan en el momento de establecer la configuración del sistema o por una intervención activa del gestor de la red. Para llevar a cabo la adquisición de vecino, un dispositivo envía al otro un mensaje OPEN. Si el otro dispositivo acepta la relación, envía un mensaje de KEEPALIVE.

Una vez establecida la relación de vecino, se utiliza el procedimiento de detección e vecino alcanzable para mantener la relación. Este procedimiento consiste en enviarse entre los dos vecinos periódicamente mensajes de KEEPALIVE para asegurarse de que la relación sigue establecida. El último procedimiento especificado por BGP es la detección de red alcanzable. Cada dispositivo de encaminamiento mantiene una base de datos con las redes que puede alcanzar y la ruta preferida para llegar hasta esa red. Siempre que se realiza un cambio en esa base de datos, el dispositivo de almacenamiento envía un mensaje de UPDATE por difusión a todos los dispositivos de encaminamiento que implementan BGP.

3.8.3 Mensajes BGP

Los mensajes BGP tienen una cabecera común de 19 octetos que contiene los siguientes tres campos:

- **Marcador:** reservado para autentificación. El emisor puede insertar un valor en este campo para permitir al receptor comprobar la veracidad del emisor.
- **Longitud:** longitud del mensaje en octetos.
- **Tipo:** tipo de mensaje; OPEN, UPDATE, NOTIFICATION, KEEPALIVE.

3.8.3.1. Mensaje OPEN

Para adquirir un vecino, un dispositivo de encaminamiento abre primero una conexión TCP con el dispositivo vecino y después envía un mensaje OPEN. Este mensaje identifica al AS al que pertenece el emisor y suministra la dirección IP del dispositivo de encaminamiento.

En la figura 17 se muestra el formato del mensaje OPEN:

Figura 17. Formato del mensaje OPEN

Campo	Long (bytes)
Marcador	16
Longitud	2
Tipo	1
Versión	1
AS	2
Tiempo permanente.	2
Identificador BGP	4
Long. Opciones	1
Opciones	Variable

Fuente: NETWORK ROUTING Algorithms, Protocols, and Architectures.

Versión: indica la versión del protocolo del mensaje. La versión actual es 4.
AS: identifica al sistema autónomo del emisor del mensaje.
Tiempo de permanencia: indica el tiempo de que propone el emisor como Hold Time.
Identificador de BGP: identifica al BGP emisor.

3.8.3.2 Mensaje KEEPALIVE

El mensaje KEEPALIVE consta solo de la cabecera. Cada dispositivo de mantenimiento envía regularmente estos mensajes para evitar que expire el temporizador mantenimiento.

En la figura 18 se muestra el formato del mensaje KEEPALIVE:

Figura 18. Formato del mensaje KEEPALIVE

Campo	Long (bytes)
Marcador	16
Longitud	2
Tipo	1

Fuente: Protocolos de Routing Externo: BGP (Border Gateway Protocol). Disponible en:http://www.docstoc.com/docs/22801295/PROTOCOLOS-DE-ROUTING-EXTERNO-BGP-(BORDER-GATEWAY-PROTOCOL)

3.8.3.3 Mensaje UPDATE

El mensaje UPDATE facilita dos tipos de información:

- Información sobre una ruta particular a través del conjunto de redes. Esa información se puede incorporar a la base de datos de cada dispositivo de encaminamiento que la recibe.

- Una lista de rutas previamente anunciadas por este dispositivo de encaminamiento que van a ser eliminadas.

En la figura 19 se visualiza el formato del mensaje UPDATE:

Campo	Long (bytes)
Marcador	16
Longitud	2
Tipo	1
Longitud Rutas no factibles	2
Rutas retiradas	Variable
Longitud Total atributos de camino	2
Atributos de camino	Variable
Información. De accesibilidad de la capa de red	Variable

Figura 19. Formato del mensaje UPDATE

Fuente: Protocolos de Routing Externo: BGP (Border Gateway Protocol). Disponible en:http://www.docstoc.com/docs/22801295/PROTOCOLOS-DE-ROUTING-EXTERNO-BGP-(BORDER-GATEWAY-PROTOCOL)

Un mensaje UPDATE puede contener uno o ambos tipos de información. Consideremos primero el tipo de información 1. La información sobre una ruta particular a través de la red implica tres campos, campo de información sobre la capacidad de alcanzar la capa de red (NLRI), campo de longitud de los atributos del camino total, y el campo de los atributos de camino. El campo NLRI contiene una lista de identificadores de redes que se pueden alcanzar por esta ruta. Cada red se identifica por su dirección IP, que es en realidad una parte de la dirección IP completa.

El campo atributos de camino contiene una lista de atributos que se aplican a esta ruta particular. Los atributos definidos son los siguientes:

- Origen: indica si la información fue generada por un protocolo de dispositivo de encaminamiento interior o exterior.
- Camino AS: una lista de los AS que son atravesados por la ruta.
- Siguiente salto: dirección IP del dispositivo de encaminamiento frontera que se debe usar como siguiente salto para alcanzar los destinos indicados en el NLRI.
- Multi exit disc: se usa para comunicar alguna información sobre rutas internas a un AS.
- Local pref: usado por un dispositivo de encaminamiento para informar a otros dispositivos de encaminamiento dentro del mismo AS de su grado de preferencia por una ruta particular. No tiene significado alguno para dispositivos de encaminamiento en otros AS.
- Agregado atómico, Agente unión: estos dos campos implementan el concepto de unión de rutas. En esencia, un conjunto de redes y su espacio de direcciones correspondiente se pueden organizar jerárquicamente, o como un árbol. En este caso las direcciones de las redes se estructuran en dos o más partes. Todas las redes de un subárbol comparten una dirección Internet parcial común. Usando esta dirección parcial común, la cantidad de

información que se debe comunicar en NLRI se puede reducir significativamente.

El atributo Camino AS sirve realmente para dos objetivos. Ya que indica los AS que debe atravesar un datagrama si sigue esta ruta, la información de camino AS habilita a un dispositivo de encaminamiento a que implemente un criterio de encaminamiento. Esto es un dispositivo de encaminamiento puede construir un camino para pasar por un determinado AS.

3.8.3.4 Mensaje NOTIFICATION

Se envían cuando se detecta algún tipo de error. Se puede informar de los siguientes tipos de errores:

- Error en la cabecera del mensaje: incluye errores de sintaxis y autentificación.
- Error en mensaje OPEN: incluye errores de sintaxis y opciones no reconocidas en un mensaje OPEN. Este mensaje también se puede utilizar para indicar que el tiempo de mantenimiento en el mensaje OPEN es inaceptable.
- Error en el mensaje UPDATE: incluye errores de sintaxis y validación en un mensaje UPDATE.
- Tiempo de mantenimiento expirado: si el dispositivo de encaminamiento que envía no recibe mensajes sucesivos de KEEPALIVE y/o UPDATE y/o NOTIFICATION durante el tiempo de mantenimiento, entonces se comunica este error y se cierra la conexión.
- Error en la máquina de estados finitos: incluye cualquier error de procedimiento.

- Cese: utilizado por un dispositivo de encaminamiento para cerrar una conexión con otro dispositivo de encaminamiento en ausencia de cualquier otro error.

En la figura se muestra el formato del mensaje NOTIFICATION:

Figura 20. Formato del mensaje NOTIFICATION

Campo	Long (bytes)
Marcador	16
Longitud	2
Tipo	1
Código error	1
Sub-código error	1
Datos	Variable

Fuente: Protocolos de Routing Externo: BGP (Border Gateway Protocol). Disponible en:http://www.docstoc.com/docs/22801295/PROTOCOLOS-DE-ROUTING-EXTERNO-BGP-(BORDER-GATEWAY-PROTOCOL)

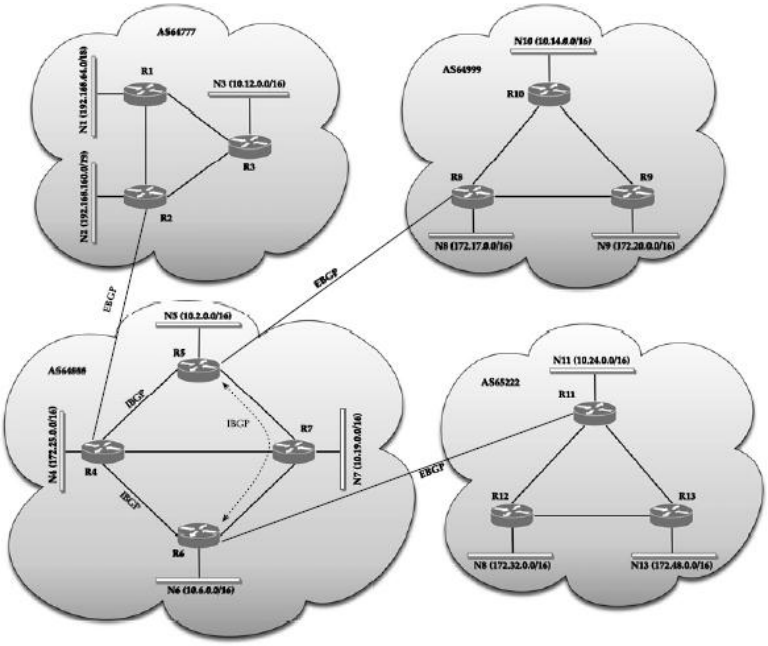
El sub-código de error nos da más información sobre el error, los posibles códigos son los siguientes:

Message Header Error subcodes, OPEN Message Error subcodes, UPDATE Message Error subcodes.

3.8.4 External BGP y Internal BGP

BGP se utiliza para establecer conexión de parejas de vecindad (neighbor) entre dos BGP speakers dentro de un AS, conocido como internal BGP (IBGP) speaker. Para saber cuando un BGP speaker se está comunicando con una pareja externa BGP speaker o una pareja interna BGP speaker, se puede determinar comparando el número del AS comunicado por su pareja BGP en el mensaje de apertura (OPEN) con el valor interno, así este vecino es un IBGP speaker, y si no lo es, será un EBGP speaker. En la figura 21 se puede apreciar las parejas IBGP y EBGP.

Figura 21. Peers IBGP y EBGP



Fuente: Protocolos de Routing Externo: BGP (Border Gateway Protocol). Disponible en:http://www.docstoc.com/docs/22801295/PROTOCOLOS-DE-ROUTING-EXTERNO-BGP-(BORDER-GATEWAY-PROTOCOL)

3.9. ¿QUÉ ES OPNET *MODELER*?

Es un lenguaje de simulación orientado a las comunicaciones. Proporciona acceso directo al código fuente siendo esto una gran ventaja para los nuevos programadores que se aventuren a programar con OPNET. Actualmente es utilizado por grandes empresas de telecomunicaciones, por ejemplo para desarrollar proyectos gubernamentales y del ejército, etc.

Para más detalle se dispone de su página oficial *http: //www.opnet.com*, donde se puede encontrar toda la información referente a cómo descargar el software necesario, qué es OPNET, etc.

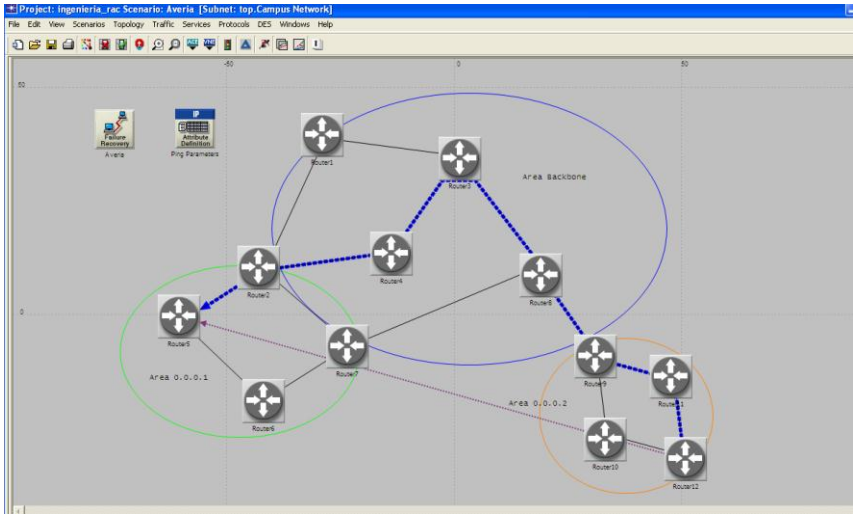
3.9.1 Project Editor

El *Project editor* es el principal escenario en la creación del entorno de la simulación de la red. Es usado para crear un modelo de red utilizando otros ya existentes que se pueden encontrar en la librería estándar, recolectar estadísticas sobre la red, comenzar la simulación y observar los resultados. También se pueden crear nodos, construir formatos de paquetes, etc. Este editor contiene tres tipos básicos de objetos: subredes, nodos y enlaces.

Las paletas, accesibles mediante un icono situado en la parte superior izquierda del editor (ver figura 22), ordenan los objetos disponibles en categorías. Por ejemplo, en la paleta *ethernet*, se encuentran los nodos y enlaces más utilizados para el diseño de este tipo de red.

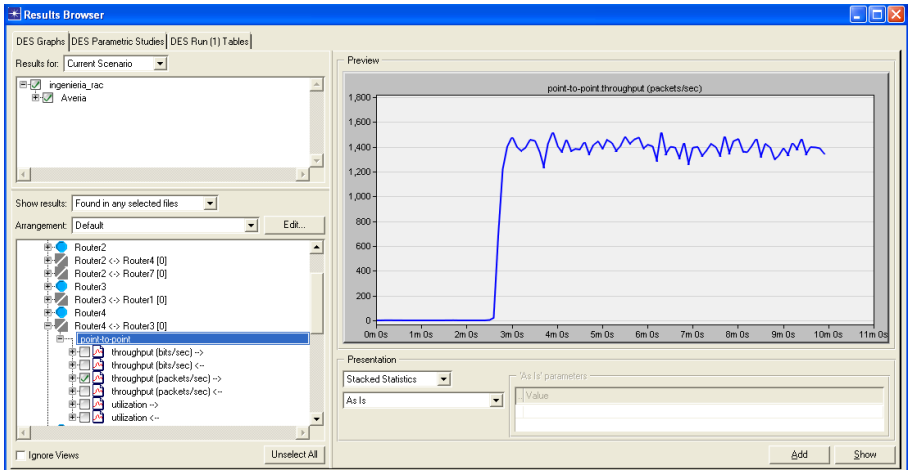
En este editor como se ha mencionado se pueden observar los resultados obtenidos. Al seleccionar la opción de ver resultados (*view results*), aparecen las estadísticas disponibles. Esta opción se logra visualizar como se observa en la figura 22, donde se plasma la visualización de un resultado de retardo. También se puede distinguir en la zona izquierda inferior de la figura una selección, ésta son los diferentes resultados que permite analizar el programa.

Figura 22. Formato Project Editor



Fuente: Imágenes de las pruebas de Simulaciones realizadas por el autor del proyecto

Figura 23. Visualización de resultados



Fuente: Imágenes de las pruebas de Simulaciones realizadas por el autor del proyecto

4. METODOLOGÍA DE LA TESIS

4.1 DESARROLLO DE LA TESIS

Se realizó un estudio acerca de los protocolos de enrutamiento en la red y la importancia que tienen al desarrollar ingeniería de tráfico. Para implementar las guías de laboratorio; además de la información necesaria para entender el funcionamiento básico de cada protocolo, se estudió las operaciones generales y especificas del software de simulación (Opnet Modeler) para desarrollar las respectivas configuraciones y así analizar los resultados obtenidos. El análisis de cada protocolo se basó en: la tabla de enrutamiento de cada router, la métrica, ancho de banda, balanceo de carga y tráfico en la red. A continuación se describirán las simulaciones realizadas y los resultados obtenidos.

Se diseñaron las guías de laboratorio con la ayuda del software de simulación Opnet Modeler, el cual la Universidad Pontificia Bolivariana cuenta con la última versión de la licencia académica permitiendo que se puedan desarrollar estas simulaciones. En las guías de laboratorio se encuentra todo el procedimiento de implementación y de configuración para cada protocolo.

4.2 REALIZACIÓN DE LAS SIMULACIONES

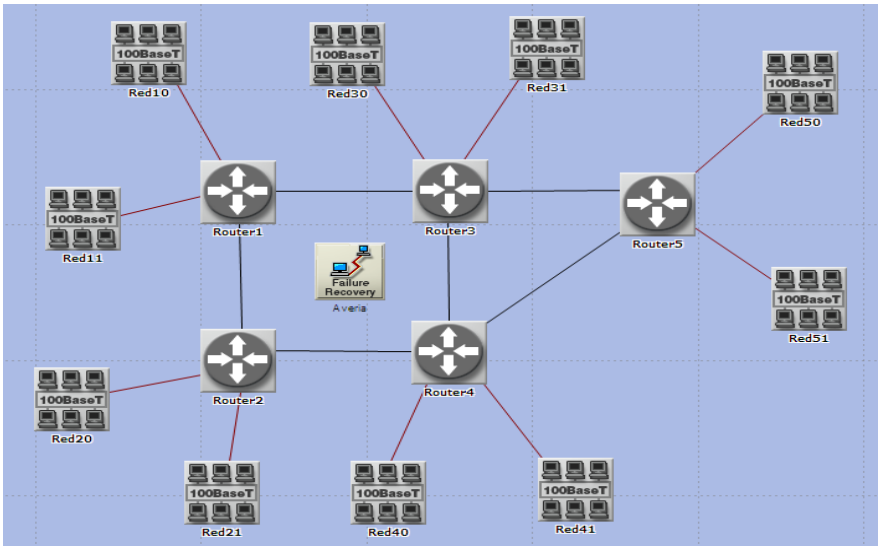
4.2.1 Prueba 1: RIP (ROUTING INFORMATION PROTOCOL)

- **Objetivo:** Generar tráfico RIP y analizar las prestaciones del protocolo para los dos escenarios (Averia y Sin_averia)

- **Arquitectura de la red:**

La estructura de la red está conformada por: 5 routers *ethernet4_slip8_gtwy*, 10 redes LAN *100BaseT_LAN* de tipo Fast Ethernet, 1 objeto *(Failure Recovery)* para modelar recuperación/fallos en los escenarios y los tipos de enlace *100BaseT* y *PPP_DS3* para la interconexión entre estos objetos. Los routers se configuraron con el protocolo de enrutamiento RIP y se establecieron las estadísticas para ver las prestaciones de este mismo, como son: Número total de actualizaciones, tráfico recibido y tráfico enviado de toda la red. Además, se exportaron las tablas de enrutamiento de cada router. En la figura 24 se puede apreciar la respectiva configuración.

Figura 24. Arquitectura de red utilizando el protocolo RIP



- **Metodología:**

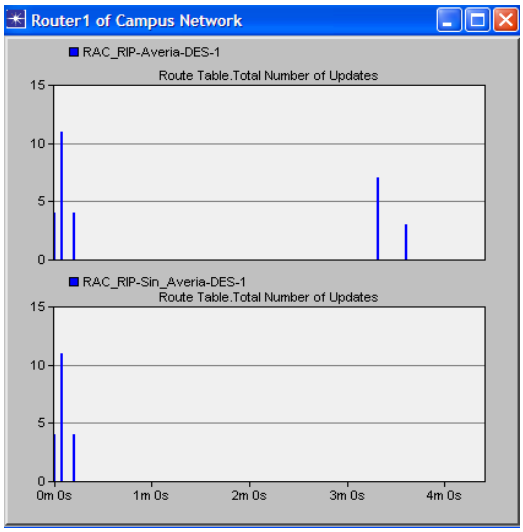
Se ejecutaron dos escenarios, el primero (Sin_averia) se configuró en condiciones normales para ver las prestaciones del protocolo RIP, luego en el segundo escenario (Averia) se configuró el objeto Failure Recovery para modelar un daño sobre el enlace entre los Routers 1 y 2; y de esta manera comparar los dos escenarios. Finalmente se ejecuta la simulación.

- **Resultados:**

Para verificar que se cumplió con los parámetros establecidos, se obtuvieron las siguientes gráficas:

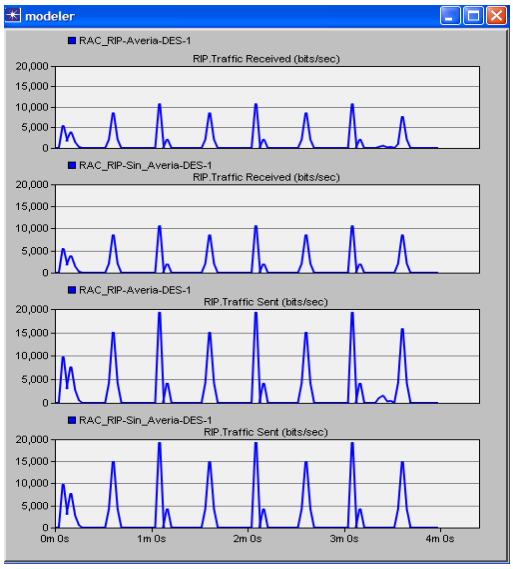
En la figura 25 se puede apreciar que el número total de actualizaciones de la tabla de enrutamiento del Router1 para el escenario Averia, se ve afectado 200 seg después de comenzar la simulación por el daño del enlace.

Figura 25. Total number of updates modo (Bar Chart)



En la figura 26 se muestra el tráfico recibido y el tráfico enviado de toda la red para los dos escenarios (Averia y Sin_averia).

Figura 26. Traffic Received y Traffic Sent para ambos escenarios



En la figura 27 se obtiene la tabla de enrutamiento del Router 4, permitiendo identificar cada una de las direcciones IP asignada a las interfaces.

Figura 27. Tabla de enrutamiento del Router 4

Performance.IP Forwarding Table at End of Simulation for Campus Network.Router4

File Edit View Help

	Destination	Source Protocol	Route Preference	Metric	Next Hop Address	Next Hop Node	Outgoing Interface	Outgoing LSP	Insertion Time (secs)
1	192.0.0.0/24	RIP	120	2	192.0.6.1	Campus Network.Router3	IF4	N/A	6.971
2	192.0.1.0/24	RIP	120	2	192.0.6.1	Campus Network.Router3	IF4	N/A	6.971
3	192.0.2.0/24	RIP	120	1	192.0.6.1	Campus Network.Router3	IF4	N/A	6.971
4	192.0.3.0/24	RIP	120	16	192.0.13.1	Campus Network.Router2	IF10	N/A	204.335
5	192.0.4.0/24	RIP	120	1	192.0.6.1	Campus Network.Router3	IF4	N/A	6.971
6	192.0.5.0/24	RIP	120	1	192.0.6.1	Campus Network.Router3	IF4	N/A	6.971
7	192.0.6.0/24	Direct	0	0	192.0.6.2	Campus Network.Router4	IF4	N/A	0.000
8	192.0.7.0/24	RIP	120	1	192.0.6.1	Campus Network.Router3	IF4	N/A	6.971
9	192.0.8.0/24	RIP	120	1	192.0.10.1	Campus Network.Router5	IF11	N/A	9.971
10	192.0.9.0/24	RIP	120	1	192.0.10.1	Campus Network.Router5	IF11	N/A	9.971
11	192.0.10.0/24	Direct	0	0	192.0.10.2	Campus Network.Router4	IF11	N/A	0.000
12	192.0.11.0/24	RIP	120	1	192.0.13.1	Campus Network.Router2	IF10	N/A	6.975
13	192.0.12.0/24	RIP	120	1	192.0.13.1	Campus Network.Router2	IF10	N/A	6.975
14	192.0.13.0/24	Direct	0	0	192.0.13.2	Campus Network.Router4	IF10	N/A	0.000
15	192.0.14.0/24	Direct	0	0	192.0.14.1	Campus Network.Router4	IF0	N/A	0.000
16	192.0.15.0/24	Direct	0	0	192.0.15.1	Campus Network.Router4	IF1	N/A	0.000
17									
18	Gateway of last resort is	not set							
19									

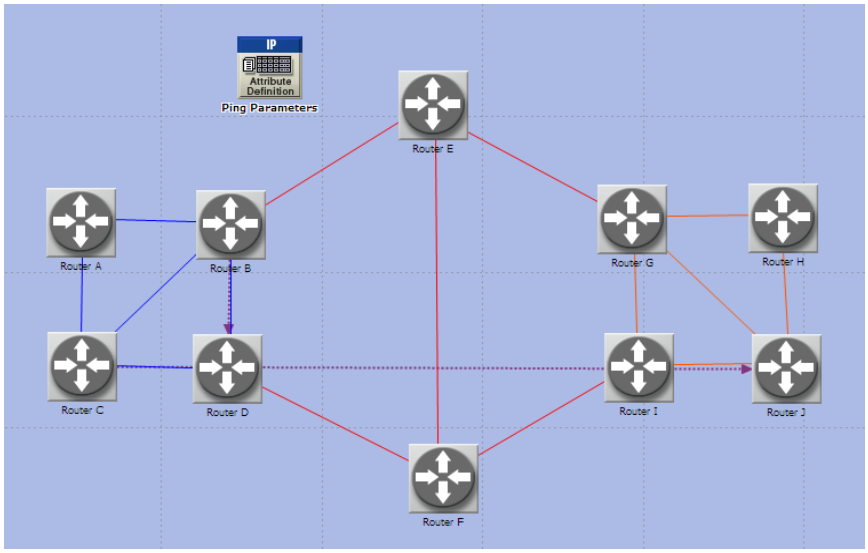
4.2.2 Prueba 2: OSPF (OPEN SHORTEST PATH FIRST)

- **Objetivo:** Establecer los niveles jerárquicos (backbone y áreas) en la estructura de la red y distribuir los pesos de los enlaces para obtener rutas alternativas, teniendo en cuenta las características del protocolo OSPF.

- **Arquitectura de la red:**

La estructura de la red está conformado por: 10 routers *slip8_gtwy*, 1 objeto *(Ping Parameters)* para definir la configuración de *Traffic Demands* y el tipo de enlace *PPP_DS3* para la interconexión entre routers. Los routers se configuraron con el protocolo de enrutamiento OSPF y se establecieron los niveles jerárquicos, además se creó demanda de tráfico entre parejas de routers para ver las rutas del flujo de tráfico (desde router origen a router destino), asignando pesos a los enlaces e incluso cambiándolos para crear rutas alternativas. También se exportaron las tablas de enrutamiento de cada router.
En la figura 28 se puede apreciar la respectiva configuración.

Figura 28. Arquitectura de red utilizando el protocolo OSPF



- **Metodología:**

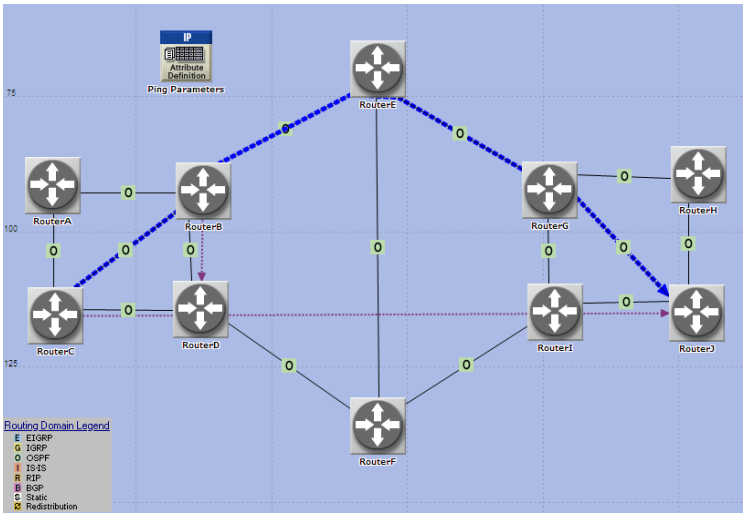
Se ejecutaron dos escenarios (Sin_areas y ruta_alternativa), en el primero se configuraron los pesos sobre los enlaces y se estableció la demanda de tráfico entre los Routers B-D y Routers C-J, luego en el segundo escenario (ruta_alternativa) se configuraron las respectivas áreas y se hizo distribución de pesos sobre los enlaces. También se habilitó la exportación de la tabla de enrutamiento de cada router.

- **Resultados:**

Para verificar que se cumplió con los parámetros establecidos, se obtuvieron las siguientes gráficas:

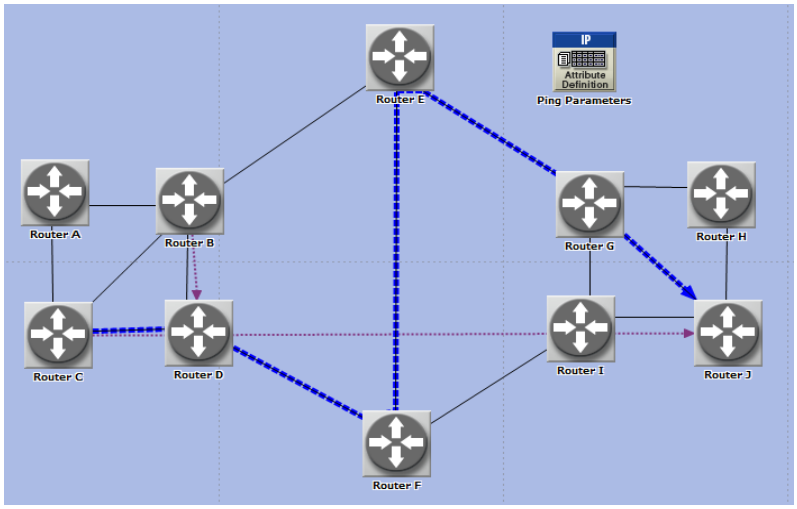
En la figura 29, para el escenario Sin_areas se puede apreciar la ruta que toma el flujo de tráfico desde el Router C hasta el Router J, basado en la ruta de menor costo.

Figura 29. Ruta basada en las características del protocolo OSPF (tráfico entre los Routers C – J)



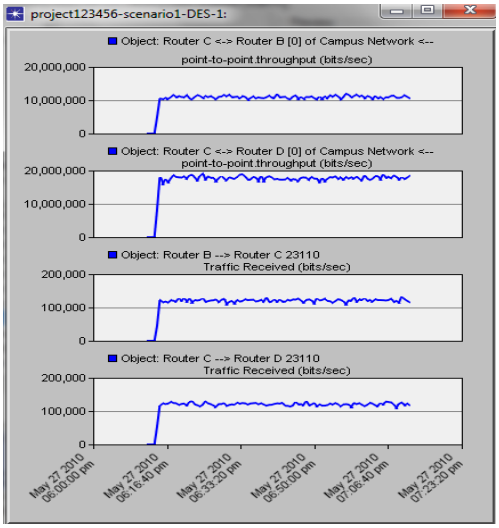
En la figura 30, para el escenario *Ruta_alternativa* se muestra la ruta que toma el flujo de tráfico desde el Router C hasta el Router J basado en la distribución de pesos sobre los enlaces teniendo en cuenta la ruta de menor costo.

Figura 30. Ruta alternativa para la demanda de tráfico entre los Routers C-J



En la figura 31, se puede apreciar los resultados obtenidos del ancho de banda y de tráfico recibido entre los Routers C-D para el escenario *Sin_areas*.

Figura 31. Representación del ancho de banda y tráfico recibido entre los Routers C- D y Routers B - C



4.2.3 Prueba 3: IS-IS (Intermediate System to Intermediate System)

- **Objetivo:** Establecer los tipos de sistemas (L1, L2, L1/L2) de cada router en su respectiva área y garantizar el balanceo de carga a través de los enlaces, dependiendo de la ruta de la demanda de tráfico.

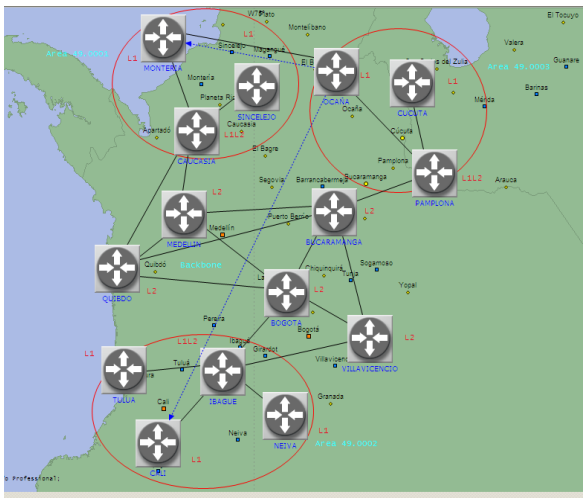
- **Arquitectura de la red:**

La estructura de red está conformado por: 15 routers *Ethernet2_slip8_gtwy*, 1 objeto *(Ping Parameters)* para definir la configuración de *Traffic Demands* y el tipo de enlace *PPP_SONET_OC12* para la interconexión entre routers.

Los routers se configuraron con el protocolo de enrutamiento IS-IS y se establecieron los niveles jerárquicos definiendo el tipo de sistema. Además se creó demanda de tráfico entre parejas de routers para ver las rutas del flujo de tráfico (desde router origen a router destino). Sobre el Router Bucaramanga se configuró la opción de balanceo de carga y también se exportaron las tablas de enrutamiento de cada router.

En la figura 32 se puede apreciar la respectiva configuración.

Figura 32. Arquitectura de la red utilizando el protocolo IS-IS



- **Metodología:**

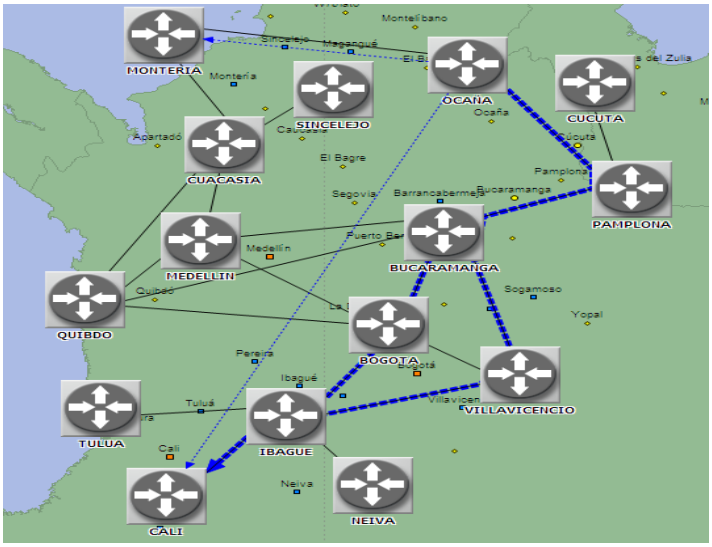
Se ejecutaron dos escenarios (Sin_jerarquia y red_jerarquica), en el primero se configuraron los routers con sus respectivos identificadores NET y tipos de sistemas Level 1-2, también se estableció la demanda de tráfico entre los Routers Ocaña-Cali y los Routers Ocaña-Monteria, luego en el segundo escenario (red_jerarquica) se configuraron las respectivas áreas, identificadores NET y su correspondiente tipo de sistema.

- **Resultados:**

Para verificar que se cumplió con los parámetros establecidos, se obtuvieron las siguientes gráficas:

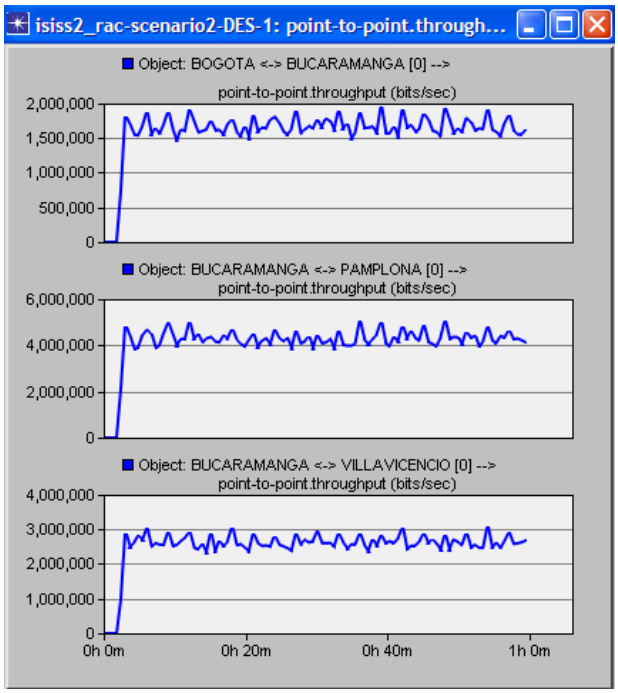
En la figura 33 se puede apreciar la ruta del flujo de tráfico desde el Router Ocaña hasta el Router Cali, proporcionando balanceo de carga a través del Router Bucaramanga.

Figura 33. Balanceo de carga, Ruta Ocaña – Cali (Escenario Red_jerarquia)



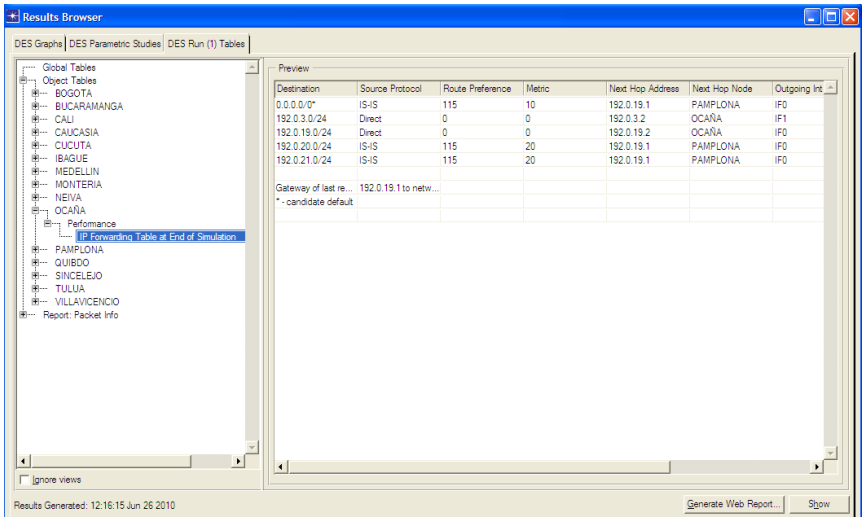
En la figura 34 se puede apreciar la garantia del balanceo de carga a través del ancho de banda entre los Routers Bucaramanaga-Bogota y los Routers Bucaramanga-Villavicencio.

Figura 34. Throughput entre los Routers: Bogota – Bucaramanga, Bucaramanga – Pamplona y Bucaramanga – Villaviencio. (Escenario sin_jerarquia)



En la figura 35 se puede apreciar que la tabla de enrutamiento del Router Ocaña posee pocas interfaces; esto se debe a la configuración de áreas establecidas permitiendo que se resuma la información en cada área y garantice escalabilidad al sistema.

Figura 35. Tabla de enrutamiento para el Router Ocaña (escenario red_jerarquica).



4.2.4 Prueba 4: BGP (Border Gateway Protocol)

- **Objetivo:** Implementar una red BGP garantizando las características generales que rige este protocolo, como son: establecer parejas de vecindad IBGP y EBGP; asignar sistemas autónomos y crear la tabla de vecinos. También, utilizar la opción throughput como una forma de visualización del ancho de banda, a partir del tráfico generado entre las corporaciones

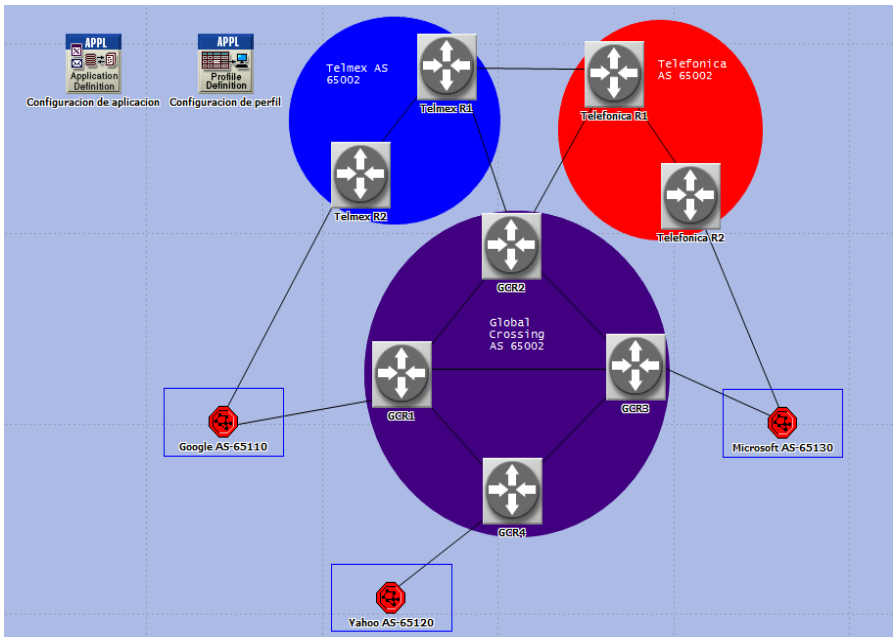
- **Arquitectura de la red:**

La estructura de red está formada por: 8 routers *atm4_ethernet2_slip8_gtwy_int*, 3 routers *ethernet4_slip8_gtwy,* 1 objeto *(Profile Definition)* y 1 *(Application Definition)* para definir la configuración de las prestaciones de servicio, 8 redes LAN de tipo *10BaseT_LAN,* 6 servidores, 3 switches 3Com y los tipos de enlaces *PPP_DS3* - *PPP_DS1* para la interconexión entre routers. Las parejas de routers

que se encuentran dentro del mismo AS se configuraron con la opción IBGP *peers* y la parejas de routers que se encuentran en diferente AS se configuraron con EBGP *peers*. A cada en router se le configuró la opción redistribución, sincronización y la tabla de las interfaces estableciendo: las direcciones próximas, el protocolo de enrutamiento y la máscara de subred. También, fue necesario construir la tabla de vecindad ya que BGP no descubre sus vecinos. Además, se creó envío de tráfico como prestación de servicio E-mail y Http entre las corporaciones Google, Yahoo y Microsoft.

En la figura 36 se puede apreciar la respectiva configuración.

Figura 36. Arquitectura de la red utilizando el protocolo BGP



- **Metodología:**

Se ejecutó un sólo escenario (Corporaciones), con el fín de enviar información (Email y Http) desde la corporación Google AS-65110 a las corporaciones Yahoo AS-65120 y Microsoft 65130.

- **Resultados:**

Para el escenario Corporaciones se obtuvieron los siguientes resultados, teniendo en cuenta los parámetros a analizar.

En las figura 37 se puede apreciar que el ancho de banda entre los Routers Telmex R2 y Router de Google es prácticamente cero. Debido a que la ruta que emplea el menor número de AS es a través de Global Crossing, de este modo se puede apreciar en la figura 40 el ancho de banda entre el Router GCR1 y Router de Google.

Figura 37. Ancho de banda (Google AS-65110 – Telmex R2)

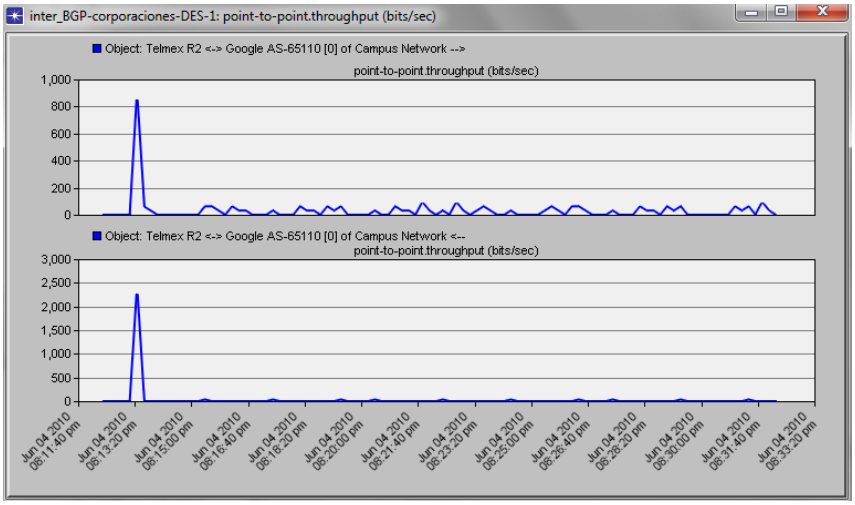
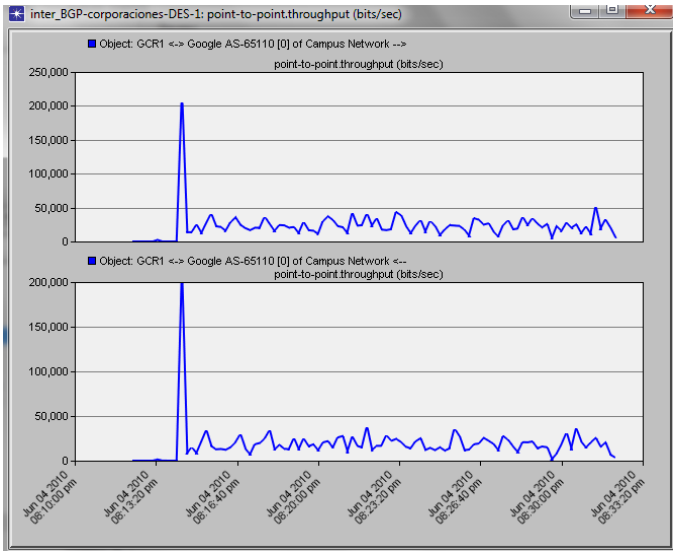
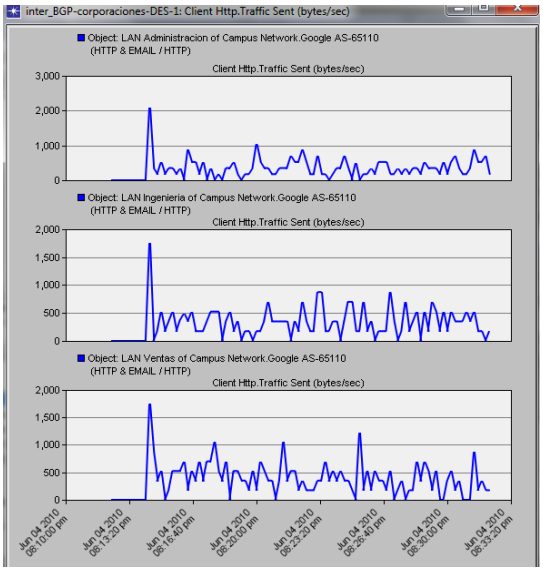


Figura 38. Ancho de banda (Google AS-65110 – GCR1)



En la figura 39 se aprecia el envió de información E-mail y Http desde la red LAN Administración perteneciente a la corporación de Google.

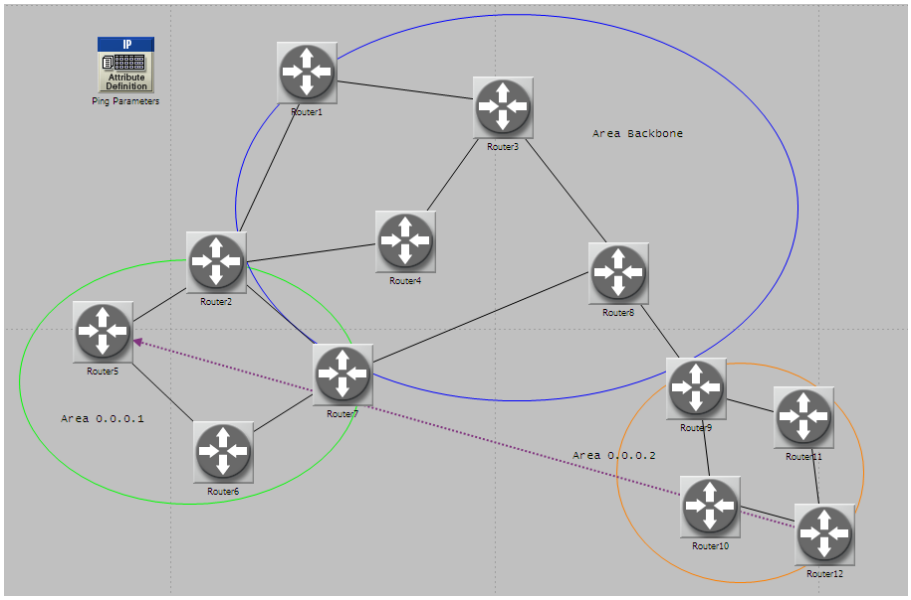
Figura 39. Tráfico enviado (LAN Administración)



4.2.5 Prueba 5: APLICACIÓN DEL PROTOCOLO OSPF PARA DESARROLLAR INGENIERIA DE TRÁFICO.

Para la quinta guía de laboratorio, se implementó una estructura de red con: 12 routers *slip8_gtwy*, 1 objeto *(Ping Parameters)* para definir la configuración de *Traffic Demands*, 1 objeto *(Failure Recovery)* para modelar recuperación/fallos en los escenarios y el tipo de enlace *PPP_DS3* para la interconexión entre routers. En la figura 40 se puede apreciar la respectiva configuración.

Figura 40. Arquitectura de la red utilizando el protocolo OSPF para desarrollar Ingeniería de Tráfico



Para los 4 escenarios (Ruta, Avería, Balanceo y Distribución) se obtuvieron los siguientes resultados, teniendo en cuenta los parámetros a analizar: ruta de menor costo, balanceo de carga, distribución de pesos, tabla de enrutamiento, utilización y ancho de banda sobre los enlaces.

En las figuras 41, 42, 43, 44, 45 y 46 se pueden apreciar los resultados obtenidos:

Figura 41. Ruta de menor costo

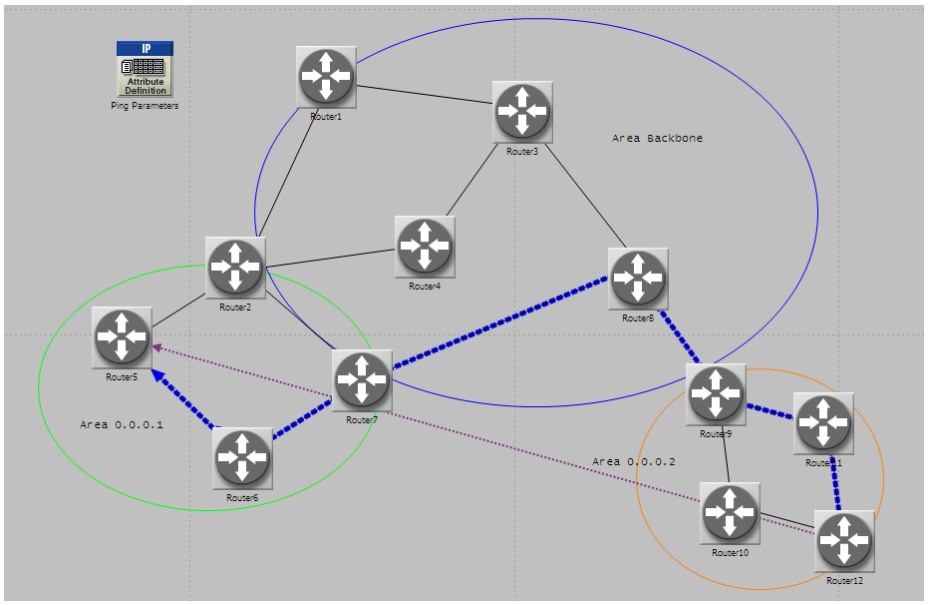


Figura 42. Ruta alternativa de menor costo

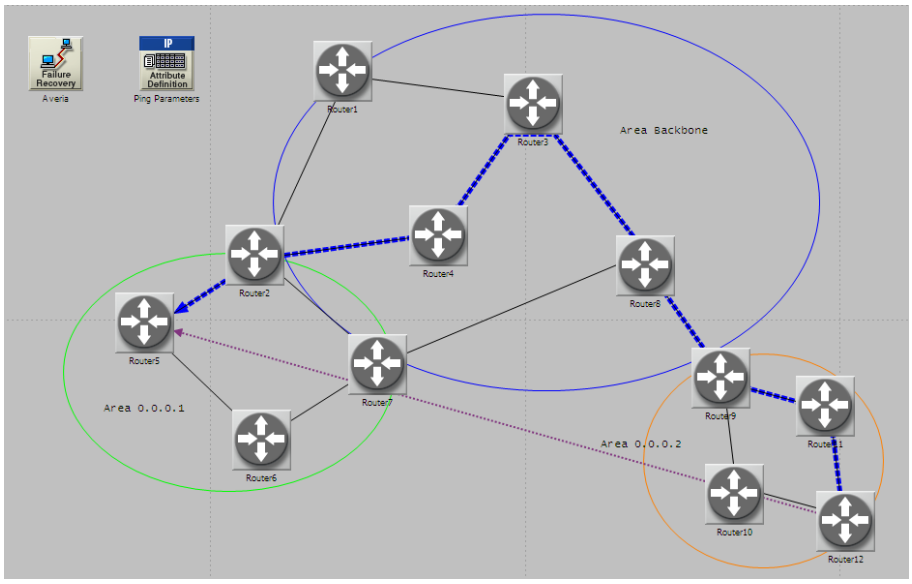


Figura 43. Balanceo de carga

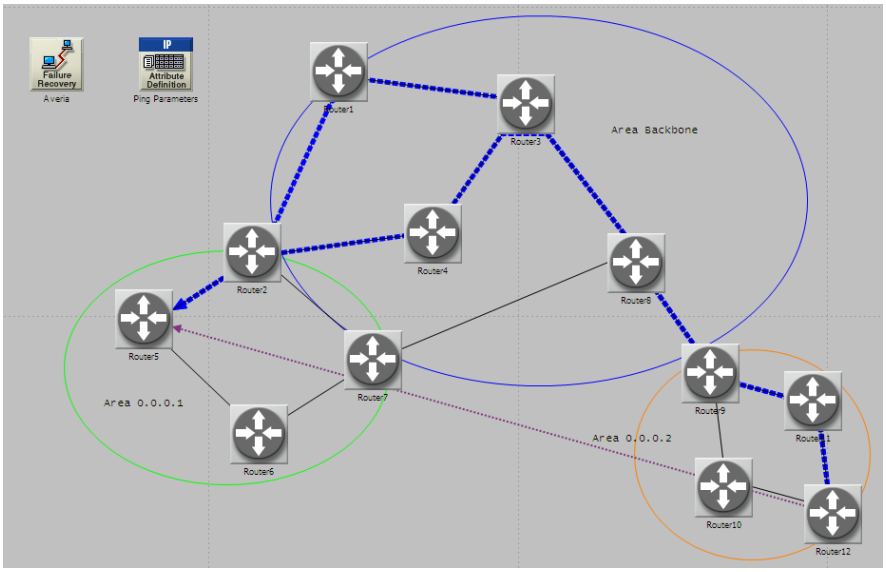


Figura 44. Ancho de banda (Escenario Balanceo)

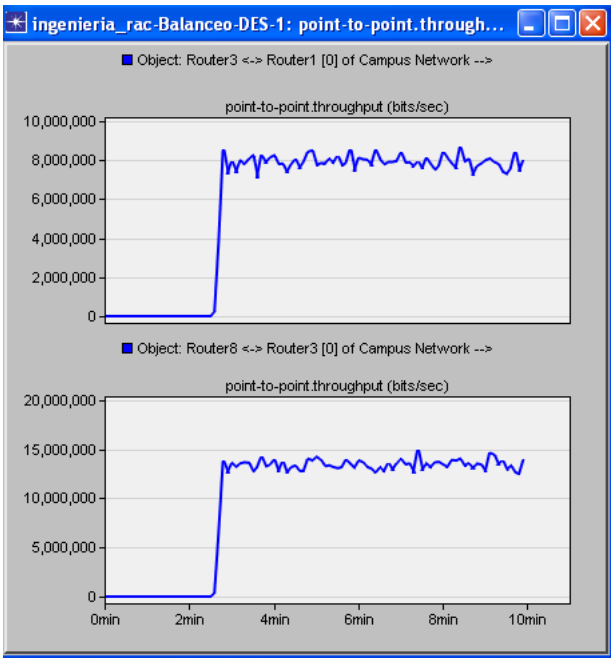
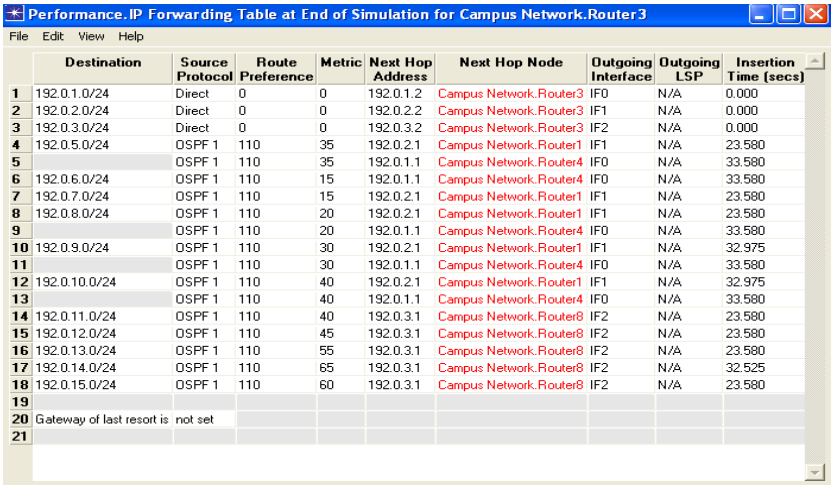


Figura 45. Tabla de enrutamiento – Router 3 (Escenario Balanceo)

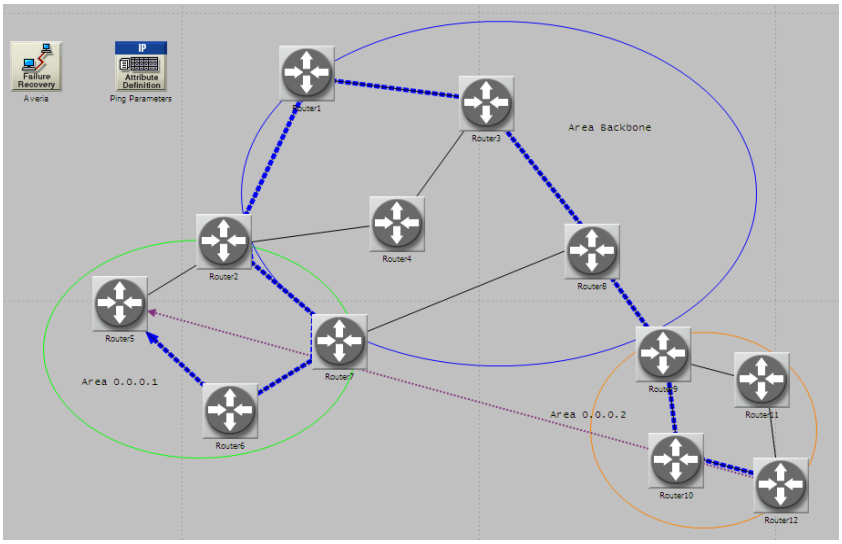


Performance.IP Forwarding Table at End of Simulation for Campus Network.Router3

File Edit View Help

	Destination	Source Protocol	Route Preference	Metric	Next Hop Address	Next Hop Node	Outgoing Interface	Outgoing LSP	Insertion Time (secs)
1	192.0.1.0/24	Direct	0	0	192.0.1.2	Campus Network.Router3	IF0	N/A	0.000
2	192.0.2.0/24	Direct	0	0	192.0.2.2	Campus Network.Router3	IF1	N/A	0.000
3	192.0.3.0/24	Direct	0	0	192.0.3.2	Campus Network.Router3	IF2	N/A	0.000
4	192.0.5.0/24	OSPF 1	110	35	192.0.2.1	Campus Network.Router1	IF1	N/A	23.580
5		OSPF 1	110	35	192.0.1.1	Campus Network.Router4	IF0	N/A	33.580
6	192.0.6.0/24	OSPF 1	110	15	192.0.1.1	Campus Network.Router4	IF0	N/A	33.580
7	192.0.7.0/24	OSPF 1	110	15	192.0.2.1	Campus Network.Router1	IF1	N/A	23.580
8	192.0.8.0/24	OSPF 1	110	20	192.0.2.1	Campus Network.Router1	IF1	N/A	23.580
9		OSPF 1	110	20	192.0.1.1	Campus Network.Router4	IF0	N/A	33.580
10	192.0.9.0/24	OSPF 1	110	30	192.0.2.1	Campus Network.Router1	IF1	N/A	32.975
11		OSPF 1	110	30	192.0.1.1	Campus Network.Router4	IF0	N/A	33.580
12	192.0.10.0/24	OSPF 1	110	40	192.0.2.1	Campus Network.Router1	IF1	N/A	32.975
13		OSPF 1	110	40	192.0.1.1	Campus Network.Router4	IF0	N/A	33.580
14	192.0.11.0/24	OSPF 1	110	40	192.0.3.1	Campus Network.Router8	IF2	N/A	23.580
15	192.0.12.0/24	OSPF 1	110	45	192.0.3.1	Campus Network.Router8	IF2	N/A	23.580
16	192.0.13.0/24	OSPF 1	110	55	192.0.3.1	Campus Network.Router8	IF2	N/A	23.580
17	192.0.14.0/24	OSPF 1	110	65	192.0.3.1	Campus Network.Router8	IF2	N/A	32.525
18	192.0.15.0/24	OSPF 1	110	60	192.0.3.1	Campus Network.Router8	IF2	N/A	23.580
19									
20	Gateway of last resort is	not set							
21									

Figura 46. Ruta 2 (Escenario Distribución)



CONCLUSIONES

- Se realizó diferentes guías de laboratorio sobre los protocolos de enrutamiento (RIP, BGP, OSPF, IS-IS) en la red que ofrecen una mejor comprensión además de la parte teórica; para así establecer una configuración práctica del funcionamiento de cada protocolo en la red.

- La implementación de los protocolos de enrutamiento en la red (RIP, BGP, OSPF, IS-IS) permiten que se pueda desarrollar ingeniería de tráfico garantizando que la comunicación sea de mejor calidad posible. Para ello se manejan diferentes métricas ó características de las rutas como son: ancho de banda, retardo, carga, confiabilidad, número de saltos, costo, etc. Y de esta manera brindar QoS en las aplicaciones ofrecidas al usuario.

- La configuración de los atributos que describen la métrica BGP, garantizan la preferencia para determinar el trayecto del tráfico proporcionando alternativas en la entrega fiable de la información.

- La configuración jerárquica de áreas en una estructura de red OSPF e ISIS garantiza que haya escalabilidad en el sistema, permitiendo que la información en cada AS se pueda resumir para el resto de la red. Obteniendo asi, tiempos de convergencia mas rapidos a través de las actualizaciones generadas por inundaciones de LSA y las mejores rutas para el árbol SPF de cada tabla de enrutamiento.

- OPNET *Modeler*, en una herramienta de simulación de redes, confiable y estable en sus procesos, reconocida a nivel mundial por los mejores fabricantes y desarrolladores para dispositivos de *networking*. La proyección que este *software* puede brindar a su grupo de investigación en telecomunicaciones (GITEL),la asignatura de Redes (Optativa) y a los programas de postgrado y maestría de la facultad de ingeniería electrónica, para nuevos proyectos de investigación.

BIBLIOGRAFÍA

- HEDRICK, C. Routing Information Protocol (RIP): RFC 1058, Rutgers University. June 1988.Disponible en: http://www.freesoft.org/CIE/RFC/1058/index.htm
- RFC 2328, (OSPF) Open Shortest Path First, Abril 1998.
- RFC 3784, (IS-IS) Intermediate System to Intermediate System, Junio 2004.
- RFC 4271, (BGP) Border Gateway Protocol, Enero 2006.
- QUINTERO, Edison y ALVARO, Luis. ESTADO DEL ARTE EN LA APLICACIÓN DE INGENIERIA DE TRAFICO EN REDES IP. pdf. Universidad Pontificia Bolivariana.2010
- MEDHI, Deepankar y RAMASAMY, Karthikeyan. NETWORK ROUTING Algorithms, Protocols, and Architectures. Oxford, Elsevier. 2007.
- STALLINGS, William. Comunicaciones y Redes de Computadores. Séptima edición; 2004.
- MALHOTRA, Ravi. IP Routing. United States of America, O'Reilly & Associates. 2002.
- SHEWANDAGN, Esuendale y ATHAR, Syed. Performance Comparison of EIGRP/ IS-IS and OSPF/ IS-IS. pdf. Blekinge Institute of Technology. 2009

ANEXOS

GUÍAS DE LABORATORIO SOBRE PROTOCOLOS DE ENRUTAMIENTO EN LA RED

AUTORES:
ROBINSON ALVARADO CADENA
JHON JAIRO PADILLA AGUILAR

REDES DE COMPUTADORES (OPTATIVA)
FACULTAD DE INGENIERIA ELECTRÓNICA
UNIVERSIDAD PONTIFICIA BOLIVARIANA

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE INGENIERÍA Y ADMINISTRACIÓN
PROGRAMA DE INGENIERÍA ELECTRÓNICA
REDES DE COMPUTADORES (OPTATIVA)

ANEXO 1

GUÍA PRÁCTICA SOBRE PROTOCOLOS DE ENRUTAMIENTO EN LA RED

Práctica N°1

TÍTULO: RIP (ROUTING INFORMATION PROTOCOL)

OBJETIVOS:

- Analizar las tablas de enrutamiento de los routers a partir de los diferentes escenarios (Avería y Sin Avería) diseñados en la práctica de laboratorio.
- Generar tráfico RIP y compararlo a partir de las gráficas obtenidas en diferentes escenarios
- Familiarizar al estudiante con el uso del software de simulación Opnet Modeler; para las aplicaciones del protocolo de enrutamiento RIP en la red.

1. MARCO TEÓRICO:

Sistema Autónomo (AS, Autonomous System)

Un sistema autónomo es un conjunto de redes administradas por una misma organización que tiene definida una única política de encaminamiento y posee las siguientes características:

- Un AS se compone de un conjunto de encaminadores y redes gestionados por una única organización.
- Un AS se compone de un grupo de dispositivos de encaminamiento que intercambian información a través de un protocolo de encaminamiento común.
- Excepto en momentos de avería, un AS está conectado (en un sentido teórico de grafo). Es decir, existe un camino entre cualquier par de nodos.

Un protocolo común de encaminamiento, al que nos referimos como protocolo de encaminador interior (IRP, Interior Router Protocol), distribuye la información de encaminamiento entre los dispositivos de encaminamiento dentro de un AS. El protocolo que se emplea dentro de un sistema autónomo no necesita ser implementado fuera del sistema. Esta flexibilidad permite que los IRP se hagan a medida para aplicaciones y requisitos específicos.

Ahora, una forma diferente de caracterizar protocolos de encaminamiento para redes interconectadas, es que emplean diferentes enfoques para recopilar y utilizar información de encaminamiento; como es el encaminamiento por vector distancia. El protocolo de información de encaminamiento RIP (Routing Information Protocol) utiliza este enfoque.

RIP es un protocolo de *vector de distancia*, es decir que cada router le comunica al resto de los routers la distancia que los separa (cantidad de saltos que los separa). Por lo tanto, cuando un router recibe uno de estos mensajes incrementa esta distancia en 1, y envía el mensaje a los routers directamente accesibles. De esta manera, los routers pueden mantener la ruta óptima de un mensaje, al almacenar la dirección del router siguiente en la tabla de enrutamiento de manera tal que la cantidad de saltos para alcanzar una red se mantenga al mínimo. Sin embargo,

este protocolo sólo tiene en cuenta la distancia entre equipos en cuanto a saltos y no considera el estado de la conexión para seleccionar el mejor ancho de banda.[40]

2. PROCEDIMIENTO:

A continuación veremos en la figura 1 el diseño de la arquitectura de red que emplearemos en la simulación, seguido de los pasos para desarrollar la práctica.

Elementos:

- **Router IP (ethernet4_slip8_gtwy):** El modelo representa un nodo ethernet4_slip8_gtwy, el cual opera como una puerta de enlace IP y contiene cuatro interfaces Ethernet hub, y ocho interfaces de línea seriales. Los paquetes IP que llegan a cualquier interfaz se enrutan a la interfaz de salida adecuada en función de su dirección IP de destino.

- **Fast EthernetLAN (100BaseT_LAN):** Se usa este objeto para representar una red LAN de tipo Fast Ethernet en una topología conmutada. Este objeto contiene un servidor y un número de clientes especificado por el usuario. El tráfico de los clientes puede ser dirigido hacia el servidor interno, así como a servidores externos.

- **Link (PPP_DS3):** Enlace que utiliza el protocolo PPP y que tiene una capacidad de 44,736 Mbps.

- **Link (100BaseT):** El enlace duplex 100BaseT representa una conexión Ethernet que opera a 100 Mbps. Puede conectar cualquier combinación de los siguientes nodos: Estación, hub, puente, switch, nodos LAN.

[40] STALLINGS, William. Comunicaciones y Redes de Computadores. Séptima edición; 2004. p. 642 – 643

- **Failure Recovery:** Este modulo puede ser utilizado para modelar recuperación/fallos en los escenarios. Proporciona atributos para controlar el tiempo y el estado de diferentes objetos del modelo.

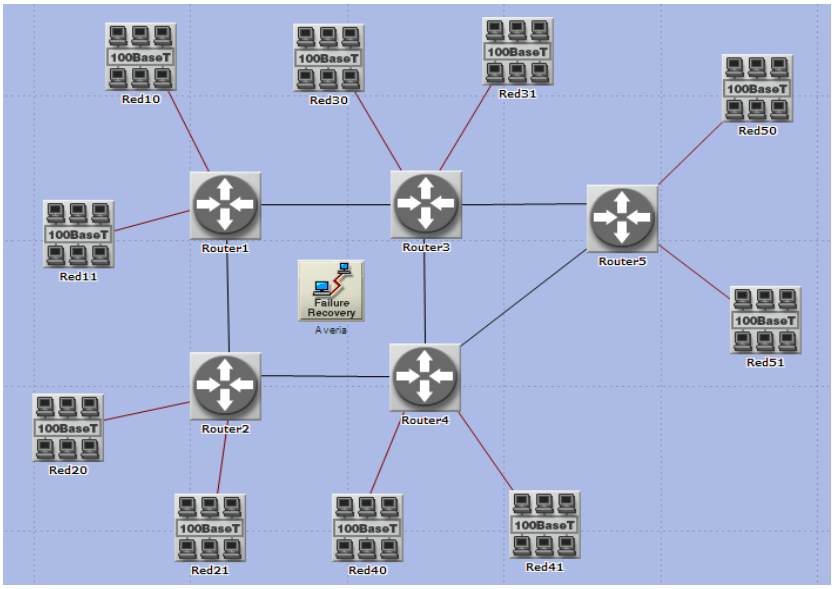


Figura 1. Arquitectura de red utilizando el protocolo RIP

2.1 Creación del proyecto:

I. Inicie el simulador Opnet Modeler, para la creación del nuevo proyecto elija en la barra de menú la opción **File** y seleccione **New** para crear el proyecto, luego presione Click en **Project** y por último **Ok**. Ahora dele un nombre al proyecto, por ejemplo: *tu nombre_RIP*; dele el nombre *Sin_Averia* al escenario a crear y presione **Ok.** Aparecerá la ventana de *Startup Wizard,* haga Click en **Next** para elegir el área sobre la cual se desea crear la arquitectura de red, seleccione la opción **Campus** y presione **Next.** Ahora, para adecuar el tamaño de la red, asigne los valores **x=60** y **y=40**. Finalmente presione **Next** dos veces y luego **Finish.**

2.2 Creación y configuración de la red:

I. Seguidamente aparecerá la paleta de dialogo (Object Pallete), la cual permitirá acceder a los elementos de trabajo para el diseño de la red, en caso de que no aparezca pulse en la barra de menú el botón  .Al desplegarlo es necesario que la opción **internet tool_box** esté seleccionada.

II. En la paleta de dialogo seleccione el router **ethernet4_slip8_gtwy** y sitúe 5 de estos mismos en el espacio de trabajo presionando Click izquierdo (para terminar de colocar los objetos presione Click derecho). Utilice el enlace bidireccional **100BaseT** para conectar los routers y renómbrelos como aparece en la figura 2, para esto debe dar Click derecho sobre el objeto y seleccione **Set Name.** En la figura 2 veremos la respectiva conexión.

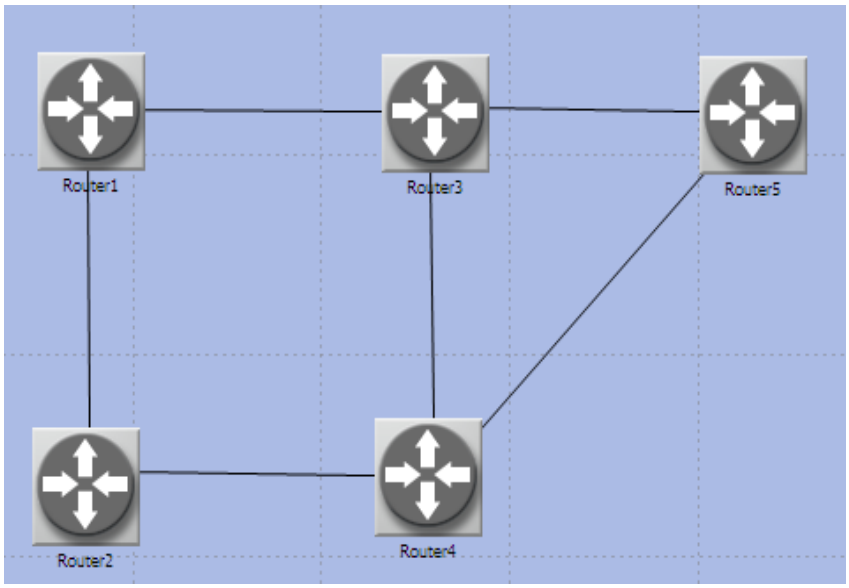


Figura 2. Interconexión de los routers ethernet4_slip8_gtwy utilizando el enlace 100BaseT

III. Salve el proyecto, luego seleccione en la paleta de dialogo la topología de red **100BaseT_LAN** y despliegue 10 objetos de este mismo tipo en el espacio de trabajo. Utilice el enlace **PPP_DS3** y conecte los objetos **100BaseT_LAN** con los routers, como se ve continuación en la figura 3.

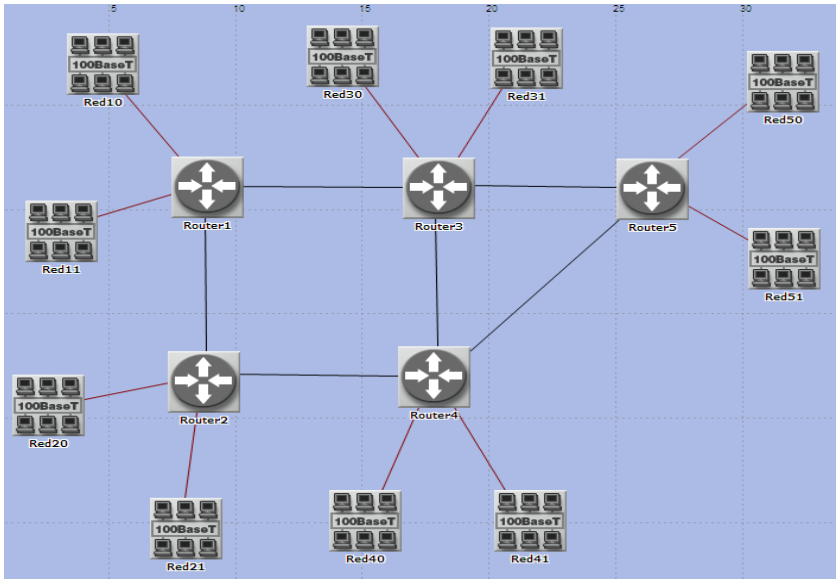


Figura 3. Conexión entre las topologías de red y los routers

IV. Seleccione el Router 4 y dele Click derecho, escoja **Edit Attributes** y luego en **Reports** despliegue la jerarquía **IP Forwarding Table**, habilite **Status= Enabled** y al frente de **IP Forwarding Table** en el campo de **Value** dale **Export at End of Simulation** (esta opción permitirá que el Router 4 exporte su tabla de enrutado al final de la simulación).

2.3 Configuración de estadísticas y atributos globales de la red:

I. Es necesario configurar las estadísticas para ver las prestaciones del protocolo RIP. Para esto debe dar Click derecho sobre el campo de trabajo y escoge **Choose Individual DES Statistics**. Ahora en el cuadro de diálogo despliegue

Global Statistics, seleccione **RIP** y por último marque **Traffic Received (bits/sec)** y **Traffic Sent (bits/sec)**. En el mismo cuadro de diálogo despliegue **Node Statistics**, seleccione **Route Table** y por último marque **Total Number of Updates**. Presione Click en **Ok** y salve el proyecto.

II. Seleccione en la barra de menú el botón  , ahora despliegue la opción **Inputs** y escoja **Global Atributes**, para hacer que RIP sea el protocolo de enrutado en todos los routers de la red; dele Click en **IP**, escoja **IP Dynamic Routing Protocol = RIP** y por último seleccione **IP Interface Addressing Mode = Auto Addessed / Export.**

Para que el protocolo siga actualizando la tabla de enrutado a pesar de algún cambio en la red; debe desplegar **Simulation Efficiency** y seleccione **Disabled**. Dale **Apply** y salve el proyecto.

2.4 Creación de nuevo escenario (Avería):

I. En la barra de menú despliegue **Scenarios** y seleccione **Duplicate Scenario** (dele el nombre de **Avería**), dale Ok.

II. Seleccione **Object Palette**  y escoja el objeto **Failure Recovery** (si no aparece, escriba en **Search by name** el nombre de este objeto) , sitúelo en el espacio de trabajo y llámelo **Avería**, ahora dele Click derecho sobre el objeto y escoja **Edit Atributes**, al frente de **Link Failure/Recovery Specification** escoja **Edit** y dele Click en **Insert**, al hacer esto **Number of rows** se pone en 1, ahora cambie **Time (seconds)** por 200 segundos y en **Name** seleccione **Campus Network.Router1<>Router2**; esto hará que en el enlace entre los nodos 1 y 2 ocurra un daño 200 segundos después de comenzar la simulación; por último dele **Ok** y salve el proyecto. Esta configuración se puede apreciar en la figura 3 y 4.

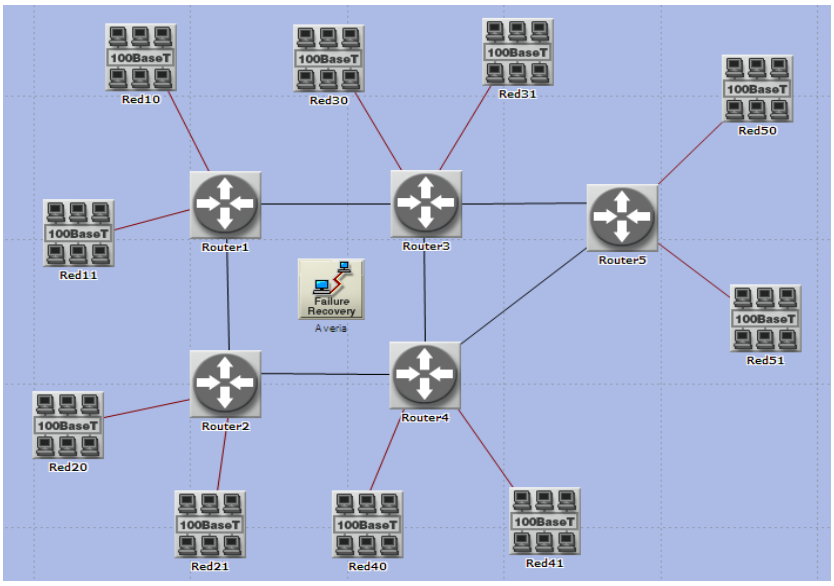


Figura 3. Diseño de la red (escenario Daño)

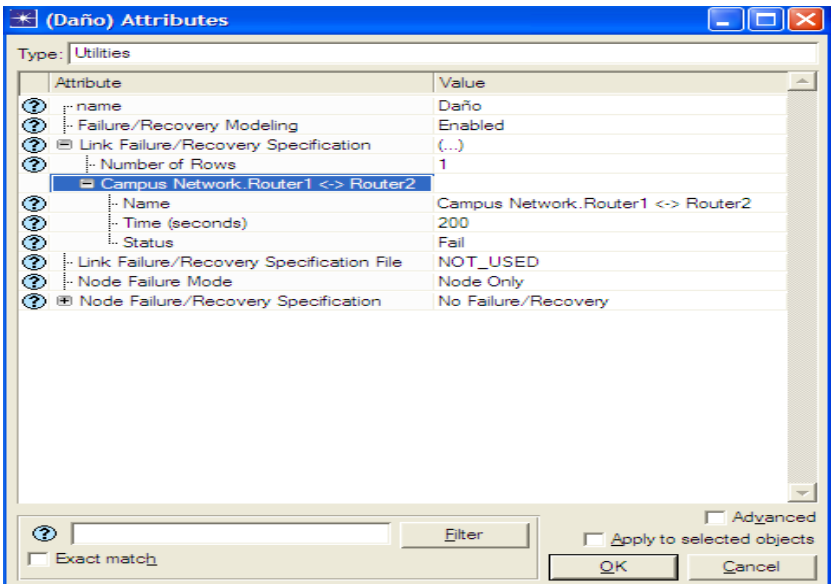


Figura 4. Configuración del objeto Failure Recovery

2.5 Ejecutar la simulación y ver los resultados:

I. Despliegue el menú **Scenarios** y seleccione **Manage Scenarios**, luego en el campo de **results** cambie para cada escenario la opción **collect** o **recollect**. Ahora para establecer el tiempo de la simulación; en el campo **Sim Duration** escriba 4 y en **Time Units** escoja **min**, dele **Ok**. Al finalizar presione **Close** y salve el proyecto.

II. En la barra de menú seleccione **DES**, luego en **Results** escoja **Compare Results,** aparecerá la ventana **Result Browser** y seleccione los campos **Avería y Sin Avería**, despliegue en **Object Statistics** la opción **Campus Network** y por ultimo **Router1**.

A continuación se puede apreciar en la figura 5 y 6; el número total de actualizaciones de los dos escenarios para el Router1. (Para ver mejor la imagen seleccione **Show** y dele Click derecho sobre la gráfica, escoge **Draw Style** y por último **Bar Chart**).

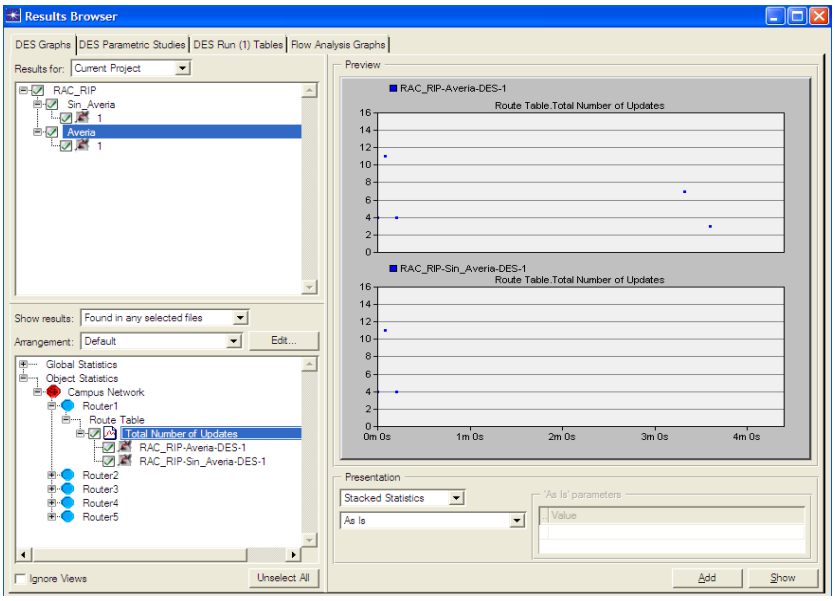


Figura 5. Graficas del número total de actualizaciones para los dos escenarios (Avería y Sin Avería)

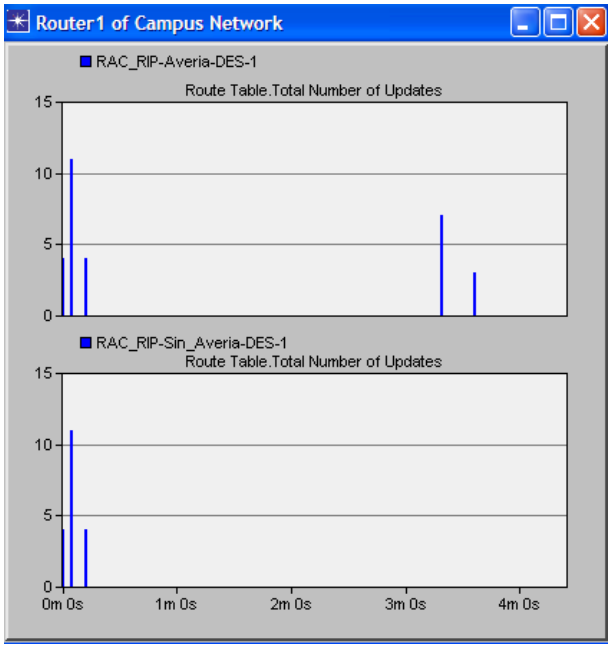


Figura 6. Representación de la gráfica en modo Bar Chart

III. Ahora, para visualizar la comparación del tráfico RIP sobre toda la red en los dos escenarios, seleccione los campos: **Avería y Sin Avería**, despliegue en **Global Statistics** la opción **RIP**, escoja **Traffic Received (bits/sec)** y aparecerá como se ve en la figura 7.

Si desea ver las gráficas de ambos tráficos (Traffic Received y Traffic Sent) para los dos escenarios, adicionalmente seleccione **Traffic Sent (bits/sec)**. Para una mejor visualización de las gráficas seleccione Show como aparece en la figura 8.

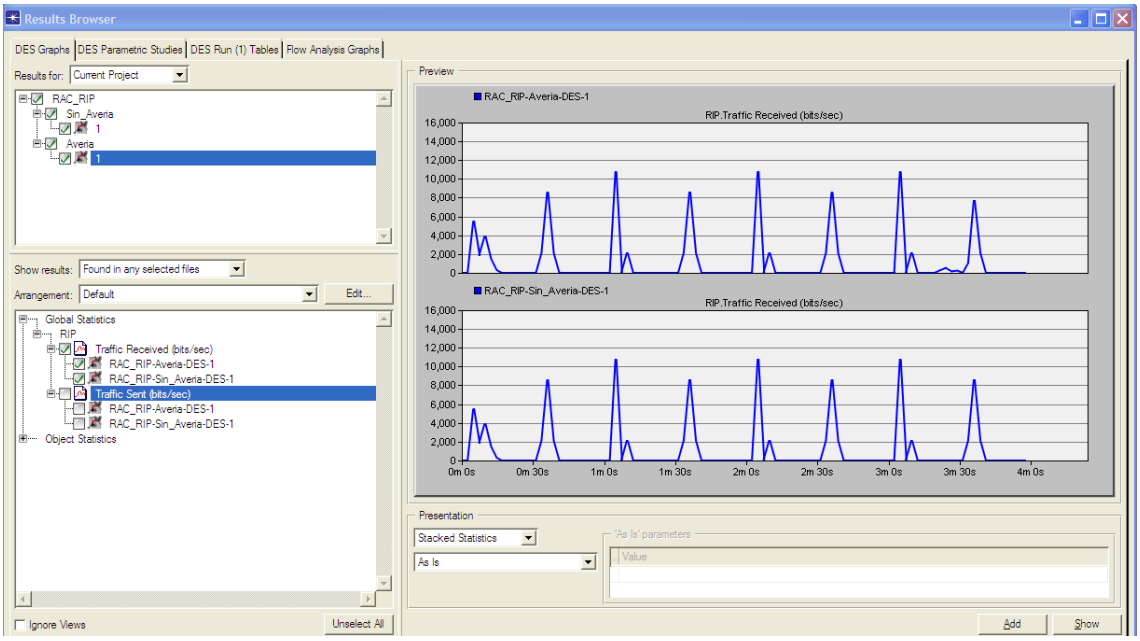


Figura 7. Visualización del tráfico RIP (Traffic Received) para ambos escenarios

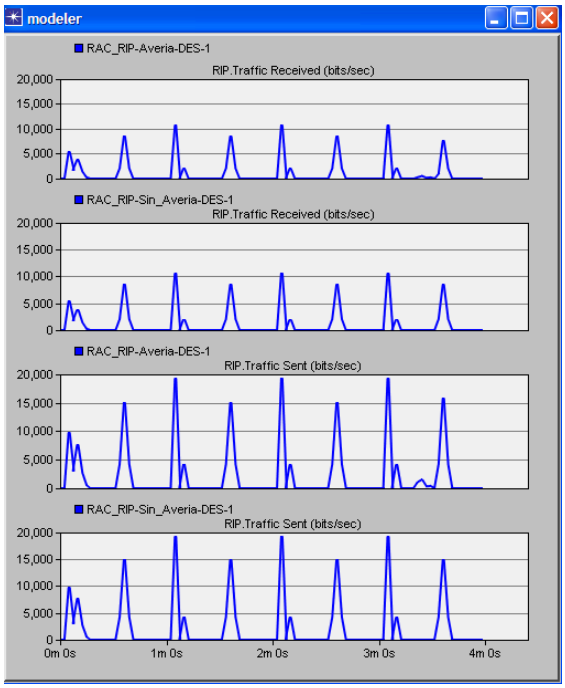


Figura 8. Visualización del tráfico RIP (Traffic Received y Traffic Sent) para ambos escenarios

IV. Para obtener la tabla de enrutamiento del Router 4, debe seleccionar sobre la barra de menú de **Results Browser** la opción **DES Run (1) Tables**, despliegue **Object Tables** y seleccione las siguientes opciones en cadena: **Campus Network**, después **Router 4**, luego **Performance** y por último **IP Forwarding Table at End of Simulation**.

En la figura 9 se aprecia la respectiva tabla de enrutamiento para el Router 4.

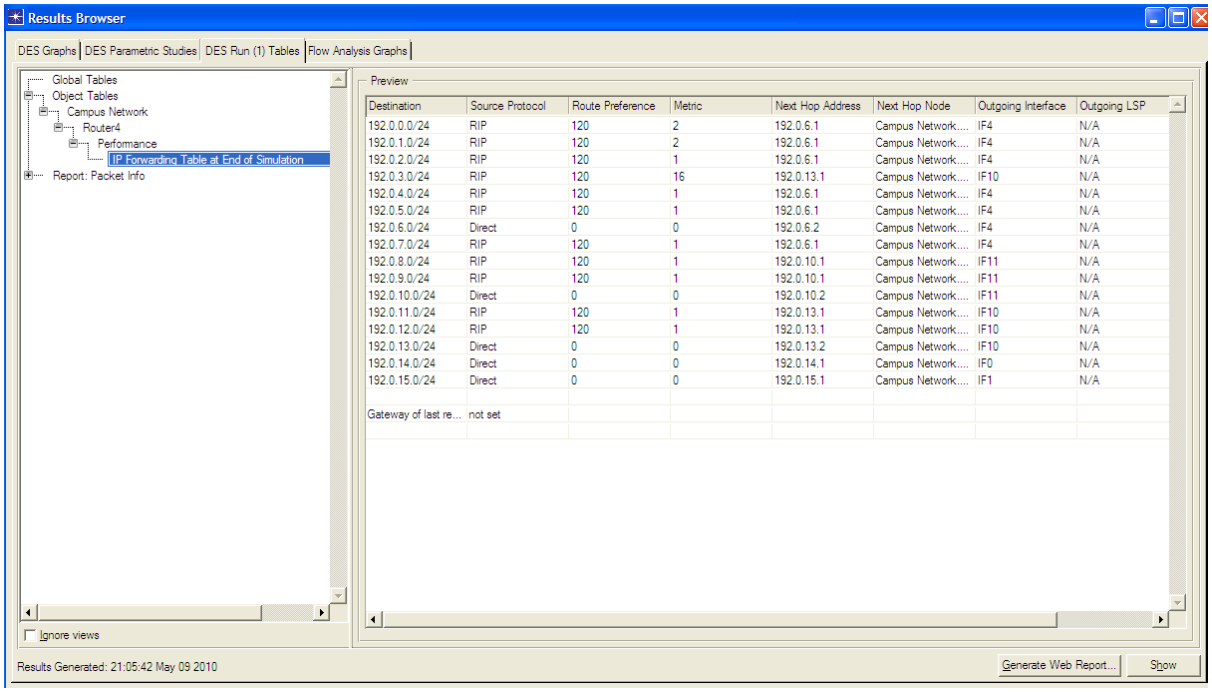
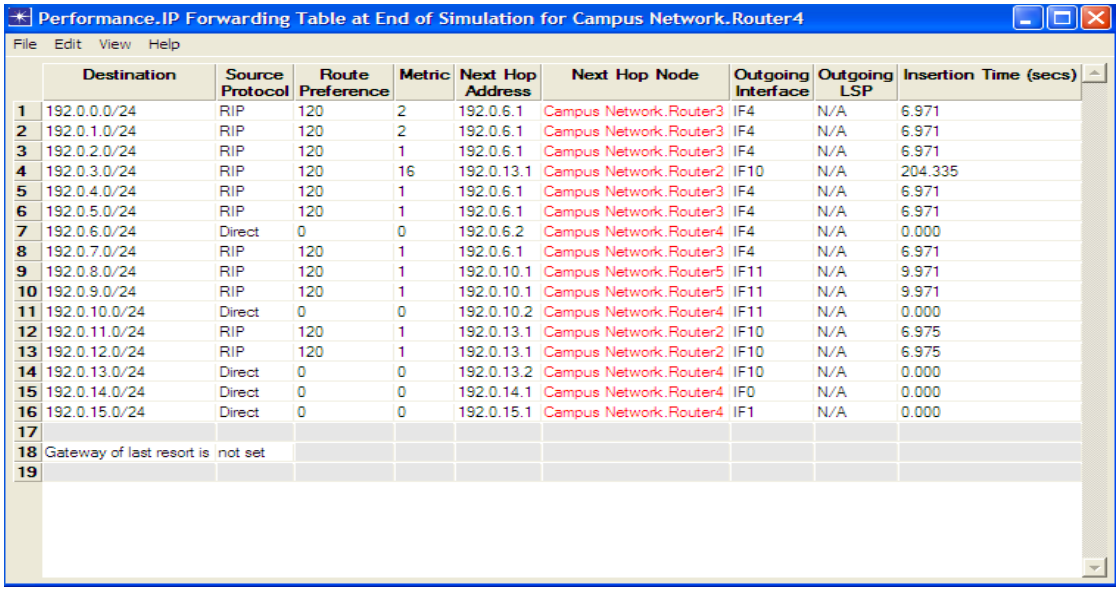


Figura 9. Tabla de enrutamiento del Router 4

Si desea ver sólo la tabla de enrutamiento (mayor comodidad) debe presionar Click sobre la tabla de enrutamiento y se desplegara de esta forma como se ve en la figura 10.



Performance.IP Forwarding Table at End of Simulation for Campus Network.Router4

File Edit View Help

	Destination	Source Protocol	Route Preference	Metric	Next Hop Address	Next Hop Node	Outgoing Interface	Outgoing LSP	Insertion Time (secs)
1	192.0.0.0/24	RIP	120	2	192.0.6.1	Campus Network.Router3	IF4	N/A	6.971
2	192.0.1.0/24	RIP	120	2	192.0.6.1	Campus Network.Router3	IF4	N/A	6.971
3	192.0.2.0/24	RIP	120	1	192.0.6.1	Campus Network.Router3	IF4	N/A	6.971
4	192.0.3.0/24	RIP	120	16	192.0.13.1	Campus Network.Router2	IF10	N/A	204.335
5	192.0.4.0/24	RIP	120	1	192.0.6.1	Campus Network.Router3	IF4	N/A	6.971
6	192.0.5.0/24	RIP	120	1	192.0.6.1	Campus Network.Router3	IF4	N/A	6.971
7	192.0.6.0/24	Direct	0	0	192.0.6.2	Campus Network.Router4	IF4	N/A	0.000
8	192.0.7.0/24	RIP	120	1	192.0.6.1	Campus Network.Router3	IF4	N/A	6.971
9	192.0.8.0/24	RIP	120	1	192.0.10.1	Campus Network.Router5	IF11	N/A	9.971
10	192.0.9.0/24	RIP	120	1	192.0.10.1	Campus Network.Router5	IF11	N/A	9.971
11	192.0.10.0/24	Direct	0	0	192.0.10.2	Campus Network.Router4	IF11	N/A	0.000
12	192.0.11.0/24	RIP	120	1	192.0.13.1	Campus Network.Router2	IF10	N/A	6.975
13	192.0.12.0/24	RIP	120	1	192.0.13.1	Campus Network.Router2	IF10	N/A	6.975
14	192.0.13.0/24	Direct	0	0	192.0.13.2	Campus Network.Router4	IF10	N/A	0.000
15	192.0.14.0/24	Direct	0	0	192.0.14.1	Campus Network.Router4	IF0	N/A	0.000
16	192.0.15.0/24	Direct	0	0	192.0.15.1	Campus Network.Router4	IF1	N/A	0.000
17									
18	Gateway of last resort is	not set							
19									

Figura 10. Tabla de enrutamiento (Router 4)

Trabajo en Clase:

1. Analizar las gráficas obtenidas que comparan el tráfico RIP sobre la red a partir de los dos escenarios propuestos.

2. Repita las simulaciones haciendo que el enlace que une al Router 1 y el Router 2 se dañe a los 100seg después de comenzar la simulación, y se recupere a los 500seg de simulación. Genere y analice las gráficas.

3. Dibuje el esquema de la red y a partir de la tabla de enrutamiento del Router 4 escriba las direcciones IP asociadas a cada router y subred.

4. Compare la tabla de enrutado del Router 1 en ambos escenarios, teniendo en cuenta la avería del enlace que une a éste con el Router 2.

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE INGENIERÍA Y ADMINISTRACIÓN
PROGRAMA DE INGENIERÍA ELECTRÓNICA
REDES DE COMPUTADORES (OPTATIVA)

ANEXO 2

GUÍA PRÁCTICA SOBRE PROTOCOLOS DE ENRUTAMIENTO EN LA RED

Práctica N°2

TÍTULO: OSPF (OPEN SHORTHEST PATH FIRST)

OBJETIVOS:

- Establecer los niveles jerárquicos (backbone y áreas) en la estructura de la red.
- Distribuir los pesos de los enlaces para obtener rutas alternativas, teniendo en cuenta las características del protocolo OSPF: ruta más corta, menor costo y disminución de flujo tráfico.
- Analizar la tabla de enrutamiento de los Routers para cada uno de los dos escenarios a analizar: con áreas y sin áreas.

1. MARCO TEÓRICO:

El protocolo del primer camino más corto disponible (OSPF, Open Shortest Path First) se usa de forma generalizada como protocolo de encaminador interior en redes TCP/IP. OSPF calcula una ruta a través de una interconexión de redes que supone el menor coste de acuerdo a una métrica de coste configurable por el usuario para que exprese una función del retardo, la velocidad de trasmisión, el coste económico u otros factores. Además, OSPF es capaz de equilibrar las

cargas entre múltiples caminos de igual coste.[41]

OSPF funciona dividiendo una Intranet o un sistema autónomo en unidades jerárquicas de menor tamaño. Cada una de estas áreas se enlaza a un área backbone mediante un router fronterizo. Todos los paquetes enviados desde una dirección de una estación de trabajo de un área a otra atraviesan el área backbone, independientemente de la existencia de una conexión directa entre las dos áreas. Aunque es posible el funcionamiento de una red OSPF únicamente con el área backbone (sin organización por áreas), OSPF escala bien cuando la red se subdivide en un número de áreas más pequeñas, ya que la definición de áreas reduce el gasto de procesamiento, acelera la convergencia, limita la inestabilidad de la red a un área y mejora el rendimiento.

OSPF es un protocolo de enrutamiento por estado de enlace en el cual, los routers OSPF envían Publicaciones del Estado de Enlace LSA (Link-State Advertisment) a todos los routers pertenecientes a la misma área jerárquica mediante una multidifusión de IP, estas LSA construyen tablas de enrutamiento basándose en una base de datos de la topología; esta base de datos se elabora a partir de paquetes de estado de enlace que se pasan entre todos los routers para describir el estado de una red. La LSA contiene información sobre las interfaces conectadas, la métrica utilizada y otros datos adicionales necesarios para calcular las bases de datos de la ruta y la topología de red.

Los routers OSPF acumulan información sobre el estado de enlace y ejecutan el algoritmo SPF (que también se conoce con el nombre de su creador, Dijkstra) para calcular la ruta más corta a cada nodo.

[41] STALLINGS, William. Comunicaciones y Redes de Computadores. Séptima edición; 2004. p. 651

2. PROCEDIMIENTO:

A continuación veremos en la figura 1 el diseño de la topología de red que emplearemos en la simulación, seguido de los pasos para desarrollar la práctica.

Elementos:

- **Router IP (slip8_gtwy):** El modelo representa un nodo slip8_gtwy, el cual opera como una puerta de enlace IP y contiene 8 interfaces de línea seriales a una velocidad seleccionable. Los paquetes IP que llegan a cualquier interfaz son enrutados a la interfaz de salida adecuada en función de su dirección IP de destino.

- **Ping Parameters:** Define diferentes opciones de configuración que sólo los routers/hosts pueden usar para determinar la conectividad al destino especificado garantizando que el nivel de red funciona adecuadamente. De esta forma *ping* confirma que un paquete IP es capaz de alcazar la máquina destino y que ese mismo paquete IP es capaz de volver a la máquina origen.

- **Link (PPP_DS3):** Enlace que utiliza el protocolo PPP y que tiene una capacidad de 44,736 Mbps.

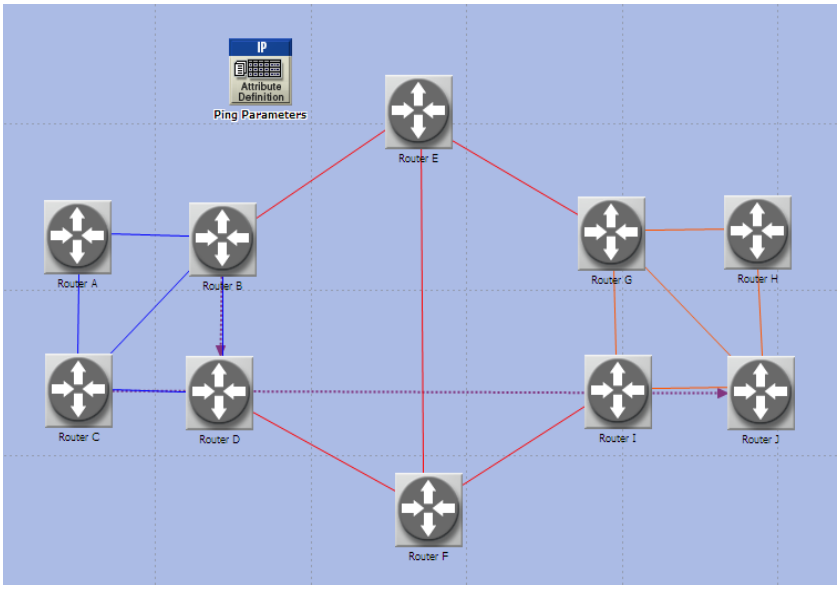


Figura 1. Arquitectura de la red utilizando el protocolo OSPF

2.1 Creación del proyecto:

I. Inicie el simulador Opnet Modeler, para la creación del nuevo proyecto elija en la barra de menú la opción **File** y seleccione **New** para crear el proyecto, luego dale Click en **Project** y por último **Ok**. Ahora dele nombre al proyecto, por ejemplo: *tu nombre_OSPF,* luego al escenario a crear dele el nombre *Sin_areas*, presione **Ok.** Aparecerá la ventana de *Startup Wizard,* haga Click en **Next** para elegir el área sobre el cual se desea crear la arquitectura de red, seleccione la opción **Campus** y presione **Next,** ahora para adecuar el tamaño de la red; coloca en el campo **x**=**100** y **y=100**. Finalmente dele **Next** dos veces y luego **Finish.**

2.2 Creación y configuración de la red:

I. Seguidamente aparecerá la paleta de dialogo (Object Pallete), el cual permitirá acceder a los elementos de trabajo para el diseño de la red, en caso de que no

aparezca pulse en la barra de menú el botón  .Al desplegarlo es necesario que la opción **internet tool_box** esté seleccionado.

II. En la paleta de diálogo seleccione el router **slip8_gtwy** y sitúe 10 de estos mismos en el espacio de trabajo presionando Click izquierdo (para terminar de colocar los objetos presione Click derecho). Utilice el enlace **PPP_DS3** para conectar los routers y renómbrelos como aparece en la figura 2, para esto debe dar Click derecho sobre el objeto y seleccione **Set Name.** En la figura 2 veremos la respectiva conexión.

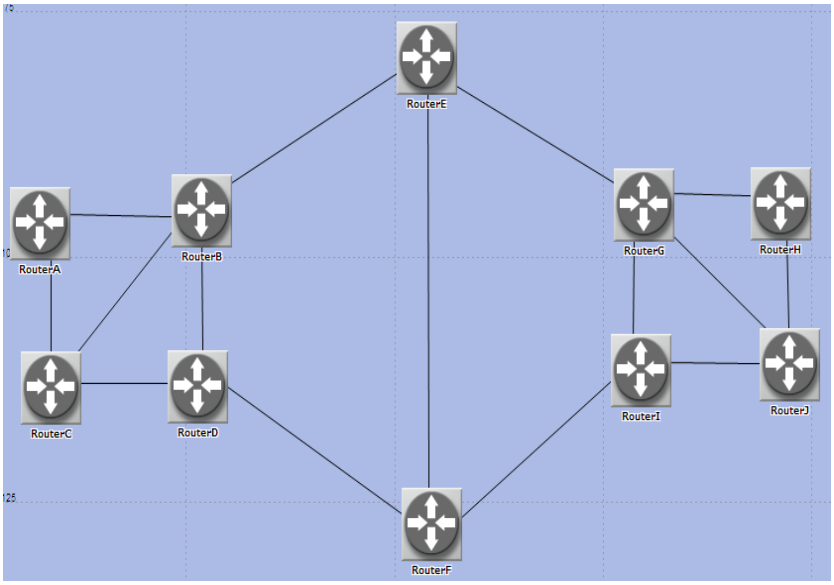


Figura 2. Conexión de los routers slip8_gtwy utilizando el enlace PPP_DS3.

III. Salve el proyecto y designe el protocolo de enrutamiento desplegando en la barra de menú la opción **Protocols**, seleccione **Routing** y luego **Configure Routing Protocols**. Ahora deshabilite el protocolo **RIP** y escoja el protocolo **OSPF**, presione **Ok**.

En la figura 3 se puede ver el procedimiento de configuración del protocolo de enrutamiento OSPF y en la figura 4 la visualización de este protocolo sobre los

enlaces de la red; habilitando la opción **Visualize routing domains** en la ventana **Routing Protocol Configuration**. Para quitar la visualización del uso del protocolo OSPF sobre los enlaces pulse *Ctrl+Shift+C*.

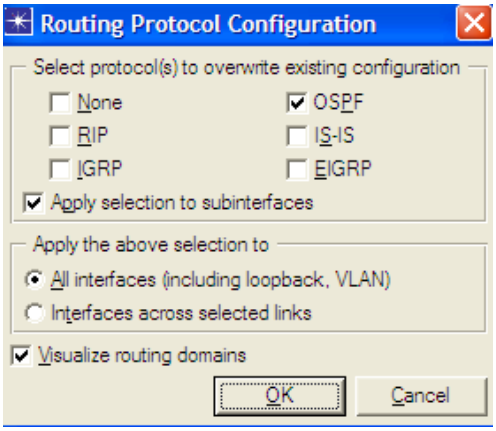


Figura 3. Configuración del protocolo de enrutamiento (OSPF)

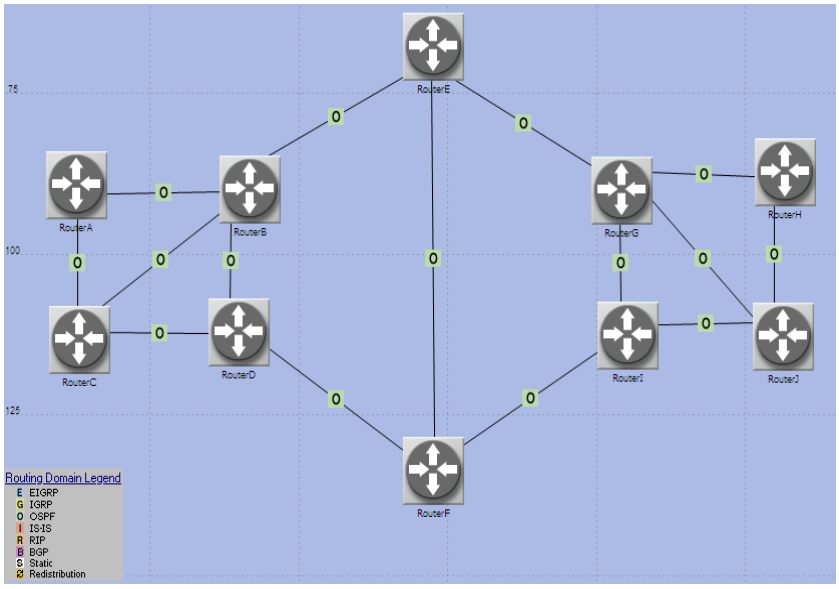


Figura 4. Visualización del protocolo OSPF utilizando la opción Routing Domain Legend

IV. Para asignar una única dirección IP a las interfaces IP conectadas; debe desplegar en la barra de menú la opción **Protocols**, seleccione **IP**, luego **Addressing** y por último haga Click en **Auto Assign IP Addresses**.

V. Al igual que muchos routers comerciales, los modelos de routers de OPNET aceptan un parámetro llamado *reference bandwith* para calcular el coste real, de esta manera:

Coste = (*Reference bandwith*)/(Ancho de banda del enlace)

Donde el valor por defecto de *Reference bandwith* es 1.000.000Kbps. Por ejemplo, para asignar un coste de 5 a un enlace, se le asigna un ancho de banda de 200000 Kbps. Hay que tener en cuenta que ese no es el ancho de banda real del enlace en el sentido de velocidad de transmisión, sino simplemente un parámetro que se utiliza para calcular costes. Ahora seleccione los enlaces indicados en la tabla 1, tabla 2 y tabla 3, asigne el respectivo *Bandwidth,* para esto debe desplegar en la barra de menú la opción **Protocols**, seleccione **IP**, luego haga Click en **Routing** y por último escoge **Configure Interface Metric Information**.

Enlace	Bandwidth (Kbps)
Router A - Router B	50000
Router B - Router D	50000
Router D - Router C	50000
Router C - Router A	50000
Router B- Router C	50000

Tabla 1. Coste de los enlaces para un valor de 20

Enlace	Bandwidth (Kbps)
Router B - Router E	200000
Router E - Router G	200000
Router I - Router F	200000
Router F - Router D	200000
Router E – Router F	200000

Tabla 2.Coste de los enlaces para un valor de 5

Enlace	Bandwidth (Kbps)
Router G - Router H	100000
Router H - Router J	100000
Router J - Router I	100000
Router I - Router G	100000
Router G- Router J	100000

Tabla 3. Costo de los enlaces para un valor de 10

VI. Una forma de visualizar y confirmar los valores establecidos sobre los enlaces es hacer que se muestren los valores de los pesos en la topología de red. Para ello despliegue en la barra de menú la opción **View**, seleccione **Visualize Protocol Configuration**, seleccione **IPv4 Interface Metrics** y por último dele Click sobre **OSPF Metrics**, de esta manera aparecerá como se ve en la figura 5 el valor asignado a cada enlace.

Para quitar la visualización del coste sobre los enlaces pulse *Ctrl+Shift+C*.

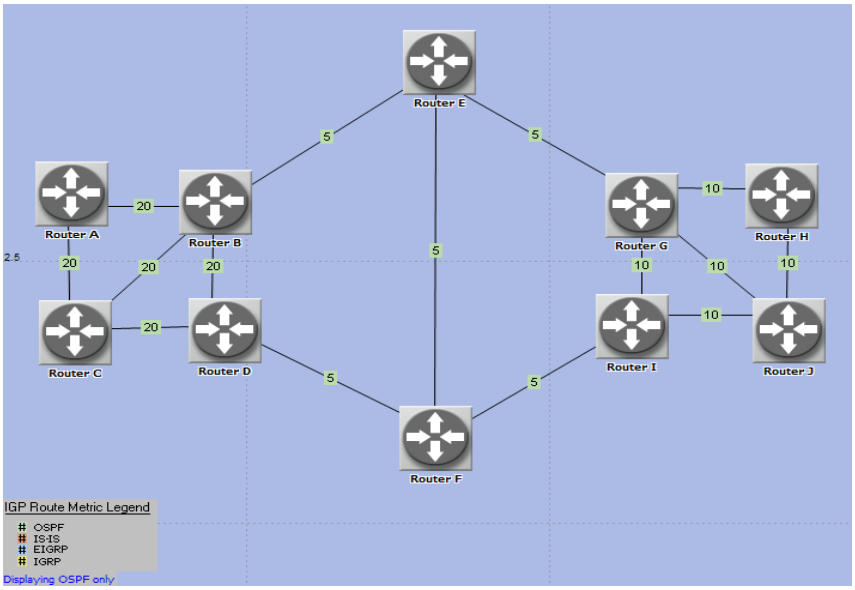


Figura 6. Valores asignados sobre los enlaces

VII. Ahora para crear la demanda de tráfico seleccione los **Routers B** y **D**, presionando Shift y dando Click sobre ellos. Luego, en la barra de menú despliegue la opción **Protocols**, seleccione **IP**, seguidamente **Demands** y por último **Configure Ping Traffic on Selected Nodes**. Aparecerá una ventana para seleccionar el origen y destino de la demanda de tráfico, seleccione **From B** y dale **Ok**. Salve el proyecto.

En la figura 6 se puede ver el procedimiento de configuración de la demanda de tráfico y en la figura 7 la visualización de este mismo entre los routers; además la representación del objeto **Ping Parameters** en el área de trabajo.

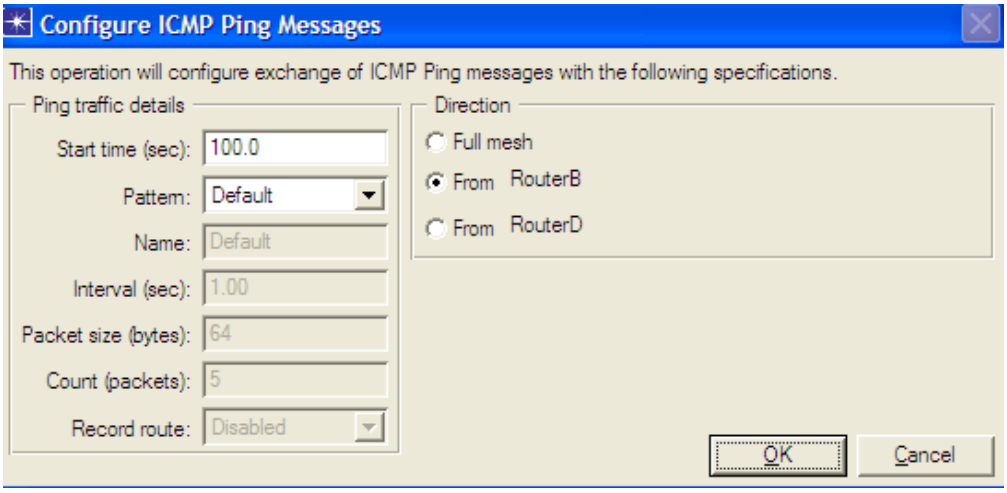


Figura 6. Configuración de la demanda de tráfico

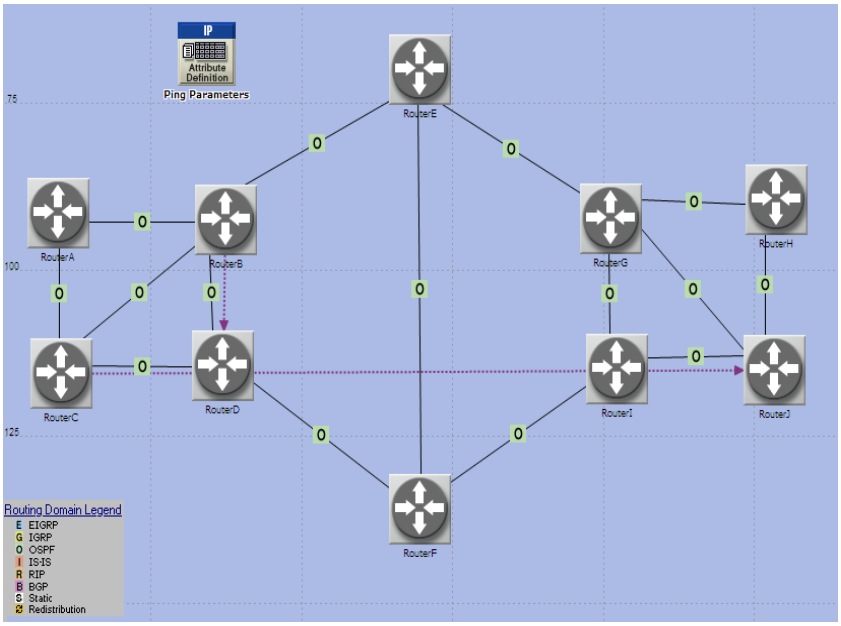


Figura 7. Representación de la demanda de tráfico entre los Routers B – D y los Routers C - J

2.3 Creación de un nuevo escenario (Ruta_alternativa):

I. En la barra de menú despliegue **Scenarios** y seleccione **Duplicate Scenario** (llámelo **Ruta_alternativa**), dale Ok.

Seleccione los enlaces que aparecen a continuación en la Tabla 4, para dividir la jerarquía de la red en áreas e identificarlas.

Enlace
Router A - Router B
Router B - Router D
Router D - Router C
Router C - Router A
Router B- Router C

Tabla 4. Representación del área 0.0.0.1

II. Ahora despliegue en la barra de menú la opción **Protocols**, seleccione **OSPF** y por último **Configure Areas**. Aparecerá una ventana y en el campo de **Area identifier** escriba **0.0.0.1**.

III. Seleccione los siguientes enlaces que aparecen en la Tabla 5, repita el paso 2 y escriba en el parámetro **Area identifier** el valor **0.0.0.0** (backbone).

Enlace
Router B - Router E
Router E - Router G
Router I - Router F
Router F - Router D
Router E – Router F

Tabla 5. Representación del área 0.0.0.0

IV. Seleccione los siguientes enlaces que aparecen en la Tabla 6, repite el paso 2 y escribe en Area identifier 0.0.0.2.

Enlace
Router G - Router H
Router H - Router J
Router J - Router I
Router I - Router G
Router G- Router J

Tabla 6. Representación del área 0.0.0.2

V. Para observar las respectivas áreas despliegue **View** en la barra de menú, seleccione **Vizualize Protocol Configuration**, luego haga Click sobre **OSPF** y finalmente seleccione la opción **Area Configuration**. Aparecerá una ventana con las respectivas áreas y su identificación; puede asignarle un color a cada área para distinguirlas. En la figura 8 se puede ver la asignación del color para cada área.

Si desea quitar la visualización de la división de áreas *Ctrl+Shift+C*.

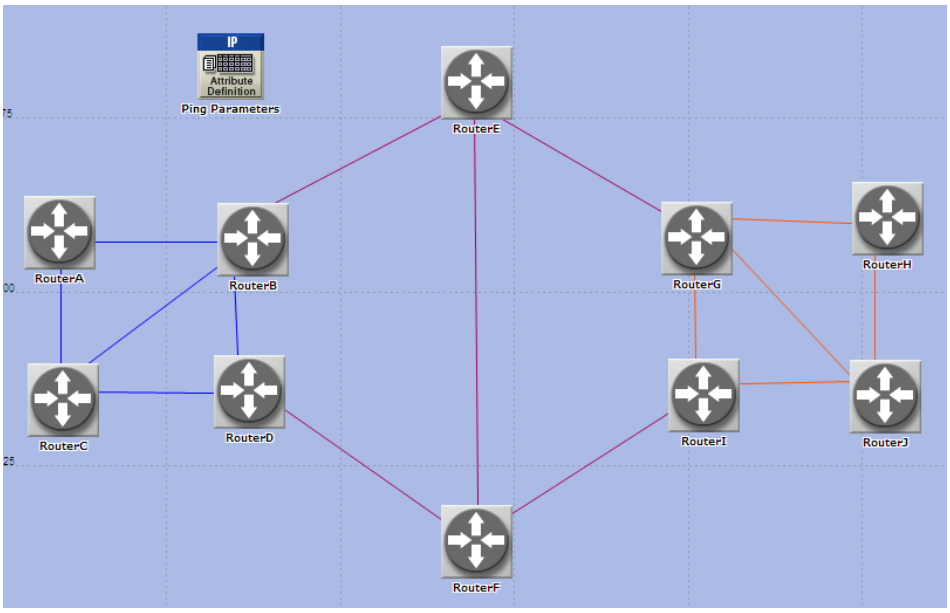


Figura 8. Asignación de áreas e identificación de estas mismas basadas en el color de los enlaces.

VI. Ahora, es necesario asignar nuevos costes a los enlaces para obtener una ruta alternativa teniendo en cuenta el tráfico establecido entre los **Routers B-D** y **Routers C-J**, y también se analizará el ancho de banda.

VII. Seleccione los enlaces indicados en la tabla 7 y asigne el respectivo *Bandwidth,* para esto debe desplegar en la barra de menú la opción **Protocols**, seleccione **IP**, luego dale Click en **Routing** y por último escoja **Configure Interface Metric Information**. En la figura 9 se puede apreciar la respectiva asignación de los valores sobre los enlaces.

Enlace	Bandwidth (Kbps)
Router C - Router D	200000
Router E - Router F	200000
Router G - Router J	200000
Router H - Router J	200000
Router A - Router B	100000
Router B - Router C	100000
Router D - Router F	100000
Router E - Router G	100000
Router G - Router I	100000
Router A - Router C	50000
Router F - Router I	50000
Router G - Router H	50000
Router B - Router E	25000
Router I - Router J	25000
Router B - Router D	10000

Tabla 7. Costo de los enlaces

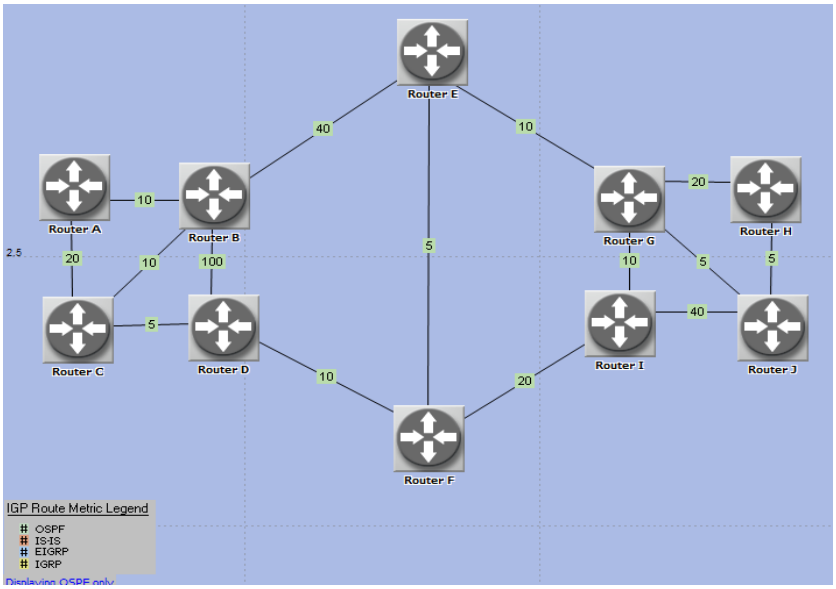


Figura 9. Valores asignados sobre los enlaces

2.4 Ejecutar la simulación y ver los resultados:

I. Despliegue el menú **Scenarios** y seleccione **Manage Scenarios**, luego en el campo de **results** cambie la opción para cada escenario por **collect** o **recollect**. Ahora para establecer el tiempo de la simulación; en el campo **Sim Duration** escriba 10 y en **Time Units** escoja **min**, dale **Ok**. Al finalizar presione **Close** y salve el proyecto.

II. En la barra de menú despliegue **Scenarios**, seleccione **Switch to scenario** y escoge **Sin_ Areas**.

III. A continuación, se debe generar la carga de tráfico. Para esto se generaran flujos entre todos los nodos. Despliegue en la barra de menú la opción **Traffic**, seleccione **Create Traffic Flows,** luego **IP** y por último **Unicast Full mesh between all nodes**, presione **Create**. Corra de nuevo el programa, ahora despliegue de nuevo la opción **Traffic** y seleccione **Open Traffic Center** para

ver el flujo de tráfico. Aparecerá la ventana de **Traffic center** y habilite la carpeta **Flow.** En la figura 10 se puede ver la configuración de la creación del tráfico y en la figura 11 la visualización de las posibles rutas de tráfico entre los routers.

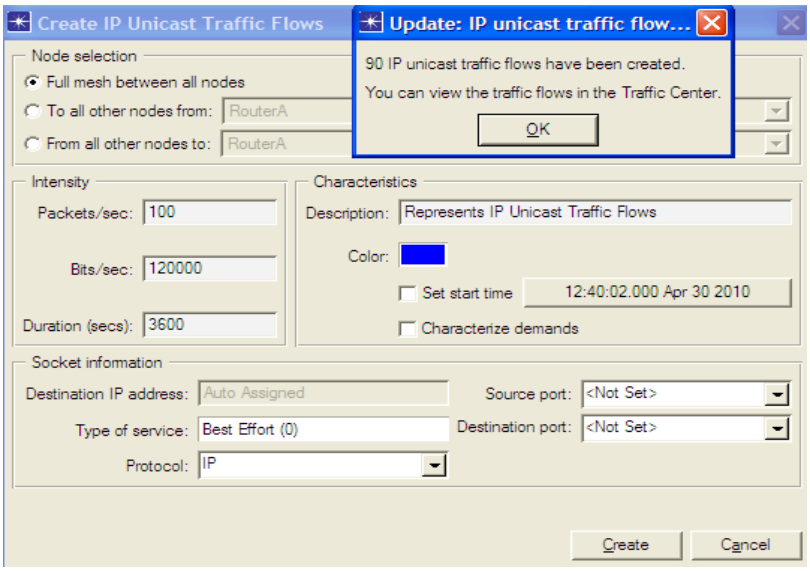


Figura 10. Creación del flujo de tráfico

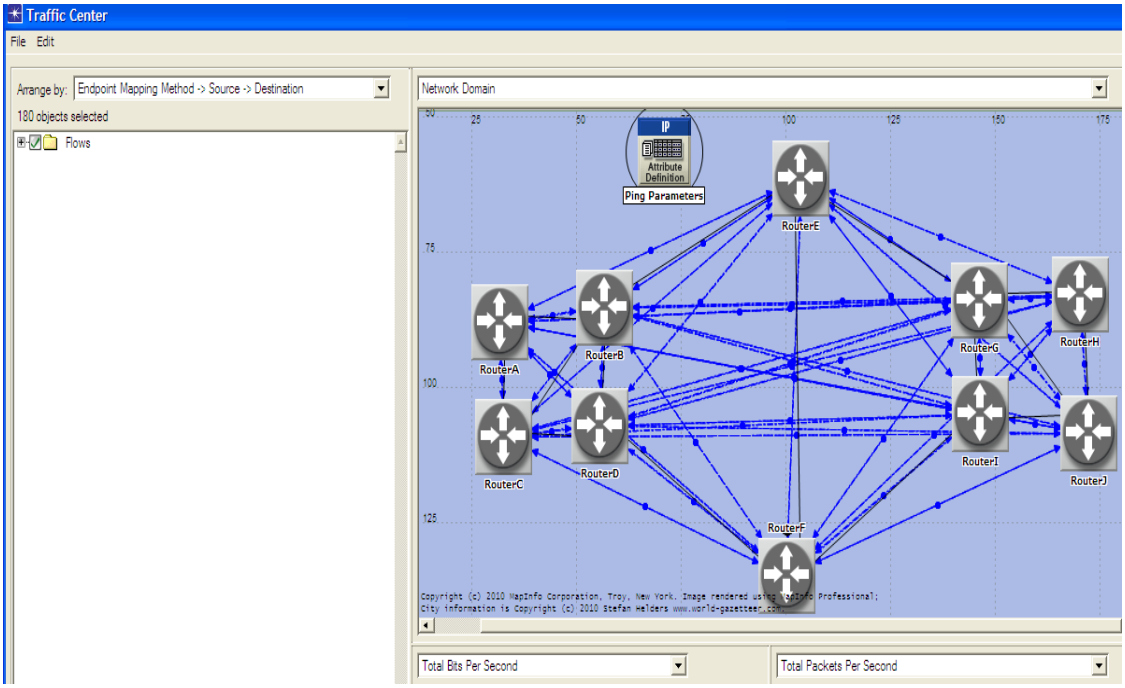


Figura 11. Visualización del tráfico

IV. Cierre la ventana de **Traffic center** y en la barra de menú despliegue la opción **Protocols**, seleccione **IP**, escoja **Demands** y ahora **Display Routes for Configure Demands** (aparecerá la ventana **Route Report for IP Traffic Flows**), ahora despliegue la opción **Router B** y ahí mismo seleccione **Router D**. Para ver el flujo de tráfico del escenario **Sin _Areas** cambie el campo de **Display** por **Yes.**

V. Para ver la ruta alternativa teniendo en cuenta el tráfico entre los **Routers C – J**, deshabilite la opción anterior de **Display** por **No**, y ahora despliegue la opción **Router C** y ahí mismo seleccione **Router J**.

En la figura 12 se puede ver el procedimiento de configuración para ver el reporte de ruta del flujo de tráfico IP y en las figura 13 y 14 la visualización de este mismo teniendo en cuenta las características del protocolo OSPF.

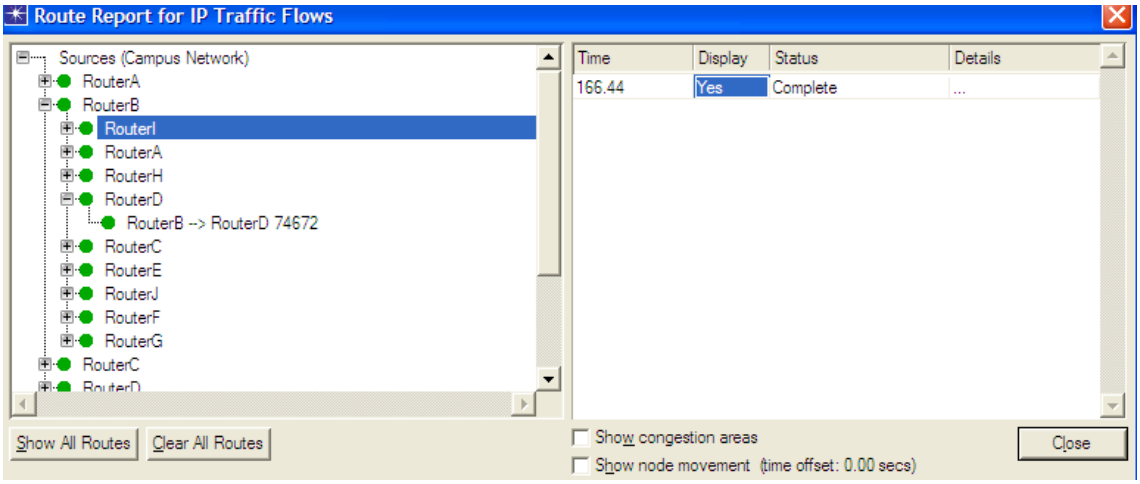


Figura 12. Configuración del Reporte de ruta para el flujo de tráfico IP

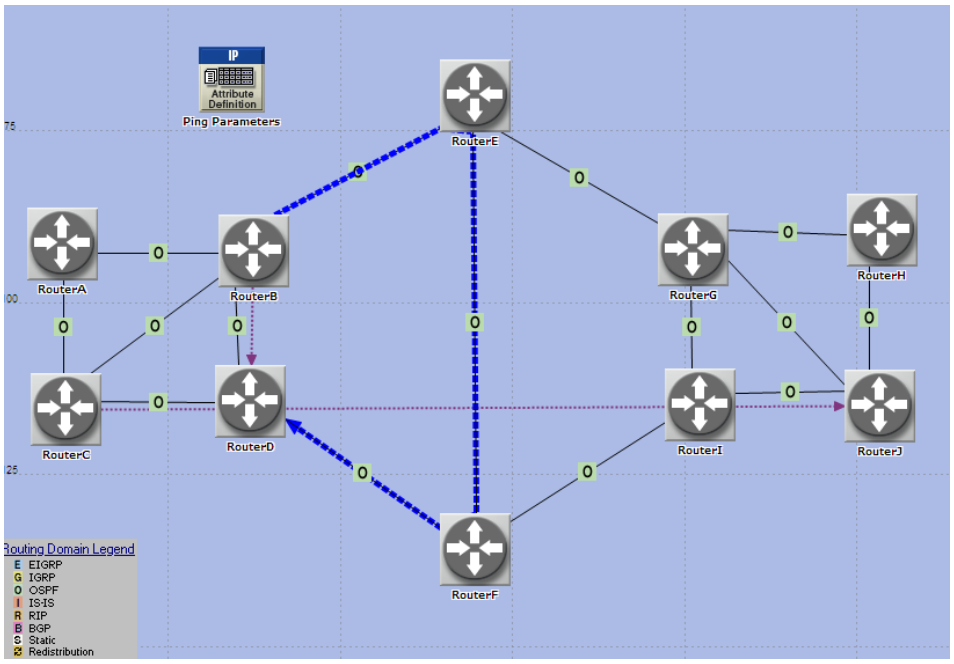


Figura 13. Ruta basada en las características del protocolo OSPF (tráfico entre los Routers B – D)

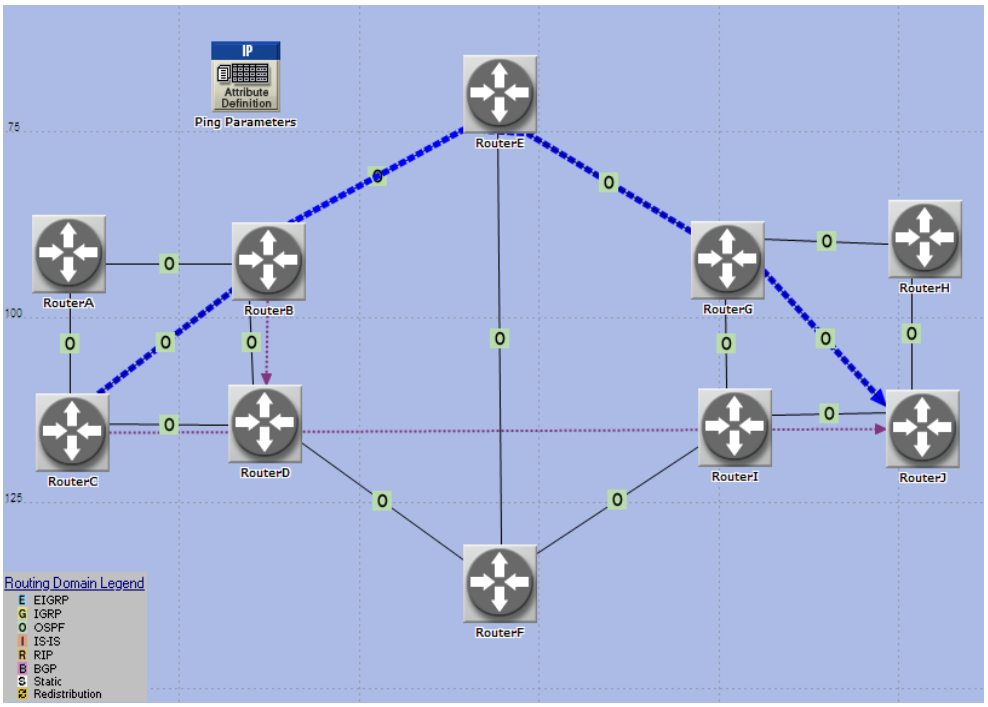


Figura 14. Ruta basada en las características del protocolo OSPF (tráfico entre los Routers C – J)

VI. A continuación en la barra de menú despliegue **Scenarios**, seleccione **Switch to scenario** y escoge **Ruta_alternativa**.

VII. Genere de nuevo la demanda de tráfico y corra el programa, seleccione **Open Traffic Center** para ver el flujo de tráfico. Aparecerá la ventana de **Traffic center** y habilite la carpeta **Flow**, cierre la ventana y en la barra de menú despliegue la opción **Protocols**, seleccione **IP**, escoja **Demands** y ahora **Display Routes for Configure Demands** (aparecerá la ventana **Route Report for IP Traffic Flows**), ahora despliegue la opción **Router C** y ahí mismo seleccione **Router J**. Para ver el flujo de tráfico del escenario **Ruta_alternativa** cambie el campo de **Display** por **Yes.**

En la figura 15 y 16 se pueden apreciar las rutas alternativas para la demanda de tráfico basado en las características del protocolo OSPF.

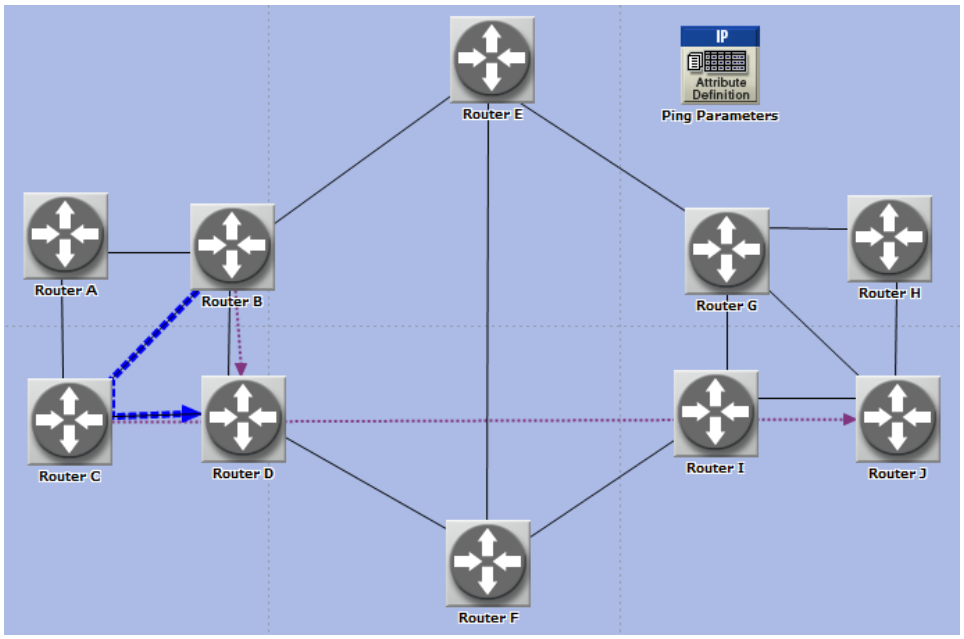


Figura 15. Ruta alternativa para la demanda de tráfico entre los Routers B-D

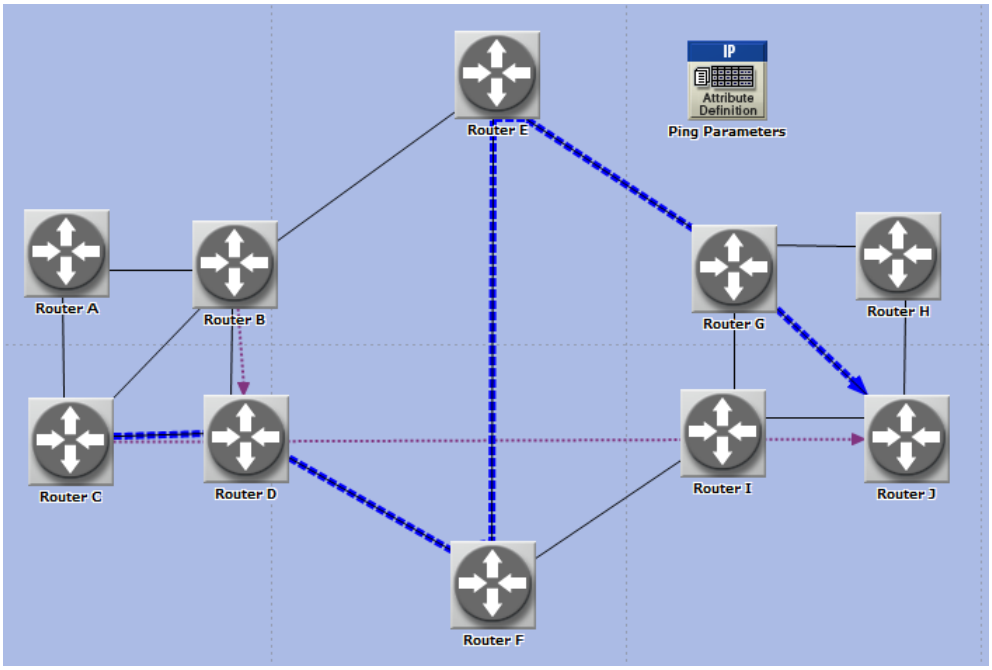


Figura 16. Ruta alternativa para la demanda de tráfico entre los Routers C-J

VIII. Ahora, una forma de visualizar el ancho de banda es utilizando la opción *throughput*. Presione Click derecho sobre el espacio de trabajo y escoja **Choose Individual DES Statistics**, aparecerá la ventana de *Choose Results* y seleccione **Link Statistics**, escoja **Point to Point** y por último **throughput (bits/sec)**.Para realizar un análisis del tráfico sobre los nodos teniendo en cuenta el ancho de banda utilizado sobre los enlaces, seleccione en la misma ventana de *Choose Results* la opción **Demand Statistics** y luego escoge **Traffic Received (bits/sec).**

IX. Corra de nuevo el programa y seleccione el escenario *Ruta_alternativa,* luego despliegue en la barra de menú la opción **DES**, escoja **Results** y por último dale Click en **Compare Results.** De esta manera aparecerá la ventana de *Results Browser*, cerciórese que esté seleccionado el escenario *Ruta_alternativa* y en la opción de *Campus Network* habilite los enlaces entre los Routers C-D y Routers

B-C, tanto para el tráfico recibido como para el ancho de banda. En la figura 17 se puede apreciar las gráficas correspondientes.

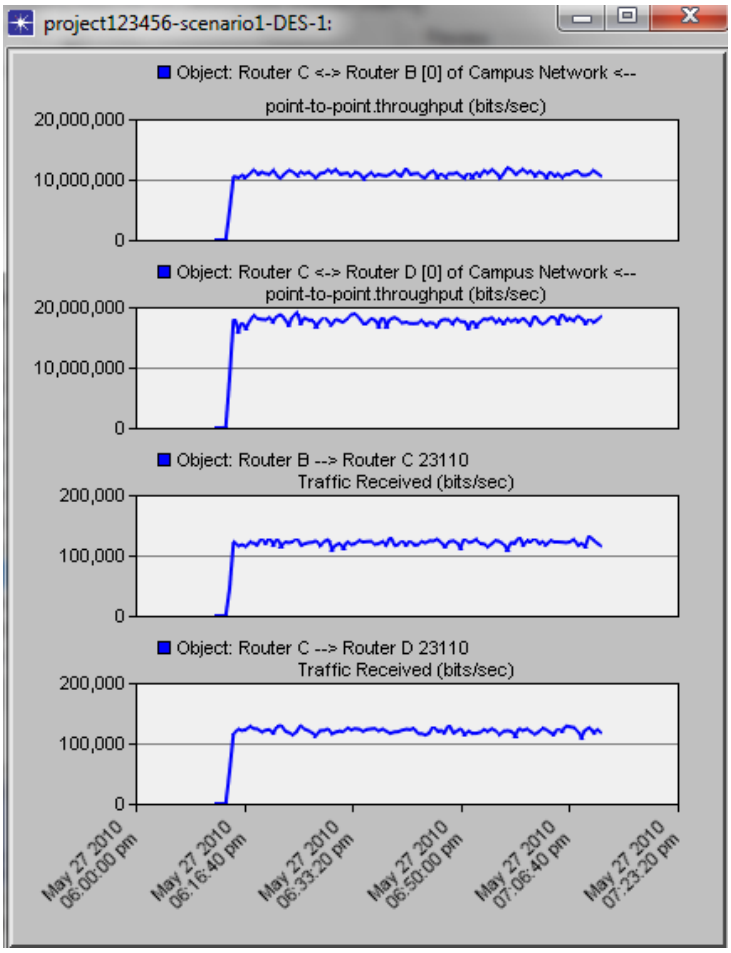


Figura 17. Representación del ancho de banda y tráfico recibido entre los Routers C- D y Routers B - C

Trabajo en Clase:

1. Basado en las características del protocolo OSPF, explique por qué en los escenarios Sin_ Areas y Ruta_alternativa se obtienen rutas diferentes.

2. Realice un análisis completo de las gráficas obtenidas en el escenario Ruta alternativa (representación del ancho de banda y el tráfico recibido sobre los enlaces entre los Routers B - C y Routers C - D), teniendo en cuenta la demanda de tráfico.

3. Exporte la tabla de enrutado del Router B para cada uno de los escenarios y explique los valores asignados en la columna *Metric* de cada ruta.

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE INGENIERÍA Y ADMINISTRACIÓN
PROGRAMA DE INGENIERÍA ELECTRÓNICA
REDES DE COMPUTADORES (OPTATIVA)

ANEXO 3

GUÍA PRÁCTICA SOBRE PROTOCOLOS DE ENRUTAMIENTO EN LA RED

Práctica N°3

TÍTULO: IS-IS (INTERMEDIATE SYSTEM TO INTERMEDIATE SYSTEM)

OBJETIVOS:

- Implementar y configurar una red basada en las características del protocolo de enrutamiento IS-IS.
- Establecer los tipos de sistemas (L1, L2, L1/L2) de cada router en su respectiva área.
- Garantizar el balanceo de carga a través de los enlaces, dependiendo de la ruta de la demanda de tráfico.
- Analizar las tablas de enrutamiento y la forma de visualización del ancho de banda con la opción *throughput* a partir de las gráficas obtenidas.

1. MARCO TEÓRICO:

IS-IS es un protocolo de enrutamiento de estado de enlace creado por ISO. Para intercambiar información, los routers IS-IS calculan el costo de la ruta basados en una sola métrica. El protocolo de enrutamiento IS-IS es muy similar a OSPF. IS-IS está designado para proveer enrutamiento intradominio o enrutamiento dentro de

un área. Una red IS-IS está compuesta por sistemas finales, sistemas intermedios, áreas y dominios. En una red IS-IS, los routers son sistemas intermedios organizados en grupos locales llamados áreas. Muchas áreas son agrupadas juntas para formar dominios. Los dispositivos usuarios son sistemas finales. IS-IS y OSPF son protocolos de enrutamiento de estado de enlace que pueden ser usados para grandes redes. IS-IS utiliza el algoritmo Dijkstra para determinar el camino más corto y utiliza una base de datos del estado de enlace para enrutar los paquetes entre los sistemas intermedios. Una característica importante del computo del enrutamiento para ambos protocolos (OSPF e IS-IS) es la opción de múltiples caminos de igual costo; de esta manera, si dos rutas tienen el mismo camino de más bajo costo, el enlace de salida (siguiente hop) para ambos puede ser llamado en la tabla de enrutamiento y así la demanda de tráfico pueda ser divido, garantizando el balanceo de carga a través de múltiples rutas.

IS-IS usualmente utiliza dos niveles de jerarquía de enrutamiento en el cual, un router de nivel 1 puede identificar la topología del área incluyendo cada router y cada host. Sin embargo, un router de nivel 1 no puede saber la identidad de los routers fuera de su área. Los routers de nivel 1 son similares a los routers OSPF de área interna desde que no tenga conexión al exterior. Los routers de nivel 2 no son requeridos para identificar la topología dentro del área de nivel 1 pero hay una posibilidad de que un router de nivel 2 pueda ser un router de nivel 1 en una sola área. Nivel 2 para IS-IS es similar al área 0 de OSPF que comprende el área de backbone a fin de conectar diferentes áreas.

En la figura 1 se puede apreciar la distribución de áreas para una red IS-IS.

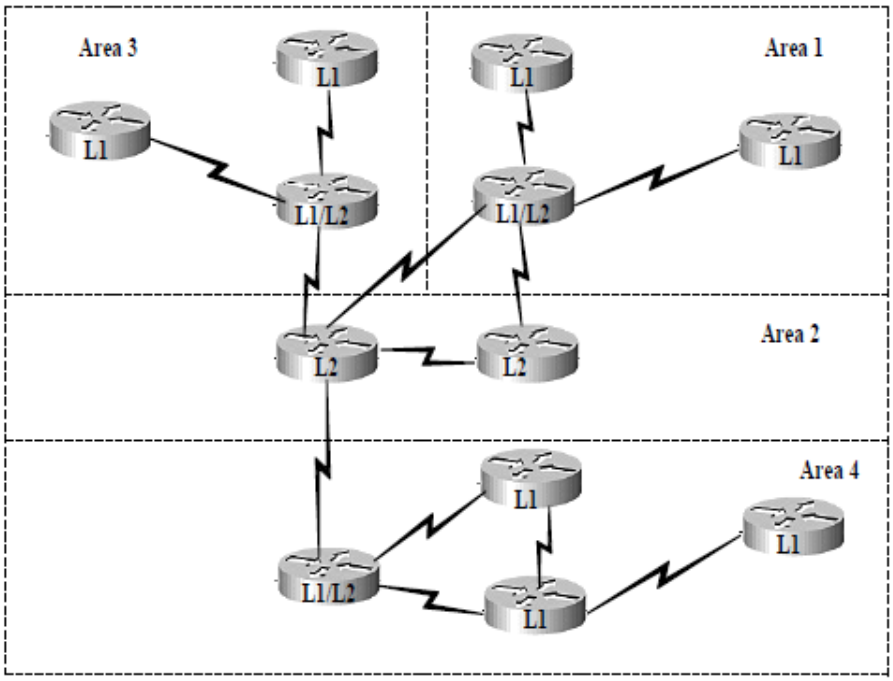


Figura 1. Distribución de Áreas (IS-IS)

Tipos de Sistemas

Router Nivel 1: Un router de configuración L1 sólo identifica los routers de su propia área y tiene vecinos de configuración L1 o L1/L2 en su área. Este incluye una base de datos del estado de enlace L1 con toda la información de enrutamiento del área interna. Para enviar paquetes fuera de su área, el router L1 utiliza el router L2 más cercano disponible en su área.

Router Nivel 2: Los routers de configuración L2 pueden incluir vecinos en la misma o diferente área y consiste de una base de datos del estado de enlace L2 con información para enrutamiento de área interna. Un router L2 sólo puede identificar otras áreas pero no tiene información de L1.

Router Nivel L1/L2: Un router de configuración L1/L2 puede incluir vecinos en cualquier área y consta de las siguientes dos bases de datos de estado de enlace.

- Una base de datos de estado de enlace L1 para entutamiento área interna.
- Una base de datos de estado de enlace L2 para entutamiento área externa

Un router L1/L2 ejecuta dos SPFs lo cual requiere más memoria y procesamiento.

La estructura del protocolo IS-IS cuenta con una configuración importante para el área máxima de direcciones, el cual es el número de áreas de direcciones permitidas e IS-IS tiene dos clases de direcciones:

- **Network Service Access Point (NSAP):** Las direcciones NSAP descubren los servicios de la capa de red.
- **Network Entity Title (NET):** Las direcciones NET descubren entidades de capa de red o procesos en lugar de servicios.
- Existe la posibilidad de que un dispositivo tenga más de un tipo de dirección, NET´s y el sistema de identificación por parte de NSAP debe ser único para cada sistema.[42]

2. PROCEDIMIENTO:

A continuación veremos en la figura 2 el diseño de la topología de red que emplearemos en la simulación, seguido de los pasos para desarrollar la práctica.

[42] SHEWANDAGN, Esuendale y ATHAR Syed. Performance Comparison of EIGRP/ IS-IS and OSPF/ IS-IS. pdf. Blekinge Institute of Technology. 2009

Elementos:

- **Router IP (Ethernet2_slip8_gtwy):** El modelo representa un nodo ethernet2_slip8_gtwy, el cual opera como una puerta de enlace IP y contiene dos interfaces Ethernet, también contiene ocho interfaces de línea seriales a una velocidad seleccionable. Los paquetes IP que llegan a cualquier interfaz se enrutan a la interfaz de salida adecuada en función de su dirección IP de destino.

- **IP traffic flow:** Representa el flujo de tráfico sobre la capa IP entre el origen y destino especificado

- **Link (PPP_SONET_OC12):** Enlace que utiliza el protocolo PPP y que tiene una capacidad de 594.43 Mbps.

- **NET:** Es un tipo de dirección de red definido por la arquitectura de red ISO. El identificador NET es utilizado en redes basadas en CLNS para identificar la capa de red de un sistema sin asociar a este sistema con una entidad de capa de transporte específico (como lo hace una dirección NSAP).NETs son útiles para direccionar sistemas intermedios (ISs), tales como routers que no interactúan con la capa de transporte. Un IS puede tener un solo NET o múltiples NETs, si participa en múltiples áreas o dominios.

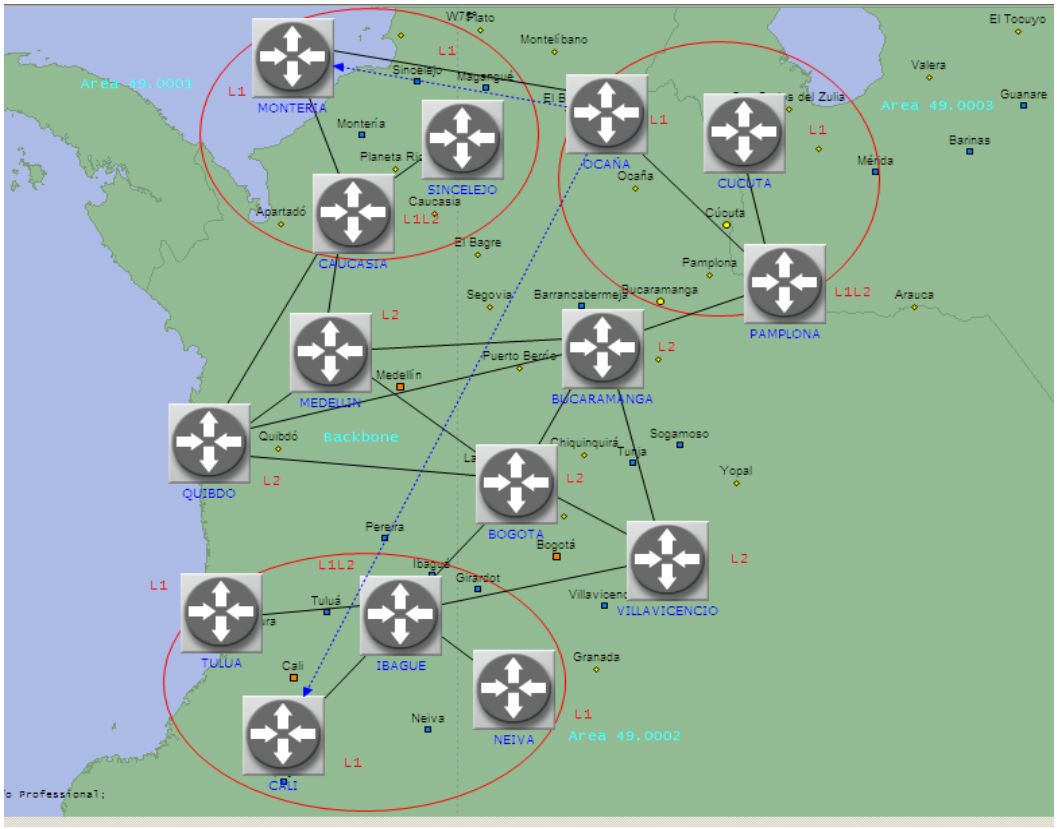


Figura 2. Arquitectura de la red utilizando el protocolo IS-IS

2.1 Creación del proyecto:

I. Inicie el simulador Opnet Modeler, para la creación del nuevo proyecto elija en la barra de menú la opción **File** y seleccione **New** para crear el proyecto, luego haga Click en **Project** y por último **Ok**. Ahora dele nombre al proyecto, por ejemplo: *tu nombre_ISIS,* luego al escenario a crear dele el nombre *Sin_jerarquia*, presione **Ok.** Aparecerá la ventana de *Startup Wizard,* haga Click en **Next** para elegir el área sobre el cual se desea crear la arquitectura de red, seleccione la opción **World** y presione 2 veces **Next** y luego **Finish.**

2.2 Creación y configuración de la red:

I. Seguidamente aparecerá la paleta de dialogo (Object Pallete), el cual permitirá acceder a los elementos de trabajo para el diseño de la red, en caso de que no aparezca pulse en la barra de menú el botón  .Al desplegarlo es necesario que la opción **internet tool_box** esté seleccionado.

II. En la paleta de dialogo seleccione el router **ethernet2_slip8_gtwy** y sitúe 15 de estos mismos en el espacio de trabajo presionando Click izquierdo (para terminar de colocar los objetos presione Click derecho). Ubique estos objetos en el mapa de Colombia de forma similar como aparece en la figura 3 y a cada router asígnele el nombre de la ciudad en la cual se encuentra ubicado, para esto debe presionar Click derecho sobre el objeto y seleccione **Set Name**. Renombre cada objeto como aparece en la figura 3. (Para agrandar el mapa de Colombia sitúese sobre el territorio y seleccione en la barra de menú la lupa )

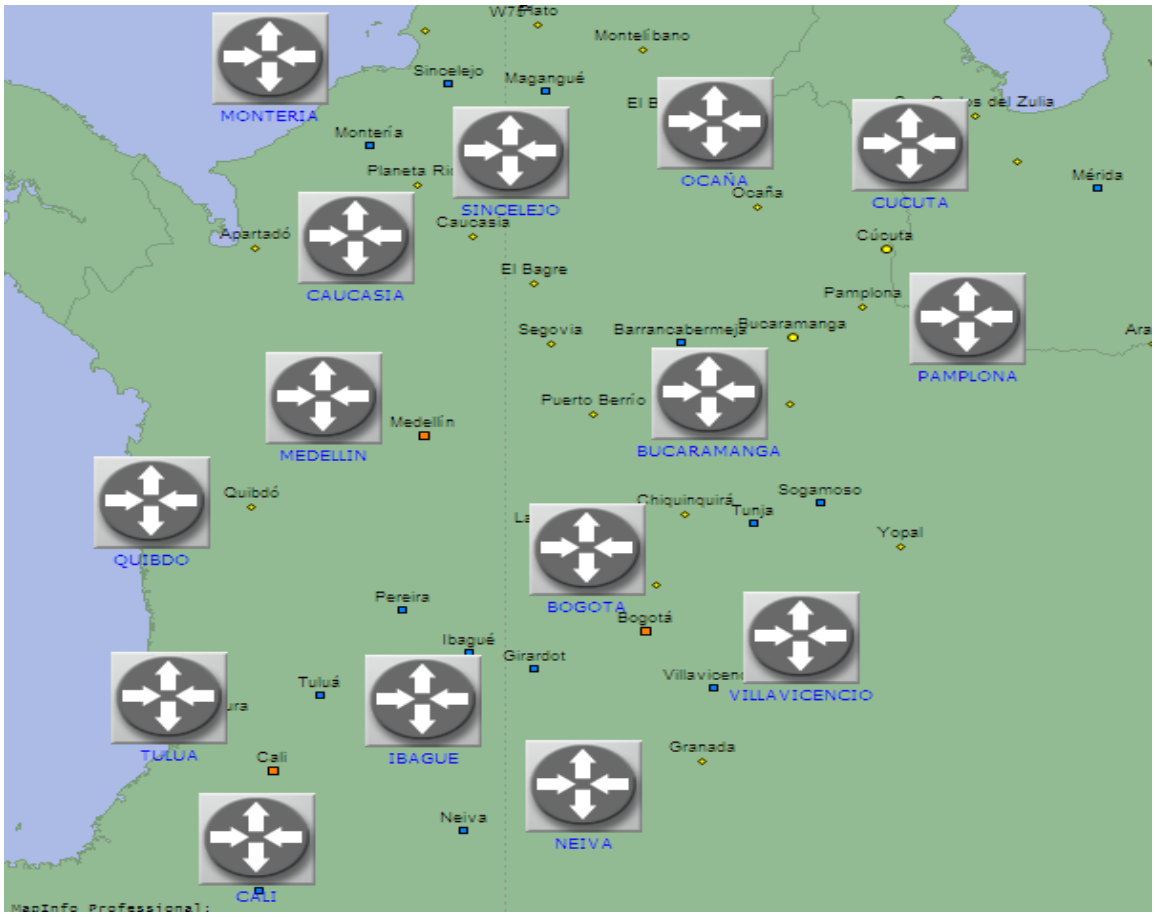


Figura 3. Ubicación y renombramiento de los routers

III. Ahora, despliegue en la paleta de dialogo la opción **Links** y seleccione el enlace **PPP_SONET_OC12** para interconectar los routers tal cual como aparece en la figura 4.

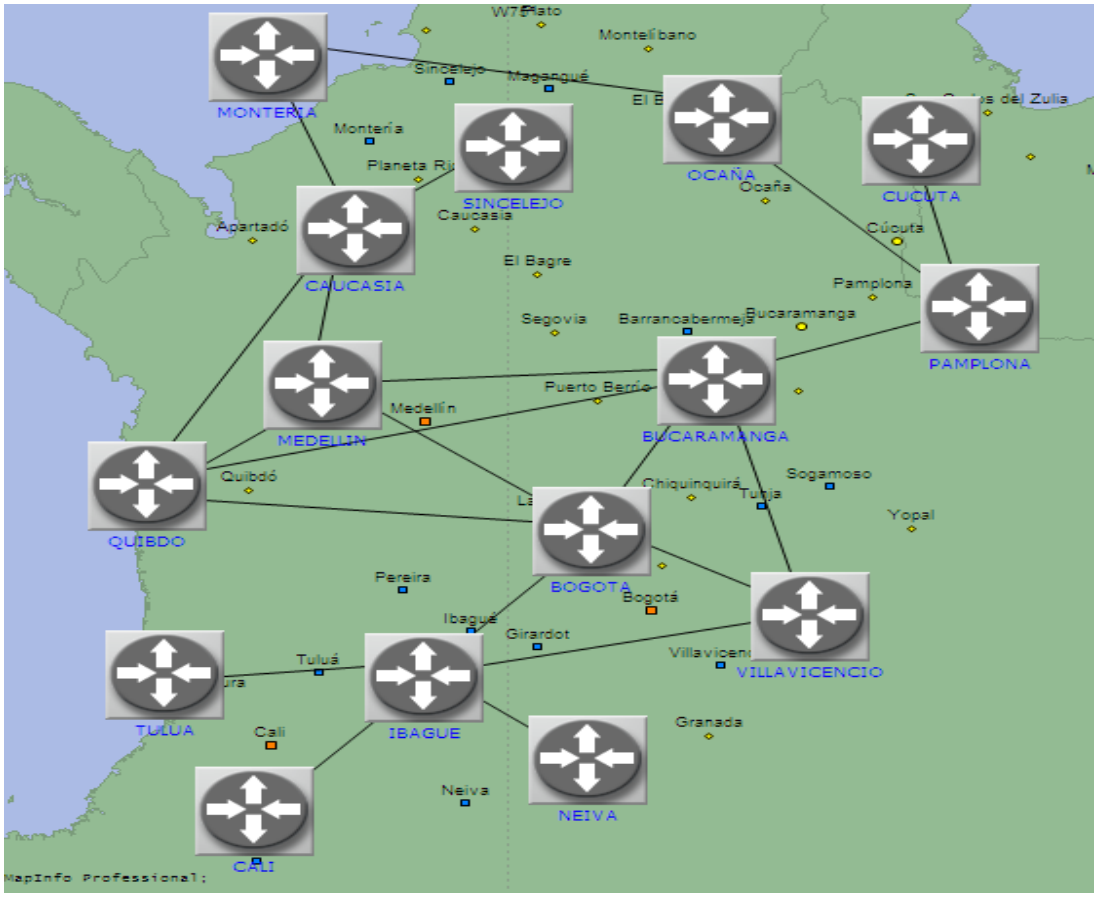


Figura 4. Interconexión de routers utilizando el enlace PPP_SONET_OC12

IV. Para habilitar IS-IS sobre los routers y que haya intercambio de información de enrutamiento con otros routers IS-IS habilitados, se debe realizar los siguientes dos pasos:

- Configurar **Network Entity Title:**

  Especifica uno o más identificadores del router. Cada router debe tener al menos una entidad de red especificada (NET). Un router puede tener múltiples NETs, pero cada NET debe ser único dentro de la red. Un identificador NET válido consiste de un Area ID, un System ID, y un N-Selector (N-Sel). Cada carácter de un NET representa un digito hexagesimal (el cual representa medio byte). El N-Sel es opcional, un 1 byte, y debe ser siempre cero (00). La longitud

de System ID es como se especifica en la configuración de procces. Todos los caracteres precediendo del System ID representan el Area ID. El Area ID puede ser de 1 a 13 bytes.

En la figura 5 se aprecia la representación de un NET

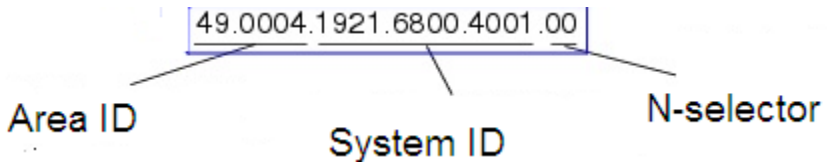


Figura 5. Representación de un NET

- Habilitar IS-IS para el enrutamiento IP sobre las interfaces.

V. Seleccione el respectivo router y presione Click derecho, escoja **Edit Atributes** y despliegue en cadena: **IP Routing Protocols**, luego **IS-IS Parameters**, seguidamente **Processes**, seleccione el número **1**, dele Click sobre **Processes Parameters** y por último **Network Entity Title**. En la tabla 1 aparecerá el identificador (NET) de cada router y en la figura 6 el procedimiento del paso 5. (Verifique que en la opción **Processes Parameters** la configuración de System Type para cada router es Level-1-2).

Router	**NET**	**System Type**
Montería	**49.0001.1920.0004.5001.00**	**Level -1-2**
Sincelejo	**49.0001.1920.0004.4001.00**	**Level -1-2**
Caucásea	**49.0001.1920.0004.6001.00**	**Level -1-2**
Tuluá	**49.0001.1920.0004.9001.00**	**Level -1-2**
Cali	**49.0001.1920.0007.0001.00**	**Level -1-2**

Neiva	**49.0001.1920.0004.8001.00**	**Level -1-2**
Ibagué	**49.0001.1920.0005.0001.00**	**Level -1-2**
Ocaña	**49.0001.1920.0004.1001.00**	**Level -1-2**
Cúcuta	**49.0001.1920.0003.3001.00**	**Level -1-2**
Pamplona	**49.0001.1920.0004.2001.00**	**Level -1-2**
Medellín	**49.0001.1920.0003.2001.00**	**Level -1-2**
Quibdó	**49.0001.1920.0004.3001.00**	**Level -1-2**
Bogotá	**49.0001.1920.0003.4001.00**	**Level -1-2**
Bucaramanga	**49.0001.1920.0003.1001.00**	**Level -1-2**
Villavicencio	**49.0001.1920.0003.0001.00**	**Level -1-2**

Tabla 1. Identificador (NET) y System Type de cada router

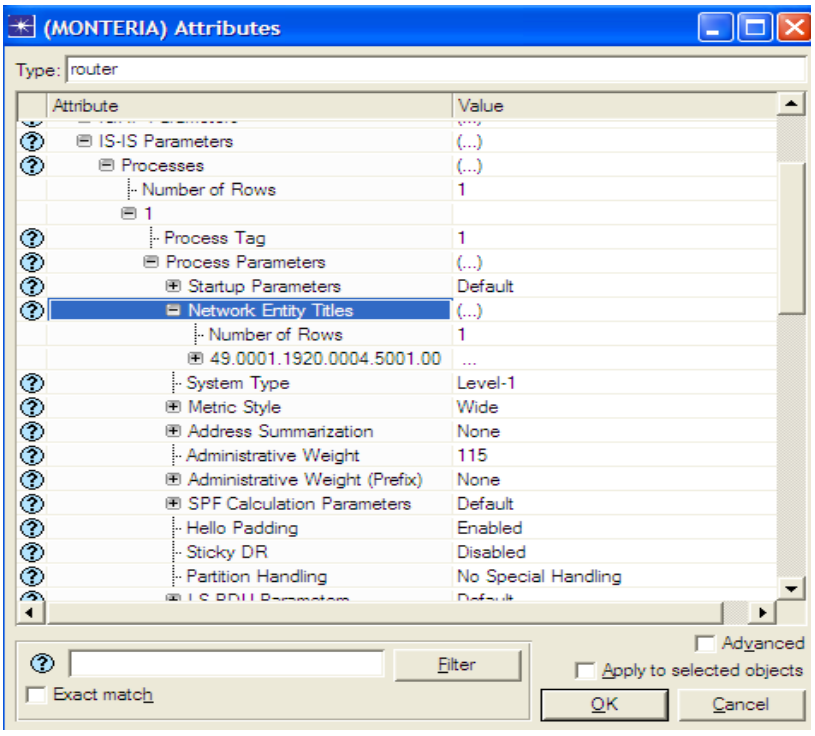


Figura 6. Configuración del respectivo identificador (NET) y System Type

VI. Es necesario asignar las direcciones IP para todas las interfaces, despliegue en la barra de menú la opción **Protocols**, seleccione **IP**, luego escoja **Addressing** y por último dele Click en **Auto Assign IP Addresses**. En la figura 7 se puede apreciar la configuración automática de las direcciones IP.

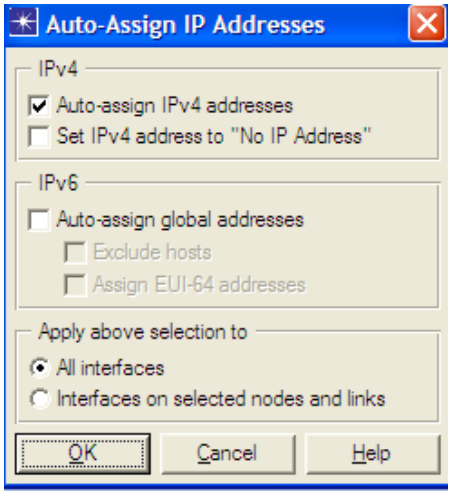


Figura 7. Asignación automática de direcciones IP

VII. Para establecer el protocolo de enrutamiento sobre toda la red, debe desplegar en la barra de menú la opción **Protocols**, seleccione **IP**, luego escoja **Routing**, haga Click en **Configure Routing Protocols** y por último habilite **IS-IS**. (Deshabilite **Visualize Routing Domains** y presiones **Ok**). En la figura 8 se puede apreciar la configuración del protocolo.

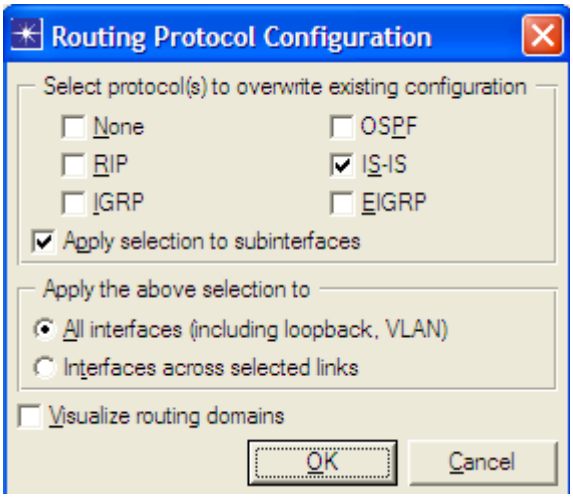


Figura 8. Configuración del protocolo de enrutamiento IS-IS

VIII. Para configurar la métrica sobre todas las interfaces de la red despliegue en la barra de menú la opción **Protocols**, seleccione **IS-IS**, escoja **Configure interface metrics** y luego aparecerá la ventana de configuración, dele Click en OK. (Por defecto Level 1 y Level 2 tienen asignados el valor de 10, pero se puede cambiar). En la figura 9 se puede apreciar la respectiva configuración.

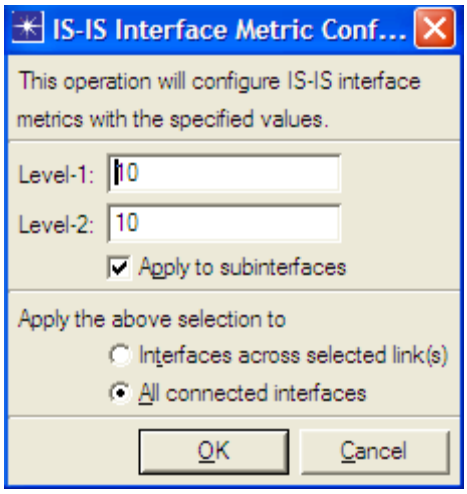


Figura 9. Configuración de la métrica

IX. A continuación, seleccione en la paleta de dialogo el objeto **ip_traffic_flow** para crear flujo de tráfico desde el router **Ocaña** hacia los routers **Monteria** y **Cali.** En la figura 10 se puede apreciar el flujo de tráfico entre los routers.

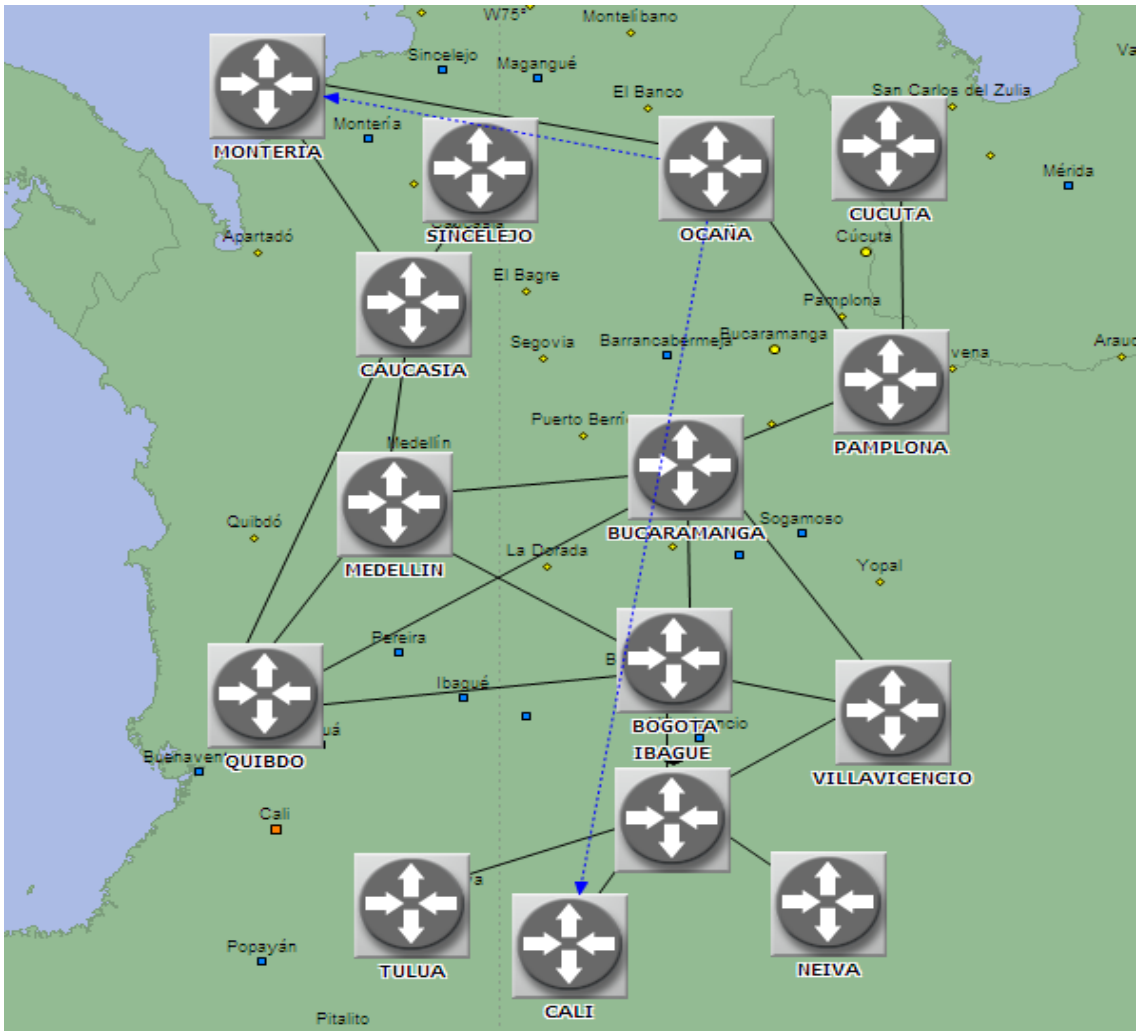


Figura 10. Configuración del flujo de tráfico

X. Luego, aplique la opción para exportar las tablas de enrutamiento de cada router; despliegue en la barra de menú la opción **Protocols**, seleccione **IP**, escoja **Routing** y por último dele Click en **Export Routing Table** *(all nodes*)**.**

XI. Una de las características del protocolo IS-IS es la capacidad para el balanceo de carga a través de caminos de igual costo, asigne esta configuración sobre el router **Bucaramanga**, para esto despliegue en la barra de menú la opción

Protocols, seleccione **IP**, escoge **Routing** y por último **Configure Load Balancing Options.** Aparecerá una ventana, asigne **Packet Based** y habilite **Selected routers.**

XII. Ahora, una forma de visualizar el ancho de banda es utilizando la opción *throughput*. Para configurar esta opción presione Click derecho sobre el espacio de trabajo y escoja **Choose Individual DES Statistics**, aparecerá la ventana de *Choose Results* y seleccione **Link Statistics**, escoge **Point to Point** y por último **throughput (bits/sec)**.

2.3 Creación de un nuevo escenario (Red_jerarquica):

I. En la barra de menú despliegue **Scenarios** y seleccione **Duplicate Scenario** (llámelo **Red_jerarquica**), dele Ok.

II. Despliegue en la barra de menú la opción **Topology**, seleccione **Annotation Palette** y escoja la imagen del círculo  para establecer las áreas de la red. Encierre el grupo de routers: **Monteria-Sincelejo-Caucasia**, **Ocaña-Cucuta-Pamplona** e **Ibague-Tulua-Cali-Neiva**. En la figura 11 se puede apreciar la respectiva asignación de áreas.

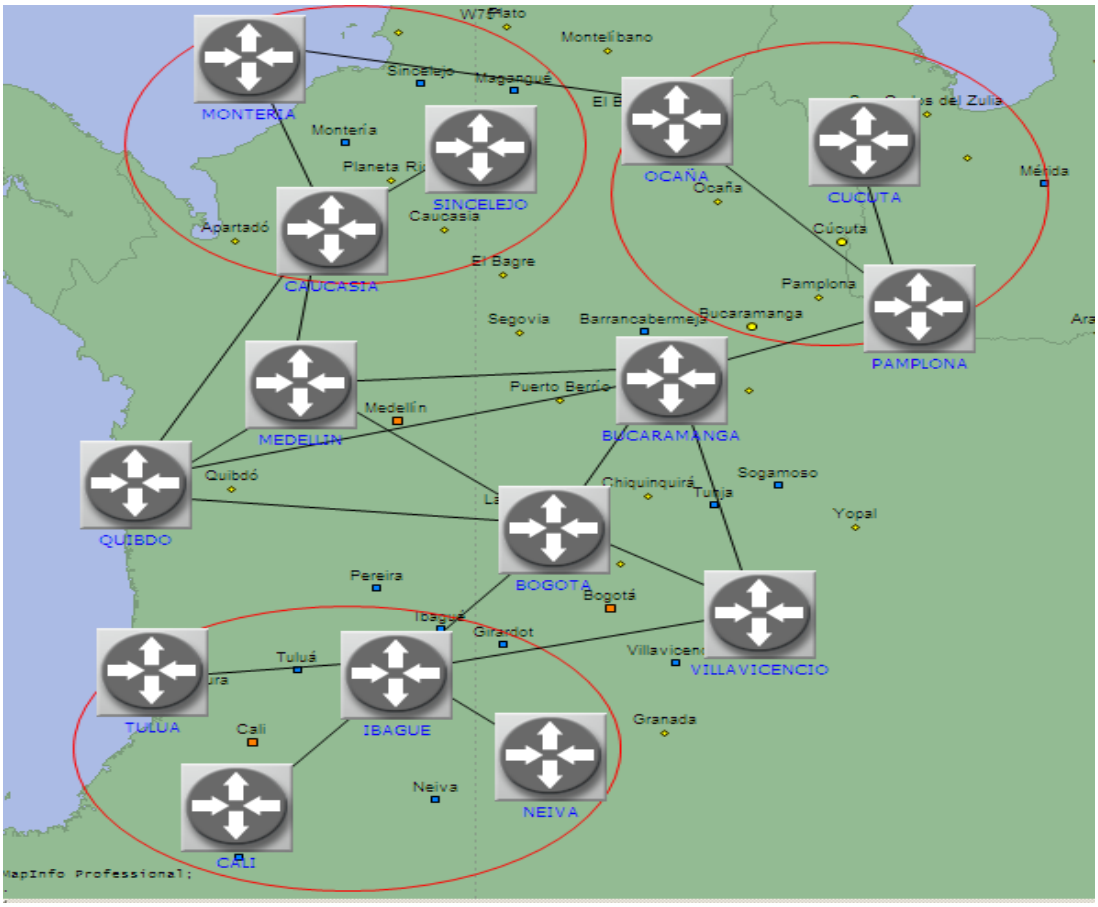


Figura 11. Representación de áreas

III. Ahora, es necesario configurar los tipos de sistemas de cada router y su respectivo identificador; ya que se pretende establecer la jerarquía de la red.

Seleccione el respectivo router y presione Click derecho, escoja **Edit Atributes** y despliegue en cadena: **IP Routing Protocols**, luego **IS-IS Parameters**, seguidamente **Processes**, seleccione el número **1**, haga Click sobre **Processes Parameters** y por último **Network Entity Title**. En la tabla 2 aparecerá el identificador (NET) y el tipo de sistema de cada router.

Router	NET	System Type	Área
Montería	**49.0001.1920.0004.5001.00**	**Level 1**	**49.0001**
Sincelejo	**49.0001.1920.0004.4001.00**	**Level 1**	**49.0001**
Caucásia	**49.0001.1920.0004.6001.00**	**Level -1-2**	**49.0001**
Tuluá	**49.0002.1920.0004.9001.00**	**Level 1**	**49.0002**
Cali	**49.0002.1920.0007.0001.00**	**Level 1**	**49.0002**
Neiva	**49.0002.1920.0004.8001.00**	**Level 1**	**49.0002**
Ibagué	**49.0002.1920.0005.0001.00**	**Level -1-2**	**49.0002**
Ocaña	**49.0003.1920.0004.1001.00**	**Level 1**	**49.0003**
Cúcuta	**49.0003.1920.0003.3001.00**	**Level 1**	**49.0003**
Pamplona	**49.0003.1920.0004.2001.00**	**Level -1-2**	**49.0003**
Medellín	**49.0001.1920.0003.2001.00**	**Level 2**	**49.0001(Backbone)**
Quibdó	**49.0001.1920.0004.3001.00**	**Level 2**	**49.0001(Backbone)**
Bogotá	**49.0001.1920.0003.4001.00**	**Level 2**	**49.0001(Backbone)**
Bucaramanga	**49.0001.1920.0003.1001.00**	**Level 2**	**49.0001(Backbone)**
Villavicencio	**49.0001.1920.0003.0001.00**	**Level 2**	**49.0001(Backbone)**

Tabla 2. Identificador (NET), System Type y Área de cada router.

IV. Despliegue en la barra de menú la opción **Topology**, seleccione **Open Annotation Pallete**, escoja  para asignar las áreas y los tipos de sistemas de cada router que cumplen su función en cada área y en el área backbone. De esta manera se puede distinguir la configuración de cada router, para esto

tenga en cuenta la tabla 2. (Presione *ctrl S* para trasladar la palabra al espacio de trabajo). En la figura 12 se puede apreciar la identificación del tipo de sistema de cada router y en la figura 13 la asignación de áreas.

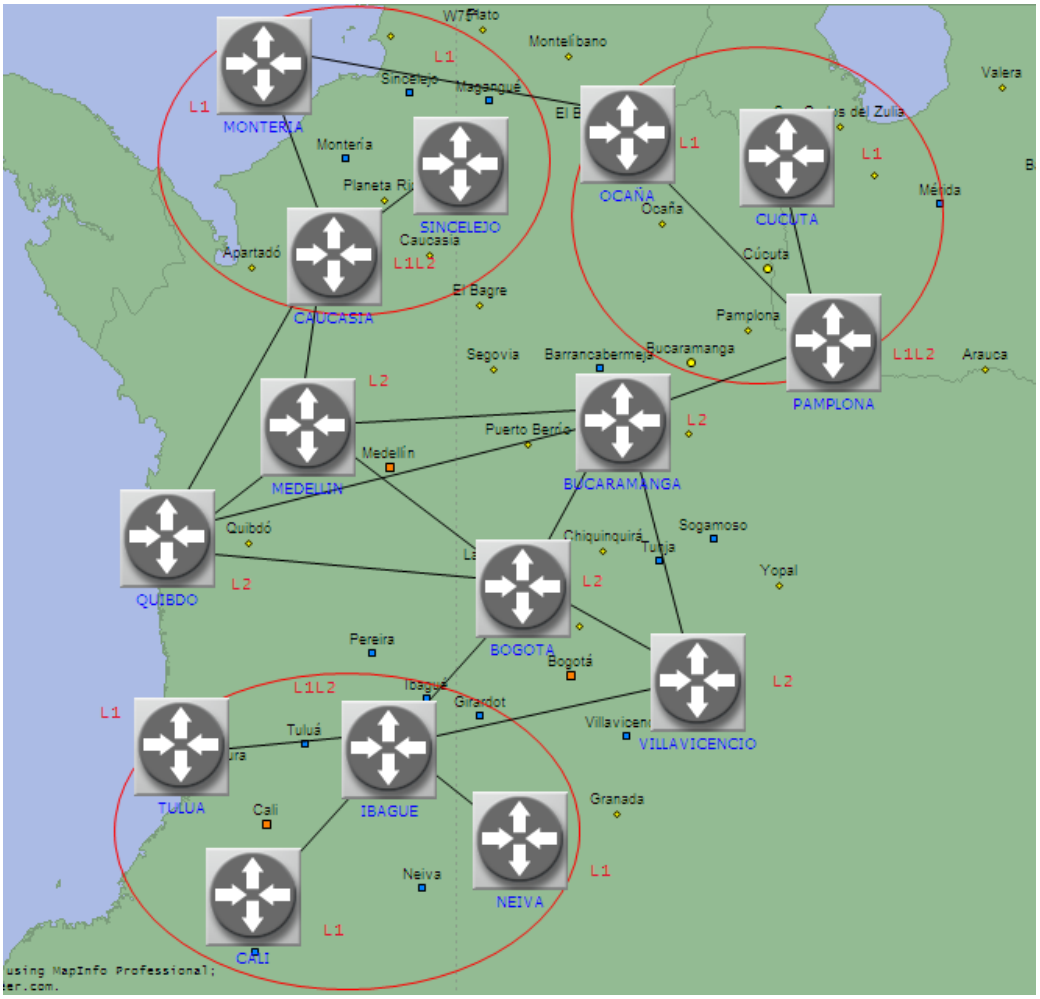


Figura 12. Asignación de los tipos de sistemas.

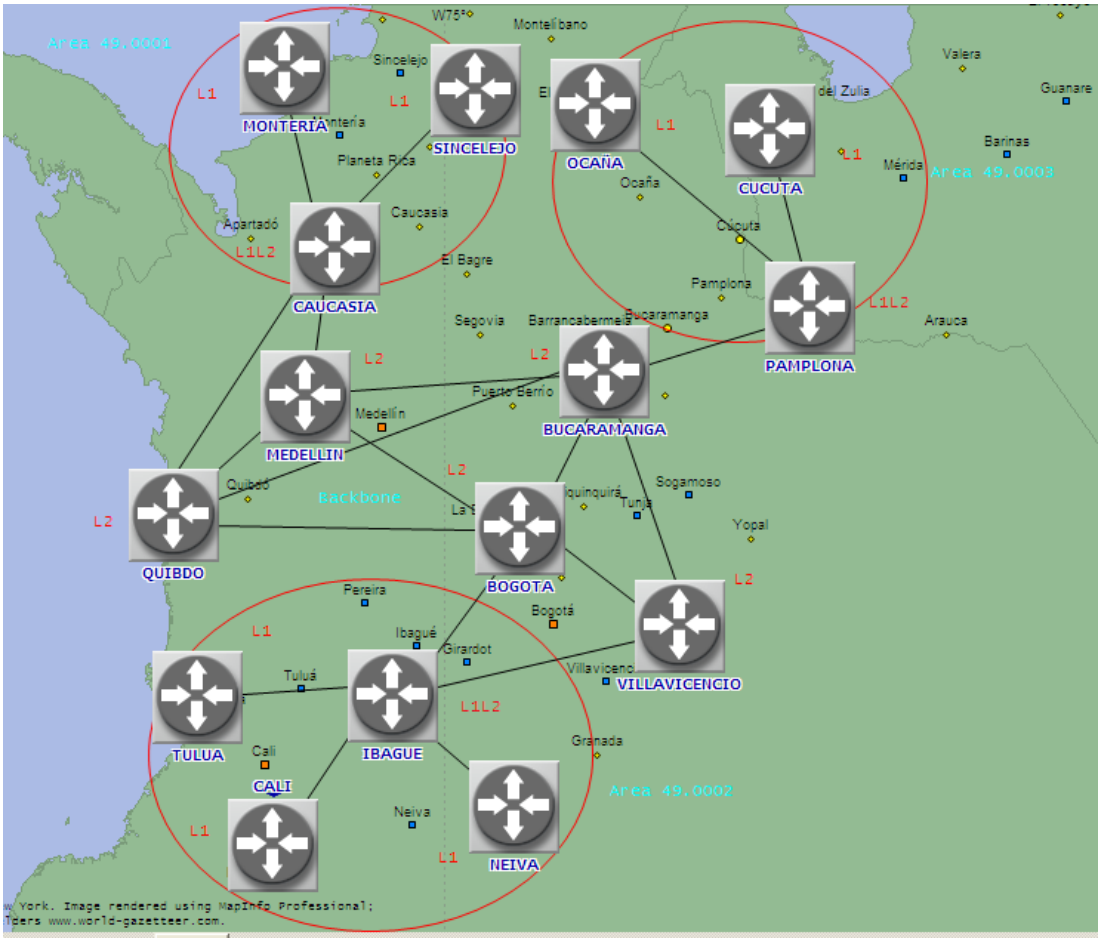


Figura 13. Asignación de áreas

V. A continuación, seleccione en la paleta de dialogo el objeto **ip_traffic_flow** para crear flujo de tráfico desde el router **Ocaña** hacia los routers **Monteria** y **Cali.** En la figura 14 se puede apreciar el flujo de tráfico.

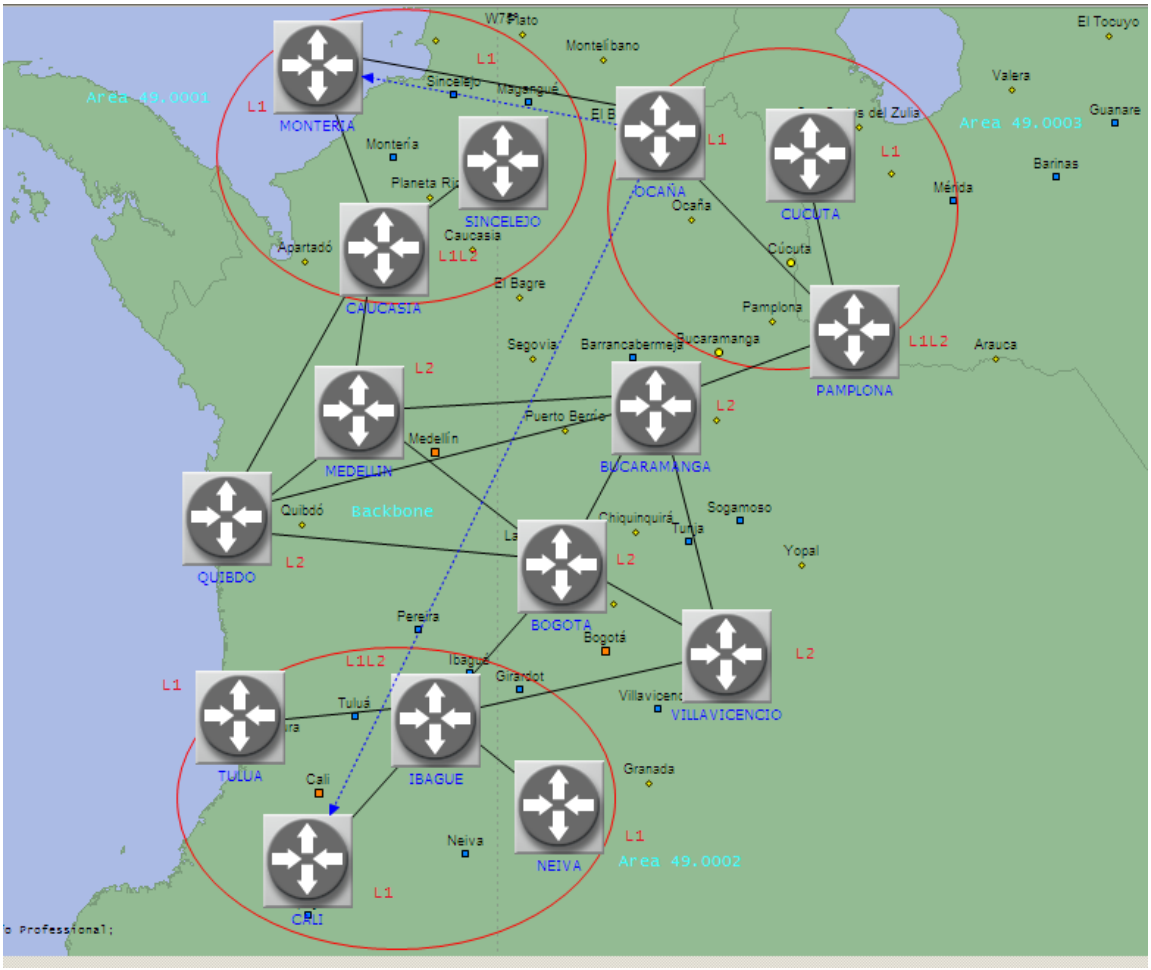


Figura 14. Flujo de tráfico entre routers

VI. Basado en las características del protocolo IS-IS se efectuará el balanceo del flujo de tráfico desde el router Ocaña hacia los routers **Monteria** y **Cali,** configurado en el router **Bucaramanga**. Para asignar el balanceo de carga seleccione el router **Bucaramanga**, despliegue en la barra de menú la opción **Protocols**, seleccione **IP**, escoge **Routing** y por último dele Click sobre **Configure Load Balancing Options.** Aparecerá la ventana de configuración, asigne **Packet Based** y habilite **Selected routers.**

VII. Para visualizar el ancho de banda utilice la opción *throughput*. Para configurar esta opción presione Click derecho sobre el espacio de trabajo y escoge **Choose Individual DES Statistics**, aparecerá la ventana de *Choose Results* y seleccione **Link Statistics**, escoge **Point to Point** y por último **throughput (bits/sec)**.

2.4. Ejecutar la simulación y ver los resultados:

I. Despliegue el menú **Scenarios** y seleccione **Manage Scenarios**, luego en el campo de **results** cambie la opción para cada escenario por **collect** o **recollect**. Ahora para establecer el tiempo de la simulación; en el campo **Sim Duration** escribe 1 y en **Time Units** escoge **hour**, dale **Ok**. Al finalizar presione **Close** y salve el proyecto.

II. En la barra de menú despliegue **Scenarios**, seleccione **Switch to scenario** y escoja **Sin_ jerarquia**.

III. A continuación, se debe generar la carga de tráfico. Para esto se generaran flujos entre todos los nodos. Despliegue en la barra de menú la opción **Traffic**, seleccione **Create Traffic Flows,** luego **IP** y por último **Unicast Full mesh between all nodes**, presione **Create**. Corra de nuevo el programa, ahora despliegue de nuevo la opción **Traffic** y seleccione **Open Traffic Center** para ver el flujo de tráfico. Aparecerá la ventana de **Traffic center** y habilite la carpeta **Flow.** En la figura 15 se puede ver la configuración de la creación del tráfico y en la figura 16 la visualización de las posibles rutas de tráfico entre los routers.

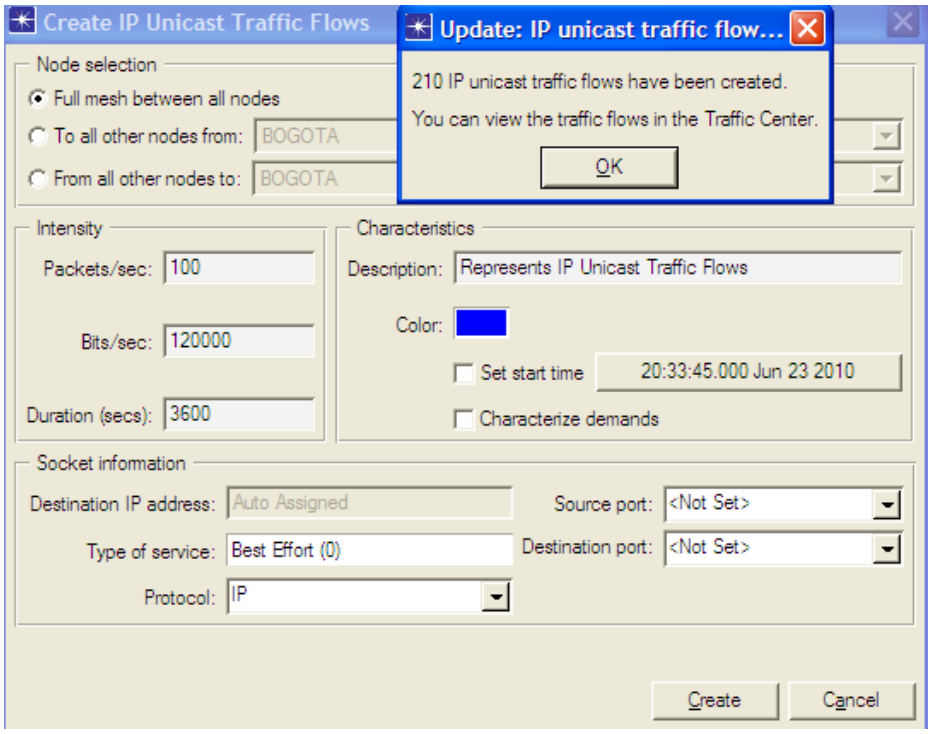


Figura 15. Configuración del flujo de tráfico

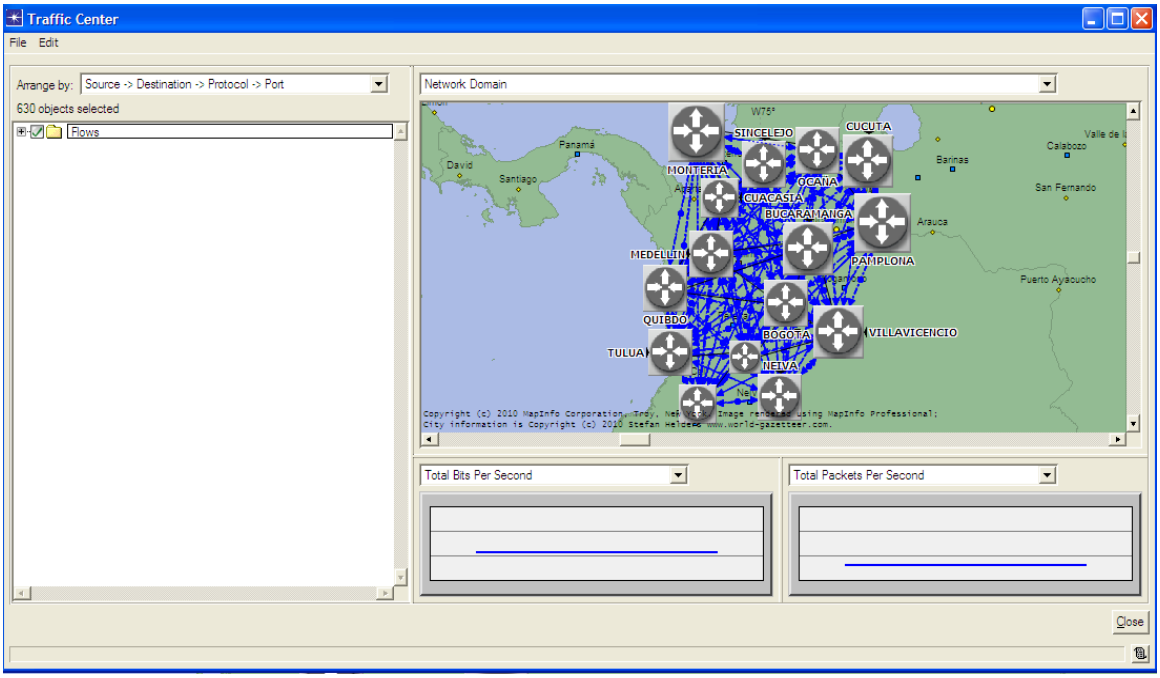


Figura 16. Posibles rutas entre routers

IV. Cierre la ventana de **Traffic center** y en la barra de menú despliegue la opción **Protocols**, seleccione **IP**, escoja **Demands** y ahora **Display Routes for Configure Demands** (aparecerá la ventana **Route Report for IP Traffic Flows**), ahora despliegue la opción **Ocaña** y ahí mismo seleccione **Monteria**. Para ver el flujo de tráfico del escenario **Sin _jerarquia** cambie el campo de **Display** por **Yes.**

En la figura 17 se puede ver el procedimiento de configuración para ver el reporte de ruta del flujo de tráfico IP y en las figuras 18 y 19 la visualización de este mismo.

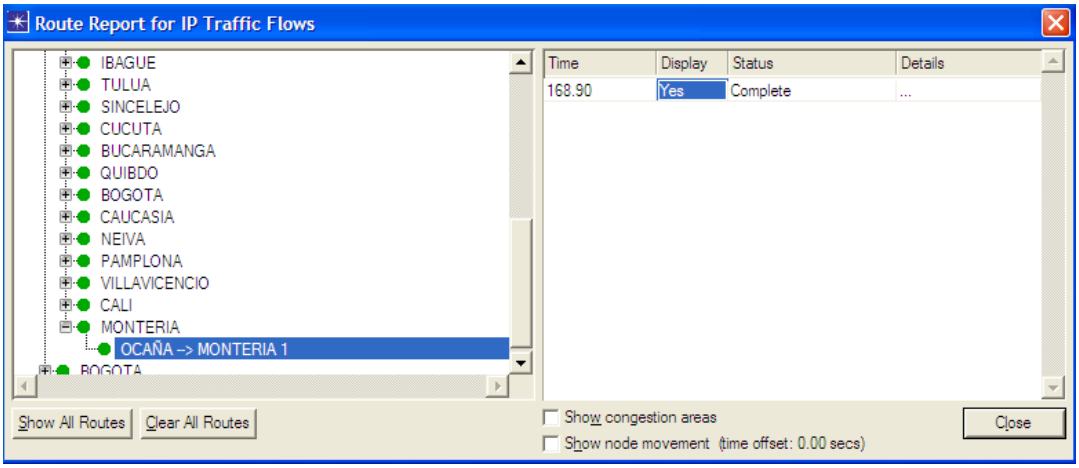


Figura 17. Congifuracion para ver el reporte de ruta

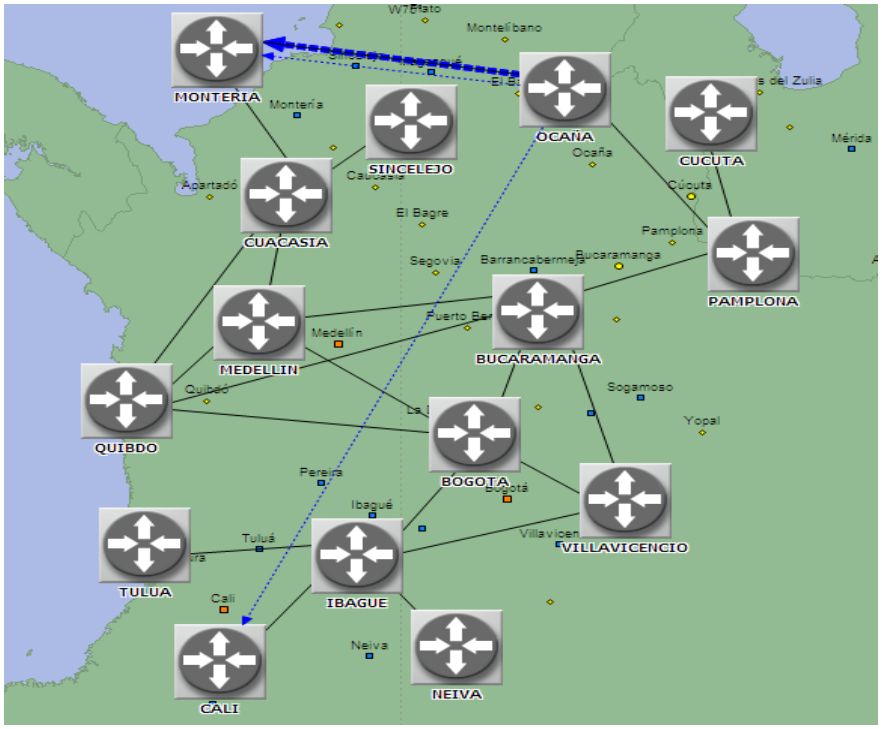


Figura 18. Ruta Ocaña – Monteria (Escenario Sin_jerarquia)

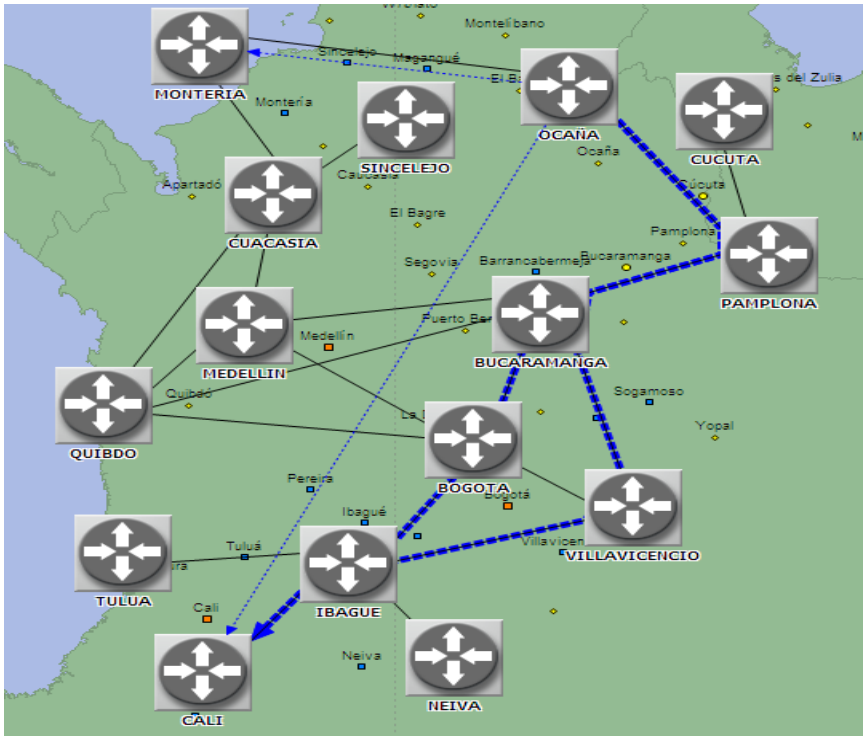


Figura 19. Ruta Ocaña – Cali (Escenario Sin_jerarquia)

V. Para visualizar el ancho de banda seleccione en la barra de menú la opción **DES**, escoge **Results** y por último dale Click en **Compare Results.** De esta manera aparecerá la ventana de *Results Browser*, cerciórese que esté seleccionado el escenario *sin_jerarquia* y en la opción de *Campus Network* habilite los enlaces de tráfico enviado (→) entre los Routers: Ocaña – Monteria, Pamlpona - Bucaramanga, Bucaramanga - Bogota y Bucaramanaga – Villavicencio. tanto para el tráfico recibido como para el ancho de banda. En la figura 20 y 21 se pueden apreciar las gráficas correspondientes.

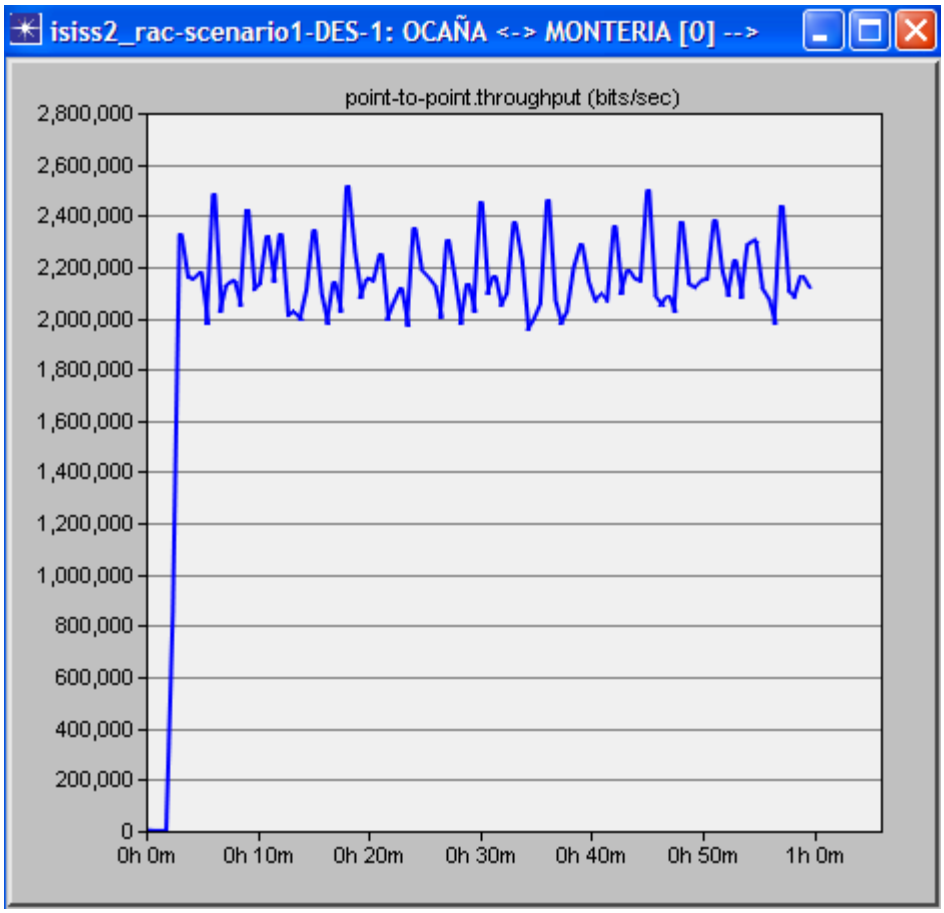


Figura 20. Throughput entre los Routers Ocaña – Monteria. (Escenario sin_jerarquia)

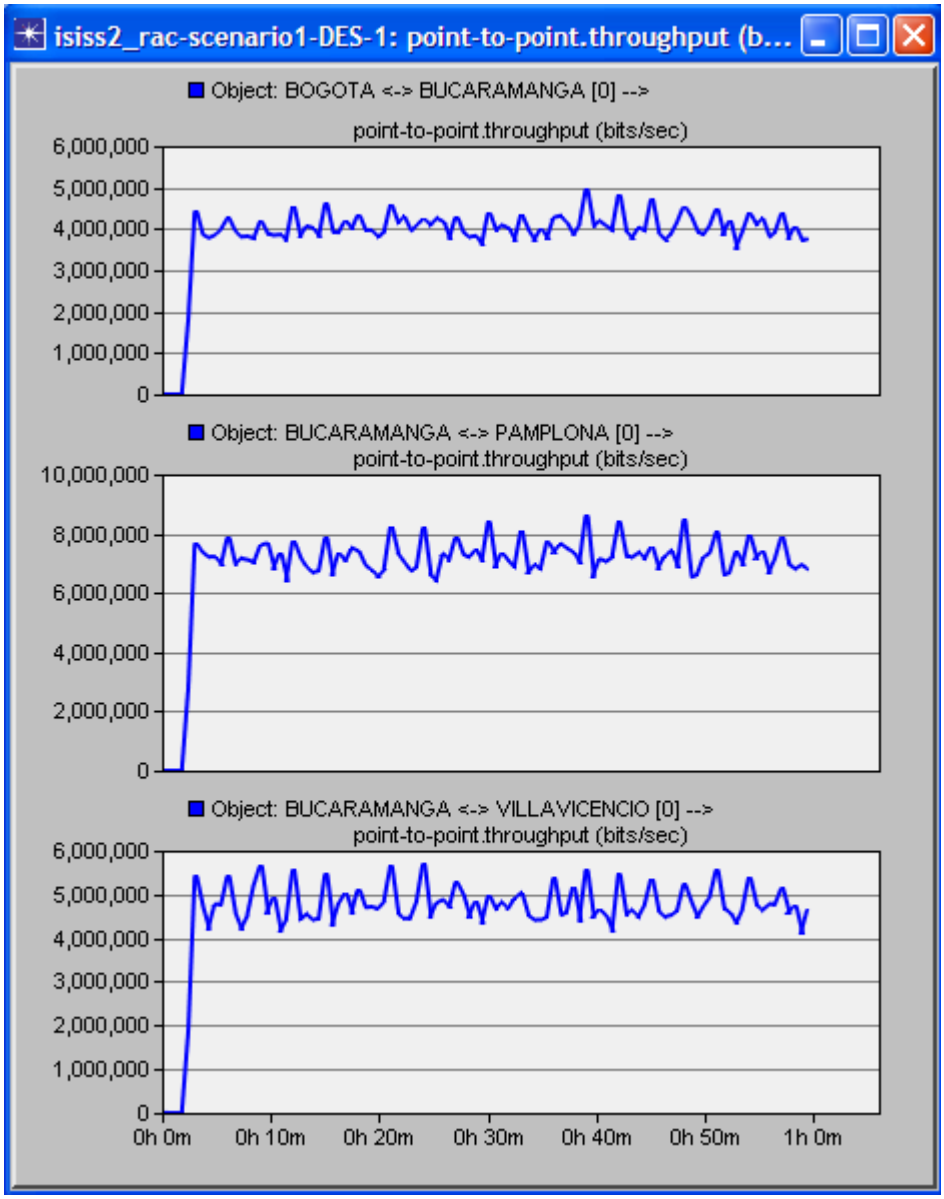


Figura 21. Throughput entre los Routers: Bogota – Bucaramanga, Bucaramanga – Pamplona y Bucaramanga – Villaviencio. (Escenario sin_jerarquia)

VI. Genere la tabla de enrutamiento del router Ocaña para el escenario sin_jerarquia, para esto seleccione sobre la barra de menú de **Results Browser** la opción **DES Run (1) Tables**, despliegue **Object Tables** y seleccione las siguientes opciones en cadena: **Campus Network**, después

Router Ocaña, luego **Performance** y por último **IP Forwarding Table at End of Simulation**. En la figura 22 se puede apreciar la respectiva tabla de enrutamiento.

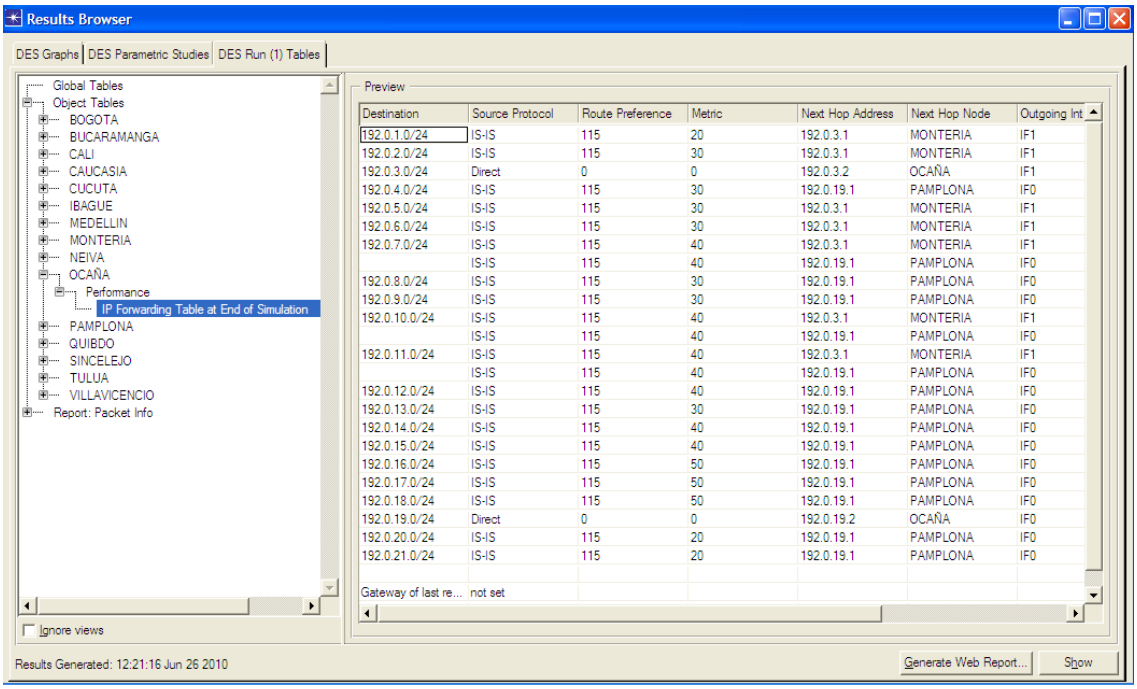


Figura 22. Tabla de enrutamiento para el Router Ocaña (escenario sin_jerarquia).

VII. En la barra de menú despliegue **Scenarios**, seleccione **Switch to scenario** y escoja **red_jerarquica**.

VIII. Repita el paso 4 para ver las rutas del flujo de tráfico del escenario red_jerarquica. En la figura 23 y 24 se puede apreciar las respectivas rutas.

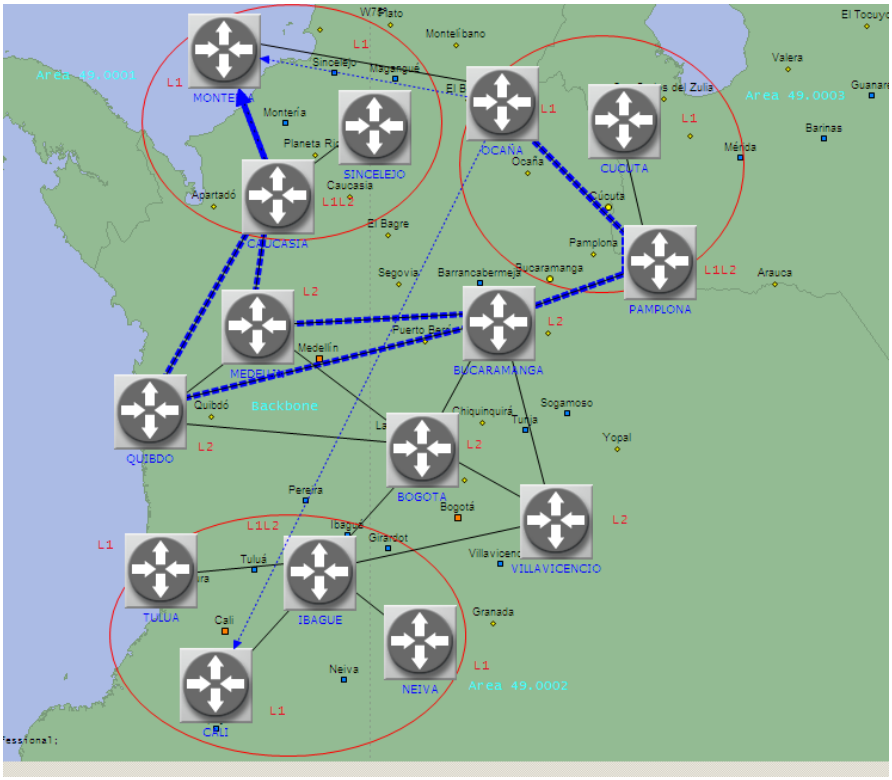


Figura 23. Ruta Ocaña – Monteria (Escenario Red_jerarquia)

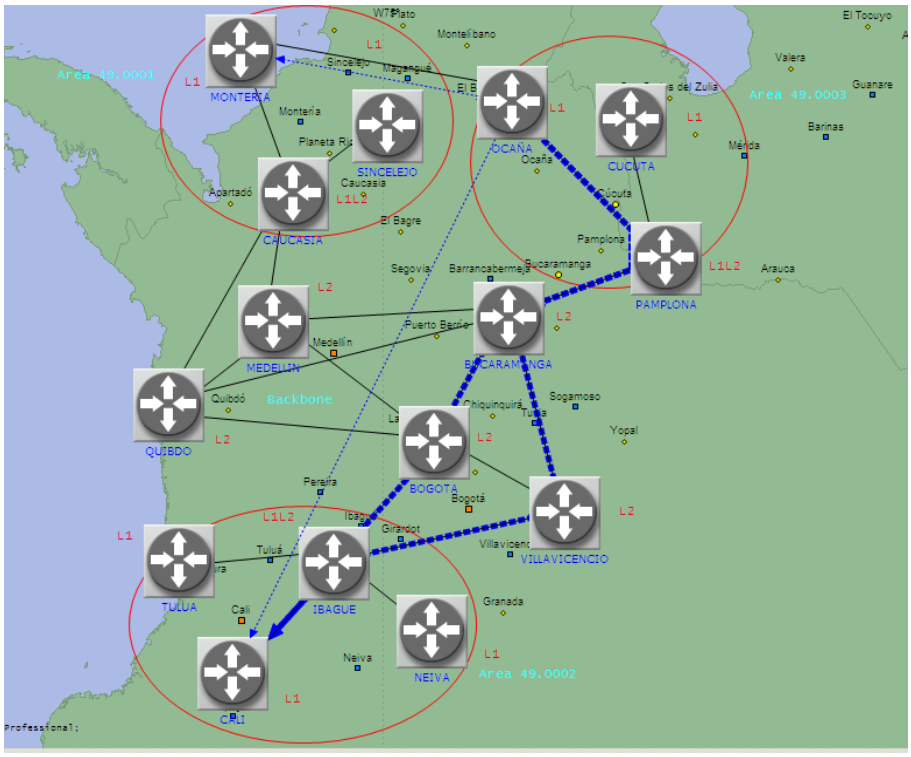


Figura 24. Ruta Ocaña – Cali (Escenario Red_jerarquia)

IX. Repita el paso 5 para visualizar el ancho de banda del escenario red_jerarquica. En la figura 25 y 26 se pueden apreciar las gráficas correspondientes.

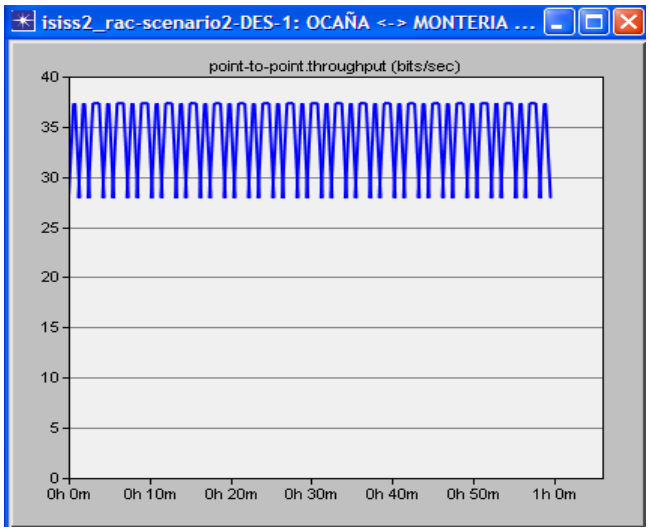


Figura 25. Throughput entre los Routers Ocaña – Monteria. (Escenario red_jerarquia)

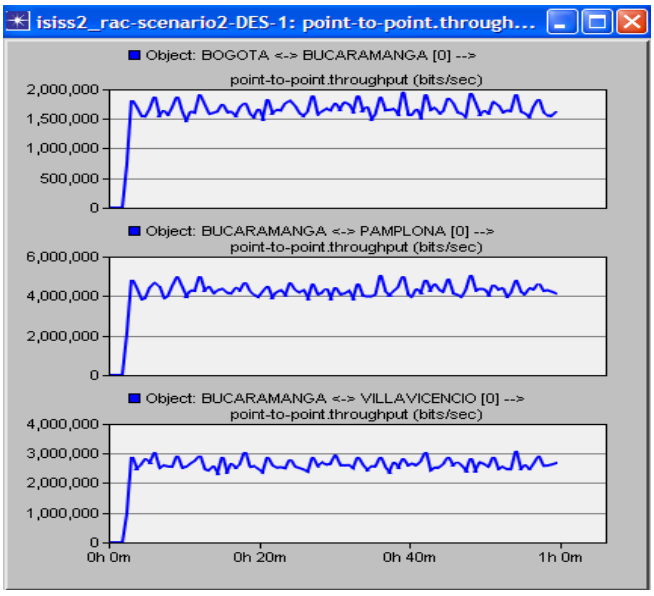


Figura 26. Throughput entre los Routers: Bogota – Bucaramanga, Bucaramanga – Pamplona y Bucaramanga – Villaviencio. (Escenario sin_jerarquia)

X. Repita el paso 6 para generar la tabla de enrutamiento del router Ocaña del escenario red_jerarquica.

En la figura 27 se puede apreciar la respectiva tabla de enrutamiento.

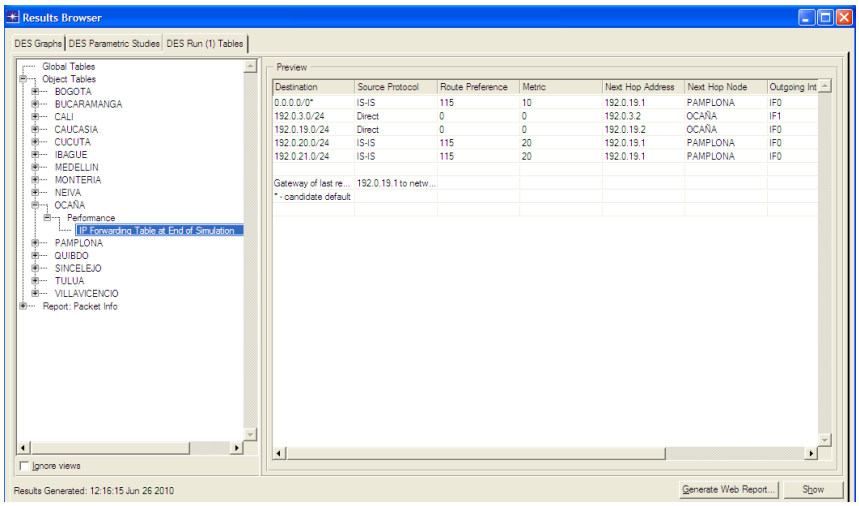


Figura 27. Tabla de enrutamiento para el Router Ocaña (escenario red_jerarquica).

Trabajo en clase:

1. Analice la tabla de enrutamiento del router Ocaña, para los dos escenarios. Tenga en cuenta las ventajas y desventajas del protocolo de enrutamiento y la configuración de la red.

2. Que beneficios se generan al aplicar el balanceo de carga sobre el Router Bucaramanga. Analice las graficas obtenidas de la representación del ancho de banda (throuhput) sobre el enlace entre el par de routers

3. Explique porque en los escenarios sin_jerarquia y red_jerarquica se obtienen diferentes rutas.

4. Haga un paralelo de características entre los protocolos IS-IS y OSPF.

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE INGENIERÍA Y ADMINISTRACIÓN
PROGRAMA DE INGENIERÍA ELECTRÓNICA
REDES DE COMPUTADORES (OPTATIVA)

ANEXO 4

GUIA PRÁCTICA SOBRE PROTOCOLOS DE ENRUTAMIENTO EN LA RED

Práctica N°4

TÍTULO: BGP (BORDER GATEWAY PROTOCOL)

OBJETIVOS:

- Implementar una red BGP garantizando las características generales que rige este protocolo, como son: establecer parejas de vecindad IBGP y EBGP; asignar sistemas autónomos y crear la tabla de vecinos para cada router.
- Utilizar la opción throughput como una forma de visualización del ancho de banda, a partir del tráfico generado entre las corporaciones.
- Analizar las tablas de enrutamiento para cada uno de los Routers.

3. MARCO TEÓRICO:

El protocolo de pasarela frontera (BGP, Border Gateway Protocol) se desarrolló para su uso en conjunción con interconexiones de redes que empleen la arquitectura de protocolos TCP/IP, aunque los conceptos son aplicables a cualquier conexión de redes, BGP se ha convertido en el protocolo de dispositivo de encaminamiento exterior preferido para internet. Principalmente BGP se diseñó para permitir la cooperación en el intercambio de información de encaminamiento entre dispositivos de encaminamiento de diferentes sistemas autónomos (AS),

llamados pasarelas en el estándar. El protocolo opera en términos de mensajes, que se envían utilizando conexiones TCP.

Generalmente un sistema autónomo corre algún protocolo IGP. Estos protocolos IGP se caracterizan porque anuncian redes y describen la métrica para alcanzar estas redes, por otro lado BGP describe trayectos y las redes que se pueden alcanzar al final del trayecto, BGP describe estos trayectos mediante atributos de manera equivalente a la métrica de los IGPs.

El término vecinos empleado en los IGPs se reemplaza por el término *peers*, la razón se debe a que el término vecinos se aplicaba a enrutadores que estaban directamente conectados, sin embargo los vecinos BGP no necesariamente tienen que estar conectados directamente. Cuando BGP corre en dos *routers* que pertenecen a distintos sistemas autónomos, la relación se denomina EBGP. Por otro lado, cuando BGP se ejecuta en dos *peers* en un mismo AS, la relación se denomina IBGP. [43]

2. PROCEDIMIENTO:

A continuación veremos en la figura 1 el diseño de la arquitectura de red que emplearemos en la simulación, seguido de los pasos para desarrollar la práctica.

- **Router IP (atm4_ethernet2_slip8_gtwy_int):** El modelo representa un nodo atm4_ethernet2_slip8_gtwy_int, el cual opera como una puerta de enlace IP y contiene dos interfaces Ethernet, también contiene ocho interfaces de línea seriales a una velocidad seleccionable. Los paquetes IP que llegan a cualquier

[43] PEREZ, Duber. SISTEMAS DE COMUNICACIÓN MOVIL Y REDES DE BANDA ANCHA. Pdf. Universidad Privada Antenor Orrego.2009.

interfaz se enrutan a la interfaz de salida adecuada en función de su dirección IP de destino.

- **Fast EthernetLAN (10BaseT_LAN):** Se usa este objeto para representar una red LAN en una topología conmutada. Este objeto contiene un servidor y un número de clientes especificado por el usuario. El tráfico de los clientes puede ser dirigido hacia el servidor interno, así como a servidores externos.

- **Link (PPP_DS1):** Enlace que utiliza el protocolo PPP y que tiene una capacidad de 1,544 Mbps.

- **Link (PPP_DS3):** Enlace que utiliza el protocolo PPP y que tiene una capacidad de 44,736 Mbps.

- **Link (10BaseT):** El enlace duplex 10BaseT representa una conexión Ethernet que opera a 10 Mbps. Puede conectar cualquier combinación de los siguientes nodos: Estación, hub, puente, switch, nodos LAN.

- **Profile Config:** Este nodo puede ser usado para representar perfiles de usuario. Estos perfiles de usuario luego pueden ser especificados sobre nodos diferentes en la red para generar tráfico en la capa de aplicación.

- **Application Config:** Especifica las aplicaciones que utilizan tipos disponibles de la aplicación. Se puede especificar un nombre y la descripción correspondiente en el proceso de crear nuevas aplicaciones.

  Por ejemplo: Web Browsing (Heavy HTTP), indica una aplicación de la web.

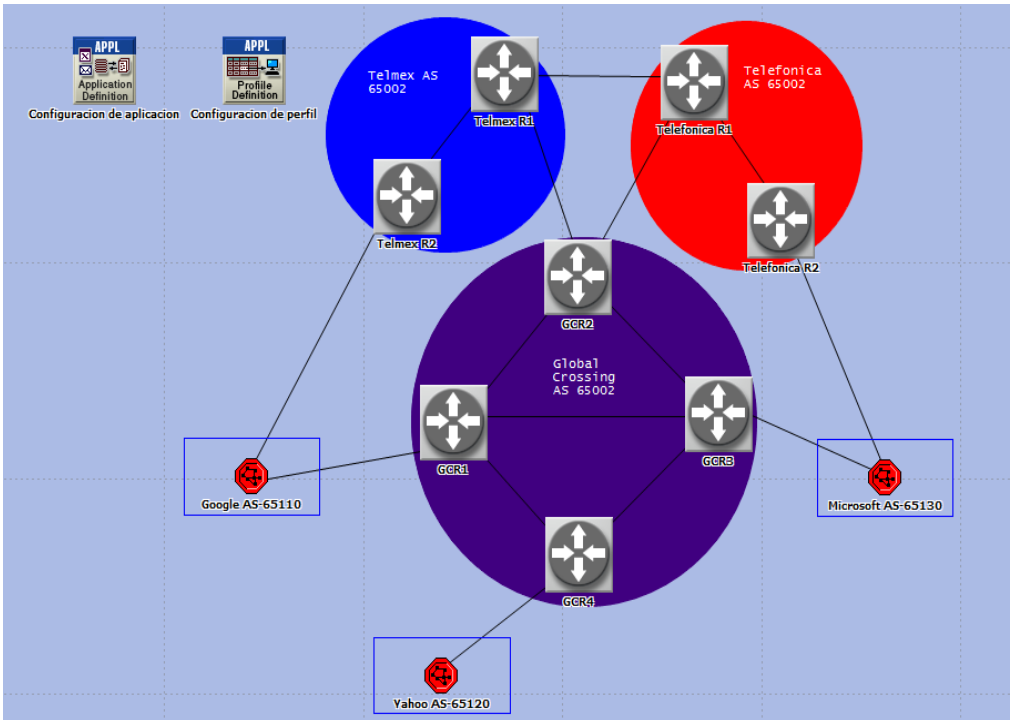


Figura 1. Arquitectura de la red utilizando el protocolo BGP

2.1 Creación del proyecto:

I. Inicie el simulador Opnet Modeler, para la creación del nuevo proyecto elige en la barra de menú la opción **File** y seleccione **New** para crear el proyecto, luego dale Click en **Project** y por último **Ok**. Ahora dele nombre al proyecto, por ejemplo: *tu nombre_Corporaciones,* luego al escenario a crear dele el nombre *Corporaciones*, presione **Ok.** Aparecerá la ventana de *Startup Wizard,* haga Click en **Next** para elegir el área sobre el cual se desea crear la arquitectura de red, seleccione la opción **Campus** y presione **Next,** ahora para adecuar el tamaño de la red; coloque en el campo **x=100** y **y=100**. Finalmente dele **Next** dos veces y luego **Finish.**

2.2 Creación y configuración de la red:

I. Seguidamente aparecerá la paleta de dialogo (Object Pallete), el cual permitirá acceder a los elementos de trabajo para el diseño de la red, en caso de que no aparezca pulse en la barra de menú el botón  .Al desplegarlo es necesario que la opción **internet tool_box** esté seleccionado.

II. En la paleta de diálogo seleccione el router **atm4_ethernet2_slip8_gtwy_int**, sitúe 3 de este mismo en el espacio de trabajo y utilice el enlace **PPP_DS3** para conectar los routers como aparece en la figura 2, luego sitúe 5 routers de este mismo tipo e interconéctelos utilizando el enlace **PPP_DS3** y renómbrelos tal cual como se aprecia en la figura 3 para identificar los routers de cada área (AS).

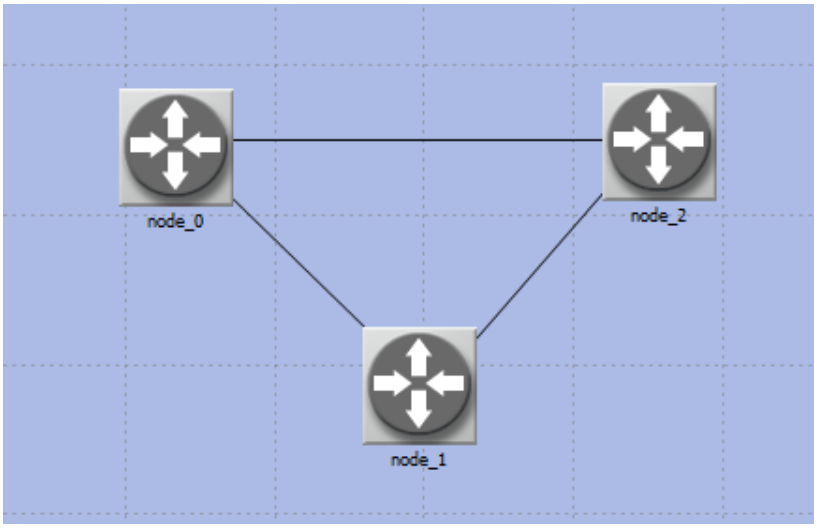


Figura 2. Interconexión entre routers

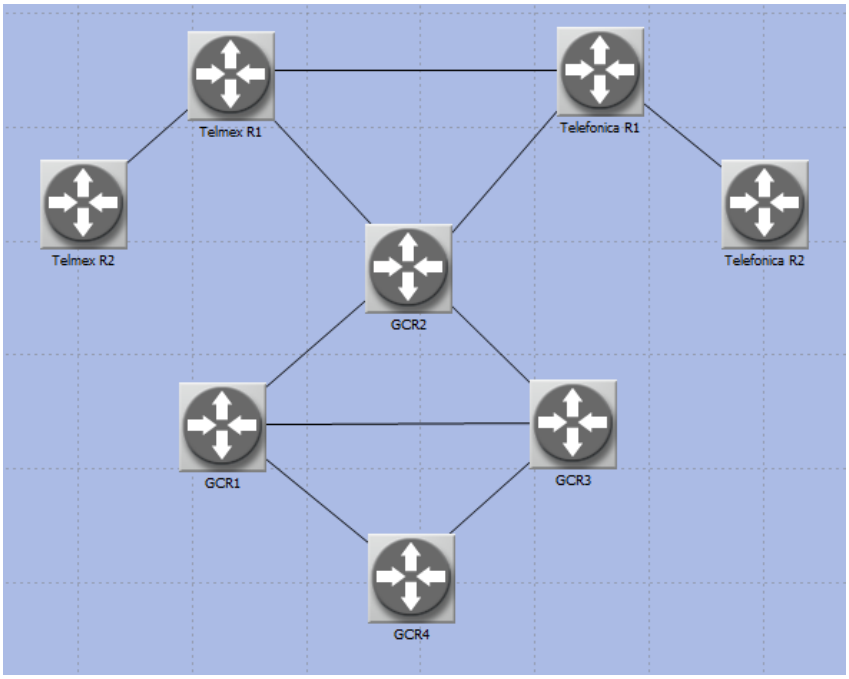


Figura 3. Interconexión y renombramiento de routers

III. Ahora sitúe en el área de trabajo el elemento que representa una subestación 

, selecciónelo; ubique 3 objetos de este mismo y dele el nombre a cada uno con su respectivo número de AS: **Google AS-65110, Yahoo AS-65120 y Microsoft AS-65130**. Presione dos veces Click izquierdo sobre uno de estos sistemas autónomos, para crear dentro de esta subestación la arquitectura de red.

Luego, seleccione un router **ethernet4_slip8_gtwy**, 3 redes LAN **10BaseT_LAN**, un switch **3C_CB3500_4s_ae12_ge2**, 2 servidores **ethernet_server** y sitúelos en el espacio de trabajo para interconectarlos con el enlace duplex **10BaseT**.

La conexión y el renombramiento de cada elemento se pueden apreciar en la figura 4.

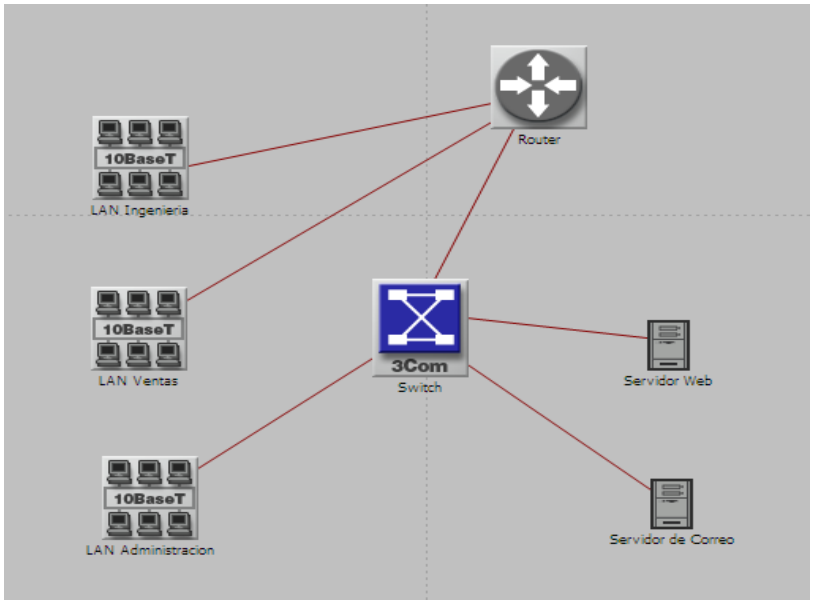


Figura 4. Arquitectura de red de la subnet

IV. Seleccione todos los elementos que se encuentran dentro de la estación *subnet* y presione *ctrl C*. Ahora, para salir de la estación haga Click derecho sobre el área de trabajo y escoja *Go To Parent Subnet,* luego dentro de cada una de las dos estaciones restantes, presione *ctrl V* para crear la misma arquitectura establecida en la primera estación. (para la subnet de *Yahoo AS-65120* elimine el servidor web y el enlace).

V. Después de realizar el paso 4, vuelva a la arquitectura general de toda la red para unir a través del enlace **PPP_DS1;** los routers **Telmex R2** y **GCR1** con el router de la subestación **Google AS-65110**.

Interconecte de la misma manera los routers **Telefonica R2** y **GCR3** con el router de la sub estación de **Microsoft AS-65130** y por último una el router **GCR3** con el router de la subestación de **Yahoo AS-65120.**

Para esto haga Click derecho sobre la subnet y seleccione *Expand Subnet* y de esta manera poder seleccionar el respectivo router.

En la figura 5 se puede apreciar la respectiva conexión.

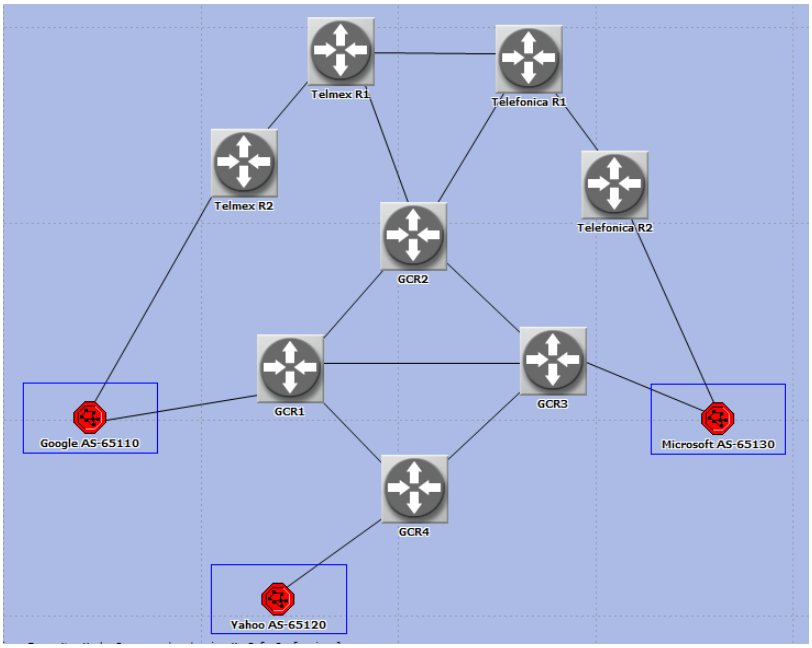


Figura 5. Interconexión entre corporaciones y routers

VI. Para obtener una mejor visualización e identificación de los sistemas autónomos de la arquitectura de la red, despliegue la opción **Topology** en la barra de menú, seleccione **Open Annotation Pallete** y escoge la imagen del circulo, de esta manera agrande el ovalo y enmarque cada pareja de routers **Telmex R1 – Telmex R2**, **Telefónica R1 – Telefónica R2** y los cuatro routers **GCR1, GCR2, GCR3 y GCR4**.

Existe la opción de cambiar el color de cada área para diferenciar los sistemas autónomos, seleccione el ovalo y presione Click derecho, escoge **Edit Attributes**, seguidamente haga Click en el campo ***value*** al frente de ***color*** y seleccione el color de su preferencia. Luego seleccione T y asigne el nombre a las corporaciones con su respectivo AS. (Presione *ctrl S* para trasladar el nombre al espacio de trabajo).

En la figura 6 se puede apreciar la identificación de los sistemas autónomos.

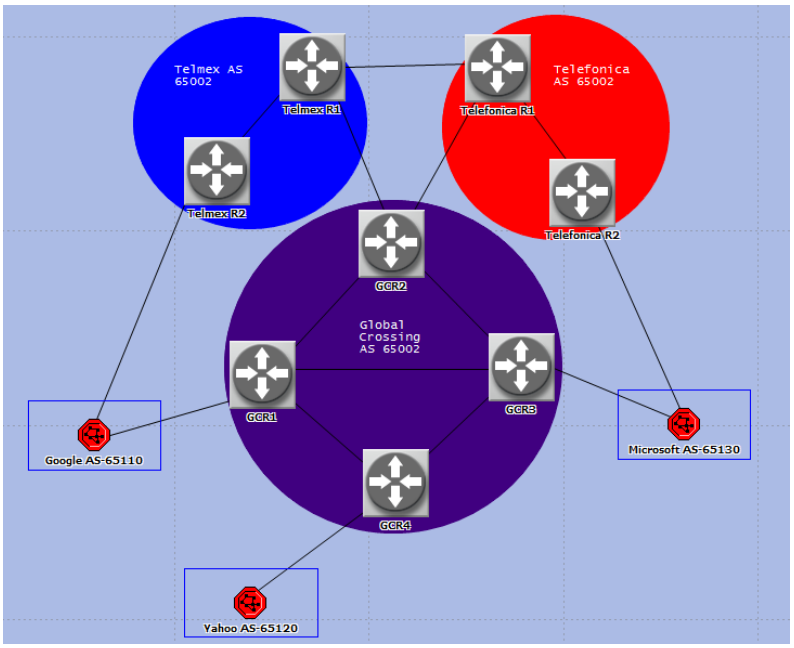


Figura 6. Representacón de ASs

VII. A continuación verificamos los puertos de cada router asignados predeterminadamente por el software, ya que de esta manera permitirá que se establezca correctamente las interfaces interconectadas en la misma subred. (En el caso que no se encuentren en la misma subred se debe de editar las propiedades del enlace y especificar las interfaces correctas).

Para verificar, seleccione el enlace entre el par de routers y presione Click derecho, escoge **Edit Ports** y aparecerá el puerto asignado para la respectiva interfaz. En la figura 7 se puede apreciar la respectiva configuración.

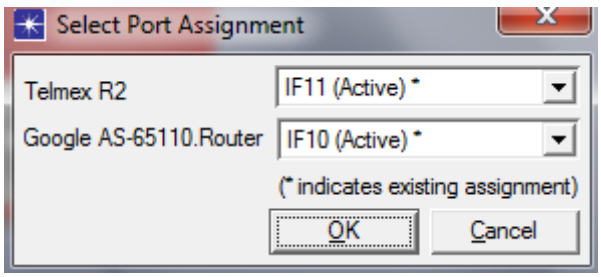


Figura 7. Configuración de puertos

VIII. Al tener claridad de los puertos asignados para cada interfaz, se procede a configurar la tabla de las interfaces de cada router y demás propiedades. Seleccione el respectivo router, presione Click derecho y escoge **Edit Attributes**. Ahora, despliegue la opción **IP**, luego **IP Routing Parameters** para obtener las respectivas opciones y configurar: **Autonomous System Number**, **Interface Information** y **Loopback Interface**.

(En este caso se utilizaron los valores predeterminados de los puertos para las interfaces de cada router). Configure cada uno de los parámetros a partir de la información establecida en las siguientes tablas para cada router.

Router Google (AS-65110)	Interface	Address	Subnet Mask	Protocol	Loopback
	IF0	192.0.1.2	255.255.255.0	RIP	192.0.25.1
	IF1	192.0.2.2	255.255.255.0	RIP	
	IF2	192.0.3.1	255.255.255.0	RIP	
	IF10	192.0.24.1	255.255.255.0	None	
	IF11	192.0.17.1	255.255.255.0	None	

Tabla 1. Configuración Router Google

Router Yahoo (AS-65120)	Interface	Address	Subnet Mask	Protocol	Loopback
	IF0	192.0.7.2	255.255.255.0	RIP	192.0.35.1
	IF1	192.0.8.2	255.255.255.0	RIP	
	IF2	192.0.9.1	255.255.255.0	RIP	
	IF10	192.0.16.2	255.255.255.0	None	

Tabla 2. Configuración Router Yahoo

Router Microsoft (AS-65130)	Interface	Address	Subnet Mask	Protocol	Loopback
	IF0	192.0.4.2	255.255.255.0	RIP	192.0.26.1
	IF1	192.0.5.2	255.255.255.0	RIP	
	IF2	192.0.6.1	255.255.255.0	RIP	
	IF10	192.0.18.1	255.255.255.0	None	
	IF11	192.0.19.1	255.255.255.0	None	

Tabla 3. Configuración Router Microsoft

Telmex Router2 (AS-65002)	Interface	Address	Subnet Mask	Protocol	Loopback
	IF10	192.0.21.1	255.255.255.0	RIP	192.0.27.1
	IF11	192.0.24.2	255.255.255.0	None	

Tabla 4. Configuración Telmex Router2

Telmex Router 1 (AS-65002)	Interface	Address	Subnet Mask	Protocol	Loopback
	IF10	192.0.20.1	255.255.255.0	None	192.0.28.1
	IF11	192.0.14.1	255.255.255.0	None	
	IF12	192.0.21.2	255.255.255.0	RIP	

Tabla 5. Configuración Telmex Router1

Telefónica Router1 (AS-65003)	Interface	Address	Subnet Mask	Protocol	Loopback
	IF10	192.0.15.1	255.255.255.0	None	192.0.30.1
	IF11	192.0.14.2	255.255.255.0	None	
	IF12	192.0.22.2	255.255.255.0	RIP	

Tabla 6. Configuración Telefónica Router1

Telefónica Router2 (AS-65003)	Interface	Address	Subnet Mask	Protocol	Loopback
	IF10	192.0.22.1	255.255.255.0	RIP	192.0.29.1
	IF11	192.0.18.2	255.255.255.0	None	

Tabla 7.Configuración Telefónica Router2

GCR1 (AS-65001)	Interface	Address	Subnet Mask	Protocol	Loopback
	IF10	192.0.13.2	255.255.255.0	RIP	192.0.34.1
	IF11	192.0.10.2	255.255.255.0	RIP	
	IF12	192.0.23.2	255.255.255.0	RIP	
	IF13	192.0.17.2	255.255.255.0	None	

Tabla 8. Configuración Router GCR1

	Interface	Address	Subnet Mask	Protocol	Loopback
GCR2 (AS-65001)	IF10	192.0.20.2	255.255.255.0	None	192.0.33.1
	IF11	192.0.12.2	255.255.255.0	RIP	
	IF12	192.0.13.1	255.255.255.0	RIP	
	IF13	192.0.15.2	255.255.255.0	None	

Tabla 9. Configuración Router GCR2

	Interface	Address	Subnet Mask	Protocol	Loopback
GCR3 (AS-65001)	IF10	192.0.11.2	255.255.255.0	RIP	192.0.32.1
	IF11	192.0.12.1	255.255.255.0	RIP	
	IF12	192.0.23.1	255.255.255.0	RIP	
	IF13	192.0.19.2	255.255.255.0	None	

Tabla 10. Configuración Router GCR3

	Interface	Address	Subnet Mask	Protocol	Loopback
GCR4 (AS-65001)	IF10	192.0.10.1	255.255.255.0	RIP	192.0.31.1
	IF11	192.0.11.1	255.255.255.0	RIP	
	IF12	192.0.16.1	255.255.255.0	None	

Tabla 11. Configuración Router GCR4

IX. Como BGP no descubre sus vecinos automáticamente, se debe configurar manualmente la tabla de vecindad para cada router y para esto se debe tener conocimiento de las interfaces de todos los routers. Seleccione el respectivo router y siga los siguientes pasos (la información de cada router se especifica en las siguientes tablas): presione Click derecho y escoge **Edit Attributes**. Despliegue la opción **IP Routing Protocols,** haga Click sobre **BGP Parameters** y ahora seleccione **Neighbors**. En la figura 8 se puede apreciar la configuración de la tabla de vecindad.

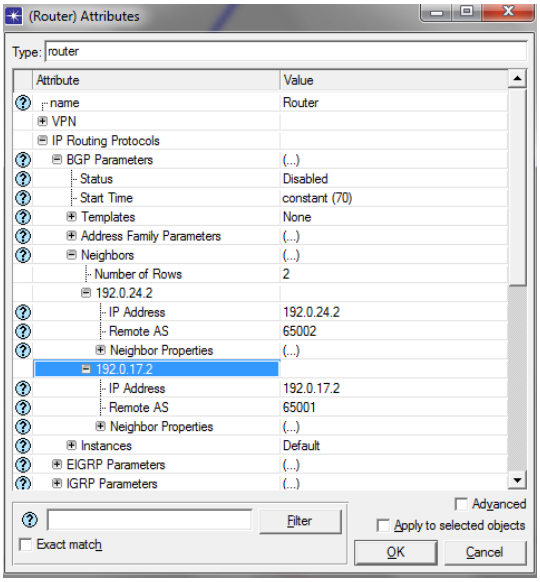


Figura 8. Configuración de la tabla de vecindad

Router Google	IP Address	Remote AS
	192.0.24.2	65002
	192.0.17.2	65001

Tabla 12. Configuración Router Google

Router Yahoo	IP Address	Remote AS
	192.0.16.1	65001

Tabla 13. Configuración Router Yahoo

Router Microsoft	IP Address	Remote AS
	192.0.18.2	65003
	192.0.19.2	65001

Tabla 14. Configuración Router Microsoft

Telmex Router1	IP Address	Remote AS
	192.0.21.1	65002
	192.0.20.2	65110
	192.0.14.2	65001

Tabla 15. Configuración Telmex Router1

Telmex Router2	IP Address	Remote AS
	192.0.21.2	65002
	192.0.24.1	65110

Tabla 16. Configuración Telmex Router2

Telefónica Router1	IP Address	Remote AS
	192.0.22.1	65003
	192.0.14.1	65002
	192.0.15.2	65001

Tabla 17. Configuración Telefónica Router1

Telefónica Router2	IP Address	Remote AS
	192.0.21.2	65003
	192.0.18.1	65130

Tabla 18. Configuración Telefónica Router 2

GCR1	IP Address	Remote AS
	192.0.13.1	65001
	192.0.23.1	65001
	192.0.10.1	65001
	192.0.17.1	65110

Tabla 19. Configuración Router GCR1

GCR2	IP Address	Remote AS
	192.0.12.1	65001
	192.0.13.2	65001
	192.0.15.1	65003
	192.0.20.1	65002

Tabla 20. Configuración Router GCR2

GCR3	IP Address	Remote AS
	192.0.12.2	65001
	192.0.23.2	65001
	192.0.11.1	65001
	192.0.19.1	65120

Tabla 21. Configuración Router GCR3

GCR4	IP Address	Remote AS
	192.0.11.2	65001
	192.0.10.2	65001
	192.0.16.2	65120

Tabla 22. Configuración Router GCR4

X. Es necesario establecer las parejas de vecindad (IBGP y EBGP) para cada uno de los routers que se encuentran dentro y fuera de cada sistema autónomo. Ahora, seleccione para cada pareja de routers que se encuentran dentro de cada AS, por ejemplo: TelmexR1- TelmexR2 y despliegue en la barra de menú la opción **IP**, seleccione **BGP** y por último escoge **IBGP Peers.** Repita este mismo paso para las parejas de Routers situados en diferentes ASs con la opción **EBGP Peers**, por ejemplo: TelmexR1-TelefonicaR1.

XI. Para habilitar la opción de *Route Redistribution* despliegue en la barra de menú la opción **IP**, seleccione **BGP** y por último escoge **Configure Route Redistribution,** aparecerá la ventana de configuración y para esto cambie el campo *Status* perteneciente a Directly Conneted por **Enabled.** Adicionalmente deshabilite la opción *Synchronization Status* para todos los routers.

XII. Ahora, es necesario verificar la adecuada configuración de la red de enrutamiento. Despliegue en la barra de menú la opción **View,** seleccione **Visualize Protocol Configuration**, luego escoja **IP Routing Protocols** y por último **IPv4 Routing Protocols.** De esta manera en la figura 9 se puede

apreciar cómo es posible visualizar qué protocolos de enrutamiento están corriendo en la red. Los protocolos IGP se muestran sobre los enlaces, puesto que su configuración es por interfaz. El enrutamiento BGP se indica en el *router* al igual que la redistribución debido a que BGP y la redistribución no están asociados a un enlace.

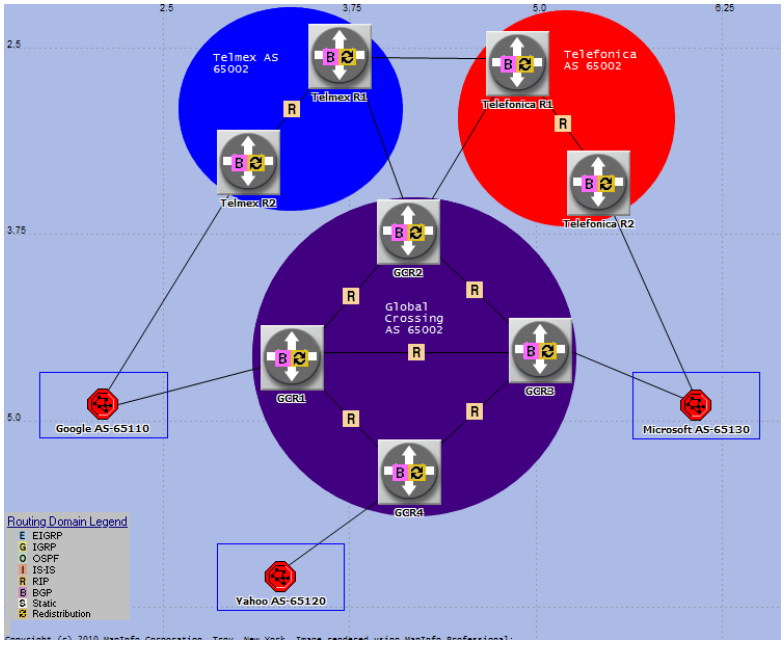


Figura 9. Visualización de protocolos de enrutamiento y la redistribución

XIII. El otro análisis que se debe realizar ara verificar la configuración de BGP consiste en visualizar los vecinos BGP. Despliegue de nuevo en la barra de menú la opción **View,** seleccione **Visualize Protocol Configuration** y luego escoja **BGP Peers.** En la figura 10 se muestra los vecinos BGP en donde se ha pintando de un color distinto los vecinos IBGP y los EBGP.

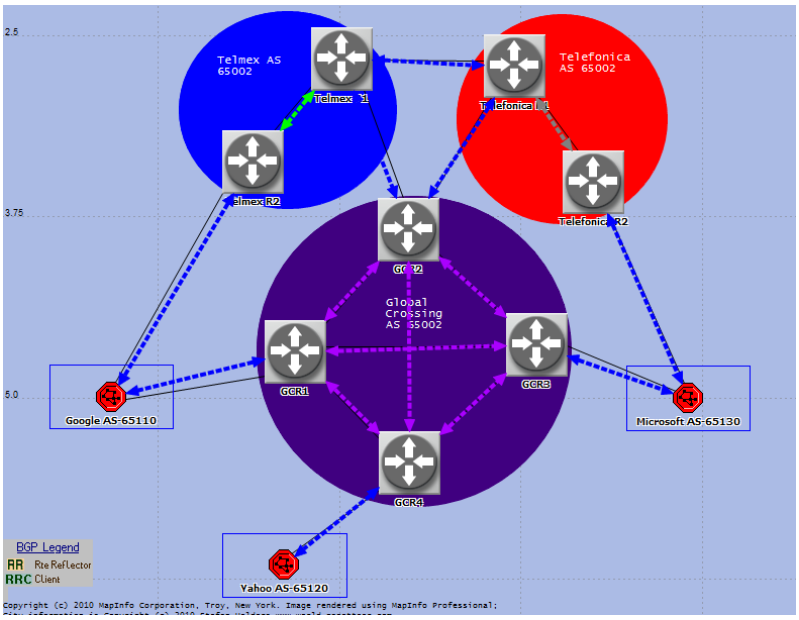


Figura 10. Visualización IBGP y EBGP Peers

XIV. En la paleta de diálogo seleccione los objetos **Application Definitions** y **Profile Deffinitions,** y sitúelos en el espacio de trabajo.

XV. A continuación se procede a configurar **Applications Definition**, haga click sobre este objeto y seleccione **Edit Attributes**; busque la opción **Application Definition,** oprima click sobre **(…)** y seleccione **Edit,** aparecerá la ventana de configuración y en la parte inferior agregue **2 rows,** luego edite el nombre para cada aplicación por EMAIL y HTTP. Ahora, haga click sobre el campo de Description para cada aplicación y edite lo siguiente: Para la aplicación EMAIL, seleccione **Email** que tiene por defecto el valor **Off,** busque **High Load** y para la aplicación HTTP, seleccione **Http** que tiene por defecto el valor **Off,** busque **Heavy Browsing**. En la figura 11 se puede apreciar la respectiva configuración.

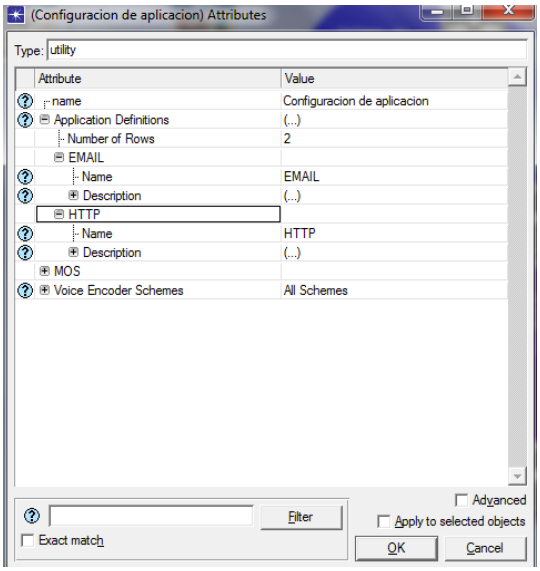


Figura 11. Configuración de aplicaciones

XVI. Para configurar **Profile Definition**, se oprime click sobre este objeto y seleccione **Edit Attributes**; busque la opción **Profile Configuration,** oprima click sobre **None**, busque **edit,** aparece una tabla y agreguele **2 rows**. Modifique el **Profile Name** de un row por HTTP & EMAIL y el otro row por HTTP. En la figura 12 se puede apreciar la respectiva configuración.

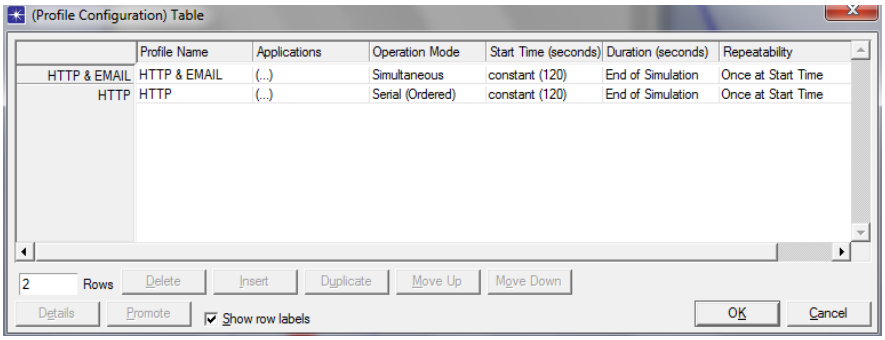


Figura 12. Configuración del perfil

XVII. Luego, En la opción **Applications** de **Http & EMAIL**, que se encuentra en **(Profile Configuration Table)** y esta por defecto en el valor **None,** busque **edit**,

aparecera una tabla, y agregue **2 row**. Para cada row modifique la opción **Name** por EMAIL y el otro por HTTP. Presiones ok.

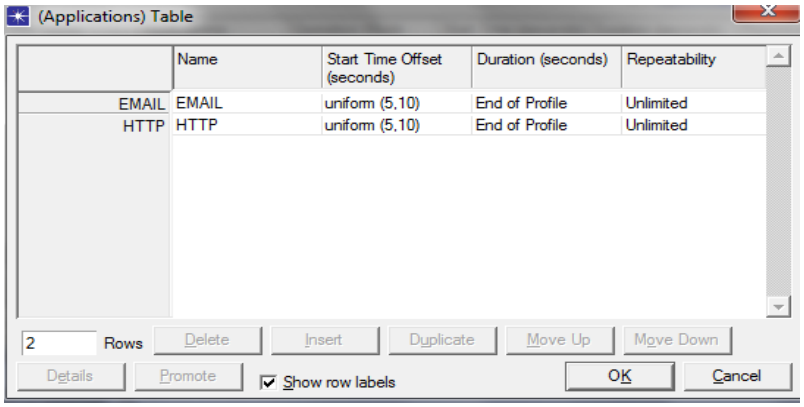


Figura 13. Aplicaciones

XVIII. Ahora para habilitar las configuraciones que se hicieron en el punto anterior se realiza lo siguiente: Ubíquese en red LAN Ventas de la corporación Google AS-65110 **,** oprima click derecho y busque **Edit Attributes,** despliegue el menú **Applications,** seleccione **Application: Supported Profiles,** que se encuentra con el valor **None,** al oprimir en **edit** se abrirá una ventana, agregue **1 Rows,** coloque en *Profile name* **HTTP & EMAIL** y verifique en la opción **Application Delay Tracking** que esté habilitado. Ahora seleccione la opción **Application: Supported Services,** y asigne el valor **All,** finalice presionando Ok. En la figura 14 y 15 se aprecia la respectiva configuración. Repita este paso para configurar las redes LAN de las otras corporaciones.

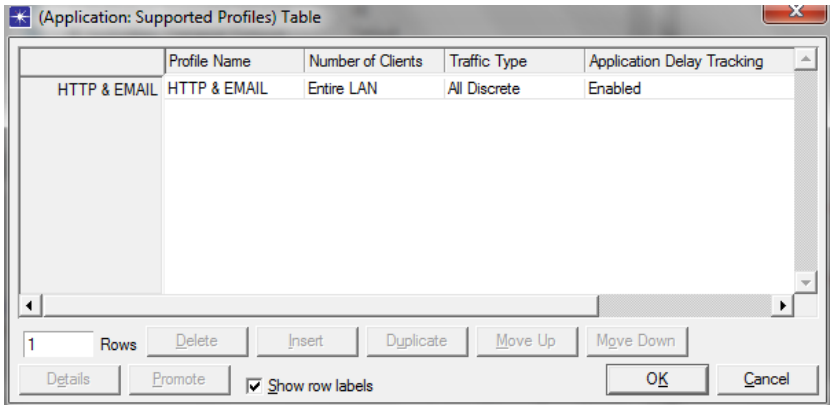


Figura 14. Habilitación de las Aplicaciones

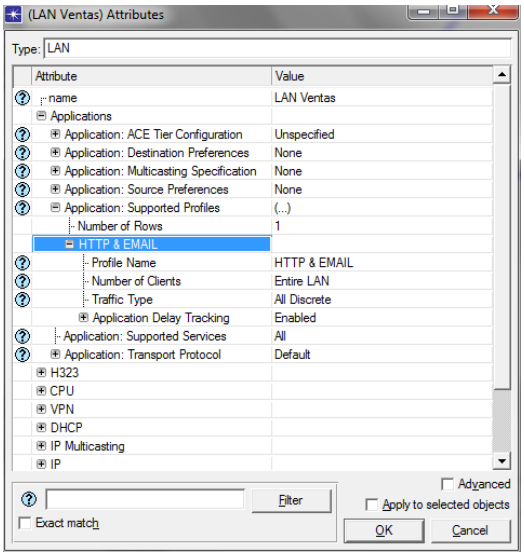


Figura 15. Verificación de Application Delay Tracking

XIX. Ahora se habilita el soporte en cada servidor de la siguiente manera: En **Servidor de correo** oprima click derecho y busque **Edit Attributes,** despliegue el menú **Applications,** seleccione **Application: Supported Services,** y habilite la opción **All.**

XX. En el escenario principal, realice click derecho, seleccione la opción **Choose individual DES statistics,** desplegué el menú **Link Statistics,** busque y

seleccione lo siguiente; **point-to-point** y habilite **throughput(bits/sec)- ->, throughput(bits/sec) <- -.** Luego seleccione **Node Statistics** y habilite **Email y HTTP**.

2.3 Ejecutar la simulación y ver los resultados:

I. Despliegue el menú **Scenarios** y seleccione **Manage Scenarios**, luego en el campo de **results** cambie la opción para el escenario por **collect** o **recollect**. Ahora para establecer el tiempo de la simulación; en el campo **Sim Duration** escribe 10 y en **Time Units** escoge **min**, haga click en **Ok**. Al finalizar presione **Close** y salve el proyecto.

II. Para ver los resultados seleccione **View Results.**

III. Seleccione los enlaces que unen el Router de la corporación de *Google* con el *Router GCR1* y el *Router TelmexR2*. De esta manera se puede apreciar en la figura 16 que prácticamente no hay tráfico entre el enlace que une al Router de la corporación de Google con el Router TelmexR2; basado en el ancho de banda.

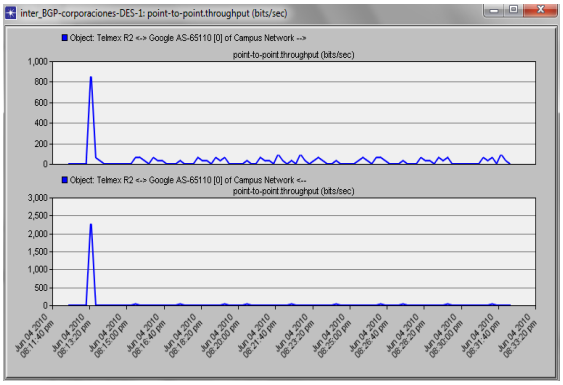


Figura 16. Ancho de banda entre el router de la corporación Google y TelmexR2

En la figura 17 se aprecia la existencia de tráfico entre el enlace que une al router de la corporación de Google con el Router GCR1. Ya que en este caso a pesar que la corporación está conectada con dos ISP, solamente empleará uno de sus enlaces para enviar todo este tráfico. El enlace que emplea el sistema autónomo de Google es el que lo conecta con Global Crossing. Por defecto BGP considera la mejor ruta a la ruta que está compuesta por el menor número de sistemas autónomos. Para enviar tráfico de Google hacia Yahoo se considera la ruta a través de Global Crossing al igual que para enviar tráfico de Google a Microsoft.

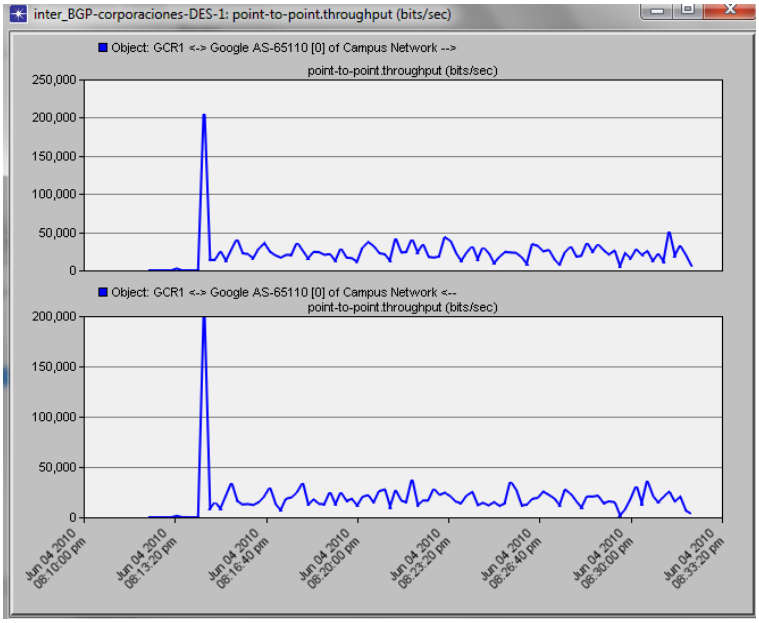


Figura 17. Ancho de banda entre el router de la corporación Google y el Router GCR1

En la figura 18 se puede apreciar el tráfico generado de la red LAN Administración en la corporación de Google.

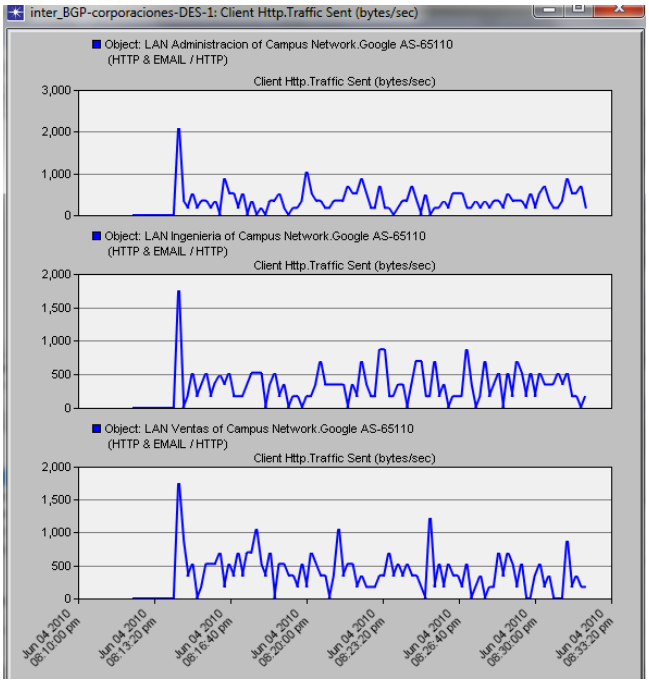


Figura 17. Tráfico generado (LAN Administración)

Trabajo en clase:

1. Genere y analice las tablas de enrutamiento para los routers: GCR1, TelmexR2 y el router de la corporación Google.

2. ¿Qué otros atributos existen para describir la métrica del protocolo BGP?

3. Plantee una situación de avería sobre el enlace que une a los Routers GCR1 y GCR2. Analice el tráfico y el ancho de banda sobre los enlaces.

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE INGENIERÍA Y ADMINISTRACIÓN
PROGRAMA DE INGENIERÍA ELECTRÓNICA
REDES DE COMPUTADORES (OPTATIVA)

ANEXO 5

GUÍA PRÁCTICA SOBRE PROTOCOLOS DE ENRUTAMIENTO EN LA RED

Práctica N°5

TÍTULO: APLICACIÓN DEL PROTOCOLO OSPF PARA DESARROLLAR INGENIERÍA DE TRÁFICO

OBJETIVOS:

- Implementar y configurar una red basada en las características del protocolo de enrutamiento OSPF, para analizar las formas de desarrollo de Ingeniería de Tráfico.
- Distribuir los pesos de los enlaces para crear rutas alternativas ante la demanda de tráfico.
- Configurar los routers para garantizar el balanceo de carga y así obtener las rutas más cortas; de igual y más bajo costo.
- Analizar las tablas de enrutamiento de los routers.

1. MARCO TEÓRICO

Se debe tener en cuenta que como mínimo, el ancho de banda de un enlace es de gran importancia para efectos de aplicar la ingeniería de tráfico. Además, un enlace puede permitir mayor ancho de banda reservado debido al aumento anunciado de multiplexado estadístico para determinados tipos de tráfico, lo que significa que el número de ofertas puede ser tolerable. También, un enlace podrá

tener un ancho de banda en la actualidad sin reservas, el cual es útil para los cálculos de los caminos de enrutamiento, pero que no necesariamente se basa en un cálculo de la ruta más corta. Dado que una red puede proporcionar más de un tipo de servicios priorizados, sería útil anunciar el ancho de banda sin reserva permitido para cada clase de prioridad. Además, un proveedor de red puede utilizar una métrica diferente, distinta a la relación métrica estándar; ésta métrica del enlace podría tener un significado interno es decir solamente para el proveedor.

En resumen se debe considerar para un enlace:

- Máximo ancho de banda del enlace que se puede utilizar.
- Máxima reserva de ancho de banda en caso de permitirse múltiples demandas.
- Ancho de banda sin ser reservado disponible en diferentes niveles de prioridad.
- Métricas de ingeniería de tráfico.

La pregunta es: ¿Cómo es comunicada esta información?

Esto da lugar a la aparición de dos protocolos de enrutamiento de estados de enlace denominados OSPF / IS-IS. Estos dos protocolos se han ampliado para tener en cuenta las consideraciones anteriores para un determinado enlace.

2. PROCEDIMIENTO:

A continuación veremos en la figura 1 el diseño de la topología de red que emplearemos en la simulación, seguido de los pasos para desarrollar la práctica.

Elementos:

- **Router IP (slip8_gtwy):** El modelo representa un nodo slip8_gtwy, el cual opera como una puerta de enlace IP y contiene 8 interfaces de línea seriales a una velocidad seleccionable. Los paquetes IP que llegan a cualquier interfaz son enrutados a la interfaz de salida adecuada en función de su dirección IP de destino.

- **Ping Parameters:** Define diferentes opciones de configuración que sólo los routers/hosts pueden usar para determinar la conectividad al destino especificado garantizando que el nivel de red funciona adecuadamente. De esta forma *ping* confirma que un paquete IP es capaz de alcazar la máquina destino y que ese mismo paquete IP es capaz de volver a la máquina origen.

- **Link (PPP_DS3):** Enlace que utiliza el protocolo PPP y que tiene una capacidad de 44,736 Mbps.

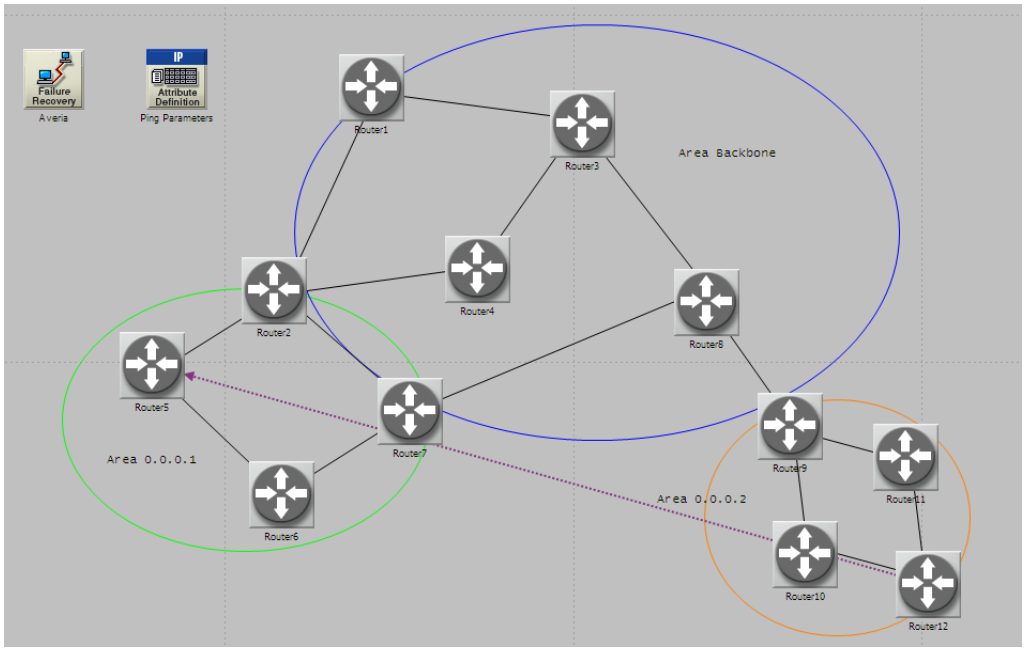


Figura 1. Arquitectura de la red utilizando el protocolo OSPF para desarrollar Ingeniería de Tráfico

2.1 Creación del proyecto:

I. Inicie el simulador Opnet Modeler, para la creación del nuevo proyecto elija en la barra de menú la opción **File** y seleccione **New** para crear el proyecto, luego dale Click en **Project** y por último **Ok**. Ahora dele nombre al proyecto, por ejemplo: *tu nombre_OSPF,* luego al escenario a crear dele el nombre *Ruta_uno*, presione **Ok.** Aparecerá la ventana de *Startup Wizard,* haga Click en **Next** para elegir el área sobre el cual se desea crear la arquitectura de red, seleccione la opción **Campus** y presione **Next,** ahora para adecuar el tamaño de la red; coloque en el campo **x**=**100** y **y=100**. Finalmente dele **Next** dos veces y luego **Finish.**

2.2 Creación y configuración de la red:

I. Seguidamente aparecerá la paleta de dialogo (Object Pallete), el cual permitirá acceder a los elementos de trabajo para el diseño de la red, en caso de que no aparezca pulse en la barra de menú el botón  .Al desplegarlo es necesario que la opción **internet tool_box** esté seleccionado.

II. En la paleta de diálogo seleccione el router **slip8_gtwy** y sitúe 12 de estos mismos en el espacio de trabajo presionando Click izquierdo (para terminar de colocar los objetos presione Click derecho). Utilice el enlace **PPP_DS3** para conectar los routers y renómbrelos como aparece en la figura 2, para esto debe dar Click derecho sobre el objeto y seleccione **Set Name.** En la figura 2 veremos la respectiva conexión.

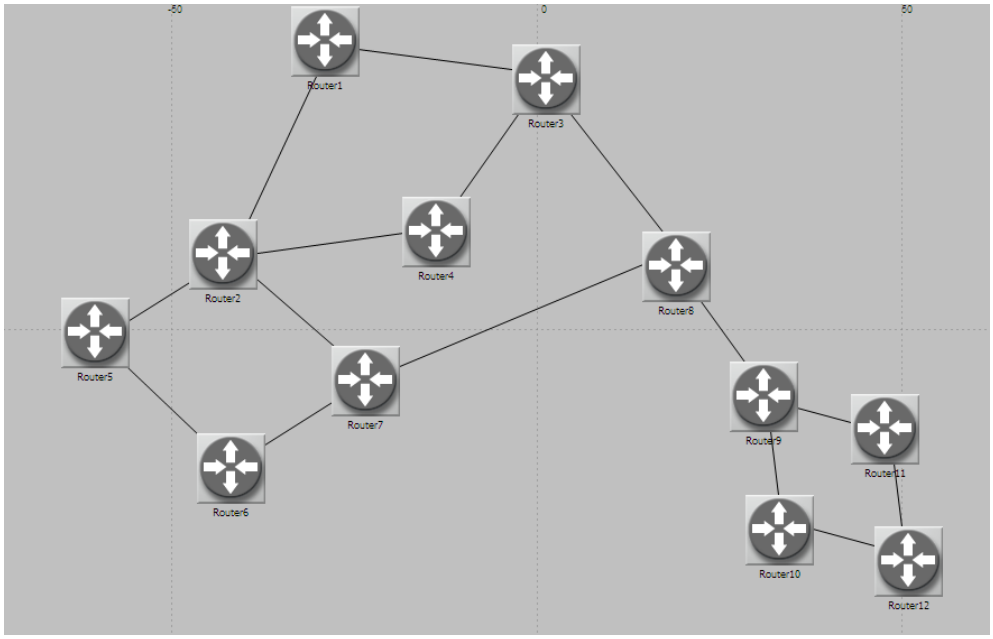


Figura 2. Conexión de los routers slip8_gtwy utilizando el enlace PPP_DS3.

III. Salve el proyecto y designe el protocolo de enrutamiento desplegando en la barra de menú la opción **Protocols**, seleccione **Routing** y luego **Configure Routing Protocols**. Ahora deshabilite el protocolo **RIP** y escoja el protocolo **OSPF**, presione **Ok**.

IV. En la figura 3 se puede ver el procedimiento de configuración del protocolo de enrutamiento OSPF y en la figura 4 la visualización de este protocolo sobre los enlaces de la red; habilitando la opción **Visualize routing domains** en la ventana **Routing Protocol Configuration**. Para quitar la visualización del uso del protocolo OSPF sobre los enlaces pulse *Ctrl*+*Shift*+*C*.

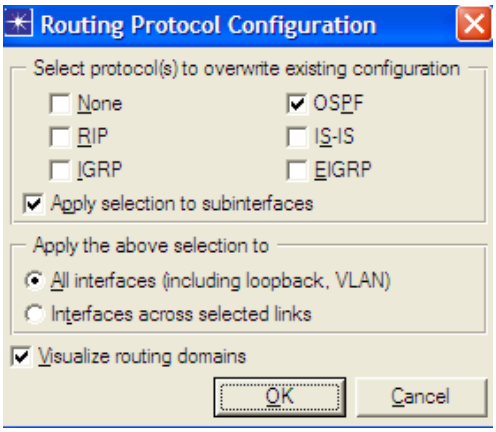


Figura 3. Configuración del protocolo de enrutamiento (OSPF)

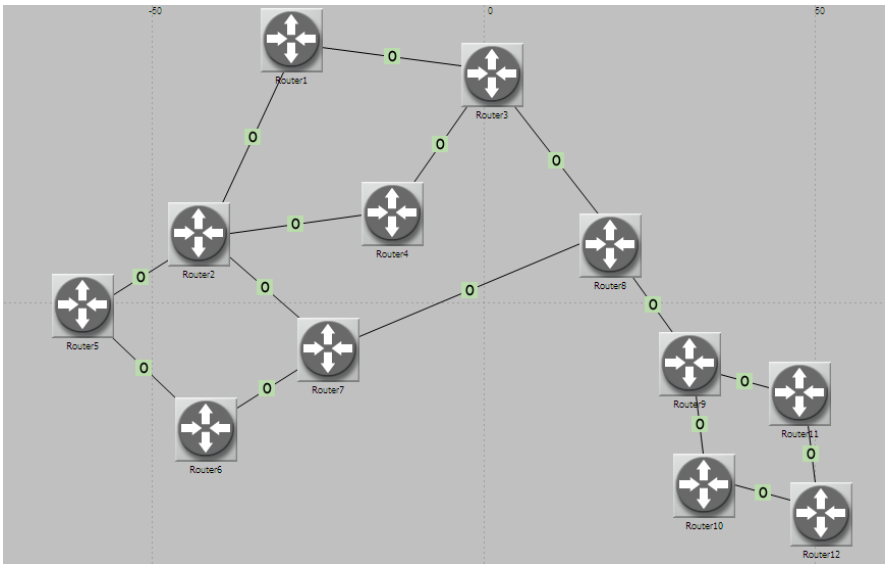


Figura 4. Visualización del protocolo OSPF utilizando la opción Routing Domain Legend

V. Para asignar una única dirección IP a las interfaces IP conectadas; debe desplegar en la barra de menú la opción **Protocols**, seleccione **IP**, luego **Addressing** y por último haga Click en **Auto Assign IP Addresses**.

VI. Al igual que muchos routers comerciales, los modelos de routers de OPNET aceptan un parámetro llamado *reference bandwith* para calcular el coste real:

Coste = (*Reference bandwith*)/(Ancho de banda del enlace)

De esta manera se realiza la configuración de este parámetro como ya se había mencionado en la práctica de OSPF.

Ahora seleccione los enlaces indicados en la tabla 1, tabla 2 y tabla 3, asigne el respectivo *Bandwidth,* para esto debe desplegar en la barra de menú la opción **Protocols**, seleccione **IP**, luego haga Click en **Routing** y por último escoge **Configure Interface Metric Information**.

Enlace	Bandwidth (Kbps)
Router 1 - Router 3	50000
Router 2 - Router 5	50000
Router 2 - Router 7	50000
Router 2 - Router 4	50000
Router 3 - Router 8	50000
Router 8 - Router 9	50000
Router 9 - Router 10	50000

Tabla 1. Coste de los enlaces para un valor de 20

Enlace	Bandwidth (Kbps)
Router 9 - Router 11	200000

Tabla 2.Coste de los enlaces para un valor de 5

Enlace	Bandwidth (Kbps)
Router 1 - Router 2	100000
Router 3 - Router 4	100000
Router 5 - Router 6	100000
Router 6 - Router 7	100000
Router 10 - Router 12	100000
Router 11 - Router 12	100000

Tabla 3. Costo de los enlaces para un valor de 10

VII. Una forma de visualizar y confirmar los valores establecidos sobre los enlaces es hacer que se muestren los valores de los pesos en la topología de red. Para ello despliegue en la barra de menú la opción **View**, seleccione **Visualize Protocol Configuration**, seleccione **IPv4 Interface Metrics** y por último dele Click sobre **OSPF Metrics**. De esta manera aparecerá el valor asignado sobre cada enlace, como se aprecia en la figura 5. Para quitar la visualización del coste sobre los enlaces pulse *Ctrl+Shift+C*.

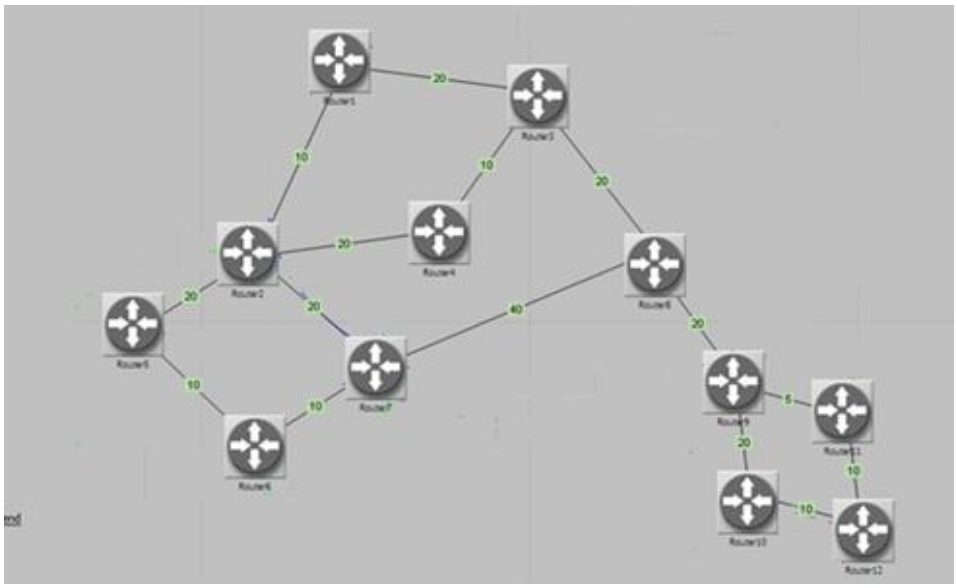


Figura 5. Valores asignados sobre los enlaces

VIII. Seleccione los enlaces que aparecen a continuación en la Tabla 4, para dividir la jerarquía de la red en áreas e identificarlas.

Enlace
Router 2 - Router 5
Router 5 - Router 6
Router 6 - Router 7
Router 2 - Router 7

Tabla 4. Representación del área 0.0.0.1

IX. Ahora despliegue en la barra de menú la opción **Protocols**, seleccione **OSPF** y por último **Configure Areas**. Aparecerá una ventana y en el campo de **Area identifier** escriba **0.0.0.1**

X. Seleccione los siguientes enlaces que aparecen en la Tabla 5, repita el paso 2 y escriba en el parámetro **Area identifier** el valor **0.0.0.0** (backbone).

Enlace
Router 1 - Router 2
Router 1 - Router 3
Router 2 - Router 4
Router 3 - Router 4
Router 7 – Router 8
Router 3 – Router 8
Router 8 – Router 9

Tabla 5. Representación del área 0.0.0.0

XI. Seleccione los siguientes enlaces que aparecen en la Tabla 6, repite el paso 2 y escribe en Area identifier 0.0.0.2.

Enlace
Router 9 - Router 10
Router 9 - Router 11
Router 10 - Router 12
Router 11 - Router 12

Tabla 6. Representación del área 0.0.0.2

XII. Para observar las respectivas áreas despliegue **View** en la barra de menú, seleccione **Vizualize Protocol Configuration**, luego haga Click sobre **OSPF** y finalmente seleccione la opción **Area Configuration**. Aparecerá una ventana

con las respectivas áreas y su identificación; puede asignarle un color a cada área para distinguirlas. En la figura 6 se puede ver la asignación del color para cada área.

También puede utilizar las herramientas de **Annotation Pallete** como se ha hecho en las guías anteriores para identificar las áreas, ver figura 7.

(Si desea quitar la visualización de la división de áreas *Ctrl+Shift+C*)

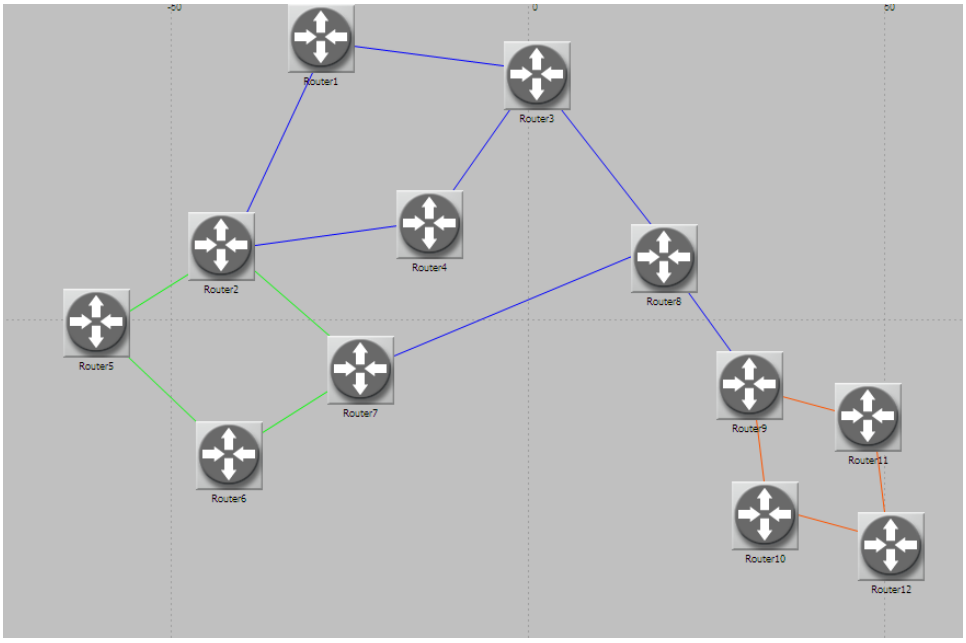


Figura 6. Asignación de áreas e identificación de estas mismas basadas en el color de los enlaces.

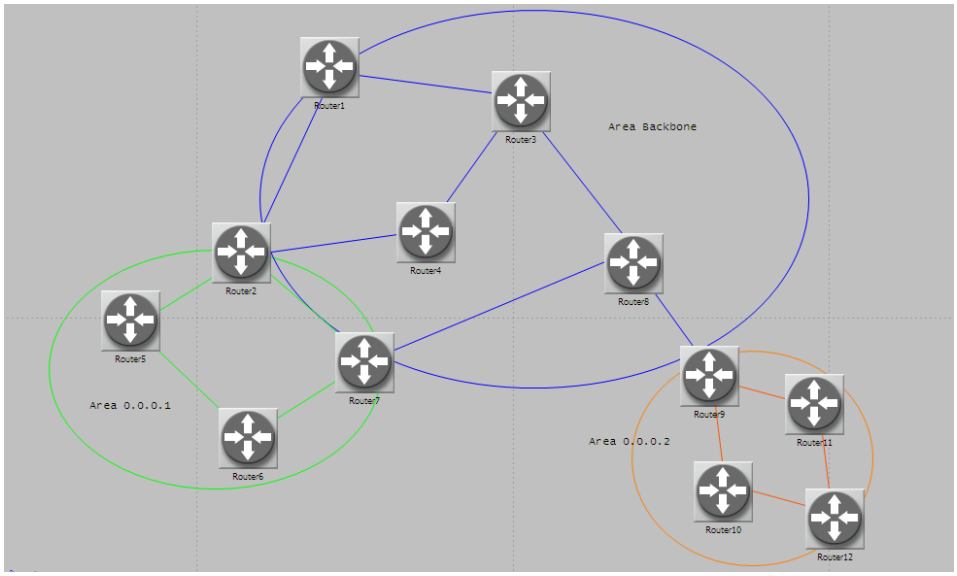


Figura 7. Identificación de áreas utilizando la herramienta Annotation Pallete

XIII. Ahora para crear la demanda de tráfico seleccione los **Routers 12** y **5**, presionando Shift y dando Click sobre ellos. Luego, en la barra de menú despliegue la opción **Protocols**, seleccione **IP**, seguidamente **Demands** y por último **Configure Ping Traffic on Selected Nodes**. Aparecerá una ventana para seleccionar el origen y destino de la demanda de tráfico, seleccione **From 12** y presione **Ok**. Salve el proyecto.

XIV. En la figura 8 se puede ver el procedimiento de configuración de la demanda de tráfico y en la figura 9 la visualización de este mismo entre los routers; además la representación del objeto **Ping Parameters** en el área de trabajo.

Figura 8. Configuración de la demanda de tráfico

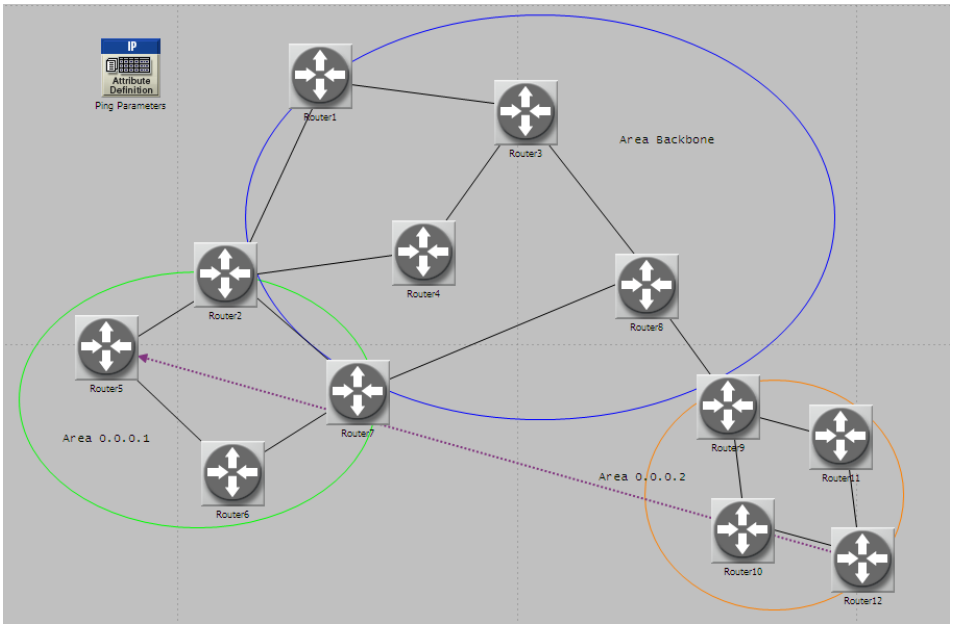


Figura 9. Representación de la demanda de tráfico entre los Routers 12 y 5.

XV. Ahora, se debe configurar los parámetros a analizar. Presione Click derecho sobre el espacio de trabajo y escoja **Choose Individual DES Statistics**, aparecerá la ventana de *Choose Results* y seleccione **Link Statistics**, escoja

Point to Point y habilite las opciones **throughput (bits/sec)** y **Utilization**. En la figura 10 se puede apreciar la respectiva configuración.

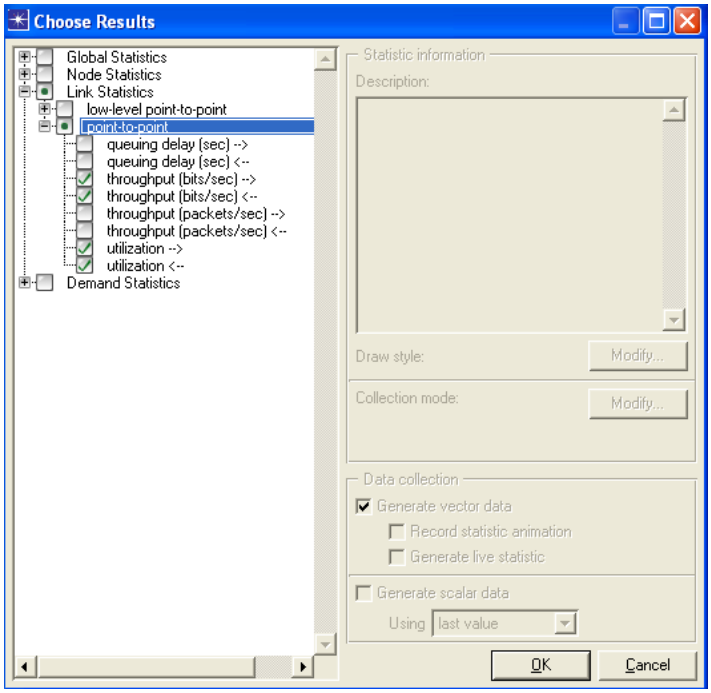


Figura 10. Configuración de Choose DES Individual Statistics

XVI. Luego, aplique la opción para exportar las tablas de enrutamiento de cada router; despliegue en la barra de menú la opción **Protocols**, seleccione **IP**, escoja **Routing** y por último dele Click en **Export Routing Table** *(all nodes*)**.**

XVII. Salve el proyecto

2.3 Creación de un nuevo escenario (Ruta_alternativa):

I. En la barra de menú despliegue **Scenarios** y seleccione **Duplicate Scenario** (llámelo **Ruta_alternativa**), presione Ok.

II. Es necesario que compruebe que las configuraciones básicas establecidas en el escenario *Ruta_uno* se encuentren aún para este nuevo escenario (de lo contrario, no los cambie): asignación del protocolo de enrutamiento, direcciones de las interfaces, exportar la tabla de enrutamiento de los routers y los parámetros choose individual DES statistics.

III. Seleccione **Object Palette**  y escoja el objeto **Failure Recovery** (si no aparece, escriba en **Search by name** el nombre de este objeto) , sitúelo en el espacio de trabajo y llámelo **Avería**, ahora dele Click derecho sobre el objeto y escoja **Edit Atributes**, al frente de **Link Failure/Recovery Specification** escoja **Edit** y dele Click en **Insert**, al hacer esto **Number of rows** se pone en 1, ahora cambie **Time (seconds)** por 200 segundos y en **Name** seleccione **Campus Network.Router7<>Router8**; esto hará que en el enlace entre los Routers 7 y 8 ocurra un daño 200 segundos después de comenzar la simulación; por último dele **Ok** y salve el proyecto.

IV. Salve el proyecto.

2.4 Creación de un nuevo escenario (Balanceo_Averia):

I. En la barra de menú despliegue **Scenarios** y seleccione **Duplicate Scenario** (llámelo **Balanceo_Averia**), presione Ok.

II. Compruebe de nuevo las configuraciones hechas en el escenario *Ruta_alternativa* para este nuevo escenario.

III. Una de las características del protocolo OSPF es la capacidad para el balanceo de carga a través de caminos de igual costo, asigne esta configuración sobre los **Routers 2 y 3**, para esto despliegue en la barra de menú la opción **Protocols**, seleccione **IP**, escoja **Routing** y por último **Configure Load**

Balancing Options. Aparecerá una ventana, asigne **Packet Based** y habilite **Selected routers.**

IV. Salve el proyecto.

2.5 Creación de un nuevo escenario (Distribucion_Averia):

I. En la barra de menú despliegue **Scenarios** y seleccione **Duplicate Scenario** (llámelo **Distribucion_Averia**), presione Ok.

II. Compruebe de nuevo las configuraciones hechas en el escenario *Balanaceo_Averia* para este nuevo escenario.

III. Seleccione los enlaces indicados en la tabla 7 y asigne el respectivo *Bandwidth,* para esto debe desplegar en la barra de menú la opción **Protocols**, seleccione **IP**, luego dale Click en **Routing** y por último escoja **Configure Interface Metric Information**. En la figura 11 se puede apreciar la respectiva asignación de los valores sobre los enlaces.

Enlace	Bandwidth (Kbps)
Router 5 - Router 6	200000
Router 6 - Router 7	200000
Router 10 - Router 12	200000
Router 1 – Router 2	100000
Router 11 - Router 12	100000
Router 1 - Router 3	50000
Router 3 - Router 8	50000
Router 2 - Router 7	50000
Router 2 - Router 4	50000
Router 8 - Router 9	50000

Router 9 - Router 11	50000
Router 9 - Router 10	50000
Router 7 - Router 8	250000
Router 2 - Router 5	250000

Tabla 7. Costo de los enlaces

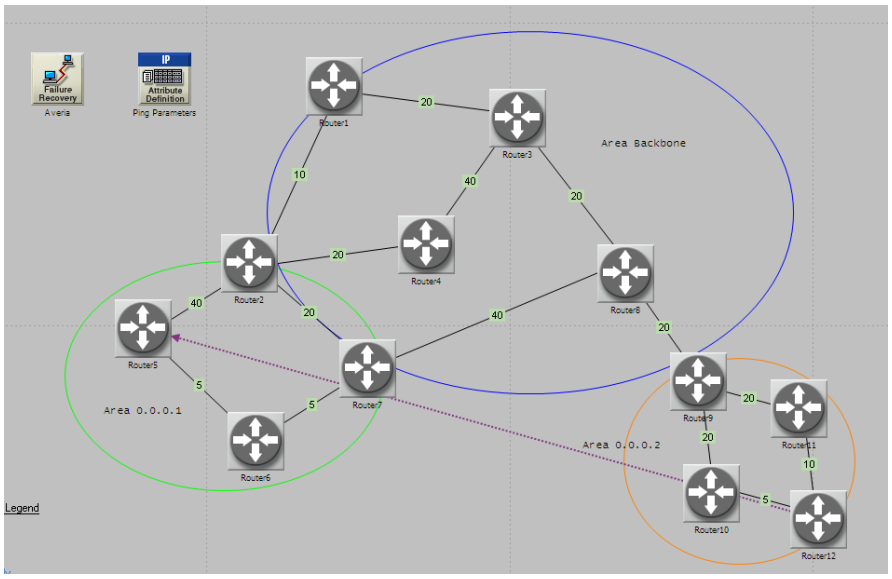


Figura 11. Asignación de pesos sobre los enlaces

IV. Salve el proyecto

2.6 Ejecutar la simulación y ver los resultados:

1. En la barra de menú despliegue **Scenarios**, seleccione **Switch to scenario** y escoja *Ruta_uno.*

2. A continuación, se debe generar la carga de tráfico. Para esto se generaran flujos entre todos los nodos. Despliegue en la barra de menú la opción **Traffic**,

seleccione **Create Traffic Flows,** luego **IP** y por último **Unicast Full mesh between all nodes**, presione **Create**.

3. Despliegue el menú **Scenarios** y seleccione **Manage Scenarios**, luego en el campo de **results** cambie la opción para cada escenario por **collect** o **recollect**. Ahora para establecer el tiempo de la simulación; en el campo **Sim Duration** escriba 10 y en **Time Units** escoja **min**, haga Click en **Ok**. Al finalizar presione **Close** y salve el proyecto.

4. Ahora, seleccione de nuevo la opción **Traffic** y escoja **Open Traffic Center** para ver el flujo de tráfico. Aparecerá la ventana de **Traffic center** y habilite la carpeta **Flow.**

5. Cierre la ventana de **Traffic center** y en la barra de menú despliegue la opción **Protocols**, seleccione **IP**, escoja **Demands** y ahora **Display Routes for Configure Demands** (aparecerá la ventana **Route Report for IP Traffic Flows**), ahora despliegue la opción **Router 12** y ahí mismo seleccione **Router 5**. Para ver el flujo de tráfico del escenario *Ruta_uno* cambie el campo de **Display** por **Yes.** En la figura 12 se puede apreciar la respectiva configuración y en la figura 13 se muestra la ruta obtenida en base a las características del protocolo OSPF. (Note que es la ruta más corta y de más bajo costo)

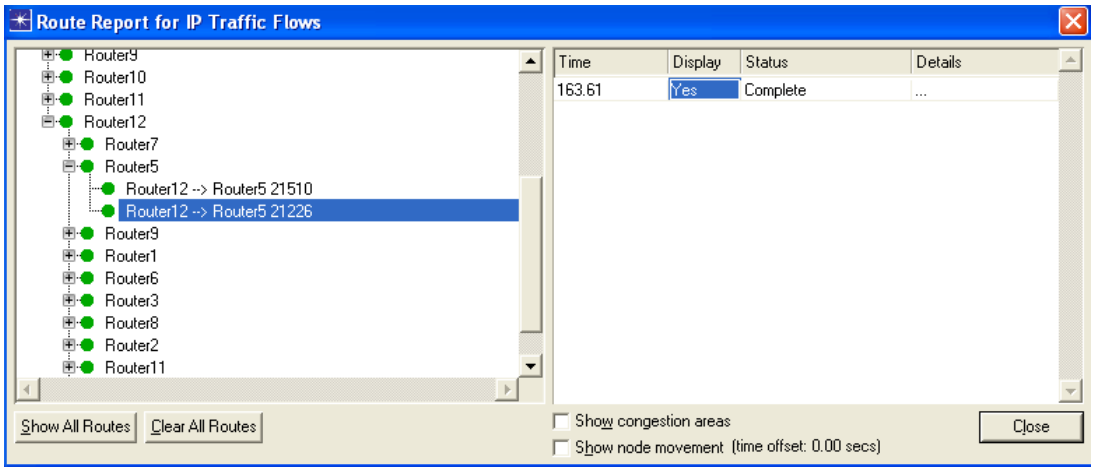


Figura 12. Configuración de Route Report

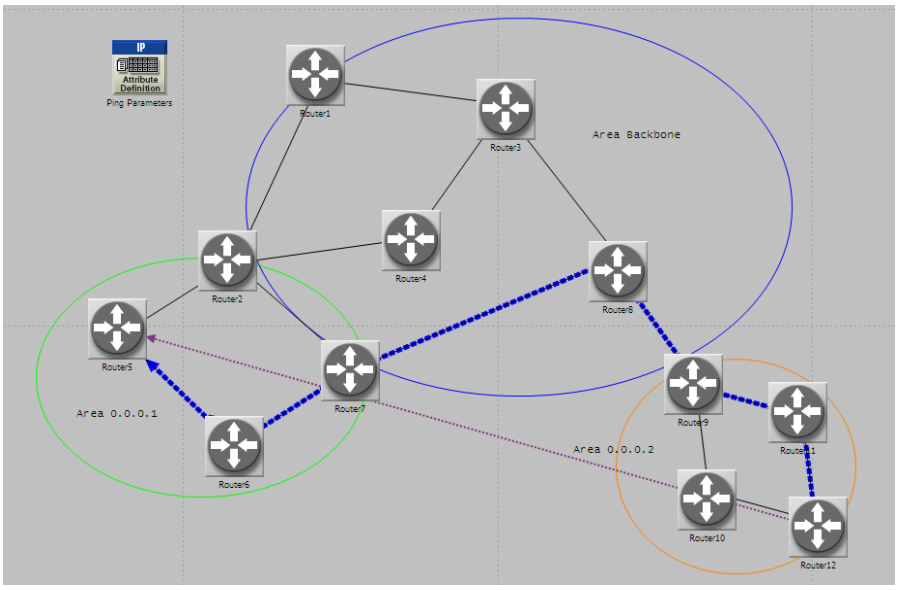


Figura 13. Ruta corta y de más bajo costo (OSPF)

6. Seleccione la opción *View Results* para analizar el ancho de banda entre los Routers 8 y 7, como se puede apreciar en la figura 14.

También obtenga la tabla de enrutamiento del Router 12 como se puede ver en figura 15.

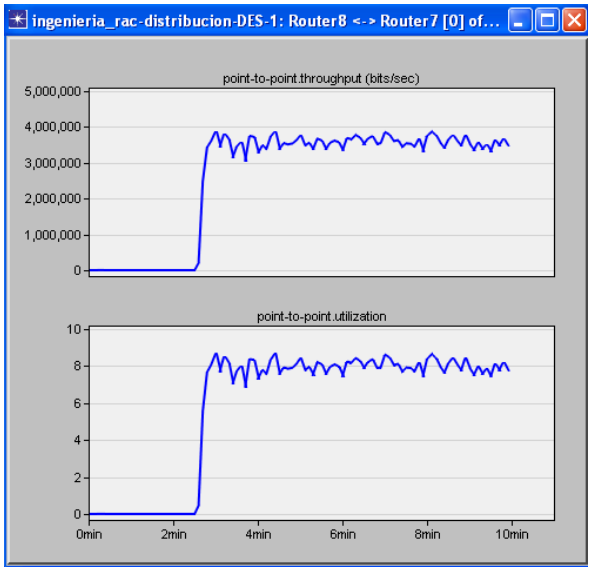


Figura14. Ancho de banda y utilización del enlace entre los Routers 8 y 7

Performance.IP Forwarding Table at End of Simulation for Campus Network.Router12

File Edit View Help

	Destination	Source Protocol	Route Preference	Metric	Next Hop Address	Next Hop Node	Outgoing Interface	Outgoing LSP	Insertion Time (secs)
1	192.0.1.0/24	OSPF 1	110	65	192.0.13.2	Campus Network.Router11	IF1	N/A	32.299
2	192.0.2.0/24	OSPF 1	110	75	192.0.13.2	Campus Network.Router11	IF1	N/A	32.299
3	192.0.3.0/24	OSPF 1	110	55	192.0.13.2	Campus Network.Router11	IF1	N/A	32.299
4	192.0.4.0/24	OSPF 1	110	75	192.0.13.2	Campus Network.Router11	IF1	N/A	32.299
5	192.0.5.0/24	OSPF 1	110	95	192.0.13.2	Campus Network.Router11	IF1	N/A	32.299
6	192.0.6.0/24	OSPF 1	110	85	192.0.13.2	Campus Network.Router11	IF1	N/A	32.299
7	192.0.7.0/24	OSPF 1	110	85	192.0.13.2	Campus Network.Router11	IF1	N/A	32.299
8	192.0.8.0/24	OSPF 1	110	105	192.0.13.2	Campus Network.Router11	IF1	N/A	32.299
9	192.0.9.0/24	OSPF 1	110	95	192.0.13.2	Campus Network.Router11	IF1	N/A	32.299
10	192.0.10.0/24	OSPF 1	110	85	192.0.13.2	Campus Network.Router11	IF1	N/A	32.299
11	192.0.11.0/24	OSPF 1	110	35	192.0.13.2	Campus Network.Router11	IF1	N/A	32.299
12	192.0.12.0/24	OSPF 1	110	15	192.0.13.2	Campus Network.Router11	IF1	N/A	32.299
13	192.0.13.0/24	Direct	0	0	192.0.13.1	Campus Network.Router12	IF1	N/A	0.000
14	192.0.14.0/24	Direct	0	0	192.0.14.2	Campus Network.Router12	IF0	N/A	0.000
15	192.0.15.0/24	OSPF 1	110	30	192.0.14.1	Campus Network.Router10	IF0	N/A	32.299
16									
17	Gateway of last resort is	not set							
18									

Figura 15. Tabla de enrutamiento del Router 12

7. Ahora, seleccione **Switch to scenario** y escoja *Ruta_alternativa.*

8. Repita los pasos 2,3,4 y 5 para generar la demanda de tráfico en este escenario entre todos los routers y analizar la ruta obtenida. En la figura 16 se puede apreciar la ruta alternativa.

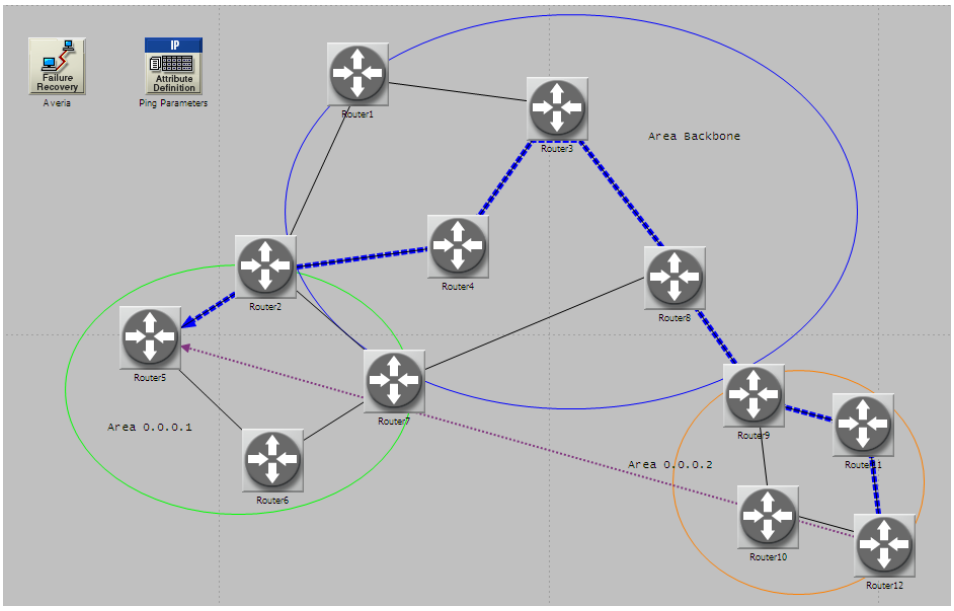


Figura 16. Ruta alternativa

9. Note en la figura 17 que el ancho de banda a través del enlace entre los Routers 7 y 8 es cero, debido a la avería que se produjo sobre el enlace. Pero, en la figura 18 se puede apreciar el ancho de banda entre los Routers 8 y 3, garantizando el flujo normal de tráfico.

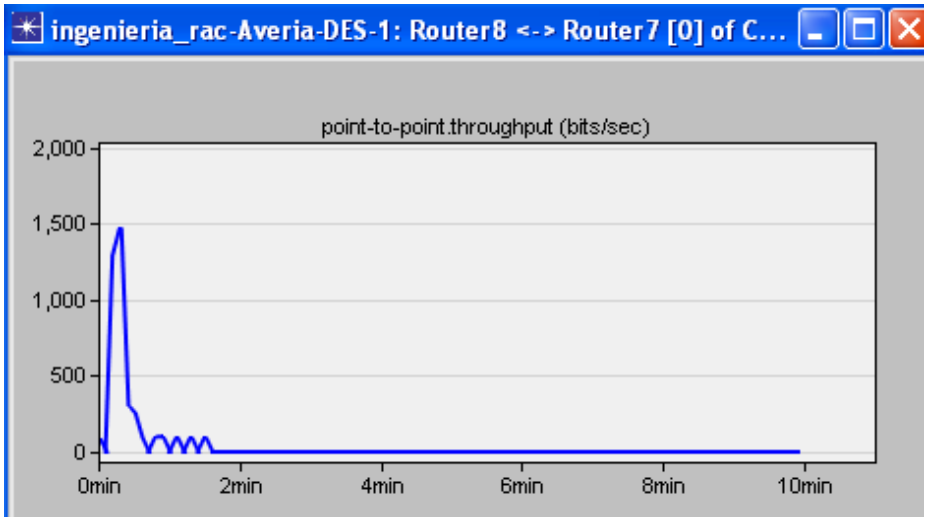


Figura 17. Ancho de banda entre los Routers 7 y 8

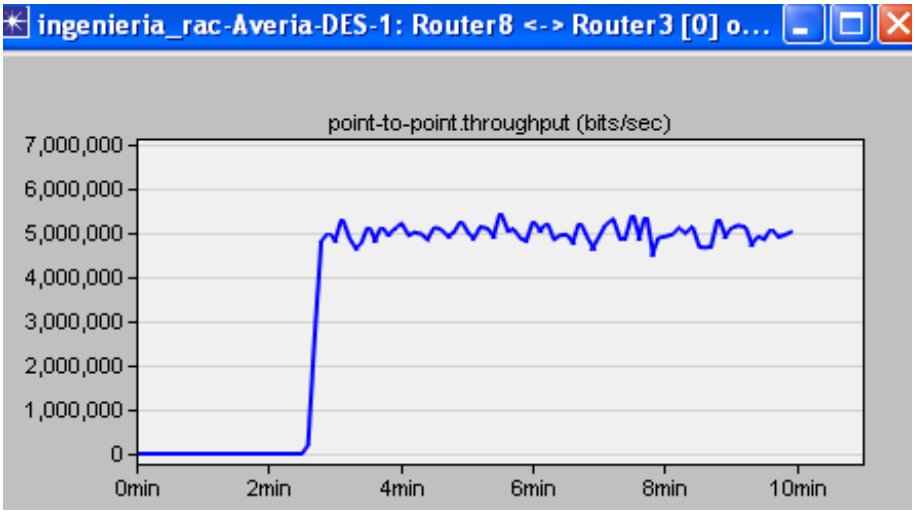


Figura 18. Ancho de banda entre los Routers 8 y 3

10. Ahora, seleccione **Switch to scenario** y escoja *Balanceo_averia.*

11. Repita los pasos 2,3,4 y 5 para generar de nuevo la demanda de tráfico en este escenario entre todos los routers y analizar la ruta obtenida. En la figura 19 se puede apreciar el balanceo de carga entre las rutas de igual costo que unen a los Routers 2 y 3.

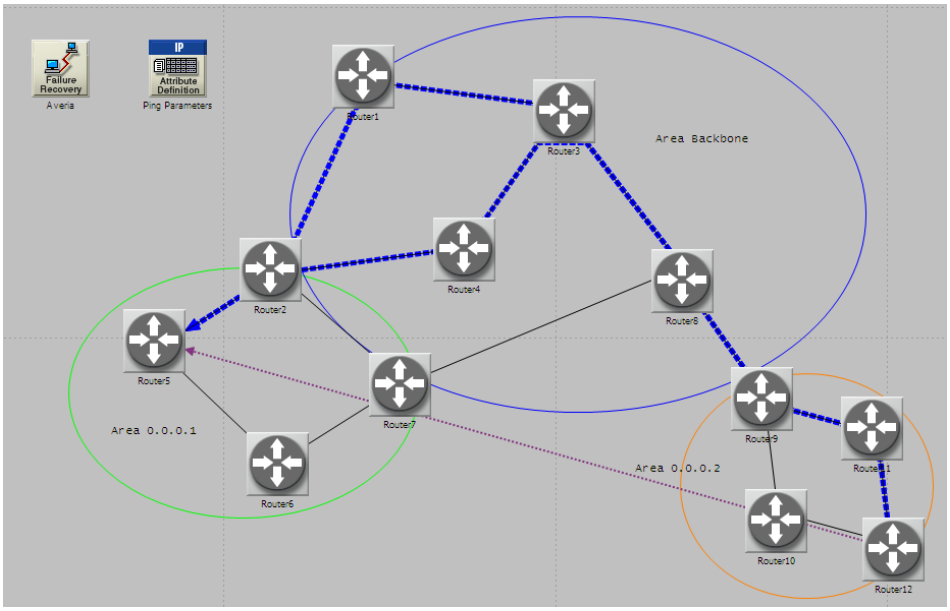


Figura 19. Balanceo de carga

12. Para analizar que efectivamente se cumple el balanceo de carga, genere las gráficas del ancho de banda entre los Routers 3 -1 y los Routers 8-3. En la figura 20 se puede apreciar esta comparación.

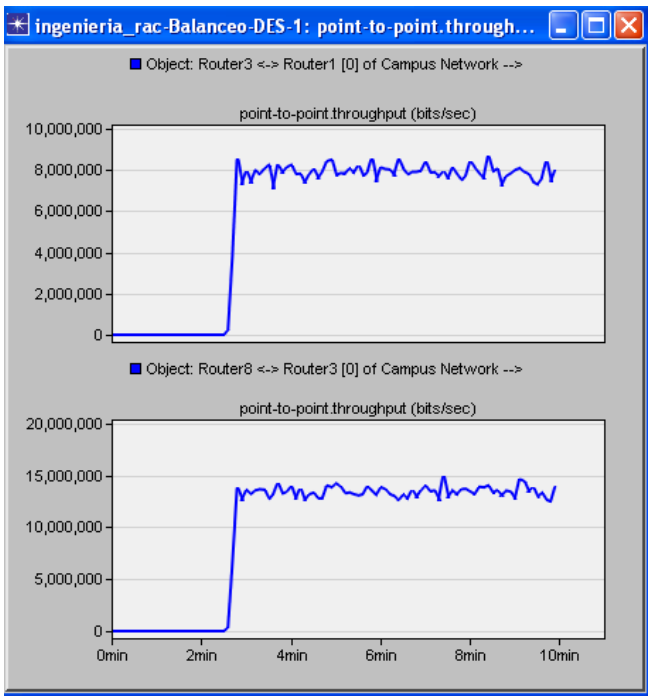


Figura 20. Comparación del ancho de banda aplicando la configuración de balanceo de carga

13. Ahora, para obtener con más detalle el análisis de balanceo de carga genere las gráficas de ancho de banda y utilización entres los Routers 3 -1 y los Routers 4 – 3. En la figura 21 se puede apreciar estas características.

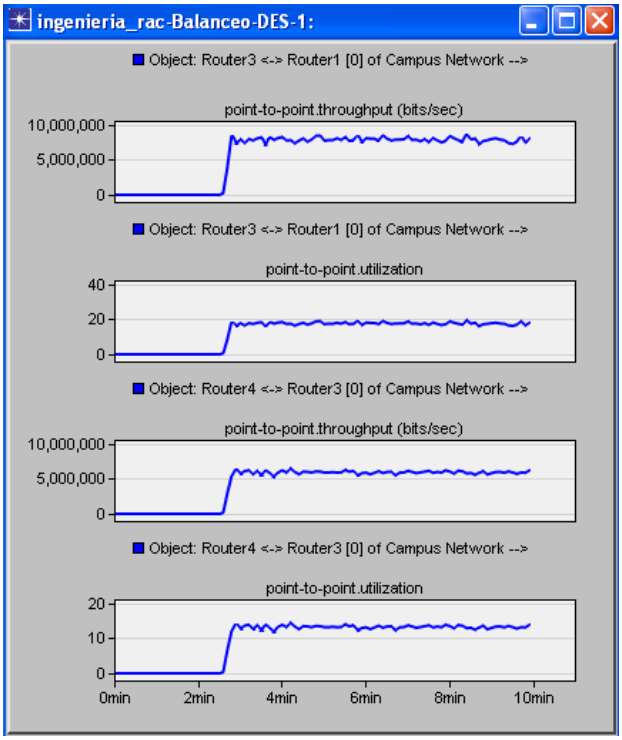


Figura 21. Utilización y ancho de banda entre los Routers 3 – 1 y los Routers 4 – 3

14. Ahora, seleccione **Switch to scenario** y escoja *Distribucion_averia.*

15. Repita los pasos 2,3,4 y 5 para generar la demanda de tráfico en este escenario entre todos los routers y analizar la ruta obtenida. En la figura 22 se puede apreciar la ruta alternativa a través de la distribución de pesos sobre los enlaces.

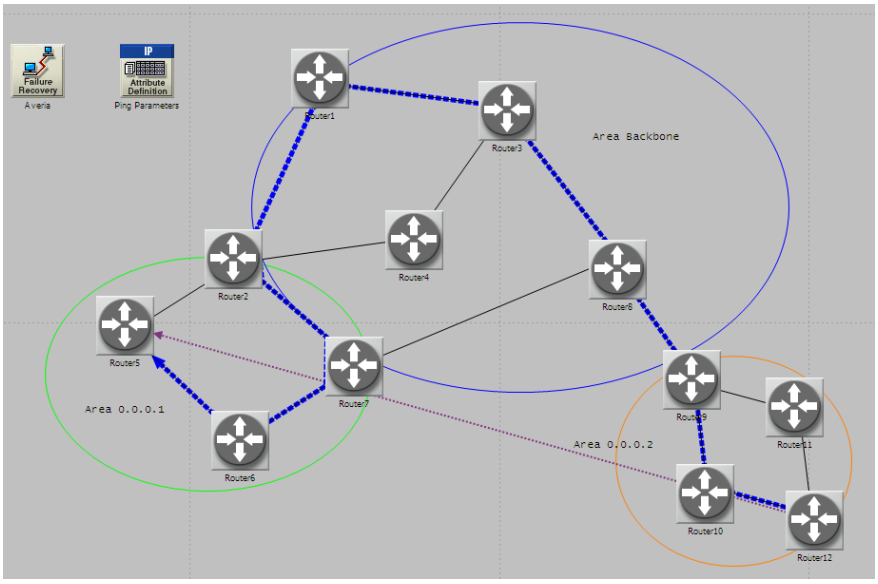


Figura 22. Ruta alternativa utilizando distribución de pesos

16. Genere las gráficas de utilización y ancho de banda entre los Routers 1 y 3. En la figura 23 se pueden apreciar estas características.

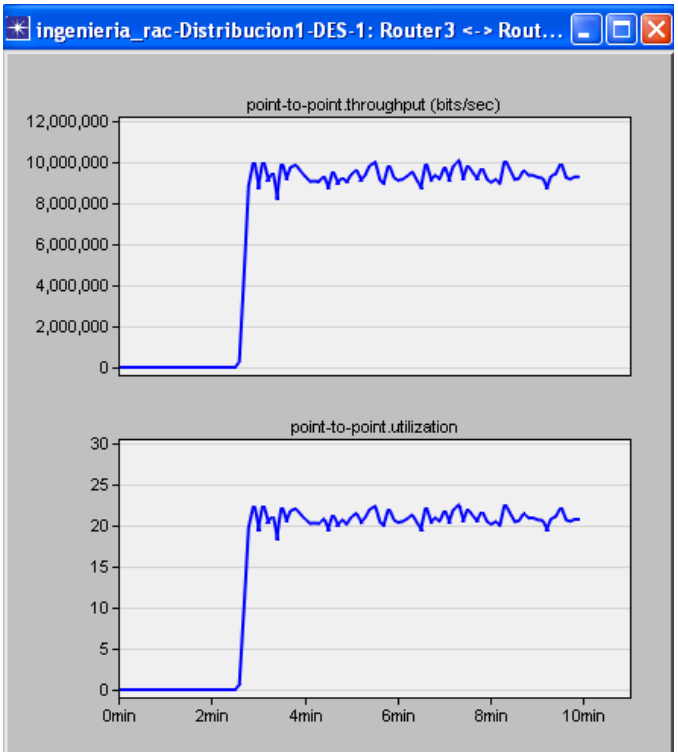


Figura 23. Utilización y ancho de banda entre los Routers 1 y 3

Trabajo en clase:

- Analice las aplicaciones (ventajas y desventajas) que se implementaron con el protocolo OSPF, como una forma de desarrollar Ingeniería de Tráfico en los 4 escenarios.

- ¿Existen más situaciones o alternativas para desarrollar Ingeniería de Tráfico con el protocolo OSPF?

- Genere y analice la tabla de enrutamiento del Router 3, para los escenarios *Balanceo_averia y Ruta_alternativa.*

- Habilite las prestaciones del protocolo OSPF para cada escenario configurando *Choose Individual DES Statistic*. Para esto despliegue *Global Statistics,* seleccione *OSPF* y corra de nuevo el programa. Analice las gráficas obtenidas.